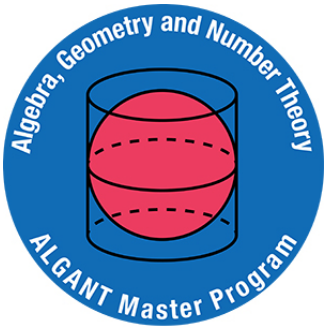
Chabauty's second youth: the linear case, effective versions and beyond

Stevell Muller



ALGANT Master thesis - Fall 2021

Chabauty's second youth: the linear case, effective versions and beyond

Student Stevell MULLER

Advisor Pierre PARENT

Universiteit Leiden, The Netherlands

Université de Bordeaux, France

Contents

Introduction

Diophantine[1] problems have been challenging mathematicians throughout centuries despite their elementary statements. The methods arising from the study of these problems turned out to be applicable to a larger range than needed. In fact, important tools were developed for solving specific types of Diophantine equations and they are used even outside the arithmetic context (one could think of the theory of quadratic forms). Most of the modern arithmetic geometry theory studied today was founded while working on Diophantine problems: for instance, there is the particular case of the study of arithmetic curves.

Given an algebraic curve C, in an arithmetic context, one may wonder how the set $C(\mathbb{Q})$ of $\mathbb{Q}$-rational points of this curve looks like. It was proved to be strongly depending on an invariant of this geometric object, called the *genus* g of the curve. If this genus g is null, the curve has either no $\mathbb{Q}$-rational points, or infinitely many of them. In the second case, it has been proved that as such a curve has at least one $\mathbb{Q}$-rational point, then it can be seen as a conic in $\mathbb{P}^2_{\mathbb{Q}}$, isomorphic to a copy of $\mathbb{P}^1_{\mathbb{Q}}$. Therefore, it can be represented as the zero set of a *quadratic form*. The study of $C(\mathbb{Q})$ can eventually be carried out, for instance, by the local-global principle of Hasse[2]:

Theorem 0.1 (Hasse-Minkowski[3])**.** *Let $q(X)$ be a quadratic form over $\mathbb{Q}$. $q(X)$ is isotropic over $\mathbb{Q}$ if, and only if, it is isotropic over $\mathbb{Q}_\nu$ for all places ν of $\mathbb{Q}$.*

In the case where the genus of C is 1, then $C(\mathbb{Q})$ is either empty, or there is at least one $\mathbb{Q}$-rational point on C, which is therefore an *elliptic curve*. Then, the well-known theorem of Mordell[4] provides us the following:

Theorem 0.2 (Mordell)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is of the form $\mathbb{Z}^r \times T$ where r is called the Mordell rank of E and T is a finite torsion group.*

This gives us that the set of $\mathbb{Q}$-rational points on C is a finitely generated abelian group. In 1922, Mordell conjectured that for higher genera, one might expect $C(\mathbb{Q})$ to be finite. This result has been proved by Gerd Faltings in 1983 and can be stated as follows:

Theorem 0.3 (Faltings)**.** *Let X be a curve defined over $\mathbb{Q}$. Suppose that the genus of X is greater or equal to 2. Then, the set $X(\mathbb{Q})$ of $\mathbb{Q}$-rational points on X is finite.*

Note that these 3 results have been generalised to the study of K-rational points for an arbitrary number field K. In practice, finding an explicit description of $C(\mathbb{Q})$ might not be easy, but some effective methods have been developed. However, despite its huge generality, Faltings's theorem fails at providing any algorithm to find an explicit description of this set. This can be an issue while trying to conclude on Diophantine problems: for instance, while solving the famous equations $x^n + y^n = z^n$ over the integers, for n natural. Translating this problem into geometry, seeing the set of solutions as a curve embedded into $\mathbb{P}^2_{\mathbb{R}}$, it can be proved that the genus of the curve obtained is going to the infinite as n becomes infinitely large. Therefore, Faltings' result states that the numbers of rational points is finite for n sufficiently large. However, a priori, we don't have any more information on the cardinality of these sets of points. We know, that except the trivial points, there are no rational points as soon as $n \geq 3$. To be able to give such an answer to the first Diophantine problem, using the geometric tools, it is necessary to resort to effective methods in order to sharply bound the number of rational points.

In 1941, inspired by an idea of Skolem[5], Chabauty[6] stated and proved a weaker version of Mordell's conjecture. The aforementioned idea, known as the *Skolem's p-adic method*, was to treat Diophantine problems over $\mathbb{Q}$ by extending it to p-adic completions of $\mathbb{Q}$. This trick transforms an arithmetic problem into a p-adically analytic one, considering Diophantine equations as defining equations of p-adic manifolds. (for further reading, I recommend the following bachelor thesis

[1] Diopanthus of Alexandria (circa 3rd century AD), Alexandrian mathematician
[2] Helmut Hasse (1898-1979), German mathematician
[3] Hermann Minkowski (1864-1909), German mathematician
[4] Louis Joel Mordell (1888–1972), American-born British mathematician
[5] Thoralf Albert Skolem (1887-1963), Norwegian mathematician
[6] Claude Chabauty (1910-1990), French mathematician

[Box14] dedicating to Skolem's p-adic method which is a good introduction with applications of this method. One may also read [BS86, Chapter 4, Part 6]). Let us formulate Chabauty's theorem in the following way, according to [Ser97, Subsection 5.1] :

Theorem 0.4 (Chabauty)**.** *Let A be an abelian variety defined over $\mathbb{Q}$ and let C be a generating curve in A. Then, for any finitely generated subgroup Γ in $A(\mathbb{Q})$ of rank r, such that $r < \dim A$, $C(\mathbb{Q}) \cap \Gamma$ is finite.*

Roughly speaking, what is meant by *generating curve* is a curve C embedded in a abelian variety A such that any point in A can be described as a linear combination of points of C (one can actually find a finite number of points on C generating all points in A). For a curve C of genus g, there exists an abelian variety J, called the *jacobian* of the curve, in which C can be embedded and C is a generating curve of J. Moreover, it can be proved that if A is an arbitrary abelian variety for which C is a generating curve, then A is a quotient of J; in the sense that there is a surjective homomorphism from J to A. The jacobian J is a g-dimensional variety, for which a generalized version of Mordell's theorem by Weil[7] provides that $J(\mathbb{Q})$ is finitely generated, say of rank r. So in this particular case, the previous theorem states that if r is less than the genus of C, then $C(\mathbb{Q})$ is finite.

The aim of this paper is to introduce a non-abelian variant of the so-called *Chabauty's method*. For convenience, we will describe the theory over $\mathbb{Q}$, though the work over an arbitrary number field has been carried out and, conceptually, it is not much more complicated. The structure will be the following: the first part of the thesis will be devoted to the description of the classical method of Chabauty with its effective approach developed by Coleman[8]. We will then introduce the geometric context to a first 'extension' of this method, known as *geometric Chabauty*. From this point, we will go to the main topic of this paper: the promising first non-trivial case of the Minhyong Kim's program, via a geometric description due to Bas Edixhoven and Guido Lido ([EL21]). The goal is to offer an overview of the tools involved and what one might expect from this geometric point of view.

We expect the reader to understand that the goal of Chabauty-like methods is not to reprove Faltings' result but to provide ideas and tools trying to make the study of rational points on curves more explicit. It may therefore appear that some results seem 'light' or 'incomplete': they are actually not in the sense that, providing finite bounds (even not sharp enough and under some 'restrictive' conditions) reifies the finiteness result of Faltings and let us expect a more precise, or complete, answer in some particular cases.

Acknowledgement

I would like to thank Pierre Parent for suggesting me this subject, and for all the talks we had during this last semester. I would also like to thank Bas Edixhoven for the small talk we had about his article but also for the support he provided me in Leiden during my first year of Master degree. Talking about support, I am grateful to all my classmates, who turned out to become my friends, and to my roommates who have helped me during the year.

I want to dedicate this thesis to my teammates Debam and Pano; to my close friends Léo, Mélanie and Bianca; to my parents and to my niece.

Finally, I would like to conclude by thanking Dajano Tossici who has been following me and advising me during my academic career for 3 years now: our discussions and collaborations were really helpful.

[7] André Weil (1906-1998), French mathematician
[8] Robert Frederick Coleman (1954-2014), American mathematician

1 Classical Chabauty

Let us consider an algebraic curve C of genus g defined over $\mathbb{Q}$. Without lost of generality, apart from a finite set of explicitly computable rational points, we assume this curve to be proper, smooth and geometrically connected. To fit in the context of Chabauty's theorem, we consider an abelian variety J associated to C, also defined over $\mathbb{Q}$: the jacobian variety of C. As the Albanese[9] variety generated by C, it is given with a map (a so-called *Abel*[10]*-Jacobi*[11] *map*) embedding C as a subvariety of J. Namely, if $b \in C(\mathbb{Q})$ is a rational point (supposing that $C(\mathbb{Q}) \neq \varnothing$), then one may define the embedding as follows:

$$\begin{array}{rccc} j_b & : & C & \to & J \\ & & P & \mapsto & [P-b] \end{array}$$

where $[\cdot]$ denotes the class of degree 0 divisors on C modulo principal ones. Indeed, a geometric description of J is to be the group scheme of equivalence classes of degree 0 divisors on C modulo principal divisors. One gets from its definition that J enjoys the 'good properties' of C, namely being smooth, proper and geometrically connected too. The dimension of J as a variety coincides with the genus of C, which has been denoted by g in our context.

From this point, a first idea to bound $\#C(\mathbb{Q})$ from above would be to prove the finiteness of $J(\mathbb{Q})$. However, thanks to the Mordell-Weil theorem, given J to be an abelian variety, $J(\mathbb{Q})$ is a finitely generated abelian group of rank $r \in \mathbb{N}$. Therefore, we cannot directly conclude since $J(\mathbb{Q})$ might be infinite in a general case. The idea of Chabauty was to embed the sets of $\mathbb{Q}$-rational points of C and J, respectively, into their sets of $\mathbb{Q}_p$-rational points, for a certain integral prime p. This gives rise to a well-known kind of commutative diagram (which will be completed later, see subsection 1.2):

$$\begin{array}{ccc} C(\mathbb{Q}) & \hookrightarrow & C(\mathbb{Q}_p) \\ \downarrow{\scriptstyle j_b} & & \downarrow{\scriptstyle j_b} \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p) \end{array}$$

For the sake of convenience, we will restrict ourselves to choosing a prime p at which C (and so J) has good reduction. Once we have established this square, we can provide more details on Chabauty's idea. In order to prove the finiteness of $C(\mathbb{Q})$, we embed it in $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p \subseteq J(\mathbb{Q}_p)$ and we prove that the previous intersection is finite. Note that the notation $\overline{(\cdot)}^p$ refers to the closure inside $J(\mathbb{Q}_p)$ for the p-adic topology. To do so, using the compactness of $J(\mathbb{Q}_p)$ as a p-adic manifold, it is sufficient to prove that $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ is discrete. This can be done by proving that the dimension cannot exceed 0, using a logarithm map from the p-adic Lie group $J(\mathbb{Q}_p)$ to its tangent space at 0. In fact, such a map being a local diffeomorphism, we will show that it implies that the dimension of $\overline{J(\mathbb{Q})}^p$ as a p-adic manifold do not exceed r, the Mordell-Weil rank of J. Therefore under the *Chabauty condition* $r < g$, we conclude using vanishing differential 1-forms that the dimension of $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ inside $J(\mathbb{Q}_p)$ has to be null.

The previous proof does not actually provide an effective bound from above for $\#C(\mathbb{Q})$. This part has been developed by Coleman, using p-adic integrals on C ([Col85]). Indeed, considering that the set of $\mathbb{F}_p$-rational points on C is finite, it is sufficient to bound the number of $\mathbb{Q}$-rational points reducing to each of the points of $C(\mathbb{F}_p)$: such a set of pre-images by reduction map is called a *residue disc* or *residue class*. The idea of Coleman was to compute power series on $\mathbb{Q}_p$ vanishing on the residue classes and whose *derivative* satisfies some good properties (which are going to be made explicit later). In fact, by choosing some interesting 1-form ω, Coleman has defined an *antiderivative* which vanishes on $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$. Making the correspondence between this antiderivative and a formal power series derived in ω, it just remained to estimate the number of zeroes of such a formal power series in $p\mathbb{Z}_p$ to conclude. This was the strategy used and proved

[9] Giacomo Albanese (1890-1947), Italian mathematician
[10] Niels Henrik Abel (1802-1829), Norwegian mathematician
[11] Carl Gustav Jakob Jacobi (1804-1851), German mathematician

to be effective by Coleman, as explained in [MP12, Section 5].

The next following parts will be devoted to describing and expliciting more precisely what have been explained above.

1.1 A proof of Chabauty's theorem

In order to prove Chabauty's theorem, one needs to describe the structure of $J(\mathbb{Q}_p)$ as a p-adic Lie group. This would help to introduce the log map mentioned earlier and to conclude on the dimension of $\overline{J(\mathbb{Q})}^p$, as a p-adic manifold.

Since any $\mathbb{Q}_p$-rational points on J can be expressed, in some local system of coordinates, by convergent power series for the p-adic topology, the group law on J is therefore locally p-adically analytic. This justifies the p-adic Lie group structure carried by $J(\mathbb{Q}_p)$. It is also compact for the p-adic topology, of dimension g as a manifold and we will now describe its differential structure. For this, we will change the base field over which we study J and denote $J_p := J_{\mathbb{Q}_p}$, the base change of J to $\mathbb{Q}_p$. (Note that $J(\mathbb{Q}_p) = J_p(\mathbb{Q}_p)$ since we do not change anything on the structure of J, just the base field over which we study it). This change made, we can define

$$\Omega_{J,p} := \Omega^1_{J_p/\mathbb{Q}_p}$$

the sheaf of regular differential 1-forms on J_p (over $\mathbb{Q}_p$). The set of global sections of this sheaf, denoted by $H^0(J_p, \Omega^1_{J,p})$, is actually a $\mathbb{Q}_p$-vector space of dimension $g = \dim(J(\mathbb{Q}_p))$.

Remark. The fact that $J(\mathbb{Q}_p)$ is g-dimensional could be understood from the $\mathbb{C}$-analytic description of J. As explained in [DS05, Chapter 6], $J(\mathbb{C})$ is isomorphic to a quotient of $\mathbb{C}^g$ by a full $\mathbb{Z}$-lattice. Therefore, as a complex analytic manifold, it is of dimension g and by showing that one can find a model over $\mathbb{Q}$ and then extend the scalars to $\mathbb{Q}_p$, one can expect $J(\mathbb{Q}_p)$ to be g-dimensional too. Moreover, as an analytic manifold, its tangent and cotangent spaces at a regular point are of the same dimension g. (Here $H^0(J_p, \Omega^1_{J,p})$ is identified with the cotangent bundle over J_p at 0).

The p-adic Lie group structure on $J_p(\mathbb{Q}_p)$ defines a g-dimensional formal group, isomorphic to the g-dimensional additive formal group $\mathbb{G}_a(\mathbb{Q}_p)$ since $\mathrm{char}(\mathbb{Q}_p) = 0$. Therefore, everywhere locally, there exists a basis of regular differential 1-forms invariant for the addition defined on J. For the additive formal group on J_p, such a basis can be given by the differentials of a local system of coordinates. Any such system of local parameters is associated with a g-dimensional *logarithm* associated to their differentials, for the formal group on J. By the p-adic manifold structure on $J_p(\mathbb{Q}_p)$, these local coordinates are p-adically analytic and therefore, the regular 1-forms associated to them are locally p-adically analytic too. Our goal is to describe the previous on a certain neighborhood of $0 \in J(\mathbb{Q}_p)$, and to gather all these information into an unique map, which will be called log (as mentionned earlier)

Let U denote the kernel of the reduction modulo p map

$$J(\mathbb{Q}_p) \twoheadrightarrow J(\mathbb{F}_p)$$

In fact, as made precise earlier, J has good reduction at p (since C has too) and therefore, there exists a smooth and complete fibered variety $\mathcal{J}$ over $\mathbb{Z}_p$ having J as generic fiber and whose special fiber is smooth over $\mathbb{F}_p$ (this is actually the *Néron model* of J). By smoothness, we have that any closed point on the special fiber is specialized by a closed point on the generic fiber, i.e. there exists a surjective map as above (where by the notation $J(\mathbb{F}_p)$ we actually refer to $\mathcal{J}_{\mathbb{F}_p}(\mathbb{F}_p)$, the $\mathbb{F}_p$-points on the special fiber). We have that U is actually an open neighborhood of $0 \in J(\mathbb{Q}_p)$ and one may define a system of local parameters, say $x_1, \ldots, x_g$,x on U. On this open set, $\omega_i := dx_i$ $(1 \leq i \leq g)$ form a basis of translation-invariant regular 1-forms, for this system of coordinates. We therefore have the following:

Proposition 1.1. *Let $\omega \in H^0(J_p, \Omega^1_{J,p})$ be a translation-invariant regular 1-form. Then, there exists an homomorphism*

$$\begin{array}{rccc} \eta_\omega & : & J(\mathbb{Q}_p) & \to & \mathbb{Q}_p \\ & & Q & \mapsto & \displaystyle\int_0^Q \omega \end{array}$$

Moreover, on U, η_ω is given by a p-adically convergent power series in the local coordinates of U.

Proof.
- ω being translation-invariant (for the group law on J) one has that any pullback of ω by a translation t_P is equal to ω itself. Namely, if $P \in J(\mathbb{Q}_p)$, $t_P^*\omega = \omega$. Therefore, for $P, Q \in J(\mathbb{Q}_p)$, one has
  - $\eta_\omega(0) = \int_0^0 \omega = 0$
  - $\eta_\omega(-Q) = \int_0^{-Q} \omega = -\int_{-Q}^0 \omega = -\int_0^Q t_{-Q}^*\omega = -\eta_\omega(Q)$
  - $\eta_\omega(P+Q) = \int_0^{P+Q} \omega = \eta_\omega(P) + \int_P^{P+Q} \omega = \eta_\omega(P) + \int_0^Q t_P^*\omega = \eta_\omega(P) + \eta_\omega(Q)$

  and η_ω is a homomorphism.
- Since $\omega_i = dx_i$ form a basis of $H^0(J_p, \Omega^1_{J,p})$ on U, there are multivariable functions f_i such that $\omega = \sum_i f_i dx_i$ on U. Therefore, by expanding into power series and formally integrating the f_i's on U, one has that η_ω is given (again on U) by a p-adically convergent power series on the x_i's.

□

Remark. For such a $\omega \in H^0(J_p, \Omega^1_{J,p})$, we will refer to η_ω from the proposition as the *antiderivative* of ω, vanishing at $0 \in J(\mathbb{Q}_p)$. It can be shown that η_ω, providing the two properties of the proposition, is actually unique. Moreover, we see by this definition that, since for $1 \le i \le g$, $dx_i = \omega_i$, one has $\eta_{\omega_i} = x_i$ $(1 \le i \le g)$.

As a corollary of the previous proposition and remark, we see that there is a well-defined bilinear pairing

$$\begin{array}{rccc} N & : & J(\mathbb{Q}_p) \times H^0(J_p, \Omega_{J,p}) & \to & \mathbb{Q}_p \\ & & (Q, \omega) & \mapsto & \eta_\omega(Q) \end{array}$$

from which we define the desired log map, namely

$$\begin{array}{rccc} \log & : & J(\mathbb{Q}_p) & \to & H^0(J_p, \Omega_{J,p})^\vee \\ & & Q & \mapsto & (\omega \mapsto N(Q, \omega)) \end{array}$$

which turns out to be a local diffeomorphism. In fact, as $H^0(J_p, \Omega_{J,p})$ is (non-canonically) the cotangent space of $J(\mathbb{Q}_p)$ at 0 (by definition), its dual is the tangent space of $J(\mathbb{Q}_p)$ at 0. So, for the tangent map of log at 0, both $T_0(J(\mathbb{Q}))$ and $T_0(H^0(J_p, \Omega^1_{J,p})^\vee)$ can be identified to $T_{J,p} := H^0(J_p, \Omega_{J,p})^\vee$, and so $T_0(\log) = \mathrm{Id}_{T_{J,p}}$ on a neighborhood of 0. This last point gives some information on the local structure of $J(\mathbb{Q}_p)$. Indeed, as a p-adic submanifold, $\overline{J(\mathbb{Q})}^p$ inside $J(\mathbb{Q}_p)$ has positive codimension under the Chabauty condition, as shown by this next result:

Lemma 1.1. $\dim(\overline{J(\mathbb{Q})}^p) \le r$, *where we recall that r is the Mordell-Weil rank of J.*

Proof. Since log is a local diffeomorphism, it preserves dimension and therefore, one observes that

$$\dim(\overline{J(\mathbb{Q})}^p) = \dim\left(\log(\overline{J(\mathbb{Q})}^p)\right)$$

as p-adic manifolds. Now, log is continuous and the compactness of $J(\mathbb{Q}_p)$ for the p-adic topology induces compactness on the p-adic closure of $J(\mathbb{Q})$. Therefore, one has that $\log(\overline{J(\mathbb{Q})}^p) = \overline{\log(J(\mathbb{Q}))}^p$. The latter is the p-adic closure of $\log(J(\mathbb{Q}))$ sitting in $T_{J,p}$ which can be identified, as a p-adic manifold, to $\mathbb{Q}_p^{\oplus g}$. In such a space, the p-adic closure coincides with the $\mathbb{Z}_p$-span, which gives us, in particular

$$\dim\left(\log(\overline{J(\mathbb{Q})}^p)\right) = \dim\left(\overline{\log(J(\mathbb{Q}))}^p\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(\mathbb{Z}_p \log(J(\mathbb{Q}))\right)$$

To conclude, we would like to compare this value with $r = \mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$. We remark that, for dimension reasons, $\ker(\log)$ is zero dimensional, and since $J(\mathbb{Q}_p)$ is compact, log has finite kernel. Therefore, the $\mathbb{Z}$-ranks of $J(\mathbb{Q})$ and $\log(J(\mathbb{Q}))$ are equal. But, any $\mathbb{Z}$-free system of points in $\log(J(\mathbb{Q}))$ may not be $\mathbb{Z}_p$-free and so, we have that

$$\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p \log(J(\mathbb{Q}))) \le \mathrm{rank}_{\mathbb{Z}}(\log(J(\mathbb{Q})))$$

□

Remark. This argument of dimension is actually the key point of Chabauty's method and it motivates the use of p-adic numbers. In fact, if we decided to localise at the Archimedean place and we wanted to apply the same argument with the following Chabauty's diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \hookrightarrow & C(\mathbb{R}) \\ \downarrow{\scriptstyle j_b} & & \downarrow{\scriptstyle j_b} \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{R}) \end{array}$$

we would not have obtained the same result in general. Indeed, as made precise by a conjecture of Barry Charles Mazur (see [Maz92, Conjecture 5]), if $J(\mathbb{Q}) \subseteq J$ is dense with J simple, then the conjecture says that $\overline{J(\mathbb{Q})} \subseteq J(\mathbb{R})$, for the real topology, is open. Therefore, $C(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ would contain a neighborhood of 0 sitting in $C(\mathbb{R})$, implying that the intersection would be infinite. It does not provide any contradiction on the finiteness of $C(\mathbb{Q})$, but this real-analytic approach is not helpful for our task.

Under the assumption $r < g$, we indeed have that $\overline{J(\mathbb{Q})}^p$ inside $J(\mathbb{Q}_p)$ has positive codimension. The proof of Chabauty's theorem will rely on this and a last result, linking the differential forms on C and on J. Namely:

Lemma 1.2. *One has that $j_b^*: H^0(J_p, \Omega_{J,p}) \to H^0(C_{\mathbb{Q}_p}, \Omega^1_{C_{\mathbb{Q}_p}/\mathbb{Q}_p})$ is an isomorphism. In particular, if ω is a non-zero regular differential 1-form on J over $\mathbb{Q}_p$, then its restriction to C is non-zero too.*

Proof. Once again, such a result could be proved using a similar result on $\mathbb{C}$. Indeed, the complex Abel-Jacobi map $C/\mathbb{C} \to J/\mathbb{C}$ is given by looking at the classes of path-integration modulo loop-integration of a basis of differential forms on C (see [DS05, Chapter 6]). From the description of this map, it is clear that taking the pullback along it will define an isomorphism between the spaces of regular differential 1-forms. Therefore, once again by restricting scalars to $\mathbb{Q}$ and extending them to $\mathbb{Q}_p$, the isomorphism holds again.
For a more direct and adapted proof to the case of $\mathbb{Q}$, see [Mil86, Proposition 2.2.] □

Theorem 1.1. *With the same notation as before, let's suppose that $r < g$. Then, $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ is finite.*

Proof. The following is adapted from a proof of Jean-Pierre Serre which can be found in [Ser97, Chapter 5, Section 1] :
Let's suppose that the intersection is infinite. C being proper, we have that $C(\mathbb{Q}_p) \subseteq J(\mathbb{Q}_p)$ is closed and therefore, $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ is closed in $J(\mathbb{Q}_p)$ is compact. Therefore, by compactness (a closed subspace of a compact space is compact too) one may find a sequence of distinct points $(P_n)_{n\in\mathbb{N}} \subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ converging to $P \in C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$. Acting continuously by translation on all these points, we can assume that $P = 0$ and by truncating the sequence, we can assume that all the P_n's sit in U (like P). According to Lemma 1.1, we know that $\dim(\overline{J(\mathbb{Q})}^p) \leq r < g = \dim(J(\mathbb{Q}_p))$ and therefore, we can assume that $(P_n)_{n\in\mathbb{N}}$ and P are in the hyperplane $\{x_1 = 0\}$ ($\{x_i\}_{1\leq i\leq g}$ was defined to be a system of local coordinates on U). Therefore, since all the P_n's are on C, we see that the curve C intersects the hyperplane $\{x_1 = 0\}$ in infinitely many ($\mathbb{Q}_p$-)rational points. This means that, the analytic p-adic function x_1 has infinitely many zeroes on U, which is a neighborhood of 0 in J. Since the zero set of a p-adic analytic function on the curve C has to be discrete (so finite in our compact context), we finally have that $x_1 = 0$ in a neighborhood $U_C \subseteq U \cap C$ of 0 in C. Therefore, $\omega_1 = dx_1$ has infinitely many zeroes on C since it is 0 on U_C. But any non-zero differential forms on C has at most $2g - 2$ zeroes. Whence, ω_1 is zero on C which contradicts Lemma 1.2 (The ω_i's form a basis of differential forms on U, so in particular ω_1 is non zero). □

1.2 Coleman's approach

In order to, in a sense, make Chabauty's result explicit, Coleman considered residue discs of $\mathbb{Q}_p$-points reducing to some $\mathbb{F}_p$-points on C. The latter being of finite numbers, it was sufficient to

bound the number of points on each residue discs, sitting in $\overline{J(\mathbb{Q})}^p$, to effectively bound $\#C(\mathbb{Q})$. To do so, the main idea was to extend the parametrisation of p-adic integration made on J to the curve C, and then define an *antiderivation* map vanishing on the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$. In fact, it can be shown that such a map is locally expressed with p-adically convergent power series, for which one can find an effective bound of their zeroes on residue discs. This will give rise to such a new kind of diagram:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \hookrightarrow & C(\mathbb{Q}_p) & & \\ \downarrow{\scriptstyle j_b} & & \downarrow{\scriptstyle j_b} & \searrow & \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0(J_p, \Omega^1_{J,p})^\vee \end{array}$$

To go through Coleman's approach, we will start by defining what a residue disc is and by giving some interesting properties of it.

We recall that we assumed the curve C to have good reduction at the prime p. Therefore, in the same way as described earlier for J, there exists a smooth and complete fibered surface $\mathcal{C}$ over $\mathbb{Z}_p$ for which $C/\mathbb{Q}_p$ is the generic fiber. As before, the smoothness of the special fiber $\mathcal{C}_{\mathbb{F}_p}$ over $\mathbb{F}_p$ provides that there is a surjective *reduction modulo p* map

$$C(\mathbb{Q}_p) \twoheadrightarrow \mathcal{C}_{\mathbb{F}_p}(\mathbb{F}_p)$$

(for convenience, we will again denote by $C(\mathbb{F}_p)$ the $\mathbb{F}_p$-points on the special fiber of $\mathcal{C}$)

Definition 1.1. *Let $Q \in C(\mathbb{F}_p)$. We will denote by $C(\mathbb{Q}_p)_Q$ the set of $\mathbb{Q}_p$-points on C reducing modulo p to Q (via the previous mapping). $C(\mathbb{Q}_p)_Q$ is called the* residue disc/class *over Q in C.*

Remark. Since $\#C(\mathbb{F}_p)$ is finite, there are only finitely many residue classes. Therefore, to effectively bound $\#C(\mathbb{Q})$, we just need to focus on one residue class and then extend our results to the global study of residues.

From now on to the statement and proof of Coleman's theorem, we will fix a residue $Q \in C(\mathbb{F}_p)$ and $C(\mathbb{Q}_p)_Q$ the residue class over it. We will also denote $U_Q \subseteq \mathcal{C}$ an open neighborhood of Q in $\mathcal{C}$.

Proposition 1.2. *If t is a regular function on U_Q such that $t_{|\mathcal{C}_{\mathbb{F}_p}}$ (its reduction modulo p) is an uniformiser at Q, then*

$$t(C(\mathbb{Q}_p)_Q) \simeq p\mathbb{Z}_p$$

Proof. Let $\alpha \in p\mathbb{Z}_p$. The functional $t - \alpha$ has Q as a simple root modulo p, so by a multivariable version of Hensel[12]'s lemma (seeing t as a multivariable polynomial on the coordinates of a point of the curve), there exists an unique point $\beta \in C(\mathbb{Q}_p)$ such that $t(\beta) = \alpha$ and β reduces to Q modulo p. This proves that t sends bijectively $C(\mathbb{Q}_p)_Q$ into $p\mathbb{Z}_p$. □

The preceding proposition actually says that we can extend any uniformiser at Q to an uniformiser on $C(\mathbb{Q}_p)_Q$. Let's fix such an uniformiser t. Thanks to this, we will be able to formally describe the theory of p-adic integration of differential forms on C in an easiest way (since we can keep the same local coordinate)

Keeping the same notations used earlier, we will write C_p when referring to the curve C but studied over $\mathbb{Q}_p$, and $\Omega_{C,p} := \Omega^1_{C_p/\mathbb{Q}_p}$ its sheaf of regular differential 1-forms over $\mathbb{Q}_p$. According to Lemma 1.2, the natural embedding $C \hookrightarrow J$ induces the restriction of differential

$$H^0(J_p, \Omega^1_{J,p}) \to H^0(C_p, \Omega^1_{C,p})$$

which is an isomorphism of $\mathbb{Q}_p$-vector spaces. This isomorphism will let us define p-adic integration of differential forms on C from the description used on J. Namely, let $\omega' \in H^0(C_p, \Omega^1_{C,p})$ be the restriction of a non-zero translation-invariant differential form ω on J and let $P, P' \in C(\mathbb{Q}_p)$. Then, one defines

$$\int_P^{P'} \omega' := \int_0^{[P'-P]} \omega = \eta_\omega([P' - P])$$

where $[P' - P] = j_b(P') - j_b(P)$ for the group law on J (as an abelian variety).

[12]Kurt Wilhelm Sebastian Hensel (1861-1941), German mathematician

Proposition 1.3. *1. If $(P_i)_{i\in I}, (P_i')_{i\in I}$ are families of points in $C(\mathbb{Q}_p)$ such that the divisor $\sum_{i\in I}(P_i' - P_i)$ is principal, then*

$$\sum_{i\in I}\int_{P_i}^{P_i'}\omega' = 0$$

2. If $P, P' \in C(\mathbb{Q}_p)_Q$, then $\int_P^{P'}\omega'$ is given by a p-adically convergent power series in t, evaluated at the local coordinates of P and P'.

Proof. Those two properties follow directly from the description given of integration on C thanks to one on J, and Proposition 1.1. □

This proposition gives us that the restriction $\lambda_{\omega'} := (\eta_\omega)_{|C(\mathbb{Q}_p)}$ given by

$$\begin{array}{rccc} \lambda_{\omega'} & : & C(\mathbb{Q}_p) & \to & \mathbb{Q}_p \\ & & P & \mapsto & \int_0^P \omega' \end{array}$$

is locally p-adically analytic. The following makes this result even clearer:

Lemma 1.3. *Assume that the reduction modulo p of ω' on the special fiber $\mathcal{C}_{\mathbb{F}_p}$ is non-zero. Then*

1. *There exists a convergent power series $w(t) \in \mathbb{Z}_p[[t]]$ with $w(t)$ modulo p being non-trivial and such that $\omega'_{|C(\mathbb{Q}_p)_Q} = w(t)dt$;*
2. *There exists a convergent power series $\Lambda(t) \in \mathbb{Q}_p[[t]]$ such that $(\lambda_{\omega'})_{|C(\mathbb{Q}_p)_Q} = \Lambda(t)$ and $\Lambda'(t) = w(t)$ on $C(\mathbb{Q}_p)_Q$.*

Proof. 1. Thanks to Proposition 1.2, we have that t is also an uniformiser on $C(\mathbb{Q}_p)_Q$. Therefore, on $C(\mathbb{Q}_p)_Q$, dt is a generator of 1-differentials and one can find a p-adically convergent power series $w(t) \in \mathbb{Q}_p[[t]]$ such that $\omega'_{|C(\mathbb{Q}_p)_Q} = w(t)dt$. Since the reduction modulo p of ω' is non-zero, $w(t)$ is non-trivial modulo p and by rescaling if necessary ω' by an element of $\mathbb{Q}_p^\times$, we can choose $w(t) \in \mathbb{Z}_p[[t]]$.

2. From the previous point, we can formally integrate $w(t)$ on $C(\mathbb{Q}_p)_Q$, giving rise to a power series $\Lambda(t) \in \mathbb{Q}_p[[t]]$ (in fact, after integrating, one might observe that some coefficients of $\Lambda(t)$ are not p-adic integers). Then $\Lambda'(t) = w(t)$ on $C(\mathbb{Q}_p)_Q$ and by modifying the constant term of $\Lambda(t)$, the last property follows directly from the definition of $\lambda_{\omega'}$.

□

We will use this result to show that, by choosing an interesting candidate for ω (and so ω'), one has that $\lambda_{\omega'}$ vanishes on $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$. Therefore, it will just remain to bound the number of zeroes of this locally p-adically analytic function to conclude.

Recall that in Lemma 1.1, we proved that $\dim_{\mathbb{Z}_p}(\log(\overline{J(\mathbb{Q})}^p)) \leq r$. So, under the Chabauty condition $r < g$, we see that in $H^0(J_p, \Omega^1_{J,p})^\vee$ (of dimension g), $\log(\overline{J(\mathbb{Q})}^p)$ is contained in an hyperplane defined as the zero locus of some non-zero form $L: H^0(J_p, \Omega^1_{J,p})^\vee \to \mathbb{Q}_p$. By duality, $L \in (H^0(J_p, \Omega^1_{J,p})^\vee)^\vee \cong H^0(J_p, \Omega^1_{J,p})$. Since L is non-trivial, it corresponds bijectively to a non-zero regular 1-form ω, for which $\mathbb{Q}_p$-linearity of L implies that it is translation-invariant (for the group law on J). Moreover, by the description given of the log map, we have that

$$\eta_\omega = L \circ \log$$

and so η_ω vanishes on $\overline{J(\mathbb{Q})}^p$. We therefore deduce the following corollary:

Corollary 1.3.1. *Let ω' be the restriction of ω on C_p. Then :*

1. *If $(P_i)_{i\in I}, (P_i')_{i\in I}$ are families of points in $C(\mathbb{Q}_p)$ such that the class of the divisor $\sum_{i\in I}(P_i' - P_i)$ lies in $\overline{J(\mathbb{Q})}^p$, then*

$$\sum_{i\in I}\int_{P_i}^{P_i'}\omega' = 0$$

2. $\lambda_{\omega'} = (\eta_\omega)_{|C(\mathbb{Q}_p)}$ *vanishes on* $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$.

Finally, before stating and proving an effective version of Chabauty's theorem by Coleman, we need the following lemma using results from the theory of Newton polygons of power series:

Lemma 1.4. *Suppose that* $S(X) = (a_k)_{k\geq 0} \in \mathbb{Q}_p[[X]]$ *is convergent with formal derivative* $S'(X) = (b_k)_{k\geq 0} \in \mathbb{Z}_p[[X]]$ *(for all* $k \geq 0$, $b_k = (k+1)a_{k+1}$*) and let* $m_S := \min\{k \geq 0 \mid b_k \in \mathbb{Z}_p^\times\}$. *Then, under the assumption* $m_S < p-2$, S *has at most* $m_S + 1$ *zeroes in* $p\mathbb{Z}_p$.

Proof. Suppose that $m_S < p-2$. By definition, for $0 \leq i < m_S$, $\nu_p(b_i) \geq 0$ and so, since $b_i = (i+1)a_{i+1}$ with $i+1 < p$ (so with trivial p-adic valuation), we have that $a_{i+1} \in p\mathbb{Z}_p$. Similarly, since $\nu_p(m_S+1) = 0$ and $\nu_p(b_{m_S}) = 0$ by definition of m_S, one has that $\nu_p(a_{m_S+1}) = 0$. For $i-1 > m_S$, we have that $\nu_p(b_{i-1}) \geq 0$ since they are p-adic integers and so, $\nu_p(ia_i) \geq 0$, implying that

$$\nu_p(a_i) \geq -\nu_p(i)$$

and since we assumed that $m_S < p-2$, one has that for $i > m_S + 1$, $-\nu_p(i) > m_S + 1 - i$. Therefore, for $i > j > m_S + 1$, one has that

$$\begin{aligned}
\frac{\nu_p(a_i) - \nu_p(a_j)}{i-j} &> \frac{m_S + 1 - i - \nu_p(a_j)}{i - (m_S+1)} \\
&> -1 + \frac{\nu_p(a_j)}{m_S + 1 - i} \\
&> -1 + \frac{\nu_p(a_j)}{m_S + 1 - j} \\
&> -1
\end{aligned}$$

(The same result holds if $j = m_S + 1$). So, if we draw the Newton polygon of S, it will not have any slopes less than -1 on the right of the point $(m_S+1, 0)$. Therefore, the total horizontal length N_S of all segments of the Newton polygon of S of slope ≤ -1 is finite equal to $m_S + 1$. Therefore, by a p-adic Weierstrass preparation theorem (see [Kob12, Chapter 4, Theorem 14]), S can have at most $m_S + 1$ zeroes in $p\mathbb{Z}_p$. □

Remark. The assumption $m_S < p-2$ is necessary because, in the case of equality, for $i = p > m_S+1$, one would have $-\nu_p(i) = -1$ and $m_S + 1 - i = -1$ too. Therefore, the condition $-\nu_p(i) > m_S + 1 - i$ is not satisfied. In a general case, from this point, nothing can ensure that N_S would be finite, and so we cannot conclude on the finiteness of zeroes of S in (p).

Therefore, using the convergent power series $\Lambda(t) \in \mathbb{Q}_p[[t]]$ representing $\lambda_{\omega'}$ on $C(\mathbb{Q}_p)_Q$ (provided by Lemma 1.3), if $m := m_\Lambda < p-2$, $\Lambda(t)$ has at most $m+1$ zeroes in $p\mathbb{Z}_p \simeq C(\mathbb{Q}_p)_Q$. This actually translates to: $\lambda_{\omega'}$ has at most $m+1$ zeroes in $C(\mathbb{Q}_p)_Q$. Such a result holds on each residue disc and therefore $\lambda_{\omega'}$ has only finitely many zeroes. Hence, the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ is necessarily finite. The following theorem and its proof will summarize all this, and will provide an effective bound on $\#C(\mathbb{Q})$:

Theorem 1.2. *Let* $Q \in C(\mathbb{F}_p)$ *and let* $C(\mathbb{Q})_Q = C(\mathbb{Q}_p)_Q \cap C(\mathbb{Q})$. *Suppose that* $\Lambda_Q(t_Q) \in \mathbb{Q}_p[[t_Q]]$ *represents* $\lambda_{\omega'}$ *on* $C(\mathbb{Q}_p)_Q$ *(as in Lemma 1.3) for an uniformiser* t_Q *at* Q. *If we moreover assume that* $C(\mathbb{Q})_Q \neq \emptyset$, *then*

$$(m_{\Lambda_Q} < p-2) \implies (\#C(\mathbb{Q})_Q \leq m_{\Lambda_Q} + 1)$$

Remark. The conditions on the m_{Λ_Q}'s, being less or equal to $p-2$, could let understand that one has to choose a 'big' prime p for which the curve has good reduction and for which all the m_{Λ_Q} (of finite numbers $\leq \#C(\mathbb{F}_p)$) satisfy the condition of the theorem. In such case, it is expected to consider several residue classes and therefore to get a bound not sharp enough (yet computable if implemented in some computer algebra system). However, in most interesting cases for which this method is applied, one can expect this not to happen, or that a lower prime of good reduction will provide enough information to do the calculations (see [MP12, Section 8]).

Proof. Let $P \in C(\mathbb{Q})_Q$. Then, for any other $P' \in C(\mathbb{Q})_Q$, we have that $[P - P'] \in \overline{J(\mathbb{Q})}^p$ (because both points are in $C(\mathbb{Q})$) and therefore thanks to Corollary 1.3.1, one has that

$$\int_P^{P'} \omega' = 0$$

But since both P and P' are in $C(\mathbb{Q}_p)_Q$, Lemma 1.3, tells us that

$$P' \mapsto \int_P^{P'} \omega'$$

can be expressed on $C(\mathbb{Q}_p)_Q \simeq p\mathbb{Z}_p$ by a convergent power series $\Lambda_Q(t_Q) \in \mathbb{Q}_p[[t_Q]]$ where t_Q is an uniformiser at Q, satisfying $\Lambda'_Q(t_Q) \in \mathbb{Z}_p[[t_Q]]$. Therefore, applying the preceding lemma to $\Lambda_Q(t_Q)$, we see that the previous integration operator may have at most $m_{\Lambda_Q}+1$ zeroes on $C(\mathbb{Q}_p)_Q$, under the assumption $m_{\Lambda_Q} < p-2$. But since the integration operator vanishes in $C(\mathbb{Q})_Q$, this set may have at most $m_{\Lambda_Q} + 1$ points. □

A well-known corollary of this result can be stated as follows

Corollary 1.2.1. *If $p > 2g$, then $\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + (2g-2)$.*

Remark. This corollary provides an actual sharp bound in the case of a low genus curve and whenever such a curve has good reduction at a 'small' prime number. However, we see that for higher genera, such an upper bound tends to be bigger than expected. It is possible to give an explicit bound in the case where $p < 2g$, but in practice, such a bound may not be helpful.

All the preceding theory can be adapted to extend it to the study of the curve over an arbitrary number field. For instance, in the original paper of Chabauty ([Cha41]), the curves were studied over finite extensions of the number field generated by the coefficients of their defining polynomials. In another fashion, J.-P. Serre ([Ser97]) made a proof of a generalisation of Chabauty's theorem over an arbitrary number field by embedding C into any abelian variety A for which C is a generating curve (so not only into J). Moreover, one may find in the survey [MP12] examples of application of this method but also an appendix for the study at bad reduction primes.

1.3 Further comments and literature

This subsection will be dedicated to giving information about possible issues of Chabauty-Coleman method but also about generalisations and applications of this method.

1.3.1 Comments on effectiveness

We first give, without too many details, which kind of situation one may encounter while trying to effectively perform Chabauty-Coleman method on a given curve:

- What would happen if $r \geq g$? In such case, this is highly probable (but not necessary) that $\dim(\overline{J(\mathbb{Q})}^p) = g$ and so, $\overline{J(\mathbb{Q})}^p \subseteq J(\mathbb{Q}_p)$ would be open for the p-adic topology. Therefore, the existence of at least 1 point in the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ will imply the existence of infinitely many of them. Hence, we would not have any finite upper bounds for $\#C(\mathbb{Q})$. However, in the particular case $\dim(\overline{J(\mathbb{Q})}^p) < g \leq r$, it should be possible to find a subgroup of $J(\mathbb{Q})$ of rank equal to $\dim(\overline{J(\mathbb{Q})}^p)$ and having the same p-adic closure. In which case, one could replace $J(\mathbb{Q})$ by this smaller subgroup to perform Chabauty-Coleman.

- In the case where $r < g-1$, we see that for some dimension arguments, one may expect the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ inside $J(\mathbb{Q}_p)$ to be trivial (consisting only on the base-point b). Therefore, by choosing a 'good' prime, it might be possible to make this previous method effective. However, it is not clear that it would be an easy task, even using the effective version by Coleman.

- For our choice of η_ω, it may happen that its kernel is strictly larger than $\overline{J(\mathbb{Q})}^p$. As mentioned in [MP12, Section 7], this problem will not be necessarily solved even if we take several differential 1-forms for which the common set of zeroes G has dimension equal to $\dim(\overline{J(\mathbb{Q})}^p)$: in fact, it could happen that $(G : \overline{J(\mathbb{Q})}^p) > 1$.

- While performing Chabauty, at one point, there is the need to know a bit about the Mordell-Weil group $J(\mathbb{Q})$ for which a set of generators modulo torsion is quite tough to compute. Actually, for high genus g, one could expect that r would be high too and one may have a hard time trying to compute this rank. Even if there are methods (based on generalisation of the infinite descent) or conjecture (BSD-conjecture) that try to achieve this computation, we are not certain about the success of such research. Another idea would be to compute generators, but this would ask to have information bounding r, and finding generators is still a challenging computational problem. However, it appears in practice that we don't need to have a full knowledge of $J(\mathbb{Q})$ to perform Chabauty (see [MP12, Sections 6 & 8] and [Spe20, Section 5])

- Even if we can bound $\#(C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p)$ from above, it may happen that $\#C(\mathbb{Q})$ is (significantly) smaller that this bound. In this case, even if we have found all the points in $C(\mathbb{Q})$, we don't have any information ensuring it. With good intuition, it is possible to conjecture that we have found all the points, but without an sharp-enough bound, we can't conclude. However, there exists methods to try to reduce such a gap.

1.3.2 Some alternatives

- The method previously presented intrinsically relies on the choice of a prime p. It may happen that no prime number chosen, after several attempts, will help to make the search effective. Nonetheless for each prime, even the ones of bad reduction, we could gather 'interesting' information and use parts of this to conclude. This is called the *Mordell-Weil sieve* and has been first introduced by Victor Scharaschkin [Sch98] (even if the term 'Mordell-Weil sieve' doesn't appear clearly in this preprint, the actual method is equivalent to the one exposed on this paper). We refer to the Appendix to read more about this technique.

- In the case of $g = 2$, Eugene Victor Flynn describes a method not requiring the full knowledge of $J(\mathbb{Q})$ and which remedies the third problem mentioned earlier. The idea is to find functions on $J(\mathbb{Q}_p)$ vanishing on $C(\mathbb{Q}_p)$ and to restrict them to $\overline{J(\mathbb{Q})}^p$ in order to pursue in performing Chabauty-like computations. (see [Fly97])

1.3.3 More about Chabauty

To read more about Chabauty's method, one may refer to the two next following well-known standard references on the subject. The first is an article of William McCallum ([McC94]) which is mainly focused to the application to the case of Fermat curves. The second is the PhD thesis of Joseph Loebach Wetherell ([Wet97]) in which the author tackled a case in which Chabauty-Coleman method is not applicable, using a descent and performing Chabauty on finite étale covers on the curve. This effective method has been used, for instance, to prove that arbitrary odd degree hyperelliptic curves of bounded height and of high genus are likely to have only one rational point (see [PS14])

2 A geometric approach

2.1 Preliminary context

As seen earlier, the method of Chabauty and, especially, the effective version by Coleman provides a more concrete approach to finding rational points on curves, rather than Faltings' general result. Even if the Chabauty condition $r < g$ is enough for the study of many curves, some interesting cases (e.g. modular curves) do not satisfy this condition in general. One may think about the so-called *cursed curve* $X_{\text{split}}(13)$ for which $g = 3$ and $r \geq 3$.

Remark. This curve was known to have 7 $\mathbb{Q}$-rational points since 2002, thanks to Steven Galbraith and Burcu Baran. Nonetheless, none of the methods used trying to prove that there were no more points succeeded at this task, until 2017. The gap between the simplicity of the explicit description of this curve and the complexity of bounding its number of rational points justify the naming 'cursed curve'[13].

In order to cover more generally the hypotheses of Mordell's conjecture, the Chabauty condition $r < g$ has to be avoided, or at least relaxed: this is the aim of what is called *Kim's program*. Even if a general theory is not yet developed, some improvement on this condition will bring enough work with them to keep many mathematicians busy. In 2005 ([Kim05]) and 2009 ([Kim09]), Minhyong Kim published two papers aiming to give a first approach to relaxing the Chabauty condition. The main idea is to work on 'big' quotients of the fundamental group of the curve. In fact, as explained in [Cor20], we can notice that, with the same notation as in the previous part, the fundamental group of J is the abelianisation of this of C. From this point, Kim described a *descending central series filtration* on $\pi_1(C)$ defined as follows:

$$\pi_1(C)^{(0)} := \pi_1(C)$$
$$\pi_1(C)^{(n)} := [\pi_1(C)^{(n-1)}, \pi_1(C)] \ \forall n \geq 1$$

where the notation $[-,-]$ refers to the commutator. Taking quotient of $\pi_1(C)$ by any term (of positive index) of this filtration will give rise to a quotient group which is in principal bigger than $\pi_1(C)^{\text{ab}}$ and so no more abelian. Let us denote each of these quotients by $\pi_1(C)_n := \pi_1(C)/\pi_1(C)^n$ $(n \geq 1)$. The goal of Kim's program is to find, for each $n \geq 1$, a variety J_n in which C embeds and for which, the map induced by this embedding on fundamental groups is isomorphic to the quotient map $\pi_1(C) \twoheadrightarrow \pi_1(C)_n$. We already know that J, the jacobian of C, will do for the case $n = 1$: we therefore often refer to this case as *linear Chabauty* (or since $\pi_1(J)$ is an abelian group, we also refer to it as *abelian Chabauty*). For general n, it is still an open problem to find such a variety J_n. Nonetheless, the first non-abelian case, when $n = 2$, has been treated and solved in a way during the last decade. We refer to this case as *quadratic Chabauty*. As expected, it has been shown that in such a context, the Chabauty condition can be relaxed to $r < g + \rho - 1$ where ρ, called the *Picard number* of the curve C, is the $\mathbb{Z}$-rank of the Neron-Severi group of the jacobian variety J.

In 2017, as mentioned earlier, Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman and Jan Vonk submitted on arXiv a paper about 'cracking' the cursed curve using quadratic Chabauty method (see [BDM$^+$19] for the published version). Using preliminary works on p-adic heights by J. S. Balakrishnan and N. Dogra ([BD18], [BD17] for more details) and working with p-adic Hodge theory, they have been able to remedy the lack of the variety J_2 by rewriting Chabauty's only in terms of C and $\pi_1(C)$. This led them to consider an alternative quotient of $\pi_1(C)$, stuck between $\pi_1(C)_1$ and $\pi_1(C)_2$. Their technical approach has been proved successful and was promising for the future of quadratic Chabauty. However, this approach forgets about the geometric nature of the curve, only to rely on some p-adic techniques. From 2017 to 2019, B. Edixhoven and G. Lido have been working on a paper aiming to rewrite quadratic Chabauty in terms of standard algebraic geometry (considering regular models over $\mathbb{Z}$ and working with geometric line bundles over J). They have been able to find a potential candidate for J_2 from their geometric description (see section 3). This approach has been later adapted to the linear case of Chabauty by Pim Spelier

[13] it appears that some mathematical joke was also hidden in this name... somehow related with the curses carried by the number 13.

in his Msc thesis [Spe20]. The following section will focus on gently introducing this translation of linear chabauty to what is called *geometric Chabauty*.

As expected by the naming 'geometric', we are going to work with curves as schemes. We will therefore start this new section by describing most of the tools of last section in terms of scheme theory. After this, it will be explained in which way one can perform Chabauty's method with this new setup (the main philosophy stays the same, though the way of doing it strongly varies from Coleman's approach). Although the following is going to be explained in some standard algebraic geometry, it is expected that the reader is familiar with basic theory of schemes.

2.2 From Coleman to geometric Chabauty

Let $C/\mathbb{Q}$ be a curve, that is $C \to \mathrm{Spec}(\mathbb{Q})$ is an integral scheme of finite type over $\mathbb{Q}$, separated and of dimension 1. We will assume this curve to be 'nice', meaning as before that it is actually proper, smooth and geometrically connected. Let us denote its genus by g and let us choose an odd prime $p \leftrightarrow \mathfrak{p} \in \mathrm{Spec}(\mathbb{Z})$ of good reduction.

Remark. It is not necessary to actually take p odd. However, some of the results that will be stated may require some thorough adjustments in the case $p = 2$. Since this paper aims to guide into the Chabauty's world of the study of curves, we will choose to only consider the most favorable cases.

There exists a proper smooth model $\mathcal{C}/\mathbb{Z}_\mathfrak{p}$ of C (which is a variety of relative dimension 1) and one has the first following result:

Proposition 2.1.

$$C(\mathbb{Q}) = \mathcal{C}(\mathbb{Q}) = \mathcal{C}(\mathbb{Z}_\mathfrak{p})$$

Proof. The first equality trivially follows from the universal property of base change over $\mathrm{Spec}(\mathbb{Z}_\mathfrak{p})$ (Since $C = \mathcal{C} \times_{\mathrm{Spec}(\mathbb{Z}_\mathfrak{p})} \mathrm{Spec}(\mathbb{Q})$). For the second one, we remark that, by definition, $\mathcal{C} \to \mathrm{Spec}(\mathbb{Z}_\mathfrak{p})$ is proper, and $\mathrm{Frac}(\mathbb{Z}_\mathfrak{p}) = \mathbb{Q}$. So, if σ is a $\mathbb{Z}_\mathfrak{p}$-point on $\mathcal{C}$, pre-composing (uniquely) by $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z}_\mathfrak{p})$ (given by the inclusion $\mathbb{Z}_\mathfrak{p} \hookrightarrow \mathbb{Q}$), we get an unique $\mathbb{Q}$-point on $\mathcal{C}$ associated to σ. Conversely, given $\tau \in \mathcal{C}(\mathbb{Q})$, we get the following commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{Q}) & \xrightarrow{\tau} & \mathcal{C} \\ \downarrow & \nearrow & \downarrow \\ \mathrm{Spec}(\mathbb{Z}_\mathfrak{p}) & \longrightarrow & \mathrm{Spec}(\mathbb{Z}_\mathfrak{p}) \end{array}$$

for which a valuative criterion of properness (see [Har77, Chapter 2, Theorem 4.7]) provides a unique dashed map, that is a unique $\mathbb{Z}_\mathfrak{p}$-point on $\mathcal{C}$ associated to τ. This two constructions are obviously inverse of each others and, therefore,

$$\mathcal{C}(\mathbb{Q}) = \mathcal{C}(\mathbb{Z}_\mathfrak{p})$$

□

This first result gives us the possibility of studying the $\mathbb{Q}$-rational points on C by studying the $\mathbb{Z}_\mathfrak{p}$-rational points of its model $\mathcal{C}$. The extension of the geometry to such a smaller ring will therefore let us work with models instead of the curve itself. To keep going on the track of Chabauty's method, we need to define the *relative jacobian* $\mathcal{J}$ of $\mathcal{C}$ over $\mathbb{Z}_\mathfrak{p}$. For this, we define $J/\mathbb{Q}$ and $J^p/\mathbb{F}_p$ the respective jacobian varieties of the respective curves $C/\mathbb{Q}$ and $\mathcal{C}_{\mathbb{F}_p}/\mathbb{F}_p$. One can show that $\mathcal{J}/\mathbb{Z}_\mathfrak{p}$ is a proper smooth scheme of relative dimension g, having J as generic fiber and J^p as special fiber.

Remark. We call $\mathcal{J}$ 'relative jacobian' by duality with the notion of relative Picard scheme. In fact a description of the jacobian variety is to have isomorphic T-points to this of the Picard scheme for all $\mathbb{Z}_\mathfrak{p}$-scheme T. (in our context)

The same result from the proposition applies to $\mathcal{J}$ and so

$$J(\mathbb{Q}) = \mathcal{J}(\mathbb{Q}) = \mathcal{J}(\mathbb{Z}_{\mathfrak{p}})$$

and we denote $r := \mathrm{rank}_{\mathbb{Z}}(J(\mathbb{Q}))$ the Mordell-Weil rank of $J/\mathbb{Q}$. From now on to the end of this section, we will assume that the Chabauty condition holds true: that is $r < g$.

We can embed $\mathcal{C}$ into $\mathcal{J}$ over $\mathbb{Z}_{\mathfrak{p}}$. In fact, suppose that we have a $\mathbb{Q}$-point b on $\mathcal{C}$ and let us define the following Abel-Jacobi map:

$$\begin{array}{rccc} j_b & : & \mathcal{C}(S) & \to & \mathcal{J}(S) \\ & & Q & \mapsto & \mathcal{O}_{\mathcal{C}_S}(Q-b) \end{array}$$

for any $\mathbb{Q}$-scheme S (here we use the description of $\mathcal{J}$ as parametrizing degree 0 line bundles over $\mathcal{C}$ even though explicit description of j_b is not really needed for our purpose). Now, since $\mathbb{Z}_{\mathfrak{p}} \hookrightarrow \mathbb{Z}_p$, we see that we can embed $\mathcal{X}(\mathbb{Z}_{\mathfrak{p}})$ into $\mathcal{X}(\mathbb{Z}_p)$ ($\mathcal{X} = \mathcal{C}$ or $\mathcal{J}$ here). Therefore, this gives rise to the following Chabauty diagram

$$\begin{array}{ccc} \mathcal{C}(\mathbb{Z}_{\mathfrak{p}}) & \xrightarrow{j_b} & \mathcal{J}(\mathbb{Z}_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ \mathcal{C}(\mathbb{Z}_p) & \xrightarrow{j_b} & \mathcal{J}(\mathbb{Z}_p) \end{array}$$

Using the fact that $\mathcal{C}(\mathbb{Z}_{\mathfrak{p}}) = C(\mathbb{Q})$, we see that we could perform Chabauty from this diagram by embedding $\mathcal{C}(\mathbb{Z}_{\mathfrak{p}})$ into the intersection $\mathcal{C}(\mathbb{Z}_p) \cap \overline{\mathcal{J}(\mathbb{Z}_{\mathfrak{p}})}^p \subseteq \mathcal{J}(\mathbb{Z}_p)$. Actually, as in Coleman's approach, we will consider residue discs over $\mathbb{F}_p$-points and then, we will describe the bottom horizontal map and the right vertical on residue discs in order to understand the previous intersection.

Let $\mathcal{X} = \mathcal{C}$ or $\mathcal{J}$. The quotient map

$$\mathbb{Z}_p \xrightarrow{\mathrm{mod}\ p} \mathbb{F}_p$$

induces the following morphism on spectra

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{F}_p) & \to & \mathrm{Spec}(\mathbb{Z}_p) \\ \{0\} & \mapsto & p\mathbb{Z}_p \end{array}$$

where $p\mathbb{Z}_p$ is the closed point of $\mathrm{Spec}(\mathbb{Z}_p)$. Therefore, any $\mathbb{Z}_p$-point $\sigma : \mathrm{Spec}(\mathbb{Z}_p) \to \mathcal{X}$ can be mapped to its *reduction modulo p* pre-composing it with this last morphism. It gives us a well-defined morphism

$$\begin{array}{rccc} \mathrm{mod}_p & : & \mathcal{X}(\mathbb{Z}_p) & \to & \mathcal{X}(\mathbb{F}_p) \\ & & \sigma & \mapsto & (\tilde{\sigma} : \{0\} \mapsto \sigma(p\mathbb{Z}_p)) \end{array}$$

In terms of morphisms on the proper smooth model $\mathcal{X}/\mathbb{Z}_{\mathfrak{p}}$ of $\mathcal{X}_{\mathbb{Q}}$, it means that any closed points on the generic fiber specialises a closed point on the special fiber. But by smoothness over $\mathbb{F}_p$ coming from good reduction at p, specialising closed points on the special fiber is actually surjective. Therefore, our mod_p map is surjective and as earlier, for $Q \in \mathcal{X}(\mathbb{F}_p)$ we denote by $\mathcal{X}(\mathbb{Z}_p)_Q$ the set of $\mathbb{Z}_p$-points on $\mathcal{X}$ reducing to Q via the mod_p map.

Now, let $P \in \mathcal{C}(\mathbb{F}_p)$ and let $\tilde{P} \in \mathcal{C}(\mathbb{Z}_p)_P$. By commutativity, denoting again by b the reduction modulo p of b, $j_b(\tilde{P}) \in \mathcal{J}(\mathbb{Z}_p)_t$ where $t := j_b(P)$. Therefore, we get the new following commutative diagram which will be our basis for performing geometric Chabauty

$$\begin{array}{ccc} \mathcal{C}(\mathbb{Z}_{\mathfrak{p}})_P & \xrightarrow{j_b} & \mathcal{J}(\mathbb{Z}_{\mathfrak{p}})_t \\ \downarrow & & \downarrow \\ \mathcal{C}(\mathbb{Z}_p)_P & \xrightarrow{j_b} & \mathcal{J}(\mathbb{Z}_p)_t \end{array}$$

Since there are only finitely many $\mathbb{F}_p$-points on $\mathcal{C}$, it is indeed sufficient to bound $\#\mathcal{C}(\mathbb{Z}_{\mathfrak{p}})_P$ for all $P \in \mathcal{C}(\mathbb{F}_p)$ to conclude. For this, as mentionned earlier, we are going to bound the cardinality of $\mathcal{C}(\mathbb{Z}_p)_P \cap \overline{\mathcal{J}(\mathbb{Z}_{\mathfrak{p}})_t}^p \subseteq \mathcal{J}(\mathbb{Z}_p)_t$ from above. To effectively prove the finiteness of this intersection,

we need to understand how both $\mathcal{C}(\mathbb{Z}_p)_P$ and $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$ embed into $\mathcal{J}(\mathbb{Z}_p)_t$ and how to characterise the formal p-adic closure of $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$ inside $\mathcal{J}(\mathbb{Z}_p)_t$ (seen as a formal p-adic Lie group). The conclusion will differ from Coleman's approach in the sense that, instead of describing antiderivative of regular 1-forms on J to be restricted to C, we will define p-adically convergent formal power series on $\mathcal{C}(\mathbb{Z}_p)_P$, seen as embedded into $\mathcal{J}(\mathbb{Z}_p)_t$, to pull them back to $\overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t}^p$. The next following subsections will be devoted to explaining the geometric machinery behind the theory.

2.3 Description of $\mathbb{Z}_p$-points on smooth models

Let $\mathcal{X}/\mathbb{Z}_p$ be $\mathcal{C}/\mathbb{Z}_p$ or $\mathcal{J}/\mathbb{Z}_p$, which is a smooth $\mathbb{Z}_p$-scheme of relative dimension say d ($d = 1$ for $\mathcal{X} = \mathcal{C}$; $d = g$ for $\mathcal{X} = \mathcal{J}$). Let $x \in \mathcal{X}(\mathbb{F}_p)$: we want to describe $\mathcal{X}(\mathbb{Z}_p)_x$.

Since smoothness is a local property, one may assume that $\mathcal{X} = \mathrm{Spec}(A)$ where A is a regular $\mathbb{Z}_p$-algebra of dimension d (we assume our models to be smooth, e.g. Néron models). By smoothness at x, there exists d elements $t_1, \dots, t_d \in A$ such that $p, t_1, \dots, t_d$ generate the maximal ideal $\mathfrak{m}_x$ of $\mathcal{O}_{\mathcal{X},x}$. These elements are called *uniformisers* or *local parameters* at x; meaning that there exists an open affine neighborhood $U = \mathrm{Spec}(B) \subseteq \mathcal{X}$ of x such that $k(x)/\mathbb{F}_p$ is separable algebraic and the natural map

$$\begin{array}{rccc} \tau & : & \mathbb{Z}_p[T_1, \dots, T_d] & \to & B \\ & & T_i & \mapsto & t_i \end{array}$$

is flat and sends $(p, T_1, \dots, T_d)$ to $\mathfrak{m}_x$ (indeed, $\mathcal{O}_{\mathcal{X},x} = \mathcal{O}_{U,x}$). Again, since our study is local, we can suppose that $U = \mathcal{X}$ and that the induced map

$$t := \mathrm{Spec}(\tau) : \mathcal{X} \to \mathrm{Spec}(\mathbb{Z}_p[T_1, \dots, T_d])$$

is étale and the fiber of the origin over $\mathbb{F}_p$ by t consists only on x. Let us consider the blow-up $\widetilde{\mathcal{X}}_x$ of $\mathcal{X} = \mathrm{Spec}(A)$ along $\{x\} = \mathrm{Spec}(A/\mathfrak{m}_x)$. Then, following [Liu02, Chapter 8, Lemma 1.4], one has

$$\widetilde{\mathcal{X}}_x = \bigcup_{a \in \{p, t_1, \dots, t_d\}} \mathrm{Spec}(A\,[\mathfrak{m}_x/a])$$

and we denote by $\widetilde{\mathcal{X}}_x^p$ the open affine part of $\widetilde{\mathcal{X}}_x$ on which all the t_i's are multiple of p, that is $\widetilde{\mathcal{X}}_x^p = \mathrm{Spec}(A[\widetilde{t_1}, \dots, \widetilde{t_d}])$ where $\widetilde{t_i} = t_i/p$ for all i. In order to work with this blow-up, we need to describe the map $\pi : \widetilde{\mathcal{X}}_x^p \to \mathcal{X}$. For this, we use our assumptions on t: in fact, since t is étale with $t^{-1}(\{0_{\mathbb{F}_p}\}) = \{x\}$, $\widetilde{\mathcal{X}}_x \to \mathcal{X}$ corresponds to the pullback by t of $\widetilde{\mathbb{A}^d_{\mathbb{Z}_p 0_{\mathbb{F}_p}}} \to \mathbb{A}^d_{\mathbb{Z}_p}$ along the ideal of $\mathbb{A}^d_{\mathbb{Z}_p}$ defining the origin $0_{\mathbb{F}_p}$ (which is $(p, T_1, \dots, T_d)$). Therefore, $\pi : \widetilde{\mathcal{X}}_x^p \to \mathcal{X}$ corresponds to the pullback of the corresponding p-part $\widetilde{\mathbb{A}^d_{\mathbb{Z}_p 0_{\mathbb{F}_p}}}^p \to \mathbb{A}^d_{\mathbb{Z}_p}$ given by

$$\mathbb{Z}_p[T_1, \dots, T_d] \to \mathbb{Z}_p[\widetilde{T_1}, \dots, \widetilde{T_d}], T_i \mapsto p\widetilde{T_i}$$

Whence, one has that $\pi : \widetilde{\mathcal{X}}_x^p \to \mathcal{X}$ is given by

$$A \hookrightarrow A[\widetilde{t_1}, \dots, \widetilde{t_d}]$$

since the local parameters t_i's belong to A. Therefore, via the following result, we will show that this p-part corresponds to the point on $\mathcal{X}$ reducing to x via mod_p:

Lemma 2.1. *The map*

$$\widetilde{\mathcal{X}}_x^p(\mathbb{Z}_p) \to \mathcal{X}(\mathbb{Z}_p)$$

induced a natural bijection between $\widetilde{\mathcal{X}}_x^p(\mathbb{Z}_p)$ *and* $\mathcal{X}(\mathbb{Z}_p)_x$.

Proof. Let $\sigma \in \mathcal{X}(\mathbb{Z}_p)_x$, that is σ is a morphism of affine schemes $\mathrm{Spec}(\mathbb{Z}_p) \to \mathrm{Spec}(A)$ with $\sigma(p\mathbb{Z}_p) = \mathfrak{m}_x$ by definition of residue discs. Let $\phi := \sigma^\#(\mathrm{Spec}(A)) : A \to \mathbb{Z}_p$. According to the definition of ϕ, ($\sigma = \mathrm{Spec}(\phi)$) $\phi^{-1}(p\mathbb{Z}_p) = \mathfrak{m}_x$ and for all $a \in A \setminus \mathfrak{m}_x$, $\phi(a) \in \mathbb{Z}_p^\times$. Therefore, ϕ *uniquely* factors (by the universal property of localisation) through $A \to A_{\mathfrak{m}_x} \to \mathbb{Z}_p$, meaning that σ factors uniquely

$$\sigma : \mathrm{Spec}(\mathbb{Z}_p) \xrightarrow{\exists! \tau} \mathrm{Spec}(A_{\mathfrak{m}_x}) \to \mathrm{Spec}(A)$$

where the last map is the canonical map induced by the localisation $A \to A_{\mathfrak{m}_x}$. Hence, to σ corresponds bijectively a $\tau \in \mathrm{Spec}(A_{\mathfrak{m}_x})(\mathbb{Z}_p)$, which itself corresponds bijectively to a morphism of local ring $\psi \in \mathrm{Hom}_{\mathrm{local}}(A_{\mathfrak{m}_x}, \mathbb{Z}_p)$. By the local property of ψ, since $\mathfrak{m}_x = (p, t_1, \dots, t_d)$, we have that for all $j = 1, \dots, d$, $p \mid \psi(t_j)$. Therefore, ψ extends uniquely to a morphism $\widetilde{\psi}\colon A[\widetilde{t_1}, \dots, \widetilde{t_d}] \to \mathbb{Z}_p$. Following all the bijection, we get that to any $\sigma \in \mathcal{X}(\mathbb{Z}_p)_x$ corresponds an unique $\widetilde{\psi} \in \widetilde{\mathcal{X}}^p_x(\mathbb{Z}_p)$. □

This result gives a characterisation of the residue disc above x, via the description of the blow-up of $\mathcal{X}$ at x. Now, using the theory of formal p-adic completion on $\mathcal{O}_{\widetilde{\mathcal{X}}^p_x}(\widetilde{\mathcal{X}}^p_x) = \mathcal{O}_{\mathcal{X}}(\mathcal{X})[\widetilde{t_1}, \dots, \widetilde{t_d}]$, we are going to show that this residue disc can be made in bijection with the free product of d copies of $p\mathbb{Z}_p$.

Lemma 2.2.

$$\widetilde{\mathcal{X}}^p_x(\mathbb{Z}_p) \simeq \mathbb{Z}_p^d$$

Proof. By extending t to a map of p-parts of blow-ups, also called $t\colon \widetilde{\mathcal{X}}^p_x \to \widetilde{\mathbb{A}^d_{\mathbb{Z}_p 0_{\mathbb{F}_p}}}^p$, we still have t being of finite presentation and étale. Therefore, according to [Gro67, Chapter IV, Proposition 17.6.3], the p-adic formal completions of $\mathcal{O}_{\widetilde{\mathcal{X}}^p_x}(\widetilde{\mathcal{X}}^p_x)$ and $\mathcal{O}_{\widetilde{\mathbb{A}^d_{\mathbb{Z}_p 0_{\mathbb{F}_p}}}^p}(\widetilde{\mathbb{A}^d_{\mathbb{Z}_p 0_{\mathbb{F}_p}}}^p) = \mathbb{Z}_p[\widetilde{T_1}, \dots, \widetilde{T_d}]$ are naturally in bijection. It consequently implies that

$$\mathcal{O}_{\widetilde{\mathcal{X}}^p_x}(\widetilde{\mathcal{X}}^p_x)^{\wedge p} \cong \mathbb{Z}_p\left\langle \widetilde{t_1}, \dots, \widetilde{t_d} \right\rangle$$

where the latter is the ring of convergent power series and $(-)^{\wedge p}$ refers to formal p-adic completion. Now, the universal property of the completion implies that this extension of f induces a bijection

$$\mathrm{Hom}(\mathcal{O}_{\widetilde{\mathcal{X}}^p_x}(\widetilde{\mathcal{X}}^p_x), \mathbb{Z}_p) \xrightarrow{\sim} \mathrm{Hom}(\mathbb{Z}_p\left\langle \widetilde{t_1}, \dots, \widetilde{t_d} \right\rangle, \mathbb{Z}_p)$$

(since $\mathbb{Z}_p$ is complete for the p-adic topology) where the right-hand side is naturally in bijection with $\mathbb{Z}_p^d$ by choosing images of the variables. Finally, by identifying the first Hom-set with the $\mathbb{Z}_p$-points on $\widetilde{\mathcal{X}}^p_x$ we get the desired bijection. □

Whence, using the natural bijection of Lemma 2.1 given by multiplication by p on local rings, we see that evaluation by t gives a bijection

$$t(\mathcal{X}(\mathbb{Z}_p)_x) \simeq (p\mathbb{Z}_p)^d$$

which can be seen as the geometric twin of Proposition 1.2. The preceeding construction is actually functorial in $\mathcal{X}$, and so we will be able to map $\mathcal{C}(\mathbb{Z}_p)_P$ to $\mathcal{J}(\mathbb{Z}_p)_t$ by mapping the p-parts of their respective blow-ups in the following way:

The map $j_b\colon \mathcal{C} \to \mathcal{J}$ is a morphism of smooth $\mathbb{Z}_p$-schemes satisfying $j_b(P) = t$. The inverse image along j_b of the ideal sheaf defining t, is the ideal sheaf defining P, and so, since the inverse image of this ideal along $\widetilde{\mathcal{C}}^p_P \to \mathcal{C}$ is the ideal generated by the prime p, we have that

$$\widetilde{\mathcal{C}}^p_P \to \mathcal{C} \to \mathcal{J}$$

factors uniquely through $\widetilde{\mathcal{J}}_t \to \mathcal{J}$ and the image of $\widetilde{\mathcal{C}}^p_P$ lies in $\widetilde{\mathcal{J}}^p_t$. Therefore, there exists a unique morphism $\widetilde{j_b}$ making the following diagram commutes

$$\begin{array}{ccccc}
\widetilde{\mathcal{C}}^p_P & \hookrightarrow & \widetilde{\mathcal{C}}_P & \longrightarrow & \mathcal{C} \\
\downarrow{\scriptstyle \widetilde{j_b}} & & \downarrow{\scriptstyle \widetilde{j_b}} & & \downarrow{\scriptstyle j_b} \\
\widetilde{\mathcal{J}}^p_t & \hookrightarrow & \widetilde{\mathcal{J}}_t & \longrightarrow & \mathcal{J}
\end{array}$$

On $\mathbb{Z}_p$-points, we can therefore combine all the previous results to get the commutative diagram

$$\begin{array}{ccccccc}
\mathbb{Z}_p & \xrightarrow{\simeq} & \widetilde{\mathcal{C}}^p_P(\mathbb{Z}_p) & \xrightarrow{\simeq} & \mathcal{C}(\mathbb{Z}_p)_P & \xrightarrow{\mathrm{mod}_p} & \mathcal{C}(\mathbb{F}_p) \ni P \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}_p^g & \xrightarrow{\simeq} & \widetilde{\mathcal{J}}^p_t(\mathbb{Z}_p) & \xrightarrow{\simeq} & \mathcal{J}(\mathbb{Z}_p)_t & \xrightarrow{\mathrm{mod}_p} & \mathcal{J}(\mathbb{F}_p) \ni t
\end{array}$$

By the functoriality described earlier, we have that the ideal defining the image of $\widetilde{\mathcal{C}}_P^p$ via $\widetilde{j_b}$ inside $\widetilde{\mathcal{J}}_t^p$ is generated by $g-1$ (for dimension reason) regular functions, say $f_1,\dots,f_{g-1} \in \mathcal{O}_{\widetilde{\mathcal{J}}_t^p}(\widetilde{\mathcal{J}}_t^p) \simeq \mathcal{O}_{\mathcal{J}}(\mathcal{J})[s_1/p,\dots,s_g/p]$ (where $p, s_1,\dots,s_g$ generate the maximal ideal of t in $\mathcal{O}_{\mathcal{J},t}$). We may choose those elements in such a way that the left vertical map maps $\mathbb{Z}_p$ to the last coordinate of $\mathbb{Z}_p^g$; they define the other uniformisers at t (the first one being the image of the uniformiser at P via $\widetilde{j_b}$). Therefore, via the isomorphism mentioned in the proof of Lemma 2.2, we have that there are p-adically convergent power series $f_1,\dots,f_{g-1} \in \mathbb{Z}_p[[s_1/p,\dots,s_g/p]]$, linear modulo p since our isomorphisms are all $\mathbb{Z}_p$-linear, and such that

$$\mathcal{C}(\mathbb{Z}_p)_P \simeq V(f_1,\dots,f_{g-1}) \subseteq \mathcal{J}(\mathbb{Z}_p)_t$$

As mentioned earlier, the idea now is to describe the map $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$ to $\mathcal{J}(\mathbb{Z}_p)_t$ along which we are going to pullback the defining power series f_i's of $\mathcal{C}(\mathbb{Z}_p)_P$ to $\overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})}_t^p$. We will show that the Zariski closure of these pullbacks surjects on the intersection $\mathcal{C}(\mathbb{Z}_p)_P \cap \overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})}_t^p$. Therefore, and this is going to be our final result, if we are able to bound the cardinality of this ideal from above, then the intersection will be finite, and so will be $\#C(\mathbb{Q})$.

From before, we already know that $\mathcal{J}(\mathbb{Z}_p)_t \simeq \mathbb{Z}_p^g$ by evaluating at parameters and then dividing out by p. But what about $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$? From the Mordell-Weil theorem, we have that

$$\mathcal{J}(\mathbb{Z}_\mathfrak{p}) = J(\mathbb{Q}) \simeq \mathbb{Z}^r \times T$$

where r is the Mordell-Weil rank of $J/\mathbb{Q}$, and T is a finite torsion group. By reduction modulo p, we can map $\mathcal{J}(\mathbb{Z}_\mathfrak{p})$ to $\mathcal{J}(\mathbb{F}_p)$. The behaviour of T through this mapping is interesting as shown by the following:

Proposition 2.2. *If P is a torsion point of $\mathcal{J}(\mathbb{Z}_\mathfrak{p})$ with trivial reduction modulo p, then P is the neutral element.*

Proof. Since we have taken p to be odd, by a direct application of [Par00, Proposition 2.4] (with $l = r = p$), we get that any torsion point of $\mathcal{J}(\mathbb{Z}_\mathfrak{p})$ reducing to the trivial section in $\mathcal{J}(\mathbb{F}_p)$ as order 1. However, the only torsion element of order 1 is the unit section of $\mathcal{J}(\mathbb{Z}_\mathfrak{p})$. □

This proposition tells us that T injects into $\mathcal{J}(\mathbb{F}_p)$ and therefore, looking at the residue class over 0, we see that $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_0 \simeq \mathbb{Z}^r$. Furthermore, since we can map bijectively (but non canonically) $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$ to $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_0$ by translation via a lift of t, we conclude that

$$\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t \simeq \mathbb{Z}^r$$

The inclusion map studied results to be of the form $\kappa_t : \mathbb{Z}^r \to \mathbb{Z}_p^g$ and has some interesting properties. Before stating them, we will develop a little bit on the formal group on $\mathcal{J}$ from its group scheme structure. We will avoid the general theory by adapting P. Spelier results ([Spe20, Subsection 3.1]) directly to our special case.

2.4 Formal group on the jacobian

We recall that $\mathcal{J}$ is a smooth $\mathbb{Z}_p$-group scheme of relative dimension g. Let $e \in \mathcal{J}(\mathbb{Z}_p)$ be the unit section and let's denote by $\mathfrak{m}$ the defining ideal of e in $\mathcal{O}_{\mathcal{J},e}$. By smoothness and dimension, there are g parameters at e, $x_1,\dots,x_g \in \mathcal{O}_{\mathcal{J}}(\mathcal{J})$, generating (together with p) $\mathfrak{m}$ and one can show that the formal $\mathfrak{m}$-adic completion of $\mathcal{O}_{\mathcal{J},e}$ is topologically isomorphic to the ring of power series $\mathbb{Z}_p[[x_1,\dots,x_g]]$. It will be denoted $\widehat{\mathcal{O}}_{\mathcal{J},e}$.

Definition 2.1. *We define the* formal scheme associated to *the triplet $(\mathcal{J}, \mathbb{Z}_p, e)$ to be the scheme*

$$\mathrm{Spf}(\widehat{\mathcal{O}}_{\mathcal{J},e}) := \left(\mathrm{Spec}(\widehat{\mathcal{O}}_{\mathcal{J},e}/\mathfrak{m}), \lim_n(\mathcal{O}_{\mathrm{Spec}(\widehat{\mathcal{O}}_{\mathcal{J},e}/\mathfrak{m}^n)})\right) = \left(\mathrm{Spec}(\mathbb{Z}_p), \lim_n(\mathcal{O}_{\mathrm{Spec}(\mathcal{O}_{\mathcal{J},e}/\mathfrak{m}^n)})\right)$$

Remark. 1. This definition is actually the definition of the formal scheme of the $\mathfrak{m}$-adically complete $\mathbb{Z}_p$-algebra $\widehat{\mathcal{O}}_{\mathcal{J},e}$.

2. For any $\mathbb{Z}_p$-algebra A of finite length, one has

$$\mathrm{Spf}(\widehat{\mathcal{O}}_{\mathcal{J},e})(A) \simeq \widetilde{\mathrm{Hom}}(\widehat{\mathcal{O}}_{\mathcal{J},e}, A)$$

where the last set corresponds to continuous homomorphisms of $\mathbb{Z}_p$-algebra. Actually, $\mathrm{Spf}(\widehat{\mathcal{O}}_{\mathcal{J},e})$ can be seen as a functor from the category of $\mathbb{Z}_p$-algebras of finite length to the category of sets.

3. $\mathcal{O}_{\mathrm{Spf}(\widehat{\mathcal{O}}_{\mathcal{J},e})}(\mathrm{Spf}(\widehat{\mathcal{O}}_{\mathcal{J},e})) = \varprojlim_n (\mathcal{O}_{\mathrm{Spec}(\mathcal{O}_{\mathcal{J},e}/\mathfrak{m}^n)}(\mathrm{Spec}(\mathbb{Z}_p)) \simeq \varprojlim_n (\mathcal{O}_{\mathcal{J},e}/\mathfrak{m}^n) = \widehat{\mathcal{O}}_{\mathcal{J},e}$

Since $\mathcal{J}$ is actually a group scheme, for all finite length $\mathbb{Z}_p$-algebra A, $\widetilde{\mathrm{Hom}}(\widehat{\mathcal{O}}_{\mathcal{J},e}, A)$ carries a group structure. By functoriality in A, this group structure can be described by a coproduct

$$\delta : \widehat{\mathcal{O}}_{\mathcal{J},e} \to \widehat{\mathcal{O}}_{\mathcal{J},e} \widehat{\otimes}_{\mathbb{Z}_p} \widehat{\mathcal{O}}_{\mathcal{J},e}$$

We get a commutative diagram

$$\begin{array}{ccc} \widehat{\mathcal{O}}_{\mathcal{J},e} & \xrightarrow{\quad\delta\quad} & \widehat{\mathcal{O}}_{\mathcal{J},e} \widehat{\otimes}_{\mathbb{Z}_p} \widehat{\mathcal{O}}_{\mathcal{J},e} \\ \wr\downarrow & & \wr\downarrow \\ \mathbb{Z}_p[[x_1, \dots, x_g]] & \xrightarrow{\delta'} & \mathbb{Z}_p[[y_1, \dots, y_g, z_1, \dots, z_g]] \end{array}$$

and for all $i = 1, \dots, g$, we define $F_i := \delta'(x_i) \in \mathbb{Z}_p[[\underline{y}, \underline{z}]]$. By commutativity, and thanks to the vertical isomorphisms (fixed but not canonical), we have that $\mathcal{F} := (F_1, \dots, F_g)$ is a g-dimensional formal group scheme on $\mathcal{J}$. Actually, via the bijection between $\mathcal{J}(\mathbb{Z}_p)_0$ and $(p\mathbb{Z}_p)^g$, $\mathcal{F}$ corresponds to the multiplication on $\mathcal{J}(\mathbb{Z}_p)_0$ coming from the group scheme structure on $\mathcal{J}$. Therefore, to $\mathcal{F}$ corresponds a logarithm $\log \in \mathbb{Q}_p[[\underline{x}]]^g$ and we define $\log_p(\underline{x}) := \log(p\underline{x})/p$. We state without proof the following lemma (the same lemma with an actual proof can be found in [Spe20, Lemma 3.7]):

Lemma 2.3. *1. $\log_p(\underline{x})$ is a g-tuple of convergent power series and it therefore defines a map from $\mathbb{Z}_p^g$ to itself.*

2. From the consecutive bijections $\mathcal{J}(\mathbb{Z}_p)_0 \to (p\mathbb{Z}_p)^g \xrightarrow{1/p} \mathbb{Z}_p^g$, we denote by $+_{\mathcal{J}}$ the group structure endowed by $\mathbb{Z}_p^g$. Then $\log_p$ is actually a group morphism from $(\mathbb{Z}_p^g, +_{\mathcal{J}})$ to $(\mathbb{Z}_p^g, +)$.

3. If $p > 2$, then $\log_p$ is a bijection of inverse $\exp_p$ which is also a g-tuple of convergent power series with constant term 0 (such as $\log_p$).

4. For $m \in \mathbb{Z}_{>0}$ and $p > m + 1$, $\log_p$ and $\exp_p$ are of degree at most m modulo p^m.

This lemma will let us understand the behaviour of the map κ_t seen before. In fact, we will use all these properties about the formal group scheme on $\mathcal{J}$ to prove the following theorem:

Theorem 2.1. *There are uniquely determined convergent power series $\kappa_1, \dots, \kappa_g \in \mathbb{Z}_p[[z_1, \dots, z_r]]$ such that for all $\underline{z} \in \mathbb{Z}^r$, $\kappa_t(\underline{z}) = (\kappa_1(\underline{z}), \dots, \kappa_g(\underline{z}))$ and such that the reduction $\overline{\kappa_i} \in \mathbb{F}_p[z_1, \dots, z_r]$ of κ_i modulo p is linear or constant ($i = 1, \dots, g$). Moreover, for all integer $m > 0$ with $m < p - 1$, all the κ_i's are of degree at most m modulo p^m.*

Proof. Recall that we can pass bijectively from $\mathcal{J}(\mathbb{Z}_p)_0$ to $\mathcal{J}(\mathbb{Z}_p)_t$ by translating by a lift of t. Therefore, we get that $\kappa_t = \kappa_0 +_{\mathcal{J}} t$ where κ_0 is given by the first inclusion $\mathcal{J}(\mathbb{Z}_{\mathfrak{p}})_0 \to \mathcal{J}(\mathbb{Z}_p)_0$. Following bijections and using the previous lemma, we can write

$$\kappa_t = \exp_p(\log_p \circ \kappa_t)$$

were $\log_p \circ \kappa_t : (\mathbb{Z}^g, +) \to (\mathbb{Z}_p^g, +)$ is $\mathbb{Z}$-linear. Therefore, the composition with $\exp_p$, which is given by convergent power series, will be also given by convergent power series. The $\mathbb{Z}$-linearity ensures that reduction of the components of κ_t would have degree at most 1 modulo p. Finally, we conclude that for $m = 2, \dots, p-2$, since $\exp_p$ is of degree at most m modulo p^m, and $\log_p \circ \kappa_t$ is linear, the composite κ_t is at most of degree m modulo p^m too. □

As a consequence of this theorem, we see that we can extend κ_t to a continuous map, for the p-adic topology, $\kappa_t : \mathbb{Z}_p^r \to \mathbb{Z}_p^g$ given by the exact same power series. Since κ_t firstly corresponded to the inclusion of $\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t$ into $\mathcal{J}(\mathbb{Z}_p)_t$, this new map will correspond to the inclusion of the p-adic closure. Whence

$$\kappa_t(\mathbb{Z}_p^r) = \overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t}^p \subseteq \mathcal{J}(\mathbb{Z}_p)_t$$

Combining this last result to the one found earlier, we see that we can describe our so-wanted intersection $\mathcal{C}(\mathbb{Z}_p)_P \cap \overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t}^p$ inside $\mathcal{J}(\mathbb{Z}_p)_t$ as

$$V(f_1, \dots, f_{g-1}) \cap \kappa_t(\mathbb{Z}_p^r) \subseteq \mathbb{Z}_p^g$$

and we therefore state the following main-key theorem of geometric Chabauty (the proof is actually straightforward according to what we have previously done) :

Theorem 2.2 (Theorem 4.1, [Spe20])**.** *Define, for $i = 1, \dots, g-1$*

$$\lambda_i := \kappa_t^* f_i$$

the pullbacks of the defining equations of $\mathcal{C}(\mathbb{Z}_p)_P$ along κ_t. Then, if we denote $V := V(\lambda_1, \dots, \lambda_{g-1}) \subseteq \mathbb{Z}_p^r$ one has that κ_t restricted to V is a surjection onto $\mathcal{C}(\mathbb{Z}_p)_P \cap \overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t}^p$.

Remark. At this point we can actually see the difference with Coleman's approach. Earlier, while describing Coleman's method, we defined convergent power series vanishing on $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}^p$ and we bounded the cardinality of this intersection by bounding the number of zeroes of such power series on residue discs. In the geometric approach, we directly start by working on residue discs and we pullback convergent power series vanishing on the intersection of residue discs to a bigger set for which we aim to bound from above its cardinality.

Since V surjects on $\mathcal{C}(\mathbb{Z}_p)_P \cap \overline{\mathcal{J}(\mathbb{Z}_\mathfrak{p})_t}^p$, containing $\mathcal{C}(\mathbb{Q})_P$, an upper bound for $\#V$ will be an upper bound for $\#\mathcal{C}(\mathbb{Q})_P$. A way to prove it, which was the one selected in [EL21] while firstly describing geometric Chabauty, is the following. We let $I := I(\lambda_1, \dots, \lambda_{g-1}) \subseteq \mathbb{Z}_p \langle \underline{z} \rangle$ and we denote by A the quotient $\mathbb{Z}_p \langle \underline{z} \rangle / I$. One can remark that $V = \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)$ and reducing our calculations modulo p, it is possible to find an upper bound on this Hom-set, providing that A/pA is finite. This result has been stated as follows, according to [Spe20, Proposition 4.2]:

Proposition 2.3. *Denote by $\overline{A} := A/pA$ and assume it to be finite. Then, $\overline{A} = \prod_{\underline{m} \in \mathrm{MaxSpec}(\overline{A})} \overline{A}_{\underline{m}}$ and*

$$\#(\mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)) \leq \sum_{\substack{\underline{m} \in \mathrm{MaxSpec}(\overline{A}) \\ \overline{A}/\underline{m} = \mathbb{F}_p}} \dim_{\mathbb{F}_p} \overline{A}_{\underline{m}}$$

Remark. Actually this theorem relies on the condition that $\overline{A} = \mathbb{F}_p[\underline{z}]/\overline{I}$ is finite. According to a remark of B. Edixhoven during the Arizona Winter School 2020, it is expected to happen for most of the primes provided that $r < g$ and even more, one can expect this to always work if $r < g - 1$ (since we define the zero set of more polynomials than there are variables). Nonetheless, it is not proved that it is always true. Therefore, if while doing computations, one finds out that $\overline{A}$ is not finite, it will be necessary to work with another prime number.

3 Performing Chabauty in higher dimension

As made precised earlier, in the introduction of the previous part, we need to find a variety J_2 in which to embed C and such that $C \hookrightarrow J_2$ induces a quotient map of fundamental group $\pi_1(C) \twoheadrightarrow \pi_1(C)_2$. The p-adic approach used in [BDM+19] bypasses this. The idea of the geometric setting from the last section is to bring back the study of the curve into a concrete context and to find such a variety J_2. For this, B. Edixhoven and G. Lido decided to consider a semi-abelian variety living above the jacobian and having a trivial pullback over C. Doing so, it will be then possible to embed C into this variety which have, a priori, higher relative dimension than the Jacobian itself. However, we would like to keep track of the Mordell-Weil rank r of the Jacobian, to we ensure that we can keep a new Chabauty condition of the form $r < f(g)$ where $f(g) > g$.
A first idea was to consider $\mathbb{G}_m$-extensions of J by group varieties. But, in this context, we will not win any flexibility in dimension (which kills the theory since we want to embed C in an higher dimensional variety than J). In fact, if one can lift the Abel-Jacobi embedding to such an extension, which will be a product of a power of $\mathbb{G}_m$ with J, then the lifting will be the same as the first embedding since any map from C to a power of $\mathbb{G}_m$ is zero. It is therefore necessary to find another variety, which has fundamental group being, at least, a quotient of $\pi_1(C)_2$ surjecting non-trivially onto $\pi_1(C)_1$, and to which we can 'strictly' lift the Abel-Jacobi map; that is a non trivial extension of J by $\mathbb{G}_m$.
The potential candidate considered in [EL21] is a certain pullback T of the *Poincaré torsor* on J (actually, it will be described as a finite product of such pullbacks). We will show that the resulting variety is actually strictly 'bigger' than J (in terms of relative dimension) whenever $\rho := \mathrm{rank}_{\mathbb{Z}}(\mathrm{NS}_{J/\mathbb{Q}}) > 1$. In fact, T will be of relative dimension $g+\rho-1$, and by its defintion, we will have $T = J$ whenever $\rho = 1$, letting us link both linear Chabauty and quadratic Chabauty through the geometric setting. As it will be explained the Poincaré torsor is a $\mathbb{G}_m$-torsor, a line bundle without the zero section, defined naturally from the *Poincaré bundle* whose existence comes from the fact that J is an abelian variety. We already see why the translation to geometry is necessary, since the construction of line bundles and torsors rely on the geometric structure of the varieties considered. As a small warning, we can notice that working with $\mathbb{G}_m$-torsors to compute $\mathbb{Q}$-rational points might cause some $\mathbb{Z}$-rank problems: indeed, we will show that $T(\mathbb{Q})$ will be a $\mathbb{G}_m(\mathbb{Q})^{\rho-1}$-extension of $J(\mathbb{Q})$, meaning that $\mathrm{rank}_{\mathbb{Z}}(T(\mathbb{Q})) = r + \rho - 1 \neq r$ whenever $\rho > 1$. This will motivate the extension of the geometry of the curve to the ring $\mathbb{Z}$ in order to make sure to keep the same rank between J and T. This manoeuvre will ask us to consider a (regular) model of C and (Néron) models of J and $J^\vee$ (*the dual abelian variety* of J) over some extension of $\mathbb{Z}$ in which we will invert all primes of bad reduction. Then, after updating our geometric objects (we will also notice that we will not be able to treat the model of C itself but some dense opens of its smooth subscheme), we will apply the theory as before to perform Chabauty in an higher dimensional context. At some point, it will be mentioned how and in which way to apply the quadratic improvement of geometric Chabauty.

All proofs are going to be omitted but the reader can expect to be redirected to the references needed to understand the general theory. This part is based on the description made by B. Edixhoven and G. Lido in their article [EL21]. The structure will be similar to the one chosen by B. Edixhoven during the lectures at Arizona Winter School 2020 [Edi20] (which has been turned into a cartoon guide by Sachi Hashimoto [Has20])

3.1 The Poincaré torsor

In this subsection, we are going to introduce the main character of the geometric approach, as mentioned in the introductory part, the Poincaré torsor. For this, we are first going to review some bases of arithmetic geometry for which all details can be found in [CS86].

3.1.1 Dual variety and universal line bundle

Let us keep the same notations and context as at the beginning of subsection 2.2. We recall, from a previous remark, that J can be seen as the subgroup scheme $\mathrm{Pic}^0_{C/\mathbb{Q}}$ of $\mathrm{Pic}_{C/\mathbb{Q}}$, parametrising degree 0 line bundles over $C/\mathbb{Q}$. It is an abelian variety, whose geometric fibers are of dimension

$g =$ genus(C) and having the 'nice' properties of $C/\mathbb{Q}$ (namely being proper, smooth and geometrically connected). We call the *dual variety* of $J/\mathbb{Q}$, denoted $J^\vee/\mathbb{Q}$ the subgroup scheme $\mathrm{Pic}^0_{J/\mathbb{Q}}$ of $\mathrm{Pic}_{J/\mathbb{Q}}$, parametrising degree 0 line bundles over $J/\mathbb{Q}$. Roughly speaking, where J parametrises degree 0 line bundles over C, $J^\vee$ does the same over J. This is an abelian variety which is given with an isomorphism λ, called the *principal polarisation* of the pair $(J, J^\vee)/\mathbb{Q}$ and satisyfing $-\lambda^{-1} = j_b^\star$ (We recall that $j_b : C \to J$ is the Abel-Jacobi map parametrising the embedding of C into J). Moreover, there exists an uniquely determined (up to a unique isomorphism) line bundle $\mathcal{P}$ over $J \times J^\vee$, called the *Poincaré bundle* and which satisfies the following properties

1. $\mathcal{P}_{|\{0\}\times J^\vee}$ is trivial and $\mathcal{P}_{|J\times\{a\}}$ is (a line bundle) of degree 0 over $J_{k(a)}$ for all $a \in J^\vee$;
2. for every $\mathbb{Q}$-scheme T, and every $\mathcal{L} \in \mathrm{Pic}(J \times T)$ such that $(J, T, \mathcal{L})$ satisfies 1., there exists a unique morphism $f : T \to J^\vee$ such that $(1, f)^\star\mathcal{P}$ is isomorphic to $\mathcal{L}$

Example 1 (Elliptic curves)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then standard results from the theory of elliptic curves give us that we can both identify $J/\mathbb{Q}$ and $J^\vee/\mathbb{Q}$ to $E/\mathbb{Q}$. In this special case, the Poincaré bundle is given by $\mathcal{P} = \mathcal{O}_{E\times E}(\Delta - \{0\}\times E - E\times\{0\})$ where Δ is the diagonal inside $E \times E$.*

Both embeddings of group schemes $J \hookrightarrow \mathrm{Pic}_{C/\mathbb{Q}}$ and $J^\vee \hookrightarrow \mathrm{Pic}_{J/\mathbb{Q}}$ give rise to exact sequences in the following commutative diagram of group schemes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & J^\vee & \hookrightarrow & \mathrm{Pic}_{J/\mathbb{Q}} & \twoheadrightarrow & \mathrm{NS}_{J/\mathbb{Q}} & \longrightarrow & 1 \\ & & \wr\downarrow{\scriptstyle j_b^\star} & & \downarrow{\scriptstyle j_b^\star} & & \downarrow{\scriptstyle j_{b,\mathrm{NS}}^\star} & & \\ 1 & \longrightarrow & J & \hookrightarrow & \mathrm{Pic}_{C/\mathbb{Q}} & \twoheadrightarrow & \mathrm{NS}_{C/\mathbb{Q}} & \longrightarrow & 1 \end{array}$$

where $\mathrm{NS}_{(-)}$ stands for the *Néron-Severi groups* defined as the natural quotient $\mathrm{Pic}_{(-)}/\mathrm{Pic}^0_{(-)}$. In our context:

- $\mathrm{NS}_{J/\mathbb{Q}}$ can be identified with the group scheme $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^{+}$[14] of symmetric endomorphisms of J, after identifying $J^\vee$ with J via λ. It is a free $\mathbb{Z}_{\mathbb{Q}}$-module of rank ρ (the *Picard number* of $C/\mathbb{Q}$). The resulting map $\mathrm{Pic}_{J/\mathbb{Q}} \to \underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+$, on $\mathbb{Q}$-points, send $\mathcal{L} \in \mathrm{Pic}_{J/\mathbb{Q}}(\mathbb{Q})$ to $\varphi_{\mathcal{L}} : J(\mathbb{Q}) \to J^\vee(\mathbb{Q})$ given by
$$\varphi_{\mathcal{L}}(a) = t_a^\star\mathcal{L} \otimes \mathcal{L}^{-1}$$
for any $a \in J(\mathbb{Q})$ and t_a being the translation map.
- $\mathrm{NS}_{C/\mathbb{Q}}$, since $C/\mathbb{Q}$ is of relative dimension 1, is identified to the group scheme $\mathbb{Z}_{\mathbb{Q}}$ (seen as a rank 1 free module over itself). The resulting map $\mathrm{Pic}_{C/\mathbb{Q}} \to \mathbb{Z}_{\mathbb{Q}}$, on $\mathbb{Q}$-points, is the degree map which associates to any line bundles over $C/\mathbb{Q}$ its degree.
- Looking at the $\mathbb{C}$-points on $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+$, we can make an identification between $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+(\mathbb{C})$ and $H_1(J(\mathbb{C}), \mathbb{Z})$ which is equipped with a trace map to $\mathbb{Z}$. Restricting this action, then, to $\mathbb{Q}$-points gives us that the map $j_{b,\mathrm{NS}}^\star$ can be seen as a non-zero trace map on the group of self-dual morphisms $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+$. For rank arguments, the kernel $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+_0$ of such a map (group scheme of self-dual morphisms of trace 0) is a $\mathbb{Z}_{\mathbb{Q}}$-module of rank $\rho - 1$. Moreover, applying the Snake Lemma to the previous diagram gives us that $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+_0 \simeq \ker(j_b^\star)$

From now on, we will assume that $\rho > 1$: as explained in the remark of the next subsection, this is not true for generic curves. However, it is true for some relevant examples (such as modular curves) and actually needed to apply the non-abelian Chabauty theory. We consider the following commutative diagram

$$\begin{array}{ccccccccc} & & & & \ker(j_b^\star) & \xrightarrow{\sim} & \underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+_0 & & \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & J^\vee & \hookrightarrow & \mathrm{Pic}_{J/\mathbb{Q}} & \xrightarrow{\varphi_{(-)}} & \underline{\mathrm{Hom}}_{\mathbb{Q}}(J, J^\vee)^+ & \longrightarrow & 1 \\ & & \wr\downarrow{\scriptstyle j_b^\star} & & \downarrow{\scriptstyle j_b^\star} & & \downarrow{\scriptstyle \mathrm{Trace}} & & \\ 1 & \longrightarrow & J & \hookrightarrow & \mathrm{Pic}_{C/\mathbb{Q}} & \xrightarrow{\deg} & \mathbb{Z}_{\mathbb{Q}} & \longrightarrow & 1 \end{array}$$

[14] where the exponent '+' refers to the invariance under the Rosati involution

Actually, $\varphi_{(-)}$ admits a section which corresponds to pulling-back the Poincaré bundle, that is the map, on $\mathbb{Q}$-points, given by $f \mapsto (1,f)^\star\mathcal{P}$. Therefore, following the diagram, we can map $\underline{\mathrm{Hom}}_{\mathbb{Q}}(J,J^\vee)^+_0(\mathbb{Q})$ to $\mathrm{Pic}_{J/\mathbb{Q}}(\mathbb{Q})$ in two different ways. By commutativity, taking the difference of these two maps gives a mapping on $\mathbb{Q}$-points

$$\underline{\mathrm{Hom}}_{\mathbb{Q}}(J,J^\vee)^+_0(\mathbb{Q}) \to J^\vee(\mathbb{Q}),\ f \mapsto b_f$$

and we see that, for any $f \in \underline{\mathrm{Hom}}_{\mathbb{Q}}(J,J^\vee)^+_0(\mathbb{Q})$, $(1,f)^\star\mathcal{P}$ is in the kernel of $j_b^\star$ if and only if $b_f = 0$. If $b_f \neq 0$, we can translate f by this b_f and the resulting pullback will therefore be in the kernel. This means that, for any $f \in \underline{\mathrm{Hom}}_{\mathbb{Q}}(J,J^\vee)^+_0(\mathbb{Q})$

$$j_b^\star(1, t_{b_f} \circ f)^\star\mathcal{P} \in \mathrm{Pic}_{C/\mathbb{Q}}(\mathbb{Q})$$

is trivial. Now we know how to create trivial bundles over $C/\mathbb{Q}$ from a fixed line bundle over $J \times J^\vee$. In order to keep track of computations on J and $J^\vee$ and to make then compatible, we need a certain geometric object carrying a structure of *biextension* over the product $J \times J^\vee$. This object is the *Poincaré torsor*, which is a $\mathbb{G}_m$-torsor (a line bundle without the 0-section) lying over $J \times J^\vee$

3.1.2 Poincaré torsor and biextension structure

We define the Poincaré torsor $\mathcal{P}^\times$ to be the $\mathbb{G}_m$-torsor over $J \times J^\vee$ defined as

$$\mathcal{P}^\times := \underline{\mathrm{Isom}}_{J\times J^\vee}(\mathcal{O}_{J\times J^\vee}, \mathcal{P})$$

(which can be seen as $\mathcal{P}$ without zero sections by looking at the image of the unit section in $\mathcal{O}_{J\times J^\vee}(J \times J^\vee)$). In terms of points, for any scheme $S \to J \times J^\vee$, $\mathcal{P}^\times(S)$ is the set of isomorphisms from $\mathcal{O}_S$ to $\mathcal{P}_S$ with a free and transitive action of $\mathbb{G}_m(S) = \mathcal{O}_S(S)^\times$. Identifying $J^\vee$ with $\mathrm{Ext}^1_{\mathbb{Q}}(J,\mathbb{G}_m)$ and J with $\mathrm{Ext}^1_{\mathbb{Q}}(J^\vee,\mathbb{G}_m)$, we have that $\mathcal{P}^\times$ can be both seen as the universal extension J by $\mathbb{G}_m$, indexed by $J^\vee$ and vice-versa (this follows from the definition of $\mathcal{P}$). This gives a structure of $\mathbb{G}_m$-biextension on $\mathcal{P}^\times$ over $J \times J^\vee$. In fact, thanks to the theorem of the cube, for any $x, x_1, x_2 \in J(\mathbb{Q})$ and $y, y_1, y_2 \in J^\vee(\mathbb{Q})$ there are maps

$$(x_1,y)^\star\mathcal{P}^\times \times_{\mathbb{Q}} (x_2,y)^\star\mathcal{P}^\times \to (x_1+x_2,y)^\star\mathcal{P}^\times$$

and

$$(x,y_1)^\star\mathcal{P}^\times \times_{\mathbb{Q}} (x,y_2)^\star\mathcal{P}^\times \to (x,y_1+y_2)^\star\mathcal{P}^\times$$

giving rise to partial group laws $+_1$ and $+_2$ on $\mathcal{P}^\times$ which are compatible. Indeed, as explained in more details in [EL21, Section 2], for $z_1 \in ((x_1,y)^\star\mathcal{P}^\times)(\mathbb{Q})$ and $z_2 \in ((x_2,y)^\star\mathcal{P}^\times)(\mathbb{Q})$, the first partial group law on $\mathcal{P}^\times \to J^\vee$ (that is, indexed by points on $J^\vee$) is given by the following commutative diagram:

$$\begin{array}{ccc} ((x_1,y)^\star\mathcal{P}^\times \times_{\mathbb{Q}} (x_2,y)^\star\mathcal{P}^\times)(\mathbb{Q}) & \longrightarrow & ((x_1+x_2,y)^\star\mathcal{P}^\times)(\mathbb{Q}) \\ \downarrow & & \downarrow \\ (J\times J^\vee)(\mathbb{Q}) & \longrightarrow & (J\times J^\vee)(\mathbb{Q}) \end{array} \qquad \begin{array}{ccc} (z_1,z_2) & \longmapsto & z_1 +_1 z_2 \\ \downarrow & & \downarrow \\ ((x_1,y),(x_2,y)) & \longmapsto & (x_1+x_2,y) \end{array}$$

and we define similarly $+_2$ on the extension $\mathcal{P}^\times \to J$. Finally, the compatibility is given by the following: for $z_{i,j} \in ((x_i,y_j)^\star\mathcal{P}^\times)(\mathbb{Q})$ $(i,j \in \{1,2\})$, we have

$$\begin{array}{ccccc} ((x_1+x_2,y_1+y_2)^\star\mathcal{P}^\times)(\mathbb{Q}) & & (z_{1,1}+_1 z_{2,1}) +_2 (z_{1,2}+_1 z_{2,2}) & = & (z_{1,1}+_2 z_{1,2}) +_1 (z_{2,1}+_1 z_{2,2}) \\ \downarrow & & \searrow & & \swarrow \\ (J\times J^\vee)(\mathbb{Q}) & & & (x_1+x_2,y_1+y_2) & \end{array}$$

Now, fix a basis $(f_1,\dots,f_{\rho-1}) \in \underline{\mathrm{Hom}}_{\mathbb{Q}}(J,J^\vee)^+_0(\mathbb{Q})$ (which is a free $\mathbb{Z}$-module of rank $\rho-1$). According to what we did before, we know that for $i = 1,\dots,\rho-1$, $j_b^\star(1, t_{b_{f_i}} \circ f_i)^\star\mathcal{P}^\times$ is trivial over $C/\mathbb{Q}$. Therefore, taking the product T of all the pullbacks $(1, t_{b_{f_i}} \circ f_i)^\star\mathcal{P}^\times$, we get a $\mathbb{G}_m^{\rho-1}$-torsor

over $J/\mathbb{Q}$ in which C embeds since $j_b^\star T$ is trivial over $C/\mathbb{Q}$ by definition. This gives rise to the following commutative diagram

$$\begin{array}{ccccc} & & T & \longrightarrow & \mathcal{P}^{\times,\rho-1} \\ & \nearrow & \downarrow & & \downarrow \\ C & \xrightarrow{j_b} & J & \xrightarrow[(1,t_{b_{f_1}}\circ f_1,\ldots,t_{b_{f_{\rho-1}}}\circ f_{\rho-1})]{} & J\times (J^\vee)^{\rho-1} \end{array}$$

and the idea is to apply geometric Chabauty to such a diagram, where $T/\mathbb{Q}$ will take the role of $J/\mathbb{Q}$. Here, $T/\mathbb{Q}$ is a semi-abelian variety of relative dimension $g+\rho-1$ and this dimension argument justifies the motivation of passing through quadratic Chabauty when working with curves not satisfying the *abelian Chabauty condition* ($r < g$).

Remark. Actually, as mentioned in a paper of Samir Siksek ([Sik17]), for a generic curve, ρ appears to be equal to 1: for example, in the case where the Jacobian J is simple, $\rho = 1$ and it is likely to happen for most of the curves. We therefore does not win more flexibility working with quadratic Chabauty (in such a context) since we easily see that in the case where $\rho = 1$, all the constructions will lead to considering the geometric description made in the last section. However, for families of modular curves, S. Siksek explains in his paper that the Néron-Séveri group of J is actually non trivial and is isogeneous to a product of several abelian varieties, and therefore ρ is in general strictly bigger than 1. This also illustrates how the use of quadratic Chabauty was efficient in the paper about cracking the cursed curve ([BDM$^+$19])

In order to perform Chabauty, we want to understand what is the intersection $C(\mathbb{Q}_p)\cap\overline{T(\mathbb{Q})}^p \subseteq T(\mathbb{Q}_p)$. Here, as before, $T(\mathbb{Q}_p)$ is a p-adic manifold of dimension $g+\rho-1$. However, since T is a $\mathbb{G}_m^{\rho-1}$-torsor over $J/\mathbb{Q}$, it appears that $T(\mathbb{Q}) \simeq (\mathbb{Q}^\times)^{\rho-1}\times J(\mathbb{Q})$ where the latter is known to be finitely generated of rank r thanks to Mordell-Weil. However, the first factor is infinitely generated, and hence, even if we can bound from above the dimension, as a p-adic manifold, of $\overline{T(\mathbb{Q})}^p$ by $r+\rho-1$, we are not going to win flexibility compared to linear Chabauty. To ensure some improvement, we need to change the ring over which we study our curve, for instance by $\mathbb{Z}$ since $\mathbb{G}_m(\mathbb{Z})$ is finite.

3.2 Extension of the geometry to $\mathbb{Z}$

Let $\mathcal{C}/\mathbb{Z}$ be a complete, flat and regular model of $C/\mathbb{Q}$ (we recall that $C/\mathbb{Q}$ was supposed to be proper, smooth and geometrically connected). Since $\mathcal{C}(\mathbb{Z}) = C(\mathbb{Q})$, we may keep the same basepoint $b \in C(\mathbb{Q})$ chosen earlier. Now, let $\mathcal{J}/\mathbb{Z}$ be the Néron model of $J/\mathbb{Q}$ and $\mathcal{J}^\vee/\mathbb{Z}$ the Néron model of the dual of $\mathcal{J}/\mathbb{Z}$. It turns out that we cannot extend $\mathcal{P}^\times$ to $\mathcal{J}\times\mathcal{J}^\vee$. However, $\mathcal{P}^\times$ extends uniquely to a $\mathbb{G}_m$-biextension $\mathcal{P}_0^\times \to \mathcal{J}\times\mathcal{J}^{\vee,0}$ where the second factor is the fiberwise connected component of 0 in $\mathcal{J}^\vee$. The component group $\Phi_{\mathcal{J}^\vee} := \mathcal{J}^\vee/\mathcal{J}^{\vee,0}$ is finite étale, supported on $\mathbb{Z}/n\mathbb{Z}$ where n is the product of all primes of bad reduction for $\mathcal{C}/\mathbb{Z}$. We denote by m the annihilator of $\Phi_{\mathcal{J}^\vee}$ (therefore, multiplication by m will ensure that we can map $\mathcal{J}$ to $\mathcal{J}^{\vee,0}$ to get similar result as before).

Remark. Earlier, by smoothness of $C/\mathbb{Q}$, we knew that for all $i = 1,\ldots,\rho-1$, $j_b^\star(1, t_{b_{f_i}}\circ f_i)^\star\mathcal{P}^\times$ were trivial above $C/\mathbb{Q}$. Here, $\mathcal{C}$ is smooth only above $\mathbb{Z}[1/n]$ (where we invert every primes of bad reduction). In order to ensure that our pullbacks along j_b of the $\mathbb{G}_m$-torsors $(1, m\cdot\circ t_{b_{f_i}}\circ f_i)^\star\mathcal{P}^\times$ are trivial, we need to consider them above some dense open of $\mathcal{C}/\mathbb{Z}$ containing smooth points and for which every fibers are made of only one geometrically irreducible component.

Let us cover $\mathcal{C}^{\mathrm{sm}}/\mathbb{Z}$, the smooth locus of $\mathcal{C}/\mathbb{Z}$ (note that $C(\mathbb{Q}) = \mathcal{C}(\mathbb{Z}) = \mathcal{C}^{\mathrm{sm}}(\mathbb{Z})$), by a finite family of open subschemes U_k obtained by removing, for all $q \mid n$ of bad reduction, all irreducible components of $\mathcal{C}^{\mathrm{sm}}_{\mathbb{F}_q}$ except one being geometrically irreducible. Since there are only finitely many primes of bad reduction and since, for each prime, there are only finitely many choices of removing possible, we see that there are only finitely many such U_k's. Moreover, we can remark that for each U_k, $\mathrm{Pic}_{U_k/\mathbb{Z}} \simeq \mathrm{Pic}_{C/\mathbb{Q}}$ and $\mathcal{O}_{\mathcal{C}}(U_k) = \mathbb{Z}$. Whence, we can apply the previous theory to the U_k's

and according to their definition, for all U_k and for all $i = 1, \dots, \rho - 1$, we can lift $j_{b,k} := (j_b)_{|U_k}$

$$\begin{array}{ccccc} & & T_i & \longrightarrow & \mathcal{P}_0^{\times} \\ & \widetilde{j_{b,k,i}} \nearrow & \downarrow & & \downarrow \\ U_k & \xrightarrow{j_{b,k}} & \mathcal{J} & \xrightarrow[(1, m\cdot\circ t_{b_{f_i}} \circ f_i)]{} & \mathcal{J} \times \mathcal{J}^{\vee,0} \end{array}$$

and this lift is unique up to multiplication by an element of $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. So, if we denote by T the product of all the T_i's, we get for all U_k

$$\begin{array}{ccccc} & & T & \longrightarrow & \mathcal{P}_0^{\times,\rho-1} \\ & \widetilde{j_{b,k}} \nearrow & \downarrow & & \downarrow \\ U_k & \xrightarrow{j_{b,k}} & \mathcal{J} & \xrightarrow[(1, m\cdot\circ t_{b_{f_i}} \circ f_i)_{i=1,\dots,\rho-1}]{} & \mathcal{J} \times (\mathcal{J}^{\vee,0})^{\rho-1} \end{array}$$

and we will be able to apply a similar method as the one described in the last section, for all the U_k's. This will gives us, combining the finite number of upper bounds of the $\widetilde{j_{b,k}}(U_k(\mathbb{Z})) \subseteq \widetilde{j_{b,k}}(U_k(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}^p \subseteq T(\mathbb{Z}_p)$ for a choice of a good prime number p, an upper bound for $C(\mathbb{Q})$. Here, $T(\mathbb{Z}_p)$ is a p-adic manifold of dimension $g + \rho - 1$ and it is expected that the dimension of $\overline{T(\mathbb{Z})}^p$, as in the linear case, will be at most r and therefore, geometric quadratic Chabauty should be successful under the *quadratic Chabauty condition* $r < g + \rho - 1$.

3.3 Geometric quadratic Chabauty

Let p be an odd prime number of good reduction, fix an $U := U_k$ for some k, $j := j_{b,k}$ and let $P \in U(\mathbb{F}_p)$ whose image by $\tilde{j}$ will be denoted by $t := \tilde{j}(P) \in T(\mathbb{F}_p)$. We want to bound the cardinality of $\tilde{j}(U(\mathbb{Z}_p)_P) \cap \overline{T(\mathbb{Z})_t}^p \subseteq T(\mathbb{Z}_p)_t$ from above. To do so, as before, we need to describe what is the closure of $T(\mathbb{Z})_t$ inside $T(\mathbb{Z}_p)_t$. Then, we will use defining equation of $U(\mathbb{Z}_p)_P$ seen as embedded inside $T(\mathbb{Z}_p)_t$ to pull them back to $\overline{T(\mathbb{Z})_t}^p$.

Suppose that $T(\mathbb{Z})_t$ is non empty and let us consider the following commutative diagram:

$$\begin{array}{ccccc} & & T(\mathbb{F}_p) & \xleftarrow{\mathrm{mod}_p} & T(\mathbb{Z}) \\ & \tilde{j} \nearrow & & & \downarrow \\ U(\mathbb{F}_p) & \xrightarrow[j]{} & \mathcal{J}(\mathbb{F}_p) & \xleftarrow[\mathrm{mod}_p]{} & \mathcal{J}(\mathbb{Z}) \end{array} \qquad \begin{array}{ccc} & t & \longmapsto \tilde{t} \\ \nearrow & & \downarrow \\ P & \longmapsto j(P) & \longmapsto x_{\tilde{t}} \end{array}$$

and let $x_1, \dots, x_r$ be a $\mathbb{Z}$-basis of $\mathcal{J}(\mathbb{Z})_0$. For convenience, we will denote by $f := (f_1, \dots, f_{\rho-1}) : \mathcal{J} \to \mathcal{J}^{\vee,\rho-1}$ and $b_f := (b_{f_1}, \dots, b_{f_{\rho-1}}) \in \mathcal{J}^{\vee,\rho-1}(\mathbb{Z})$ which have been defined previously. Then, as explained in [EL21, Section 4], for $i, j = 1, \dots, r$ we *choose* elements $P_{i,j}, R_{i,\tilde{t}}, S_{\tilde{t},j} \in \mathcal{P}_0^{\times,\rho-1}(\mathbb{Z})$ having respective images in $(\mathcal{J} \times (\mathcal{J}^{\vee,0})^{\rho-1})(\mathbb{Z})$ being $(x_i, f(mx_j)), (x_i, (m \cdot \circ t_{b_f} \circ f)(x_{\tilde{t}}))$ and $(x_{\tilde{t}}, f(mx_j))$. From the $\mathbb{G}_m^{\rho-1}$-biextension structure on $\mathcal{P}^{\times,\rho-1}$ it is therefore possible to define, for all $n := (n_1, \dots, n_r) \in (p-1)\mathbb{Z}^r$, points $A_{\tilde{t}}(n), B_{\tilde{t}}(n), C(n) \in \mathcal{P}_0^{\times,\rho-1}(\mathbb{Z})$ whose respective images are $(x_{\tilde{t}}, \sum_{i=1}^r n_i f(mx_i))$, $\left(\sum_{i=1}^r n_i x_i, (m \cdot \circ t_{b_f} \circ f)(x_{\tilde{t}})\right)$ and $(\sum_{i=1}^r n_i x_i, \sum_{i=1}^r n_i f(mx_i))$. Whence, for the biextension structure in the Poincaré torsor, taking linear combination of those points with $\tilde{t}$ leads to define a point, for all $n \in (p-1)\mathbb{Z}^r$,

$$D_{\tilde{t}}(n) := (C(n) +_2 B_{\tilde{t}}(n)) +_1 (A_{\tilde{t}}(n) +_2 \tilde{t}) \in \mathcal{P}^{\times,\rho-1}(\mathbb{Z})$$

whose image in $\mathcal{J}(\mathbb{Z})$ reduces to $j(P)$ modulo p. Hence, this construction defines a map

$$\kappa_{\mathbb{Z}} : \mathbb{Z}^r \to T(\mathbb{Z})_t, \quad n \mapsto D_{\tilde{t}}((p-1)n)$$

which turns out to have good properties, such as the kappa map of last section.

Since T is $\mathbb{G}_m^{\rho-1}$-extension of $\mathcal{J}$ of relative dimension g, we can find elements $j_1, \dots, j_g \in$

$\mathcal{O}_{J,j(P)}$ such that together with p they generate $\mathfrak{m}_{j(P)}$ and elements $t_1, \dots, t_{\rho-1} \in \mathcal{O}_{T,t}$ such that $p, j_1, \dots, j_g, t_1, \dots, t_{\rho-1}$ generate $\mathfrak{m}_t$. Therefore, using the previous description of $\mathbb{Z}_p$-points on smooth models, we find that evaluating at these parameters and then dividing by p gives a bijection

$$T(\mathbb{Z}_p)_t \to \mathbb{Z}_p^{g+\rho-1}$$

and we have the following result excerpt from [EL21]

Theorem 3.1 (Theorem 4.10, [EL21]). *The composition of the last bijection with $\kappa_{\mathbb{Z}}$ is given by uniquely determined $\kappa_1, \dots, \kappa_{g+\rho-1} \in \mathbb{Z}_p\langle \underline{z} \rangle$. The reductions modulo p of the first g are of degree at most 1, and the reductions of the others $\rho - 1$ are of degree at most 2. Finally, we can extend uniquely $\kappa_{\mathbb{Z}}$ to $\mathbb{Z}_p^r$ into a map κ whose image is $\overline{T(\mathbb{Z})_t}^p \subseteq T(\mathbb{Z}_p)_t$.*

Remark. The fact that the reductions modulo p of $\kappa_{g+1}, \dots, \kappa_{g+\rho-1}$ are of degree at most 2 could justify the naming 'quadratic' (which also refers to the subscript 2 of $\pi_1(C)_2$, as the second case of Kim's program) . Indeed, since those are from the pullback extension structure on T, the fact that $\mathrm{id}_{\mathcal{J}}$ and $m \cdot \circ t_{b_f} \circ f$ are linear maps, when evaluating on the diagonal of $\mathcal{J}$, we get a quadratic mapping. Furthermore, we see that if $\rho = 1$, then $T = \mathcal{J}$ and all the κ_i's have reductions of degree at most 1: we go back to the linear case.

Finally, since U is of relative dimension 1, and T of relative dimension $g+\rho-1$ as a $\mathbb{G}_m^{\rho-1}$-extension of $\mathcal{J}$ of relative dimension g, one can find p-adically convergent power series $h_1, \dots, h_{g+\rho-2}$ where $h_1, \dots, h_{g-1} \in \mathcal{O}_{\widetilde{\mathcal{J}}^p_{j(P)}}(\widetilde{\mathcal{J}}^p_{j(P)})^{\wedge p}$ and $h_g, \dots, h_{g+\rho-2} \in \mathcal{O}_{\widetilde{T}^p_t}(\widetilde{T}^p_t)^{\wedge p}$ which are linear modulo p and such that $U(\mathbb{Z}_p)_P \simeq V(h_1, \dots, h_{g+\rho-2}) \subseteq T(\mathbb{Z}_p)_t$. We denote by $\lambda_i := \kappa^\star h_i$ the pullbacks of the h_i along κ. As in the previous section, we have that, denoting $V := V(\lambda_1, \dots, \lambda_{g+\rho-2}) \subseteq \mathbb{Z}_p^r$, $\kappa_{|V}$ is a surjection onto $U(\mathbb{Z}_p)_P \cap \overline{T(\mathbb{Z})_t}^p \subseteq T(\mathbb{Z}_p)_t$. Therefore, it is sufficient to bound the cardinality of V from above. For this, let $I := (\lambda_i)_{i=1,\dots,g+\rho-2}\mathbb{Z}_p\langle \underline{z} \rangle$ and let $A := \mathbb{Z}_p\langle \underline{z} \rangle / I$. We assume that its reduction modulo p, $\overline{A} := A/pA$, is finite. Then, we have a similar result as Proposition 2.3, which will be formulated (without proof) as follows:

Theorem 3.2 (Theorem 4.12, [EL21]). *The reductions modulo p of $\lambda_1, \dots, \lambda_{g-1}$ in $\mathbb{F}_p[\underline{z}]$ are of degree at most 1, and those of $\lambda_g, \dots, \lambda_{g+\rho-2}$ are of degree at most 2. Moreover, $\overline{A}$ is the product of its localisation $\overline{A}_{\underline{m}}$ at its finitely many maximal ideals $\underline{m}$. The sum of $\dim_{\mathbb{F}_p} \overline{A}_{\underline{m}}$ over the $\underline{m}$ such that $\overline{A}/\underline{m} \simeq \mathbb{F}_p$ is an upper bound for the number of elements of $\mathbb{Z}_p^r$ whose image under κ is in $U(\mathbb{Z}_p)_P$ and also an upper bound for the number of elements of $U(\mathbb{Z})$ with image P in $U(\mathbb{F}_p)$.*

Remark.

- In the situation where $r < g + \rho - 1$, as we remarked in the linear classical case, for dimension reasons, one could expect to find a prime p of good reduction and for which, for all U_k and all P_k in some $U_k(\mathbb{F}_p)$, the upper bound on $U_k(\mathbb{Z})_{P_k}$ is actually sharp. In fact, one may expect that for many of the U_k's, $U_k(\mathbb{Z})$ is trivial in this context.
- This approach has been adapted to the study of curves over number fields. This has been carried out by Pavel Coupek, David Lilienfeldt, Luciena X. Xaio and Zijian Yao following the exposition of B. Edixhoven at the AWS 2020. See [CLXY21] for further literature on the subject.

3.4 Final comment on calculation

We will conclude this section by giving an idea on why this approach has advantages when having to do calculations.

For degree reasons mentioned in Theorem 3.2, we should only have to compute the λ_i's modulo p^2. In fact, these λ_i's take their arguments in the image of residue discs (by parameters), after dividing out by p. Since we then conclude by looking at the image of I after reducing modulo p, roughly speaking, all the information needed from points in the residue discs are concentrated in $\mathbb{Z}_p/p^2\mathbb{Z}_p$. Therefore, it should be sufficient to work with residue discs described over $\mathbb{Z}/p^2\mathbb{Z}$ instead of over $\mathbb{Z}_p$ itself. This offers the possibility of doing actual calculations, which turn out to be of reliable precision, even if we do not have any explicit description of $\mathcal{J}$ and T.

Remark. Actually, in practice, it might be needed to reduce to an higher power of p, for precision reasons. However, we will explain how it is possible to have enough information doing calculations modulo p^2.

This has been treated with more details in the reference paper of B. Edixhoven and G. Lido. (we refer in particular to Section 8 of the paper for an explicit example, from which one could be convinced by the restriction modulo p^2). In this subsection, we will try to give some hints/intuitions on what can be done. Let p be still a prime number of good reduction, we assume that C is smooth over $\mathbb{Z}/p^2\mathbb{Z}$ and that there exists a non-special split reduced divisor of degree g on $C_{\mathbb{F}_p}$. Then, let $b_1, \ldots, b_g \in C(\mathbb{Z}/p^2\mathbb{Z})$ having pairwise distinct reductions modulo p and being such that $h^0(C_{\mathbb{F}_p}, \overline{b_1} + \ldots, \overline{b_g}) = 1$ and let $b_{g+1}, \ldots, b_{2g} \in C(\mathbb{Z}/p^2\mathbb{Z})$ having, in the same way, pairwise distinct reductions modulo p and being such that $h^0(C_{\mathbb{F}_p}, \overline{b_{g+1}} + \ldots, \overline{b_{2g}}) = 1$. Let's consider a pullback $\mathcal{M}$ of the Poincaré bundle $\mathcal{P}$ over $J \times J$ along the map

$$\mathrm{id}_J \times j_b^{\star,-1} \colon J \times J \to J \times J^\vee$$

fitting in the following square

$$\begin{array}{ccc} \mathcal{M} & \longleftarrow & \mathcal{P} \\ \big| & & \big| \\ J \times J & \xrightarrow[\mathrm{id}_J \times j_b^{\star,-1}]{} & J \times J^\vee \end{array}$$

and as for $\mathcal{P}^\times$, we define the $\mathbb{G}_m$-torsor $\mathcal{M}^\times$.

Now, let $D, E \in J(\mathbb{F}_p)$ be relative degree 0 Cartier divisors on C and write $D = D^+ - D^-$, $E = E^+ - E^-$. We can parametrise the *residue polydisc* $((J \times J)(\mathbb{Z}/p^2\mathbb{Z}))_{(D,E)}$ in the following way: let us define two maps f, f' by

$$\begin{array}{rccc} f & : & C^g & \to & J \\ & & (c_1, \ldots, c_g) & \mapsto & [\mathcal{O}_C(c_1 + \ldots + c_g - (b_1 + \ldots + b_g) + D] \end{array}$$

$$\begin{array}{rccc} f' & : & C^g & \to & J \\ & & (c_1, \ldots, c_g) & \mapsto & [\mathcal{O}_C(c_1 + \ldots + c_g - (b_{g+1} + \ldots + b_{2g}) + E] \end{array}$$

which are respectively étale at the respective base-points $b = (b_1, \ldots, b_g)$ and $b' = (b_{g+1}, \ldots, b_{2g})$ by their definition. Therefore, by similar results used during this paper, f and f' induce isomorphisms

$$C^g(\mathbb{Z}/p^2\mathbb{Z})_b \simeq J(\mathbb{Z}/p^2\mathbb{Z})_D \qquad C^g(\mathbb{Z}/p^2\mathbb{Z})_{b'} \simeq J(\mathbb{Z}/p^2\mathbb{Z})_E$$

Therefore, if we consider any point $c \in C(\mathbb{Z}/p^2\mathbb{Z})$ (instead of in $C(\mathbb{Z}_p)$ entirely), we have that $C(\mathbb{Z}/p^2\mathbb{Z})_c$ consists of points $\overline{c} + \lambda p$ where $\overline{c}$ is the reduction modulo p of c and λ ranges over $\mathbb{F}_p$. This means that giving a 'direction' $\lambda \in \mathbb{F}_p$ defines a bijection

$$\begin{array}{ccc} \mathbb{F}_p & \to & C(\mathbb{Z}/p^2\mathbb{Z})_c \\ \lambda & \mapsto & c_\lambda := \overline{c} + \lambda p \end{array}$$

and this works also for the b_i's defined earlier. Rises then the following

$$\begin{array}{ccccc} \mathbb{F}_p^g & \xrightarrow{\sim} & C^g(\mathbb{Z}/p^2\mathbb{Z})_b & \xrightarrow{\sim} & J(\mathbb{Z}/p^2\mathbb{Z})_D \\ \lambda = (\lambda_1, \ldots, \lambda_g) & \mapsto & b_\lambda = (b_{1,\lambda_1}, \ldots, b_{g,\lambda_g}) & \mapsto & D_\lambda = D + (b_{1,\lambda_1} + \ldots + b_{g,\lambda_g}) - (b_1 + \ldots + b_g) \end{array}$$

and the same can be done for f', b' and E. Therefore, by the description of $\mathcal{M}^\times$ over $J \times J$ and by the previous, it is possible to express $\mathcal{M}^\times(\mathbb{Z}/p^2\mathbb{Z})_{(D,E)}$ in terms of at most $(pg)^2$ computable explicit line bundles over $C \times C$. Whence, we see that considering p-adic points to a degree-2 'precision' should be in fact enough to be able to do calculations.

4 Appendix: The Mordell-Weil sieve

As stated earlier, the idea of this method is to gather information obtained while performing Chabauty, at different primes of good or bad reduction. We will briefly describe how this technique helps to conclude while trying to compute rational points on curves. The first case considered, as described more explicitly in the paper [BS10] of Niels Bruin and Michael Stoll, is the one in which one wants to prove that the curve has no rational points. The second application, explained by S. Siksek in [Sik15], is to prove that a given set of rational points is complete (in the sense that there are no more rational points on the curve outside this set).

How to conclude that $C(\mathbb{Q}) = \varnothing$?

We consider the same context as in the first section of this paper. We suppose that $g \geq 2$ but instead of embedding C into J via the Abel-Jacobi embedding, depending on the existence of a $\mathbb{Q}$-rational point on C, we will consider an arbitrary embedding $j: C \hookrightarrow J$ (which can be explicitly given while knowing a rational divisor of positive degree on C), defined over $\mathbb{Q}$. Moreover, we suppose that one has been able to compute r and generators for the torsion-free part of $J(\mathbb{Q})$. Let $M_{\mathbb{Q}}$ the set of places of $\mathbb{Q}$ (archimedean and non-archimedean). We have the following diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\quad j \quad} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{\nu \in M_{\mathbb{Q}}} C(\mathbb{Q}_\nu) & \xrightarrow[j]{} & \prod_{\nu \in M_{\mathbb{Q}}} J(\mathbb{Q}_\nu) \end{array}$$

and it appears that

$$(C(\mathbb{Q}) = \varnothing) \iff \left(j\Big(\prod_{\nu \in M_{\mathbb{Q}}} C(\mathbb{Q}_\nu) \Big) \cap \alpha(J(\mathbb{Q})) = \varnothing \right)$$

Hence, being able to prove that such an intersection is empty would be sufficient to conclude on the emptiness of $C(\mathbb{Q})$. Nonetheless, in practice, the considered images of j and α are, a priori, infinite and it is not clear that one can compute their intersection. To remedy this, we consider $S \underset{\text{finite}}{\subseteq} M_{\mathbb{Q}}$ and N a positive integer, fitting in the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\quad j \quad} & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{\nu \in S} C(\mathbb{Q}_\nu) & \xrightarrow[\beta]{} & \prod_{\nu \in S} J(\mathbb{Q}_\nu)/NJ(\mathbb{Q}_\nu) \end{array}$$

It is now possible to compute the images of α and β in this context and there is the first example of using the Mordell-Weil sieve, by finite appromixations. Actually, for S and N 'large enough' (in terms of finite number of places for S), the images of α and β will be disjoint if, and only if, $\prod_{\nu \in S} j(C(\mathbb{Q}_\nu))$ does not meet the topological closure of $J(\mathbb{Q})$ inside $\prod_{p \in S \setminus \{\infty\}} J(\mathbb{Q}_p) \times J(\mathbb{R})/J(\mathbb{R})^0$. Therefore, we see that by 'induction on the sizes of S and N', it is possible to show that $C(\mathbb{Q})$ is empty by using information gathered for the Chabauty-study of C at different prime numbers.

Is a certain set of points complete ?

Under the same assumption, this time we suppose that we know a finite set of rational points $K \subseteq C(\mathbb{Q})$ and we take $b \in K$. Therefore, we can embed C into J via the Abel-Jacobi map $j_b: C \to J$ which has been used several times in this paper. Let p be a prime number of good reduction and let $P \in C(\mathbb{Q}_p)$. We will denote, for k positive integer

$$B_{p,k}(P) := \{Q \in C(\mathbb{Q}_p) \mid Q \text{ has the same reduction as } P \text{ modulo } p^k\}$$

(we note that for $k = 1$, this is a similar definition to the one of residue discs previously defined: $B_{p,1}(P) = C(\mathbb{Q}_p)_{\overline{P}}$ where $\overline{P}$ is the reduction of P modulo p)

Under the Chabauty condition $r < g$, for any $P \in C(\mathbb{Q})$, linear Chabauty let us find a prime number p of good reduction and a positive integer $C_p(P)$ satisfying

$$\#(C(\mathbb{Q}) \cap B_{p,1}(P)) \leq C_p(P)$$

and therefore, if $\#(K \cap B_{p,1}(P)) = C_p(P)$, then

$$C(\mathbb{Q}) \cap B_{p,1}(P) = K \cap B_{p,1}(P)$$

meaning that we have found all the points on this residue disc. However, it may happen that there are more non-trivial residue discs and so we shall combine results for different prime numbers. Moreover, it may also happen that $\#(K \cap B_{p,1}(P)) < C_p(P)$, in which case, one would have to go to $B_{p,2}(P)$, for instance, to get more information. All this can be summarized in the inductive research of a 'small' finite set $W \subseteq J(\mathbb{Q})$ and a subgroup $L < J(\mathbb{Q})$ of 'high' index such that $j_b(C(\mathbb{Q})) \subseteq W + L := \bigcup_{D \in W}(D + L)$. These can be defined by induction by finding finite index subgroups $L_i < J(\mathbb{Q})$ and finite subsets $W_i \subseteq J(\mathbb{Q})$ $(i \geq 0)$ such that $(L_i)_{i \geq 0}$ is a decreasing sequence of subgroup of $J(\mathbb{Q})$ and, for all $i \geq 0$, we have

$$j_b(C(\mathbb{Q})) \subseteq W_i + L_i$$

as in the following process:

We start by setting $L_0 := J(\mathbb{Q})$ and let W_0 be trivial. It obviously satisfies the induction result so now, we suppose we know L_i and W_i for $i = 0, \ldots, m$. We pick a prime p of good reduction and we look at the following commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{j_b} & W_m + L_m \\ \downarrow & & \downarrow \\ C(\mathbb{F}_p) & \xrightarrow[j_b]{} & J(\mathbb{F}_p) \end{array}$$

We define from this $L_{m+1} := \ker(L_m \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p))$ and $W'_{m+1} = W_m + (L_m / L_{m+1})$ where the last quotient refers to a choice of representatives for the cosets. By definition, we have that $W'_{m+1} + L_{m+1} = W_m + L_m$ and if we define W_{m+1} to be the set of points of W'_{m+1} whose reduction modulo p lies in $j_b(C(\mathbb{F}_p))$, one gets that W_{m+1} is finite and $j_b(C(\mathbb{Q})) \subseteq W_{m+1} + L_{m+1}$ as expected. Furthermore, it should be possible, in practice, to choose the prime p at each step such that $(L_i : L_{i+1})$ is 'small', meaning that W'_{i+1} and W_i do not differ from a large number of points. Finally, it appears that good choices of primes p will lead to find a non-negative integer i such that $W_i = j_b(K)$ while the indices $[J(\mathbb{Q}) : L_j]$ are growing as j goes to i.

Remark

It is not trivial that one of these two methods will succeed, neither when one should try one of them. Actually, there is a part of 'mathematical intuition' showing up here. In fact, to be able to make one of those two techniques successful, one has to have a good intuition on the result they have in mind, which happens sometimes. While trying to find points on the curve, if after some rough time, nobody has been able to find any rational points, it is likely that $C(\mathbb{Q}) = \varnothing$ in which case, one should pick the first application. Otherwise, if after several different tries, it appears that one finds a set of rational points which seems to be complete, it would better to do the second one rather than the first, to be able to show that there are no more rational points outside the already-known set.

References

[BD17] Jennifer S. Balakrishnan and Netan Dogra. *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*. International Mathematics Research Notices, 2017.

[BD18] Jennifer S. Balakrishnan and Netan Dogra. *Quadratic Chabauty and rational points I: p-adic heights*. Duke Mathematical Journal, 167(11):1981–2038, 2018.

[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*. Annals of mathematics, 189(3):885–944, 2019.

[Box14] Josha Box. *An introduction to Skolem's p-adic method for solving Diophantine equations*, 2014. https://warwick.ac.uk/fac/sci/maths/people/staff/box/bachelorscriptie_josha_box_eindversi

[BS86] Zenon I. Borevich and Igor R. Shafarevich. *Number theory*. Academic press, 1986.

[BS10] Nils Bruin and Michael Stoll. *The Mordell–Weil sieve: proving non-existence of rational points on curves*. LMS Journal of Computation and Mathematics, 13:272–306, 2010.

[Cha41] Claude Chabauty. *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*. Comptes Rendus de l'Académie des Sciences de Paris, 212(1):882–885, 1941.

[CLXY21] Pavel Coupek, David Lilienfield, Luciena X Xiao, and Zijian Yao. *Geometric quadratic Chabauty over number fields*, 2021. https://www.math.purdue.edu/ pcoupek/Geometric_Chabauty_Part_I.pdf.

[Col85] Robert F. Coleman. *Effective chabauty*. Duke Mathematical Journal, 52(3):765–770, 1985.

[Cor20] David Corwin. *From Chabauty's Method to Kim's Non-Abelian Chabauty's Method*, 2020. https://math.berkeley.edu/ dcorwin/files/ChabautytoKim.pdf.

[CS86] Gary Cornell and Joseph H. Silverman. *Arithmetic Geometry*. Springer, 1986.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228. Springer, 2005.

[Edi20] Bas Edixhoven. *Geometric quadratic Chabauty: Lectures at the Arizona Winter School*, 2020. http://swc.math.arizona.edu/index.html.

[EL21] Bas Edixhoven and Guido Lido. *Geometric Quadratic Chabauty*. Journal of the Institute of Mathematics of Jussieu, pages 1—-55, 2021.

[Fly97] E Victor Flynn. *A flexible method for applying Chabauty's Theorem*. Compositio Mathematica, 105(1):79–94, 1997.

[Gro67] Alexander Grothendieck. *Eléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*. Publications Mathématiques de l'IHÉS, 32:5–361, 1967.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of Graduate Texts in Mathematics. Springer, 1977.

[Has20] Sachi Hashimoto. *Cartoon guide to finding $\mathbb{Q}$-points with geometric quadratic Chabauty*, 2020. https://github.com/sachihashimoto/cartoon-guide-gqc.

[Kim05] Minhyong Kim. *The motivic fundamental group of $P^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel*. Inventiones mathematicae, 161(3):629–656, 2005.

[Kim09] Minhyong Kim. *The unipotent Albanese map and Selmer varieties for curves*. Publications of the Research Institute for Mathematical Sciences, 45(1):89–133, 2009.

[Kob12] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58. Springer Science & Business Media, 2012.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6. Oxford University Press on Demand, 2002.

[Maz92] Barry Mazur. *The topology of rational points.* Experimental Mathematics, 1(1):35–45, 1992.

[McC94] William McCallum. *On the method of Coleman and Chabauty.* Mathematische Annalen, 299(3):565, 1994.

[Mil86] James S. Milne. *Jacobian varieties.* In *Arithmetic geometry*, chapter VII, pages 167–212. Springer, 1986.

[MP12] William McCallum and Bjorn Poonen. *The method of Chabauty and Coleman.* Explicit methods in number theory, 36:99–117, 2012.

[Par00] Pierre Parent. *Torsion des courbes elliptiques sur les corps cubiques.* In *Annales de l'institut Fourier*, volume 50, pages 723–749. 2000.

[PS14] Bjorn Poonen and Michael Stoll. *Most odd degree hyperelliptic curves have only one rational point.* Annals of Mathematics, 180(3):1137–1166, 2014.

[Sch98] Victor Scharaschkin. *The Brauer-Manin obstruction for curves*, 1998. https://www.jmilne.org/math/Students/b.pdf.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Springer, 3rd edition, 1997.

[Sik15] Samir Siksek. *Chabauty and the Mordell-Weil Sieve.* In Advances on Superelliptic Curves and their Applications, volume 41 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 194–224. 2015.

[Sik17] Samir Siksek. *Quadratic Chabauty for modular curves*, 2017. arXiv:1704.00473.

[Spe20] Pim Spelier. *A geometric approach to linear Chabauty.* Master's thesis, Universiteit Leiden, 2020. https://www.universiteitleiden.nl/en/science/mathematics/education/theses.

[Wet97] Joseph L. Wetherell. *Bounding the number of rational points on certain curves of high rank.* PhD thesis, University of California, Berkeley, 1997. https://www.math.arizona.edu/ swc/aws/1999/99WetherellThesis.pdf.