GEOMETRIC QUADRATIC CHABAUTY OVER NUMBER FIELDS

PAVEL ČOUPEK, DAVID LILIENFELDT, LUCIENA X. XIAO, ZIJIAN YAO

Abstract. We extend the method of geometric quadratic Chabauty, initiated over $\mathbb{Q}$ by Edixhoven and Lido, to curves of genus at least 2 defined over arbitrary number fields. This provides a conditional bound on the number of rational points of such curves.

Contents

1. Introduction

1.1. **Chabauty–Coleman.** Let $C = C_K$ be a curve of genus $g \geq 2$ defined over a number field K. The theorem of Faltings states that the set of rational points on C is finite. Faltings's spectacular proof, however, cannot be made effective and there is no general algorithm to determine the set $C(K)$ at present. On the other hand, if the Mordell–Weil rank r of the Jacobian J of C satisfies the inequality $r \leq g - 1$, the pioneering work of Chabauty and Coleman [Cha41, Col94] can be used to give upper bounds for $C(K)$, and in many cases, to explicitly compute these rational points. Let us momentarily set $K = \mathbb{Q}$ and briefly explain their strategy. Upon choosing a prime p of good reduction, one obtains a homomorphism

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

induced from a linear pairing $J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \longrightarrow \mathbb{Q}_p$ which sends (P, ω) to the Coleman integral $\int_0^P \omega$. The Abel–Jacobi map $j_b : C \to J$, after fixing a base point $b \in C(\mathbb{Q})$, then leads us to the following diagram, which lies in the central spot of the method:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \longrightarrow & C(\mathbb{Q}_p) & & \\ \downarrow & & \downarrow & \overset{\int}{\searrow} & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0(C_{\mathbb{Q}_p}, \Omega^1)^\vee. \end{array}$$

The Chabauty condition $r \geq g - 1$ guarantees that the closure $Z := \overline{J(\mathbb{Q})}^p$ of $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$ with respect to the p-adic topology has positive codimension. In particular, there exists a nontrivial differential form ω which vanishes on Z. Roughly, ω is locally given by a p-adic power series and has only finitely many zeroes on each residue disk of $C(\mathbb{Q}_p)$. Therefore, the intersection $J(\mathbb{Q}) \cap C(\mathbb{Q}_p)$, thus $C(\mathbb{Q})$, is finite. Moreover, the computation of $C(\mathbb{Q})$ amounts to computing these power series to sufficient p-adic precision on each residue disk.

1.2. **Quadratic Chabauty.** The fascinating program initiated by Kim (see [Min05, Min09]) aims to relax the Chabauty condition by considering non-abelian variants of the objects in §1.1. To this end, we first reinterpret the diagram above using the Bloch–Kato selmer groups $H^1_f(\mathbb{Q}, V)$ (resp. $H^1_f(\mathbb{Q}_p, V)$) in place of $J(\mathbb{Q})$ (resp. $J(\mathbb{Q}_p)$) via the Kummer maps, where $V := H^1_{\text{ét}}(C_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^\vee$ is the p-adic étale cohomology of C. The logarithm map above is essentially the inverse of the Bloch–Kato exponential

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

Next, we replace V by certain pro-unipotent quotients U_n of the étale fundamental group $\pi_1^{\text{ét}}(C_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, one for each $n \geq 1$, which again carries a continuous action by $\mathrm{Gal}_{\mathbb{Q}}$. Kim defines a certain Selmer subgroup $\mathrm{Sel}(U_n) \subset H^1_f(\mathbb{Q}, U_n)$, and upgrades the previous diagram to

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

Here the vertical maps j_n and $j_{n,p}$ are Kim's unipotent Kummer maps. The intersection $J(\mathbb{Q}) \cap C(\mathbb{Q}_p)$ in the Chabauty–Coleman method is now replaced by the set

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

that contains $C(\mathbb{Q})$. For sufficiently large n, Kim conjectures that $C(\mathbb{Q}_p)_n$ is finite, and even coincides with $C(\mathbb{Q})$. The first instances of Kim's program have been carried out quite successively by Balakrishnan and her collaborators. In particular, for the quadratic case where $n = 2$, if the Mordell–Weil rank r satisfies $r \leq g + \rho - 2$ where ρ is the rank of the Néron–Severi group of J, then $C(\mathbb{Q}_p)_2$ is finite and can often be explicitly determined (see [BD18, BD19] and references therein). This method has been successfully applied to determine rational points on the "cursed curve" in [BDM+19], which finishes the classification of non-CM elliptic curves over $\mathbb{Q}$ of split Cartan type.

Recently, a different, less cohomological but probably more direct approach to quadratic Chabauty has been found by Edixhoven–Lido. Their idea is to consider a certain $\mathbb{G}_m$-torsor T over the Jacobian instead of the Selmer variety $\mathrm{Sel}(U_2)$. Their method is expected to work under the same quadratic Chabauty condition $r \leq g+\rho-2$, but has the advantage of avoiding the consideration of iterated Coleman integrals and the analysis of certain complicated p-adic heights. In fact, this method is rather geometric and elementary, and even eliminates the language of (non-abelian) p-adic Hodge theory used by Kim.

1.3. **Quadratic Chabauty over number fields.** On a different direction, a natural question is how to generalize the Chabauty–Coleman method and its non-abelian variants to more general number fields K.

To put this article into context, we briefly recall the first steps towards such generalizations studied by [Sik13, BBBM19, Dog19]. In order to apply the idea of Chabauty–Coleman, Siksek [Sik13] considers the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}}J$ and studies Coleman integration in this context. The work of [BBBM19] builds on this idea and studies rational points on hyperelliptic curves satisfying a more relaxed Chabauty condition compared to [Sik13] (also see §3.3). The work of Dogra [Dog19], on the other hand, is directly related to the approach of Kim, relying on a certain arithmetic form of quadratic Chabauty condition (see Remark 3.11). We refer the interested reader to [Dog19] for more details on his results.

1.4. **Main result.** In this article and subsequent works, we generalize the geometric approach initiated by Edixhoven–Lido to arbitrary number fields. Our main theoretical result in this article is roughly the following

Theorem 1. *Let K be a number field of degree $d = r_1 + 2r_2$, where $2r_2$ is the number of complex embeddings of K. Let C_K be a smooth proper geometrically connected curve of genus $g \geq 2$ with Mordell–Weil rank r over K, satisfying*

$$r \leq d(g-1) + (\rho - 1)(r_2 + 1), \tag{1}$$

where ρ is the rank of the Néron–Severi group of the Jacobian J_K. Let $\delta := r_1 + r_2 - 1$ and

$$A := \mathbb{Z}_p\langle z_1, ..., z_{\delta(\rho-1)+r}\rangle$$

be the p-adically completed polynomial algebra over $\mathbb{Z}_p$. There exists an explicitly computable ideal I of A, such that if $\overline{A} := A/I \otimes \mathbb{F}_p$ is a finite dimensional $\mathbb{F}_p$ vector space, then the set of rational points $C_K(K)$ is finite and bounded above by $\dim_{\mathbb{F}_p} \overline{A}$.

In this case we expect $C_K(K)$ to be explicitly computable.

Remark 2. *The precise form of the main theorem (Theorem 3.9) is slightly more involved than what is stated above. For example, in order for our method to work, we need to "cover" C_K by certain open subschemes U_i and work with one U_i at a time. In particular, we shall construct an ideal $I_i \subset A$ to bound the rational points on U_i for each i.*

Remark 3. *The condition (1), which we refer to as the geometric quadratic Chabauty condition (Definition 3.10), is the "best bound" for explicit quadratic Chabauty methods over number fields in literature. See §3.3 for comparisons with other Chabauty bounds that arise in the aforementioned works in §1.3.*

1.5. **Overview of the approach.** Now we briefly explain the idea of geometric quadratic Chabauty, which we extend from [EL19]. As is the case of the methods of Chabauty–Coleman and Chabauty–Kim, the nature of this approach is inherently p-adic. Let p be a prime of good reduction for the curve C_K. The strategy is to replace the Jacobian in Chabauty's original approach by something higher dimensional in order to play the Chabauty game. Slightly more precisely, we will construct a certain $\mathbb{G}_m^{\rho-1}$-torsor T_K over J_K, where ρ is as defined in Theorem 1, which will replace J_K. This, however, introduces "too many rational points" as the fiber of T_K over J_K is ${\mathbb{G}_m}^{\rho-1}$ and $\mathbb{G}_m(K) = K^\times$ is not finitely generated, thus it is more natural to consider an integral model $\mathbf{C}$ of C_K over the ring of integers $\mathcal{O}_K$.

In other words, we shall construct a certain ${\mathbb{G}_m}^{\rho-1}$-torsor $\mathbf{T}$ over the $\mathbf{J}$, the latter being the Néron model of J_K. The idea is then to carefully lift the Abel–Jacobi map $j_b : \mathbf{C} \to \mathbf{J}$ to the torsor $\mathbf{T}$

$$\begin{array}{ccc} & & \mathbf{T} \\ & \overset{\tilde{j}_b}{\nearrow} & \downarrow \\ \mathbf{C} & \xrightarrow{j_b} & \mathbf{J} \end{array}$$

We then consider $\mathbf{C}(\mathcal{O}_K) \subset \mathbf{C}(\mathcal{O}_{K,p})$ as a subset of the p-adic points, where $\mathcal{O}_{K,p} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and arrive at the following "quadratic Chabauty diagram" over $\mathcal{O}_K$

$$\begin{array}{ccccc} \mathbf{C}(\mathcal{O}_K) & & \longrightarrow & & \mathbf{C}(\mathcal{O}_{K,p}) \\ \downarrow{\scriptstyle \tilde{j}_b} & & & & \downarrow \\ \mathbf{T}(\mathcal{O}_K) & \longrightarrow & \mathbf{Y} & \longrightarrow & \mathbf{T}(\mathcal{O}_{K,p}) \end{array} . \tag{2}$$

Here $\mathbf{Y} := \overline{\mathbf{T}(\mathcal{O}_K)}^p$ is the closure of $\mathbf{T}(\mathcal{O}_K)$ in $\mathbf{T}(\mathcal{O}_{K,p})$ for the p-adic topology. As in §1.1, the rational points $C_K(K) = \mathbf{C}(\mathcal{O}_K)$ is contained in $\mathbf{C}(\mathcal{O}_{K,p}) \cap \mathbf{Y}$, which is often finite and computable.

The key of this approach is thus to analyze the p-adic closure $\mathbf{Y}$ of the $\mathcal{O}_K$-points of the torsor $\mathbf{T}$. If $K = \mathbb{Q}$, then this can be done via 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 [EL19] decides to work over $\mathbb{Q}$. In fact, it was suggested to us by the authors of [EL19] that an approach similar to that of [Sik13] might reduce the case of general number fields K back to the case of $\mathbb{Q}$. In this article, however, we decide to take a slightly more direct approach, as one of our main observations is that one can in fact fully utilize the $\mathbb{G}_m$-action on the fibers of the torsor $\mathbf{T} \to \mathbf{J}$ to parametrize $\mathbf{Y}$, which is sufficient for our purpose. Roughly, we pick a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^r \to \mathbf{T}(\mathcal{O}_K)$ essentially by choosing basis for the Mordell–Weil group $J(K)$. We then use the $\mathbb{G}_m$-action to propagate these coordinates to get a "$\mathbb{Z}$-coordinate" map $\mathbb{Z}^{\delta(\rho-1)+r} \to \mathbf{T}(\mathcal{O}_K)$, where δ is as defined in Theorem 1. Finally, p-adically interpolating these coordinates allow us to parametrize $\mathbf{Y}$ via a surjective map

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

which turns out to be given by convergent p-adic power series. In fact, the ideal I from Theorem 1 is built such that the cardinality of $\operatorname{Spec} \overline{A}$ measures the size of $\kappa^{-1}(\mathbf{Y} \cap \mathbf{C}(\mathcal{O}_{K,p}))$. In particular, in order for our method to be able to explicitly determine the rational points on C_K, we need to choose a prime p such that

- $\mathbf{Y} \cap \mathbf{C}(\mathcal{O}_{K,p})$ is finite
- κ is "finite-to-one" on $\kappa^{-1}(\mathbf{Y} \cap \mathcal{O}_{K,p})$.

We conjecture that the first outcome is always achieved, and hope that there exists a good p such that the second condition is also satisfied.

Conjecture 4. *Let p be a prime of good reduction for C_K, then the intersection $\mathbf{Y} \cap \mathbf{C}(\mathcal{O}_{K,p})$ as in the commutative diagram (2) is finite.*

Question 5. *For a given curve C_K, does there always exist a prime p such that the ring $\overline{A}$ as in Theorem 1 is finite dimensional over $\mathbb{F}_p$.*

Remark 6. *There are, of course, further caveats hidden from the over-simplified overview above. For example, as hinted in Remark 2, in order to obtain the lifting $\widetilde{j_b} : \mathbf{C} \to \mathbf{T}$, we need to restrict to certain open subscheme $\mathbf{U}_i$ of the smooth locus $\mathbf{C}^{\mathrm{sm}}$ inside $\mathbf{C}$. Moreover, when constructing κ, we will work on one residue disk inside each $\mathbf{U}_i(\mathcal{O}_{K,p})$ at a time. The details of these complications are spread in the article, for example see §2.5 and §4.1. In particular, a precise form of Question 5 is formulated in §5.*

1.6. **Outline.** In the end of this introduction let us briefly outline the content of each section. In §2 we recall some basic background on the Poincaré torsor, from which we build the torsor T_K over J_K mentioned in the overview above. We then spread out the entire picture from $\operatorname{Spec} K$ to $\operatorname{Spec} \mathcal{O}_K$ to obtain a precise version of diagram (2). Then, in §3, we give more details of the strategy of geometric quadratic Chabauty, before stating the main technical results of this article. We also explain how the geometric quadratic Chabauty condition arises and discuss how it specializes to conditions that appear in the "classical" quadratic Chabauty method that is part of Kim's program. In §4, which is the technical core of this article, we discuss how to parametrize the p-adic closure $\mathbf{Y}$ of the "rational points" $\mathbf{T}(\mathcal{O}_K)$ via a certain p-adic interpolation. Finally, we complete the proof of the main theoretical results in §5.

Acknowledgements. This project was initiated during the Arizona Winter School in March, 2020 and was proposed to us by Bas Edixhoven. We wish to thank the organizers of the conference for making this collaboration possible. We are grateful to Bas Edixhoven and Guido Lido for offering their insights and answering many of our questions regarding their paper. We thank Jan Vonk for many helpful discussions during the project.

Notation. For the convenience of the reader we provide a list of notations used in the paper.

- $K/\mathbb{Q}$ 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 $\mathcal{O}_K^\times$.
- $h = \mathrm{cl}(\mathcal{O}_K)$ is the class number of $\mathcal{O}_K$.
- C_K is a smooth proper 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 torsor

In this section we recall some background on algebraic geometry necessary for the method of geometric quadratic Chabauty. In particular, we briefly review the key geometric object studied in this paper, namely the Poincaré torsor.

2.1. **The Poincaré torsor.** First we recall that, given a line bundle $\mathscr{L}$ on an arbitrary scheme X, its associated $\mathbb{G}_m$-torsor is $\mathscr{L}^\times = \mathbf{Isom}_X(\mathcal{O}_X, \mathscr{L})$, which is equipped with a natural free and transitive action of $\mathbb{G}_m$. Concretely, $\mathscr{L}^\times$ is (locally) obtained by deleting the zero section of $\mathscr{L}$. Note that $\mathscr{L}^\times$ is Zariski locally trivial, in particular it is represented by a scheme over X, which we again denote by $\mathscr{L}^\times$ by slightly abusing notations.

The most relevant example for this paper is the Poincaré torsor for the Jacobian of a curve, which we now discuss. As in the introduction, we let C_K be a smooth proper geometrically connected curve of genus $g \geq 2$ defined over K and J_K be its Jacobian. The dual abelian variety of J_K is $J_K^\vee$ and comes equipped with a canonical principal polarization $\lambda : J_K \xrightarrow{\sim} J_K^\vee$ by translating the theta divisor. Let P_K denote the Poicaré bundle on $J_K \times J_K^\vee$, which carries a canonical birigidification with respect to the identity sections of J_K and $J_K^\vee$. More precisely, P_K is canonically trivialized over $\{0\} \times J_K^\vee$ and $J_K \times \{0\}$ and these trivializations are compatible on $\{0\} \times \{0\}$. The Poincaré torsor $P_K^\times$ is the $\mathbb{G}_m$-torsor on $J_K \times J_K^\vee$ associated to P_K. As above, we again 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 structural morphism.

2.2. **The Poincaré torsor as a $\mathbb{G}_m$-biextension.** In this subsection we explain the biextension structure of the Poincaré torsor that plays a central role in our paper. The assertion is that $P_K^\times$ admits a unique structure as a $\mathbb{G}_m$-biextension of the couple $(J_K, J_K^\vee)$, which is compatible with its canonical birigidified $\mathbb{G}_m$-torsor structure inherited from P_K ([Gro72, VII.Definition 2.1, Exemple 2.9.5]). Instead of repeating the definition from SGA 7, let us briefly explain what this means.

• *Partial composition $+_1$.* First, 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

$$1 \longrightarrow \mathbb{G}_{m,J_K^\vee} \longrightarrow P_K^\times \longrightarrow J_{K,J_K^\vee} \longrightarrow 0. \tag{3}$$

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 $z_1, z_2 \in P_K^\vee(S)$ 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 point z_1 (resp. z_2) is equivalent to a nowhere vanishing section $\alpha_1 \in (x_1, y)^* P_K(S)$ (resp. α_2) of the pullback of the Poincaré bundle. Now, as part of the requirement of being a $\mathbb{G}_m$-biextension, we have an isomorphism of line bundles over $\mathcal{O}_S$

$$(x_1, y)^* P_K \otimes (x_2, y)^* P_K \cong (x_1 + x_2, y)^* P_K, \tag{4}$$

(supplied by the theorem of square). 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 $z_3 \in P_K^\times(S)$ that 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 displayed above. 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 couples of points $z_1, z_2 \in P_K^\times(S)$ such that

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

Let us also denote the group structure on the $J_K^\vee$-group scheme $J_{K,J_K^\vee}$ by $+_1$ (again slightly abusing notations), then the partial composition law $+_1$ on $P_K^\times$ 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 $P_K^\times$ 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

$$1 \longrightarrow \mathbb{G}_{m,J_K} \longrightarrow P_K^\times \longrightarrow J_{K,J_K}^\vee \longrightarrow 0. \tag{5}$$

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

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

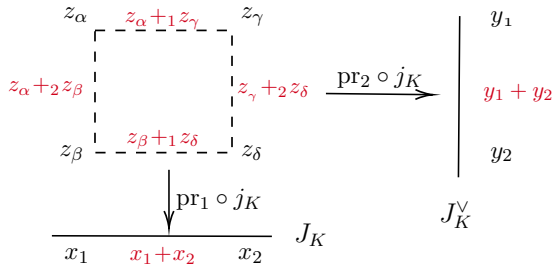
• *Compatibility.* The commutative group scheme extensions (3) and (5) are compatible in the following sense. Let S be any K-scheme. Let $z_\alpha, z_\beta, z_\gamma, z_\delta \in P_K^\times(S)$ be arbitrary S-points such that

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

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

$$(z_\alpha +_2 z_\beta) +_1 (z_\gamma +_2 z_\delta) = (z_\alpha +_1 z_\gamma) +_2 (z_\beta +_1 z_\delta) \tag{6}$$

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



Next we briefly describe the action of $\mathbb{G}_m$ on the Poincaré torsor (or more general biextensions). To this end, we let $e_{J_K} \in \mathrm{Hom}_{J_K}(J_K, P_K^\vee)$ (resp. $e_{J_K^\vee} \in \mathrm{Hom}_{J_K^\vee}(J_K^\vee, P_K^\times)$) denote the identity section of $P_K^\times$ as a J_K (resp. $J_K^\vee$)-group scheme. Restricting the short exact sequence (3) of commutative $J_K^\vee$-group schemes via the identity section $\mathrm{Spec}\, K \to J_K^\vee$, we get a short exact sequence of commutative K-group schemes

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

which is split by the section e_{J_K}. In particular, we have $P_K^\times|_{J_K \times \{0\}} = \mathbb{G}_{m,J_K}$ which is $\mathbb{G}_{m,K} \times J_K$, and by a similar reasoning (using the identity section $e_{J_K^\vee}$) $P_K^\times|_{\{0\} \times J_K^\vee} = \mathbb{G}_{m,J_K^\vee}$. 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 $(x, 0)$, corresponding to $(u, 0)$ under the identification $P_K^\times|_{J_K \times \{0\}}(S) \simeq \mathbb{G}_m(S) \times J_K(S)$.[1] The action of u on the point t is given by

$$u \cdot t = v +_2 t. \tag{7}$$

Clearly, 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 $+_2$: 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

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

and similarly for $+_1$.

2.3. **Spread out.** As will become apparent, in the method of geometric quadratic Chabauty it is crucial to spread out the geometry over $\mathcal{O}_K$. Roughly speaking, one wants to work with finitely generated $\mathbb{Z}$-modules, and $\mathbb{G}_m(\mathcal{O}_K) = \mathcal{O}_K^\times$ is a finitely generated $\mathbb{Z}$-module of rank $\delta = r_1 + r_2 - 1$ while $\mathbb{G}_m(K) = K^\times$ has infinite rank.

[1] 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 $v_{x,u_1u_2} = v_{x,u_1} +_2 v_{x,u_2}$.

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, 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 respectively the Néron models of J_K and $J_K^\vee$ over $\mathcal{O}_K$. 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 $\mathbf{J}/\mathbf{J}^\circ$ 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 leads to the Abel-Jacobi map $j_b : C_K \hookrightarrow J_K$ which sends a point x to the linear equivalence class of the divisor $(x) - (b)$. The map j_b extends uniquely to a morphism

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

over $\mathcal{O}_K$ by the Néron Mapping Property, which we shall again denote by j_b. Next we wish to extend the Poincare bundle to $\operatorname{Spec}\mathcal{O}_K$. As alluded to above, this is supplied by Grothendieck's theory of biextensions.

Proposition 2.1. *The Poincaré torsor $P_K^\times$ extends uniquely to a biextension $\mathbf{P}^\times$ over $(\mathbf{J}, \mathbf{J}^{\vee,\circ})$ by $\mathbb{G}_m$. In particular, given an $\mathcal{O}_K$-scheme S and two points $(x, y), (x, y') \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(S)$, we have an isomorphism*

$$(x, y)^*\mathbf{P} \otimes (x, y')^*\mathbf{P} \cong (x, y + y')^*\mathbf{P}, \tag{8}$$

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

Proof. This is [Gro72, VIII. Theorem 7.1(b)]. Note that we have restricted to the connected subscheme $\mathbf{J}^{\vee,\circ}$ in order to apply the theorem cited above. □

We denote the structural morphism of this $\mathbb{G}_m$-torsor by

$$j : \mathbf{P}^\times \to \mathbf{J} \times \mathbf{J}^{\vee,\circ}.$$

The uniqueness of the extension follows from the connectedness of $\mathbf{J}^{\vee,\circ}$. Let us remark that the commutative group scheme extension structures and their compatibilities (from our discussion in §2.2) extend to the integral version $\mathbf{P}^\times$.

2.4. **Integral points on the Poincaré torsor.** The goal of this subsection is to lift certain integral points on $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ across the structure map $j : \mathbf{P}^\times \to \mathbf{J} \times \mathbf{J}^{\vee,\circ}$. Let $(x, y) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$ be an $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$, and $(x, y)^*\mathbf{P}^\times$ be the pull-back of $\mathbf{P}^\times$ to $\mathcal{O}_K$, which is a $\mathbb{G}_{m,\mathcal{O}_K}$-torsor over $\operatorname{Spec}\mathcal{O}_K$ as shown in the diagram

$$\begin{array}{ccc} (x, y)^*\mathbf{P}^\times & \longrightarrow & \mathbf{P}^\times \\ \downarrow & \square & \downarrow \\ \operatorname{Spec}\mathcal{O}_K & \xrightarrow{(x,y)} & \mathbf{J} \times \mathbf{J}^{\vee,\circ}. \end{array} \tag{9}$$

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

Note that, in the case $K = \mathbb{Q}$, all $\mathbb{G}_m$-torsors are trivial over $\operatorname{Spec}\mathbb{Z}$ and admit a section over $\mathbb{Z}$, unique up to $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. Thus a lift of the integral point (x, y) to $\mathbf{P}^\times$ always exits. 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 $(x, h \cdot y)$. More precisely, we have

Lemma 2.2. *Any $\mathcal{O}_K$-point of $\mathbf{J} \times \mathbf{J}^{\vee,\circ}$ of the form $(x, h \cdot y)$ where $(x, y) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$ 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 the isomorphisms (8) and obtain an isomorphism

$$((x, y)^*\mathbf{P})^{\otimes h} \cong (x, h \cdot y)^*\mathbf{P}$$

of line bundles over $\operatorname{Spec} \mathcal{O}_K$. In particular, we know 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. □

2.5. **Trivialization of the Poincaré torsor.** Next we define and study a certain $\mathbb{G}_m^{\rho-1}$-torsor $\mathbf{T}$ over $\mathbf{J}$, where ρ is the rank of the Néron–Severi group of J_K. The goal of this subsection is to lift the Abel-Jacobi map $j_b : \mathbf{C}^{\mathrm{sm}} \to \mathbf{J}$ across $\mathbf{T} \to \mathbf{J}$. As discussed in the introduction, this is a crucial step in the geometric approach to quadratic Chabauty.

2.5.1. *Trivialization over C_K.* Let $\lambda : J_K \longrightarrow J_K^\vee$ be the canonical principal polarization. By functoriality of Pic we have the following commutative diagram of commutative K-group schemes with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_K^\vee & \longrightarrow & \operatorname{Pic}_{J_K/K} & \xrightarrow{\pi} & \operatorname{NS}_{J_K/K} & \longrightarrow & 0 \\ & & \wr\downarrow{\scriptstyle -\lambda^{-1}} & & \downarrow{\scriptstyle j_b^*} & & \downarrow{\scriptstyle j_{b,\mathrm{NS}}^*} & & \\ 0 & \longrightarrow & J_K & \longrightarrow & \operatorname{Pic}_{C_K/K} & \xrightarrow{\deg} & \mathbb{Z}_K & \longrightarrow & 0. \end{array} \tag{10}$$

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. Here we have used the fact that the map induced by j_b on Pic^0 agrees with $-\lambda^{-1}$, which is in particular an isomorphism.

Next, 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 (see [EvdGM, Proposition 7.14 & §7.18] for 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 $x \in J_K \mapsto [\mathrm{t}_x^* L \otimes L^{-1}]$ where $\mathrm{t}_x : J_K \longrightarrow J_K$ denotes 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 [EvdGM, Corollary 11.3]

$$\tilde{\varphi} : \operatorname{NS}_{J_K/K} \xrightarrow{\sim} \mathbf{Hom}(J_K, J_K^\vee)^+. \tag{11}$$

Definition 2.3. At the level of K-points, we define the group $\operatorname{Hom}(J_K, J_K^\vee)_0^+$ to be the kernel

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

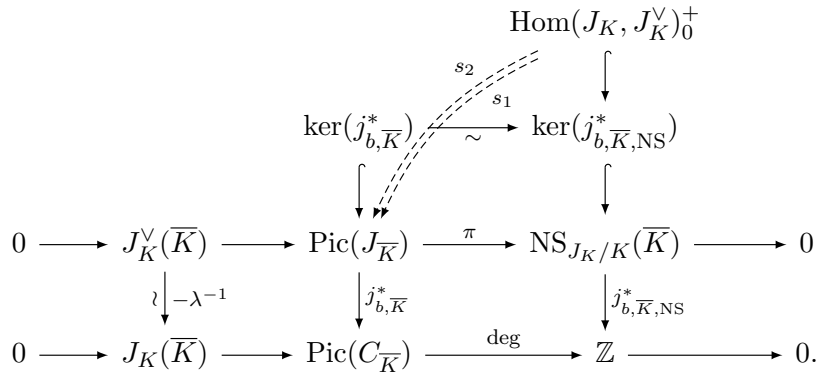
Proposition 2.4. *For all $f \in \operatorname{Hom}(J_K, J_K^\vee)_0^+$, there exists a unique element $c_f \in J_K^\vee(K)$ with the property that the following $\mathbb{G}_m$-torsor over C_K*

$$j_b^*(\mathrm{id}, \mathrm{t}_{c_f} \circ f)^* P_K^\times$$

is trivial. Here $(\mathrm{id}, \mathrm{t}_{c_f} \circ f)$ denotes the map $J_K \xrightarrow{(\mathrm{id}, \mathrm{t}_{c_f} \circ f)} J_K \times J_K^\vee$. In particular, for all $n \in \mathbb{Z}_{\geq 1}$, its n^{th} 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 (10) can be written as follows:

(12)



The map π in the first short exact sequence in 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 $\tilde{\varphi}^{-1}$. 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 in $\mathrm{Pic}(J_K) \subset \mathrm{Pic}(J_{\overline{K}})$. We observe that ([EvdGM, Proposition 11.1])

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

The second splitting is given by inverting π on $\ker(j^*_{b,\overline{K}})$, in other words, 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 $\mathrm{Pic}(J_K)$. Now, 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 $c_f \in J_K^\vee(K)$. Now we observe that, for a line bundle L on J_K corresponding to a closed point $x \in J_K^\vee$, we have

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

where pr_1 is the projection $J_K \times J_K^\vee \to J_K$. Therefore, by construction, c_f is the unique element in $J_K^\vee(K)$ such that

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

This proves the proposition. □

The group $\mathrm{NS}_{J_K/K}(K)$ is a finitely generated free $\mathbb{Z}$-module whose rank is denote by ρ (the Picard number of J_K). The kernel

$$\ker(j^*_{b,\mathrm{NS}} : \mathrm{NS}_{J_K/K}(K) \to \mathbb{Z})$$

is a free $\mathbb{Z}$-module of rank $\rho - 1$, and so is the group $\mathrm{Hom}(J_K, J_K^\vee)_0^+$.

Notation 2.5. We fix the following notations from now on.

- 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 2.4.

- For each integer $n \in \mathbb{Z}_{\geq 1}$, denote by $\alpha_{n,i,K}$ the map

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

Construction 2.6. By Proposition 2.4, 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 particular, it admits a section over C_K. This gives rise to a lift of j_b, which we shall fix and denote by $\tilde{j}_b^{(n,i)}$ as in the diagram below. This choice is unique up to $K^\times$.

(13)
$$\begin{array}{ccccc} & & \alpha_{n,i,K}^* P_K^\times & \longrightarrow & P_K^\times \\ & \overset{\tilde{j}_b^{(n,i)}}{\nearrow} & \downarrow & \square & \downarrow \\ C_K & \xrightarrow{j_b} & J_K & \xrightarrow{\alpha_{n,i,K}} & J_K \times J_K^\vee. \end{array}$$

2.5.2. *Construction over $\mathcal{O}_K$.* Now we extend the geometry over $\mathcal{O}_K$. Let us introduce and recall some notations and refer the rest to §2.3. 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 $1 \leq i \leq \rho - 1$, the homomorphism $f_i : J_K \longrightarrow J_K^\vee$ (resp. the translation map $\mathrm{t}_{c_i} : J_K^\vee \longrightarrow J_K^\vee$, resp. the multiplication $hm\cdot : J_K^\vee \longrightarrow J_K^\vee$) extends uniquely to a homomorphism $f_i : \mathbf{J} \longrightarrow \mathbf{J}^\vee$ (resp. $\mathrm{t}_{c_i} : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee$, resp. $hm\cdot : \mathbf{J}^\vee \longrightarrow \mathbf{J}^\vee$). Note that $c_i \in J_K^\vee(K) = \mathbf{J}^\vee(\mathcal{O}_K)$. Therefore, the morphism $\alpha_{hm,i,K} : J_K \longrightarrow J_K \times J_K^\vee$ extends uniquely to a morphism of $\mathcal{O}_K$-schemes

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

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

Construction 2.7. Taking the product over $i = 1, \ldots, \rho - 1$, we obtain the $\mathcal{O}_K$-morphism

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

Consider the map $\mathbf{P}^\times \to \mathbf{J} \times \mathbf{J}^{\vee,\circ} \to \mathbf{J}$ 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 in the article.

Definition 2.8. Retain notations from Construction 2.7. We 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:

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

Construction 2.9. Now we return to the lifts $\tilde{j}_b^{(hm,i)}$ obtained in Construction 2.6. By taking the product over i of these lifts $\tilde{j}_b^{(hm,i)}$, we obtain a lift $\tilde{j}_b$ of j_b to $T_K := T \times_J J_K$ as

pictured in the following commutative diagram:

$$\begin{array}{ccccc} & & T_K & \longrightarrow & P_K^{\times,\rho-1} \\ & \overset{\tilde{j}_b}{\nearrow} & \downarrow & \square & \downarrow \\ C_K & \xrightarrow{j_b} & J_K & \xrightarrow{\alpha_K} & J_K \times (J_K^{\vee,0})^{\rho-1} \end{array} \tag{14}$$

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

Our 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 not generally possible: the problem is that, for primes $\mathfrak{q}|\mathfrak{n}$, the fiber $C^{\mathrm{sm}}_{\mathbb{F}_\mathfrak{q}} := \mathbf{C}^{\mathrm{sm}} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} \mathbb{F}_\mathfrak{q}$ may contain too many components. To remedy this, we consider one geometrically irreducible component in each such fiber at a time.

Construction 2.10. 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 $C^{\mathrm{sm}}_{\mathbb{F}_\mathfrak{q}}$ that is further geometrically irreducible. We will later 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 2.11. We first remark that such a subscheme $\mathbf{U}$ exists under the assumption that C_K admits a K-rational point. Moreover, for our purposes 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 2.12. *Let X be a smooth irreducible affine curve over a finite field k that admits a k-rational point, then X is geometrically irreducible.*

Proof. Let $A = \Gamma(X, \mathcal{O}_X)$ be the ring of sections on X, which admits a map $A \to k$ of k-algebras supplied by the rational point. Let $k' = \{\alpha \in k(X) | \alpha \text{ is algebraic over } k\}$ be field of constants of X over k, as X is normal we have $k' \subset A$ which forces $k' = k$. This is equivalent to X being geometrically irreducible. □

2.5.3. *The lift to* $\mathbf{T}$. We are finally able to construct the desired lift of j_b. Our construction is analogous to that in [EL19, §2] except that we pull back $\mathbf{P}^\times$ via morphisms of the form $(\mathrm{id}, hm\cdot \circ \mathrm{t}_c \circ f) : \mathbf{J} \to \mathbf{J} \times \mathbf{J}^{\vee,\circ}$, where in the second factor we incorporate an additional multiplication by h (the class number of $\mathcal{O}_K$), to ensure the existence of such a lift.

Proposition 2.13. *Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ obtained as in Construction 2.10. Then 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:*

$$\begin{array}{ccccccc} & & & & \mathbf{T} & \longrightarrow & \mathbf{P}^{\times,\rho-1} \\ & & \overset{\tilde{j}_b^U}{\nearrow} & & \downarrow & \square & \downarrow \\ \mathbf{U} & \hookrightarrow & \mathbf{C}^{\mathrm{sm}} & \xrightarrow{j_b} & \mathbf{J} & \xrightarrow{\alpha} & \mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}. \end{array} \tag{15}$$

Proof. The restriction of the torsor

$$(\mathrm{id}, m \cdot \mathrm{t}_{c_i} \circ f_i)^* \mathbf{P}^\times$$

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 2.4. In other words, the torsor $(\mathrm{id}, m\cdot\circ \mathrm{t}_{c_i}\circ f_i)^*\mathbf{P}^\times$ when restricted to $\mathbf{U}$ gives rise to an element in the kernel

$$\ker(\mathrm{Pic}(\mathbf{U})\longrightarrow \mathrm{Pic}(C_K)).$$

Now note that we have an isomorphism of line bundles (corresponding to $\mathbb{G}_{m,\mathbf{J}}$-torsors)

$$(\mathrm{id}, hm\cdot\circ \mathrm{t}_{c_i}\circ f_i)^*\mathbf{P} \simeq ((\mathrm{id}, m\cdot\circ \mathrm{t}_{c_i}\circ f_i)^*\mathbf{P})^{\otimes h} \tag{16}$$

using equation 8. By Lemma 2.14 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 $\mathbf{U}$. Therefore, $\mathbf{T}$ 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 $\mathbb{G}_m^{\rho-1}(\mathbf{U}) = (\mathcal{O}_{\mathbf{U}}(\mathbf{U})^\times)^{\rho-1} = (\mathcal{O}_K^\times)^{\rho-1}$ again by Lemma 2.14. □

The following lemma is used in the proof above.

Lemma 2.14. *Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ as above. 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 entirely h-torsion. In other words, for a line bundle L over $\mathbf{U}$ that becomes trivial over the generic fiber C_K, $L^{\otimes h}$ is trivial over $\mathbf{U}$.*

Proof. By construction $\mathbf{U}$ is regular thus locally factorial, so we do not distinguish the class of line bundles and Weil divisors. First let D be a vertical divisor on $\mathbf{U}$, namely it 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 $\sum_{\mathfrak{p}} hn_{\mathfrak{p}}U_{\mathbb{F}_{\mathfrak{p}}}$, where $n_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. Clearly D is the image of the divisor $\sum_{\mathfrak{p}} hn_{\mathfrak{p}}$ along the natural map $\mathrm{Pic}(\mathcal{O}_K)\to \mathrm{Pic}(\mathbf{U})$, which is 0 since $\mathrm{Pic}(\mathcal{O}_K)$ has size h. Now let D be a general element of $\mathrm{Pic}(\mathbf{U})$ (which we view as a Weil divisor on $\mathbf{U}$) that lies in the kernel $\ker(\mathrm{Pic}(\mathbf{U})\to \mathrm{Pic}(C_K))$. 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. □

Remark 2.15. When $h = 1$ the lemma simply says that the restriction $\mathrm{Pic}(\mathbf{U})\to \mathrm{Pic}(C_K)$ is injective. This map is of course not in general injective when $h \neq 1$. Indeed, in the case it suffices to take $D = U_{\mathfrak{p}} \in \mathrm{Div}(\mathbf{U})$ where $\mathfrak{p}$ is a non-principal prime ideal of $\mathcal{O}_K$.

3. The main theorem

In this section we state the main theoretical results of the paper. We also describe the strategy of the geometric method in slightly more detail.

Assumption 3.1. *Throughout, we make the following assumption on the prime p.*

- *The curve C_K has good reduction at each prime $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ of K that sits above p.*
- *Each $\mathfrak{p}_i$ satisfies $e(\mathfrak{p}_i/p) < p-1$.*
- *Finally, 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 $1\le i\le s$. The set of primes p satisfying Assumption 3.1 clearly has positive density.

Notation 3.2. We further adopt the following notation:

- Let $\mathcal{O}_{K,p} := \mathcal{O}_K\otimes\mathbb{Z}_p$ be the p-adic completion of $\mathcal{O}_K$. This is isomorphic to the product of $\mathfrak{p}_i$-adic completions $\mathcal{O}_{K,\mathfrak{p}_1}\times\ldots\times\mathcal{O}_{K,\mathfrak{p}_s}$.
- $\overline{\mathcal{O}_{K,p}}$ denotes $(\mathcal{O}_K\otimes\mathbb{F}_p)_{\mathrm{red}}$, which is isomorphic to the product of the residue fields $\mathbb{F}_{\mathfrak{p}_1}\times\ldots\times\mathbb{F}_{\mathfrak{p}_s}$.

- For any $\mathcal{O}_K$-scheme X, we have natural identifications
$$X(\mathcal{O}_{K,p}) = X_{\mathcal{O}_{K,\mathfrak{p}_1}}(\mathcal{O}_{K,\mathfrak{p}_1}) \times \ldots \times X_{\mathcal{O}_{K,\mathfrak{p}_s}}(\mathcal{O}_{K,\mathfrak{p}_s}),$$
$$X(\overline{\mathcal{O}_{K,p}}) = X_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_{\mathfrak{p}_1}) \times \ldots \times X_{\mathbb{F}_{\mathfrak{p}_s}}(\mathbb{F}_{\mathfrak{p}_s}).$$
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 $X(\mathcal{O}_{K,p})$ 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 3.3. The reason to consider $\mathcal{O}_{K,p}$ (instead of $\mathcal{O}_{K,\mathfrak{p}}$ for a prime $\mathfrak{p}$ of K) is that we choose to work with all primes above p simultaneously (instead of fixing a single prime) in this article. This is in agreement with the approach in [Sik13].

3.1. **Revisiting the strategy.** Let $\mathbf{U}$ be an open subscheme of $\mathbf{C}^{\mathrm{sm}}$ obtained in Construction 2.10. 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 $\mathbf{T}$. 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 (Remark 2.11), and each $\mathbf{U}(\mathcal{O}_K)$ is the disjoint union of finitely many "residue disks" $\mathbf{U}(\mathcal{O}_K)_u$. Thus, for our purposes, it suffices to bound the size $\mathbf{U}(\mathcal{O}_K)_u$ 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 by the following commutative diagram:

$$\begin{array}{ccccc} \mathbf{U}(\mathcal{O}_K)_u & & \hookrightarrow & & \mathbf{U}(\mathcal{O}_{K,p})_u \\ \downarrow{\scriptstyle \tilde{j}_b^U} & & & & \downarrow{\scriptstyle \tilde{j}_b^U} \\ \mathbf{T}(\mathcal{O}_K)_t & \hookrightarrow & \mathbf{Y}_t & \hookrightarrow & \mathbf{T}(\mathcal{O}_{K,p})_t \end{array} \tag{17}$$

where the top horizontal arrow is induced by the inclusion $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,p}$, while
$$\mathbf{Y}_t := \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$$
denotes the p-adic completion of $\mathbf{T}(\mathcal{O}_K)_t$ in $\mathbf{T}(\mathcal{O}_{K,p})_t$. We view $\mathbf{U}(\mathcal{O}_K)_u$ (resp. $\mathbf{U}(\mathcal{O}_{K,p})_u$) as a subset of $\mathbf{T}(\mathcal{O}_K)_t$ (resp. $\mathbf{T}(\mathcal{O}_{K,p})_t$) via the map $\tilde{j}_b^U$ in the diagram above. 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, our goal is to bound the intersection
$$\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t \tag{18}$$
which takes place in the p-adic manifold $\mathbf{T}(\mathcal{O}_{K,p})_t$.

Remark 3.4. For this intersection to have a chance to be finite, some conditions must be imposed in the style of the original Chabauty condition "$r < g$". We will come back to this point in §3.3 after stating the main technical result of the paper.

3.2. **The key technical result.** In this subsection we give a description of $\mathbf{Y}_t$, which is a crucial step in bounding the intersection in 18.

Notation 3.5. We fix the following notations.

- Let $r := \operatorname{rank}_{\mathbb{Z}} J_K(K)$ be the Mordell–Weil rank of J_K over K.
- We let $\mathbf{J}(\mathcal{O}_K)_0$ denote the subgroup of $J_K(K) = \mathbf{J}(\mathcal{O}_K)$, given by kernel
$$\mathbf{J}(\mathcal{O}_K)_0 := \ker\left(\mathrm{red} : \mathbf{J}(\mathcal{O}_K) \to \mathbf{J}(\overline{\mathcal{O}_{K,p}})\right).$$
- Let q^* denote the exponent of $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, that is, the least common multiple of
$$q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$$
for $i = 1, 2, \ldots, s$.
- For each i, 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 $\sum_{\mathfrak{p}_i|p} k_i = d$.

By Assumption 3.1 on p, we know that for each i, the reduction map
$$\mathbf{J}(\mathcal{O}_K) \to \mathbf{J}(\mathbb{F}_{\mathfrak{p}_i})$$
is injective on the torsion points of $\mathbf{J}(\mathcal{O}_K)$ by [Kat80, Appendix]. Hence $\mathbf{J}(\mathcal{O}_K)_0$ is a free $\mathbb{Z}$-module of rank r. The scheme $\mathbf{T} \times_{\mathcal{O}_K} \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ is smooth over $\mathcal{O}_{K,\mathfrak{p}} \simeq \mathbb{Z}_p^{k_\mathfrak{p}}$ of relative dimension $g + \rho - 1$. By choosing a regular system of parameters for the residue disk above the point $t \in \mathbf{T}(\mathbb{F}_\mathfrak{p})$, we obtain a homeomorphism
$$\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_t \simeq \mathbb{Z}_p^{(g+\rho-1)k_\mathfrak{p}}.$$
In particular, the dimension of $\mathbf{T}(\mathcal{O}_{K,p})$ as a locally analytic p-adic manifold is
$$(g + \rho - 1) \sum_{\mathfrak{p}|p} k_\mathfrak{p} = (g + \rho - 1)d.$$

The idea is to parametrize the p-adic closure $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ using the free $\mathbb{Z}_p$-module
$$(\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p.$$
Here the subscript "tf" stands for the torsion free part. In §4.1, we will prove the following proposition (in a precise form, see Proposition 4.6).

Proposition 3.6 (Coordinates on $\mathbf{T}$: rough form)**.** *There exists a map*
$$E' : \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t \tag{19}$$
(upon fixing a basis for the free $\mathbb{Z}$-module $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0$) which can be described using the partial composition laws described in §2.2, and satisfies the following property
$$E'(q^*\mathbb{Z}^{\delta(\rho-1)+r}) \subset \mathbf{T}(\mathcal{O}_K)_t \subset E'(\mathbb{Z}^{\delta(\rho-1)+r}). \tag{20}$$
Here q^* is the integer defined in Notation 3.5.

We then p-adically interpolate the map E' to get the following result in §4.2.

Theorem 3.7 (p-adic interpolation: rough form)**.** *There is a unique map*
$$\kappa : (\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$$

which makes the diagram

$$\begin{array}{ccccccc}
\mathbb{Z}^{\delta(\rho-1)+r} & \xrightarrow{\simeq} & \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0 & \xrightarrow{E'} & \mathbf{T}(\mathcal{O}_{K,p})_t & \xrightarrow{\simeq} & \mathbb{Z}_p^{(g+\rho-1)d} \\
\downarrow & & \downarrow & & \| & & \| \\
\mathbb{Z}_p^{\delta(\rho-1)+r} & \xrightarrow{\simeq} & (\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)_{\mathrm{tf}} \times \mathbf{J}(\mathcal{O}_K)_0) \otimes \mathbb{Z}_p & \xrightarrow{\exists!\kappa} & \mathbf{T}(\mathcal{O}_{K,p})_t & \xrightarrow{\simeq} & \mathbb{Z}_p^{(g+\rho-1)d}
\end{array}$$

commute, such that the composed map in the bottom row is given by a $(g+\rho-1)d$*-tuple of convergent power series* $(\kappa_1, \dots, \kappa_{(g+\rho-1)d})$ *with* $\kappa_i \in \mathbb{Z}_p\langle z_1, \dots, z_{\delta(\rho-1)+r}\rangle$.

Corollary 3.8. *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 (20) implies that $\operatorname{Im}\kappa$ contains $\mathbf{T}(\mathcal{O}_K)_t$, 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

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

where the last containment uses (the first inclusion in) (20). This concludes the proof. □

Finally, to finish the theoretical component of the geometric quadratic Chabauty method, we prove the following result in §5. To state this result, we first remark that the course of the proof of Theorem 3.7 provides us with a certain ideal

$$I \subset \mathbb{Z}_p\langle z_1, ..., z_{\delta(\rho-1)+r}\rangle$$

which depends on $\mathbf{U}$ and the point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$ (see §5 for its precise construction). The more precise form of Theorem 1, modulo the construction of the ideal I, is the following

Theorem 3.9. *If* $\overline{A} := \left(\mathbb{Z}_p\langle z_1, ..., z_{\delta(\rho-1)+r}\rangle/I\right) \otimes \mathbb{F}_p$ *is finite dimensional over* $\mathbb{F}_p$*, then the number of rational points in* $\mathbf{U}(\mathcal{O}_K)_u$ *is bounded by*

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

As discussed in the introduction, we expect this to provide an explicit algorithm to compute rational points on C_K.

3.3. **Geometric quadratic Chabauty condition.** We finish this section with the promised discussion on the "quadratic Chabauty conditions".

We retain all notation and assumptions from the previous sections, in particular Assumption 3.1 on the prime p. From §3.2, we know that, for each prime $\mathfrak{p}$ above p, the set $\mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})$ is equipped with the structure of a p-adic manifold of dimension $(g+\rho-1)k_{\mathfrak{p}}$. Therefore, $\mathbf{T}(\mathcal{O}_{K,p})$ is a (locally analytic) p-adic manifold of dimension

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

Now, by Theorem 3.7 and Corollary 3.8, the p-adic manifold $\mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p$ is parametrized by $\mathbb{Z}_p^{\delta(\rho-1)+r}$ via the map

$$\mathbb{Z}_p^{\delta(\rho-1)+r} \xrightarrow{\kappa} \mathbf{Y}_t \hookrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t \xrightarrow{\simeq} \mathbb{Z}_p^{(g+\rho-1)d},$$

which is is given by a $(g+\rho-1)d$-tuple of elements in $\mathbb{Z}_p\langle z_1,\dots,z_{\delta(\rho-1)+r}\rangle$. Therefore, the dimension of the p-adic manifold $\mathbf{Y}_t$ is at most

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

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

Now back to our original goal. A necessary condition for the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$ in (18) to be finite is the following inequality on dimensions of p-adic 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 $\mathbf{T}(\mathcal{O}_{K,p})$. By the discussion above, this is equivalent to requiring

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

which in turn is equivalent to the condition

$$r \leq (g-1)d+(\rho-1)(r_2+1). \tag{21}$$

Definition 3.10. We say that a curve C_K of genus g over a number field K satisfies the *geometric quadratic Chabauty condition* if the inequality (21) holds.

The term geometric distinguishes our condition from the *Chabauty condition* (resp. *quadratic Chabauty condition*) associated to the classical Chabauty (resp. quadratic Chabauty) method. We briefly compare these conditions below.

Remark 3.11.

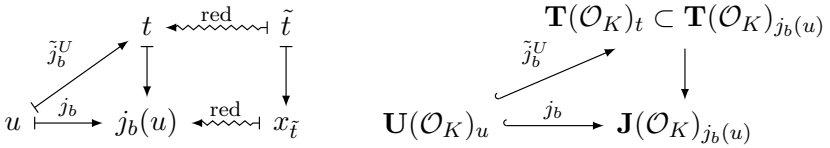
- When $K=\mathbb{Q}$ the condition (21) becomes
$$r \leq g+\rho-2,$$
which is the same condition as found in [EL19].
- In [Sik13] the classical Chabauty method was extended to arbitrary number fields. The method is expected to be successful when
$$r \leq (g-1)d.$$
Hence the geometric quadratic Chabauty method is expected to go beyond the classical Chabauty method.
- In the recent work of [BBBM19], the authors extend the method of quadratic Chabauty (as part Kim's program) for hyperelliptic curves to number fields, and relax the condition of [Sik13] above to the following (see [BBBM19, (1.4)])
$$r \leq (g-1)d+r_2+1.$$
Our geometric Chabauty condition agrees with this when ρ is equal to 2, and is fact more general for $\rho \geq 2$.
- In the recent work of [Dog19], the author shows that, under a certain stringent condition on J_K and K, a certain "arithmetic quadratic Chabauty condition" implies that the set $C_K(K\otimes\mathbb{Q}_p)_2$ appearing in the method of Chabauty-Kim is finite. If one assumes the finiteness of the p-primary part of the Tate-Shafarevich group for J_K, then the aforementioned condition in [Dog19] agrees with our geometric condition (21). See [Dog19, Proposition 1.1 & Remark 1.3].

4. p-adic interpolation

We keep the notations from §3. The goal of this section is to prove Theorem 3.7, in other words, to describe the p-adic closure $\mathbf{Y}_t$ of $\mathbf{T}(\mathcal{O}_K)_t$ inside $\mathbf{T}(\mathcal{O}_{K,p})_t$.

4.1. **Parametrization of rational points in T.** In this subsection we first construct the map E' in Proposition 3.6.

Notation 4.1.
- Fix a basis $x_1, \dots, x_r$ of $\mathbf{J}(\mathcal{O}_K)_0 = \ker\big(\mathbf{J}(\mathcal{O}_K) \to \mathbf{J}(\overline{\mathcal{O}_{K,p}})\big)$. 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 torus $\mathbf{T}$ (assumed to exist, otherwise $\mathbf{U}(\mathcal{O}_K)_u = \emptyset$ and we are done) and 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 reader's convenience, we remark that the points defined above and the set $\mathbf{T}(\mathcal{O}_K)_{j_b()u}$ fits in the following diagrams



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

$$D : \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^r \longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$$

in terms of the biextension laws. This is similar to the construction in [EL19, §4] though we have to use the $\mathbb{G}_m$ action on the Poincaré torsor in a more crucial way. We carry out this step in detail and point out differences compared to [EL19] along the way. As a starting point, let us choose points $P_{i,j}, R_i, S_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_K)$ lifting the following points of $\mathbf{J} \times (\mathbf{J}^{\vee,\circ})^{\rho-1}(\mathcal{O}_K)$:

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

Here $\underline{f}$ is given by the functions f_i in Notation 2.5. Note that the points to be lifted are of the form $(*, h\cdot *)$, thus the existence of such lifts is guaranteed by Lemma 2.2. Also note that unlike the situation of [EL19], these lifts are no longer defined up to a finite choice as they are parametrized by $\mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$.

Given $\underline{n} \in \mathbb{Z}^r$, set

$$A(\underline{n}) = \sum\nolimits_{2,j} n_j \cdot_2 S_j, \quad B(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 R_i, \quad C(\underline{n}) = \sum\nolimits_{1,i} n_i \cdot_1 \Big(\sum\nolimits_{2,j} n_j \cdot_2 P_{i,j}\Big)$$

(here $\cdot_1$ and $\cdot_2$ denote the iteration of the operation $+_1$ and $+_2$, respectively, and similarly for $\sum_1$ and $\sum_2$), so that

$$\begin{aligned} A(\underline{n}) &\longmapsto \Big(x_{\tilde{t}},\ \sum_i n_i \underline{f}(hmx_i)\Big) = \Big(x_{\tilde{t}},\ hm\underline{f}\big(\sum_i n_i x_i\big)\Big), \\ B(\underline{n}) &\longmapsto \Big(\sum_i n_i x_i,\ (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})\Big), \\ C(\underline{n}) &\longmapsto \Big(\sum_i n_i x_i,\ \sum_i n_i \underline{f}(hmx_i)\Big) = \Big(\sum_i n_i x_i,\ hm\underline{f}\big(\sum_i n_i x_i\big)\Big). \end{aligned}$$

Next, set

$$D(\underline{n}) = \big(C(\underline{n}) +_2 B(\underline{n})\big) +_1 \big(A(\underline{n}) +_2 \tilde{t}\big).$$

Thus $D(\underline{n})$ is a point lying over the point

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

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

$$(x_{\tilde{t}}, (hm\cdot \circ \mathrm{t}_{\underline{c}} \circ \underline{f})(x_{\tilde{t}})).$$

4.1.2. *Construction of E.* The next step is to involve the $\mathbb{G}_m$-action. As pointed out earlier, this is one of the main technical innovations of this article (compared to [EL19]). Our aim is to extend the map

$$D : \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^r \to \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$$

to a map

$$E : \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1} \times \mathbf{J}(\mathcal{O}_K)_0 \simeq \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_K)$$

by including the $\mathbb{G}_m^{\rho-1}$-action on fibers, that is, by the formula

$$E(\zeta, \underline{n}) = \zeta \cdot D(\underline{n}), \quad \forall \zeta \in \mathbb{G}_m(\mathcal{O}_K)_{\mathrm{tf}}^{\rho-1}$$

(here the subscript tf stands for "torsion-free part" as before). It will be, however, important later on that this expression admits a description in terms of $+_1$, $+_2$ and their iterates $\cdot_1, \cdot_2$. To make this explicit, we describe this construction as follows.

Notation 4.2.
- We fix a free basis $u_1, \dots, u_\delta$ 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 an (arbitrary) splitting.
- For each $(\rho-1)$-tuple $u_{k,l} = (1, \dots, 1, u_k, 1, \dots, 1) \in \mathbb{G}_m^{\rho-1}(\mathcal{O}_K)$ where u_k sits at the l-th spot, we denote the corresponding elements in $\mathbf{P}^\times_{|\mathbf{J}\times 0}(\mathcal{O}_K)$ above the point $(x_{\tilde{t}}, 0)$ by $V_{k,l}$ (in the sense of Formula (7) but with $\mathbf{P}^\times$ in place of $P_K^\times$), and likewise denote the corresponding element above $(x_i, 0)$ by $W_{k,l,i}$.

Construction 4.3. For $\underline{n} \in \mathbb{Z}^r$, $1 \le k \le \delta$ and $1 \le l \le \rho - 1$, we define

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

so that $U_{k,l}(\underline{n})$ is the element representing multiplication by $u_{k,l}$ and lying above the point

$$(x_{\tilde{t}} + \sum_i n_i x_i, 0).$$

Finally, for a $(\rho-1)$-tuple of δ-tuples of integers $\underline{m} = (m_{k,l})_{\substack{1\le k\le \delta \\ 1\le l\le \rho-1}} \in \mathbb{Z}^{\delta(\rho-1)}$, the map E is defined by the following formula

$$E(\underline{m}, \underline{n}) = \Big(\sum\nolimits_{2,k,l} m_{k,l} \cdot_2 U_{k,l}(\underline{n}) \Big) +_2 D(\underline{n}).$$

In particular, $E(\underline{m}, \underline{n})$ defines a point in $\mathbf{T}(\mathcal{O}_K)$.

One easily checks that $E(\underline{m}, \underline{n})$ lies over the same point

$$\big(x_{\underline{n}}, \alpha(x_{\underline{n}})\big) \in \mathbf{J} \times \mathbf{J}^{\vee,\circ}(\mathcal{O}_K)$$

as $D(\underline{n})$ does. 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 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 4.4. *The map*

$$\begin{aligned} \mathcal{O}_{K,\mathrm{tor}}^{\times,\rho-1} \times \mathbb{Z}^{\delta(\rho-1)+r} &\longrightarrow \mathbf{T}(\mathcal{O}_K)_{j_b(u)} \\ (\varepsilon, \underline{m}, \underline{n}) &\longmapsto \varepsilon \cdot E(\underline{m}, \underline{n}) \end{aligned}$$

(where the subscript tor *stands for "torsion part") 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, $\underline{n} \mapsto D(\underline{n})$ 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 (as per discussion above), what is left is the torsion part, hence the factor $\mathcal{O}_{K,\mathrm{tor}}^{\times,\rho-1}$. □

4.1.3. *Construction of E'.* For the purpose of computing rational points, we wish to parametrize $\mathbf{T}(\mathcal{O}_K)_t$ instead of all of $\mathbf{T}(\mathcal{O}_K)_{j_b(u)}$ (via p-adic interpolation). Thus in this subsection, we modify the map E to obtain a map E' that additionally lands in the correct residue disk, i.e., so 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 says that this is already satisfied by E on a certain finite-index subgroup of $\mathbb{Z}^{\delta(\rho-1)+r}$.

Proposition 4.5. *Let q^* be the exponent of $\mathbb{G}_m(\overline{\mathcal{O}_{K,p}})$, that is, the least common multiple of $q_i - 1 = \#\mathbb{F}_{\mathfrak{p}_i} - 1$, $i = 1, 2, \ldots, s$. Then*

$$E(q^*\underline{m}, q^*\underline{n}) \subseteq \mathbf{T}(\mathcal{O}_K)_t.$$

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

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

lying 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

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

respectively. 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 since at least one coordinate is zero in each case (cf. § 2.2). 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 (in 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

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

Putting this together we obtain

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

(note the clash of additive and multiplicative notations). Therefore, we have

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

This verifies the claim. □

In fact, to get the desired map $\mathbb{Z}^{\delta(\rho-1)+r} \to \mathbf{T}(\mathcal{O}_K)_t$, which agrees with E on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, is strictly speaking not possible. However, we can still obtain a map E' on the entire group $\mathbb{Z}^{\delta(\rho-1)+r}$ that agrees with E on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$ at the cost of allowing "p-adic coefficients". We prove the following more precise version of Proposition 3.6.

Proposition 4.6 (Coordinates on $\mathbf{T}$)**.** *There is a map*

$$E' = E'(\underline{m}, \underline{n}) : \mathbb{Z}^{\delta(\rho-1)+r} \longrightarrow \mathbf{T}(\mathcal{O}_{K,p})_t$$

with the following properties:

(1) *$E'(\underline{m}, \underline{n})$ can be described using the partial group laws $+_1$, $+_2$ of $P^{\times,\rho-1}(\mathcal{O}_{K,p})$, and its iterates $\cdot_1, \cdot_2$, after a choice of finitely many points; more precisely, it is built from analogous terms $A'(\underline{n}), B'(\underline{n}), C'(\underline{n})$ and $U'_{k,l}(\underline{n})$ as in the description of $E(\underline{m}, \underline{n})$.*

(2) *For each $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$, there is a unique $(\rho-1)$-tuple of roots of unity of prime-to-p orders $\xi(\underline{m}, \underline{n}) \in \mathcal{O}_{K,p}^{\times,\rho-1}$ such that $\xi(\underline{m}, \underline{n}) \cdot E(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_{K,p})_t$, and we additionally have*

$$E'(\underline{m}, \underline{n}) = \xi(\underline{m}, \underline{n}) \cdot E(\underline{m}, \underline{n}).$$

Proof. Note that there is a unique multiplicative lift of units

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

right inverse to the reduction map, mapping precisely onto the prime-to-p part of the roots of unity in $\mathcal{O}_{K,p}$. Denote also by ι the induced map $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}) \to \mathbb{G}_m^{\rho-1}(\mathcal{O}_{K,p})$.

Since the action of $\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ on $\mathbf{T}(\overline{\mathcal{O}_{K,p}})_{j_b(u)}$(= 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 from $\mathbf{T}(\mathcal{O}_{K,p})_t$. This shows the existence and uniqueness of $\xi(\underline{m}, \underline{n})$ in (2) by considering the point $E(\underline{m}, \underline{n})$ viewed inside $\mathbf{T}(\mathcal{O}_{K,p})_{j_b(u)}$ via the canonical map $\mathbf{T}(\mathcal{O}_K) \hookrightarrow \mathbf{T}(\mathcal{O}_{K,p})$.

The strategy for defining E' is to modify the choices of the initial points in the construction of 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 §2.2). Thus, the neutral element 1 in these fibers makes sense, and, for example, there is a unique $\xi_{i,j} \in \mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}})$ such that $\xi_{i,j}\overline{P_{i,j}} = 1$; then we set $P'_{i,j} = \iota(\xi_{i,j})P_{i,j}$. One obtains the points $R'_i, S'_j \in \mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$ in a similar fashion. Likewise, we make modifications to the points $V_{k,l}$ and $W_{k,l,i}$ in the same fashion.[2]

Using these points, one can define the terms $A'(\underline{n}), B'(\underline{n}), C'(\underline{n})$, etc. as in the definition of $E(\underline{m}, \underline{n})$. Denote by $E'(\underline{m}, \underline{n})$ the result of this process. A formal computation similar to the proof of Proposition 4.5 then shows that $E'(\underline{m}, \underline{n}) \in \mathbf{T}(\mathcal{O}_{K,p})_t$ for all $(\underline{m}, \underline{n}) \in \mathbb{Z}^{\delta(\rho-1)+r}$. This proves (1).

[2]Alternatively, one can multiply the chosen basis of the torsion-free part of $\mathcal{O}_K$-units $u_1, \ldots, u_\delta$ by suitable roots of unity (of prime-to-p order) in $\mathcal{O}_{K,p}$ so that the resulting units are congruent to 1 mod $p\mathcal{O}_{K,p}$.

Finally, since $E'(\underline{m},\underline{n})$ was obtained by the same operations in terms of $+_1, +_2, \cdot_1$, and $\cdot_2$ as $E(\underline{m},\underline{n})$ apart from the $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification of the initial points, it follows from Remark 7 (*iii*) that $E'(\underline{m},\underline{n})$ also differs from $E(\underline{m},\underline{n})$ only by $\iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$-action modification, that is, $E'(\underline{m},\underline{n}) = \xi(\underline{m},\underline{n})E(\underline{m},\underline{n})$ for some $\xi(\underline{m},\underline{n}) \in \iota(\mathbb{G}_m^{\rho-1}(\overline{\mathcal{O}_{K,p}}))$. Using the uniqueness part of (2), this proves the indicated equality in (2). □

It remains to prove

Proposition 4.7. (1) *We have the following inclusions*

$$\mathbf{T}(\mathcal{O}_K)_t \subseteq E'(\mathbb{Z}^{\delta(\rho-1)+r}) \subseteq \mathbf{T}(\mathcal{O}_{K,p})_t.$$

Here $\mathbf{T}(\mathcal{O}_K)$ is viewed as a subset of $\mathbf{T}(\mathcal{O}_{K,p})$ via the canonical map.

(2) $\xi(q^*\mathbb{Z}^{\delta(\rho-1)+r}) = 1$*; that is, E and E' agree on the subgroup $q^*\mathbb{Z}^{\delta(\rho-1)+r}$.*

Proof. Part (2) follows directly from Propositions 4.5 and 4.6 (2). Let us prove (1). Given $Q \in \mathbf{T}(\mathcal{O}_K)_t \subseteq \mathbf{T}(\mathcal{O}_K)_{j_b(u)}$, by Proposition 4.4, there is a unique $\varepsilon \in \mathcal{O}_{K,\mathrm{tor}}^{\times,\rho-1}$ 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 $\mathcal{O}_{K,\mathrm{tor}}^{\times}$ embeds (by the natural map) into the prime-to-p part of $\mathcal{O}_{K,p,\mathrm{tor}}^{\times}$ (recall from Assumption 3.1 that $p \nmid |\mathcal{O}_{K,\mathrm{tors}}^{\times}|$), 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 part of Proposition 4.6, we have $\varepsilon = \xi(\underline{m},\underline{n})$, so that

$$Q = \varepsilon E(\underline{m},\underline{n}) = \xi(\underline{m},\underline{n})E(\underline{m},\underline{n}) = E'(\underline{m},\underline{n}).$$

□

To summarize, we have constructed the promised map

$$E' : \mathbb{Z}^{\delta(\rho-1)+r} \to \mathbf{T}(\mathcal{O}_{K,p})_t.$$

It is described in terms of the operations $+_1, +_2$ and its iterates $\cdot_1, \cdot_2$ on $\mathbf{P}^{\times,\rho-1}(\mathcal{O}_{K,p})$, and agrees with E on $q^*\mathbb{Z}^{\delta(\rho-1)+r}$, with the property (anticipated in (20)):

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

4.2. **p-adic interpolation.** The remaining part of the section aims to prove Theorem 3.7. This is done along the same lines as [EL19, §3, §5.1], in a slightly more general context. We also provide more details of this argument.

4.2.1. *Formal geometry.*

Notation 4.8. We fix a prime $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ 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 as before, for a point $x \in X(\mathbb{F}_\mathfrak{p})$, 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 $(\pi, t_1, t_2, \dots, t_m)$.

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

$$\begin{aligned} t = (t_1, t_2, \dots, t_m) : X(\mathcal{O}_{K,\mathfrak{p}})_x &\xrightarrow{\simeq} (\mathfrak{m}_{K,\mathfrak{p}})^m \\ \tilde{x} &\longmapsto (t_1(\tilde{x}), \dots, t_m(\tilde{x})) \end{aligned}$$

and after dividing by π, one gets

$$\tilde{t} = \left(\frac{t_1}{\pi}, \frac{t_2}{\pi}, \dots, \frac{t_m}{\pi}\right) : X(\mathcal{O}_{K,\mathfrak{p}})_x \xrightarrow{\simeq} (\mathcal{O}_{K,\mathfrak{p}})^m \,. \tag{22}$$

Now let $f : X \to Y$ be a morphism of schemes that are smooth over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimensions m and n, resp. Denote the analogous choice of a regular system of parameters at Y by $s_1, s_2, \dots, s_n$ and the corresponding bijection by $\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)} \to (\mathcal{O}_{K,\mathfrak{p}})^n$. Our immediate goal is the following.

Proposition 4.9. *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 $\mathcal{O}_{K,\mathfrak{p}}\langle X_1, X_2, \dots, X_m\rangle$, the p-adic, or equivalently π-adic, completion of $\mathcal{O}_{K,\mathfrak{p}}[X_1, X_2, \dots, X_m]$.) To show this, we follow closely [EL19, §3] and investigate the geometry of the situation.

Proof. Shrinking X to a sufficiently small affine open neighbourhood of x, we may assume that $t_1, t_2, \dots, t_m$ are regular global functions, defining an étale map

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

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

Note that a point $\tilde{x} : \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}} \to X$ 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 $\mathrm{Bl}_x X$ of X at x implies that every $\tilde{x} \in X(\mathcal{O}_{K,\mathfrak{p}})_x$ factors uniquely through $\mathrm{Bl}_x X$, more precisely through the open subscheme $\mathrm{Bl}^{(\pi)}_x X$ of $\mathrm{Bl}_x X$ where π is the generator of the exceptional divisor. Thus, we have a natural identification between $X(\mathcal{O}_{K,\mathfrak{p}})_x$ and $\mathrm{Bl}^{(\pi)}_x X(\mathcal{O}_{K,\mathfrak{p}})$.

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 $o : \operatorname{Spec} \mathbb{F}_\mathfrak{p} \to \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ to get $\mathrm{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}}$ and

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

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

$$\begin{array}{ccccc} \mathrm{Bl}^{(\pi)}_x X & \hookrightarrow & \mathrm{Bl}_x X & \longrightarrow & X \\ \downarrow{\scriptstyle \tilde{t}} & \square & \downarrow & \square & \downarrow{\scriptstyle t} \\ \mathrm{Bl}^{(\pi)}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \hookrightarrow & \mathrm{Bl}_o \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} & \longrightarrow & \mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}} \,. \end{array} \tag{23}$$

The map $\tilde{t}$ from (22) is just the morphism $\tilde{t}$ in the above diagram evaluated at $\mathcal{O}_{K,\mathfrak{p}}$-points (thus, in particular, the notations are compatible).

The map $\tilde{t}_{\mathbb{F}_\mathfrak{p}}$, obtained from base-changing the diagram (23) 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 $\mathcal{O}_{K,\pi}/(\pi^j)$ for every j. Denoting the rings of global functions of the (affine) schemes in question by

$\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X), \mathcal{O}(\mathrm{Bl}_o^{(\pi)}\mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}})$, resp., we infer that their π-adic (equivalently, p-adic) completions are the same, that is,

$$\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)} \simeq \widehat{\mathcal{O}(\mathrm{Bl}_o^{(\pi)}\mathbb{A}^m_{\mathcal{O}_{K,\mathfrak{p}}})} = \mathcal{O}_{K,\mathfrak{p}}[\tilde{X}_1,\dots,\tilde{X}_m] = \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1,\dots,\tilde{X}_m\rangle, \tag{24}$$

namely the algebra of integral formal power series converging on the unit disk.

Finally, 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

$$\tilde{f} : \mathrm{Bl}_x^{(\pi)}X \to \mathrm{Bl}_{f(x)}^{(\pi)}Y$$

which on the level of $\mathcal{O}_{K,\mathfrak{p}}$-points may be identified with $f : X(\mathcal{O}_{K,\mathfrak{p}})_x \to Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x)}$. Taking the p-adic completion of the associated ring map $\mathcal{O}(\mathrm{Bl}_{f(x)}^{(\pi)}Y) \to \mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$ and conjugating by the isomorphisms (24) for X and Y then yields a map

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

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

Remark 4.10. It will be useful later to note that $\mathcal{O}_{X,x}$ naturally embeds into $\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}$. The maximal ideal of $\mathcal{O}_X(X)$ corresponding to x becomes (π) in $\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)$, hence is mapped to the radical in $\widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}$. There is thus an induced map

$$\mathcal{O}_{X,x} \longrightarrow \widehat{\mathcal{O}(\mathrm{Bl}_x^{(\pi)}X)}.$$

For injectivity: after taking completions at the maximal ideal, the map becomes

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

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

Remark 4.11 (Restriction of scalar)**.** It will be beneficial for our purposes 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 $e_1, e_2, \dots, e_k$ of $\mathcal{O}_{K,\mathfrak{p}}$ as a $\mathbb{Z}_p$-module. Expressing everything with respect to this basis, the power series description of maps $\mathcal{O}_{K,\mathfrak{p}}^m \to \mathcal{O}_{K,\mathfrak{p}}^n$ gives rise to a power series description of maps $\mathbb{Z}_p^{km} \to \mathbb{Z}_p^{kn}$. More precisely, upon the introduction of formal variables $X_{i,j}$ by the rule

$$X_i = X_{i,1}e_1 + X_{i,2}e_2 + \cdots + X_{i,k}e_k, \tag{25}$$

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

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

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

Remark 4.12. Keeping the notation from the proof of Proposition 4.9, the map

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

can be, again, identified with the tangent map of $f_{\mathbb{F}_\mathfrak{p}} : X_{\mathbb{F}_\mathfrak{p}} \to Y_{\mathbb{F}_\mathfrak{p}}$ 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 make sure that the map $(f')^\# : \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \dots, \tilde{Y}_n\rangle \to \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{X}_1, \dots, \tilde{X}_m\rangle$ is given by $\tilde{Y}_i \mapsto \tilde{X}_i$ for $i \le m$ and by $\tilde{Y}_i \mapsto 0$ for $i > m$. In other words, the parameters s_i, t_i may be chosen so that $f^\#(s_i) = t_i$ for $i \le m$ and $s_{m+1}, \dots s_n$ generate the kernel of the map $f^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$. 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 $\tilde{Y}_{m+1}, \dots, \tilde{Y}_n$. As in Remark 4.11, we can identify the embedding with the affine embedding $\mathbb{Z}_p^{km} \to \mathbb{Z}_p^{kn}$, whose image is cut out by the $k(n-m)$ variables $\tilde{Y}_{i,j}$, $m < i \le n, 1 \le j \le k$.

4.2.2. *The case of group schemes.*

Setup. Let us now focus on a special case where $Y \to \operatorname{Spec} \mathcal{O}_{K,\mathfrak{p}}$ is a smooth scheme of relative dimension n and $X = G$ is a smooth commutative group scheme over Y of relative dimension m [3]. Let $e : Y \to G$ denote the identity section. We now consider a point $y \in Y(\mathbb{F}_\mathfrak{p})$ and the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \to Y(\mathcal{O}_{K,\mathfrak{p}})_y$.

As in the beginning of this subsection, for the purposes of this map we may replace Y by $\operatorname{Spec} \mathcal{O}_{Y,y}$ and G by $G_{\mathcal{O}_{Y,y}}$. Let us fix a system of parameters $\pi, s_1, s_2, \dots, s_n$, inducing a bijection $\tilde{s} : Y(\mathcal{O}_{K,\mathfrak{p}})_y \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^n$.

By [Sta20, 05D9], there is an affine open neighborhood $\operatorname{Spec} B = U \subseteq G_{\mathcal{O}_{Y,y}}$ of $e(y)$ such that e factors through U and such that, denoting the kernel of the associated map $e^\# : B \to \mathcal{O}_{Y,y}$ by I, I/I^2 is a free $\mathcal{O}_{Y,y}$-module of rank m. Upon fixing a sequence $t_1, t_2, \dots, t_m \in I$ that becomes the free basis of I/I^2, the sequence $\pi, s_1, s_2, \dots, s_n, t_1, t_2, \dots, t_m$ forms a system of parameters of $G_{\mathcal{O}_{Y,y}}$ at $e(y)$, establishing a bijection $(\tilde{s}, \tilde{t}) : G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^{n+m}$.

We further consider the formal $\mathcal{O}_{Y,y}$-group $\widehat{G_{\mathcal{O}_{Y,y}}}$, 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 $\mathcal{O}_{Y,y}[[t_1, t_2, \dots, t_m]]$. The group operation then induces a m-dimensional commutative formal group law $F_G(\underline{U}, \underline{V}) = (F_1, \dots, F_m)(U_1, \dots, U_m, V_1, \dots, V_m)$ over $\mathcal{O}_{Y,y}$, that is, formal group in the sense of [Hon70]. By [Hon70, Theorem 1], over $\mathcal{O}_{Y,y} \otimes \mathbb{Q}$, there are mutually inverse isomorphisms of formal group laws

$$F_{G,\mathbb{Q}} \underset{\exp}{\overset{\log}{\rightleftarrows}} (\widehat{\mathbb{G}}_a)^m_{\mathbb{Q}}$$

(here $(\widehat{\mathbb{G}}_a)^m$ denotes the d-dimensional addition law, given by the polynomials $U_i + V_i$ treated as power series over $\mathcal{O}_{Y,y}$, and the subscript $\mathbb{Q}$ denotes the "formal base change" to $\mathbb{Q}$). Explicitly, fixing a basis of invariant differentials of F_G (in the sense of [Hon70, Proposition 1.1]) $\omega_1, \dots, \omega_m \in \bigoplus_{i=1}^m \mathcal{O}_{Y,y}[[t_1, \dots, t_m]]\mathrm{d}t_i$, log is given by a m-tuple of formal power series $L_1, L_2, \dots, L_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \dots, t_m]]$ characterized by the property

$$L_i(0, \dots, 0) = 0, \quad \mathrm{d}L_i = \omega_i, \quad i = 1, 2, \dots, m \tag{26}$$

(and 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 $E_1, E_2, \dots, E_m \in (\mathcal{O}_{Y,y} \otimes \mathbb{Q})[[t_1, \dots, t_m]]$

[3] Thus, m from the previous discussion corresponds to $m + n$ in the situation at hand. We hope this does not cause too much confusion

characterized by the identities

$$E_i(L_1, L_2, \dots, L_m) = t_i, \quad i = 1, 2, \dots, m \tag{27}$$

(and it again follows that each E_i equals t_i in degrees ≤ 1).

The fibers of the map $G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \to Y(\mathcal{O}_{K,\mathfrak{p}})_y$ are naturally not only abelian groups but, moreover, $\mathbb{Z}_p$-modules: given a point $\tilde{y} \in Y(\mathcal{O}_{K,\mathfrak{p}})_y$, the fiber over $\tilde{y}$ is the kernel of the reduction map $G_{\tilde{y}}(\mathcal{O}_{K,\mathfrak{p}}) \to G_{\tilde{x}}(\mathbb{F}_\mathfrak{p})$ (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, verifying 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, describe the action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \to G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ coming from the $\mathbb{Z}_p$-action on fibers, in terms of convergent power series.

Proposition 4.13. *The formal logarithm and exponential induce the mutually inverse maps* log *and* exp

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

given by convergent power series (elements of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \dots, \tilde{Y}_n, \tilde{X}_1, \dots, \tilde{X}_m \rangle$*). For* $z \in \mathbb{Z}_p$*, 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* $z \cdot g = \exp(z \cdot \log(g))$*. Consequently, the action map* $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \to G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ *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 that are components of the formal logarithm and formal exponential, respectively. It can be deduced from the identity (26) that

$$|J| a_{i,J} \in \mathcal{O}_{Y,y} \text{ for all } J, \tag{28}$$

and a formal computation of the exponential based on the identities (27) as in [Haz78, A.4.6] together with (28) shows that

$$(|J|!) b_{i,J} \in \mathcal{O}_{Y,y} \text{ for all } J. \tag{29}$$

The induced map $\log : \mathcal{O}_{K,\mathfrak{p}}^{n+m} \to \mathcal{O}_{K,\mathfrak{p}}^{n+m}$ 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

$$\tilde{L}_i(\underline{\tilde{X}}) = \pi^{-1} \sum_{J \neq 0} a_{i,J} (\pi \underline{\tilde{X}})^J = \sum_{J \neq 0} \frac{\pi^{|J|-1}}{|J|} (|J| a_{i,J}) (\underline{\tilde{X}})^J, \quad i = 1, \dots, m \tag{30}$$

on the remaining components. Here $|J| a_{i,J}$ is considered as an element of $\mathcal{O}_{K,\mathfrak{p}}\langle \tilde{Y}_1, \dots, \tilde{Y}_m \rangle$ in the sense of Remark 4.10.

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

$$\tilde{E}_i(\underline{\tilde{X}}) = \pi^{-1} \sum_{J \neq 0} b_{i,J} (\pi \underline{\tilde{X}})^J = \sum_{J \neq 0} \frac{\pi^{|J|-1}}{|J|!} ((|J|!) b_{i,J}) (\underline{\tilde{X}})^J, \quad i = 1, \dots, m \tag{31}$$

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

To conclude that the power series (30), (31) 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 $\pi^{|J|-1}/(|J|!)$ (hence also $\pi^{|J|-1}/|J|$) are integral and converge to zero p-adically as $|J| \to \infty$. This is satisfied by the imposed condition $e < p-1$ on the ramification index (see Assumption 3.1), since then the p-adic valuations are

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

which is 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 $\mathbb{Z}_p$ as in Remark 4.11. The action map $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)} \to G(\mathcal{O}_{K,\mathfrak{p}})_{e(y)}$ then becomes a p-adically continuous map $\mathbb{Z}_p \times \mathbb{Z}_p^{ef(n+m)} \to \mathbb{Z}_p^{ef(n+m)}$ extending 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 about the map given by $(z,g) \mapsto \exp(z \cdot \log(g))$ on $\mathbb{Z}_p \times \mathbb{Z}_p^{ef(n+m)}$, so 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. □

We now return to our previous setting of treating all primes above $\mathfrak{p}$ at once.

Corollary 4.14. (1) *Let X, Y be smooth schemes over $\mathcal{O}_K$ of relative dimensions m, n, respectively. Let $f : X \to Y$ be a morphism of $\mathcal{O}_K$-schemes and let $x \in X(\overline{\mathcal{O}_{K,p}})$ be a point. Then there are bijections $X(\mathcal{O}_{K,p})_x \simeq \mathbb{Z}_p^{dm}, Y(\mathcal{O}_{K,p})_{f(x)} \simeq \mathbb{Z}_p^{dn}$ such that the induced map $f : X(\mathcal{O}_{K,p})_x \to Y(\mathcal{O}_{K,p})_{f(x)}$ is given by convergent power series with coefficients in $\mathbb{Z}_p$.*

(2) *Let $G \to Y$ 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. Then the map $\mathbb{Z} \times G(\mathcal{O}_{K,p})_{e(y)} \to G(\mathcal{O}_{K,p})_{e(y)}, (z,g) \mapsto z \cdot g$, extends to a map $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \to G(\mathcal{O}_{K,p})_{e(y)}$, describing the $\mathbb{Z}_p$-module action on fibers over $Y(\mathcal{O}_{K,p})_y$, and this map is given by convergent power series with coefficients in $\mathbb{Z}_p$.*

Proof. As in (3.2), a point $x \in X(\overline{\mathcal{O}_{K,p}})$ is given by an s-tuple $x_1 \in X(\mathbb{F}_{\mathfrak{p}_1}), x_2 \in X(\mathbb{F}_{\mathfrak{p}_2}), \dots, x_s \in X(\mathbb{F}_{\mathfrak{p}_s})$, 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 of $\mathcal{O}_K$-schemes $f : X \to Y$, the induced map $f : X(\mathcal{O}_{K,p})_x \to Y(\mathcal{O}_{K,p})_{f(x)}$ decomposes into product of the maps $f : X(\mathcal{O}_{K,\mathfrak{p}})_{x_i} \to Y(\mathcal{O}_{K,\mathfrak{p}})_{f(x_i)}$. Part (1) thus follows from Proposition 4.9 and Remark 4.11.

Similarly, 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, $G(\mathcal{O}_{K,p})_{e(y)}$ have $\mathbb{Z}_p$-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 4.13, each of the action maps $\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)} \to G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)}$ 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 product of the above action maps and precomposing with $\mathbb{Z}_p \times G(\mathcal{O}_{K,p})_{e(y)} \to \prod_i (\mathbb{Z}_p \times G(\mathcal{O}_{K,\mathfrak{p}_i})_{e(y_i)})$, 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, proving (2). □

4.2.3. *The p-adic interpolation.* Finally, we return to our setting and apply the above in order to p-adically interpolate the previously constructed map E'.

Proof of Theorem 3.7. By Corollary 4.14 (1), both the 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. Similarly, Corollary 4.14 (2) implies that the operations $\cdot_1, \cdot_2$ used in the construction of E' can be interpolated and described by convergent power series over $\mathbb{Z}_p$. Since composition of convergent power series with $\mathbb{Z}_p$-coefficients produces again convergent power series with $\mathbb{Z}_p$-coeficients, the claim follows. □

5. Bounding the rational points

In this section we prove Theorem 3.9 announced in §3, that is, to give a conditional upper bound on the size of the intersection $\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t$. Let $\mathfrak{p}$ be a prime above p as usual. As in §4.2, we choose parameters $x_1^{\mathfrak{p}}, \dots, x_g^{\mathfrak{p}}$ for $\mathbf{J}$ at the point $x_{\mathfrak{p}} := j_b^U(u_{\mathfrak{p}})$ as well as parameters $t_1^{\mathfrak{p}}, \dots, t_{\rho-1}^{\mathfrak{p}} \in \mathcal{O}_{\mathbf{T},t_{\mathfrak{p}}}$ such that

$$\pi_{\mathfrak{p}}, x_1^{\mathfrak{p}}, \dots, x_g^{\mathfrak{p}}, t_1^{\mathfrak{p}}, \dots, t_{\rho-1}^{\mathfrak{p}}$$

is a system of local parameters at $t_{\mathfrak{p}}$ for the smooth scheme $\mathbf{T}$ over $\mathcal{O}_{K,\mathfrak{p}}$ of relative dimension $g+\rho-1$. We obtain the following identifications:

$$\tilde{x} : \mathbf{J}(\mathcal{O}_{K,\mathfrak{p}})_{x_{\mathfrak{p}}} \simeq (\mathcal{O}_{K,\mathfrak{p}})^g$$
$$(\tilde{x}, \tilde{t}) : \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}} \simeq (\mathcal{O}_{K,\mathfrak{p}})^{g+\rho-1}.$$

Now, the tangent map of the lifted Abel-Jacobi map $\tilde{j}_b^U : \mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_{\mathfrak{p}}} \hookrightarrow \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}}$ (see Proposition 2.13) is injective at $\mathfrak{p}$ by smoothness. It follows, by Remark 4.12, 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 $g+\rho-2$ equations

$$f_1^{\mathfrak{p}}, \dots, f_{g+\rho-2}^{\mathfrak{p}} \in \mathcal{O}(\widehat{\mathrm{Bl}_{t_{\mathfrak{p}}}^{(\pi_{\mathfrak{p}})}}(\mathbf{T})) = \mathcal{O}_{K,\mathfrak{p}}\langle \tilde{x}_1^{\mathfrak{p}}, \dots, \tilde{x}_g^{\mathfrak{p}}, \tilde{t}_1^{\mathfrak{p}}, \dots, \tilde{t}_{\rho-1}^{\mathfrak{p}} \rangle,$$

which generate the kernel of the surjection

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

As before let $k_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ be the $\mathbb{Z}_p$-rank of $\mathcal{O}_{K,\mathfrak{p}}$. Following Remark 4.11, upon choosing a $\mathbb{Z}_p$-basis of $\mathcal{O}_{K,\mathfrak{p}}$ and introducing new variables $\tilde{x}_{i,j}^{\mathfrak{p}}$ for $i = 1, \dots, g$ and $j = 1, \dots, k_{\mathfrak{p}}$ as well as $\tilde{t}_{l,k}^{\mathfrak{p}}$ for $l = 1, \dots, \rho-1$ and $k = 1, \dots, k_{\mathfrak{p}}$, each $f_i^{\mathfrak{p}}$ corresponds uniquely to a $k_{\mathfrak{p}}$-tuple of power series

$$f_{i,1}^{\mathfrak{p}}, \dots, f_{i,k_{\mathfrak{p}}}^{\mathfrak{p}} \in \mathbb{Z}_p \left\langle \tilde{x}_{i,j}^{\mathfrak{p}}, \tilde{t}_{l,j}^{\mathfrak{p}} \right\rangle_{\substack{1 \le i \le g,\ 1 \le j \le k_{\mathfrak{p}} \\ 1 \le l \le \rho-1}}.$$

In conclusion, the analytic p-adic manifold $\mathbf{U}(\mathcal{O}_{K,\mathfrak{p}})_{u_{\mathfrak{p}}} \subset \mathbf{T}(\mathcal{O}_{K,\mathfrak{p}})_{t_{\mathfrak{p}}}$ is cut out by $(g+\rho-2)k_{\mathfrak{p}}$ convergent power series in $(g+\rho-1)k_{\mathfrak{p}}$ variables with coefficients in $\mathbb{Z}_p$.

Finally, note that $\mathbf{U}(\mathcal{O}_{K,p})_u$ inside $\mathbf{T}(\mathcal{O}_{K,p})_t$ is cut out by $(g+\rho-2)\sum_{\mathfrak{p}|p} k_{\mathfrak{p}} = (g+\rho-2)d$ convergent power series with coefficients in $\mathbb{Z}_p$. By Theorem 3.7, we have

$$\begin{array}{ccccc} & & \mathbb{Z}_p^{\delta(\rho-1)+r} & & \\ & & \downarrow{\scriptstyle \kappa} & \searrow^{(\kappa_i)_{i=1}^{(g+\rho-1)d}} & \\ \mathbf{U}(\mathcal{O}_K)_u & \xrightarrow{\tilde{j}_b^U} & \mathbf{Y}_t = \overline{\mathbf{T}(\mathcal{O}_K)_t}^p & & \\ \downarrow & & \downarrow & & \\ \mathbf{U}(\mathcal{O}_{K,p})_u & \xrightarrow{\tilde{j}_b^U} & \mathbf{T}(\mathcal{O}_{K,p})_t & = & \mathbb{Z}_p^{(g+\rho-1)d}. \end{array}$$

The computation of the desired intersection is accomplished via pulling all equations back via κ.

Construction 5.1. The elements $\kappa^* f_{i,j}^{\mathfrak{p}}$ (with $1 \leq i \leq g+\rho-2$, $1 \leq j \leq k_{\mathfrak{p}}$ and $\mathfrak{p}|p$) all lie in $\mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$. Let I denote the ideal in $\mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle$ generated by these elements and let A denote the quotient ring

$$A := \mathbb{Z}_p\langle z_1, \ldots, z_{\delta(\rho-1)+r}\rangle / I.$$

The intersection is algebraically expressed as the tensor product of rings, i.e., by quotienting by I. It follows that there is a bijection

$$\mathrm{Hom}(A, \mathbb{Z}_p) \longleftrightarrow \kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t). \tag{32}$$

Let $\bar{f}_{i,j}^{\mathfrak{p}} \in \mathbb{F}_p[\tilde{x}_{i,j}^{\mathfrak{p}}, \tilde{t}_{l,j}^{\mathfrak{p}}]$ denote the reduction modulo p and $\kappa^* \bar{f}_{i,j}^{\mathfrak{p}} \in \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]$. The ideal $\bar{I} = I\mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]$ is generated by the elements $\kappa^* \bar{f}_{i,j}^{\mathfrak{p}}$ and we let

$$\bar{A} := A \otimes \mathbb{F}_p = \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]/\bar{I}.$$

We are now ready to prove Theorem 3.9, which we conveniently restate for the reader:

Theorem 3.9. If $\bar{A}$ is finite, then $|\mathbf{U}(\mathcal{O}_K)_u| \leq \dim_{\mathbb{F}_p} \bar{A}$.

Proof. The ring A is p-adically complete by the same proof of [EL19, Theorem 4.12]. Moreover, since $\bar{A}$ is finite, A is finitely generated as a $\mathbb{Z}_p$-module. Hence it follows that

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

This gives the bound

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

This established, by (32), that the number of points in $\kappa^{-1}(\mathbf{U}(\mathcal{O}_{K,p})_u \cap \mathbf{Y}_t)$ is bounded by $\dim_{\mathbb{F}_p} \bar{A}$, thus we have

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

□

Remark 5.2. The geometric quadratic Chabauty condition is implicit in the assumption of Theorem 3.9. Indeed, in order for the ring

$$\bar{A} = \mathbb{F}_p[z_1, \ldots, z_{\delta(\rho-1)+r}]/\langle \kappa^* \bar{f}_{i,j}^{\mathfrak{p}} \rangle_{i,j,\mathfrak{p}}$$

to have a chance to be finite, the number of relations we quotient by must be at least the number of variables. In other words, we need $\delta(\rho-1)+r \leq (g+\rho-2)d$ which is equivalent to the condition (21).

Finally, we state a precise form of Question 5 from the introduction.

Question 5.3. *For a given curve C_K and a fixed regular model $\mathbf{C}$ over $\mathcal{O}_K$, does there always exist a prime p such that for each open subscheme $\mathbf{U}$ constructed in §2 and each point $u \in \mathbf{U}(\overline{\mathcal{O}_{K,p}})$, the ring $\overline{A} = \overline{A}_{\mathbf{U},u}$ constructed above is finite dimensional over $\mathbb{F}_p$?*

At present, we cheerfully hope that the answer to this question is positive. The only evidence we have comes from explicitly computable examples, both from [EL19] and our ongoing subsequent works.

References

[BBBM19] J.S. Balakrishnan, A. Besser, F. Bianchi, and J.S. Müller. Explicit quadratic Chabauty over number fields. *ArXiv Preprint*, arXiv:1910.04653, 2019.

[BD18] Jennifer S Balakrishnan and Netan Dogra. Quadratic chabauty and rational points i: p-adic heights. *Duke Math. J.*, 2018.

[BD19] Jennifer S Balakrishnan and Netan Dogra. An effective chabauty-kim theorem. *Compositio Math.*, 2019.

[BDM+19] Jennifer S Balakrishnan, Netan Dogra, J Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty—Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[Cha41] C. Chabauty. Sur les points rationels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941.

[Col94] Robert 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.

[Dog19] Netan Dogra. Unlikely intersections and the Chabauty-Kim method over number fields. Arxiv Preprint arXiv:1903.05032, 2019.

[EL19] B. Edixhoven and G. Lido. Geometric quadratic Chabauty. *ArXiv Preprint*, arXiv:1910.10752, 2019.

[EvdGM] B. Edixhoven, G. van der Geer, and B. Moonen. *Abelian Varieties*. Book Project. Available on Ben Moonen's Website.

[Gro72] A Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie (SGA7)*, volume 1. 1972.

[Haz78] Michiel Hazewinkel. *Formal groups and applications, volume 78 of*, volume 78. Academic Press, Inc., New York, 1978.

[Hon70] Taira Honda. On the theory of commutative formal groups. *Journal of the Mathematical Society of Japan*, 22(2):213–246, 1970.

[Kat80] Nicholas M Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1980.

[Min05] Kim Minhyong. The motivic fundamental group of $p_1\{0, 1, \infty\}$. *Invent. Math.*, 2005.

[Min09] Kim Minhyong. The unipotent albanese map and selmer varieties for curves. *Publ. RIMS*, 2009.

[Sik13] Samir Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013.

[Sta20] The Stacks Project Authors. Stacks project. available online at http://stacks.math.columbia.edu, 2020.

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

(David Lilienfeldt) Department of Mathematics, McGill University
E-mail address: david.lilienfeldt@mail.mcgill.ca

(Luciena X. Xiao) Department of Mathematics, California Institute of Technology
E-mail address: lucienaxiao@gmail.com

(Zijian Yao) Department of Mathematics, Harvard University
E-mail address: zijian.yao.math@gmail.com