GEOMETRIC QUADRATIC CHABAUTY OVER NUMBER FIELDS

PAVEL ČOUPEK, DAVID T.-B. G. LILIENFELDT, LUCIENA X. XIAO, ZIJIAN YAO

Dedicated to the memory of Bas Edixhoven

ABSTRACT. This article generalizes the geometric quadratic Chabauty method, initiated over $\mathbb{Q}$ by Edixhoven and Lido, to curves defined over arbitrary number fields. The main result is a conditional bound on the number of rational points on curves that satisfy an additional Chabauty type condition on the Mordell–Weil rank of the Jacobian. The method gives a more direct approach to the generalization by Dogra of the quadratic Chabauty method to arbitrary number fields.

CONTENTS

1. INTRODUCTION

1.1. **Main result.** Let C be a smooth, projective, geometrically irreducible curve of genus $g \geq 2$ defined over a number field K. Let $J := \mathrm{Pic}^0_{C/K}$ denote the Jacobian of C. Let

- $r := \mathrm{rank}_{\mathbb{Z}} J(K)$ be the Mordell–Weil rank, and
- $\rho := \mathrm{rank}_{\mathbb{Z}} \mathrm{NS}(J)$ be the rank of the Néron–Severi group of J.

Mordell's conjecture (now a theorem of Faltings [19]) asserts that the set of rational points on C is finite. Faltings' spectacular proof, however, cannot be made effective and there is no general algorithm for determining the set $C(K)$[1]. More recently, following the pioneering work of Chabauty [9], methods have been developed to explicitly determine the set of rational points on curves that satisfy certain conditions on r (commonly referred to as Chabauty type conditions). Some relevant results in this direction will be surveyed in the introduction. Let us fix a prime p where C has good reduction while satisfying some additional mild ramification conditions (see Assumption 4.1). In its crudest form, our main result is an effective bound on $C(K)$ of the following form, which generalizes the work of Edixhoven and Lido [17].

Theorem 1.1 (crude version). *Suppose that C satisfies the "quadratic Chabauty condition"*

$$(1.1) \qquad\qquad r + \delta(\rho - 1) \leq (g + \rho - 2)d,$$

[1]though recently Alpöge and Lawrence found an algorithm that terminates assuming standard conjectures (see [1, Ch. 7-9]).

where $\delta = \mathrm{rank}_{\mathbb{Z}} \mathcal{O}_K^{\times}$ and d is the degree of K. Let $R := \mathbb{Z}_p\langle z_1, ..., z_{r+\delta(\rho-1)}\rangle$ be the p-adically completed polynomial algebra over $\mathbb{Z}_p$. There exists an ideal I of R, which is explicitly computable mod p, such that if $\overline{A} := (R/I) \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ is finite dimensional over $\mathbb{F}_p$, then the set of rational points $C(K)$ is finite, and its cardinality is bounded by $\dim_{\mathbb{F}_p} \overline{A}$.

Remark 1.2. The precise form of this theorem (Corollary 6.3) is slightly more involved. As in the work of Edixhoven and Lido, we need to work integrally with a regular proper model $\mathbf{C}$ of C over $\mathcal{O}_K$ and cover the smooth locus $\mathbf{C}^{\mathrm{sm}}$ by certain open subschemes $\mathbf{U}_i$. More precisely, for each p-adic residue disk of $\mathbf{U}_i$ (indexed by the residue points $u \in \mathbf{U}_i(\mathcal{O}_K \otimes \mathbb{F}_p)$), we produce a bound on the size of $\mathbf{U}_i(\mathcal{O}_K)_u$ by constructing an ideal $I_{i,u} \subset R$. The bound on the size of $C(K)$ is then obtained by summing the bounds for each i and u.

1.2. **Effective methods over $\mathbb{Q}$.** To put our result into context, we give a brief overview of some of the existing effective methods.

1.2.1. *The Chabauty–Coleman method.* If the Mordell–Weil rank r of the Jacobian J of C satisfies the inequality $r < g$, then the work of Chabauty [9] and Coleman [10] can be used to give upper bounds on the size of $C(K)$, and in many cases, to explicitly compute the set of rational points. Their method works over general number fields, but let us take $K = \mathbb{Q}$ to explain their strategy. Upon choosing a sufficiently large prime p of good reduction, one obtains a homomorphism

$$\log_p : J(\mathbb{Q}_p) \longrightarrow H^0(C_{\mathbb{Q}_p}, \Omega^1)^{\vee} \simeq H^0(J_{\mathbb{Q}_p}, \Omega^1)^{\vee}$$

using Coleman integration (see [11] for details). The Abel–Jacobi map $j_b : C \hookrightarrow J$, which relies on a fixed base point $b \in C(\mathbb{Q})$, leads to the following commutative diagram:

(1.2)
$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) \\ \downarrow{\scriptstyle j_b} & & \downarrow{\scriptstyle j_b} \quad \searrow{\scriptstyle \int} \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) \xrightarrow{\log_p} H^0(C_{\mathbb{Q}_p}, \Omega^1)^{\vee}. \end{array}$$

The Chabauty condition $r < g$ guarantees that the closure $\overline{J(\mathbb{Q})}^p$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with respect to the p-adic topology has positive codimension. In particular, there exists a nontrivial differential form ω for which $\log_p(\omega)$ vanishes on $\overline{J(\mathbb{Q})}^p$. Roughly, on each residue disk of the curve C, the Coleman integral $\log_p(\omega) \circ j_b = \int \omega$ is given by a convergent p-adic power series and has only finitely many zeros. Since it vanishes on $C(\mathbb{Q})$, this set is finite. Moreover, using Newton polygons, Coleman [10] was able to count the number of zeros of these p-adic power series and prove, when $p > 2g$, that

$$|C(\mathbb{Q})| \leq |C(\mathbb{F}_p)| + (2g - 2).$$

1.2.2. *Quadratic Chabauty.* The tantalizing non-abelian Chabauty program, initiated by Kim [28,29], aims to relax the Chabauty condition $r < g$ by considering non-abelian variants of the objects in Section 1.2.1. To this end one first reinterprets the diagram (1.2) above using the Bloch–Kato Selmer groups $H_f^1(\mathbb{Q}, V)$ (resp. $H_f^1(\mathbb{Q}_p, V)$) in place of $J(\mathbb{Q})$ (resp. $J(\mathbb{Q}_p)$) via the Kummer maps, where $V := V_p J$ denotes the p-adic Tate module of J. The logarithm map above is essentially the inverse of the Bloch–Kato exponential

$$H^0(C_{\mathbb{Q}_p}, \Omega^1)^{\vee} \simeq \mathrm{D}_{\mathrm{dR}}(V)/\mathrm{D}_{\mathrm{dR}}^+(V) \xrightarrow{\exp} H_f^1(\mathbb{Q}_p, V).$$

Next one replaces V by certain pro-unipotent quotients U_n of the étale fundamental group $\pi_1^{\mathrm{ét}}(C_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, one for each $n \geq 1$, which again carry a continuous Galois action. Kim then defines a certain Selmer

subgroup $\mathrm{Sel}(U_n) \subset H^1_f(\mathbb{Q}, U_n)$, and upgrades the previous diagram to the following one:

$$
\begin{array}{ccc}
C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) \\
\downarrow{\scriptstyle j_n} & & \downarrow{\scriptstyle j_{n,p}} \quad\searrow^{\textstyle \int} \\
\mathrm{Sel}(U_n) \xrightarrow{\ \mathrm{loc}_p\ } & H^1_f(\mathbb{Q}_p, U_n) \xrightarrow{\ \mathrm{loc}_n\ } & \pi_1^{\mathrm{dR}}(C_{\mathbb{Q}_p})_n/\mathrm{Fil}^0.
\end{array}
$$

Here the vertical maps j_n and $j_{n,p}$ are Kim's unipotent Kummer maps. Define the (nested) sets

$$
C(\mathbb{Q}_p)_n := j_{n,p}^{-1}\big(\mathrm{loc}_p(\mathrm{Sel}(U_n))\big) \subset C(\mathbb{Q}_p),
$$

which contain $C(\mathbb{Q})$ and satisfy $C(\mathbb{Q}_p)_{n+1} \subset C(\mathbb{Q}_p)_n$. For sufficiently large n, Kim conjectures that $C(\mathbb{Q}_p)_n$ is finite and even coincides with $C(\mathbb{Q})$. The set $C(\mathbb{Q}_p)_1$ is the one studied in the Chabauty–Coleman method in Section 1.2.1. The first non-abelian instance of Kim's program (namely the quadratic case where $n = 2$) has been carried out quite successfully by Balakrishnan, Dogra, and their collaborators (see [3–5] and the references therein). In particular, they show that if the Mordell–Weil rank r satisfies $r < g + \rho - 1$, then $C(\mathbb{Q}_p)_2$ is finite and can often be explicitly determined. This method has been applied to determine the rational points of the "cursed curve" in [6] by Balakrishnan, Dogra, Müller, Tuitman, and Vonk, which completes the classification of non-CM elliptic curves over $\mathbb{Q}$ of split Cartan type.

1.3. **Geometric quadratic Chabauty (over $\mathbb{Q}$).** Recently, Edixhoven and Lido have explored in [17] a different, and arguably more direct, approach to quadratic Chabauty. Their method is referred to as the geometric quadratic Chabauty method (with an emphasis on geometric), and works under the same condition $r < g + \rho - 1$ as in Section 1.2.2. It has the advantage of avoiding the consideration of iterated Coleman integrals and the analysis of certain complicated p-adic heights. The strategy of Edixhoven and Lido is close in spirit to the original idea of Chabauty: their idea is to replace the Jacobian J by a certain $\mathbb{G}_m^{\rho-1}$-torsor T over J in order to relax the condition $r < g$. This torsor comes equipped, by construction, with a lift $\tilde{j}_b : C \longrightarrow T$ of the Abel–Jacobi map. Upon choosing a prime p of good reduction, one obtains the following diagram

(1.3)
$$
\begin{array}{ccc}
C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) \\
\downarrow{\scriptstyle \tilde{j}_b} & & \downarrow{\scriptstyle \tilde{j}_b} \\
T(\mathbb{Q}) \longrightarrow & \overline{T(\mathbb{Q})}^p \longrightarrow & T(\mathbb{Q}_p),
\end{array}
$$

where $\overline{T(\mathbb{Q})}^p$ denotes the closure of $T(\mathbb{Q})$ in $T(\mathbb{Q}_p)$ with respect to the p-adic topology. In practice, they need to work with certain integral versions of the above objects and diagrams over $\mathrm{Spec}(\mathbb{Z})$ (see Remark 1.3). The method then consists in bounding the size of the intersection

(1.4)
$$
\tilde{j}_b^{-1}\big(\overline{T(\mathbb{Z})}^p \cap \tilde{j}_b(C(\mathbb{Z}_p))\big),
$$

which contains the set of rational points. Using this method, Edixhoven and Lido are able to reprove Faltings' theorem for curves defined over $\mathbb{Q}$ satisfying $r < g + \rho - 1$. Furthermore, they have made their method effective and successfully used it to compute the rational points on the quotient of the modular curve $X_0(129)$ by the Atkin–Lehner group $\langle w_3, w_{43}\rangle$.

Remark 1.3. The reason for working with integral models is that the torsor T has too many rational points (its fiber over J is $\mathbb{G}_m^{\rho-1}$). More precisely, one starts with a regular proper integral model $\mathbf{C}$ of C, and further restricts to open subschemes on which the Abel–Jacobi map can be lifted integrally (as mentioned in Remark 1.2).

1.4. **Effective methods over number fields.** The methods summarized so far deal with curves defined over $\mathbb{Q}$ satisfying Chabauty type conditions, for example,

$$\begin{cases} r < g & \text{(Chabauty condition)} \\ r < g + \rho - 1 & \text{(quadratic Chabauty condition).} \end{cases}$$

Next we briefly review some recent developments in generalizing the methods in Section 1.2 to curves over arbitrary number fields.

1.4.1. *The Chabauty–Coleman method.* As remarked earlier, the Chabauty–Coleman method works over an arbitrary number field K. In fact, Coleman already works at this level of generality in [10].

1.4.2. *The Restriction of Scalars (RoS) Chabauty method.* In [32], Siksek extends the Chabauty–Coleman method by studying the Weil restrictions from K to $\mathbb{Q}$ of the curve C and its Jacobian J. In this way Siksek reduces the problem to working entirely over $\mathbb{Q}$ at the cost of considering higher dimensional varieties. Siksek's method, known as Restriction of Scalars (RoS) Chabauty, requires the RoS Chabauty condition $r \leq (g-1)d$, where $d = [K : \mathbb{Q}]$ is the degree of K. Note, however, that this method can fail to produce a bound on the number of rational points even if the condition $r \leq (g-1)d$ is satisfied. Examples include the case where the curve C is the base change of a curve C' defined over $\mathbb{Q}$, which does not satisfy the Chabauty condition $\mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}(C') < g$. Aware of this, Siksek asks in [32] whether a sufficient condition for his method to prove finiteness is that for all extensions $\mathbb{Q} \subset L \subset K$ over which C admits a good model C_L, we should have

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{Jac}(C_L) \leq (g-1)[L : \mathbb{Q}].$$

Failures of the method of RoS Chabauty have been studied by Triantafillou [35], who introduces Base-Change-Prym (BCP) obstructions, which account for all known failures to date.

1.4.3. *RoS quadratic Chabauty.* More recently, Dogra [15] combines ideas of the RoS Chabauty method with Kim's non-abelian Chabauty program. This has led to a generalization of Kim's program to arbitrary number fields. As in Section 1.2.2, he obtains (nested) Chabauty–Kim sets $C(K_{\mathfrak{p}})_n$ for $\mathfrak{p} \mid p$, indexed by $n \in \mathbb{Z}_{\geq 1}$. Dogra provides a negative answer to Siksek's question using a BCP obstruction. Assuming p is a split prime of good reduction, he also gives a sufficient condition for there to exist a prime $\mathfrak{p} \mid p$ such that $C(K_{\mathfrak{p}})_1$ is finite under the Chabauty condition $r \leq (g-1)d$: namely that

$$(1.5) \qquad \mathrm{Hom}(J_{\bar{\mathbb{Q}},\sigma_1}, J_{\bar{\mathbb{Q}},\sigma_2}) = 0 \text{ for any two distinct embeddings } \sigma_1, \sigma_2 : K \hookrightarrow \bar{\mathbb{Q}}.$$

Moreover, his results imply that if in addition to Condition (1.5) the quadratic (RoS) Chabauty condition (1.1) as in our main theorem is satisfied, then there exists $\mathfrak{p} \mid p$ such that $C(K_{\mathfrak{p}})_2$ is finite. The work of Dogra sets the theoretical stage for the quadratic RoS Chabauty method, which has been made effective recently by Balakrishnan, Besser, Bianchi, and Müller in [2] for odd degree hyperelliptic curves and genus 2 bielliptic curves.

1.5. **Overview of the geometric method.** Next we explain the proof of Theorem 1.1. Following suggestions by the referee, we first describe the geometric method in a more general setup. Our main theorem can then be viewed as carrying out this method in a special case. To this end, let X_K be a proper variety over a number field K which admits a regular proper model $\mathbf{X}$ over $\mathcal{O}_K$. The key idea from [17] is to replace the Jacobian in Chabauty's original approach by something higher dimensional. To phrase their approach in a more general setup, let us *assume* that we are given closed embeddings

$$X_K \xrightarrow{j} J_K \xrightarrow{f} A_K \times B_K$$

where J_K, A_K, B_K are abelian varieties and f is a homomorphism. Let us further *assume* that there is a G_K-biextension F_K of (A_K, B_K) where G_K is a torus, such that the map j lifts to an embedding $\tilde{j} : X_K \to Q_K$, where Q_K is the G_K-torsor over J_K obtained as the pullback of F_K along f:

(1.6)
$$
\begin{array}{ccc}
& Q_K \longrightarrow F_K \\
\tilde{j} \nearrow & \downarrow \quad \square \quad \downarrow \\
X_K \xrightarrow{\ j\ } J_K \xrightarrow{\ f\ } A_K \times B_K.
\end{array}
$$

In view of Remark 1.3, we *assume* that the diagram above spreads out over $\mathcal{O}_K$:

(1.7)
$$
\begin{array}{ccc}
& \mathbf{Q} \longrightarrow \mathbf{F} \\
\tilde{j} \nearrow & \downarrow \quad \square \quad \downarrow \\
\mathbf{X} \xrightarrow{\ j\ } \mathbf{J} \xrightarrow{\ f\ } \mathbf{A} \times \mathbf{B}^\circ.
\end{array}
$$

Here the abelian varieties A_K, J_K (resp. B_K) are replaced by their Néron models (resp. the connected component of identity of its Néron model), and $\mathbf{F}$ is the (unique) $\mathbf{G}$-biextension of $(\mathbf{A}, \mathbf{B}^\circ)$ where $\mathbf{G}$ is the Néron–Raynaud model of G_K.

Remark 1.4. In practice, we often have to replace $\mathbf{X}$ by a Zariski open cover $\mathbf{U}_i$ of $\mathbf{X}^{\mathrm{sm}}$ (where $\mathbf{X}^{\mathrm{sm}}$ denotes the smooth locus in $\mathbf{X}$), and work with one $\mathbf{U}_i$ at a time.

For a prime p of good reduction for $\mathbf{X}$, we let $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\overline{\mathcal{O}_{K,p}} := (\mathcal{O}_K \otimes \mathbb{F}_p)_{\mathrm{red}}$. Working residue disk by residue disk, we fix $u \in \mathbf{X}(\overline{\mathcal{O}_{K,p}})$ and $t = \tilde{j}(u) \in \mathbf{Q}(\overline{\mathcal{O}_{K,p}})$. Consider the following commutative quadratic Chabauty diagram on residue disks:

(1.8)
$$
\begin{array}{ccc}
\mathbf{X}(\mathcal{O}_K)_u & \longrightarrow & \mathbf{X}(\mathcal{O}_{K,p})_u \\
\downarrow{\scriptstyle \tilde{j}} & & \downarrow{\scriptstyle \tilde{j}} \\
\mathbf{Q}(\mathcal{O}_K)_t \longrightarrow \mathbf{Y}_t & \longrightarrow & \mathbf{Q}(\mathcal{O}_{K,p})_t.
\end{array}
$$

Here $\mathbf{Y}_t := \overline{\mathbf{Q}(\mathcal{O}_K)_t}^p$ is the closure of $\mathbf{Q}(\mathcal{O}_K)_t$ in $\mathbf{Q}(\mathcal{O}_{K,p})_t$ for the p-adic topology. The points in $X_K(K) = \mathbf{X}(\mathcal{O}_K)$ that reduce to u modulo p are contained in the intersection $\tilde{j}(\mathbf{X}(\mathcal{O}_{K,p}))_u \cap \mathbf{Y}_t$, which is often computable. The framework to explicitly determine this intersection can be described as follows: using the structure of the rational points on J_K and the $\mathbf{G}$-torsor structure of $\mathbf{Q} \to \mathbf{J}$, one constructs a certain "coordinate map" $\mathbb{Z}^m \to \mathbf{Q}(\mathcal{O}_K)_t$, from which one can build a map $\kappa : \mathbb{Z}_p^m \twoheadrightarrow \mathbf{Y}_t$ between p-adic analytic spaces, where $m = \mathrm{rank}_{\mathbb{Z}} J_K(K) + \mathrm{rank}_{\mathbb{Z}} \mathbf{G}(\mathcal{O}_K)$. The map κ is then used to give effective bounds on the intersection $\tilde{j}(\mathbf{X}(\mathcal{O}_{K,p})_u) \cap \mathbf{Y}_t$ when it is finite. In the next subsection, we explain this procedure in more detail for the primary example treated in this article, namely when X_K is a higher genus curve over K.

Remark 1.5. While in principle we expect the method of this article to work whenever we are given the setup as in diagram (1.7), in practice is seems rare to find such a lift $\tilde{j}$. This is the main reason why we choose to treat only the case when X_K is a higher genus curve. For example, in [8] a Chabauty–Coleman type bound was proved for hyperbolic surfaces contained in abelian varieties. However, for a hyperbolic surface contained in a principally polarized abelian variety, we do not know how to construct a torsor which fits in (the analogue of) Diagram (1.7).

1.6. **Higher genus curves over number fields.** Let C_K be a curve of genus ≥ 2 over K and consider a regular proper model $\mathbf{C}$ of C_K over $\mathcal{O}_K$. In this case, we will produce Diagram (1.7) by considering the Poincaré bundle over $J_K \times J_K^\vee$ where J_K denotes the Jacobian of C_K. In order to produce the desired lift $\tilde{j}_b$ (dependent on a base point $b \in C_K(K)$), we in fact consider the $(\rho - 1)$-fold self-product of the Poincaré bundle over J_K, where ρ is the Néron–Severi rank. Our map $J_K \to J_K \times J_K^\vee$ in diagram (1.6) depends on a choice of (sub-)basis of the Néron–Severi group, and

is obtained by translating these basis elements by certain points of $J_K^\vee(K)$ that are closely related to Chow–Heegner points (see Section 3.1 and Remark 3.3). With this carefully chosen map, we obtain a $\mathbb{G}_m^{\rho-1}$-torsor T_K over J_K, which spreads out to a $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$, the latter being the Néron model of J_K. The construction of $\mathbf{T}$ allows us to lift the Abel–Jacobi map $j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$ to a map[2]

$$\tilde{j}_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{T}$$

as required by Diagram (1.7). Fixing $u \in \mathbf{C}^{\mathrm{sm}}(\overline{\mathcal{O}_{K,p}})$ and letting $t := \tilde{j}_b(u) \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$, we thus arrive at the following commutative diagram on residue disks:

(1.9)
$$
\begin{array}{ccc}
\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)_u & \longrightarrow & \mathbf{C}^{\mathrm{sm}}(\mathcal{O}_{K,p})_u \\
\downarrow{\scriptstyle \tilde{j}_b} & & \downarrow{\scriptstyle \tilde{j}_b} \\
\mathbf{T}(\mathcal{O}_K)_t & \longrightarrow \mathbf{Y}_t \longrightarrow & \mathbf{T}(\mathcal{O}_{K,p})_t.
\end{array}
$$

The key of the approach is to analyze the p-adic closure $\mathbf{Y}_t$ of the $\mathcal{O}_K$-points of the torsor $\mathbf{T}$ reducing to t modulo p. If $K = \mathbb{Q}$, this can be done by parametrizing the p-adic closure of $\mathbf{J}(\mathbb{Z}) = J(\mathbb{Q})$, as $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. This is a major simplification and essentially why [17] decided to work over $\mathbb{Q}$. In fact, it was suggested to us by Edixhoven and Lido that a restriction of scalars approach might reduce the case of general number fields K back to the case of $\mathbb{Q}$. In this work, however, we decide to take a more direct approach, which departs from the RoS arguments of [2, 15, 32] (see Remark 1.9 below). One of the main observations is that one can fully utilize the $\mathbb{G}_m$-action on the fibers of the torsor $\mathbf{T} \longrightarrow \mathbf{J}$ to parametrize $\mathbf{Y}_t$, which is sufficient for the purpose of this paper. Roughly, we pick a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^r \longrightarrow \mathbf{T}(\mathcal{O}_K)_t$, essentially by choosing a basis for the Mordell–Weil group $J_K(K)$. We then use the $\mathbb{G}_m$-action to propagate these coordinates to get a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)_t$. Finally, interpolating these coordinates p-adically allows us to parametrize $\mathbf{Y}_t$ via a surjective map

$$\kappa : \mathbb{Z}_p^{\delta(\rho-1)+r} \twoheadrightarrow \mathbf{Y}_t,$$

which turns out to be given by convergent p-adic power series. The ideal I in Theorem 1.1 is built such that the cardinality of $\mathrm{Spec}(R/I)(\mathbb{Z}_p)$ is the size of $\kappa^{-1}(\mathbf{Y}_t \cap \tilde{j}_b(\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_{K,p})_u))$. In particular, in order for the method to effectively determine the rational points on C_K, we need to choose a prime p such that

- $\mathbf{Y}_t \cap \tilde{j}_b(\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_{K,p})_u)$ is finite, and
- κ is finite-to-one on $\kappa^{-1}(\mathbf{Y}_t \cap \tilde{j}_b(\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_{K,p})_u))$.

This observation prompts the following question (see Section 7):

Question 1.6. *Let p be a prime of good reduction for $\mathbf{C}$. What conditions would guarantee that the intersection $\mathbf{Y}_t \cap \tilde{j}_b(\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_{K,p})_u)$ is finite?*

Remark 1.7. There are some further caveats hidden from the overview above. For example, as hinted at in Remark 1.2, in order to obtain the lift $\tilde{j}_b : \mathbf{C}^{\mathrm{sm}} \to \mathbf{T}$, we need to restrict to certain open subschemes $\mathbf{U}_i$ of $\mathbf{C}^{\mathrm{sm}}$. The details of these complications are spread throughout the article (see for instance Sections 3.1 and 5.1).

Remark 1.8. As our approach has a theoretical component (the geometric method) and an effective component, it is appropriate to distinguish between the required Chabauty type conditions. The requirement for the geometric method is the condition (1.1), called the geometric quadratic Chabauty condition. Effectiveness relies on the map κ being finite-to-one, for which we need to (at least) impose the additional condition $\dim \mathbf{Y}_t = r + \delta(\rho - 1)$. The combination of the two conditions is the "effective geometric quadratic Chabauty condition". We refer to Section 7 for further details.

---

[2]upon replacing $\mathbf{C}^{\mathrm{sm}}$ by a certain Zariski open cover

Remark 1.9 (Restriction of scalars)**.** In our approach we work with all primes of K above p simultaneously (similar to the work of Siksek). If we were to work with a single fixed prime over p, the method would only have a chance of working if the following condition was satisfied:

$$r + \delta(\rho - 1) < g + \rho - 1.$$

When K is imaginary quadratic, this amounts to the same quadratic Chabauty condition as over $\mathbb{Q}$. However, if K is real quadratic, the condition becomes $r < g$ and the Chabauty–Coleman method can already be applied. When considering higher degree number fields, the above condition is more restrictive than the classical Chabauty condition. Therefore, it seems necessary to work with all primes above p simultaneously in order to study curves satisfying Condition (1.1). This comes as no surprise, as Condition (1.1) coincides with the condition coming from Dogra's quadratic RoS Chabauty method, which also involves all primes above p. However, the present generalization of the geometric quadratic Chabauty method does not make use of restriction of scalars in the same way as the RoS methods of Siksek and Dogra. While they use Weil restrictions to reduce the geometric situation to working over $\mathbb{Q}$, we work directly over K, and even integrally over $\mathcal{O}_K$. Only at the end of the argument do we apply a restriction of scalars and work with all primes above p simultaneously. More conceptually, the method of this paper is equivalent to applying the general geometric method described in Section 1.5 to the situation over $\mathbb{Q}$ with $X_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(C_K)$, $J_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(J_K)$, $Q_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(T_K)$, $A_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(J_K)$, $B_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(J_K)^{\vee, \rho - 1}$, and $F_{\mathbb{Q}} := \operatorname{Res}_{K/\mathbb{Q}}(P_K^{\times})^{\rho - 1}$. Here T_K is the special torsor mentioned in Section 1.6 and constructed in Section 3, and $P_K^{\times}$ denotes the Poincaré $\mathbb{G}_m$-biextension of $(J_K, J_K^{\vee})$ (see Section 2.1.3). In contrast, a perhaps more natural approach to geometric quadratic Chabauty via restriction of scalars would have been to consider F_K to be the Poincaré $\mathbb{G}_m$-biextension of $(\operatorname{Res}_{K/\mathbb{Q}}(J), \operatorname{Res}_{K/\mathbb{Q}}(J_K)^{\vee})$, or a power thereof. This was the approach originally suggested to us by Edixhoven and Lido. However, it seems difficult in this case to produce the diagrams (1.6) and (1.7) required for the geometric method of Section 1.5.

Remark 1.10 (p-saturation)**.** In [22, Theorem 4.1], Hashimoto and Spelier prove that (a linear version of) geometric Chabauty strictly outperforms Chabauty–Coleman, at least theoretically, although it is more difficult to implement for explicit examples. The reason is essentially that Chabauty–Coleman computes the p-saturation of the set computed in geometric (linear) Chabauty. Similarly, the geometric quadratic Chabauty method (both over $\mathbb{Q}$ and over number fields) is likely to remain unaffected by questions of p-saturation.

1.7. **Outline.** In Section 2, we recall the necessary background on the Poincaré torsor, from which we build the torsor T_K over J_K. We then spread out the geometry from $\operatorname{Spec} K$ to $\operatorname{Spec} \mathcal{O}_K$. In Section 3, we construct the torsor **T**. Section 4 makes the strategy of the geometric quadratic Chabauty method precise. We then state the main technical results of this article and discuss how the condition (1.1) arises. In Section 5, which is the technical core of the paper, we parametrize the p-adic closure $\mathbf{Y}_t$ of the rational points $\mathbf{T}(\mathcal{O}_K)_t$ by a p-adic interpolation argument. We complete the proof of the main theorem in Section 6. Some questions are discussed in Section 7, including Question 1.6 raised above.

1.8. **Notation.** For the convenience of the reader we provide a list of notations used in the main body of the paper. We have chosen to use notations similar to [17] in order to facilitate the comparison with the original approach over $\mathbb{Q}$.

- $K/\mathbb{Q}$ is a number field of degree $d = r_1 + 2r_2$, where r_1 and r_2 are respectively the number of real embeddings and pairs of complex embeddings of K.
- $\mathcal{O}_K$ denotes the ring of integers of K.
- $\delta = r_1 + r_2 - 1$ is the rank of the unit group $\mathcal{O}_K^{\times}$.
- $h = \operatorname{cl}(\mathcal{O}_K)$ is the class number of $\mathcal{O}_K$.
- C_K is a smooth, proper, and geometrically connected curve over K of genus $g \geq 2$.

- $J_K = \mathrm{Pic}^0_{C_K/K}$ is the Jacobian of C_K. It is an abelian variety of dimension g over K.
- $J_K^\vee = \mathrm{Pic}^0_{J_K/K}$ is the dual abelian variety of J_K.
- $P_K^\times \longrightarrow J_K \times J_K^\vee$ is the Poincaré torsor. It is a biextension of J_K and $J_K^\vee$ by $\mathbb{G}_m$.
- $\mathbf{C}$ is a regular proper model of C_K over $\mathcal{O}_K$ that we fix in this article.
- $\mathbf{J}$ is the Néron model of J_K over $\mathcal{O}_K$.
- $\mathbf{J}^\vee$ is the Néron model of $J_K^\vee$ over $\mathcal{O}_K$.
- $\mathbf{J}^{\vee,\circ}$ is the fiber-wise connected component of 0 of $\mathbf{J}^\vee$.
- $\mathbf{P}^\times \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}$ is the unique biextension of $\mathbf{J}$ and $\mathbf{J}^{\vee,\circ}$ by $\mathbb{G}_m$ whose base change to K is the Poincaré torsor.
- $j_b : C_K \longrightarrow J_K$ is the Abel–Jacobi map associated to a choice of point $b \in C_K(K)$.
- $r = \mathrm{rank}_\mathbb{Z} J_K(K)$ is the Mordell–Weil rank over K.
- $\rho = \mathrm{rank}_\mathbb{Z} \mathrm{NS}_{J_K/K}(K)$ is the rank of the Néron–Severi group of J_K over K.

2. The Poincaré biextension

We define the key geometric object studied in this article, namely the Poincaré torsor, along with its biextension structure, and explain how to spread out the geometry to $\mathrm{Spec}\, \mathcal{O}_K$.

2.1. The Poincaré biextension over K.

2.1.1. *The Poincaré bundle.* Let C_K be a smooth, proper, geometrically connected curve of genus $g \geq 2$ defined over K with $C_K(K) \neq \emptyset$. Let $J_K := \mathrm{Pic}^0_{C_K/K}$ be its Jacobian, that is, the connected component of the identity of the Picard scheme $\mathrm{Pic}_{C_K/K}$. This is an abelian variety of dimension g defined over K. We denote its zero section by $0 \in J_K(K)$, or alternatively by $e : \mathrm{Spec}\, K \longrightarrow J_K$. Consider the Picard scheme $\mathrm{Pic}_{J_K/K}$ over K as the contravariant functor from the category of K-schemes to abelian groups given by

$$(2.1) \qquad\qquad T \mapsto \mathrm{Pic}(J_K \times T)/\, \mathrm{pr}_T^* \mathrm{Pic}(T),$$

where $\mathrm{pr}_T : J_K \times T \longrightarrow T$ is the base-change of the structure morphism $J_K \longrightarrow \mathrm{Spec}\, K$. Denote by $J_K^\vee := \mathrm{Pic}^0_{J_K/K}$ the dual abelian variety of J_K, which comes equipped with a canonical principal polarization $\lambda : J_K \xrightarrow{\sim} J_K^\vee$, given by translating the theta divisor. The functor described by (2.1) is isomorphic to the functor given by

$$T \mapsto \{ \text{ isomorphism classes of rigidified line bundles } (L, \alpha) \text{ on } J_K \times T \,\}.$$

Here a rigidification of the line bundle L is an isomorphism $\alpha : \mathcal{O}_T \xrightarrow{\sim} e_T^* L$, where the section $e_T : T \longrightarrow J_K \times T$ is the one induced by e. Let (P_K, ν) denote the universal rigidified line bundle over $J_K \times \mathrm{Pic}_{J_K/K}$. It satisfies the following universal property: if (L, α) is a rigidified line bundle on $J_K \times T$ the zero section e, then there is a unique morphism $g : T \longrightarrow \mathrm{Pic}_{J_K/K}$ such that $(L, \alpha) \simeq (\mathrm{id}_{J_K} \times g)^*(P_K, \nu)$. The Poincaré bundle of J_K is the restriction of the universal line bundle P_K to $J_K \times J_K^\vee$ equipped with its canonical rigidification ν, which we denote again by P_K by a slight abuse of notation. The canonical rigidification of the Poincaré bundle gives rise to an isomorphism $\nu : \mathcal{O}_{J_K^\vee} \xrightarrow{\sim} P_K|_{\{0\} \times J_K^\vee}$. Let 0 denote the identity of the abelian variety $J_K^\vee$. There is a unique rigidification $\nu' : \mathcal{O}_{J_K} \xrightarrow{\sim} P_K|_{J_K \times \{0\}}$, such that ν and ν' agree at the origin $(0,0)$ in $(J_K \times J_K^\vee)(K)$. As a consequence, (P_K, ν, ν') is a birigidified line bundle on $J_K \times J_K^\vee$ with respect to the identity elements.

2.1.2. *The Poincaré torsor.* Recall that given a line bundle L on a scheme X, its associated $\mathbb{G}_m$-torsor is $L^\times := \mathbf{Isom}_X(\mathcal{O}_X, L)$, which is equipped with a free and transitive action of $\mathbb{G}_m$. Note that $L^\times$ is Zariski locally trivial. In particular, it is represented by a scheme over X which we again denote by $L^\times$ by slight abuse of notation (concretely, $L^\times$ is locally obtained by deleting the zero section of L). The Poincaré torsor $P_K^\times$ is the $\mathbb{G}_m$-torsor on $J_K \times J_K^\vee$ associated to the

Poincaré bundle P_K. Again, we denote by $P_K^\times$ the scheme represented by the Poincaré torsor and denote by $j_K : P_K^\times \longrightarrow J_K \times J_K^\vee$ the structure morphism. The torsor $P_K^\times$ inherits the compatible birigidification over $J_K \times \{0\}$ and $\{0\} \times J_K^\vee$ coming from P_K.

Remark 2.1. Note that $\mathbb{G}_m$-torsors on X are classified by the Čech cohomology $\check{H}^1(X, \mathbb{G}_m)$, thus the operation $L \mapsto L^\times$ gives the inverse $\mathrm{Pic}(X) \longrightarrow \check{H}^1(X, \mathbb{G}_m)$ of the canonical isomorphism $\check{H}^1(X, \mathbb{G}_m) \longrightarrow H^1(X, \mathbb{G}_m) \simeq \mathrm{Pic}(X)$. In particular, every $\mathbb{G}_m$-torsor on X arises in this way, and $\mathrm{Pic}(X)$ classifies isomorphism classes of $\mathbb{G}_m$-torsors on X.

2.1.3. *The Poincaré biextension.* The birigidified torsor $P_K^\times$ admits a unique compatible structure of $\mathbb{G}_m$-biextension of the pair $(J_K, J_K^\vee)$ (see [20, VII Definition 2.1 & Exemple 2.9.5]). Let us briefly explain what this means, without repeating the technical definition from SGA 7.

- **Partial composition $+_1$:** We may view $P_K^\times$ as a scheme over $J_K^\vee$ via the structure morphism $\mathrm{pr}_2 \circ j_K$. As such, $P_K^\times$ becomes a commutative $J_K^\vee$-group scheme which is an extension of $J_{K,J_K^\vee} := J_K \times J_K^\vee$ by $\mathbb{G}_{m,J_K^\vee} = \mathbb{G}_m \times J_K^\vee$. In other words, $P_K^\times$ fits into the following short exact sequence of $J_K^\vee$-group schemes

  (2.2) $$1 \longrightarrow \mathbb{G}_{m,J_K^\vee} \longrightarrow P_K^\times \longrightarrow J_{K,J_K^\vee} \longrightarrow 0.$$

  To wit, let S be a K-scheme, $y \in J_K^\vee(S)$ be an S-point of $J_K^\vee$, and $x_1, x_2 \in J_K(S)$ be two S-points of J_K. Let $z_1, z_2 \in P_K^\times(S)$ be two S-points lying above (x_1, y) and (x_2, y) respectively via the structure map j_K. This group structure can be described as follows. The data of the points z_1 and z_2 is equivalent to the data of two nowhere vanishing sections $\alpha_1, \alpha_2 \in (x_1, y)^* P_K(S)$ of the pullback of the Poincaré bundle. As part of the requirement of being a $\mathbb{G}_m$-biextension, we have an isomorphism of line bundles over $\mathcal{O}_S$

  (2.3) $$(x_1, y)^* P_K \otimes (x_2, y)^* P_K \simeq (x_1 + x_2, y)^* P_K,$$

  supplied in this case by the theorem of the cube. Under this canonical isomorphism, the tensor product $\alpha_1 \otimes \alpha_2$ corresponds to a nowhere zero section α_3 of $(x_1 + x_2, y)^* P_K$, thus producing a point $z_3 \in P_K^\times(S)$, which lies above the point $(x_1 + x_2, y)$ of $J_K \times J_K^\vee$. The commutativity of $P_K^\times$ as a $J_K^\vee$-group is clear, as well as the exact sequence (2.2). We denote by $+_1$ the resulting partial composition law on $P_K^\times$, which provides the group structure of $P_K^\times$ over $J_K^\vee$, but not over K. In other words, it is defined on pairs of points $z_1, z_2 \in P_K^\times(S)$ such that

  $$\mathrm{pr}_2(j_K(z_1)) = \mathrm{pr}_2(j_K(z_2)).$$

  We also denote the group structure on the $J_K^\vee$-group scheme $J_{K,J_K^\vee}$ by $+_1$, again slightly abusing notations. The partial composition law $+_1$ on $P_K^\times$ then satisfies

  $$z_1 +_1 z_2 \in P_K^\times(S) \longmapsto (x_1, y) +_1 (x_2, y) = (x_1 + x_2, y) \in J_{K,J_K^\vee}(S).$$

- **Partial composition $+_2$:** On the other hand, we may view $P_K^\times$ as a J_K-scheme via the structure morphism $\mathrm{pr}_1 \circ j_K$. As above, this makes $P_K^\times$ into an extension of $J_{K,J_K}^\vee$ by $\mathbb{G}_{m,J_K}$, which fits into a short exact sequence of commutative J_K-group schemes

  (2.4) $$1 \longrightarrow \mathbb{G}_{m,J_K} \longrightarrow P_K^\times \longrightarrow J_{K,J_K}^\vee \longrightarrow 0.$$

  We denote by $+_2$ the resulting partial composition law on $P_K^\times$, this time defined on couples of points $z_1, z_2 \in P_K^\times(S)$ that satisfy

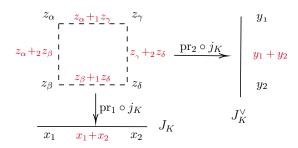 $$\mathrm{pr}_1(j_K(z_1)) = \mathrm{pr}_1(j_K(z_2)).$$

- **Compatibility:** The commutative group scheme extensions (2.2) and (2.4) are compatible in the following sense. Let S be any K-scheme. Let $z_\alpha, z_\beta, z_\gamma, z_\delta \in P_K^\times(S)$ be arbitrary S-points such that

$$j_K(z_\alpha) = (x_1, y_1), \quad j_K(z_\beta) = (x_1, y_2), \quad j_K(z_\gamma) = (x_2, y_1), \quad j_K(z_\delta) = (x_2, y_2),$$

for some S-points $x_1, x_2 \in J_K(S)$ and $y_1, y_2 \in J_K^\vee(S)$. Then

(2.5) $$(z_\alpha +_2 z_\beta) +_1 (z_\gamma +_2 z_\delta) = (z_\alpha +_1 z_\gamma) +_2 (z_\beta +_1 z_\delta).$$

We summarize this compatibility in the following picture for the convenience of the reader:

2.1.4. *Action of* $\mathbb{G}_m$. We briefly describe the action of $\mathbb{G}_m$ on the Poincaré torsor. To this end, we let $e_{J_K} \in \mathrm{Hom}_{J_K}(J_K, P_K^\vee)$ and $e_{J_K^\vee} \in \mathrm{Hom}_{J_K^\vee}(J_K^\vee, P_K^\times)$ denote the identity sections of $P_K^\times$ viewed as a J_K-group scheme and a $J_K^\vee$-group scheme respectively. Restricting the short exact sequence (2.2) of commutative $J_K^\vee$-group schemes via the identity section $\mathrm{Spec}\, K \longrightarrow J_K^\vee$ yields a short exact sequence of commutative K-group schemes

$$1 \longrightarrow \mathbb{G}_{m,K} \longrightarrow P_K^\times|_{J_K \times \{0\}} \overset{e_{J_K}}{\underset{\longleftarrow}{\longrightarrow}} J_K \longrightarrow 0,$$

which is split by the section e_{J_K}. In particular, we have $P_K^\times|_{J_K \times \{0\}} = \mathbb{G}_{m,J_K} = \mathbb{G}_{m,K} \times J_K$. By a similar reasoning using the identity section $e_{J_K^\vee}$, we also have $P_K^\times|_{\{0\} \times J_K^\vee} = \mathbb{G}_{m,J_K^\vee}$. These canonical splittings allow for a useful description of the $\mathbb{G}_m$-action on $P_K^\times$ in terms of the partial group laws $+_2$ and $+_1$. For a $(J_K \times J_K^\vee)$-scheme S, consider $t \in P_K^\times(S)$ and $u \in \mathbb{G}_m(S)$, and let (x,y) be the image of t in $(J_K \times J_K^\vee)(S)$. Consider a point $v = v_{x,u} \in P_K^\times(S)$ lying over $(x,0)$ and corresponding to $(u,0)$ under the identification $P_K^\times|_{J_K \times \{0\}}(S) \simeq \mathbb{G}_m(S) \times J_K(S)$. The action of u on the point t is then given by

(2.6) $$u \cdot t = v +_2 t.$$

The point $v_{x,u}$ does not depend on t, only on x and u. The change of $v_{x,u}$ in the parameter x is described by the relative group law $+_1$, namely $v_{x_1+x_2,u} = v_{x_1,u} +_1 v_{x_2,u}$. Similarly, we have $v_{x,u_1 u_2} = v_{x,u_1} +_2 v_{x,u_2}$.

Instead of using the point $(x,0)$, one could work with $(0,y)$ and the operation $+_1$. These two points of view are equivalent by the compatibility between $+_1$ and $+_2$. As a consequence, the $\mathbb{G}_m$-action commutes with the operations $+_1$ and $+_2$ in the following sense. Given two points $a, b \in P_K^\times(S)$ lying over points of the form $(x,*)$ in $J_K \times J_K^\vee(S)$, and $u, u' \in \mathbb{G}_m(S)$, we have

(2.7)
$$\begin{aligned}
(u \cdot a) +_2 (u' \cdot b) &= (v_{x,u} +_2 a) +_2 (v_{x,u'} +_2 b) \\
&= (v_{x,u} +_2 v_{x,u'}) +_2 (a +_2 b) \\
&= (uu') \cdot (a +_2 b).
\end{aligned}$$

The same holds for $+_1$.

2.2. **Spreading out the geometry.** In the method of geometric quadratic Chabauty, it is crucial to spread out the geometry to $\mathcal{O}_K$. Roughly speaking, the reason is that it is necessary to work with finitely generated $\mathbb{Z}$-modules. The module $\mathbb{G}_m(K) = K^\times$ is not finitely generated, whereas $\mathbb{G}_m(\mathcal{O}_K) = \mathcal{O}_K^\times$ is. Indeed, if r_1 and r_2 denote respectively the number of real embeddings and pairs of complex embeddings of K, then Dirichlet's Unit Theorem implies that $\delta := \mathrm{rank}_{\mathbb{Z}} \mathcal{O}_K^\times = r_1 + r_2 - 1$.

2.2.1. *Models over $\mathcal{O}_K$.* Let $\mathbf{C}$ denote a regular proper model of C_K over $\mathcal{O}_K$. Let $\mathbf{C}^{\mathrm{sm}}$ denote the smooth locus of $\mathbf{C}$. By properness and regularity respectively, we have the identifications

$$C_K(K) = \mathbf{C}(\mathcal{O}_K) = \mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K).$$

Let $\mathbf{J}$ and $\mathbf{J}^\vee$ denote the Néron models over $\mathcal{O}_K$ of J_K and $J_K^\vee$ respectively. Denote by $\mathbf{J}^\circ$ and $\mathbf{J}^{\vee,\circ}$ the fiberwise connected components of 0 in $\mathbf{J}$ and $\mathbf{J}^\vee$ respectively. The quotient $\mathbf{J}^\vee/\mathbf{J}^{\vee,\circ}$ is an étale group scheme over $\mathcal{O}_K$ with finite fibers.

Suppose that $C_K(K)$ is non-empty, and let $b \in C_K(K)$ be a fixed rational point. Such a choice yields an Abel–Jacobi embedding $j_b : C_K \hookrightarrow J_K$, by sending a point x to the linear equivalence class of the divisor $(x) - (b)$. The map j_b extends uniquely to a morphism

$$j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$$

over $\mathcal{O}_K$ by the Néron Mapping Property. The extension of the Poincaré biextension to $\mathrm{Spec}\,\mathcal{O}_K$ is supplied by work of Grothendieck.

Proposition 2.2. *The Poincaré torsor $P_K^\times$ extends uniquely to a biextension $\mathbf{P}^\times$ of $(\mathbf{J}, \mathbf{J}^{\vee,\circ})$ by $\mathbb{G}_m$. In particular, given an $\mathcal{O}_K$-scheme S and two points $(x,y),(x,y') \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(S)$, there is an isomorphism*

(2.8) $$(x,y)^*\mathbf{P} \otimes (x,y')^*\mathbf{P} \simeq (x, y+y')^*\mathbf{P},$$

where $\mathbf{P}$ is the line bundle over $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ corresponding to $\mathbf{P}^\times$.

Proof. This is [20, VIII. Theorem 7.1(b) & Remark 7.2]. $\qquad\square$

We denote the structure morphism of this $\mathbb{G}_m$-torsor by $j : \mathbf{P}^\times \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}$. The uniqueness of the extension follows from the connectedness of $\mathbf{J}^{\vee,\circ}$. We remark that the commutative group scheme extension structures and their compatibilities discussed in Section 2.1.3 extend to the integral version $\mathbf{P}^\times$.

2.2.2. *Integral points on the Poincaré torsor.* We show how to lift certain integral points on $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ across the structure map $j : \mathbf{P}^\times \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}$. Let (x,y) be an $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$, and let $(x,y)^*\mathbf{P}^\times$ be the pull-back of $\mathbf{P}^\times$ to $\mathcal{O}_K$, as pictured in the Cartesian diagram

(2.9)
$$
\begin{array}{ccc}
(x,y)^*\mathbf{P}^\times & \longrightarrow & \mathbf{P}^\times \\
\downarrow & \square & \downarrow \\
\mathrm{Spec}\,\mathcal{O}_K & \xrightarrow{(x,y)} & \mathbf{J} \times \mathbf{J}^{\vee,\circ}.
\end{array}
$$

Lifting the point (x,y) to $\mathbf{P}^\times$ amounts to finding a section of the torsor $(x,y)^*\mathbf{P}^\times \longrightarrow \mathrm{Spec}\,\mathcal{O}_K$.

In the case $K = \mathbb{Q}$, all $\mathbb{G}_m$-torsors are trivial over $\mathrm{Spec}\,\mathbb{Z}$ and thus admit a section over $\mathbb{Z}$, which is unique up to $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. A lift of the integral point (x,y) to $\mathbf{P}^\times$ therefore always exists. In the case of a general number field K, it is not always possible to lift an $\mathcal{O}_K$-point (x,y) of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ to $\mathbf{P}^\times$ when the class number h of K is non-trivial. However, the previous argument carries over to $\mathcal{O}_K$-points of the form $(x, h \cdot y)$.

Lemma 2.3. *Any $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ of the form $(x, h \cdot y)$ with $(x,y) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$ admits a lift to an $\mathcal{O}_K$-point of the Poincaré torsor $\mathbf{P}^\times$. This lift is unique up to multiplication by an element of $\mathcal{O}_K^\times$.*

Proof. We repeatedly apply (2.8) to obtain an isomorphism $((x,y)^*\mathbf{P})^{\otimes h} \simeq (x, h \cdot y)^*\mathbf{P}$ of line bundles over $\operatorname{Spec}\mathcal{O}_K$. It follows that $(x, h \cdot y)^*\mathbf{P}^\times$ is trivial as a $\mathbb{G}_m$-torsor over $\mathcal{O}_K$, since $\operatorname{Pic}(\mathcal{O}_K)$ has size h. $\qquad\square$

3. Construction of the torsor $\mathbf{T}$

The goal of this section is to construct a certain $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$ along with a lift of the Abel–Jacobi map $j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$. Here ρ denotes the rank of the Néron-Severi group of J_K. We begin by constructing the corresponding torsor T_K over J_K, and then proceed to spread out the geometry. Once the torsor $\mathbf{T}$ has been defined, we construct the desired lift of the Abel–Jacobi map.

3.1. Trivialization of the Poincaré torsor.

Let $\lambda : J_K \xrightarrow{\sim} J_K^\vee$ be the canonical principal polarization defined in Section 2.1.1. By functoriality of Pic, we have a commutative diagram of commutative K-group schemes with exact rows

$$(3.1) \quad \begin{array}{ccccccccc}
0 & \longrightarrow & J_K^\vee & \longrightarrow & \operatorname{Pic}_{J_K/K} & \xrightarrow{\pi} & \operatorname{NS}_{J_K/K} & \longrightarrow & 0 \\
& & \wr\downarrow{-\lambda^{-1}} & & \downarrow{j_b^*} & & \downarrow{j_{b,\mathrm{NS}}^*} & & \\
0 & \longrightarrow & J_K & \longrightarrow & \operatorname{Pic}_{C_K/K} & \xrightarrow{\deg} & \mathbb{Z}_K & \longrightarrow & 0.
\end{array}$$

Here $\operatorname{NS}_{J_K/K}$ denotes the Néron–Severi group scheme of J_K, i.e., the étale K-group scheme of components of the Picard scheme associated to J_K. Note that we have used the fact that the map induced by j_b on Pic^0 via pull-back agrees with $-\lambda^{-1}$. It is in particular an isomorphism.

Let $\mathbf{Hom}(J_K, J_K^\vee)^+ \subset \mathbf{Hom}(J_K, J_K^\vee)$ denote the closed subgroup scheme of self-dual homomorphisms. We refer to [18, Proposition 7.14 & §7.18] for questions of representability. There is a map

$$\varphi : \operatorname{Pic}_{J_K/K} \longrightarrow \mathbf{Hom}(J_K, J_K^\vee)^+,$$

defined by sending the class of a line bundle L to the map φ_L, which maps a closed point $x \in J_K$ to $[\mathrm{t}_x^* L \otimes L^{-1}]$, where $\mathrm{t}_x : J_K \longrightarrow J_K$ denotes the translation by x. The kernel of φ is equal to $\operatorname{Pic}^0_{J_K/K} = J_K^\vee$, and the map φ induces an isomorphism of K-group schemes [18, Corollary 11.3]
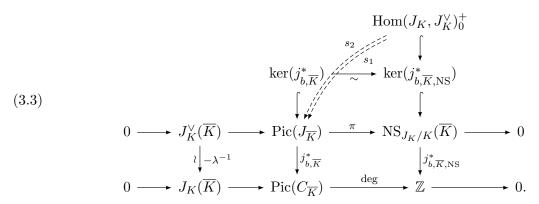
$$(3.2) \quad \tilde{\varphi} : \operatorname{NS}_{J_K/K} \xrightarrow{\sim} \mathbf{Hom}(J_K, J_K^\vee)^+.$$

Definition 3.1. At the level of K-points, we define the group $\operatorname{Hom}(J_K, J_K^\vee)_0^+$ to be

$$\operatorname{Hom}(J_K, J_K^\vee)_0^+ := \ker\left(j_{b,\mathrm{NS}}^* \circ \tilde{\varphi}^{-1} : \operatorname{Hom}(J_K, J_K^\vee)^+ \longrightarrow \mathbb{Z}\right).$$

Proposition 3.2. *For all $f \in \operatorname{Hom}(J_K, J_K^\vee)_0^+$, there exists a unique element $c_f \in J_K^\vee(K)$ with the property that the $\mathbb{G}_m$-torsor $j_b^*(\mathrm{id}, \mathrm{t}_{c_f} \circ f)^* P_K^\times$ over C_K is trivial. In particular, for all $n \in \mathbb{Z}_{\geq 1}$, its nth power $j_b^*(\mathrm{id}, n \cdot \circ \mathrm{t}_{c_f} \circ f)^* P_K^\times$ is also trivial.*

Proof. At the level of $\overline{K}$-points, the diagram (3.1) gives rise to the commutative diagram

$$(3.3)$$

$$\begin{array}{ccccccccc}
& & & & & & \operatorname{Hom}(J_K, J_K^\vee)_0^+ & & \\
& & & & s_2 \nearrow & & \downarrow & & \\
& & & & & s_1 & & & \\
& & \ker(j_{b,\overline{K}}^*) & & \xrightarrow{\sim} & \ker(j_{b,\overline{K},\mathrm{NS}}^*) & & \\
& & \downarrow & & & \downarrow & & \\
0 & \longrightarrow & J_K^\vee(\overline{K}) & \longrightarrow & \operatorname{Pic}(J_{\overline{K}}) & \xrightarrow{\pi} & \operatorname{NS}_{J_K/K}(\overline{K}) & \longrightarrow & 0 \\
& & \wr\downarrow{-\lambda^{-1}} & & \downarrow{j_{b,\overline{K}}^*} & & \downarrow{j_{b,\overline{K},\mathrm{NS}}^*} & & \\
0 & \longrightarrow & J_K(\overline{K}) & \longrightarrow & \operatorname{Pic}(C_{\overline{K}}) & \xrightarrow{\deg} & \mathbb{Z} & \longrightarrow & 0.
\end{array}$$

The map π in the first short exact sequence of this diagram admits two splittings when restricted to $\mathrm{Hom}(J_K, J_K^\vee)_0^+$, which is viewed as a subgroup of $\ker(j_{b,\overline{K},\mathrm{NS}}^*)$ via the map $\tilde{\varphi}^{-1}$. The first section

$$s_1 : \mathrm{Hom}(J_K, J_K^\vee)^+ \longrightarrow \mathrm{Pic}(J_{\overline{K}})$$

is defined by mapping a self-dual homomorphism f defined over K to the isomorphism class of the $\mathbb{G}_m$-torsor $L_f^\times := (\mathrm{id}, f)^* P_K^\times$ on J_K, which is an element of $\mathrm{Pic}(J_K) \subset \mathrm{Pic}(J_{\overline{K}})$. We observe, by [18, Proposition 11.1], that

$$\tilde{\varphi} \circ \pi \circ s_1(f) = \varphi_{L_f} = f + f^\vee = 2f.$$

The second splitting is given by inverting π on $\ker(j_{b,\overline{K}}^*)$, i.e., by

$$s_2 : \mathrm{Hom}(J_K, J_K^\vee)_0^+ \hookrightarrow \ker(j_{b,\overline{K},\mathrm{NS}}^*) \xrightarrow{\pi^{-1}} \ker(j_{b,\overline{K}}^*) \subset \mathrm{Pic}(J_{\overline{K}}).$$

Again the image of s_2 lies in $\mathrm{Pic}(J_K)$. Given $f \in \mathrm{Hom}(J_K, J_K^\vee)_0^+$ we define

$$c_f := 2s_2(f) - s_1(f) \in \mathrm{Pic}(J_K).$$

As $c_f \in \ker(\pi)$, we thus have $c_f \in J_K^\vee(K)$. We observe that for a line bundle L on J_K corresponding to a closed point $x \in J_K^\vee$, we have

$$(\mathrm{id}, f)^* \Big((\mathrm{id} \times \mathrm{t}_x)^* P_K \Big) \simeq (\mathrm{id}, f)^* \big(P_K \otimes \mathrm{pr}_1^* L \big) \simeq (\mathrm{id}, f)^* P_K \otimes L,$$

where pr_1 is the projection $J_K \times J_K^\vee \longrightarrow J_K$. By construction, c_f is therefore the unique element in $J_K^\vee(K)$ such that

$$s_1(f) + c_f = [(\mathrm{id}, \mathrm{t}_{c_f} \circ f)^* P_K^\times] \in \ker j_b^*.$$

<div align="right">□</div>

Remark 3.3. Proposition 3.2 defines a homomorphism $\mathrm{Hom}(J_K, J_K^\vee)_0 \longrightarrow J_K^\vee(K)$ mapping f to the point c_f. The association takes the line bundle $L_f := (\mathrm{id}, f)^* P_K$ on J_K and pulls its back to the degree 0 line bundle $j_b^* L_f$ on C_K. The latter is naturally an element of $J_K(K)$. Then $c_f := \lambda(j_b^* L_f) \in J_K^\vee(K)$. Indeed, $L_f + c_f \in \mathrm{Pic}(J_K)$ satisfies $j_b^*(L_f + c_f) = j_b^* L_f - \lambda^{-1}(c_f) = 0$. With this description in hand, it becomes apparent that c_f is a Zhang point, as defined in [14, Definition 3.3.1]. In the notation therein, $c_f = P(L_f, \lambda, \mathrm{id}_{J_K}, b)$. It follows that $2c_f$ is a Chow–Heegner point associated with the modified diagonal cycle on $(C_K)^3$ based at b [14, Proposition 3.3.3]. For details about Chow–Heegner points attached to diagonal cycles we refer to [12, 13]. Such points naturally arise in the context of bounding rational points on modular curves in [16]. Computing the points c_f, which is required for any explicit implementation of the geometric method of this paper, is of independent interest.

The group $\mathrm{NS}_{J_K/K}(K)$ is a finitely generated free $\mathbb{Z}$-module whose rank is denoted by ρ and called the Picard number of J_K. The kernel $\ker(j_{b,\mathrm{NS}}^* : \mathrm{NS}_{J_K/K}(K) \longrightarrow \mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $\rho - 1$, and so is the group $\mathrm{Hom}(J_K, J_K^\vee)_0^+$.

Notation 3.4.

- Let $f_1, \ldots, f_{\rho-1}$ be a basis of $\mathrm{Hom}(J_K, J_K^\vee)_0^+$.
- For each $i = 1, \ldots, \rho - 1$, let $c_i := c_{f_i} \in J_K^\vee(K)$ be the element corresponding to f_i in Proposition 3.2.
- For each integer $n \in \mathbb{Z}_{\geq 1}$, denote by $\alpha_{n,i,K}$ the map

$$\alpha_{n,i,K} : J_K \xrightarrow{(\mathrm{id}, n \cdot \mathrm{t}_{c_i} \circ f_i)} J_K \times J_K^\vee.$$

Definition 3.5. By Proposition 3.2, the pull-back $j_b^* \big(\alpha_{n,i,K}^* P_K^\times \big)$ is a trivial $\mathbb{G}_m$-torsor over C_K. In other words, it admits a section over C_K. This gives rise to a lift of j_b, unique up to $K^\times$, which we shall fix and denote by $\tilde{j}_b^{(n,i)}$. This is pictured in the diagram

$$
(3.4) \qquad
\begin{array}{ccc}
& \alpha_{n,i,K}^* P_K^\times \longrightarrow & P_K^\times \\
{\scriptstyle \tilde{j}_b^{(n,i)}} \nearrow \quad \downarrow \quad \square \quad & & \downarrow \\
C_K \xrightarrow{\ j_b\ } J_K \xrightarrow{\ \alpha_{n,i,K}\ } & J_K \times J_K^\vee.
\end{array}
$$

3.2. **Definition of the torsor.** We introduce and recall some notations, and refer the rest to Section 2.2.1. Let $\mathfrak{n}$ be the product of prime ideals in $\mathcal{O}_K$ such that $\mathbf{C}$ is smooth away from $\mathrm{Spec}(\mathcal{O}_K/\mathfrak{n})$. Let $\Phi^\vee = \mathbf{J}^\vee/\mathbf{J}^{\vee,\circ}$ be the group scheme of connected components of $\mathbf{J}^\vee$. It is trivial outside $\mathcal{O}_K/\mathfrak{n}$ with finite étale fibers over $\mathcal{O}_K/\mathfrak{n}$. Let m denote the least common multiple of the exponents of $\Phi^\vee(\bar{\mathbb{F}}_\mathfrak{q})$ over all prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$. Finally, recall that h denotes the class number of K.

By the Néron Mapping Property, for each $i \in \{1, \ldots, \rho-1\}$, the maps

$$
\begin{cases}
f_i : J_K \longrightarrow J_K^\vee \\
t_{c_i} : J_K^\vee \longrightarrow J_K^\vee \\
hm \cdot : J_K^\vee \longrightarrow J_K^\vee
\end{cases}
\qquad \text{extend uniquely to} \qquad
\begin{cases}
f_i : \mathbf{J} \longrightarrow \mathbf{J}^\vee \\
t_{c_i} : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee \\
hm \cdot : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee.
\end{cases}
$$

The map $\alpha_{hm,i,K} : J_K \longrightarrow J_K \times J_K^\vee$ therefore extends uniquely to a map of $\mathcal{O}_K$-schemes

$$
\alpha_{hm,i} = (\mathrm{id}, hm \cdot \circ\, t_{c_i} \circ f_i) : \mathbf{J} \longrightarrow \mathbf{J} \times \mathbf{J}^\vee.
$$

The integer m is chosen so that the image of this map lies in $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$.

Definition 3.6. Taking the product over $i \in \{1, \ldots, \rho-1\}$, we obtain the $\mathcal{O}_K$-morphism

$$
\alpha = (\mathrm{id}, (hm \cdot \circ\, t_{\underline{c}} \circ \underline{f})) := (\mathrm{id}, (hm \circ t_{c_i} \circ f_i)_{i=1}^{\rho-1}) : \mathbf{J} \longrightarrow \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}.
$$

Consider the map $\mathbf{P}^\times \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ} \longrightarrow \mathbf{J}$ defined as the composition of the structure map j with the first projection. Using this morphism, we form the $(\rho-1)$-fold self-product

$$
\mathbf{P}^{\times,\rho-1} := \mathbf{P}^\times \times_{\mathbf{J}} \ldots \times_{\mathbf{J}} \mathbf{P}^\times.
$$

We naturally have a morphism $\mathbf{P}^{\times,\rho-1} \longrightarrow \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$, which endows $\mathbf{P}^{\times,\rho-1}$ with the structure of a $\mathbb{G}_m^{\rho-1}$-torsor over $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$. This leads to the following key construction.

Definition 3.7. Define the $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$ to be the pull-back of the $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{P}^{\times,\rho-1}$ over $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}$ by the map α, i.e.,

$$
\mathbf{T} := \mathbf{P}^{\times,\rho-1} \times_\alpha \mathbf{J} = \alpha^* \mathbf{P}^{\times,\rho-1} = (\mathrm{id}, hm \cdot \circ\, t_{c_1} \circ f_1)^* \mathbf{P}^\times \times_{\mathbf{J}} \ldots \times_{\mathbf{J}} (\mathrm{id}, hm \cdot \circ\, t_{c_{\rho-1}} \circ f_{\rho-1})^* \mathbf{P}^\times.
$$

3.3. **Lifting the Abel–Jacobi map.** By taking the product over i of the lifts $\tilde{j}_b^{(hm,i)}$ of Definition 3.5, we obtain a lift $\tilde{j}_b$ of j_b to $T_K := \mathbf{T} \times_J J_K$, as pictured in the commutative diagram

$$
(3.5) \qquad
\begin{array}{ccc}
& T_K \longrightarrow & P_K^{\times,\rho-1} \\
{\scriptstyle \tilde{j}_b} \nearrow \quad \downarrow \quad \square \quad & & \downarrow \\
C_K \xrightarrow{\ j_b\ } J_K \xrightarrow{\ \alpha_K\ } & J_K \times (J_K^{\vee,0})^{\rho-1},
\end{array}
$$

where α_K denotes the base change of the map α to K.

The goal is to extend this diagram over $\mathcal{O}_K$. However, lifting the map $j_b : \mathbf{C}^{\mathrm{sm}} \longrightarrow \mathbf{J}$ to the torsor $\mathbf{T}$ is generally not possible, the problem being that the fibers $C_{\mathbb{F}_\mathfrak{q}}^{\mathrm{sm}} := \mathbf{C}^{\mathrm{sm}} \times_{\mathrm{Spec}\,\mathcal{O}_K} \mathrm{Spec}\,\mathbb{F}_\mathfrak{q}$, for primes $\mathfrak{q}|\mathfrak{n}$, may contain too many components. To remedy this, we consider one geometrically irreducible component in each such fiber at a time.

Definition 3.8. Let $\mathbf{U} \subset \mathbf{C}^{\mathrm{sm}}$ be an open subscheme obtained by removing, for every $\mathfrak{q}|\mathfrak{n}$, all but one irreducible component of $C_{\mathbb{F}_\mathfrak{q}}^{\mathrm{sm}}$ that is furthermore geometrically irreducible. We will lift the map j_b to a map $\tilde{j}_b^U : \mathbf{U} \longrightarrow \mathbf{T}$ for each such open subscheme $\mathbf{U}$.

Remark 3.9. We first remark that such a subscheme $\mathbf{U}$ exists under the assumption that C_K admits a K-rational point. Secondly, for the purpose of determining the set of rational points $C_K(K) = \mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$, it suffices to consider subschemes of the form $\mathbf{U}$, as there are finitely many of them and each point in $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$ lies in exactly one such $\mathbf{U}$. Both remarks follow from the following simple lemma.

Lemma 3.10. *Let X be an irreducible variety over a field k that admits a smooth k-rational point. Then X is geometrically irreducible.*

Proof. Let $A = \Gamma(U, \mathcal{O}_X)$ be the ring of functions on a normal affine open neighborhood U of the smooth rational point. Then A admits a map $A \longrightarrow k$ of k-algebras. Let k' be the separable algebraic closure of k in the function field $k(X) = \mathrm{Frac}(A)$. Since U is normal, we have $k' \subset A$ which forces $k' = k$. This is equivalent to X being geometrically irreducible by [21, Corollaire 4.5.10]. □

The construction of the desired lift of j_b is analogous to the one in [17, §2], except that we pull back $\mathbf{P}^\times$ via morphisms of the form $(\mathrm{id}, hm \cdot \circ \, \mathrm{t}_c \circ f) : \mathbf{J} \longrightarrow \mathbf{J} \times \mathbf{J}^{\vee,\circ}$, where in the second factor we incorporate an additional multiplication by the class number h to ensure the existence of such a lift.

Proposition 3.11. *Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as in Definition 3.8. There exists a lift $\tilde{j}_b^U$ of $j_b|_{\mathbf{U}}$ to $\mathbf{T}$, unique up to $\mathcal{O}_K^{\times,\rho-1}$, which makes the following diagram commute:*

(3.6)

$$
\begin{array}{ccc}
& \mathbf{T} \longrightarrow & \mathbf{P}^{\times,\rho-1} \\
\tilde{j}_b^U \nearrow & \downarrow \quad \square & \downarrow \\
\mathbf{U} \hookrightarrow \mathbf{C}^{\mathrm{sm}} \xrightarrow{j_b} \mathbf{J} \xrightarrow{\alpha} & \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}.
\end{array}
$$

Proof. The restriction of the torsor $(\mathrm{id}, m \cdot \circ \, \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P}^\times$ to $\mathbf{U}$ gives an element of $\mathrm{Pic}(\mathbf{U})$, whose pull-back to C_K equals $j_b^* \alpha_{m,i,K}^* P_K^\times$ and is trivial by Proposition 3.2. In other words, when restricted to $\mathbf{U}$, the torsor $(\mathrm{id}, m \cdot \circ \, \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P}^\times$ gives rise to an element of the kernel $\ker(\mathrm{Pic}(\mathbf{U}) \longrightarrow \mathrm{Pic}(C_K))$. Note that we have an isomorphism of line bundles

(3.7)
$$
(\mathrm{id}, hm \cdot \circ \, \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P} \simeq ((\mathrm{id}, m \cdot \circ \, \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P})^{\otimes h},
$$

obtained by using (2.8). By Lemma 3.12 below, we conclude that $(\mathrm{id}, hm \cdot \circ \, \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P}^\times$ becomes a trivial $\mathbb{G}_{m,\mathbf{U}}$-torsor when restricted to $\mathbf{U}$. It follows that $\mathbf{T}$ pulls back to the trivial $\mathbb{G}_{m,\mathbf{U}}^{\rho-1}$-torsor over $\mathbf{U}$. In particular, the map $j_b|_{\mathbf{U}}$ admits a lift to $\mathbf{T}$, which is unique up to $\mathbb{G}_m^{\rho-1}(\mathbf{U})$. The latter is equal to $(\mathcal{O}_{\mathbf{U}}(\mathbf{U})^\times)^{\rho-1} = (\mathcal{O}_K^\times)^{\rho-1}$ by Lemma 3.12 below. □

The following lemma is used in the proof above.

Lemma 3.12. *Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as in Definition 3.8. Then $\mathcal{O}_{\mathbf{U}}(\mathbf{U}) = \mathcal{O}_K$ and the kernel of the restriction $\ker(\mathrm{Pic}(\mathbf{U}) \longrightarrow \mathrm{Pic}(C_K))$ is h-torsion. In other words, given a line bundle L over $\mathbf{U}$, which is trivial over the generic fiber C_K, its h-th power $L^{\otimes h}$ is trivial over $\mathbf{U}$.*

Proof. By construction, $\mathbf{U}$ is regular and thus locally factorial. We do therefore not distinguish between isomorphism classes of line bundles and Weil divisors. Let D be a vertical divisor on $\mathbf{U}$, i.e., a divisor that does not intersect the generic fiber C_K. We claim that $hD = 0$ in $\mathrm{Pic}(\mathbf{U})$. As every irreducible vertical divisor on $\mathbf{U}$ is of the form $\mathbf{U}_\mathfrak{p}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$, we may write hD as $\sum_\mathfrak{p} h n_\mathfrak{p} U_{\mathbb{F}_\mathfrak{p}}$, where $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$. Clearly, hD is the image of the divisor $\sum_\mathfrak{p} h n_\mathfrak{p} \mathfrak{p}$ along the natural map $\mathrm{Pic}(\mathcal{O}_K) \longrightarrow \mathrm{Pic}(\mathbf{U})$, which is trivial since $\mathrm{Pic}(\mathcal{O}_K)$ has size h.

Now let D be a general element of $\mathrm{Pic}(\mathbf{U})$, viewed as a Weil divisor on $\mathbf{U}$, that lies in the kernel $\ker(\mathrm{Pic}(\mathbf{U}) \longrightarrow \mathrm{Pic}(C_K))$. In other words, the restriction of D to C_K is a principal divisor $D_K = \mathrm{div}(f)$ for some f in the function field of C_K. Then $\mathrm{div}(f)$ extends to a principal divisor on $\mathbf{U}$, which differs from D only by a vertical divisor. The lemma thus follows. $\qquad\square$

Remark 3.13. When $h = 1$, the lemma simply says that the restriction $\mathrm{Pic}(\mathbf{U}) \longrightarrow \mathrm{Pic}(C_K)$ is injective. This map is of course not in general injective when $h \neq 1$. Indeed, in this case it suffices to take $D = U_{\mathfrak{p}} \in \mathrm{Div}(\mathbf{U})$, where $\mathfrak{p}$ is a non-principal prime ideal of $\mathcal{O}_K$.

4. The main theorem

In this section, we state a precise version of the main theoretical result of the article. We give a detailed description of the strategy of the geometric quadratic Chabauty method.

Assumption 4.1. *Throughout, we make the following assumptions on the prime p.*
  (a) *The curve C_K has good reduction at each prime $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of K that lies above p.*
  (b) *Each $\mathfrak{p}_i$ satisfies $e(\mathfrak{p}_i/p) < p - 1$.*
  (c) *The prime p does not divide $|\mathcal{O}_{K,\mathrm{tors}}^{\times}|$.*

Note that the first condition is equivalent to requiring that $\mathfrak{p}_i \nmid \mathfrak{n}$ for each $i \in \{1, \ldots, s\}$, and that Assumption 4.1 excludes only finitely many primes.

Remark 4.2. We comment on the use and necessity of Assumption 4.1. Condition (a) on good reduction is used in the beginning of Section 6 to argue that the tangent map of the lifted Abel–Jacobi map on $\mathfrak{p}$-adic residue disks is injective. It is worth mentioning that the idea of using primes of bad reduction in the Chabauty–Coleman method has been explored in [25, 26, 34]. Condition (b) on the ramification degree not being too large is used to deduce that the kernel of reduction $\mathbf{J}(\mathcal{O}_K)_0$ is a free $\mathbb{Z}$-module (see Section 4.2), and to prove the integrality of certain power series defining formal exponential and logarithm maps (see the proof of Proposition 5.18). The condition excludes the case $p = 2$ even though this case can be particularly interesting, see for instance [31]. Similarly, the case $p = 2$ is excluded in [17], as well as in the geometric linear Chabauty method [22]. Condition (c) is used in the proof of Proposition 5.9 below.

Notation 4.3.
  • Let $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes \mathbb{Z}_p$ be the p-adic completion of $\mathcal{O}_K$. It is isomorphic to the product of the $\mathfrak{p}_i$-adic completions $\mathcal{O}_{K,\mathfrak{p}_1} \times \ldots \times \mathcal{O}_{K,\mathfrak{p}_s}$.
  • Let $\overline{\mathcal{O}_{K,p}} := (\mathcal{O}_K \otimes \mathbb{F}_p)_{\mathrm{red}} \simeq \mathbb{F}_{\mathfrak{p}_1} \times \ldots \times \mathbb{F}_{\mathfrak{p}_s}$.
  • For any $\mathcal{O}_K$-scheme X, we have natural identifications

$$X(\mathcal{O}_{K,p}) = \prod_{i=1}^{s} X_{\mathcal{O}_{K,\mathfrak{p}_i}}(\mathcal{O}_{K,\mathfrak{p}_i}) \qquad \text{and} \qquad X(\overline{\mathcal{O}_{K,p}}) = \prod_{i=1}^{s} X_{\mathbb{F}_{\mathfrak{p}_i}}(\mathbb{F}_{\mathfrak{p}_i}).$$

We denote the natural reduction map by

$$\mathrm{red} : X(\mathcal{O}_{K,p}) \longrightarrow X(\overline{\mathcal{O}_{K,p}}).$$

  • Given a point $x \in X(\overline{\mathcal{O}_{K,p}})$, we denote by $X(\mathcal{O}_{K,p})_x$ the set $\mathrm{red}^{-1}(x)$, namely the residue disk in $X(\mathcal{O}_{K,p})$ of points that reduces to the point x. Likewise, we denote by $X(\mathcal{O}_K)_x$ the pre-image of $X(\mathcal{O}_{K,p})_x$ under the natural inclusion $X(\mathcal{O}_K) \hookrightarrow X(\mathcal{O}_{K,p})$, which consists of rational points in the residue disk $X(\mathcal{O}_{K,p})_x$.

Remark 4.4. The reason for working with all primes above p simultaneously, as opposed to fixing a single prime, is explained in Section 1.9.

4.1. **Revisiting the strategy.** Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as in Definition 3.8. Let u be an element in the finite set $\mathbf{U}(\overline{\mathcal{O}_{K,p}})$, and let $t := \tilde{j}_b^U(u) \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$ be its image in $\mathbf{T}$ under the lift $\tilde{j}_b^U : \mathbf{U} \longrightarrow \mathbf{T}$ of Proposition 3.11. Note that $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$ is the disjoint union of $\mathbf{U}(\mathcal{O}_K)$ for the finitely many choices of $\mathbf{U}$'s by Remark 3.9, and each $\mathbf{U}(\mathcal{O}_K)$ is the disjoint union of finitely many residue disks $\mathbf{U}(\mathcal{O}_K)_u$. Thus, for the purposes of this work, it suffices to bound the size of $\mathbf{U}(\mathcal{O}_K)_u$ for each $\mathbf{U}$ and each point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$.

The key idea of the approach can be represented using the commutative diagram

(4.1)
$$
\begin{array}{ccc}
\mathbf{U}(\mathcal{O}_K)_u & \lhook\joinrel\longrightarrow & \mathbf{U}(\mathcal{O}_{K,p})_u \\
\Big\uparrow{\scriptstyle\tilde{j}_b^U} & & \Big\uparrow{\scriptstyle\tilde{j}_b^U} \\
\mathbf{T}(\mathcal{O}_K)_t \lhook\joinrel\longrightarrow & \mathbf{Y}_t \lhook\joinrel\longrightarrow & \mathbf{T}(\mathcal{O}_{K,p})_t,
\end{array}
$$

where the top horizontal arrow is induced by the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,p}$, and $\mathbf{Y}_t := \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ denotes the p-adic closure of $\mathbf{T}(\mathcal{O}_K)_t$ in $\mathbf{T}(\mathcal{O}_{K,p})_t$. We view $\mathbf{U}(\mathcal{O}_K)_u$ and $\mathbf{U}(\mathcal{O}_{K,p})_u$ as a subsets of $\mathbf{T}(\mathcal{O}_K)_t$ and $\mathbf{T}(\mathcal{O}_{K,p})_t$ respectively via the map $\tilde{j}_b^U$. In particular, we have inclusions $\mathbf{U}(\mathcal{O}_K)_u \hookrightarrow \mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$. As explained in the introduction, the goal is to bound the intersection

(4.2)
$$
\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t,
$$

which takes place in the p-adic analytic manifold $\mathbf{T}(\mathcal{O}_{K,p})_t$.

Remark 4.5. For this intersection to have a chance to be finite, some condition must be imposed in the style of the original Chabauty condition $r < g$. We will come back to this point in Section 4.3 after stating the main technical result of the paper.

4.2. **The key technical result.** We give a description of $\mathbf{Y}_t$, which is a crucial ingredient in bounding the intersection (4.2).

Notation 4.6.
- Recall that $r := \mathrm{rank}_{\mathbb{Z}} J_K(K)$ is the Mordell–Weil rank of J_K over K.
- Let $\mathbf{J}(\mathcal{O}_K)_0$ denote the subgroup of $J_K(K) = \mathbf{J}(\mathcal{O}_K)$ given by kernel

$$
\mathbf{J}(\mathcal{O}_K)_0 := \ker\big(\mathrm{red} : \mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\overline{\mathcal{O}_{K,p}})\big).
$$

- Let q^* denote the exponent of $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, i.e., the least common multiple of $q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$ for $i \in \{1, \ldots, s\}$.
- For each $i \in \{1, \ldots, s\}$, let $k_i = k_{\mathfrak{p}_i} = e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}$ be the $\mathbb{Z}_p$-rank of $\mathcal{O}_{K,\mathfrak{p}_i}$. Note that the rank of $\mathcal{O}_{K,p}$ as a $\mathbb{Z}_p$-module is $\sum_{\mathfrak{p}_i | p} k_i = d$, where d is the degree of K over $\mathbb{Q}$.

By Assumption 4.1 (b) on p, for each $i \in \{1, \ldots, s\}$, the reduction $\mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\mathbb{F}_{\mathfrak{p}_i})$ is injective on the torsion points of $\mathbf{J}(\mathcal{O}_K)$ by [27, Appendix]. Hence $\mathbf{J}(\mathcal{O}_K)_0$ is a free $\mathbb{Z}$-module of rank r. We fix a basis $\mathbf{x} = \{x_1, \ldots, x_r\}$.

The idea is to parametrize the p-adic closure $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ using the set

$$
(\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)}) \otimes \mathbb{Z}_p,
$$

where the subscript "tf" stands for the torsion free quotient viewed as a free subgroup of $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$ via a fixed lift $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \longrightarrow \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$. In Section 5.1 (see Definition 5.7), we will define a map

$$
E' : \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t,
$$

which depends on an initial choice of finitely many points of $\mathbf{P}^{\times,\rho-1}(\mathcal{O}_K)$, a choice which itself depends on the basis $\mathbf{x}$ fixed above. The map E' enjoys the following properties (see Propositions 5.9 and 5.10):

Proposition 4.7. *Upon fixing a basis for the free $\mathbb{Z}$-module $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \subset \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$, and identifying the set $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)}$ with $\mathbb{Z}^{\delta(\rho-1)+r}$ using the basis $\mathbf{x}$ above, the map E' can be viewed as a map $\mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$. With respect to these choices of bases, E' admits an explicit description in terms of the partial composition laws of Section 2.1.3, and satisfies*

$$(4.3) \qquad\qquad E'(q^*\mathbb{Z}^{\delta(\rho-1)+r}) \subset \mathbf{T}(\mathcal{O}_K)_t \subset E'(\mathbb{Z}^{\delta(\rho-1)+r}),$$

where q^* is the integer defined in Notation 4.6.

From now on, we fix a basis $\mathbf{u} = \{u_1, \ldots, u_\delta\}$ of $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \subset \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$ and view E' as a map $\mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$. The domain of this map is a dense subspace of $\mathbb{Z}_p^{\delta(\rho-1)+r}$ endowed with the p-adic topology. On the other hand, the target space $\mathbf{T}(\mathcal{O}_{K,p})_t$ naturally carries a p-adic topology. In Section 5.2, we "p-adically interpolate" the map E' to get the following result:

Theorem 4.8. *With respect to the fixed bases $\mathbf{x}$ and $\mathbf{u}$ above, there is a unique continuous map $\kappa = \kappa_{\mathbf{x},\mathbf{u}}$ making the diagram*

$$\begin{array}{ccc} \mathbb{Z}^{\delta(\rho-1)+r} & \xrightarrow{\;\;E'\;\;} & \mathbf{T}(\mathcal{O}_{K,p})_t \\ \downarrow & \nearrow & \\ \mathbb{Z}_p^{\delta(\rho-1)+r} & \;^{\exists!\kappa} & \end{array}$$

commute. We call the map κ the p-adic interpolation of E' (with respect to the bases $\mathbf{x}$ and $\mathbf{u}$). Moreover, the choice of a regular system of parameters $\mathbf{t}_\mathfrak{p}$ for $\mathbf{T} \longrightarrow \mathbf{J}$ at $t_\mathfrak{p} \in \mathbf{T}(\mathbb{F}_\mathfrak{p})$ for each $\mathfrak{p}$, as well as an isomorphism of $\mathbb{Z}_p$-modules $\mathcal{O}_{K,\mathfrak{p}} \simeq \mathbb{Z}_p^{k_\mathfrak{p}}$, yields a homeomorphism $\tilde{\mathbf{t}} : \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_t \simeq \mathbb{Z}_p^{(g+\rho-1)k_\mathfrak{p}}$ and uniquely determines a $(g+\rho-1)d$-tuple of convergent power series $\kappa_i \in \mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$ such that

$$\tilde{\mathbf{t}} \circ \kappa = (\kappa_1, \ldots, \kappa_{(g+\rho-1)d}) : \mathbb{Z}_p^{\delta(\rho-1)+r} \longrightarrow \mathbb{Z}_p^{(g+\rho-1)d}.$$

Thus, κ is a map of p-adic analytic manifolds.

Remark 4.9. A lot of dependencies have been suppressed in the above notations. The map κ of Theorem 4.8 depends on the point $t \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$ and a choice of lift $\tilde{t}$ in $\mathbf{T}(\mathcal{O}_K)$, the choice of basis $\mathbf{x}$ for the free $\mathbb{Z}$-module $\mathbf{J}(\mathcal{O}_K)_0$, the finitely many choices of initial points of $\mathbf{P}^{\rho-1}(\mathcal{O}_K)$ needed to define the map E', and finally the basis $\mathbf{u}$ for the free $\mathbb{Z}$-module $\mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}} \subset \mathbb{G}_m(\mathcal{O}_K)$. Note however, that κ does not depend on the choice of local parameters for $\mathbf{T}(\mathcal{O}_{K,p})_t$, even though its expression in terms of convergent p-adic power series does.

Corollary 4.10. *The image of the map κ is the p-adic closure $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$.*

Proof. Since $\mathbb{Z}_p^{\delta(\rho-1)+r}$ is compact and κ is continuous, the image of κ is closed in $\mathbf{T}(\mathcal{O}_{K,p})_t$. Since κ extends E', the second containment of (4.3) implies that $\mathrm{Im}\,\kappa$ contains $\mathbf{T}(\mathcal{O}_K)_t$, and thus also contains $\mathbf{Y}_t$. On the other hand $q^*\mathbb{Z}^{\delta(\rho-1)+r}$ is dense in $\mathbb{Z}_p^{\delta(\rho-1)+r}$ since q^* is coprime to p. By continuity of κ, we have

$$\mathrm{Im}\,\kappa = E'\left(\overline{q^*\mathbb{Z}^{\delta(\rho-1)+r}}\right) \subset \overline{E'(q^*\mathbb{Z}^{\delta(\rho-1)+r})} \subset \mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p,$$

where the last containment uses the first inclusion of (4.3). This concludes the proof. $\qquad\square$

In Section 6, we use the map κ to pull-back the p-adically convergent power series cutting out $\mathbf{U}(\mathcal{O}_{K,p})_u$ inside $T(\mathcal{O}_{K,p})_t$. These pull-backs belong to $R := \mathbb{Z}_p\langle z_1, ..., z_{\delta(\rho-1)+r}\rangle$ and generate an ideal $I_{\mathbf{U},u} = I_{\mathbf{U},u,\kappa}$ whose precise definition is given in Definition 6.1. The more precise form of Theorem 1.1 is then the following, which we prove in Section 6:

Theorem 4.11. *If* $\overline{A}_{\mathbf{U},u} := \big(R/I_{\mathbf{U},u}\big) \otimes \mathbb{F}_p$ *is finite dimensional over* $\mathbb{F}_p$, *then the number of rational points in* $\mathbf{U}(\mathcal{O}_K)_u$ *is finite and bounded by*

$$|\mathbf{U}(\mathcal{O}_K)_u| \leq \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}.$$

As discussed in the introduction, we expect this bound to prove useful in determining the rational points of curves in many new examples.

4.3. **Chabauty conditions.** We end this section with a discussion of the Chabauty condition. We retain all notations and assumptions from the previous sections, in particular Assumption 4.1 on the prime p.

For each prime $\mathfrak{p}$ above p, the scheme $\mathbf{T} \times_{\mathcal{O}_K} \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ is smooth over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension $g + \rho - 1$ and the set $\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})$ is equipped with the structure of a p-adic analytic manifold of dimension $(g + \rho - 1)k_{\mathfrak{p}}$. In particular, $\mathbf{T}(\mathcal{O}_{K,p})$ is a p-adic analytic manifold of dimension

$$(g + \rho - 1) \sum_{\mathfrak{p}|p} k_{\mathfrak{p}} = (g + \rho - 1)d.$$

By Theorem 4.8 and Corollary 4.10, the p-adic analytic submanifold $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ is parametrized by $\mathbb{Z}_p^{\delta(\rho-1)+r}$ via the map of p-adic analytic manifolds $\kappa : \mathbb{Z}_p^{\delta(\rho-1)+r} \twoheadrightarrow \mathbf{Y}_t$. The dimension of the p-adic analytic manifold $\mathbf{Y}_t$ is therefore bounded above by

$$\dim \mathbf{Y}_t \leq \delta(\rho - 1) + r.$$

Finally, we observe that $\mathbf{U}(\mathcal{O}_{K,p})$ has dimension d as a p-adic analytic manifold.

A necessary condition for the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$ in (4.2) to be finite is the inequality on dimensions of p-adic analytic manifolds

$$\operatorname{codim} \mathbf{U}(\mathcal{O}_{K,p}) + \operatorname{codim} \mathbf{Y}_t \geq \dim \mathbf{T}(\mathcal{O}_{K,p}),$$

where the codimensions are taken with respect to the ambient manifold $\mathbf{T}(\mathcal{O}_{K,p})$. This inequality is satisfied if we require the weaker inequality

$$\delta(\rho - 1) + r \leq (g + \rho - 2)d,$$

which in turn is equivalent to the condition

$$(4.4) \qquad\qquad r \leq (g - 1)d + (\rho - 1)(r_2 + 1).$$

Definition 4.12. We say that a smooth, projective and geometrically connected curve C_K of genus $g \geq 2$ over a number field K satisfies the geometric quadratic Chabauty condition if the inequality (4.4) holds.

Remark 4.13. The term "geometric" distinguishes condition (4.4) from other Chabauty type conditions associated to the various methods discussed in Sections 1.2 and 1.4. We briefly compare these conditions:

- When $K = \mathbb{Q}$, the condition (4.4) becomes $r \leq g + \rho - 2$, which is the same condition as in the geometric quadratic Chabauty method over $\mathbb{Q}$ of Edixhoven and Lido [17] discussed in Section 1.3.
- Siksek [32] extended the classical Chabauty–Coleman method to arbitrary number fields using Weil restrictions. This is the Restriction of Scalars (RoS) Chabauty method of Section 1.4.2. The method is expected to be successful when $r \leq (g - 1)d$ and certain additional conditions are assumed (see the discussion in Sections 1.4.2 and 1.4.3). Under such conditions, the geometric quadratic Chabauty method is thus expected to go beyond the RoS Chabauty method.

- In their recent work [2], Balakrishnan, Besser, Bianchi, and Müller extended the method of quadratic Chabauty to number fields in the case of hyperelliptic or bielliptic curves. In Section 1.4.3, we referred to this method as the effective RoS quadratic Chabauty method. It performs under the relaxed condition $r \leq (g-1)d + r_2 + 1$. The geometric Chabauty condition agrees with this when ρ is equal to 2, and in fact generalizes this bound for $\rho \geq 2$.
- Dogra [15] has recently proved that, under the extra condition (1.5) on J_K and K, a certain "arithmetic quadratic Chabauty condition" implies that the set $C_K(K_{\mathfrak{p}})_2$ appearing in the RoS Chabauty–Kim method of Section 1.4.3 is finite for some $\mathfrak{p}$ above the split prime p. If one assumes the finiteness of the p-primary part of the Shafarevich–Tate group for J_K, then the aforementioned Chabauty condition of Dogra is (a slightly relaxed version of) the geometric condition (4.4). We refer to [15, Proposition 1.1 & Remark 1.5] for further details.

5. The parametrization of $\mathbf{Y}_t$

We retain the notations of Section 4. The goal of this section is to prove Theorem 4.8, i.e., to describe the p-adic closure $\mathbf{Y}_t$ of $\mathbf{T}(\mathcal{O}_K)_t$ inside $\mathbf{T}(\mathcal{O}_{K,p})_t$.

5.1. **Construction of the map E'.** We construct the map E' of Proposition 4.7. This map, and subsequently its p-adic interpolation κ of Theorem 4.8, depends on the choice of $r^2 + 2r$ initial points in $\mathbf{P}^{\times,\rho-1}(\mathcal{O}_K)$. The definition of E' is achieved in 3 steps.

Notation 5.1.

- Fix a basis $\mathbf{x} = \{x_1, \ldots, x_r\}$ of the free $\mathbb{Z}$-module $\mathbf{J}(\mathcal{O}_K)_0 = \ker\left(\mathbf{J}(\mathcal{O}_K) \longrightarrow \mathbf{J}(\overline{\mathcal{O}_{K,p}})\right)$.
- Recall that u is a fixed $\overline{\mathcal{O}_{K,p}}$-point of $\mathbf{U}$ and $t = \tilde{j}_b^U(u)$. Denote by $\tilde{t}$ any lift of t to an $\mathcal{O}_K$-point of the torsor $\mathbf{T}$. Such a lift is assumed to exist, as otherwise $\mathbf{U}(\mathcal{O}_K)_u = \emptyset$, and we are done. Denote by $x_{\tilde{t}}$ its image in $\mathbf{J}(\mathcal{O}_K)$.
- Let $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ be the set of points of $\mathbf{T}(\mathcal{O}_K)$ whose image in $\mathbf{J}(\overline{\mathcal{O}_{K,p}})$ is $j_b(u)$.

For the reader's convenience, the points and sets are pictured in the following diagrams:

$$
\begin{array}{ccc}
& t \xleftarrow{\ \text{red}\ } \tilde{t} & \\
\tilde{j}_b^U \nearrow & \downarrow \quad \downarrow & \\
u \xmapsto{\ j_b\ } j_b(u) \xleftarrow{\ \text{red}\ } x_{\tilde{t}} &
\end{array}
\qquad
\begin{array}{ccc}
& \mathbf{T}(\mathcal{O}_K)_t \subset \mathbf{T}(\mathcal{O}_K)_{j_b(u)} \\
\tilde{j}_b^U \nearrow & \downarrow \\
\mathbf{U}(\mathcal{O}_K)_u \xhookrightarrow{\ j_b\ } \mathbf{J}(\mathcal{O}_K)_{j_b(u)}.
\end{array}
$$

5.1.1. *Construction of the map D.* The first step is the construction of a section

$$D : \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)},$$

essentially by choosing a lift for each point $x \in \mathbf{J}(\mathcal{O}_K)_{j_b(u)}$. This can be done in a coherent way using the biextension laws (important for the p-adic interpolation below), once we choose finitely many initial points $P_{i,j}, R_i, S_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_K)$, $0 \leq i,j \leq r$, lifting the following points of $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}(\mathcal{O}_K)$:

$$
\begin{aligned}
P_{i,j} &\longmapsto \left(x_i, \underline{f}(hmx_j)\right) = \left(x_i, hm\underline{f}(x_j)\right), \\
R_i &\longmapsto \left(x_i, (hm \cdot \circ \, \mathsf{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})\right), \\
S_j &\longmapsto \left(x_{\tilde{t}}, \underline{f}(hmx_j)\right) = \left(x_{\tilde{t}}, hm\underline{f}(x_j)\right).
\end{aligned}
$$

Here $\underline{f}$ is given by the functions f_i of Notation 3.4. Note that the points to be lifted are of the form $(*, h \cdot *)$, and the existence of such lifts is guaranteed by Lemma 2.3. Note also that unlike the situation of [17], these lifts are no longer defined up to a finite choice, as they are now parametrized by $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$.

As a set, $\mathbf{J}(\mathcal{O}_K)_{j_b(u)} = x_{\tilde{t}} + \mathbf{J}(\mathcal{O}_K)_0 = x_{\tilde{t}} + \bigoplus_{i=1}^r \mathbb{Z}x_i$ is in bijection with $\mathbb{Z}^r$: any point of $\mathbf{J}(\mathcal{O}_K)_{j_b(u)}$ can be expressed as $x_{\underline{n}} := x_{\tilde{t}} + \sum_{i=1}^r n_i x_i$ for a unique $\underline{n} \in \mathbb{Z}^r$. Given $\underline{n} \in \mathbb{Z}^r$, we will now define a lift $D(\underline{n}) := D(x_{\underline{n}})$ of $x_{\underline{n}}$ using the above initial points and the biextension laws. Define

$$
\begin{aligned}
A(\underline{n}) &:= \sum_{2,j} n_j \cdot_2 S_j &&\longmapsto \left(x_{\tilde{t}},\, hm\underline{f}\left(\sum_i n_i x_i\right)\right), \\
B(\underline{n}) &:= \sum_{1,i} n_i \cdot_1 R_i &&\longmapsto \left(\sum_i n_i x_i,\, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})\right), \\
C(\underline{n}) &:= \sum_{1,i} n_i \cdot_1 \left(\sum_{2,j} n_j \cdot_2 P_{i,j}\right) &&\longmapsto \left(\sum_i n_i x_i,\, hm\underline{f}\left(\sum_i n_i x_i\right)\right).
\end{aligned}
$$

Here $\cdot_1$ and $\cdot_2$ denote the iterations of the operations $+_1$ and $+_2$ respectively, and similarly for $\sum_1$ and $\sum_2$. We then define

$$
D(\underline{n}) := \left(C(\underline{n}) +_2 B(\underline{n})\right) +_1 \left(A(\underline{n}) +_2 \tilde{t}\right),
$$

lying over the point

$$
\left(x_{\underline{n}}, \alpha(x_{\underline{n}})\right) := \left(x_{\tilde{t}} + \sum_i n_i x_i,\, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})\left(x_{\tilde{t}} + \sum_i n_i x_i\right)\right)
$$

in $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}(\mathcal{O}_K)$. To see this, note that the point $\tilde{t} \in \mathbf{T}(\mathcal{O}_K)$, when viewed as an point in $\mathbf{P}^{\times,\rho-1}$, lies over the point $(x_{\tilde{t}}, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}}))$. In particular, $D(\underline{n})$ belongs to $\mathbf{T}(\mathcal{O}_K)$ and lies above $x_{\underline{n}}$ in $J(\mathcal{O}_K)_{j_b(u)}$.

5.1.2. *Construction of the map E.* The second step is one of the main technical innovations of this work compared to [17]: we extend $D : \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ to a map

$$
E : \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}, \qquad E(\zeta, x) := \zeta \cdot D(x).
$$

The subscript tf stands for "torsion-free quotient" as before, viewed as a subgroup of $\mathbb{G}_m(\mathcal{O}_K)^{\rho-1}$ via a map determined by an arbitrary but fixed choice of a splitting $\mathcal{O}_{K,\mathrm{tf}}^\times \longrightarrow \mathcal{O}_K^\times$. It will be important later on that this map admits an expression in terms of $+_1$, $+_2$ and their iterates $\cdot_1, \cdot_2$.

Notation 5.2.
- Fix a free basis $\mathbf{u} = \{u_1, \ldots, u_\delta\}$ of $\mathcal{O}_{K,\mathrm{tf}}^\times = \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}$, viewed as a subgroup of $\mathcal{O}_K^\times$ via the same choice of splitting as above.
- For each $(\rho-1)$-tuple $u_{k,l} = (1, \ldots, 1, u_k, 1, \ldots, 1) \in \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$, where u_k sits in the l-th coordinate, we denote the corresponding elements in $\mathbf{P}_{|\mathbf{J}\times 0}^\times(\mathcal{O}_K)$ above the point $(x_{\tilde{t}}, 0)$ by $V_{k,l}$, in the sense of Formula (2.6) but with $\mathbf{P}^\times$ in place of $P_K^\times$. Likewise we denote the corresponding element above $(x_i, 0)$ by $W_{k,l,i}$.

Definition 5.3. For $\underline{n} \in \mathbb{Z}^r$, $k \in \{1, \ldots, \delta\}$ and $l \in \{1, \ldots, \rho-1\}$, we define the element

$$
U_{k,l}(\underline{n}) := V_{k,l} +_1 \sum_{1,i} n_i \cdot_1 W_{k,l,i},
$$

which represents multiplication by $u_{k,l}$ and lies above the point $(x_{\underline{n}}, 0)$.

Any element of $\mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1}$ can be described as $\zeta_{\underline{m}} := (\prod_{k=1}^\delta u_k^{m_{k,l}})_{l=1}^{\rho-1}$ for a unique $(\rho-1)$-tuple of δ-tuples of integers $\underline{m} = (m_{k,l})_{\substack{1 \le k \le \delta \\ 1 \le l \le \rho-1}} \in \mathbb{Z}^{\delta(\rho-1)}$. Given $\underline{m} = (m_{k,l})_{\substack{1 \le k \le \delta \\ 1 \le l \le \rho-1}} \in \mathbb{Z}^{\delta(\rho-1)}$, the map E is described explicitly by the following formula:

(5.1) $$\qquad E(\underline{m}, \underline{n}) := E(\zeta_{\underline{m}}, x_{\underline{n}}) = \left(\sum_{2,k,l} m_{k,l} \cdot_2 U_{k,l}(\underline{n})\right) +_2 D(\underline{n}) \in \mathbf{T}(\mathcal{O}_K).$$

One easily checks that $E(\underline{m}, \underline{n})$ lies over the same point $\left(x_{\underline{n}}, \alpha(x_{\underline{n}})\right) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$ as does $D(\underline{n})$. After all, the parameters $\underline{m}$ just encode part of the $\mathbb{G}_m^{\rho-1}$-action on the fibers, as was previously

indicated. Passing from $\mathcal{O}_K$ to $\overline{\mathcal{O}_{K,p}}$, the contribution of the x_i's vanishes and the point becomes $(j_b(u), (hm \cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(j_b(u)))$. In other words, we have $E(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$.

Proposition 5.4. *The map* $\mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1} \times \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ *defined by mapping* $(\varepsilon, \underline{m}, \underline{n})$ *to* $\varepsilon \cdot E(\underline{m}, \underline{n})$ *is bijective.*

Proof. This is immediate after tracking the definitions. As $\underline{n} \in \mathbb{Z}^r$ varies, $x_{\underline{n}} = x_{\tilde{t}} + \sum_i n_i x_i$ runs over all the points of $\mathbf{J}(\mathcal{O}_K)$ that reduce to $j_b(u)$, and $D(\underline{n})$ provides a single point in $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ lying above $x_{\underline{n}}$. In particular, the map D is injective. To get all the points of $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$, one needs to move these around by the simply transitive $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$-action. Since $E(\underline{m}, \underline{n}) = \zeta_{\underline{m}} \cdot D(\underline{n})$ accounts for the torsion-free part of the action by the above discussion, what is left is the torsion part, hence the factor $\mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1}$. $\qquad\square$

5.1.3. *Construction of the map* E'. For the purpose of computing rational points, we wish to parametrize $\mathbf{T}(\mathcal{O}_K)_t$ instead of all of $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$. In this section, we modify the choices of initial points in the above construction of the map E to obtain a map E' that has the advantage that it lands in the correct residue disk, i.e., such that $E'(\underline{m}, \underline{n})$ reduces to t in $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$ for all $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$.

The starting point is the following observation, which asserts that the desired property is already satisfied by E on a certain finite index subgroup of $\mathbb{Z}^{\delta(\rho-1)+r}$.

Proposition 5.5. *Let* q^* *be the exponent of* $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, *or in other words the least common multiple of* $q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$ *for* $i \in \{1, 2, \ldots, s\}$. *Then*

$$E(q^* \underline{m}, q^* \underline{n}) \in \mathbf{T}(\mathcal{O}_K)_t, \qquad \text{for all } (\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}.$$

Proof. We need to show that $E(q^* \underline{m}, q^* \underline{n})$ reduces to the point t in $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$. To that end, we consider the elements

$$A(q^* \underline{n}), \qquad\qquad B(q^* \underline{n}), \qquad\qquad C(q^* \underline{n}), \qquad U_{k,l}(q^* \underline{n}),$$

lying respectively in the fibers of the $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$-torsor $\mathbf{P}^{\times,\rho-1}(\overline{\mathcal{O}_{K,p}})$ above the points

$$(j_b(u), 0), \qquad (0, (hm \cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(j_b(u))), \qquad\qquad (0, 0), \qquad\qquad (j_b(u), 0).$$

The $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$-torsors obtained from $\mathbf{P}^{\times,\rho-1}$ by taking the fibers over each of these points in $\mathbf{J} \times \mathbf{J}^{\vee,\circ}(\overline{\mathcal{O}_{K,p}})$ are all trivial, as at least one coordinate is zero in each case. That is, they are groups isomorphic to $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$, whose group operation is given by $+_2$ in the cases of A and the $U_{k,l}$'s, by $+_1$ in the case of B, and by either of the two operations in the case of C, since $+_1$ and $+_2$ agree above the point $(0, 0)$. By linearity of their definitions, we obtain

$$A(q^* \underline{n}) = q^* \cdot_2 A(\underline{n}) = 1, \qquad B(q^* \underline{n}) = q^* \cdot_1 B(\underline{n}) = 1, \qquad U_{k,l}(q^* \underline{n}) = q^* \cdot_2 U_{k,l}(\underline{n}) = 1,$$

as elements of $\overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$. Finally, for C we have

$$C(q^* \underline{n}) = q^* \cdot_1 \left(\sum_{1,i} n_i \cdot_1 \left(\sum_{2,j} q^* n_j \cdot_2 P_{i,j} \right) \right) = 1.$$

Putting these equations together, we obtain

$$D(q^* \underline{n}) = (1 +_2 1) +_1 (1 +_2 t) = t.$$

Beware of the clash of additive and multiplicative notations here. We therefore have

$$E(q^* \underline{m}, q^* \underline{n}) = q^* \cdot_2 \left(\sum_{2,k,l} m_{k,l} \cdot_2 U_{k,l}(q^* \underline{n}) \right) +_2 D(q^* \underline{n}) = 1 +_2 t = t.$$

This verifies the claim. $\qquad\square$

To get the desired map $\mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \simeq \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)_t$, which agrees with E on $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, is strictly speaking not possible. We can however still obtain a map E' on the entire group $\mathbb{Z}^{\delta(\rho-1)+r}$ that agrees with E on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, but at the cost of allowing p-adic coefficient, i.e., a map

$$E' : \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \simeq \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t.$$

The following proposition is the key to defining this map.

Proposition 5.6. *For any $(\underline{m},\underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$, there is a unique $(\rho-1)$-tuple of roots of unity of prime-to-p orders $\xi(\zeta_{\underline{m}}, x_{\underline{n}}) = \xi(\underline{m},\underline{n}) \in \mathcal{O}_{K,p}^{\times,\rho-1}$ such that $\xi(\underline{m},\underline{n}) \cdot E(\underline{m},\underline{n})$ belongs to $\mathbf{T}(\mathcal{O}_{K,p})_t$.*

Proof. There is a unique multiplicative lift of units

(5.2) $$\iota : \overline{\mathcal{O}_{K,p}}^{\times} = \mathbb{F}_{\mathfrak{p}_1}^{\times} \times \cdots \times \mathbb{F}_{\mathfrak{p}_s}^{\times} \hookrightarrow \mathcal{O}_{K,\mathfrak{p}_1}^{\times} \times \cdots \times \mathcal{O}_{K,\mathfrak{p}_s}^{\times} = \mathcal{O}_{K,p}^{\times},$$

which is right inverse to the reduction map, and which maps precisely onto the prime-to-p part of the roots of unity in $\mathcal{O}_{K,p}$. Denote by ι the induced map $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}) \longrightarrow \mathbb{G}_m^{\rho-1}(\mathcal{O}_{K,p})$ also. Since the action of $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ on $\mathbf{T}(\overline{\mathcal{O}_{K,p}})_{j_b(u)}$ (i.e., the fiber of $\mathbf{T}(\overline{\mathcal{O}_{K,p}})$ containing t) is simply transitive, it follows that each $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-orbit of $\mathbf{T}(\mathcal{O}_{K,p})_{j_b(u)}$ contains a unique point of $\mathbf{T}(\mathcal{O}_{K,p})_t$. The assertion follows. $\square$

Definition 5.7. Given the above notations, we define the map

$$E' : \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_{j_b(u)} \simeq \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t, \qquad E'(\underline{m},\underline{n}) := \xi(\underline{m},\underline{n}) \cdot E(\underline{m},\underline{n}),$$

where $\xi(\underline{m},\underline{n})$ is the $(\rho-1)$-tuple of roots of unity of prime-to-p orders of Proposition 5.6.

Remark 5.8. Note that the definition of E' depends on the fixed basis $\mathbf{x}$ of $\mathbf{J}(\mathcal{O}_K)_0$ and the initial choice of finitely many points of $\mathbf{P}^{\rho-1}(\mathcal{O}_K)$ needed to define the map D. However, it does not depend on the choice of the basis $\mathbf{u}$ of $\mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}$.

Proposition 5.9. *The map E' satisfies the following properties:*
  (1) *The inclusions $\mathbf{T}(\mathcal{O}_K)_t \subseteq E'(\mathbb{Z}^{\delta(\rho-1)+r}) \subseteq \mathbf{T}(\mathcal{O}_{K,p})_t$ hold, where $\mathbf{T}(\mathcal{O}_K)$ is viewed as a subset of $\mathbf{T}(\mathcal{O}_{K,p})$ via the canonical map.*
  (2) *We have the equality $\xi(q^*\mathbb{Z}^{\delta(\rho-1)+r}) = 1$. In particular, the maps E and E' agree on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$.*

Proof. Part (2) follows directly from Propositions 5.5 and the uniqueness of $\xi(\underline{m},\underline{n})$ in Proposition 5.6. Let us prove (1). Given Q in $\mathbf{T}(\mathcal{O}_K)_t \subseteq \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$, there is by Proposition 5.4 a unique ε in $\mathcal{O}_{K,\mathrm{tors}}^{\times,\rho-1}$ and a unique $(\underline{m},\underline{n})$ in $\mathbb{Z}^{\delta(\rho-1)+r}$ such that $\varepsilon E(\underline{m},\underline{n}) = Q$. Using the fact that $\mathcal{O}_{K,\mathrm{tors}}^{\times}$ embeds into the prime-to-p part of $\mathcal{O}_{K,p,\mathrm{tors}}^{\times}$ by Assumption 4.1 (c) that p does not divide $|\mathcal{O}_{K,\mathrm{tors}}^{\times}|$, it follows that ε may be treated as a uniquely determined element of $\mathcal{O}_{K,p}^{\times,\rho-1}$, whose order is finite and coprime to p. By the uniqueness of $\xi(\underline{m},\underline{n})$ in Proposition 5.6, we have $\varepsilon = \xi(\underline{m},\underline{n})$, so that $Q = \varepsilon E(\underline{m},\underline{n}) = \xi(\underline{m},\underline{n})E(\underline{m},\underline{n}) = E'(\underline{m},\underline{n})$. $\square$

5.1.4. *Description of E' in terms of biextension laws.* An important feature for proving a p-adic interpolation statement (Theorem 4.8) is an explicit description of E' in terms of the biextension laws. The following can also be taken as an alternative construction of the map E'.

The strategy for describing E' is to modify the choices of the initial points in the construction of the maps D and E. Note that the images $\overline{P_{i,j}}, \overline{R_i}, \overline{S_j}$ in $\mathbf{P}^{\times,\rho-1}(\overline{\mathcal{O}_{K,p}})$ lie over points of the form $(0,*), (0,*)$ and $(*,0)$ respectively. The fibers over these points are canonically isomorphic to $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}) = \overline{\mathcal{O}_{K,p}}^{\times,\rho-1}$ by the discussion in Section 2.1.3. The neutral element 1 in these fibers thus makes sense, and, e.g., there is a unique $\xi_{i,j} \in \mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ such that $\xi_{i,j}\overline{P_{i,j}} = 1$, and we set $P'_{i,j} = \iota(\xi_{i,j})P_{i,j}$, where ι is the lift (5.2). One defines points $R'_i, S'_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$ in a similar

fashion. We similarly modify the points $V_{k,l}$ and $W_{k,l,i}$ of Notation 5.2. Alternatively, one can multiply the chosen basis of the torsion-free part of $\mathcal{O}_K$-units $\mathbf{u} = \{u_1, \ldots, u_\delta\}$ by suitable roots of unity of prime-to-p order in $\mathcal{O}_{K,p}$, so that the resulting units are congruent to 1 modulo $p\mathcal{O}_{K,p}$.

Using these points, we define

$$A'(\underline{n}) = \sum\nolimits_{2,j} n_j \cdot_2 S'_j, \quad B'(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 R'_i, \quad C'(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 \left(\sum\nolimits_{2,j} n_j \cdot_2 P'_{i,j} \right),$$

and

$$U'_{k,l}(\underline{n}) := V'_{k,l} +_1 \sum_{1,i} n_i \cdot_1 W'_{k,l,i}.$$

Proposition 5.10. *With the above notations, given $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$, we have*

$$E'(\underline{m}, \underline{n}) = \left(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U'_{k,l}(\underline{n}) \right) +_2 \left(\left(C'(\underline{n}) +_2 B'(\underline{n}) \right) +_1 \left(A'(\underline{n}) +_2 \tilde{t} \right) \right).$$

Proof. A formal computation similar to the proof of Proposition 5.5 shows that the expression defined by the right hand side lies in $\mathbf{T}(\mathcal{O}_{K,p})_t$. Since this expression is obtained by the same operations in terms of $+_1, +_2, \cdot_1,$ and $\cdot_2$ as $E(\underline{m}, \underline{n})$ (see (5.1)), apart from the $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification of the initial points, it follows from an analogue of (2.7) that the right hand side expression differs from $E(\underline{m}, \underline{n})$ only by $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification. In other words, the right hand side must equal $\xi'(\underline{m}, \underline{n}) E(\underline{m}, \underline{n})$ for some $\xi'(\underline{m}, \underline{n}) \in \iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$. Using the uniqueness of $\xi(\underline{m}, \underline{n})$ in Proposition 5.6, this proves the indicated equality. $\square$

5.2. **The p-adic interpolation.** The remaining part of this section aims to prove Theorem 4.8. This is done along the same lines as [17, §3 & §5.1], but in a more general context. We will use the following result, whose proof will be given shortly, to deduce Theorem 4.8.

Proposition 5.11.

(1) *Let X and Y be smooth schemes over $\mathcal{O}_K$ of relative dimensions m and n respectively. Let $f : X \longrightarrow Y$ be a morphism of $\mathcal{O}_K$-schemes and let $x \in X(\overline{\mathcal{O}_{K,p}})$ be a point. Any choice of local parameters (see Notation 5.13) followed by restriction of scalars (see Remark 5.16) induces identifications $X(\mathcal{O}_{K,p})_x \simeq \mathbb{Z}_p^{dm}$ and $Y(\mathcal{O}_{K,p})_{f(x)} \simeq \mathbb{Z}_p^{dn}$ such that the composition of maps*

$$\mathbb{Z}_p^{dm} \simeq X(\mathcal{O}_{K,p})_x \xrightarrow{f} Y(\mathcal{O}_{K,p})_{f(x)} \simeq \mathbb{Z}_p^{dn}$$

is given by convergent power series with $\mathbb{Z}_p$-coefficients.

(2) *Let $G \longrightarrow Y$ be a smooth group scheme with identity section e, where Y is smooth over $\mathcal{O}_K$. Let $y \in Y(\overline{\mathcal{O}_{K,p}})$ be a point. The map*

$$\mathbb{Z} \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow G(\mathcal{O}_{K,p})_{e(y)}, \qquad (z, g) \mapsto z \cdot g$$

extends to a map $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow G(\mathcal{O}_{K,p})_{e(y)}$, which describes the $\mathbb{Z}_p$-module action on fibers over $Y(\mathcal{O}_{K,p})_y$, and which is given by convergent power series with $\mathbb{Z}_p$-coefficients after choosing local parameters for $G \longrightarrow Y$ at $e(y)$ and restricting scalars.

Remark 5.12. We postpone the proof of this result to the end of this section. The proof of (1) relies on the description of local parameters at a point x using blow-ups. The proof of (2) uses the formal logarithm and exponential maps to interpret the action $z \cdot g$ as $\exp(z \cdot \log(g))$. Since exp and log are given by convergent power series (see Proposition 5.18 below), one can extend $z \cdot g$ to allow $\mathbb{Z}_p$-coefficients. The proofs are technical and quite general. For the sake of clarity and readability, we have chosen to defer them to after the proof of Theorem 4.8.

Proof of Theorem 4.8. By Proposition 5.10, the map E' is described by the operations $+_1$ and $+_2$, and their iterates $\cdot_1$ and $\cdot_2$. Proposition 5.11 (2) applied respectively to the group schemes $\mathbf{P}^\times \longrightarrow \mathbf{J}^{\vee,\circ}$ and $\mathbf{P}^\times \longrightarrow \mathbf{J}$, implies that the operations $(n, g) \mapsto n \cdot_1 g$ and $(n, g) \mapsto n \cdot_2 g$ for

$n \in \mathbb{Z}$ extend to $n \in \mathbb{Z}_p$, and the resulting operations are given by convergent power series with $\mathbb{Z}_p$-coefficients. The expression in Proposition 5.10 therefore makes sense with $(\underline{m}, \underline{n}) \in \mathbb{Z}_p^{\delta(\rho-1)} \times \mathbb{Z}_p^r$. Allowing for $\mathbb{Z}_p$-coefficients using the extended actions $\cdot_1$ and $\cdot_2$ thus gives rise via the formula in Proposition 5.10 to the desired map

$$\kappa := \kappa_{\mathbf{x}, \mathbf{u}} : \mathbb{Z}_p^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t,$$

$$\kappa(\underline{m}, \underline{n}) := \left(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U'_{k,l}(\underline{n}) \right) +_2 \left((C'(\underline{n}) +_2 B'(\underline{n})) +_1 \left(A'(\underline{n}) +_2 \tilde{t} \right) \right),$$

depending on the bases $\mathbf{x}$ of $\mathbf{J}(\mathcal{O}_K)_0$ and $\mathbf{u}$ of $\mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}$, and which by definition agrees with E' when restricted to $\mathbb{Z}^{\delta(\rho-1)+r} \subset \mathbb{Z}_p^{\delta(\rho-1)+r}$.

By Proposition 5.11 (1), both operations

$$+_1 : \mathbf{P}^{\times, \rho-1} \times_{(\mathbf{J}^\vee, \circ)^{\rho-1}} \mathbf{P}^{\times, \rho-1} \longrightarrow \mathbf{P}^{\times, \rho-1},$$

$$+_2 : \mathbf{P}^{\times, \rho-1} \times_{\mathbf{J}} \mathbf{P}^{\times, \rho-1} \longrightarrow \mathbf{P}^{\times, \rho-1}$$

induce maps given by convergent power series over $\mathbb{Z}_p$ on the appropriate residue disks after choosing a regular system of local parameters inducing $\mathbf{P}^{\times, \rho-1}(\mathcal{O}_{K,p})_x \simeq \mathbb{Z}_p^{d(g+g(\rho-1)+\rho-1)}$ upon restricting scalars from $\mathcal{O}_{K,p}$ to $\mathbb{Z}_p$. Since the composition of convergent power series with $\mathbb{Z}_p$-coefficients again produces convergent power series with $\mathbb{Z}_p$-coefficients, the map κ is indeed given by a tuple of convergent p-adic power series. $\qquad\square$

5.2.1. *Local parameters and blow-ups.*

Notation 5.13. We fix a prime $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ above p. Denote by π a uniformizer of $\mathcal{O}_{K,\mathfrak{p}}$. Let X be a smooth scheme over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension m. Similarly to before, for a point $x \in X(\mathbb{F}_{\mathfrak{p}})$, we denote by $X(\mathcal{O}_{K,\mathfrak{p}})_x$ the set of all $\mathcal{O}_{K,\mathfrak{p}}$-points reducing to x modulo $\mathfrak{p}$. By smoothness, the maximal ideal $\mathfrak{m}_x$ admits a regular system of parameters $(\pi, t_1, t_2, \ldots, t_m)$.

The point x factors through the natural map $\mathrm{Spec}\,\widehat{\mathcal{O}_{X,x}} \longrightarrow X$, and $X(\mathcal{O}_{K,\mathfrak{p}})_x$ bijectively corresponds to $\mathrm{Spec}\,\widehat{\mathcal{O}_{X,x}}(\mathcal{O}_{K,\mathfrak{p}})_x$. The isomorphism $\mathcal{O}_K[[t_1, \ldots, t_m]] \simeq \widehat{\mathcal{O}_{X,x}}$ then shows that there is a bijection of sets

$$t = (t_1, t_2, \ldots, t_m) : X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{\sim} (\mathfrak{m}_{K,\mathfrak{p}})^m$$
$$\tilde{x} \longmapsto (t_1(\tilde{x}), \ldots, t_m(\tilde{x})).$$

After dividing by π, one gets

$$(5.3) \qquad \tilde{t} = \left(\frac{t_1}{\pi}, \frac{t_2}{\pi}, \ldots, \frac{t_m}{\pi} \right) : X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{\sim} (\mathcal{O}_{K,\mathfrak{p}})^m .$$

Let $f : X \longrightarrow Y$ be a morphism of schemes, which are smooth over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimensions m and n respectively. Denote the analogous choice of a regular system of parameters of Y at $f(x)$ by $s_1, s_2, \ldots, s_n$, and the corresponding bijection by

$$\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)} \longrightarrow (\mathcal{O}_{K,\mathfrak{p}})^n.$$

The immediate goal is the following.

Proposition 5.14. *In the above setting, the composition*

$$f' : (\mathcal{O}_{K,\mathfrak{p}})^m \xrightarrow{\tilde{t}^{-1}} X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{f} Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)} \xrightarrow{\tilde{s}} (\mathcal{O}_{K,\mathfrak{p}})^n$$

is given by a n-tuple of convergent power series with coefficients in $\mathcal{O}_{K,\mathfrak{p}}$.

Here by convergent power series we mean elements of $\mathcal{O}_{K,\mathfrak{p}}\langle X_1, X_2, \ldots, X_m \rangle$, the p-adic, or equivalently π-adic, completion of $\mathcal{O}_{K,\mathfrak{p}}[X_1, X_2, \ldots, X_m]$. The proof of Proposition 5.14 follows closely [17, §3] by investigating the geometry of the situation.

Proof. By shrinking X to a sufficiently small affine open neighbourhood of x, we may assume that $t_1, t_2, \ldots, t_m$ are regular global functions, which define an étale map

$$t = (t_1, t_2, \ldots, t_m) : X \longrightarrow \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} = \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}[X_1, \ldots, X_m],$$

mapping x to the origin over $\mathbb{F}_{\mathfrak{p}}$, i.e., the point corresponding to $(\pi, X_1, \ldots, X_d)$. By possibly shrinking X further, we may assume that x is in fact the only preimage of the origin.

Note that a point $\tilde{x} : \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}} \longrightarrow X$ reduces to x if and only if the pullback of x along $\tilde{x}$ is the effective Cartier divisor cut out by π. Consequently, the universal property of the blowup $\operatorname{Bl}_x X$ of X at x implies that every $\tilde{x} \in X(\mathcal{O}_{K,\mathfrak{p}})_x$ factors uniquely through $\operatorname{Bl}_x X$, and more precisely through the open subscheme $\operatorname{Bl}_x^{(\pi)} X$ of $\operatorname{Bl}_x X$, where π is the generator of the exceptional divisor. Thus, we have a natural identification between $X(\mathcal{O}_{K,\mathfrak{p}})_x$ and $\operatorname{Bl}_x^{(\pi)} X(\mathcal{O}_{K,\mathfrak{p}})$.

Up to this identification, the map $\tilde{t}$ can be described as follows. We consider the analogous construction for the $\mathbb{F}_{\mathfrak{p}}$-origin $o : \operatorname{Spec} \mathbb{F}_{\mathfrak{p}} \longrightarrow \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ from which we get $\operatorname{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ and

$$\operatorname{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} = \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}[\tilde{X}_1, \ldots, \tilde{X}_m],$$

where in the expression above $\tilde{X}_i = X_i/\pi$. Since blowing up commutes with flat base change, we obtain a cartesian diagram of schemes

(5.4)
$$
\begin{array}{ccccc}
\operatorname{Bl}_x^{(\pi)} X & \hookrightarrow & \operatorname{Bl}_x X & \longrightarrow & X \\
\downarrow{\scriptstyle \tilde{t}} & \square & \downarrow & \square & \downarrow{\scriptstyle t} \\
\operatorname{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \hookrightarrow & \operatorname{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \longrightarrow & \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} .
\end{array}
$$

The map $\tilde{t}$ of (5.3) is simply the morphism $\tilde{t}$ in the above diagram evaluated at $\mathcal{O}_{K,\mathfrak{p}}$-points. The notations are therefore compatible.

The map $\tilde{t}_{\mathbb{F}_{\mathfrak{p}}}$, obtained from base-changing the diagram (5.4) to $\mathbb{F}_{\mathfrak{p}}$, can be non-canonically interpreted as the tangent map at x between the respective tangent spaces. In particular, it is an isomorphism. Since $\tilde{t}$ is étale, $\tilde{t}$ is an isomorphism when base-changed to $\mathcal{O}_{K,\mathfrak{p}}/(\pi^j)$ for every j. Denoting the rings of global functions of the affine schemes in question by $\mathcal{O}(\operatorname{Bl}_x^{(\pi)} X)$ and $\mathcal{O}(\operatorname{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}})$ respectively, we infer that their π-adic completions are the same, i.e.,

(5.5) $$\mathcal{O}(\widehat{\operatorname{Bl}_x^{(\pi)} X}) \simeq \mathcal{O}(\widehat{\operatorname{Bl}_o^{(\pi)} \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}}) = \mathcal{O}_{K,\mathfrak{p}}\widehat{[\tilde{X}_1, \ldots,]}, \tilde{X}_m] = \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \ldots, \tilde{X}_m \rangle,$$

both being equal to the algebra of integral formal power series converging on the unit disk.

We perform the same analysis for Y, $f(x)$, and its fixed system of parameters s_i. Using again the universal property of the blowup of Y at $f(x)$, we obtain that f also induces a morphism

$$\tilde{f} : \operatorname{Bl}_x^{(\pi)} X \longrightarrow \operatorname{Bl}_{f(x)}^{(\pi)} Y,$$

which on the level of $\mathcal{O}_{K,\mathfrak{p}}$-points may be identified with $f : X(\mathcal{O}_{K,\mathfrak{p}})_x \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)}$. Taking the p-adic completion of the associated ring map $\mathcal{O}(\operatorname{Bl}_{f(x)}^{(\pi)} Y) \longrightarrow \mathcal{O}(\operatorname{Bl}_x^{(\pi)} X)$ and conjugating by the isomorphisms (5.5) for X and Y then yields a map

$$\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_n \rangle \longrightarrow \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \ldots, \tilde{X}_m \rangle.$$

This is described by specifying n-tuple of elements of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \ldots, \tilde{X}_m \rangle$ as images of the variables $\tilde{Y}_i$. Since the map f' is obtained from the above map of rings by applying the functor $\operatorname{Hom}_{\operatorname{Alg}_{\mathcal{O}_{K,\mathfrak{p}}}}(-, \mathcal{O}_{K,\mathfrak{p}})$, it follows that f' is described by these power series. This proves the claim. $\square$

Remark 5.15. It will be useful later to note that $\mathcal{O}_{X,x}$ naturally embeds into $\mathcal{O}(\widehat{\mathrm{Bl}_x^{(\pi)}X})$. As in the previous proof, let us replace X by a sufficiently small affine neighbourhood of x. The maximal ideal of $\mathcal{O}_X(X)$ corresponding to x becomes (π) in $\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$, and is therefore mapped to the radical in $\mathcal{O}(\widehat{\mathrm{Bl}_x^{(\pi)}X})$. There is thus an induced map $\mathcal{O}_{X,x} \longrightarrow \mathcal{O}(\widehat{\mathrm{Bl}_x^{(\pi)}X})$. Concerning the injectivity, after taking completions at the maximal ideal, the map becomes the map

$$\mathcal{O}[[X_1,\ldots,X_m]] \hookrightarrow \mathcal{O}[[\tilde{X}_1,\ldots,\tilde{X}_m]]$$

given by $X_i \mapsto p\tilde{X}_i$, which is injective.

Remark 5.16. It will be beneficial to replace the power series expressions with $\mathcal{O}_{K,\mathfrak{p}}$-coefficients by convergent power series with $\mathbb{Z}_p$-coefficients. To that end, we let

$$k = ef = \mathrm{rank}_{\mathbb{Z}_p}\mathcal{O}_{K,\mathfrak{p}},$$

following our earlier convention, and fix a free basis $e_1, e_2, \ldots, e_k$ of $\mathcal{O}_{K,\mathfrak{p}}$ as a $\mathbb{Z}_p$-module. Expressing everything with respect to this basis, the description of maps $\mathcal{O}_{K,\mathfrak{p}}^m \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^n$ in terms of power series gives rise to a power series description of maps $\mathbb{Z}_p^{km} \longrightarrow \mathbb{Z}_p^{kn}$. More precisely, upon the introduction of formal variables $X_{i,j}$ by the rule

(5.6) $$X_i = X_{i,1}e_1 + X_{i,2}e_2 + \cdots + X_{i,k}e_k,$$

any convergent power series $f \in \mathcal{O}_{K,\mathfrak{p}}\langle X_1, X_2, \ldots X_m\rangle$ can be written as

$$f = f_1e_1 + f_2e_2 + \cdots + f_ke_k,$$

for a unique k-tuple of power series $f_1, f_2, \ldots, f_k \in \mathbb{Z}_p\langle X_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq k\rangle$.

Remark 5.17. Keeping the notation from the proof of Proposition 5.14, the map

$$\tilde{f}_{\mathbb{F}_\mathfrak{p}} : (\mathrm{Bl}_x^{(\pi)}X)_{\mathbb{F}_\mathfrak{p}} \longrightarrow (\mathrm{Bl}_{f(x)}^{(\pi)}Y)_{\mathbb{F}_\mathfrak{p}}$$

can be identified with the tangent map of $f_{\mathbb{F}_\mathfrak{p}} : X_{\mathbb{F}_\mathfrak{p}} \longrightarrow Y_{\mathbb{F}_\mathfrak{p}}$ at x. Assume that this map is injective. By a lift of a suitable $\mathbb{F}_\mathfrak{p}$-affine change of coordinates on $(\mathrm{Bl}_{f(x)}^{(\pi)}Y)_{\mathbb{F}_\mathfrak{p}}$, one can ensure that the map $(f')^\# : \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_n\rangle \longrightarrow \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \ldots, \tilde{X}_m\rangle$ is given by $\tilde{Y}_i \mapsto \tilde{X}_i$ for $i \leq m$ and by $\tilde{Y}_i \mapsto 0$ for $i > m$. In other words, the parameters s_i and t_i may be chosen so that $f^\#(s_i) = t_i$ for $i \leq m$ and $s_{m+1}, \ldots s_n$ generate the kernel of the map $f^\# : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$. In that case, $X(\mathcal{O}_{K,\mathfrak{p}})_x$ is embedded in $Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)}$ and, in the chosen coordinates, equal to the vanishing locus of $\tilde{Y}_{m+1}, \ldots, \tilde{Y}_n$. As in Remark 5.16, we can identify the embedding with the affine embedding $\mathbb{Z}_p^{km} \longrightarrow \mathbb{Z}_p^{kn}$, whose image is cut out by the $k(n-m)$ variables $\tilde{Y}_{i,j}$, with $m < i \leq n$ and $1 \leq j \leq k$.

5.2.2. *The exp-log argument.* We now focus on the special case where $Y \longrightarrow \mathrm{Spec}\,\mathcal{O}_{K,\mathfrak{p}}$ is a smooth scheme of relative dimension n, and $X = G$ is a smooth commutative group scheme over Y of relative dimension m. Beware that m from the previous discussion corresponds to $m + n$ in the situation at hand. Hopefully, this will not cause too much confusion. Let $e : Y \longrightarrow G$ denote the identity section. We consider a point $y \in Y(\mathbb{F}_\mathfrak{p})$ and the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_y$.

As done previously, we may replace Y by $\mathrm{Spec}\,\mathcal{O}_{Y,y}$ and G by $G_{\mathcal{O}_{Y,y}}$. We fix a system of parameters $\pi, s_1, s_2, \ldots, s_n$, which induce a bijection $\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_y \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^n$.

By [33, 05D9], there is an affine open neighborhood $\mathrm{Spec}\,B = U \subseteq G_{\mathcal{O}_{Y,y}}$ of $e(y)$ such that e factors through U and such that, denoting by I the kernel of the associated map $e^\# : B \longrightarrow \mathcal{O}_{Y,y}$, I/I^2 is a free $\mathcal{O}_{Y,y}$-module of rank m. Upon fixing elements $t_1, t_2, \ldots, t_m \in I$ that form a free basis of I/I^2, the sequence $\pi, s_1, s_2, \ldots, s_n, t_1, t_2, \ldots, t_m$ forms a system of parameters of $G_{\mathcal{O}_{Y,y}}$ at $e(y)$. This establishes a bijection $(\tilde{s}, \tilde{t}) : G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^{n+m}$.

We consider the formal $\mathcal{O}_{Y,y}$-group $\widehat{G_{\mathcal{O}_{Y,y}}}$, i.e., the completion of $G_{\mathcal{O}_{Y,y}}$ with respect to the ideal of the identity section. In terms of the chosen coordinates, it is the formal spectrum of the I-adic completion of B, which in turn is the formal power series ring $\mathcal{O}_{Y,y}[[t_1, t_2, \ldots, t_m]]$. The group operation then induces a m-dimensional commutative formal group law

$$F_G(\underline{U}, \underline{V}) = (F_1, \ldots, F_m)(U_1, \ldots, U_m, V_1, \ldots, V_m)$$

over $\mathcal{O}_{Y,y}$, in the sense of [24]. By [24, Theorem 1], over $\mathcal{O}_{Y,y} \otimes \mathbb{Q}$, there are mutually inverse isomorphisms of formal group laws

$$F_{G,\mathbb{Q}} \xrightarrow[\overset{\log}{\underset{\exp}{\longleftarrow}}]{} (\widehat{\mathbb{G}}_a)^m_{\mathbb{Q}},$$

where $(\widehat{\mathbb{G}}_a)^m$ denotes the m-dimensional addition law given by the polynomials $U_i + V_i$ treated as power series over $\mathcal{O}_{Y,y}$. The subscript $\mathbb{Q}$ denotes the "formal base change" to $\mathbb{Q}$. Explicitly, fixing a basis of invariant differentials $\omega_1, \ldots, \omega_m \in \bigoplus_{i=1}^m \mathcal{O}_{Y,y}[[t_1, \ldots, t_m]]\mathrm{d}t_i$ of F_G in the sense of [24, Proposition 1.1], log is given by a m-tuple of formal power series

$$L_1, L_2, \ldots, L_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \ldots, t_m]]$$

characterized by the properties

(5.7) $$L_i(0, \ldots, 0) = 0, \quad \mathrm{d}L_i = \omega_i, \quad i = 1, 2, \ldots, m,$$

and that, additionally, each L_i equals t_i in degree 1. The exponential is then given as a formal inverse to log, i.e., by a m-tuple of power series $E_1, E_2, \ldots, E_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \ldots, t_m]]$ characterized by the identities

(5.8) $$E_i(L_1, L_2, \ldots, L_m) = t_i, \quad i = 1, 2, \ldots, m.$$

It follows that each E_i equals t_i in degrees ≤ 1.

The fibers of the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_y$ naturally carry the structure of $\mathbb{Z}_p$-modules. In fact, given $\tilde{y} \in Y(\mathcal{O}_{K,\mathfrak{p}})_y$, the fiber over $\tilde{y}$ is the kernel of the reduction map $G_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}) \longrightarrow G_{\tilde{y}}(\mathbb{F}_\mathfrak{p})$, where $G_{\tilde{y}}$ denotes the $\mathcal{O}_{K,\mathfrak{p}}$-group scheme obtained from G by base change along $\tilde{y}$. This kernel is the set of $\mathcal{O}_{K,\mathfrak{p}}$-points of the associated formal group, $\widehat{G}_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}) = \varprojlim_j \widehat{G}_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}/p^j \mathcal{O}_{K,\mathfrak{p}})$, and the group law of $\widehat{G}_{\tilde{y}}$ may be viewed as the "formal base change" of the formal group law for $\widehat{G_{\mathcal{O}_{Y,y}}}$ above. The fact that any formal group law is of the form $\underline{U} + \underline{V} +$ (higher order terms) shows that $\widehat{G}_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}/p^j \mathcal{O}_{K,\mathfrak{p}})$ is an abelian group annihilated by p^j. This verifies the claim.

The goal is to p-adically interpolate the function $z \mapsto z \cdot g$ for $g \in G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$, or more precisely, to describe the action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ arising from the $\mathbb{Z}_p$-action on the fibers, in terms of convergent power series. This is done by interpreting the formal logarithm and exponential as convergent power series.

Proposition 5.18. *The formal logarithm and exponential induce the mutually inverse maps* log *and* exp

$$G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \xrightarrow[\simeq]{(\tilde{s}, \tilde{t})} (\mathcal{O}_{K,\mathfrak{p}})^{n+m} \xrightarrow[\overset{\log}{\underset{\exp}{\longleftarrow}}]{} (\mathcal{O}_{K,\mathfrak{p}})^{n+m},$$

which are given by convergent power series, i.e., elements of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_n, \tilde{X}_1, \ldots, \tilde{X}_m \rangle$. Given $z \in \mathbb{Z}_p$ and $g \in G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$, viewed as an element of $(\mathcal{O}_{K,\mathfrak{p}})^{n+m}$ via $(\tilde{s}, \tilde{t})$, we have the equality $z \cdot g = \exp(z \cdot \log(g))$. Consequently, the action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ is described by convergent power series with coefficients in $\mathbb{Z}_p$.

Proof. Write $L_i = \sum_{J \neq 0} a_{i,J} \underline{t}^J$ and $E_i = \sum_{J \neq 0} b_{i,J} \underline{t}^J$ for the formal power series, which are respectively the components of the formal logarithm and formal exponential. It can be deduced from the identity (5.7) that

(5.9) $$|J| a_{i,J} \in \mathcal{O}_{Y,y}, \qquad \text{for all } J,$$

and a formal computation of the exponential based on the identities (5.8) as in [23, A.4.6], together with (5.9), shows that

$$(5.10) \qquad (|J|!)b_{i,J} \in \mathcal{O}_{Y,y}, \qquad \text{for all } J.$$

The induced map $\log : \mathcal{O}_{K,\mathfrak{p}}^{n+m} \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^{n+m}$ is then given by the identity on the first n components, which correspond to the base $Y(\mathcal{O}_{K,\mathfrak{p}})_y$, and by the power series

$$(5.11) \qquad \tilde{L}_i(\underline{\tilde{X}}) = \pi^{-1} \sum_{J \neq 0} a_{i,J} (\pi \underline{\tilde{X}})^J = \sum_{J \neq 0} \frac{\pi^{|J|-1}}{|J|} (|J| a_{i,J})(\underline{\tilde{X}})^J, \qquad i = 1, \ldots, m$$

on the remaining components. Here $|J| a_{i,J}$ is considered as an element of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_m \rangle$ in the sense of Remark 5.15.

Its formal inverse is given by the analogous modification of the formal exponential. Namely, $\exp : \mathcal{O}_{K,\mathfrak{p}}^{n+d} \longrightarrow \mathcal{O}_{K,\mathfrak{p}}^{n+d}$ is given by the identity on the first n components and on the remaining m components by the formal power series

$$(5.12) \qquad \tilde{E}_i(\underline{\tilde{X}}) = \pi^{-1} \sum_{J \neq 0} b_{i,J} (\pi \underline{\tilde{X}})^J = \sum_{J \neq 0} \frac{\pi^{|J|-1}}{|J|!} ((|J|!)b_{i,J})(\underline{\tilde{X}})^J, \qquad i = 1, \ldots, m,$$

where $(|J|!)b_{i,J}$ is again considered as an element of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \ldots, \tilde{Y}_m \rangle$.

To conclude that the power series (5.11) and (5.12) define elements of the ring $\mathcal{O}_{K,\mathfrak{p}}\langle \underline{\tilde{Y}}, \underline{\tilde{X}} \rangle$, it is enough to observe that the coefficients $\pi^{|J|-1}/(|J|!)$, and thereby also $\pi^{|J|-1}/|J|$, are integral and converge to zero p-adically as $|J| \to \infty$. These properties hold thanks to the imposed condition $e < p - 1$ in Assumption 4.1 (b) on the ramification index, since the p-adic valuations satisfy

$$v_p \left(\frac{\pi^{k-1}}{k!} \right) \geq \frac{k-1}{e} - \frac{k-1}{p-1} = \frac{(k-1)(p-1-e)}{e(p-1)},$$

which is then non-negative for all $k \geq 1$ and tends to ∞ as $k \to \infty$.

Finally, we may interpret log and exp as given by $ef(n+m)$ power series with coefficients in $\mathbb{Z}_p$ following Remark 5.16. The action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ then becomes a p-adically continuous map $\mathbb{Z}_p \times \mathbb{Z}_p^{ef(n+m)} \longrightarrow \mathbb{Z}_p^{ef(n+m)}$, which extends the map

$$(z, g) \mapsto z \cdot g = \exp(z \cdot \log(g))$$

from $\mathbb{Z} \times \mathbb{Z}_p^{ef(n+m)}$ to $\mathbb{Z}_p \times \mathbb{Z}_p^{ef(n+m)}$. The same is true concerning the map on $\mathbb{Z}_p \times \mathbb{Z}_p^{ef(n+m)}$ given by $(z, g) \mapsto \exp(z \cdot \log(g))$, and it follows that these two maps agree. In particular, the $\mathbb{Z}_p$-action map is described by convergent power series with $\mathbb{Z}_p$-coefficients as claimed. $\square$

5.2.3. *Proof of Proposition 5.11.*

Proof. As in (4.3), a point $x \in X(\overline{\mathcal{O}_{K,p}})$ is given by a s-tuple $x_1 \in X(\mathbb{F}_{\mathfrak{p}_1}), \ldots, x_s \in X(\mathbb{F}_{\mathfrak{p}_s})$, and we have $X(\mathcal{O}_{K,p})_x = \prod_{i=1}^s X(\mathcal{O}_{K,\mathfrak{p}_i})_{x_i}$. Similarly, for any map $f : X \longrightarrow Y$ of $\mathcal{O}_K$-schemes, the induced map $f : X(\mathcal{O}_{K,p})_x \longrightarrow Y(\mathcal{O}_{K,p})_{f(x)}$ decomposes into the product over i of the maps $f : X(\mathcal{O}_{K,\mathfrak{p}})_{x_i} \longrightarrow Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x_i)}$. Part (1) thus follows from Proposition 5.14 and Remark 5.16.

Likewise, we have $G(\mathcal{O}_{K,p})_{e(y)} = \prod_{i=1}^s G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)}$, and thus $G(\mathcal{O}_{K,p})_{e(y)}$ has a $\mathbb{Z}_p$-module structure on fibers over $Y(\mathcal{O}_{K,p})_y = \prod_{i=1}^s Y(\mathcal{O}_{K,\mathfrak{p}_i})_{y_i}$. By Proposition 5.18, each of the action maps $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)} \longrightarrow G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)}$ is given by convergent power series with $\mathbb{Z}_p$-coefficients. The action map for $G(\mathcal{O}_{K,p})_{e(y)}$ is then obtained by taking the product of the above action maps and precomposing with $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \longrightarrow \prod_i (\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)})$, where $\mathbb{Z}_p$ is embedded into the s copies of $\mathbb{Z}_p$ diagonally. It follows that the map has a description in terms of convergent power series over $\mathbb{Z}_p$ as well, which proves (2). $\square$

6. BOUNDING THE NUMBER OF RATIONAL POINTS

We are now in a position to prove Theorem 4.11 of Section 4, which gives a conditional upper bound on the size of the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$.

The tangent map of the lifted Abel–Jacobi map $\tilde{j}_b^U : \mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_{\mathfrak{p}}} \hookrightarrow \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}}$ of Proposition 3.11 is injective at $\mathfrak{p}$ by smoothness (Assumption 4.1 (a)). It follows, by Remark 5.17, that $\mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_{\mathfrak{p}}}$ is a complete intersection in $\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}}$, i.e., it is cut out by $g + \rho - 2$ elements

$$f_1^{\mathfrak{p}}, \dots, f_{g+\rho-2}^{\mathfrak{p}} \in \mathcal{O}(\widehat{\mathrm{Bl}_{t_{\mathfrak{p}}}^{(\pi_{\mathfrak{p}})}}(\mathbf{T})),$$

which generate the kernel of the surjection

$$(\tilde{j}_b^U)_{\mathfrak{p}}^{\#} : \mathcal{O}(\widehat{\mathrm{Bl}_{t_{\mathfrak{p}}}^{(\pi_{\mathfrak{p}})}}(\mathbf{T})) \longrightarrow \mathcal{O}(\widehat{\mathrm{Bl}_{u_{\mathfrak{p}}}^{(\pi_{\mathfrak{p}})}}(\mathbf{U})).$$

After restricting scalars from $\mathcal{O}_{K,\mathfrak{p}}$ to $\mathbb{Z}_p$ (see Remark 5.16), each $f_i^{\mathfrak{p}}$ corresponds uniquely to a $k_{\mathfrak{p}}$-tuple $(f_{i,1}^{\mathfrak{p}}, \dots, f_{i,k_{\mathfrak{p}}}^{\mathfrak{p}})$ of power series in $(g + \rho - 1)k_{\mathfrak{p}}$ variables with coefficients in $\mathbb{Z}_p$.

In conclusion, the p-adic analytic submanifold $\mathbf{U}(\mathcal{O}_{K,p})_u$ of $\mathbf{T}(\mathcal{O}_{K,p})_t$ is cut out by $(g + \rho - 2)\sum_{\mathfrak{p}|p} k_{\mathfrak{p}} = (g + \rho - 2)d$ convergent power series with coefficients in $\mathbb{Z}_p$. The computation of the desired intersection is accomplished by pulling all equations back via the map of p-adic analytic manifolds $\kappa = \kappa_{\mathbf{x},\mathbf{u}} : \mathbb{Z}_p^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$ of Theorem 4.8 whose image is $\mathbf{Y}_t$ by Corollary 4.10.

Definition 6.1. The elements $\kappa^* f_{i,j}^{\mathfrak{p}}$, with $1 \le i \le g + \rho - 2$, $1 \le j \le k_{\mathfrak{p}}$, and $\mathfrak{p}|p$, all lie in $R = \mathbb{Z}_p\langle z_1, \dots, z_{\delta(\rho-1)+r}\rangle$. Let $I_{\mathbf{U},u} := I_{\mathbf{U},u,\kappa}$ denote the ideal of R generated by these elements, and denote by $A_{\mathbf{U},u} := R/I_{\mathbf{U},u}$ the resulting quotient ring.

The intersection is algebraically expressed as the tensor product of rings, i.e., by taking the quotient by $I_{\mathbf{U},u}$. It follows that there is a bijection

(6.1) $$\mathrm{Hom}(A_{\mathbf{U},u}, \mathbb{Z}_p) \longleftrightarrow \kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t).$$

Let $\overline{\kappa^* f_{i,j}^{\mathfrak{p}}} \in \mathbb{F}_p[z_1, \dots, z_{\delta(\rho-1)+r}]$ denote the reductions of the convergent power series modulo p. These elements generate the ideal $\bar{I}_{\mathbf{U},u} = I_{\mathbf{U},u}\mathbb{F}_p[z_1, \dots, z_{\delta(\rho-1)+r}]$. Consider the quotient $\mathbb{F}_p$-algebra

$$\overline{A}_{\mathbf{U},u} := A_{\mathbf{U},u} \otimes \mathbb{F}_p = \mathbb{F}_p[z_1, \dots, z_{\delta(\rho-1)+r}]/\bar{I}_{\mathbf{U},u}.$$

We are now ready to prove Theorem 4.11, which we restate.

Theorem 4.11. *If $\overline{A}_{\mathbf{U},u}$ is finite, then $|\mathbf{U}(\mathcal{O}_K)_u| \le \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}$.*

Proof. For the sake of notation, we drop the subscripts $(\mathbf{U}, u)$ in this proof. The ring A is p-adically complete by the same proof as of [17, Theorem 4.12]. Moreover, since $\overline{A}$ is finite, A is finitely generated as a $\mathbb{Z}_p$-module. It follows that

$$\mathrm{Hom}(A, \mathbb{Z}_p) = \coprod_{\mathfrak{m}} \mathrm{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p) = \coprod_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \mathrm{Hom}(A_{\mathfrak{m}}, \mathbb{Z}_p),$$

where the union is over the maximal ideals of A. This gives the bound

$$|\mathrm{Hom}(A, \mathbb{Z}_p)| \le \sum_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \mathrm{rank}_{\mathbb{Z}_p} A_{\mathfrak{m}} = \sum_{A_{\mathfrak{m}}/\mathfrak{m}=\mathbb{F}_p} \dim_{\mathbb{F}_p} \overline{A}_{\mathfrak{m}} \le \dim_{\mathbb{F}_p} \overline{A}.$$

This establishes, by (6.1), that the number of points in $\kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t)$ is bounded by $\dim_{\mathbb{F}_p} \overline{A}$, and we thus have

$$|\mathbf{U}(\mathcal{O}_K)_u| \le |\kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t) \cap \overline{T(\mathcal{O}_K)_t}^p| \le \dim_{\mathbb{F}_p} \overline{A}.$$

$\square$

Remark 6.2. The geometric quadratic Chabauty condition is implicit in the assumption of Theorem 4.11. Indeed, in order for the ring $\overline{A}_{\mathbf{U},u} = \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]/\langle \overline{\kappa^* f_{i,j}^{\mathfrak{p}}} \rangle_{i,j,\mathfrak{p}}$ to have a chance to be finite, the number of relations we quotient by must be at least the number of variables. We therefore need $\delta(\rho - 1) + r \leq (g + \rho - 2)d$, which is equivalent to (4.4).

Corollary 6.3. *Suppose that $\overline{A}_{\mathbf{U},u}$ is finite for all $\mathbf{U}$ as in Definition 3.8 and all $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$. Then the set of rational points $C_K(K)$ is finite and satisfies*

$$|C_K(K)| \leq \sum_{\mathbf{U}} \sum_{u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})} \dim_{\mathbb{F}_p} \overline{A}_{\mathbf{U},u}.$$

Proof. There are finitely many $\mathbf{U} \subset \mathbf{C}^{\mathrm{sm}}$ satisfying the conditions of Definition 3.8 and the union of the $\mathbf{U}(\mathcal{O}_K)$ covers $\mathbf{C}^{\mathrm{sm}}(\mathcal{O}_K)$, which is equal to $C_K(K)$ by properness and regularity of the model $\mathbf{C}$. Moreover, each $\mathbf{U}(\mathcal{O}_K)$ is the disjoint union of its residue disks $\mathbf{U}(\mathcal{O}_K)_u$. The result follows. $\square$

7. Discussion and questions

7.1. Finiteness of intersections.

A more precise form of Question 1.6 from the introduction is the following:

Question 7.1. *Given a subscheme $\mathbf{U}$ as in Definition 3.8 and $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$ mapping to the point $\tilde{j}_b^U(u) = t \in \mathbf{T}(\overline{\mathcal{O}_{K,p}})$, what conditions would guarantee the finiteness of the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathcal{O}_{K,p})_u$?*

In [17, §9], Edixhoven and Lido give a new proof of Faltings' theorem using their method in the case of higher genus curves defined over $\mathbb{Q}$ satisfying $r < g + \rho - 1$. Their argument is quite elegant: it uses complex analytic methods to prove a Zariski density statement, which can then be bridged with their p-adic geometric situation using formal geometry. This proves the finiteness of the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathbb{Z}_p)_u$ and, in particular, the finiteness of $C_{\mathbb{Q}}(\mathbb{Q})$.

The setting over arbitrary number fields is more complicated. Reminiscent of the failures of Siksek's method described in Section 1.4.2, there are examples of curves satisfying (4.4) for which the intersection $\mathbf{Y}_t \cap \mathbf{U}(\mathcal{O}_{K,p})_u$ is not finite. Examples include curves base changed from $\mathbb{Q}$, which do not satisfy the quadratic Chabauty condition over $\mathbb{Q}$. Based on the results of Dogra [15] (discussed in Section 1.4.3), it seems reasonable to expect (although we have no proof) that the intersection is finite under the conditions (4.4) and

$$(7.1) \qquad \mathrm{Hom}(J_{\overline{\mathbb{Q}},\sigma_1}, J_{\overline{\mathbb{Q}},\sigma_2}) = 0 \text{ for any two distinct embeddings } \sigma_1, \sigma_2 : K \hookrightarrow \overline{\mathbb{Q}}.$$

It should be added that even if the condition (4.4) fails, we do expect a similar outcome as long as $\dim \mathbf{Y}_t < (g + \rho - 2)d$ holds.

A natural further question is to find a necessary and sufficient condition for the finiteness of the intersection. At this stage, we have no insights to offer in this direction.

7.2. A finite-to-one condition.

Assume the finiteness of the intersections $\mathbf{Y}_t \cap \mathbf{U}(\mathcal{O}_{K,p})_u$ (for the open subschemes $\mathbf{U}$ of Definition 3.8 and each point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$) discussed in Section 7.1. In order to extract an explicit bound for $|C_K(K)|$, the method of this paper relies on the existence of a prime p with the property that the $\mathbb{F}_p$-algebras $\overline{A}_{\mathbf{U},u}$ of Definition 6.1 are finite dimensional. Over $\mathbb{Q}$, assuming $r \leq g + \rho - 2$, Edixhoven and Lido hope (but also expect) [17, Remark 4.13] that it is always possible in practice to choose p with this property. The purpose of this section is to discuss what conditions would guarantee the existence of such a prime.

Fix an open subscheme $\mathbf{U}$ and a point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$. Given the definition of the algebra $A_{\mathbf{U},u}$, it is natural to tackle the question of $\overline{A}_{\mathbf{U},u}$ being finite or not by investigating the closely related question of when the map $\kappa = \kappa_{\mathbf{U},u} : \mathbb{Z}_p^{r+\delta(\rho-1)} \twoheadrightarrow \mathbf{Y}_t$ of Theorem 4.8 is expected to have finite fibers. Throughout the discussion, we assume the condition (4.4).

Let $d_J := \dim \overline{\mathbf{J}(\mathcal{O}_K)_x}^p$ and $d_T := \dim \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ be the dimensions as p-adic analytic manifolds. Similarly, let $d_{\mathcal{O}_K^\times}$ denote the $\mathbb{Z}_p$-module rank of the p–adic closure of the image of $\mathbb{G}_m(\mathcal{O}_K)_1$ (where the subscript 1 indicates principal units, i.e., taking the residue disk of $1 \in \mathcal{O}_K \otimes \mathbb{F}_p$) embedded diagonally in $\mathbb{G}_m(\mathcal{O}_{K,p})_1 = \prod_{\mathfrak{p}|p} \mathbb{G}_m(\mathcal{O}_{K,\mathfrak{p}})_1$. The following inequalities of dimensions hold:

- $d_{\mathcal{O}_K^\times} \leq \delta$,   (an equality assuming Leopoldt's conjecture [30] for K and p)
- $d_J \leq \min(r, gd)$,
- $d_T \leq \min(r + \delta(\rho - 1), (g + \rho - 1)d)$,
- $d_J + d_{\mathcal{O}_K^\times}(\rho - 1) \leq d_T$.

In order for κ to be finite-to-one, the equality of dimensions $d_T = r + \delta(\rho - 1)$ is needed. Hence, under our current assumptions, we expect the geometric quadratic Chabauty method over number fields to produce an effective bound on the size of the set of rational points when $\rho \geq 2$ and

$$(7.2) \qquad r + \delta(\rho - 1) = d_T \leq (g + \rho - 2)d.$$

This condition should perhaps aptly be called the *effective geometric quadratic Chabauty condition* in contrast to the weaker condition (4.4).

It is then natural to ask the following:

Question 7.2. *Is it possible that $d_J + d_{\mathcal{O}_K^\times}(\rho - 1) < d_T$?*

Remark 7.3. We currently have no definite answer to offer. However, using the fact that the torsor $\mathbf{T}$ is set up in a manner such that $t^*\mathbf{T}$ is trivial over $\operatorname{Spec}\mathcal{O}_K$ for every $t \in \mathbf{J}(\mathcal{O}_K)$, it can be shown that there exists a Zariski open cover $\mathbf{J} = \bigcup_i \mathbf{V}_i$ which is trivializing for $\mathbf{T}$ and such that $\mathbf{J}(\mathcal{O}_K) = \bigcup_i \mathbf{V}_i(\mathcal{O}_K)$ (i.e., every $\mathcal{O}_K$–point factors through the open subscheme $\mathbf{V}_i$ for some i). If such a cover can additionally be taken to be finite, then the equality $d_T = d_J + d_{\mathcal{O}_K^\times}(\rho - 1)$ follows. Nonetheless, such finiteness appears (at least to us) to be a non-trivial condition on the torsor.

If the answer to the above question is negative, implying that $d_T = d_J + d_{\mathcal{O}_K^\times}(\rho - 1)$, then the condition $d_T = r + \delta(\rho - 1)$ in (7.2) would force $d_J = r$ and $d_{\mathcal{O}_K^\times} = \delta$. In particular, we must have

$$(7.3) \qquad r \leq gd.$$

In this case, the geometric quadratic Chabauty method is expected to yield an effective bound under the condition

$$(7.4) \qquad d_J + d_{\mathcal{O}_K^\times}(\rho - 1) = r + \delta(\rho - 1) \leq (g + \rho - 2)d.$$

Remark 7.4. Of course, within (7.3), the most interesting case is the range

$$(7.5) \qquad (g-1)d < r \leq gd,$$

since for $r \leq (g-1)d$ Siksek's RoS linear Chabauty can be applied (with finiteness of the Chabauty set guaranteed by the work of Dogra discussed in Section 1.4.3, under the additional assumption (7.1)). The restriction (7.5) on r also appears in [2] as a consequence of Condition 4.1 therein. Specializing to $K = \mathbb{Q}$, the above inequalities reduce to the equality $r = g$, and the condition (7.4) then implies that $g = r < g + \rho - 1$. This coincides with the condition assumed in the setting of the effective quadratic Chabauty method of [6, 7].

Even when $r \leq gd$, failures of the equality $d_J = r$ can occur. Examples include cases when the Jacobian is isogenous to a product of abelian varieties of large and small Mordell–Weil ranks. For instance, suppose $C_\mathbb{Q}$ has genus 2 and $J_\mathbb{Q}$ is isogenous to the product of two elliptic curves E and A with $\operatorname{rank}_\mathbb{Z} E(\mathbb{Q}) = 0$ and $\operatorname{rank}_\mathbb{Z} A(\mathbb{Q}) = 2$. Then $\dim \overline{E(\mathbb{Q})}^p = 0$ while $\dim \overline{A(\mathbb{Q})}^p = 1$ since $A(\mathbb{Q}_p)$ has dimension 1. Thus, $d_J = 1 < r = g = 2$. In the presence of such isogeny factors, the condition (7.4) fails (conditional on the answer to Question 7.2 being negative) and κ is not finite-to-one. In particular, $\overline{A}_{\mathbf{U},u}$ is infinite. Note that this issue is independent of the chosen prime and persists

when varying p, providing a conditional (on a negative answer to Question 7.2) counter-example to the existence of a prime p such that $\overline{A}_{\mathbf{U},u}$ is finite, even over $\mathbb{Q}$.

Remark 7.5. The existence of such conditional counter-examples to the hopes and expectations expressed by Edixhoven and Lido might be seen as an indication in favour of Question 7.2 having an affirmative answer. It is worth noting though that the example treated by Edixhoven and Lido in [17, §8] satisfies $r = g = \rho = 2$ with Jacobian isogenous to the product of two rank 1 elliptic curves, and thus falls outside the small and large isogeny factor cases discussed above.

Remark 7.6. For a related discussion of isogeny factors in the linear geometric Chabauty method over $\mathbb{Q}$, see [22, Remark 2.1]. However, since $r < g$ is assumed therein, it is still possible to perform a linear method when $d_J < r$.

In conclusion, it seems to be slightly non-trivial to come up with the right theoretical condition for the effectiveness of the method. In practice, we do hope and expect that the method can be used to compute rational points in interesting new instances (as illustrated over $\mathbb{Q}$ in [17, §8]).

References

[1] L. H. A. Alpöge. *Points on Curves*. ProQuest LLC, Ann Arbor, MI, 2020. Thesis (Ph.D.)–Princeton University.

[2] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller. Explicit quadratic Chabauty over number fields. *Israel J. Math.*, 243(1):185–232, 2021.

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

[4] J. S. Balakrishnan and N. Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6):1057–1075, 2019.

[5] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: generalised height functions on Selmer varieties. *Int. Math. Res. Not. IMRN*, 2020.

[6] 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. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[7] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. Preprint, arXiv:2101.01862, 2021.

[8] J. Caro and H. Pasten. A Chabauty-Coleman bound for surfaces. Preprint, arXiv:2102.01055, 2021.

[9] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941.

[10] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[11] R. F. Coleman. A p-adic Shimura isomorphism and p-adic periods of modular forms. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemp. Math.*, pages 21–51. Amer. Math. Soc., Providence, RI, 1994.

[12] H. Darmon, M. Daub, S. Lichtenstein, and V. Rotger. Algorithms for Chow-Heegner points via iterated integrals. *Math. Comp.*, 84(295):2505–2547, 2015.

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

[14] M. W. Daub. *Complex and p-adic Computations of Chow-Heegner Points*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–University of California, Berkeley.

[15] N. Dogra. Unlikely intersections and the Chabauty-Kim method over number fields. Preprint, arXiv:1903.05032v4, 2019.

[16] N. Dogra and S. Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one. *Math. Ann.*, 380(1-2):393–448, 2021.

[17] B. Edixhoven and G. Lido. Geometric quadratic Chabauty. *J. Inst. Math. Jussieu*, pages 1–55, 2021. https://doi.org/10.1017/S1474748021000244.

[18] B. Edixhoven, G. van der Geer, and B. Moonen. *Abelian Varieties*. Book Project. https://www.math.ru.nl/~bmoonen/research.html#bookabvar.

[19] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[20] A. Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie (SGA7)*, volume 1. 1972.

[21] A. Grothendieck and J. Dieudonné. Éléments de géométrie algébrique IV. *Publ. Math. IHES*, 24:5–231, 1965.

[22] S. Hashimoto and P. Spelier. A geometric linear Chabauty comparison theorem. *Acta Arith.*, 202(1):67–88, 2022.

[23] M. Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1978.

[24] T. Honda. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22(2):213–246, 1970.

[25] E. Katz, J. Rabinoff, and D. Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell-Weil rank. *Duke Math. J.*, 165(16):3189–3240, 2016.

[26] E. Katz and D. Zureick-Brown. The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compos. Math.*, 149(11):1818–1838, 2013.

[27] N. M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1980.

[28] M. Kim. The motivic fundamental group of $\mathbb{P}_1$ - $\{0, 1, \infty\}$. *Invent. Math.*, 2005.

[29] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 2009.

[30] H.-W. Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[31] B. Poonen and M. Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.

[32] S. Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013.

[33] The Stacks Project Authors. Stacks project. Available online at http://stacks.math.columbia.edu, 2020.

[34] M. Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006.

[35] N. Triantafillou. Restriction of Scalars Chabauty and the S-unit equation. Preprint, arXiv:2006.10590, 2020.

(Pavel Čoupek) Department of Mathematics, Purdue University
Email address: pcoupek@purdue.edu

(David T.-B. G. Lilienfeldt) Einstein Institute of Mathematics, Hebrew University of Jerusalem
Email address: davidterborchgram.lilienfeldt@mail.huji.ac.il

(Luciena X. Xiao) Department of Mathematics and Statistics, University of Helsinki
Email address: xiao.xiao@helsinki.fi

(Zijian Yao) Department of Mathematics, Université Paris Saclay/CNRS
Email address: zijian.yao.math@gmail.com