Restriction of Scalars, the Chabauty–Coleman Method, and $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$

by

Nicholas George Triantafillou

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Mathematics

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2019

Author .....
Department of Mathematics
April 18, 2019

Certified by .....
Bjorn Poonen
Claude Shannon Professor of Mathematics
Thesis Supervisor

Accepted by .....
Davesh Maulik
Chairman, Department Committee on Graduate Theses

Restriction of Scalars, the Chabauty–Coleman Method, and $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$

by

Nicholas George Triantafillou

Submitted to the Department of Mathematics
on April 18, 2019 , in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy in Mathematics

Abstract

We extend Siksek's development of Chabauty's method for restriction of scalars of curves to give a method to compute the set of S-integral points on certain $\mathcal{O}_{K,S}$-models $\mathcal{C}$ of punctured genus g curves C over a number field K. Our assumptions on $\mathcal{C}$ guarantee that it carries a morphism $j : \mathcal{C} \to \mathcal{J}$ to a commutative group scheme $\mathcal{J}$ over $\mathcal{O}_{K,S}$ which is analogous to the Abel-Jacobi map from a proper curve of positive genus to its Jacobian.

While Chabauty's method (generally) requires that $\operatorname{rank} \mathcal{J}(\mathcal{O}_{K,S}) \leq \dim \mathcal{J}_K - 1$ in order to compute a finite subset p-adic points on $\mathcal{C}$ containing $\mathcal{C}(\mathcal{O}_{K,S})$, Chabauty's method for restriction of scalars computes a subset $\Sigma_{\mathcal{C}}$ of p-adic points of $\operatorname{Res}\mathcal{C}$ which contains $\mathcal{C}(\mathcal{O}_{K,S})$. Naïvely, one might expect that $\Sigma_{\mathcal{C}}$ is finite whenever the RoS inequality $\operatorname{rank} \mathcal{J}(\mathcal{O}_{K,S}) \leq [K : \mathbb{Q}](\dim \mathcal{J}_K - 1)$ is satisfied. However, even if this inequality is satisfied, $\Sigma_{\mathcal{C}}$ can be infinite for geometric reasons, which we call base change obstructions and full Prym obstructions.

When attempting to compute the $\mathcal{O}_{K,S}$-points of $\mathcal{C} = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$, we show that $\mathcal{C}$ can be replaced with a suitable descent set $\mathscr{D}$ of covers $\mathcal{D}$, such that for each $\mathcal{D} \in \mathscr{D}$ the RoS Chabauty inequality holds for $\mathcal{D}$. Although we do not prove that the $\Sigma_{\mathcal{D}}$ are finite, we do prove that the $\Sigma_{\mathcal{D}}$ are not forced to be infinite for any of the known geometric reasons. In other words, there are no base change or full Prym obstructions to RoS Chabauty for $\mathcal{D}$.

We also give several examples of the method. For instance, when both 3 splits completely in K and $[K : \mathbb{Q}]$ is prime to 3 we show that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K) = \emptyset$. We also give new proofs that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ is finite for several classes of number fields K of low degree. These results represent the first infinite class of cases where Chabauty's method for restrictions of scalars is proved to succeed where the classical Chabauty's method does not.

Thesis Supervisor: Bjorn Poonen
Title: Claude Shannon Professor of Mathematics

Acknowledgments

First and foremost, I would like to thank my advisor, Bjorn Poonen. Bjorn, it is no exaggeration to say that this thesis would not exist without you. Over the past five years, I have learned so much from you, both about mathematics and how to be a good mentor. Thank you for your many patient hours answering my mathematical questions, for sharing your ideas, and for helping me to refine my own ideas. Thank you for letters of recommendation (too often at the last minute), for your mathematical guidance, and for giving me the freedom and support to explore and grow both mathematically and personally. And thank you for believing in me even when I had trouble believing in myself. I would not be the mathematician that I am without you. Among the many things I will miss about MIT, our weekly meetings to discuss my progress will be near the top of the list.

Next and equally much, I would like to thank my parents, Jean Farrington and George Triantafillou. Mom and Dad, thank you so much for being there for me throughout my life. Thank you for answering my first-grade request for extra math homework and for always nurturing my love of learning. Thank you for always being there with wise advice and a listening ear when I needed it. Thank you for understanding when the demands of graduate school kept me from spending as much time with you (or even on the phone with you) as we would all have liked. Thank you for listening and caring about what I do, even when you don't understand most of what I'm talking about. I couldn't have asked for better parents. I love both of you to the moon and back. Thank you also to all the rest of my family, especially my Yiayia and my aunt Maryrose. You have all been a tremendous source of support.

I have many mathematical mentors to thank. Thank you to my committee members, Wei Zhang and Andrew Sutherland, for taking the time to read my thesis and for your thoughtful questions. Thank you to Jennifer Balakrishnan and Michael Stoll for introducing me to Chabauty's method as a topic of active research. Thank you to Henry Cohn, for teaching me about sphere packing and how ideas from pure and applied mathematics can work together. Thank you to Stephen DeBacker, Steven

Miller, and all of my other undergraduate mentors, for nurturing my love of mathematics and for doing the same for many others. Without your mentorship, I expect my career path would have been very different. And thank you to John Voight, David Zurieck-Brown, Joe Rabinoff, Barry Mazur, Tim Dokchitser, Noam Elkies, David Vogan, George Lustig, Edgar Costa, Adam Morgan, all of those listed above, and many more for helpful mathematical conversations, and for their belief in me in graduate school.

My fellow math students have been a huge source of support and knowledge thoughout my time in graduate school. Padma Srinivasan, thank you for always being there to remind me of the sense of wonder that mathematics inspires. Isabel Vogt, thank you for pushing from the very start of graduate school to learn more mathematics. You set a great example, helping me to overcome burn-out and to keep learning as I started graduate school. Ruthi Hortsch, thank you for convincing me that MIT would be a good fit for me for graduate school. Renee Bell, Vishal Arul, and Borys Kadets, thank you for listening to my frequent rants, both mathematical and non-mathematical. I realize I must have often been a distraction in the office - I hope it was more commonly welcome than unwelcome. To those above, Alex Best, Atticus Christiansen, Alex Smith, Sachi Hashimoto, and many others, thank you for many helpful mathematical conversations at tea, at conferences, at STAGE, and more. Thank you to Amelia Perry, who left us too soon. And to all of those above, Lynnelle Ye, Kevin Sackel, Paul Gallagher, Hood Chatham, Geoff Smith, Gwen McKinley, David Rolnick, and many more, thank you for your friendship and for helping me to stay sane throughout graduate school.

The Sidney-Pacific Graduate Community did so much to help me maintain balance in graduate school. Thank you to Rachael Harding and Sherry Hall for introducing me to the community. Thank you to Dan Kolodrubetz and Fabian Kozynski for inspiring me to be the best coffee hour chair I could be and for showing me how I could give back to the community. Thank you to Boris Braverman and Ahmed Helal, for your sage advice and for setting an incredible example of how to support a community, finish a PhD and have a great time while doing it. Thank you to

Jenny Wang for holding me accountable and making sure I did what was best for the community. Thank you to Andrea Carney for always being willing to listen. Thank you to Alberto Rodriguez, Nuria Jane, Julie Shah, Neel Shah, and Brian Ward for their mentorship and support. Thank you to Eric Stansifer, Leo Barlach, Jit Hin Tan, Hsin-Yu Lai, Zelda Mariet, Fabian, and Ahmed, for many great hours spent on board games and puzzle hunts. Thank you to the rest of my SPEC, Greg Izatt, Ben Yuan, Akshay Mohan, and Richard Swartwout, for being a great team. It was a real pleasure to work with all of you, pulling each other along when we needed it, and I would do it again in a heartbeat. Thank you to all of our officers who turned our ideas into reality and to the SPECs, Trustees, and officers throughout SP's history who created this great community. And thank you again to Kevin and Greg for being great roommates and friends. I hope we'll all cross paths often in the future.

Thank you to Peng Shi, Annie Chen, Sam Elder, Grace Goon, and many more from the Graduate Christian Fellowship, for showing me how to pair a life of science and faith. Thank you to Peter Su, Sarah Goodman, Daniel Curtis, Lisa Guay, Orpheus Chatzivasileiou, Malvika Verma, and many more for many good times and much good work in service of the graduate community on the Graduate Student Council. Thank you to Ian Waitz and Jag Patel and many other MIT administrators for your mentorship and support of student advocacy. And thank you to those I have forgotten or omitted for space. I have been blessed in graduate school and life to have many wonderful mentors and friends. I feel like I could have filled a novel with the names of those who have made a lasting positive impression on my life. I hope those deserving folks that I have omitted here will forgive me for the omission and know that I value them.

Contents

Chapter 1

Introduction

1.1 Overview of methods and results

Let X be a smooth, proper, geometrically integral curve over a number field K. When the genus g of X is at least 2, Faltings' theorem says that the set $X(K)$ is finite. Unfortunately, Faltings' theorem is *ineffective*. While it is possible to extract an (extremely large) bound on $\#X(K)$ from a careful analysis of Faltings' method, it seems implausible that Faltings' approach could be used to *compute* the set $X(K)$.

Fortunately, for many curves X, there is another way. Building on earlier work of Chabauty, Coleman proved:

Theorem 1.1.1 ([Col85, Theorem 4])**.** *Suppose that $K = \mathbb{Q}$, that $g > 1$, and that p is a prime of good reduction for X with $p > 2g$. Let J be the Jacobian of X. Suppose that* $\operatorname{rank} J(\mathbb{Q}) \leq g - 1$. *Then*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2)\,. \tag{1.1.2}$$

The great strength of the Chabauty–Coleman method over Faltings' proof is that the bound (1.1.2) is sometimes sharp [GG93], in which case Theorem 1.1.1 can be used to compute $X(\mathbb{Q})$. Even when (1.1.2) is not sharp, the method computes (to any desired p-adic precision) a finite subset of $X(\mathbb{Q}_p)$ which contains the set $X(\mathbb{Q})$. In combination with tools like the Mordell–Weil sieve, it is often possible to compute

the set $X(\mathbb{Q})$ exactly. For instance, Stoll has used this approach to compute $X(\mathbb{Q})$ for all 46,436 curves with Jacobian of rank 1 in a database of 'small' genus 2 curves [Sto09].

For the sake of exposition, we now give a high-level overview of the Chabauty–Coleman method. We give a more detailed exposition (in a more general context) in Chapter 3.

Suppose that $X(\mathbb{Q}) \neq \emptyset$ so that the Abel–Jacobi map $j : X \hookrightarrow J$ is defined over $\mathbb{Q}$. From the commutative diagram

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

we see that inside $J(\mathbb{Q}_p)$,

$$X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p) \cap J(\mathbb{Q})\,.$$

Considering $J(\mathbb{Q}_p)$ as a p-adic Lie group, the (p-adic) closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ is a p-adic Lie group of some dimension $\rho \leq \operatorname{rank} J(\mathbb{Q})$.

Now, $J(\mathbb{Q}_p)$ has dimension g as a p-adic Lie group. For dimension-counting reasons, it is reasonable to hope that if $\rho \leq g-1$ then the intersection

$$X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

is finite. Indeed, this is what Chabauty proved. Later, Coleman developed a theory of p-adic integration. Using this theory in Chabauty's setup, Coleman showed how to compute the set $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ explicitly as the vanishing locus of a p-adic analytic function on $X(\mathbb{Q}_p)$. Such a function is given locally by single-variable p-adic power series, so methods from the theory of Newton polygons can be used to bound the size of its set of zeroes.

The restriction $K = \mathbb{Q}$ in Theorem 1.1.1 is not serious. So long as $\operatorname{rank} J(K) \leq g-1$, Coleman's result generalizes to bound $\#X(K)$ for any number field K. Replacing the Jacobian with a generalized Jacobian, Theorem 1.1.1 can also be generalized to bound the set of S-integral points on an S-integral model of a punctured curve. (See

Chapter 3.)

Unfortunately, the restriction rank $J(\mathbb{Q}) \leq g-1$ (or more precisely $\rho \leq g-1$) is much more serious.

Several methods have been proposed to extend the method of Chabauty-Coleman to handle the case where rank $J(K) \geq g$. In all cases, the idea is to replace the Jacobian with something 'larger.'

We give three examples:

1. *Restriction of Scalars Chabauty:* If K is a number field of degree $d > 1$, replace X and J with the Weil restrictions of scalars $\mathrm{Res}_{K/\mathbb{Q}} X$ and $\mathrm{Res}_{K/\mathbb{Q}} J$.

2. *Descent + Chabauty:* Using the theory of descent, given any isogeny from an abelian variety to J, it it possible to construct a finite set of covering curves

$$\mathscr{D} := \{f_i : X_i \to X\}$$

such that $X(K) = \bigcup_i (f_i(X_i(K)))$. Then apply Chabauty's method to each curve X_i.

3. *Non-abelian Chabauty-Kim:* Replace J with a "Selmer variety" constructed from a quotient of the pro-unipotent étale fundamental group of X.

In this thesis, we study the power of the first two approaches, especially in the context of computing S-integral points on $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$. Although it is not the focus of our study, the Chabauty-Kim approach plays an important motivating role for this project, as we discuss at the end of Section 1.4.

Write $d = [K : \mathbb{Q}]$.

In the method of restriction of scalars Chabauty (or *RoS Chabauty* for short), attributed by Siksek to a talk of Wetherell [Sik13, Wet00], one replaces the inclusion

$$X(K) \subseteq X(K_\mathfrak{p}) \cap \overline{J(K)}$$

inside $J(K_{\mathfrak{p}})$ with the inclusion

$$X(K) = (\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}) \subseteq (\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})} \tag{1.1.3}$$

inside the gd-dimensional p-adic Lie group $(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q}_p)$. In order to prove that $X(K)$ is finite, we aim to show that the right-hand side is finite.

Unfortunately, the right-hand side of (1.1.3) can have positive-dimension as a naïve p-adic analytic variety. In particular, it is infinite if this happens. So we wish to understand when this intersection is finite.

As a first pass, we note that if this intersection is finite, it will typically have expected dimension less than or equal to zero. More precisely, taking dimensions of p-adic analytic varieties, we must have

$$\dim(\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}_p) + \dim \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})} \leq \dim(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q}_p)\,,$$

or equivalently

$$\dim \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})} \leq d(g-1)\,. \tag{1.1.4}$$

Since

$$\dim \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})} \leq \mathrm{rank}(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q}) = \mathrm{rank}\, J(K)\,,$$

we see that (1.1.4) holds whenever

$$\mathrm{rank}\, J(K) \leq d(g-1)\,. \tag{1.1.5}$$

If (1.1.5) is true, we say that *the RoS Chabauty inequality holds for* X. Informally, the RoS Chabauty inequality holds for X exactly when we 'expect for dimension reasons' that RoS Chabauty will prove that $X(K)$ is finite.

As with Chabauty's method, when the RoS Chabauty inequality holds for X, the intersection $(\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})}$ can be computed as the vanishing set of several d-variable p-adic analytic functions, locally expressible as p-adic power series

in d variables. Within each residue disc, the number of isolated $\mathbb{C}_p$-valued points in this vanishing locus is finite.

In contrast to what happens in the Chabauty-Coleman method, the set

$$(\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})}$$

may not be zero-dimensional even if the RoS Chabauty inequality holds for X. In particular, this set may be infinite even when the RoS Chabauty inequality holds.

Indeed, if this set were always finite, we could attempt to prove all of Faltings' Theorem as follows:

1. Given $X/\mathbb{Q}$ of genus g with Jacobian J, apply Chabauty's theorem if possible.

2. Otherwise, produce a sequence of number fields K_i of degree tending to infinity with $J(\mathbb{Q}) = J(K_i)$. (It is likely, although not proven that such K_i can be found.)

3. Then, for some $K := K_i$, the base change X_K satisfies the RoS Chabauty inequality. Apply RoS Chabauty to show that $X(K)$ is finite.

4. Conclude that $X(\mathbb{Q}) \subset X(K)$ is also finite.

Unfortunately, there is a problem with this argument. In this situation, the set

$$(\mathrm{Res}_{K/\mathbb{Q}}\, X_K)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})} = X(K \otimes \mathbb{Q}_p) \cap \overline{J(K)} \text{ in } J(K \otimes \mathbb{Q}_p)$$

will contain a subset isomorphic to $X(\mathbb{Q}_p)$. Here, he failure of RoS Chabauty for X_K is a sort of certificate of the failure of the Chabauty-Coleman method to compute the set $X(\mathbb{Q})$. This principle applies more broadly: If there is some $\kappa \subset K$ and a curve Y/κ such that both

1. $Y_K \cong X$ and

2. $(\mathrm{Res}_{\kappa/\mathbb{Q}}\, Y)(\mathbb{Q}) \cap \overline{(\mathrm{Res}_{\kappa/\mathbb{Q}}\, J_Y)(\mathbb{Q})}$ is infinite

then $(\mathrm{Res}_{K/\mathbb{Q}} X)(\mathbb{Q}) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}} J_X)(\mathbb{Q})}$ will be infinite as well. When this occurs we say that X has a *base change obstruction* to RoS Chabauty. See Section 4.2 for a more detailed discussion.

Recently, [Dog19] pointed out another geometric situation which can force $(\mathrm{Res}_{K/\mathbb{Q}} X)(\mathbb{Q}) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}} J_X)(\mathbb{Q})}$ to be infinite. If there is a curve Y/K and a morphism $f : X \to Y$ such that

1. $\overline{(\mathrm{Res}_{K/\mathbb{Q}} J_X/f^*(J_Y))(\mathbb{Q})}$ has finite index in $(\mathrm{Res}_{K/\mathbb{Q}} J_X/f^*(J_Y))(\mathbb{Q}_p)$ and
2. $(\mathrm{Res}_{\kappa/\mathbb{Q}} Y)(\mathbb{Q}) \cap \overline{(\mathrm{Res}_{\kappa/\mathbb{Q}} J_Y)(\mathbb{Q})}$ is infinite

then $(\mathrm{Res}_{K/\mathbb{Q}} X)(\mathbb{Q}) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}} J_X)(\mathbb{Q})}$ will be infinite as well. When this occurs we say that X has a *full Prym obstruction* to RoS Chabauty. See Section 4.3 for a more detailed discussion.

It seems natural to hope that RoS Chabuaty can prove that $X(K)$ is finite whenever X satisfies the RoS Chabauty inequality and has no base change obstructions or full Prym obstructions. While there are no known counterexamples, the hope seems extremely difficult to prove.

While general results may be out of range of current technology, RoS Chabauty is useful in particular examples. Siksek [Sik13] gives a sufficient criterion to determine if the intersection

$$(\mathrm{Res}_{K/\mathbb{Q}} X_K)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}} J)(\mathbb{Q})}$$

is finite and uses it to compute the set of $\mathbb{Q}(\sqrt[3]{2})$-points on several genus 2 curves.

Let S be a finite set of finite places of K and let $O_{K,S}$ be the ring of S-integers of K. In this work, we develop the method of RoS Chabauty to compute integral points on curves, in particular to compute the set $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$. This is the set of solutions to the *S-unit equation*, i.e., the set

$$\{(x, y) \in \mathcal{O}_{K,S}^\times \times \mathcal{O}_{K,S}^\times : x + y = 1\}.$$

The S-unit equation is a classical and well-studied number theoretic object. Work of Mahler [Mah33] using diophantine approximation in the style of Siegel and Thue

gave the first proof that this set is finite. The theory of linear forms in logarithms can be used to give explicit bounds on the size of the set. Let r_1 and r_2 be the number of real embeddings and conjugate pairs of complex embeddings of K. Then, the current state-of-the-art upper bound, due to Evertse [Eve84], is $3 \cdot 7^{2\#S+3r_1+4r_2}$. This theory has been developed to give efficient algorithms, implemented in Sage, to compute solutions to S-unit equations [AKM+18, Sma99]. We give a more detailed review of results on S-unit equations and their application in Section 1.4.

Although the S-unit equation has been well-studied, it remains an important testing ground for new approaches to reprove Faltings' Theorem. Both Kim's nonabelian Chabauty program [Kim05] and Lawrence and Venkatesh's recent p-adic proof of Faltings' Theorem [LV18] first found success in proving finiteness of solutions to an S-unit equation. And in both cases, studying the example of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ helped to shine a light on the full theory.

We hope that our study of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ will do the same for RoS Chabauty.

While RoS Chabauty alone is not enough to solve the S-unit equation, we are able to use the method (and related ideas) to recover several finiteness results for unit-equations with stronger bounds than are given by Evertse's more general theorem.

For example, we prove

Theorem 6.3.1. *Suppose that* $[K : \mathbb{Q}]$ *is not divisible by* 3 *and that* 3 *splits completely in* K. *Then there is no pair* $x, y \in \mathcal{O}_K^\times$ *such that* $x + y = 1$. *Equivalently,*

$$(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K) = \emptyset.$$

While Theorem 6.3.1 holds independent of the degree of the field, our other results require strong assumptions on the size of the field. In a series of examples (Corollaries/Propositions 6.2.1, 6.2.3, 6.2.4, and 6.2.5) we show that if K is a real quadratic field, mixed cubic field, or totally complex quartic field, or a mixed quartic field with a totally real subfield, then

$$\#(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K) < \infty\,. \tag{1.1.6}$$

This result provides the first infinite collection of examples of fields for which RoS Chabauty has been proven to show finiteness of integral or rational points on a curve but a straightforward application of classical Chabauty cannot prove finiteness.

Notably, for quadratic fields, the proof is sufficiently uniform in the field that it allows us to recover the elementary fact that there are finitely many solutions to the unit equation in the union of all quadratic fields [Nag64]. (In fact, there are exactly 8 such solutions!) Dan-Cohen and Wewers [DCW15] also recover a version of this result when developing explicit algorithms for computing S-unit equations based on Kim's nonabelian Chabauty.

Having discussed RoS Chabauty, we now turn to our second ingredient, the method of descent. Before stating our results, we need a definition

Definition 2.3.1. A *descent set* for $(\mathcal{C}, \mathcal{O}_{K,S})$ is a finite set $\mathscr{D}$ of clearance hole curves $\mathcal{D}$ over $\mathcal{O}_{K,S}$ (see Definition 2.1.1) equipped with morphisms $f_{\mathcal{D}} : \mathcal{D} \to \mathcal{C}$ such that

$$\mathcal{C}(\mathcal{O}_{K,S}) \subseteq \bigcup_{\mathcal{D} \in \mathscr{D}} f_{\mathcal{D}}(\mathcal{D}(\mathcal{O}_{K,S}))\,.$$

If, moreover, the generic fibers $\mathcal{D}_K$ of all of the curves $\mathcal{D}$ are punctured genus 0 curves, we say that $\mathscr{D}$ is a genus 0 descent set.

We make an analogous definition for sets of covering curves of a proper curve X over K.

Methods for constructing descent sets are well-established. We discuss the method of descent in detail in Section 2.3.

If X has genus at least 2, the Riemann-Hurwitz formula implies that the curves X_i in a descent set $\mathscr{D}$ for X will have higher genus than X. Alternatively, if $\mathcal{X}$ is a punctured genus zero curve and $\mathscr{D}$ is a genus 0 descent set, the curves $\mathcal{X}_i$ will have more punctures than $\mathcal{X}$.

As in section 2.2, define the generalized Jacobian of a punctured curve $\mathcal{X}$ to be a certain $\mathcal{O}_{K,S}$-model for the generalized Jacobian of the projective closure of the special fiber of $\mathcal{X}$ with modulus equal to the divisor consisting of the sum of the punctures, each with multiplicity 1.

Then, in either case, the dimension of the (generalized) Jacobian of the $\mathcal{X}_i$ will be higher than the dimension of the (generalized) Jacobian of the $\mathcal{X}$. If the ranks of the generalized Jacobians do not grow as quickly as the dimensions, one could attempt to apply Chabauty's method to the curves $\mathcal{X}_i$ and use this to determine the set $\mathcal{X}(\mathcal{O}_{K,S})$.

When $K = \mathbb{Q}$ and S is arbitrary, Poonen observed in a July 2005 email to Kim that one can use this approach to prove that

$$(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{\mathbb{Q},S})$$

is finite. The following result shows that with only descent by genus 0 covers and the classical Chabauty-Chabauty method (as described in Chapter 3), one cannot do much better.

Corollary 5.1.3. *Suppose that we are* not *in the following situations: (i) $K = \mathbb{Q}$, (ii) K a real quadratic field and $\#S \leq 1$, (iii) K an imaginary quadratic or totally real cubic field and $\#S = 0$.*

Then the classical Chabauty inequality (3.2.6) *is not satisfied by any descent set consisting of genus zero covers of $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$. Under Leopoldt's Conjecture, this implies that the combination of classical Chabauty and descent by genus zero covers is insufficient to prove that*

$$(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$$

is finite.

While the classical Chabauty inequality is never satisfied by descent sets consisting of punctured genus zero covers of $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$, it is not difficult to construct such descent sets where the RoS Chabauty inequality is satisfied. So, it is reasonable to hope that the method of RoS Chabauty with descent could be used to prove that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$ is finite.

It is difficult to prove in full generality when the (analogue of the) right-hand side of (1.1.3) is finite (so that RoS Chabauty will suffice to prove finiteness of rational

points). However, in all *known* cases where the right-hand side is infinite, the curve $\mathcal{C}$, this infinitude can be attributed to a combination of *base change obstructions* (see Section 4.2) and *full Prym obstructions* (see Section 4.3.)

In several circumstances, we prove that it is possible to avoid base change obstructions and Prym obstructions using descent.

To state our results, we need a definition. We say that a number field κ is CM if κ is totally complex and is a degree 2 extension of a totally real number field.

Theorem 5.2.2. *The punctured curve $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\}$ has a descent set $\mathscr{D}$ consisting of genus 0 sound clearance hole curves $\mathcal{D} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma_{\mathcal{D}}$ (see Definition 2.1.1) such that*

I. the RoS Chabauty inequality

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}) \leq d(\#\Gamma_{\mathcal{D}}(\overline{K}) - 2). \tag{5.2.2}$$

holds for all $\mathcal{D} \in \mathscr{D}$.

II. Under the further assumption that K does not contain a CM field, $\mathscr{D}$ can be chosen so that there is no base change obstruction to RoS Chabauty for $(\mathcal{D}, \mathcal{O}_{K,S})$ for any $\mathcal{D} \in \mathscr{D}$.

Theorem 5.2.4. *Let K be a number field which does not contain a CM subfield and let q be a prime. Fix an $\alpha \in K$ which is not a qth power in K and let*

$$\mathcal{C} := \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{x \in K : x^q - \alpha = 0\}.$$

For q sufficiently large (depending only on K and S), there is no full Prym obstruction to RoS Chabauty for $\mathcal{C}$. Moreover, if $\mathcal{C}$ is the base change of some curve $\mathcal{D}$, there is no full Prym obstruction to RoS Chabauty for $\mathcal{D}$.

Also, there is no base change obstruction to RoS Chabauty for $\mathcal{C}$.

While Theorems 5.2.2 and 5.2.4 may not give much new information *about solutions to the S-unit equation*, we emphasize that our primary goal in this thesis is not to prove new bounds on the number of solutions the S-unit equation, but rather

to understand the power of RoS Chabauty in combination with descent. We focus on genus 0 covers of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ because studying the ranks of their Jacobians is possible. On the other hand, understanding ranks of Jacobians of higher genus curves seems well beyond the range of current mathematical technology. Our work also helps to clarify what can be said about the S-unit equation using purely p-adic methods. It would be interesting to combine our ideas with stronger results from the theory of linear forms in p-adic logarithms to understand this more completely.

1.2 Chabauty in dimension greater than 1: History

Although Chabauty's method is traditionally discussed in context of rational points on curves, the high-level idea of the method also applies to more general projective varieties V equipped with a morphism $j : V \to A$ to an abelian variety A such that $\dim(V) + \operatorname{rank} A(K) \leq \dim(A)$ and such that we understand the rational points of the fibers of j. Of course, the restriction that we understand the rational points of the fiber of j rules out many classes of variety V (for instance K3 surfaces, which have only constant maps to abelian varieties).

Both *restrictions of scalars* of curves and *symmetric powers* of curves are examples of varieties V which are well-suited to Chabauty's method. In this section, we briefly summarize past results in these settings. Given a curve $X/\mathbb{Q}$ and a degree d extension K of $\mathbb{Q}$, we also compare the application of Chabauty's method to $\operatorname{Sym}^d X$ and $\operatorname{Res}_{K/\mathbb{Q}} X$.

1.2.1 RoS Chabauty and variants

In this thesis, we focus on the variant of Chabauty's method applied to the restriction of scalars of a curve.

In this situation, [Sik13] gives an explicit criterion to determine if several multivariable p-adic power series have a single zero in a residue disc. For several genus 2 curves X, he is able to use this criterion and RoS Chabauty to compute the set $X(\mathbb{Q}(\sqrt[3]{2}))$. This allows him to determine the set of $(x, y, z) \in \mathbb{Z}^3$ such that $x^2 + y^3 = z^{10}$. Siksek

attributes the idea to a talk of [Wet00], where the set of $\mathbb{Q}[i]$-points on a bielliptic curve was computed. Unfortunately, the results of [Wet00] have never been published, even as a preprint.

Given number fields $K \subset L$ and curves B/K and C/L with a non-constant morphism $h\colon C \to B_L$, [FT15] uses related ideas (involving both restriction of scalars and Chabauty-like techniques) to bound/compute the subset of $P \in C(L)$ such that $h(P) \in B(K)$.

1.2.2 Comparison with symmetric powers Chabauty

Several others [Sik09], [Par16], [Kla93], [GM17] have considered a similar variant of Chabauty's method that applies to symmetric powers of a curve.

Recall that RoS Chabauty starts with a variety X over a degree d number field K and attempts to bound the set

$$(\mathrm{Res}_{K/\mathbb{Q}}\, X)(\mathbb{Q}_p) \cap \overline{(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q})}$$

inside of $(\mathrm{Res}_{K/\mathbb{Q}}\, J)(\mathbb{Q}_p)$, in order to compute $X(K)$. We 'expect' that RoS Chabauty will prove that $X(K)$ is finite when $\operatorname{rank} J(K) \leq d(g-1)$.

Similarly, symmetric powers Chabauty starts with a curve X defined over $\mathbb{Q}$ (say with a rational point $P \in X(\mathbb{Q})$.) The Abel-Jacobi map $X \to J$ extends to a map $j : \mathrm{Sym}^d X \to J$. Geometrically, the fibers of j are projective spaces whose dimensions are well-understood. In particular, we understand their rational points well. Symmetric powers Chabauty attempts to bound the set

$$j(\mathrm{Sym}^d X)(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

inside $J(\mathbb{Q}_p)$ in order to bound the number of fibers of j which contain rational points. One might hope to use this bound to bound $\#(\mathrm{Sym}^d X)(\mathbb{Q}_p)$.

Unfortunately, $(\mathrm{Sym}^d X)(\mathbb{Q})$ is frequently infinite. For example, X has a morphism of degree $\leq d$ to $\mathbb{P}^1$ or an elliptic curve E of positive rank then $(\mathrm{Sym}^d X)(\mathbb{Q})$

will be infinite.

if d is greater than either the gonality of X, it will contain a copy of the projective line. If d is greater than the degree of a map from X to an elliptic curve of positive rank. Nevertheless, if one excludes a *special set* $\mathcal{S}(\mathrm{Sym}^d X)$, we 'expect' that symmetric power Chabauty will prove that

$$(\mathrm{Sym}^d X \smallsetminus \mathcal{S}(\mathrm{Sym}^d X))(\mathbb{Q})$$

is finite when $\operatorname{rank} J(\mathbb{Q}) \leq g - d - 1$. Following similar lines to our development of RoS Chabauty, it should be possible to adapt Chabauty's method for symmetric powers to study integral points on symmetric powers of affine curves.

For $X/\mathbb{Q}$, symmetric powers Chabauty may seem strictly superior to RoS Chabauty for computing $X(K)$ when both methods apply. After all, it gives information about $X(K)$ for *all* étale $\mathbb{Q}$-algebras of degree d simultaneously. Moreover, symmetric powers Chabauty may apply even if the RoS Chabauty inequality is not satisfied.

Despite these flaws, RoS Chabauty still provides additional value. First, RoS Chabauty gives access to the K-points in the special set. For example, in the case where $[K : \mathbb{Q}] = 2$ and X is a smooth proper hyperelliptic curve with affine patch $y^2 = f(x)$, RoS Chabauty gives information about how many points with x-coordinate in $\mathbb{Q}$ belong to $X(K)$. Symmetric power Chabauty has nothing to say about this, since *all* such points are defined over *some* quadratic extension.

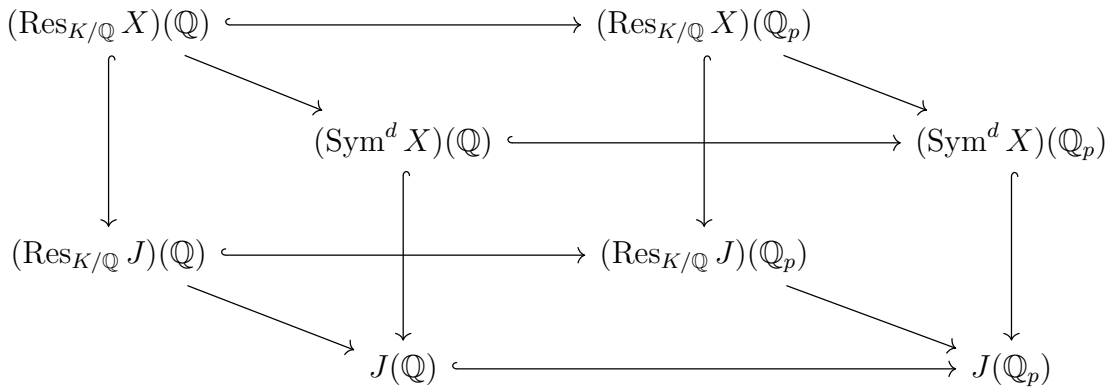
Second, RoS Chabauty may apply even when symmetric power Chabauty does not.

Finally, RoS Chabauty includes symmetric power Chabauty as a special case in the following sense. Fix a nice curve $X/\mathbb{Q}$ and let J be the Jacobian of X.

For any number field K of degree d, there is a norm map $\mathrm{Nm} : \mathrm{Res}_{K/\mathbb{Q}} J_K \to J$. Let $j : \mathrm{Res}_{K/\mathbb{Q}} X_K \to \mathrm{Res}_{K/\mathbb{Q}} J_K$ be the map induced by the Abel-Jacobi map.

Now, we claim that the composition $\mathrm{Nm} \circ j$ factors through $\mathrm{Sym}^d X$. Indeed, given a $\mathbb{Q}$-algebra A, any $P \in (\mathrm{Res}_{K/\mathbb{Q}} X)(A)$ maps to a d-tuple of 'conjugate' elements of $X(K \otimes A)$, or equivalently to an element of $(\mathrm{Sym}^d X)(A)$. The Abel-Jacobi map from

$(\mathrm{Sym}^d X)(A) \to J(A)$ is just the sum of the images of the elements in the d-tuple. The composition clearly agrees with $\mathrm{Nm} \circ j$. As a result, there is a commutative cube



Inside $J(\mathbb{Q}_p)$, we have

$$\overline{J(\mathbb{Q})} \cap (\mathrm{Res}_{K/\mathbb{Q}} X)(\mathbb{Q}_p) \subseteq \overline{J(\mathbb{Q})} \cap (\mathrm{Sym}^d X)(\mathbb{Q}_p)\,.$$

In particular, this implies that the bound from RoS Chabauty on $\#X(K)$ will never be worse than the bound which could be extracted naïvely from the result of symmetric powers Chabauty.

This observation can be interpreted as saying that symmetric powers Chabauty is a version of RoS Chabauty that holds uniformly for every base change of X to étale algebra K with $d = [K : \mathbb{Q}]$. We will see a further example of this when we consider $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ for K a (real) quadratic field in section 6.2.1.

Having introduced and compared RoS Chabauty and symmetric powers Chabauty, we now survey results from both approaches.

The first result on symmetric powers Chabauty appears in [Kla93].

In [Sik09], Siksek proved a sufficient criterion for a residue disk to contain a single rational point, computed $(\mathrm{Sym}^2 X)(\mathbb{Q})$ in two explicit examples, and a hypothesis on the gonality of X required in [Kla93].

Park developed this work further in [Par14] and [Par16], proving a bound on $\#(\mathrm{Sym}^d X \smallsetminus \mathcal{S}(\mathrm{Sym}^d X))(\mathbb{Q})$ depending only on g, d, and a prime p of good reduction, under a difficult-to-verify technical assumption on X. Unfortunately, there is an error in the proof of [Par16, Theorem 4.15 and Theorem 4.18] (and there are counter-

examples to the statements.)

Most recently, Gunther and Morrow [GM17] further refined [Par16] and combined this work with results from [BG13] on average ranks of hyperelliptic curves. For a positive proportion of genus g hyperelliptic curves over $\mathbb{Q}$ with a rational Weierstrass point, they give an explicit bound for the number of quadratic points not obtained by pulling back points of $\mathbb{P}^1(\mathbb{Q})$. Unfortunately, their bounds appear to depend on [Par16, Theorem 4.15 and Theorem 4.18].

1.3 Other improvements to Chabauty's method

Many other authors have considered variants of Chabauty's method in an attempt to compute the K or $\mathcal{O}_{K,S}$ points on curves. We give a brief survey of some such results here. Although a comprehensive survey would run very long, we hope this section will serve as a taste for what can be done with Chabauty's method and will encourage the reader to explore the area further.

Lorenzini and Tucker showed how to adapt Coleman's method to a prime p of bad reduction (as in [LT02, Corollary 1.11]). Let $\mathcal{X}$ to be a minimal proper regular model for X over $\mathbb{Z}_p$, and let $\#\mathcal{X}^{\mathrm{sm.}}_{\mathbb{F}_p}$ be the smooth locus of its special fiber. When $\operatorname{rank} J(\mathbb{Q}) < g$, they show that

$$\#X(\mathbb{Q}) \leq \#\mathcal{X}^{\mathrm{sm.}}_{\mathbb{F}_p}(\mathbb{F}_p) + (2g-2)\,.$$

Notably, the bounds of [Col85] and [LT02] depend on p. A priori, the smallest bound obtained as p varies may be quite large if all of the small primes are primes of bad reduction for X.

Some recent developments in Chabauty's method involve *uniform* bounds on rational points on curves satisfying a more restrictive rank hypothesis than the rank hypothesis appearing in classical Chabauty.

The first such uniform bound appears in [Sto19] and applies to hyperelliptic curves X whose Jacobian J satisfies with $\operatorname{rank} J(\mathbb{Q}) \leq g-3$. Perhaps the most significant

result in this direction is

Theorem 1.3.1 ([KRZB16]). *Let X be any smooth curve of genus g and let $r = \operatorname{rank} J(\mathbb{Q})$. Suppose $r \leq g-3$. Then*

$$\#X(\mathbb{Q}) \leq 84g^2 - 98g + 28\,.$$

It is also known that in certain families, 'most' curves have *very* few rational points. An argument involving equidistribution results on 2-Selmer groups from [BG13] leads to

Theorem 1.3.2 ([PS14, Theorem 10.6]). *For $g > 1$, the lower density of degree $2g+1$ hyperelliptic curves having just one rational point (namely, the point at infinity) is at least $1 - (12g+20)2^{-g}$. In particular, as g tends to infinity, the lower density of degree $2g+1$ hyperelliptic curves having just one rational point tends to 1.*

An analogous result for even degree hyperelliptic curves is proved in [BG13].

Other results have focused on making it easier to apply the Chabauty-Coleman method in practice. For instance, one usually assumes that generators for (a finite index subgroup of) $J(\mathbb{Q})$ are known when applying the method. In practice, it can be difficult to prove that a proposed generating set is complete. Stoll [Sto17] shows a way to get around computing generators of the Mordell–Weil group by replacing the Jacobian with a p–Selmer set.

Yet other results have attempted to relax the restriction that $\operatorname{rank} J(\mathbb{Q}) \leq g-1$. These methods, including *elliptic curve Chabauty* as developed in [FW99] and [Bru03], usually apply descent in some way.

1.3.1 Kim's nonabelian Chabauty

Kim has also proposed a vast generalization of Chabauty's method, which replaces $\overline{J(\mathbb{Q})}$ and $J(\mathbb{Q}_p)$ with a tower of global and local *Selmer varieties*. These Selmer varieties, constructed using the pro-unipotent étale fundamental group of X carry

the structure of algebraic varieties over $\mathbb{Q}_p$. The first level of the tower (essentially) specializes to Chabauty's original method.

As with classical Chabauty, the Chabauty-Kim method proves $X(\mathbb{Q})$ is finite when the dimension of the global Selmer variety (corresponding to $\dim \overline{J(\mathbb{Q})}$) is less than the dimension of the local Selmer variety (corresponding to $\dim J(\mathbb{Q}_p)$). As one goes up the tower, the dimensions of both varieties grow. When the dimension of the local Selmer variety grows faster than the dimension of the global Selmer variety (asymptotically), Kim's method shows that $X(K)$ is finite. Kim's method can also be used to show that the set of $\mathcal{O}_{K,S}$ points on an affine curve is finite under similar conditions.

Kim's method has been applied to give new proofs of finiteness of integral points for several classes of curves. [Kim05] uses this approach to show that $\mathbb{P}^1(\mathcal{O}_{\mathbb{Q},S})$ is finite. [CK10] uses multivariable Iwasawa theory to prove that $X(\mathbb{Q})$ is finite in the case where X is a curve of genus at least 2 whose Jacobian is isogenous to a product of abelian varieties with complex multiplication. [EH17] builds on this work to show that $X(\mathbb{Q})$ is finite whenever X is a geometrically Galois cover of $\mathbb{P}^1$ with solvable Galois group.

A variant of Kim's method using adelic points instead of p-adic points was proved in [Ove16] to cut out exactly the set of points which survive torsors for finite étale nilpotent group schemes of odd order.

Very recently, Dogra proved an unlikely intersection result for iterated integrals and used it to extend the results of finiteness results of [Kim05], [CK10], and [EH17] to give nonabelian Chabauty proofs of the finiteness of $\mathcal{X}(\mathcal{O}_{K,S})$ for curves $\mathcal{X}$ of the same forms, but over any number field K and for any finite set of places S. (See [Dog19] for details.)

Restricting the method to the second step of the tower (this is called *quadratic Chabauty*), the Chabauty-Kim method can be applied to bound the set $X(\mathbb{Q})$ in several cases even when $\operatorname{rank} J(\mathbb{Q}) = \dim J$. For instance, as a relatively easy to state example of a much more general result, there is

Theorem 1.3.3 ([BD18a, special case of Corollary 1.2]). *Let X be a smooth projective*

hyperelliptic curve of genus g with good reduction at 3 and potential good reduction at all primes. Let J be the Jacobian of X, let $r = \operatorname{rank} J(\mathbb{Q})$, and let ρ be the rank of the Néron–Severi group of J. Suppose that $r = g$ and $\rho > 1$. Then

$$\#X(\mathbb{Q}) < 24g^3 + 228g^2 + 120g + 72\,.$$

In addition to general bounds, it is often possible to use quadratic Chabauty *in practice* to compute an explicit subset of $X(\mathbb{Q}_p)$ which contains $X(\mathbb{Q})$. For instance, the method was used to complete the classification of $\mathbb{Q}$-points on the modular curves $X_{\mathrm{s}}(\ell) := X(\ell)/C_{\mathrm{s}}(\ell)^+$, where $C_{\mathrm{s}}(\ell)^+$ is the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. [BDS+17] showed

Theorem 1.3.4 ([BDS+17])**.** $\#X_s(13)(\mathbb{Q}) = 7$.

The curve $X_{\mathrm{s}}(13)(\mathbb{Q})$ has genus 3 and absolutely simple Jacobian of rank 3; this made it inaccessible to all methods used to tackle other levels.

1.3.2 The Mordell–Weil sieve

No summary of improvements to Chabauty's method would be complete without mentioning the Mordell-Weil sieve. Although, strictly speaking, it is not a part of Chabauty's method, the Mordell–Weil sieve allows one to combine information from reducing modulo many different primes to show that $X(\mathbb{Q})$ must map into certain cosets of subgroups of $J(\mathbb{Q})$. This often allows one to rule out the existence of rational points inside of some residue discs on $X_{\mathbb{Q}_p}$. Using the Mordell–Weil sieve makes it much more likely that the subset of $X(\mathbb{Q}_p)$ computed via Chabauty will be equal to the set $X(\mathbb{Q})$. We recommend [Sik15] as a reference.

1.4 History of the S–unit equation

From one perspective, much of this thesis is devoted to studying a classical object of over a century of research — the set of solutions to the S-unit equation, i.e., the set

$$U_{K,S} := \{(x,y) \in \mathcal{O}_{K,S}^{\times} \times \mathcal{O}_{K,S}^{\times} : x+y=1\} \cong (\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})\,.$$

Building on earlier work of Siegel and Mahler on S–integral points on curves of positive genus, [Lan60] shows that $U_{K,S}$ is finite. These proofs were *ineffective*. In other words, they gave no information about the following questions:

1. Can $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ be bounded uniformly in terms of $[K:\mathbb{Q}]$ and $\#S$?
2. Given K and S, is it possible to compute the set $U_{K,S}$? If so, can one compute $U_{K,S}$ efficiently?

Regarding the first question: For many years, the best known (general) upper bounds on $\#U_{K,S}$ have built on work of Baker [Bak67] and Yu [Yu89] on the theory of linear forms in logarithms and linear forms in p-adic logarithms. For instance, in [Eve84], it is proved that

$$\#U_{K,S} \leq 3 \cdot 7^{d+2\cdot\#S+2\cdot\#M_K^{\infty}} = 3 \cdot 7^{2\#S+3r_1+4r_2}\,.$$

This upper bound is far from the largest known lower bounds. [EST88] show that there exists a positive constant C and sets S with $\#S$ arbitrarily large satisfying $U_{\mathbb{Q},S} > \exp(C(s/\log s)^{1/2})$. In the context where the field K varies instead of S, [Gra96] shows that $U_{K,\emptyset} \geq C \cdot [K:\mathbb{Q}]^2$ for cyclotomic fields.

Regarding the second question: Many authors have produced effective bounds for the heights of elements of $U_{K,S}$ by combining data from linear forms in logarithms at both the infinite and the finite places of K. The current state of the art can be found in [Győ19]. It is also possible to prove effective bounds on the height of elements of $U_{K,S}$ without using the theory of linear forms in logarithms [MP13]. In principle, these bounds allow one to compute $U_{K,S}$ by exhaustively checking all elements of

$\mathcal{O}_{K,S}^{\times}$ up to a given height. In practice, it is possible to do much better by using a combination of sieving methods and LLL-based techniques for lattice reduction [Sma99]. An efficient implementation is now available in Sage [AKM+18].

At this point, bounds on $\#U_{K,S}$ and methods for computing $U_{K,S}$ are well-understood. What is the value in continuing to study this set? We propose two answers.

First, algorithms for computing $U_{K,S}$ involve a mixture of techniques. It seems likely that new ideas for studying $U_{K,S}$ could lead to more efficient computations. For instance, it may be possible to use our ideas to improve the efficiency of the sieving step of [AKM+18].

Being able to compute $U_{K,S}$ efficiently has several applications. For instance, it is a key step in computing all elliptic curves over K with good reduction outside S [Š63] (as explained in [Sil09, proof of theorem 6.1],) all genus 2 curves over K with good reduction outside 2 [MS93], or all Fermat curves with good reduction outside 2 and 3 [BKSW19]. There are also applications to the study of recurrence sequences, decomposable form equations, and much more.

Second, the unit equation has recently been an important testing ground for strategies for new proofs of Faltings' Theorem. The first triumph of Kim's nonabelian Chabauty program was a new proof that $U_{\mathbb{Q},S}$ is finite [Kim05]. This work has since been turned into an explicit algorithm for bounding $U_{\mathbb{Q},S}$ inside of the vanishing set of p-adic power series, at least when S is small (and also for number fields of small degree) [DCW15]. Further development of Kim's approach has led to new bounds on $X(\mathbb{Q})$ for X a hyperelliptic curve with rank $J(\mathbb{Q}) = g$ and Néron–Severi rank greater than 1 [BD18b, BD17], as well as the explicit computation of the $\mathbb{Q}$-points on 'cursed' modular curve $X_{ns}(13)$ with rank and genus equal to 3 [BDS+17].

Before they completed their new p-adic proof of Faltings' theorem, Lawrence and Venkatesh also reproved the finiteness of $U_{K,S}$ by their method [LV18]. It served an important motivational role, and continues to be useful as a source of intuition regarding their method.

Our (wildly optimistic) dream is that the methods we develop in this thesis, possibly adapted to the setting of Kim's nonabelian Chabauty, could someday be part

of a new, computationally-oriented proof of Faltings' theorem. This day seems far off and may well never arrive. Nevertheless, we hope this dream will serve as sufficient motivation for our study of the S-unit equation.

1.5 Outline of this thesis

The remainder of this thesis is organized as follows:

Chapter 2 sets the notation that we use throughout the paper and discusses some background material. It may be best viewed as a reference section to be consulted as needed. It focuses on three topics: generalized Jacobians, descent, and Newton polygons. Section 2.2 sets up the theory necessary to describe an embedding of the punctured curve $\mathcal{C}$ into a semi-abelian scheme over $\mathcal{O}_{K,S}$. Section 2.3 reviews the theory of descent and gives explicit examples of descent sets for punctured genus 0 curves.

Chapter 3 reviews the classical theory of Chabauty's method. While most expositions of Chabauty's method consider $\mathbb{Q}$-points on projective curves, we work in the full generality of $\mathcal{O}_{K,S}$-points on integral models of curves. Although this complicates the presentation somewhat, we hope that it will prepare the reader to understand the method of Chabauty for restrictions of scalars of curves.

In Chapter 4, we present explain the RoS Chabauty method. Our treatment differs from Siksek's [Sik13] in two main ways. Firse, we develop the theory for the more general setting of integral points on curves. Second, while Siksek always considers the $\mathbb{Z}_p$ points of $\mathrm{Res}_{K/\mathbb{Q}} X$ and $\mathrm{Res}_{K/\mathbb{Q}} J$, we often consider the $K_{\mathfrak{p}}$-points of these varieties. This allows us to simplify formulas for regular differentials substantially, at the cost of working over larger fields. In this chapter, we also explain how base change obstructions to RoS Chabauty arise.

In Chapter 5, we study the power of classical and RoS Chabauty together with descent for bounding $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$. We show that classical Chabauty and descent by genus 0 covers suffices to prove finiteness of the S-unit equation only in very special cases. In contrast, when K has does not contain a CM subfield, we show

that all known obstacles to RoS Chabauty for $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ can be avoided using descent. This should be viewed as evidence that RoS Chabauty and descent may suffice to prove finiteness of the S-unit equation.

In Chapter 6, we give several extended examples where we use RoS Chabauty to give a new proof that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ is finite. We cover the cases where K is a quadratic field, a mixed cubic field, a totally complex quartic field, a mixed quartic field with a real quadratic subfield. We also show that there are no solutions to the unit equation when $[K : \mathbb{Q}]$ is not divisible 3 and 3 splits completely in K. The last two cases involve some particularly interesting applications of the method.

Chapter 2

Preliminaries

This chapter provides notation and a variety of background material which will be used later in this thesis. The reader may find it most helpful to skip this section on a first reading and to consult it as necessary.

2.1 Notation and conventions

In this section, we collect notations. There will be several forward references justifying our notation.

Throughout this thesis, we assume that X is a *nice* curve of genus g over a number field K, i.e., X is smooth, proper, and geometrically integral. Given an effective divisor $\mathfrak{m}$ on X which is defined over K, we let C be the open subscheme of X given by $C = X \smallsetminus \mathrm{supp}(\mathfrak{m})$. We assume $\mathfrak{m}$ has multiplicity at most 1 at any point of X. We also assume that

$$\deg \mathfrak{m} \geq \begin{cases} 3, & \text{if } g = 0, \\ 1, & \text{if } g = 1, \\ 0, & \text{if } g \geq 2\,, \end{cases}$$

so that C is a hyperbolic curve.

Let $J_C := \mathrm{GJac}(C, \mathfrak{m})$ be the generalized Jacobian of X with modulus $\mathfrak{m}$. (See Section 2.2.) The group scheme J_C is a semi-abelian variety over K. This means that

J_C is the extension of an abelian variety A by a torus T. In other words, J_C is the middle term in an exact sequence

$$0 \to T \to J_C \to A \to 0\,.$$

In this sequence, the abelian variety A is the Jacobian of X and the torus T depends on the modulus $\mathfrak{m}$. Set $\gamma = \max(0, \deg \mathfrak{m} - 1)$. Then, $\dim T = \gamma$ and $\dim A = g$, so $\dim J_C = g + \gamma$.

We write $r_1 = r_1(K)$ for the number of real embeddings of K and $r_2 = r_2(K)$ pairs of complex conjugate embeddings of K. We write $d = [K : \mathbb{Q}] = r_1 + 2r_2$ for the degree of K over $\mathbb{Q}$.

We say that a number field K is CM if K is a totally complex, degree 2 extension of a totally real field.

Let S' be a finite set of *finite* places of $\mathbb{Q}$, and let S be the set of places of K lying over S'. We write $\mathcal{O}_{K,S}$ for the ring of S-integers of K and write $\mathbb{Z}_{S'} := \mathcal{O}_{\mathbb{Q},S'}$. Note that $\mathcal{O}_{K,S}$ is the integral closure of $\mathbb{Z}_{S'}$ in K and is free of rank d as a $\mathbb{Z}_{S'}$-module, so that there is a restriction of scalars functor which takes $\mathcal{O}_{K,S}$-schemes to $\mathbb{Z}_{S'}$-schemes.

In our convention, S does not contain the infinite places. We warn the reader that many authors use different conventions. We use this notation because the infinite and finite places will behave differently in many of our arguments.

Chabauty's method is a p-adic method. As such we will need to work with completions of K. Let $\mathfrak{p} \notin S$ be a prime of K. We write $K_\mathfrak{p}$ for the completion of K at $\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ for the ring of integers of $K_\mathfrak{p}$.

Given a scheme $\mathcal{Z}$ over a base T and scheme T'/T, we let $\mathcal{Z}_{T'}$ denote the base change of $\mathcal{Z}$ to T'. When $T' = \operatorname{Spec} L$ for a ring L, we abuse notation and write $\mathcal{Z}_L := \mathcal{Z}_{\operatorname{Spec} L}$.

In this thesis, we will be interested in the set of integral points on certain $\mathcal{O}_{K,S}$-models of C. We now define the models which are acceptable for our method.

Definition 2.1.1. Suppose that X is a smooth, proper, geometrically integral curve over K and let $\mathcal{X}$ be a proper regular model for X over $\mathcal{O}_{K,S}$. Then the closure

of $\mathrm{supp}(\mathfrak{m})$ in $\mathcal{X}$ is a horizontal divisor Γ of $\mathcal{X}$. Write $\mathcal{C} = \mathcal{X} \smallsetminus \Gamma$. Then, $\mathcal{C}$ is an $\mathcal{O}_{K,S}$-model for C.

We call a $\mathcal{O}_{K,S}$-model $\mathcal{C}$ of this form a *clearance hole* model for C.

If, moreover, $\mathcal{C}$ is smooth, separated, and of finite-type over $\mathcal{O}_{K,S}$ and the fibers of $\mathcal{C}$ over the closed points of $\mathcal{O}_{K,S}$ are smooth and geometrically connected, we say that $\mathcal{C}$ is a *sound* clearance hole model for C.

Also, we say a scheme $\mathcal{C}$ over $\mathcal{O}_{K,S}$ is a *(sound) clearance hole curve* if $\mathcal{C}$ is a (sound) clearance hole model for its generic fiber $\mathcal{C}_K$.

Remark 2.1.2. A clearance hole is a hole through an object which is large enough to enable the threads of a screw or bolt to pass through but not the head of the screw or bolt. In other words, it is a hole which passes all the way through an object and is exactly as large as it needs to be, but no larger. The word sound is intended in the sense of 'structurally sound'.

Remark 2.1.3. Given a clearance hole model $\mathcal{C}$ for C, it is always possible to enlarge S to get a sound clearance hole model.

Since we assume that C is a hyperbolic curve, given any clearance hole model $\mathcal{C}$ for C, the set $\mathcal{C}(\mathcal{O}_{K,S})$ is finite by Faltings' theorem and Siegel's theorem.

Given a sound clearance hold model $\mathcal{C}$ for C over $\mathcal{O}_{K,S}$, let $\mathcal{J}_{\mathcal{C}}$ be the connected component of the identity of the lft-Néron model of J_C over $\mathcal{O}_{K,S}$. We call $\mathcal{J}_{\mathcal{C}}$ the generalized Jacobian of $\mathcal{C}$. Note however, that $\mathcal{J}_{\mathcal{C}}$ depends only on C and $\mathcal{O}_{K,S}$.

Since $\mathcal{C}$ is smooth and has geometrically connected fibers, given $P \in \mathcal{C}(\mathcal{O}_{K,S})$, the Abel-Jacobi map $j : C \to J_C$ based at P extends to a map $j : \mathcal{C} \to \mathcal{J}_{\mathcal{C}}$. (See Section 2.2 for more on this construction.)

Remark 2.1.4. When $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma$, such a morphism can be realized explicitly without enlarging S, even in the absence of an S-integral point. For instance, if $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$, we can take the morphism defined by

$$\begin{aligned} \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\} &\to \mathbb{G}_{m,\mathcal{O}_{K,S}} \times \mathbb{G}_{m,\mathcal{O}_{K,S}} \\ x &\mapsto (x, x-1). \end{aligned}$$

See Section 2.2.5 for the general construction.

Finally, given a scheme $\mathcal{Z}$ over $\mathcal{O}_{K,S}$, we always use $\dim \mathcal{Z}$ to refer to the relative dimension of $\mathcal{Z}$ over $\mathcal{O}_{K,S}$. In all situations we consider, this will be equivalent to the dimension of the generic fiber $\mathcal{Z}_K$ as a K-scheme.

2.2 Generalized Jacobians

In this section we discuss the basic properties of generalized Jacobians needed for the rest of this thesis.

2.2.1 Generalized Jacobians over Algebraically Closed Fields

In this section, our exposition mostly follows that of [Ser88].

To start, let X be a nice (smooth, projective, and geometrically integral) curve defined over an algebraically closed field $\overline{K}$. Let J be the Jacobian of X.

The abelian variety J plays two main roles with respect to X.

1. The Jacobian J is the Picard variety of X; i.e., it parameterizes degree 0 divisors on X up to linear equivalence.

2. The Jacobian J is the Albanese variety of X; i.e., given a point $P \in X(\overline{K})$, the Abel-Jacobi morphism $j : X \to J$ taking P to the identity on J satisfies the following universal property: For any abelian variety A and any morphism $f : X \to A$ which takes P to the identity on A, there is a unique morphism of group schemes $\phi : J \to A$ such that $f = \phi \circ j$.

Generalized Jacobians have analogues of these properties. They have a similar relationship with the Jacobian as a ray class group has with the class group of a number field.

As when defining ray class groups, we need a notion of modulus.

A *modulus* $\mathfrak{m}$ on X is a formal nonnegative integer linear combination of points of $X(\overline{K})$, i.e., an effective divisor on X. Any modulus can be expressed a integer linear

combination

$$\mathfrak{m} = \sum_{P \in X(\overline{K})} n_P P$$

where $n_P = 0$ for all but finitely many $P \in X(\overline{K})$ and $n_P \geq 0$ always. The *support* of $\mathfrak{m}$ is the finite set

$$\operatorname{supp}(\mathfrak{m}) := \{P \in X(\overline{K}) : n_P \neq 0\}.$$

If $\varphi \in \overline{K}(X)$ is a rational function, we write $\varphi \equiv 1 \pmod{\mathfrak{m}}$ if $\varphi - 1$ has a zero of order at least n_P for each $P \in \operatorname{supp}(\mathfrak{m})$.

The generalized Jacobian $J_{\mathfrak{m}}$ of X with modulus $\mathfrak{m}$ exists and is characterized by the universal property in Theorem 2.2.3.

Before we state the theorem, we define a property of functions on X equipped with a modulus $\mathfrak{m}$.

Definition 2.2.1. Let $f : X \dashrightarrow G$ be a rational map from X to a commutative group scheme over $\overline{K}$. Given a divisor $D = \sum n_P P$ on X, let $f(D)$ denote the element of G given by $\sum n_P f(P)$ (writing the group operation additively.) If both

1. f is regular away from $\operatorname{supp}(\mathfrak{m})$, and
2. $f(D) = 0$ whenever $D = (\varphi)$ is the divisor of a function with $\varphi \equiv 1 \mod \mathfrak{m}$,

say that f is $\mathfrak{m}$-good.

Definition 2.2.2. A rational map $\varphi : H \to G$ of commutative algebraic groups is an *affine homomorphism* if φ is a composition of a homomorphism and a translation.

Theorem 2.2.3 ([Ser88, Theorem I.2]). *For every modulus $\mathfrak{m}$, there exists a commutative algebraic group $J_{\mathfrak{m}}$ and a rational map $j_{\mathfrak{m}} : X \dashrightarrow J_{\mathfrak{m}}$ such that the following property holds:*

For every commutative algebraic group G and every $\mathfrak{m}$-good rational map $f : X \dashrightarrow G$, there is a unique affine homomorphism $\theta : J_{\mathfrak{m}} \dashrightarrow G$ such that $f = \theta \circ j_{\mathfrak{m}}$.

As with the usual Abel–Jacobi morphism, $j_{\mathfrak{m}}$ is unique up to the choice of a base point $P \in X(K)$ mapping to the identity element of $J(K)$.

We will abuse notation slightly by referring to $j_{\mathfrak{m}}$ as the Abel–Jacobi morphism, in keeping with standard terminology for Jacobians. Much like the usual Abel–Jacobi morphism, the restriction of $j_{\mathfrak{m}}$ to $X \smallsetminus \mathrm{supp}(\mathfrak{m})$ is a locally closed embedding.

The structure of $J_{\mathfrak{m}}$ is well understood. For each P, let $R_P := \overline{K}[t]/(t^{n_P})$. Then, $J_{\mathfrak{m}}$ fits into the following exact sequence:

$$0 \to \left(\prod_{P \in \mathrm{supp}(\mathfrak{m})} \mathrm{Res}_{R_P/\overline{K}} \mathbb{G}_m \right) / \mathbb{G}_m \to J_{\mathfrak{m}} \to J \to 0\,. \tag{2.2.4}$$

We are most concerned with the case where $n_P = 1$ for all $P \in \mathrm{supp}(\mathfrak{m})$, i.e. the case where $\mathfrak{m}$ (viewed as a subscheme of X in the natural way) is étale over $\mathrm{Spec}(\overline{K})$. In this situation, $G_P = \mathbb{G}_m$ for all $P \in \mathrm{supp}(\mathfrak{m})$, and so $J_{\mathfrak{m}}$ is an extension of an abelian variety by a torus, i.e. a *semiabelian variety*.

Recall that $\gamma = \max(0, \deg(\mathfrak{m}) - 1)$. By 2.2.4, the toric part of $J_{\mathfrak{m}}$ has dimension γ and the abelian variety quotient has dimension $g = \mathrm{genus}(X)$.

To ease notation throughout the rest of the paper, we make the following definition:

Definition 2.2.5. Suppose that $X/\overline{K}$ is a smooth, proper, and geometrically integral curve.

Let $\mathfrak{m}$ be a modulus with $n_P = 1$ for all $P \in \mathrm{supp}(\mathfrak{m})$. Set $C := X \smallsetminus \mathfrak{m}$.

The *generalized Jacobian of* C, which we denote by $J_{\mathfrak{m}}$ or J_C or $\mathrm{GJac}(C)$, is the generalized Jacobian of X with modulus $\mathfrak{m}$.

Similarly, we denote the Jacobian of X by $\mathrm{Jac}(X)$.

2.2.2 Generalized Jacobians over (Number) Fields

Let X be a nice curve over a number field K and let $\mathfrak{m}$ be a reduced effective divisor on X. Then, $C := X \smallsetminus \mathrm{supp}(\mathfrak{m})$ is a smooth, geometrically integral curve over K. Fix an algebraic closure $\overline{K}$ of K.

Much like the usual Jacobian, generalized Jacobians descend. This means that is

there is a commutative group scheme $\mathrm{GJac}(C)$ defined over K such that

$$\mathrm{GJac}(C)_{\overline{K}} = \mathrm{GJac}(C_{\overline{K}})\,.$$

If moreover $C(K) \neq \emptyset$, fixing any $P \in C(K)$ determines an Abel-Jacobi morphism $j : C_{\overline{K}} \to \mathrm{GJac}(C)_{\overline{K}}$ which descends to a locally closed embedding

$$j\colon C \to \mathrm{GJac}(C)\,,$$

defined over K and such that $j(P)$ is the identity element of $\mathrm{GJac}(C)$.

We comment briefly on the structure of $\mathrm{GJac}(C)$. Recall that $\mathfrak{m}$ is identified with the reduced zero-dimensional subscheme $X \smallsetminus C$. Then, $\mathfrak{m} = \mathrm{Spec}(L)$ for some étale algebra L/K. Then, refining (2.2.4), $\mathrm{GJac}(C)$ fits into the exact sequence

$$0 \to (\mathrm{Res}_{L/K}\,\mathbb{G}_m)/\mathbb{G}_m \to \mathrm{GJac}(C) \to \mathrm{Jac}(X) \to 0\,.$$

We discuss the structure of $\mathrm{Res}_{L/K}\,\mathbb{G}_m$ in further detail in Section 2.2.5.

2.2.3 Néron Models

Before we define the generalized Jacobian for relative curves, we first recall some facts about Néron models of semiabelian varieties. Our exposition is mostly drawn from [BLR90].

We first recall the definition of a Néron model:

Definition 2.2.6. [BLR90, Definition 1.2.1.] Let S be a Dedekind scheme with ring of rational functions K.

Let X_K be a smooth K-scheme. A *Néron model* of X_K (resp. a Néron lft-model) is an S-model of X which is smooth, separated, and of finite type (resp. locally of finite type,) and which satisfies the following universal property, called the Néron mapping property:

For each smooth S-scheme Y and each K-morphism $u_K : Y_K \to X_K$ there is a

unique S-morphism $u : Y \to X$ extending u_K.

By the Néron mapping property, a Néron lft-model G of an algebraic group G_K over K is a group scheme over S (if it exists). Note, however, that G need not be proper over S, even if G_K is proper over K. We require the following existence result:

Theorem 2.2.7 ([BLR90, page 310])**.** *Let S be an excellent Dedekind scheme with ring of rational functions K of characteristic 0. Let G_K be a smooth, commutative, connected algebraic group over K. The following conditions are equivalent:*

1. *G_K admits a Néron lft-model over S.*
2. *G_K contains no subgroup of type $\mathbb{G}_a$.*

In particular, if G_K is a semi-abelian variety, then G_K admits a Néron lft-model over S. The Néron lft-model is of finite type if and only if G_K is an abelian variety.

Remark 2.2.8. The fibers of a Néron lft-model G of a smooth, commutative, connected algebraic group need not be connected. We let G° denote the (fiber-wise) connected component of the identity section. The subscheme G° is also a commutative group scheme.

Example 2.2.9. Suppose that $E/\mathbb{Q}_p$ is an elliptic curve. Let $\mathcal{E}/\mathbb{Z}_p$ be the minimal proper regular model of E. Then the Néron model of E is the open subscheme of $\mathcal{E}$ obtained by removing any singular points on the special fiber of $\mathcal{E}$.

Example 2.2.10. We describe the lft-Néron model G over $\operatorname{Spec}\mathbb{Z}$ of $\mathbb{G}_{m,\mathbb{Q}}$.

We construct G by gluing an infinite disjoint union of copies of $\mathbb{G}_{m,\mathbb{Z}}$, indexed by a prime and an integer. Write $p^n\mathbb{G}_{m,\mathbb{Z}}$ for the copy indexed by p and n. This is just notation, but it will be suggestive of the gluing. We have:

$$\mathbb{G}_{m,\mathbb{Z}} \cup \bigcup_{p \text{ prime}} \bigcup_{n\in\mathbb{Z}} p^n\mathbb{G}_{m,\mathbb{Z}}\,.$$

To get G, we glue $\mathbb{G}_{m,\mathbb{Z}}$ to $p^n\mathbb{G}_{m,\mathbb{Z}}$ over $\operatorname{Spec}\mathbb{Z} \smallsetminus \{p\}$ via multiplication by p^n.

The generic fiber of the resulting scheme is clearly $\mathbb{G}_{m,\mathbb{Q}}$. The special fiber over p is an disjoint union of copies of $\mathbb{G}_{m,\mathbb{F}_p}$ indexed by $\mathbb{Z}$. Writing $p^n\mathbb{G}_{m,\mathbb{F}_p}$ for the copy

indexed by n and writing m for the multiplication on $\mathbb{G}_{m,\mathbb{F}_p}$, the group law on the special fiber is given by

$$\begin{aligned} M : \bigcup_{n\in\mathbb{Z}} p^n\mathbb{G}_{m,\mathbb{F}_p} \times \bigcup_{n\in\mathbb{Z}} p^n\mathbb{G}_{m,\mathbb{F}_p} &\to \bigcup_{n\in\mathbb{Z}} p^n\mathbb{G}_{m,\mathbb{F}_p}\,, \\ = \coprod_{(i,j)\in\mathbb{Z}^2} m : p^i\mathbb{G}_{m,\mathbb{F}_p} \times p^j\mathbb{G}_{m,\mathbb{F}_p} &\to p^{i+j}\mathbb{G}_{m,\mathbb{F}_p}\,. \end{aligned}$$

The inversion maps and co-units are defined similarly.

The $\mathbb{Z}$-points of G are clearly in bijection with $\mathbb{G}_{m,\mathbb{Q}}(\mathbb{Q}) = \mathbb{Q}^\times$. Indeed, an element of $G(\mathbb{Z})$ is an element of $x \in \mathbb{Q}^\times$ together with the p-adic valuation of x and the congruence class modulo p of $p^{-v_p(x)}x$ for each prime p.

Moreover, the connected component of the identity is

$$G^\circ = \mathbb{G}_{m,\mathbb{Z}}\,.$$

One can check that the Néron property holds and that this construction generalizes to number fields without much further work. See [BLR90, Example 10.1.5] for details.

Taking Néron models 'commutes' with Weil restriction of scalars as follows.

Proposition 2.2.11. *let $T' \to T$ be a finite flat extension of Dedekind schemes with rings of rational functions L and K, respectively. Suppose that G_L is a smooth group scheme over L with Neron lft-model G over T'.*

The Weil restriction of scalars $\mathrm{Res}_{T'/T} G$ is an lft-Néron model for $\mathrm{Res}_{L/K} G_L$.

Proof. The Weil restriction of scalars $\mathrm{Res}_{T'/T} G$ is a smooth, separated, locally of finite type model for $\mathrm{Res}_{L/K} G_L$, so it suffices to check the Néron mapping property. Moreover, the universal property of restriction of scalars (twice) and the Néron

property for G imply that for any T-scheme T'',

$$\begin{aligned}\mathrm{Hom}_T(T'', \mathrm{Res}_{T'/T} G) &= \mathrm{Hom}_{T'}(T'' \times_T T', G) \\ &= \mathrm{Hom}_{\mathrm{Spec}(L)}((T'' \times_T T')_L, G_L) \\ &= \mathrm{Hom}_{\mathrm{Spec}(L)}(T''_K \times_{\mathrm{Spec}\, K} \mathrm{Spec}(L), G_L) \\ &= \mathrm{Hom}_{\mathrm{Spec}(K)}(T''_K, \mathrm{Res}_{L/K} G_L)\,.\end{aligned}$$

Hence, $\mathrm{Res}_{T'/T} G$ is a Néron model for $\mathrm{Res}_{L/K} G_L$. □

Remark 2.2.12. We claim that $(\mathrm{Res}_{T'/T} G)^\circ = (\mathrm{Res}_{T'/T} G^\circ)$. Indeed, since the universal property implies that the fibers of the restriction of scalars are the restriction of scalars of the fibers, so it suffices to check this fiber-wise. Now, the fibers of G are smooth, so [CGP15, Proposition A.5.9] shows that the fibers of $(\mathrm{Res}_{T'/T} G^\circ)$ are connected. So

$$(\mathrm{Res}_{T'/T} G)^\circ = (\mathrm{Res}_{T'/T} G^\circ)^\circ = \mathrm{Res}_{T'/T} G^\circ\,,$$

as claimed.

As an immediate application, note that if G is the Néron model over $\mathcal{O}_{K,S}$ of the group scheme $\mathrm{Res}_{L/K} \mathbb{G}_{m,K}$ and $\mathcal{O}_{L_i,S''}$ is the integral closure of $\mathcal{O}_{K,S}$ in L, then

$$G^\circ = \mathrm{Res}_{\mathcal{O}_{L,S''}/\mathcal{O}_{K,S}} \mathbb{G}_{m,\mathcal{O}_{L,S''}}\,.$$

Néron models also behave well under étale base change.

2.2.4 Generalized Jacobians over Rings of S-Integers

In this section, we assume that $\mathcal{C} = \mathcal{X} \smallsetminus \Gamma$ over $\mathcal{O}_{K,S}$ is a sound clearance hole model (see Definition 2.1.1) for the K-curve $C = X \smallsetminus \mathfrak{m}$.

Note in particular that $\mathfrak{m}$ is étale over $\mathrm{Spec}\, K$ while Γ is flat, but not necessarily étale over $\mathrm{Spec}\, \mathcal{O}_{K,S}$.

Recall that J_C is the generalized Jacobian of C. Suppose that the basepoint of the Abel-Jacobi morphism $j : C \to J_\mathfrak{m}$ extends to a point of $\mathcal{C}(\mathcal{O}_{K,S})$. Since $\mathfrak{m}$ is étale

over K, the commutative group scheme $J_{\mathfrak{m}}$ is a semiabelian variety. In particular, $J_{\mathfrak{m}}$ admits a Néron lft-model $\mathcal{J}_{\mathfrak{m}}$ over $\mathcal{O}_{K,S}$. Let $\mathcal{J}_{\mathcal{C}} := \mathcal{J}_{\mathfrak{m}}^{\circ}$ be the (fiber-wise) connected component of the identity of $\mathcal{J}_{\mathfrak{m}}$.

We call $\mathcal{J}_{\mathcal{C}}$ the *generalized Jacobian* of $\mathcal{X}$ with modulus Γ, or the generalized Jacobian of $\mathcal{C} := \mathcal{X} \smallsetminus \Gamma$. Note, however that $\mathcal{J}_{\mathcal{C}}$ depends only on C and $\mathcal{O}_{K,S}$.

We briefly justify our terminology.

By the Néron propety, the Abel-Jacobi morphism $j : C \hookrightarrow J_{\mathfrak{m}}$ extends to a morphism $j : \mathcal{C} \hookrightarrow \mathcal{J}_{\mathfrak{m}}$. Since $\mathcal{C}$ is a sound clearance hole model, the fibers of $\mathcal{C}$ are geometrically connected. Hence, the image will lie in the connected component of the identity. So in fact we have an Abel-Jacobi morphism

$$j : \mathcal{C} \hookrightarrow \mathcal{J}_{\mathfrak{m}}^{\circ} = \mathcal{J}_{\mathcal{C}} \,.$$

For example, if $\mathcal{C} = \mathbb{P}^1_{\mathbb{Z}} \smallsetminus \{0, 2, \infty\}$, then $J_{\mathfrak{m}} \cong \mathbb{G}_{m,\mathbb{Q}} \times \mathbb{G}_{m,\mathbb{Q}}$, so $\mathcal{J}_{\mathcal{C}} \cong \mathbb{G}_{m,\mathbb{Z}} \times \mathbb{G}_{m,\mathbb{Z}}$. If we fix the base point $1 \in \mathcal{C}(\mathbb{Z})$, the Abel-Jacobi morphism is given by

$$\begin{aligned} j : \mathbb{P}^1_{\mathbb{Z}} \smallsetminus \{0, 2, \infty\} &\to \mathbb{G}_{m,\mathbb{Z}} \times \mathbb{G}_{m,\mathbb{Z}} \,, \\ x &\mapsto (x, 2 - x) \,. \end{aligned}$$

2.2.5 Generalized Jacobians of Genus Zero Curves

In the examples in this article, we will focus primarily on the case where $\mathcal{C}$ is a punctured curve of genus zero. In preparation, we recall some facts about the structure of the generalized Jacobian of such a curve. Set

$$\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{(x : y) : f(x, y) = 0\}$$

for some homogeneous square-free polynomial $f \in \mathcal{O}_{K,S}[x, y]$ of content 1.

In this case, the generalized Jacobian of $\mathcal{C}$ can be understood explicitly in terms

of norm tori. Write $f = \prod_{i=1}^{c} f_i$ where each f_i is irreducible over $\mathcal{O}_{K,S}$. Set

$$R_i := \begin{cases} \text{the integral closure of } \mathcal{O}_{K,S} \text{ in } K[x]/f(x,1) & \text{if } f_i \neq y\,, \\ \mathcal{O}_{K,S} & \text{if } f_i = y\,. \end{cases}$$

Let L_i be the fraction field of R_i and let S_i be the set of places of L_i which lie over some prime in S.

Each R_i is module-finite over $\mathcal{O}_{K,S}$ and we have

$$\mathcal{J}_{\mathcal{C}} \cong \left(\prod_{i=1}^{c} \mathrm{Res}_{R_i, \mathcal{O}_{K,S}} \mathbb{G}_{m,R_i} \right) / \Delta(\mathbb{G}_{m,\mathcal{O}_{K,S}})\,, \tag{2.2.13}$$

where $\Delta(\mathbb{G}_{m,\mathcal{O}_{K,S}})$ indicates a diagonally embedded copy of $\mathbb{G}_{m,\mathcal{O}_{K,S}}$. If $f_i = y$ for some i, so that $\mathcal{C}$ is a punctured copy of $\mathbb{A}^1$, the formula can be simplified by leaving out the ith component and the quotient.

Independent of the existence of a rational point on $\mathcal{C}$, there is an Abel-Jacobi map $j : \mathcal{C} \to \mathcal{J}_{\mathcal{C}}$ defined as follows. Over an algebraic closure, f_i factors as a product of conjugates of $(\alpha_i x - \beta_i y)$ for α_i and β_i integral. Then, we have

$$\begin{aligned} j : \mathcal{C} &\to \mathcal{J}_{\mathcal{C}} \\ (x : y) &\mapsto (\alpha_1 x - \beta_1 y, \ldots, \alpha_c x - \beta_c y)\,, \end{aligned}$$

where we can naturally interpret $\alpha_1 x - \beta_1 y$ as an element of the restriction of scalars.

For example, if $f(x,y) = x(x-y)y$, so that $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$, then

$$\mathcal{J}_{\mathcal{C}} \cong \mathbb{G}_{m,\mathcal{O}_{K,S}} \times \mathbb{G}_{m,\mathcal{O}_{K,S}}\,.$$

and

$$\begin{aligned} j : \mathcal{C} &\to \mathcal{J}_{\mathcal{C}} \\ x &\mapsto (x, x-1)\,, \end{aligned}$$

where we have set $y = 1$ and forgotten the last coordinate because we are using the simplified form.

The expression (2.2.13) makes it easy to compute the dimension and rank of $\mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S})$. Since R_i is finite index in $\mathcal{O}_{L_i,S_i}$ and has the same rank as $\mathcal{O}_{L_i,S_i}$, we have

$$\dim \mathcal{J}_{\mathcal{C}} = \deg(f) - 1 = \sum_{i=1}^{c} \deg(f_i) - 1 = \sum_{i=1}^{c} [L_i : K] - [K : K]$$

and

$$\begin{aligned} \operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) &= \sum_{i=1}^{c} \operatorname{rank} R_i^{\times} - \operatorname{rank} \mathcal{O}_{K,S}^{\times} \\ &= \sum_{i=1}^{c} \operatorname{rank} \mathcal{O}_{L_i,S_i}^{\times} - \operatorname{rank} \mathcal{O}_{K,S}^{\times} \\ &= \sum_{i=1}^{c} [r_1(L_i) + r_2(L_i) + \#S_i - 1] - [r_1(K) + r_2(K) + \#S - 1]\,. \end{aligned} \tag{2.2.14}$$

We can also express the rank in terms of the action of the absolute Galois group of K on the set of punctures of our genus zero curve. We state the general result, noting that for the purpose of proving finiteness of integral points, we may assume the curve is a punctured $\mathbb{P}^1$, or else it automatically has no $\mathcal{O}_{K,S}$ points.

Lemma 2.2.15. *Let $\mathcal{X}/\mathcal{O}_{K,S}$ be a minimal proper regular model of $\mathbb{P}^1_K$.. Let $G = \operatorname{Gal}(\overline{K}/K)$ be the absolute Galois group of K and for a place $\mathfrak{p}$, let $G_{\mathfrak{p}}$ denote the decomposition group of $\mathfrak{p}$. Let Γ be a horizontal divisor on $\mathcal{X}$. Set*

$$\mathcal{C} = \mathcal{X} \smallsetminus \Gamma\,.$$

The curve $\mathcal{C}$ is a sound clearance hole model for its generic fiber $C := \mathcal{C}_K$.

Write $G\backslash\Gamma(\overline{K})$ for the set of orbits for the action of G on $\Gamma(\overline{K})$.

Then, the generic fiber J_C of $\mathcal{J}_{\mathcal{C}}$ is a torus and

$$\dim \mathcal{J}_{\mathcal{C}} = \dim J_C = \#\Gamma(\overline{K}) - 1,$$

and $\mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S})$ *is an abelian group of rank*

$$\operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) = \sum_{\mathfrak{p} \in S \cup \Sigma_\infty} [\#(G_{\mathfrak{p}} \backslash \Gamma(\overline{K})) - 1] - [\#(G \backslash \Gamma(\overline{K})) - 1] \,.$$

We omit the proof, which is a fairly straightforward computation in the character theory of tori. All of the ideas needed can be found, for example, Theorem 8.7.2 of *Cohomology of Number Fields* by Neukirch, Schmidt, and Wingberg [NSW08], or in Chapter 6 of Eisenträger's Ph.D. Thesis [Eis03].

2.3 Descent

When the pair $(\mathcal{C}, \mathcal{O}_{K,S})$ does not satisfy the classical Chabauty inequality (3.2.6) or the RoS Chabauty inequality (4.1.5), we must use another approach to prove that $\mathcal{C}(\mathcal{O}_{K,S})$ is finite. One possibility is to replace $(\mathcal{C}, \mathcal{O}_{K,S})$ with a finite set of covers of $\mathcal{C}$ such that each point in $\mathcal{C}(\mathcal{O}_{K,S})$ is the image of an integral point on some curve in the set. We define

Definition 2.3.1. A *descent set* for $(\mathcal{C}, \mathcal{O}_{K,S})$ is a finite set $\mathscr{D}$ of clearance hole curves $\mathcal{D}$ over $\mathcal{O}_{K,S}$ (see Definition 2.1.1) equipped with morphisms $f_{\mathcal{D}} : \mathcal{D} \to \mathcal{C}$ such that

$$\mathcal{C}(\mathcal{O}_{K,S}) \subseteq \bigcup_{\mathcal{D} \in \mathscr{D}} f_{\mathcal{D}}(\mathcal{D}(\mathcal{O}_{K,S})) \,.$$

If, moreover, the generic fibers $\mathcal{D}_K$ of all of the curves $\mathcal{D}$ are punctured genus 0 curves, we say that $\mathscr{D}$ is a genus 0 descent set.

Showing that $\mathcal{D}(\mathcal{O}_{K,S})$ is finite for each $\mathcal{D} \in \mathscr{D}$ proves that $\mathcal{C}(\mathcal{O}_{K,S})$ is also finite.

Remark 2.3.2. If $\mathscr{D}$ is a descent set of $(\mathcal{C}, \mathcal{O}_{K,S})$ and for some $\mathcal{D} \in \mathscr{D}$, we have that $\mathscr{E}$ is a descent set for $(\mathcal{D}, \mathcal{O}_{K,S})$, then $(\mathscr{D} \smallsetminus \{\mathcal{D}\}) \cup \mathscr{E}$ is also a descent set for $(\mathcal{C}, \mathcal{O}_{K,S})$. This iterated descent approach can be used to construct complicated descent sets from relatively simple building blocks.

In this remainder of this section, we give a brief overview of the theory of Galois descent, proving that descent sets exist and giving explicit examples.

Our exposition mostly follows [Poo17, Sections 6.5 and 8.4]. We recommend [Sko01] as a further reference.

2.3.1 Torsors

In order to explain the theory of integral descent, we first recall the notion of a torsor under a group scheme over a base scheme.

Definition 2.3.3 ([Poo17, Definition 6.5.1])**.** Let $G \to \mathcal{S}$ be an fppf group scheme. A (right) *G-torsor over $\mathcal{S}$* is an fppf $\mathcal{S}$-scheme Z equipped with a right G-action

$$Z \times_{\mathcal{S}} G \to Z$$

such that one of the following equivalent conditions holds:

1. There exists an fppf base change $\mathcal{S}' \to \mathcal{S}$ such that $Z_{\mathcal{S}'}$ is isomorphic to $G_{\mathcal{S}'}$ as $\mathcal{S}'$-schemes with $G_{\mathcal{S}'}$ action. (Here the action of $G_{\mathcal{S}'}$ on itself is by right translation.)

2. The morphism

$$\begin{aligned} Z \times_{\mathcal{S}} G &\to Z \times_{\mathcal{S}} Z \\ (x, g) &\mapsto (x, x \cdot g) \end{aligned}$$

   is an isomorphism.

The first condition says that Z is a twist of G (as a scheme with G-action). As such, it should not be a surprise that torsors are parameterized by H^1 in a suitable cohomology theory. For the remainder of this section and the following section, we make the convention $H^1 := \check{H}^1_{fppf}$. We have

Theorem 2.3.4 ([Poo17, Theorem 6.5.10])**.** *Let G be an fppf group scheme over a locally noetherian scheme S. Suppose that $G \to \mathcal{S}$ is an affine morphism. Letting H^1*

denote Čech cohomology on the fppf site, we have

$$\{G\text{-}torsors\}/isomorphism \cong H^1(\mathcal{S}, G).$$

as pointed sets. (The neutral element on the left-hand side is given by the class of the trivial torsor G with right G-action.)

We are primarily concerned with cases where G is finite over $\mathcal{S}$, so the assumption that $G \to \mathcal{S}$ is affine is not an inconvenience. Following [Poo17, Section 6.5.6] we assume that $G \to S$ is affine from now on.

Write $H = G$ viewed as a scheme with a left-action on G. Given a right G-torsor T corresponding to $\tau \in H^1(S, G)$, there is a left-action of the twisted group scheme $\mathcal{G}^\tau$ on T. So, in fact, T is a H^τ-G-bitorsor. It is also possible to give T the structure of a G-H^τ-bitorsor by inverting the group action. For instance, one can define the map $G \times T \to T$ by $g \cdot t = tg^{-1}$. The resulting G-H^τ-bitorsor is denoted T^{-1}.

Now, given two right G-torsors Z and T over S represented in $H^1(\mathcal{S}, G)$ by ζ and τ, respectively, let $Z \overset{G}{\times} T^{-1}$ be the quotient of $Z \times_{\mathcal{S}} T^{-1}$ by the G-action $(x, t) \cdot g = (xg, g^{-1}t)$. The scheme $Z \overset{G}{\times} T^{-1}$ is a G^ζ-G^τ-bitorsor over $\mathcal{S}$ and is affine over $\mathcal{S}$.

2.3.2 Constructing descent sets

Suppose now that $\mathcal{S}$ is finite-type and separated over $\mathcal{O}_{K,S}$. Let $\mathcal{G}$ be a finite flat group scheme over $\mathcal{O}_{K,S}$, and suppose that $f : Z \to \mathcal{S}$ is a $\mathcal{G}_{\mathcal{S}}$-torsor. For any $\mathcal{G}$ torsor T over $\mathcal{O}_{K,S}$ corresponding to $\tau \in H^1(\mathcal{O}_{K,S}, \mathcal{G})$, the twist

$$Z^\tau := Z \overset{\mathcal{G}_{\mathcal{S}}}{\times} (T_{\mathcal{S}})^{-1}$$

is a right $(\mathcal{G}^\tau)_{\mathcal{S}}$-torsor over $\mathcal{S}$, with structure map $f^\tau : Z^\tau \to \mathcal{S}$.

Now, slightly generalizing [Poo17, Section 8.4.1], we can define an evaluation map

$$\begin{aligned} \mathcal{S}(\mathcal{O}_{K,S}) \times H^1(\mathcal{S}, \mathcal{G}) &\to H^1(\mathcal{O}_{K,S}, \mathcal{G}) \\ (x, \zeta) &\mapsto \zeta(x) := x^*(\zeta) \end{aligned}$$

by pulling back cohomology classes.

Define

$$\mathcal{S}(\mathcal{O}_{K,S})_\tau := \{x \in \mathcal{S}(\mathcal{O}_{K,S}) : \zeta(x) = \tau\}\,.$$

Clearly,

$$\mathcal{S}(\mathcal{O}_{K,S}) = \bigcup_{\tau \in H^1(\mathcal{O}_{K,S},\mathcal{G})} \mathcal{S}(\mathcal{O}_{K,S})_\tau\,.$$

By a slight generalization of [Poo17, Theorem 8.4.1],

$$f^\tau(Z^\tau(\mathcal{O}_{K,S})) = \mathcal{S}(\mathcal{O}_{K,S})_\tau\,,$$

so in fact,

$$\mathcal{S}(\mathcal{O}_{K,S}) = \bigcup_{\tau \in H^1(\mathcal{O}_{K,S},\mathcal{G})} f^\tau(Z^\tau(\mathcal{O}_{K,S}))\,.$$

By [Poo17, Exercise 8.4], $H^1(\mathcal{O}_{K,S}, \mathcal{G})$ is finite, so in fact, we have

Proposition 2.3.5. *The set*

$$\mathcal{Z} = \left\{f^\tau : Z^\tau \to \mathcal{S} : \tau \in H^1(\mathcal{O}_{K,S}, \mathcal{G})\right\}$$

is a descent set for $(\mathcal{S}, \mathcal{O}_{K,S})$.

2.3.3 Explicit examples of descent sets

In certain cases, we can construct descent sets explicitly.

Suppose that $\mathcal{A}$ is a separated group scheme of finite type over $\mathcal{O}_{K,S}$ and we have a morphism $j : \mathcal{C} \hookrightarrow \mathcal{A}$ such that the restriction of j to the generic fiber is finite. Suppose that $\mathcal{B}$ is another separated group scheme of finite type over $\mathcal{O}_{K,S}$ equipped with a finite, flat map $\phi : \mathcal{B} \to \mathcal{A}$ of group schemes such that $\phi(\mathcal{B}(\mathcal{O}_{K,S}))$ has finite index in $\mathcal{A}(\mathcal{O}_{K,S})$. Suppose also that $\mathcal{A}(\mathcal{O}_{K,S})$ is finitely generated. For example, this holds if $\mathcal{A}$ is the connected component of the identity of the Néron model of a semiabelian variety.)

Choose (right) coset representatives $P_1, \ldots, P_n$ for $\phi(\mathcal{B}(\mathcal{O}_{K,S}))$ in $\mathcal{A}(\mathcal{O}_{K,S})$. For

each $i \in \{1, \ldots, n\}$, there is a morphism of $\mathcal{O}_{K,S}$-schemes

$$\begin{aligned} \phi_i : \mathcal{B} &\to \mathcal{A}\,, \\ Q &\mapsto \phi(Q) \cdot P_i\,. \end{aligned}$$

Then,

$$\mathcal{A}(\mathcal{O}_{K,S}) = \coprod_{i=1}^{n} \phi(\mathcal{B}(\mathcal{O}_{K,S})) \cdot P_i = \coprod_{i=1}^{n} \phi_i(\mathcal{B}(\mathcal{O}_{K,S}))\,. \tag{2.3.6}$$

Let $\mathcal{D}_i$ be the pullback of $\mathcal{C}$ by ϕ_i. From the pullback diagram

$$\begin{array}{ccc} \mathcal{D}_i & \xhookrightarrow{j_{\mathcal{D}}} & \mathcal{B} \\ \downarrow{\scriptstyle \phi_i} & & \downarrow{\scriptstyle \phi_i} \\ \mathcal{C} & \xhookrightarrow{j} & \mathcal{A} \end{array}$$

and (2.3.6), we see that $Q \in \mathcal{C}(\mathcal{O}_{K,S})$ belongs to $\phi_i(\mathcal{D}_i(\mathcal{O}_{K,S}))$ if and only if $Q \in \mathcal{B}(\mathcal{O}_{K,S}) \cdot P_i$. It follows that

$$\mathcal{C}(\mathcal{O}_{K,S}) = \coprod_{i=1}^{n} \phi_i(\mathcal{D}_i(\mathcal{O}_{K,S}))\,.$$

In particular, $\{\mathcal{D}_i : i \in \{1, \ldots, n\}\}$ will be a descent set for $(\mathcal{C}, \mathcal{O}_{K,S})$ so long as the $\mathcal{D}_i$ are sound clearance hold curves over $\mathcal{O}_{K,S}$.

In this construction, each $\mathcal{D}_i$ is a torsor over $\mathcal{C}$ for the finite group scheme $\ker(\phi_i : \mathcal{B} \to \mathcal{A})$. In particular, this construction is an example of descent.

Example 2.3.7. If $\mathcal{C}/\mathcal{O}_{K,S}$ is $\mathbb{P}^1 \smallsetminus (\{0, \infty\} \cup \Gamma')$, then there is a natural inclusion $\mathcal{C} \hookrightarrow \mathbb{G}_{m,\mathcal{O}_{K,S}}$. Taking ϕ to be the nth power map from $\mathbb{G}_m$ to itself, this procedure gives a descent set $\mathscr{D}$ for $(\mathcal{C}, \mathcal{O}_{K,S})$ indexed by elements of $\mathcal{O}_{K,S}^{\times}/\mathcal{O}_{K,S}^{\times n}$.

Every covering curve in $\mathscr{D}$ is a punctured $\mathbb{P}^1$ for which we can write down explicit equations. If we choose a polynomial f such that

$$\Gamma' = \{x : f(x) = 0\}\,,$$

and let α range over $\mathcal{O}_{K,S}^{\times}/(\mathcal{O}_{K,S}^{\times})^n$, then $\mathscr{D}$ consists of the curves

$$f_\alpha : \mathbb{P}^1 \smallsetminus \{0,\infty\} \cup \{x : f(\alpha x^n) = 0\} \to \mathbb{P}^1 \smallsetminus \{0,\infty\} \cup \{x : f(x) = 0\}$$
$$x \mapsto \alpha x^n$$

Remark 2.3.8. We show that Example 2.3.7 combined with the iterated descent described in Remark 2.3.2 is essentially the only way to produce descent sets consisting of punctured genus 0 curves which are torsors from group schemes over the base.

Let $\phi : \mathbb{P}^1_{\overline{K}} \to \mathbb{P}^1_{\overline{K}}$ be a Galois cover. I.e., suppose that the induced map on function fields identifies $\phi^*(\overline{K}(t))$ as a subgroup of $\overline{K}(s)$ such that the extension is Galois.

Let B be the set of $\overline{K}$-points on the base over which of ϕ is branched. The Riemann-Hurwitz theorem implies that

$$2\deg(\phi) - 2 = \deg(\phi) \cdot \#B - \sum_{P \in B} \#\{Q \in \mathbb{P}^1(\overline{K}) : \phi(Q) = P\}\,.$$

For any $P \in B$, we have $\#\{Q \in \mathbb{P}^1(\overline{K}) : \phi(Q) = P\} \leq d/2$, so $1 < \#B < 4$.

If $\#B = 2$, then $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is a isomorphic to the nth power map.

If $\#B = 3$, then $\deg(\phi) = 6$ and $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is an S_3-cover. Using the structure of S_3 as a solvable group, ϕ can be constructed as the composition of two Galois covers which are ramified at exactly 2 points.

Chapter 3

The Method of Chabauty-Coleman-Skolem

In this section, we recall the p-adic method of Chabauty and Coleman for bounding the number of S-integral points on a sound clearance hole curve $\mathcal{C}/\mathcal{O}_{K,S}$. (See Definition 2.1.1.) Although Chabauty's method is typically described in the special case of K-rational points on smooth, proper, and geometrically integral curves, we present the general case with an eye towards computing S-integral points on punctured genus zero curves. In a way, this makes a return to the original inspiration for Chabauty's method — an analogous strategy (due to Skolem) for solving Thue equations, i.e. computing the set

$$\{(a, b) \in \mathbb{Z}^2 : f(a, b) = c\}$$

for $f \in \mathbb{Z}[x, y]$ a homogeneous polynomial of degree $d \geq 3$. Our exposition mostly follows that of [MP12], which we enthusiastically recommend.

3.1 Chabauty's result

We begin with an overview of Chabauty's idea adapted to our more general setting.

Our setup is as in Section 2.1.

Our goal is to compute the set $\mathcal{C}(\mathcal{O}_{K,S})$ of S-integral points on the punctured

curve $\mathcal{C}$.

Fix a prime $\mathfrak{p} \notin S$. Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and let $\mathcal{O}_\mathfrak{p}$ denote the ring of integers of $K_\mathfrak{p}$. Then there is a commutative diagram:

$$\begin{array}{ccc} \mathcal{C}(\mathcal{O}_{K,S}) & \longhookrightarrow & \mathcal{C}(\mathcal{O}_\mathfrak{p}) \\ \downarrow & & \downarrow \\ \mathcal{J}(\mathcal{O}_{K,S}) & \longhookrightarrow & \mathcal{J}(\mathcal{O}_\mathfrak{p}) \,. \end{array}$$

In particular, inside of $\mathcal{J}(\mathcal{O}_\mathfrak{p})$, we have the inclusion

$$\mathcal{C}(\mathcal{O}_{K,S}) \subseteq \mathcal{J}(\mathcal{O}_{K,S}) \cap \mathcal{C}(\mathcal{O}_\mathfrak{p}) \,.$$

Now, $\mathcal{C}$ has relative dimension one over $\mathcal{O}_{K,S}$, so if we can find locally p-adic analytic functions on $\mathcal{J}(\mathcal{O}_\mathfrak{p})$ which vanish identically on $\mathcal{J}(\mathcal{O}_{K,S})$ but do not vanish identically on $\mathcal{C}(\mathcal{O}_\mathfrak{p})$, we will be able to prove that the intersection, and therefore $\mathcal{C}(\mathcal{O}_{K,S})$, is finite.

Let $\dim \mathcal{J}$ denote the relative dimension of $\mathcal{J}$ over $\mathcal{O}_{K,S}$. Then, $\mathcal{J}(\mathcal{O}_\mathfrak{p})$ is a $\mathbb{Q}_p$-analytic manifold (in the naïve sense of Serre [Ser65] or [Ser06, Part 2, Section 3]) of dimension $(\dim \mathcal{J}) \cdot [K_\mathfrak{p} : \mathbb{Q}_p]$.

Also, $\mathcal{J}(\mathcal{O}_{K,S})$ is a finitely generated group of some rank r. As we will see, its closure $\overline{\mathcal{J}(\mathcal{O}_{K,S})}$ in $\mathcal{J}(\mathcal{O}_{K_\mathfrak{p}})$ is a p-adic Lie subgroup of some dimension $\rho \leq r$. If $\rho < (\dim \mathcal{J}) \cdot [K_\mathfrak{p} : \mathbb{Q}_p]$, then $\overline{\mathcal{J}(\mathcal{O}_{K,S})} \subsetneqq \mathcal{J}(K_\mathfrak{p})$ will be a proper p-adic analytic Lie subgroup. Since $\mathcal{C}$ is an irreducible curve, if $\mathcal{C}(\mathcal{O}_\mathfrak{p})$ is not contained in $\overline{\mathcal{J}(\mathcal{O}_{K,S})}$, the intersection

$$\overline{\mathcal{J}(\mathcal{O}_{K,S})} \cap \mathcal{C}(\mathcal{O}_\mathfrak{p})$$

will be finite.

Indeed, when $K = \mathbb{Q}_p$ and $j : \mathcal{C} \to \mathcal{J}$ is an Abel-Jacobi embedding of a proper curve into its Jacobian, this is what Chabauty proved.

Theorem 3.1.1 ([Cha41], as stated in [MP12, Theorem 4.4])**.** *Let X be a smooth, projective, geometrically integral curve of genus $g \geq 2$ over $\mathbb{Q}$. Let J be the Jacobian of X. Let p be a prime and let $\rho = \dim \overline{J(\mathbb{Q})} \leq \operatorname{rank} J(\mathbb{Q})$. Suppose that $\rho < g$. Then, $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. It follows that $X(\mathbb{Q})$ is finite as well.*

Chabauty's original result was not effective. Coleman later used his theory of p-adic integration to show how to explicitly compute equations vanishing on $\overline{\mathcal{J}(\mathcal{O}_{K,S})}$. The remainder of this section is an overview of the ideas needed for Coleman's approach, followed by some more recent further improvements.

3.2 The p-adic logarithm map

In this section, we assume that $K_\mathfrak{p}$ is a p-adic field with ring of integers $\mathcal{O}_\mathfrak{p}$. Let $\mathcal{J}$ be a semi-abelian variety over $\mathcal{O}_\mathfrak{p}$ of relative dimension n.

The set $\mathcal{J}(K_\mathfrak{p})$ has the structure of a $\mathbb{Q}_p$-Lie group of dimension $n \cdot [K_\mathfrak{p} : \mathbb{Q}_p]$. Let e be the identity element of $J(K_\mathfrak{p})$ and write $\operatorname{Lie} \mathcal{J}_{K_\mathfrak{p}}$ for the Lie algebra of $\mathcal{J}(K_\mathfrak{p})$, i.e. the tangent space of $\mathcal{J}(K_\mathfrak{p})$ at e.

Since $\mathcal{J}$ is of finite type, $\mathcal{J}(\mathcal{O}_\mathfrak{p})$ has the structure of a profinite group. The profinite topology agrees with the topology from $\mathcal{J}(K_\mathfrak{p})$.

In particular, for any $x \in \mathcal{J}(\mathcal{O}_\mathfrak{p})$, there is some increasing sequence of positive integers n_i such that $\lim_{i\to\infty} x^{n_i} = e$. [Bou98, III.7.6., Proposition 10] says that there is a unique p-adic analytic homomorphism

$$\log : \mathcal{J}(\mathcal{O}_\mathfrak{p}) \to \operatorname{Lie} \mathcal{J}_{K_\mathfrak{p}} ,$$

called the *p-adic logarithm*, which is injective with analytic inverse after restricting the domain and codomain to suitable open subgroups.

The p-adic logarithm map can be understood explicitly as an antiderivative, as we now explain.

Let $H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1)_{\text{inv}}$ denote the vector space of translation-invariant global differentials on $\mathcal{J}_{K_\mathfrak{p}}$. We have

$$\dim_{K_\mathfrak{p}} H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1)_{\text{inv}} = n .$$

Let $\omega \in H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1)_{\text{inv}}$ and choose local coordinates $t_1, \ldots, t_n$ on $\mathcal{J}_{K_\mathfrak{p}}$ at e. In a

neighborhood of e, the 1-form ω can be expanded as a power series

$$\omega|_U = \sum_{i=1}^{g+\gamma} F_i(t_1, \ldots, t_{g+\gamma}) dt_i \,.$$

Integrating the power series formally, and restricting U further if necessary gives a map

$$\begin{aligned} \eta : U &\to K_{\mathfrak{p}} \,, \\ P &\to \int_e^P \omega \,. \end{aligned}$$

The map η extends uniquely to a homomorphism $\eta : \mathcal{J}(\mathcal{O}_{\mathfrak{p}}) \to K_{\mathfrak{p}}$.

We abuse notation slightly and write $\int_e^P \omega$ for η, even when P is not in the radius of convergence of the p-adic power series.

Now, formal integration is linear in the differential form, so in fact, this defines a homomorphism:

$$H^0(\mathcal{J}_{K_{\mathfrak{p}}}, \Omega^1)_{\text{inv}} \to \text{Hom}(\mathcal{J}(\mathcal{O}_{\mathfrak{p}}), K_{\mathfrak{p}}) \,.$$

Equivalently, we have a morphism of p-adic Lie groups

$$\log : \mathcal{J}(\mathcal{O}_{\mathfrak{p}}) \to (H^0(\mathcal{J}_{K_{\mathfrak{p}}}, \Omega^1)_{\text{inv}})^\vee \cong \text{Lie}\, \mathcal{J}_{K_{\mathfrak{p}}} \,,$$

which can be identified with the p-adic logarithm map defined earlier.

This map can be written explicitly as follows: Let $\{\omega_1, \ldots, \omega_n\}$ be a basis for $H^0(\mathcal{J}_{K_{\mathfrak{p}}}, \Omega^1)_{\text{inv}}$. Taking the dual basis determines an isomorphism $\text{Lie}\, \mathcal{J}_{K_{\mathfrak{p}}} \cong K_{\mathfrak{p}}^n$. In this setup, the logarithm map can be written explicitly as

$$\begin{aligned} \log : \mathcal{J}(\mathcal{O}_{\mathfrak{p}}) &\to K_{\mathfrak{p}}^n \,, \\ P &\mapsto \left(\int_e^P \omega_1, \ldots, \int_e^P \omega_n \right) \,. \end{aligned}$$

Since the logarithm map is a homomorphism and $K_{\mathfrak{p}}^n$ is torsion-free, we see that

the torsion subgroup of $\mathcal{J}(\mathcal{O}_{K_\mathfrak{p}})$ is contained in ker(log). In fact, these sets are equal.

The p-adic logarithm map is a local homeomorphism, with inverse defined on a neighborhood of 0 by a formal exponential map. As a consequence, we have:

Proposition 3.2.1. *Suppose that $G \subset \mathcal{J}(\mathcal{O}_\mathfrak{p})$ is a rank r finitely-generated subgroup. The closure $\overline{G}$ of G in $\mathcal{J}(K_\mathfrak{p})$ is a p-adic Lie subgroup of dimension $\rho \leq r$.*

Proof. Since log is a homomorphism and ker(log) consists of torsion elements, $\log G \subset K_\mathfrak{p}$ is a finitely-generated subgroup of rank r. Then, $\overline{\log G} = \mathbb{Z}_p \cdot \log G$ is a p-adic Lie subgroup of $K_\mathfrak{p}^n$. Moreover,

$$\rho = \operatorname{rank}_{\mathbb{Z}_p} \mathbb{Z}_p \cdot \log G \leq \operatorname{rank} G = r\,.$$

Since log is locally a homeomorphism, $\log \overline{G} = \overline{\log G}$ and so $\overline{G}$ is a p-adic Lie subgroup of $J(K_\mathfrak{p})$ of dimension $\rho \leq r$. □

Remark 3.2.2. Let G be as in Proposition 3.2.1. The set $\overline{G}$ has a natural $\mathbb{Z}_p$-structure, but in general will not carry an $\mathcal{O}_\mathfrak{p}$-structure. If we want to construct locally $K_\mathfrak{p}$-analytic functions which vanish on G, we can do the following.

Let $\rho' = \dim_{\mathcal{O}_\mathfrak{p}} \mathcal{O}_\mathfrak{p} \cdot \log G$. Clearly $\rho' \leq \rho$.

When $\rho' < n$, we construct $n - \rho'$ functions on $\mathcal{J}(\mathcal{O}_\mathfrak{p})$ which vanish on G.

1. Fix a set of generators $\{P_1, \ldots, P_r\}$ for a finite index subgroup of G.

2. Compute the images $\log(P_1), \ldots, \log(P_r)$ and put them in the rows of a matrix M. The resulting matrix has rank ρ' over $K_\mathfrak{p}$.

3. Let $\vec{a}_1 = (a_{1,1}, \ldots, a_{n,1}), \ldots, \vec{a}_{n-\rho'}$ span the kernel of M.

4. Set $\omega'_j = \sum_{i=1}^n a_{i,j}\omega_i$. The functions

$$\begin{aligned} \eta_j : \mathcal{J}(\mathcal{O}_\mathfrak{p}) &\to K_\mathfrak{p} \\ P &\mapsto \int_\epsilon^P \omega'_j \end{aligned} \tag{3.2.3}$$

for $j = 1, \ldots, n - \rho'$ vanish whenever $P \in \{P_1, \ldots, P_r\}$. Since the ω_i are translation-invariant, by additivity, the η_j vanish on all of G.

We typically hope to apply this construction to the finitely generated subgroup $\mathcal{J}(\mathcal{O}_{K,S})$.

Remark 3.2.4. Unfortunately, the functions constructed in Remark 3.2.2 are somewhat inefficient. As a $\mathbb{Q}_p$ Lie group, their common vanishing locus has dimension $\rho' \cdot [K_\mathfrak{p} : \mathbb{Q}_p]$, which could be much larger than $\rho = \dim \overline{G}$.

Of course this problem does not exist when $K_\mathfrak{p} = \mathbb{Q}_p$. If we replaced $\mathcal{J}_{K_\mathfrak{p}}$ with $\mathrm{Res}_{K_\mathfrak{p}/\mathbb{Q}_p} \mathcal{J}_{K_\mathfrak{p}}$ before taking integrals, this problem would go away. Later on, we take this restriction of scalars at the level of number fields, which also allows us to use information from other primes above p.

Suppose now that we are in the situation where $j : \mathcal{C} \to \mathcal{J}$ is an Abel-Jacobi embedding of a curve into generalized Jacobian (in the sense of Section 2.2). Take $G = \mathcal{J}(\mathcal{O}_{K,S})$ in Remark 3.2.2. Although is is possible that $\rho' < r$, in the typical case, we expect that $r = \rho'$. For instance, under Leopoldt's Conjecture, $r = \rho'$ whenever $g_\mathcal{C} = 0$.

In particular, we know that Chabauty's method will prove that $\mathcal{C}(\mathcal{O}_{K,S})$ is finite when $r \leq \dim \mathcal{J}_K - 1$.

To ease our future discussion of when Chabauty's method applies, we make the following definition.

Definition 3.2.5. Let $\mathcal{C}/\mathcal{O}_{K,S}$ be a sound clearance hole curve. Let $\mathcal{J}$ be the generalized Jacobian of $\mathcal{C}$.

We say that the pair $(\mathcal{C}, \mathcal{O}_{K,S})$ *satisfies the classical Chabauty inequality* if

$$\operatorname{rank} \mathcal{J}(\mathcal{O}_{K,S}) \leq \dim \mathcal{J}_K - 1\,. \tag{3.2.6}$$

3.3 Coleman's approach

In this section, we discuss Coleman's approach to computing the p-adic analytic functions constructed in Remark 3.2.2 and bounding the number of points of $\mathcal{C}(\mathcal{O}_{K,S})$.

The key idea is to replace integration on the Jacobian (which is hard to compute) with integration on the curve (which is easier to compute).

The morphism $j : \mathcal{C} \to \mathcal{J}$ induces a homomorphism of vector spaces

$$j^* : H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1) \to H^0(\mathcal{C}_{K_\mathfrak{p}}, \Omega^1)\,.$$

Remark 3.3.1. If $\mathcal{J}_{K_\mathfrak{p}}$ is the generalized Jacobian of $\mathcal{C}_{K_\mathfrak{p}}$, the morphism j^* induces an isomorphism of $K_\mathfrak{p}$-vector spaces

$$j^* : H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1)_{\text{inv.}} \to H^0(\mathcal{C}_{K_\mathfrak{p}}, \Omega^1(\log)),$$

where $\Omega^1(\log)$ denotes the sheaf of meromorphic 1-forms with poles of order at most 1 at the punctures of $\mathcal{C}_{K_\mathfrak{p}}$ and no other poles. (See [Ser88, Section V.2.10])

Suppose that P_1 and P_2 reduce to the same point of $\mathcal{C}(\mathbb{F}_\mathfrak{p})$. Then, for any $\omega \in H^0(\mathcal{J}_{K_\mathfrak{p}}, \Omega^1)_{\text{inv.}}$, we have

$$\int_e^{[P_1 - P_2]} \omega = \int_{P_1}^{P_2} j^*\omega\,,$$

where the second integral is given by formal integration of power series in terms of a local parameter on $\mathcal{C}$.

More precisely, fix $Q \in \mathcal{C}(\mathbb{F}_\mathfrak{p})$ and let $t \in \mathcal{O}_{\mathcal{C},Q}$ be such that the restriction to the special fiber $t|_{\mathcal{C}_{\mathbb{F}_\mathfrak{p}}}$ is a uniformizer at Q. The map

$$t : \{P \in \mathcal{C}(\mathcal{O}_\mathfrak{p}) : P \pmod{\mathfrak{p}} = Q\} \xrightarrow{\sim} \mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}$$

from the residue disc around P to $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a bijection. Moreover, if $\omega \neq 0$, then up to scaling by an element of $K_\mathfrak{p}^\times$, the 1-form $j^*\omega$ can be written in the form $f(t)dt$ for some $f \in \mathcal{O}_\mathfrak{p}[[t]]$. We may assume that some coefficient of f lies in $\mathcal{O}_\mathfrak{p}^\times$. Let F be the formal antiderivative of f. Then

$$\int_{P_1}^{P_2} j^*\omega = \int_{t(P_1)}^{t(P_2)} f(t)\,dt = F(t(P_2)) - F(t(P_1))\,.$$

If we take $\omega \neq 0$ such that

$$\int_e^P \omega = 0$$

for all $P \in \mathcal{J}(\mathcal{O}_{K,S})$ as in Remark 3.2.2, and fix a basepoint P_0 in each residue disc on $\mathcal{C}$, we can bound $\#\mathcal{C}(\mathcal{O}_{K,S})$ by using Newton polygons to bound the number of zeros of $F(t(P)) - F(t(P_0))$ on each residue disc based on the p-adic valuations of the coefficients of F.

With this approach, Coleman proved

Theorem 3.3.2 ([Col85, Corollary 4a]). *Let X be a smooth, projective, geometrically integral curve of genus $g \geq 2$ over K. Let J be the Jacobian of X. Let $\mathfrak{p}$ be a prime of K which is unramified over $\mathbb{Q}$, lying above $p > 2g$. Let $\rho = \dim \overline{J(\mathbb{Q})} \leq \operatorname{rank} J(\mathbb{Q})$. Suppose that $\rho < g$. Then,*

$$\#X(K) \leq \#X(\mathbb{F}_\mathfrak{p}) + (2g - 2)\,.$$

Coleman also showed how to bound $\#X(K)$ when $p \leq 2g$, although the bounds are not as good.

Remark 3.3.3. In Remark 3.2.2, we constructed at least $\dim \mathcal{J}_K - \rho$ functions simultaneously vanishing on $\mathcal{J}(\mathcal{O}_\mathfrak{p})$. If one considers all of these functions instead of a single function, [Sto06, Corollary 6.7] shows that Coleman's bound can be improved to $\#X(\mathbb{F}_\mathfrak{p}) + 2\rho$.

The same ideas used by Coleman and Stoll apply to bound $\mathcal{O}_{K,S}$ points on a sound clearance hole curve $\mathcal{C}/\mathcal{O}_{K,S}$, although the bounds produced by the method may be different.

Chapter 4

Chabauty for Restrictions of Scalars

This section aims to give an overview of Chabauty's method for restrictions of scalars of curves (or *RoS Chabauty*, for short). Our description differs from Siksek [Sik13] in two main ways. First, with an eye towards testing the theory on the unit equation, we develop the method for S-integral points on models of curves which may not be complete. Second, after taking restrictions of scalars, we consider points valued in the Galois closure of the field that we start with. This simplifies the multivariate p-adic power series that appear when applying the method.

4.1 Introduction to RoS Chabauty

The classical Chabauty inequality (3.2.6) is somewhat inefficient in two ways:

1. As we saw in Remark 3.2.4, the vanishing locus of the Chabauty functions can be much larger than $\overline{\mathcal{J}(\mathcal{O}_{K,S})}$, especially when $[K_{\mathfrak{p}} : \mathbb{Q}_p]$ is large.

2. If p splits in K, the classical Chabauty-Coleman approach uses information only at one of the primes $\mathfrak{p}$ lying over p.

We can solve both of these problems and weaken the hypothesis of classical Chabauty somewhat using restriction of scalars, as follows:

Set

$$\mathcal{V} := \mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{C} \quad \text{and} \quad \mathcal{A} := \mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}.$$

The map j induces a generically finite map $j : \mathcal{V} \hookrightarrow \mathcal{A}$. Similarly to classical Chabauty, there is a commutative diagram:

$$\begin{array}{ccccc} \mathcal{C}(\mathcal{O}_{K,S}) & = & \mathcal{V}(\mathbb{Z}_{S'}) & \hookrightarrow & \mathcal{V}(\mathbb{Z}_p) \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{J}(\mathcal{O}_{K,S}) & = & \mathcal{A}(\mathbb{Z}_{S'}) & \hookrightarrow & \mathcal{A}(\mathbb{Z}_p). \end{array} \tag{4.1.1}$$

We observe:

1. Although $\mathcal{A}$ might not be semi-abelian, there is a logarithm map

$$\log\colon \mathcal{A}(\mathbb{Z}_p) \to \mathbb{Q}_p^{d\cdot \dim \mathcal{J}_K}$$

much like in the case of classical Chabauty, even if p is ramified in K. In particular, $\mathcal{A}(\mathbb{Z}_p)$ is a p-adic Lie group of dimension $d \cdot \dim(\mathcal{J})$ over $\mathbb{Z}_p$.

2. The closure of $\mathcal{A}(\mathbb{Z}_{S'}) \subset \mathcal{A}(\mathbb{Z}_p)$ in the p-adic topology is a p-adic Lie group of dimension ρ over $\mathbb{Z}_p$ for some $\rho \leq r$. In contrast to classical Chabauty (as described in Section 3 and in particular Remark 3.2.4,) the set $\overline{\mathcal{A}(\mathbb{Z}_{S'})}$ is finite-index in some subgroup cut out by locally analytic p-adic functions obtained by composing log with linear functionals $\mathbb{Q}_p^{d\cdot \dim \mathcal{J}_K} \to \mathbb{Q}_p$.

3. Inside of $\mathcal{J}(\mathcal{O}_{\mathfrak{p}})$, we have the inclusion

$$\mathcal{C}(\mathcal{O}_{K,S}) = \mathcal{V}(\mathbb{Z}_{S'}) \subseteq \mathcal{V}(\mathbb{Z}_p) \cap \overline{\mathcal{A}(\mathbb{Z}_{S'})}. \tag{4.1.2}$$

If $\mathrm{codim}(\mathcal{V}, \mathcal{A}) + \mathrm{codim}(\overline{\mathcal{A}(\mathbb{Z}_{S'})}, \mathcal{A}(\mathbb{Z}_p)) \geq \dim \mathcal{A}$, or equivalently if

$$\rho \leq d(\dim \mathcal{J}_{\mathcal{C}} - 1), \tag{4.1.3}$$

then if the intersection is 'sufficiently generic' (e.g. transverse) the right-hand side of (4.1.2) will consist of isolated points, which would imply that $\mathcal{C}(\mathcal{O}_{K,S})$ is finite.

By analogy with the classical case, we make the following definition.:

Definition 4.1.4. Let $\mathcal{C}/\mathcal{O}_{K,S}$ be a sound clearance hole curve (see Definition 2.1.1) and let $\mathcal{J}$ be the generalized Jacobian of $\mathcal{C}$ in the sense of Section 2.2.

The pair $(\mathcal{C}, \mathcal{O}_{K,S})$ *satisfies the RoS Chabauty inequality* if

$$r \leq d(\dim \mathcal{J}_K - 1). \tag{4.1.5}$$

Since the generic fiber of $\mathcal{A}$ is a semiabelian variety, we can still understand the logarithm map in terms of integration on $\mathcal{A}$. In particular, the vector space

$$\Omega' := \left\{ \omega \in H^0(\mathcal{A}_{\mathbb{Q}_p}, \Omega^1)_{\text{inv}} : \int_0^P \omega = 0 \text{ for all } P \in \mathcal{A}(\mathbb{Z}_{S'}) \right\}, \tag{4.1.6}$$

has dimension at least $d \cdot \dim \mathcal{J}_K - r$, and

$$\overline{\mathcal{J}(\mathcal{O}_{K,S})} = \overline{\mathcal{A}(\mathbb{Z}_{S'})} \subseteq \left\{ P \in \mathcal{A}(\mathbb{Z}_p) : \int_0^P \omega = 0 \text{ for all } \omega \in \Omega' \right\}.$$

Analogously to the classical Chabauty case, when $P_1, P_2 \in \mathcal{A}(\mathbb{Z}_{S'})$ are the images of points of $\mathcal{V}(\mathbb{Z}_{S'})$ and ω is an invariant differential, we can compute the integral

$$\int_{P_1}^{P_2} \omega$$

on $\mathcal{V}$ by taking a pullback. More precisely, fix $Q \in \mathcal{V}(\mathbb{F}_p)$ and let $t_1, \ldots, t_d$ in the local ring $\mathcal{O}_{\mathcal{V},Q}$ be generators for the maximal ideal $\mathfrak{m}_{\mathcal{V},Q}$ of $\mathcal{O}_{\mathcal{V},Q}$. The functions $t_1, \ldots, t_d$ induce a map

$$(t_1, \ldots, t_d) : \{P \in \mathcal{V}(\mathcal{O}_\mathfrak{p}) : P \pmod p = Q \xrightarrow{\sim} (p\mathbb{Z}_p)^d,$$

which is a bijection from the residue disc around P to $(p\mathbb{Z}_p)^d$. Much like in the classical case, after possibly changing scaling by an element of $\mathbb{Q}_p^\times$, the 1-form $j^*\omega$

can be written in the form $\sum_{j=1}^{d} f_j(t_1, \ldots, t_d)dt_j$ for some $f_1, \ldots, f_d \in \mathbb{Z}_p[[t_1, \ldots, t_d]]$ where some f_j has a coefficient in $\mathbb{Z}_p^\times$.

Since invariant 1-forms on $\mathcal{A}$ are closed and pullbacks of closed forms are closed, there is some $F_\omega \in \mathbb{Q}_p[[t_1, \ldots, t_d]]$ such that $dF_\omega = \omega$

Then, for P_1 and P_2 in the same residue disc as P, we have

$$\int_{P_1}^{P_2} j^*(\omega) = F_\omega((t_1, \ldots, t_d)(P_2)) - F_\omega((t_1, \ldots, t_d)(P_1)) .$$

Notably, the functions F_ω are no longer expressible as (locally) p-adic analytic functions in a single variable. Instead, on sufficiently small balls, the F_ω will be given by d-variable power series which converge on a neighborhood of the balls.

Let $\mathbb{C}_p$ be a completion of $\overline{\mathbb{Q}_p}$ and let $\mathcal{O}_{\mathbb{C}_p}$ be its ring of integers.

Given d linearly independent one-forms ω and $\alpha \in \mathbb{Q}$, such that the F_ω converge on a neighborhood of $P + p^\alpha \mathcal{O}_{\mathbb{C}_p}^d$, the common vanishing locus of these power series will have finitely many isolated points in the disc $P + p^\alpha \mathcal{O}_{\mathbb{C}_p}^d$.

However, if we are unlucky (or in a bad situation), the common vanishing locus of these functions may not consist exclusively of isolated points. Unfortunately, such bad situations can occur for a geometric reason.

Before continuing with the development of RoS Chabauty, we discuss two geometric reasons why the common vanishing locus of the F_ω for the curve $\mathcal{C}/\mathcal{O}_{K,S}$ may not consist of isolated points.

One such geometric obstruction occurs when $\mathcal{C}$ is the base change of a curve $\mathcal{D}$ for which the vanishing locus of the F_ω in $(\operatorname{Res}\mathcal{D})(\mathbb{Z}_p)$ is infinite (e.g., because $\mathcal{D}$ does not satisfy the RoS Chabuaty inequality.)

A second geometric obstruction occurs when there is a morphism $f : \mathcal{C} \to \mathcal{D}$ such that the vanishing locus of the F_ω for $\mathcal{D}$ does not consist of isolated points and the Prym scheme $\mathcal{P}$ (the group scheme quotient $\mathcal{P} := \mathcal{J}_\mathcal{C}/f^*(\mathcal{J}_\mathcal{D})$) has the property that the p-adic closure

$$\overline{(\operatorname{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathcal{O}_{K,S})} \subset (\operatorname{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_p)$$

is finite-index.

We discuss these obstructions, which we call *base change obstructions* and *full Prym obstructions* in the next two sections.

In all known cases where $\mathcal{V}(\mathbb{Z}_p) \cap \overline{\mathcal{A}(\mathbb{Z}_{S'})}$ does not consist of finitely many isolated points, it can be explained by iterated application of these obstructions.

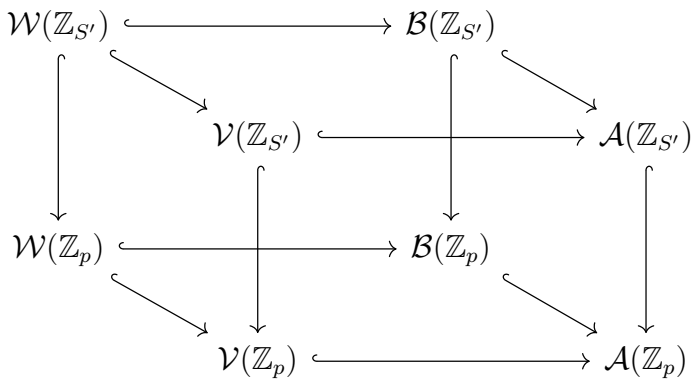
4.2 Base change obstructions

Suppose that $k \subset K$ is a subfield and that S_k is the set of primes of k lying under primes in S. Suppose also that $\mathcal{D}/\mathcal{O}_{k,S_k}$ is a sound clearance hole curve which becomes isomorphic to $\mathcal{C}$ after base change to $\mathcal{O}_{K,S}$, i.e., a curve such that

$$\mathcal{D}_{\mathcal{O}_{K,S}} \cong \mathcal{C}.$$

We also have $(\mathcal{J}_{\mathcal{D}})_{\mathcal{O}_{K,S}} \cong \mathcal{J}_{\mathcal{C}}$ compatibly with the Abel-Jacobi maps.

Letting $\mathcal{W} := (\mathrm{Res}_{\mathcal{O}_{k,S_k}/\mathbb{Z}_{S'}} \mathcal{D})$ and $\mathcal{B} := (\mathrm{Res}_{\mathcal{O}_{k,S_k}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})$, we have the following commutative diagram:



Clearly, $\mathcal{W}(\mathbb{Z}_p) \cap \overline{\mathcal{B}(\mathbb{Z}_{S'})} \subset \mathcal{V}(\mathbb{Z}_p) \cap \overline{\mathcal{A}(\mathbb{Z}_{S'})}$ inside of $\mathcal{A}(\mathbb{Z}_p)$. If

$$\dim \overline{\mathcal{B}(\mathbb{Z}_{S'})} > [k : \mathbb{Q}] \cdot (\dim \mathcal{J}_{\mathcal{D}} - 1),$$

then $\mathcal{W}(\mathbb{Z}_p) \cap \overline{\mathcal{B}(\mathbb{Z}_{S'})}$ will (typically) have positive dimension as a p-adic analytic variety in the sense of [Ser65], so $\mathcal{V}(\mathbb{Z}_p) \cap \overline{\mathcal{A}(\mathbb{Z}_{S'})}$ will have positive dimension as a p-adic analytic variety as well. In particular, both sets will be infinite.

Based on this observation, we say

Definition 4.2.1. A *base change obstruction* to RoS Chabauty for $(\mathcal{C}, \mathcal{O}_{K,S})$ is a pair $(\mathcal{D}, \mathcal{O}_{k,S_k})$ where k is a subfield of K, S_k is the set of primes of k lying under primes in S, $\mathcal{D}$ is a sound clearance hole curve over $\mathcal{O}_{k,S_k}$, and $\mathcal{D}_{\mathcal{O}_{K,S}} \cong \mathcal{C}$ such that

$$j((\mathrm{Res}_{\mathcal{O}_{k,S_k}/\mathbb{Z}_{S'}} \mathcal{D})(\mathbb{Z}_p)) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{k,S_k}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_{S'})}$$

inside $(\mathrm{Res}_{\mathcal{O}_{k,S_k}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_p)$ is infinite.

A *strong base change obstruction* to RoS Chabauty is a base change obstruction such that

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{k,S_k}) > [k : \mathbb{Q}] \cdot (\dim \mathcal{J}_{\mathcal{D}} - 1)\,. \tag{4.2.2}$$

This is the inequality that one would expect to lead to the above intersection being infinite (although this implication does not always hold.) If no such $\mathcal{D}$ exists, we say that $(\mathcal{C}, \mathcal{O}_{K,S})$ *has no strong base change obstruction to RoS Chabauty.*

Strong base change obstructions do show up in practice.

Example 4.2.3. If $\mathcal{C} = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$, K is a CM sextic field, and k is the totally real cubic subfield of K, then $\mathcal{J} \cong \mathbb{G}_m \times \mathbb{G}_m$ and

$$2 \cdot \operatorname{rank} \mathcal{O}_K^\times = 4 \leq 6 = [K : \mathbb{Q}] \cdot 1\,,$$

so (4.1.5) holds. Also

$$2 \cdot \operatorname{rank} \mathcal{O}_k^\times = 4 > 3 = [k : \mathbb{Q}] \cdot 1\,,$$

so (4.2.2) also holds. It follows that if the intersection in Definition 4.2.1 is infinite, then $(\mathbb{P}^1_{\mathcal{O}_k} \smallsetminus \{0, 1, \infty\}, \mathcal{O}_k)$ is a strong base change obstruction to RoS Chabauty for $(\mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0, 1, \infty\}, \mathcal{O}_K)$. This is the case in typical examples.

Example 4.2.4. If $\mathcal{C}/\mathbb{Q}$ is a smooth projective curve of genus g and K is a number field with

$$\operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathbb{Q}) \geq g,$$

but

$$\operatorname{rank} \mathcal{J}_{\mathcal{C}}(K) \leq [K : \mathbb{Q}] \cdot (g-1),$$

then $(\mathcal{C}, \mathbb{Q})$ is typically a strong base change obstruction to RoS Chabauty for $(\mathcal{C}, K)$.

4.3 Full Prym obstructions

In [Dog19], Dogra shows that there is another geometric reason that the intersection why RoS Chabauty sometimes fails to prove finiteness of rational points. In this section, we give a heuristic-based explanation of the situation that [Dog19] describes.

Suppose that $\mathcal{C} \to \mathcal{D}$ is a finite morphism of sound clearance hole curves over $\mathcal{O}_{K,S}$. Suppose that the following running assumptions (for this section) hold:

(i) The intersection $Z := (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{D})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_{S'})}$ is infinite. In particular, this means that RoS Chabauty fails to prove that $\mathcal{D}(\mathcal{O}_{K,S})$ is finite.

(ii) $\operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) - \operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}) \geq [K : \mathbb{Q}] \cdot (\dim \mathcal{J}_{\mathcal{C}} - \dim \mathcal{J}_{\mathcal{D}})$.

Under these conditions, we will now explain why the intersection

$$(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{C})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'})}$$

is likely to be infinite, so that RoS Chabauty will fail to prove that $\mathcal{C}(\mathcal{O}_{K,S})$ is finite.

Note that there are pullback and pushforward maps $f^*\colon \mathcal{J}_{\mathcal{C}} \to \mathcal{J}_{\mathcal{D}}$ and $f_*\colon \mathcal{J}_{\mathcal{D}} \to \mathcal{J}_{\mathcal{C}}$. Let $\mathcal{P} := \ker(f_*)$ and let $G := \operatorname{coker}(\mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) \to \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}))$.

We have the exact sequence

$$0 \to \mathcal{P}(\mathcal{O}_{K,S}) \to \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) \to \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}) \to G \to 0$$

which we can rewrite as

$$0 \to (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_{S'}) \to (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'}) \to (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_{S'}) \to G \to 0\,.$$

Now imagine that the following hypotheses hold:

1. $G = \{1\}$, i.e., $f_*\colon \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) \to \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S})$ is surjective,

2. $(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_{S'})$ is dense in $(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_p)$,

3. $f\colon \mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p) \to \mathcal{D}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p)$ is surjective.

From hypotheses 1 and 2, for each $P \in Z \subset \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_{S'})}$, the p-adic closure $\overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'})}$ would contain $(f_*)^{-1}(P)$.

$$f^{-1}(Z) \subset (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{C})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'})}\,.$$

Under hypothesis 3, $f^{-1}(P) \subset \mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}}(\mathbb{Z}_p)$ is non-empty for each $P \in Z$, so $f^{-1}(Z)$ is infinite as well. Hence, these conditions would imply that $(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{C})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'})}$ is infinite.

We illustrate this situation with the further approximation $\mathcal{J}_{\mathcal{C}} \approx \mathcal{J}_{\mathcal{D}} \times \mathcal{P}$ in Figure 4-1.

In practice, these hypotheses 1, 2, and 3 are unlikely to hold. However, as we now discuss, each is likely to hold *up to finite index/on an open subset of* Z under running assumptions (i) and (ii).

Since $f_* \circ f^*$ is the multiplication by $\deg(f)$ map and $\mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S})$ is finitely generated, G is a finite group, so 1 is true up to finite index.

For 2, note that

$$\mathrm{rank}(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_{S'}) = \mathrm{rank}\, \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) - \mathrm{rank}\, \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S})$$

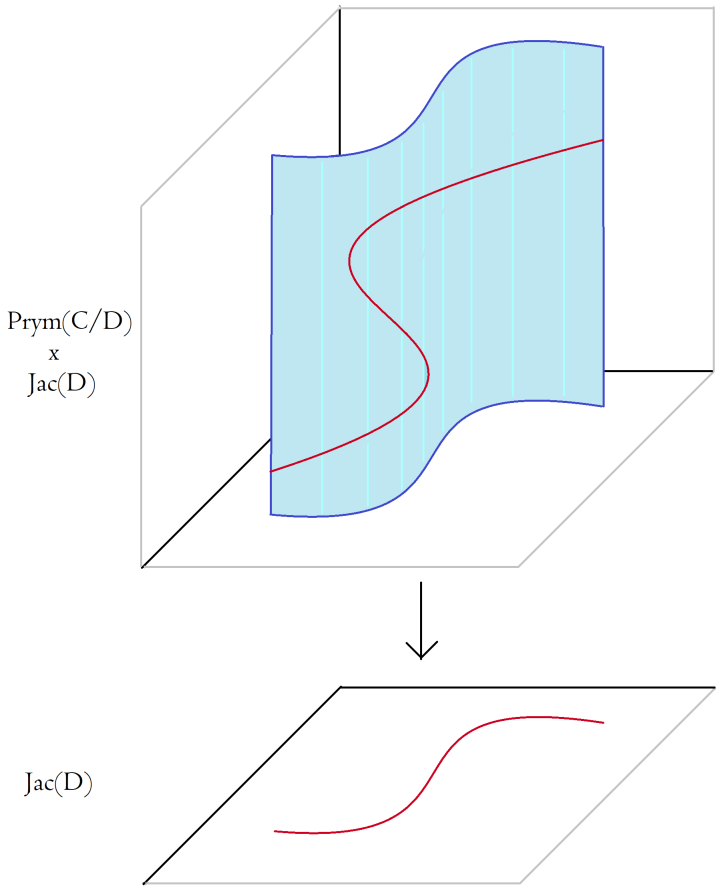


Figure 4-1: An approximate graphical illustration of a full Prym obstruction. In the notation of this section, the curve downstairs is $Z = \overline{(\mathrm{Res}\,\mathcal{J}_{\mathcal{D}})(\mathcal{O}_{K,S})} \cap (\mathrm{Res}\,\mathcal{D})(\mathbb{Z}_p)$. Upstairs, $\overline{(\mathrm{Res}(\mathcal{P} \times \mathcal{J}_{\mathcal{D}}))(\mathbb{Z}_p)}$ contains a finite index subgroup of the preimage $\pi^{-1}(Z)$ of the curve downstairs. The image of $(\mathrm{Res}\,\mathcal{C})(\mathbb{Z}_p)$ intersects $\pi^{-1}(Z)$ in the curve upstairs, and $(\phi \circ j)(\mathrm{Res}\,\mathcal{C})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}\,\mathcal{P} \times \mathcal{J}_{\mathcal{D}})(\mathcal{O}_{K,S})}$ contains this curve.

and

$$\dim(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P}) = [K:\mathbb{Q}] \cdot \dim \mathcal{P} = [K:\mathbb{Q}] \cdot (\dim \mathcal{J}_{\mathcal{C}} - \dim \mathcal{J}_{\mathcal{D}}) .$$

Running assumption (ii) says that

$$\mathrm{rank}(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_{S'}) \geq \dim(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P}),$$

so in generic situations, $\overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_{S'})}$ will be finite index in $(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{P})(\mathbb{Z}_p)$. Hence, 2 is likely to hold up to finite index.

Finally, 3 is a ultimately a statement about some collection of polynomials having roots over a local field with finite residue field. Suppose that $P \in \mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p)$. By the implicit function theorem, after a small p-adic perturbation, we may assume that f is étale at the $\mathbb{Q}_p$ points given by P. Then, by Krasner's lemma, for any $P \in \mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p)$, there is an open neighborhood U of $f(P) \in \mathcal{D}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p)$ such that $U \subset f(\mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p))$. In particular, if $\mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p) \neq \emptyset$ then $f(\mathcal{C}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p))$ contains a nonempty open subset of $\mathcal{D}(\mathcal{O}_{K,S} \otimes \mathbb{Z}_p)$.

Putting these together, under running assumptions (i) and (ii), we see that heuristically,

$$(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{C})(\mathbb{Z}_p) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{C}})(\mathbb{Z}_{S'})}$$

is likely to be infinite whenever it is nonempty, even if hypotheses 1, 2, and 3 are not satisfied on the nose. This seems especially likely in the case that $\mathcal{C}(\mathcal{O}_{K,S})$ is nonempty, which is often the case when trying to apply variants of the Chabauty–Coleman method in practice.

To capture situations where this sort of obstruction could exist, we make the following definition:

Definition 4.3.1. A *full Prym obstruction* to RoS Chabauty for $(\mathcal{C}, \mathcal{O}_{K,S})$ is a morphism $\mathcal{C} \to \mathcal{D}$ to a sound clearance hole curve $\mathcal{D}/\mathcal{O}_{K,S}$ such that both

(i)

$$j((\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{D})(\mathbb{Z}_p)) \cap \overline{(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_{S'})}$$

inside $(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}} \mathcal{J}_{\mathcal{D}})(\mathbb{Z}_p)$ is infinite and

(ii)
$$\operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) - \operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}) \geq [K:\mathbb{Q}] \cdot (\dim \mathcal{J}_{\mathcal{C}} - \dim \mathcal{J}_{\mathcal{D}}) .$$

Example 4.3.2. Full Prym obstructions (that are not simultaneously base change obstructions) do exist. Following [Dog19], take $b = \sqrt{11/27}$ and $K = \mathbb{Q}(b)$, to be the smooth projective genus 3 hyperelliptic curve C over K with affine model

$$y^2 = x^8 + \frac{2916 \cdot b + 484}{297} x^6 + \frac{-128304 \cdot b + 168112}{8019} x^4 + \frac{214057729 \cdot b - 35529472}{23181643} x^2 + \frac{-10784721024 \cdot b + 874208708}{64304361} .$$

One can compute that

$$\operatorname{rank} \mathcal{J}_C(K) = 4 < 6 = [K:\mathbb{Q}] \cdot \dim \mathcal{J}_C ,$$

so the RoS Chabauty inequality holds for C. One can also check that C is not a base change of any curve defined over $\mathbb{Q}$, so C does not have a base change obstruction.

On the other hand, C covers the base change D_K of the smooth, projective, genus 2 hyperelliptic curve $D/\mathbb{Q}$ with affine model

$$y^2 = \left(x^4 - \frac{11}{27}\right)\left(x^2 - \frac{27}{11}\right) .$$

We claim that $C \to D_K$ is a full Prym obstruction to RoS Chabuaty for C.

Now, $\mathcal{J}_D(\mathbb{Q})$ and $\mathcal{J}_D(K)$ both have rank 2. In particular,

$$\operatorname{rank} \mathcal{J}_D(\mathbb{Q}) = 2 > 1 = \dim \mathcal{J}_D - 1 ,$$

so it is plausible that D is a base change obstruction to RoS Chabauty for D_K. With a bit more work, one can show that this indeed the case. In particular, (i) of definition 4.3.1 is satisfied.

Moreover, the Prym variety of $C \to D_K$ is an elliptic curve E defined over K.

A computation shows that $\operatorname{rank} E(K) = 2$ and the p-adic closure $\overline{E(K)}$ is finite-index in $(\operatorname{Res}_{K/\mathbb{Q}} E)(\mathbb{Q}_p)$. Hence,

$$\operatorname{rank} \mathcal{J}_C(K) - \operatorname{rank} \mathcal{J}_D(K) = 2 \geq 2 = [K : \mathbb{Q}](\dim \mathcal{J}_C - \dim \mathcal{J}_D)\,,$$

so (ii) of definition 4.3.1 is also satisfied. Thus, there is a full Prym obstruction to RoS Chabauty for C. The preceding discussion suggests that the intersection of $(\operatorname{Res}_{K/\mathbb{Q}} C)(\mathbb{Q}_p)$ and $\overline{\mathcal{J}_C(K)}$ is likely to be infinite.

4.4 Simplifying regular differentials via base change

[Sik13] presents a sufficient condition to determine if the functions F_ω for $\omega \in \Omega'$ constructed in equation 4.1.6 have at most a single zero in a residue disc. The condition that [Sik13] presents is very computational and seems difficult to strengthen or to analyze in general. One difficulty is that the F_ω, when expressed as power series in local parameters on a disc, will typically have 'few' nonzero coefficients. For both computation and abstract reasoning, it would be nicer to express the F_ω in terms of sparse power series.

In this section, we describe a different approach, which allows us to do this. Our plan is to expand the F_ω as power series in local parameters which are defined only over a field extension of $\mathbb{Q}_p$. This will be useful in Chapter 6.

Suppose that p is unramified in $K/\mathbb{Q}$. Let $L_\mathfrak{P}$ be a finite extension of $\mathbb{Q}_p$ which is a splitting field for $K/\mathbb{Q}_p$. Then, $\#\operatorname{Hom}(K, L_\mathfrak{P}) = [K : \mathbb{Q}]$.

Let $\mathcal{O}_{L_\mathfrak{P}}$ denote the valuation ring of $L_\mathfrak{P}$. Then,

$$\mathcal{O}_{K,S} \otimes \mathcal{O}_{L_\mathfrak{P}} \cong \prod_\tau \mathcal{O}_{L_\mathfrak{P}}\,,$$

where τ ranges over $\operatorname{Hom}(\mathcal{O}_{K,S}, \mathcal{O}_{L_\mathfrak{P}}) = \operatorname{Hom}(K, L)$.

Now, suppose that $\mathcal{Z}$ is a quasi-projective $\mathcal{O}_{K,S}$-scheme. For τ as above, let $\mathcal{Z}_\tau$

over $\mathcal{O}_{L_\mathfrak{P}}$ be the base change. Then,

$$(\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}}\mathcal{Z})_{\mathcal{O}_{L_\mathfrak{P}}} \cong \prod_\tau \mathcal{Z}_\tau\,.$$

The composition

$$\mathcal{Z}(\mathcal{O}_{K,S}) = (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}}\mathcal{Z})(\mathbb{Z}_{S'}) \hookrightarrow (\mathrm{Res}_{\mathcal{O}_{K,S}/\mathbb{Z}_{S'}}\mathcal{Z})(\mathcal{O}_{L_\mathfrak{P}}) = \prod_\tau \mathcal{Z}_\tau(\mathcal{O}_\mathfrak{P})$$

is given by $P \mapsto (\tau(P))_\tau$.

Applying this for $\mathcal{Z} = \mathcal{C}$ and $\mathcal{Z} = \mathcal{J}$, we obtain a variant of the RoS Chabauty diagram (4.1.1). We have

$$\begin{array}{ccccccc} \mathcal{C}(\mathcal{O}_{K,S}) & = & \mathcal{V}(\mathbb{Z}_{S'}) & \hookrightarrow & \mathcal{V}(\mathcal{O}_{L_\mathfrak{P}}) & = & \prod_\tau \mathcal{C}_\tau(\mathcal{O}_\mathfrak{P}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{J}(\mathcal{O}_{K,S}) & = & \mathcal{A}(\mathbb{Z}_{S'}) & \hookrightarrow & \mathcal{A}(\mathcal{O}_{L_\mathfrak{P}}) & = & \prod_\tau \mathcal{J}_\tau(\mathcal{O}_\mathfrak{P}). \end{array} \tag{4.4.1}$$

The advantage of replacing the restrictions of scalars $\mathcal{V}$ and $\mathcal{A}$ by their base change to $\mathcal{O}_{L_\mathfrak{P}}$ is that the spaces of regular 1-forms can be related directly to the 1-forms on $\mathcal{J}$ and $\mathcal{C}$. Specifically,

$$H^0(\mathcal{A}_{L_\mathfrak{P}},\Omega^1)_{\mathrm{inv}} \cong H^0\left(\prod_\tau \mathcal{J}_\tau,\Omega^1\right)_{\mathrm{inv}} \cong \prod_\tau H^0(\mathcal{J}_\tau,\Omega^1)_{\mathrm{inv}} \cong \prod_\tau (H^0(\mathcal{J},\Omega^1)_{\mathrm{inv}} \otimes_{K,\tau} L_\mathfrak{P})$$

and similarly for $H^0(\mathcal{V}_{L_\mathfrak{P}},\Omega^1)_{\mathrm{inv}}$. For $\omega = (\omega_\tau)$ in $H^0(\mathcal{A}_{L_\mathfrak{P}},\Omega^1)_{\mathrm{inv}} = \prod_\tau (H^0(\mathcal{J},\Omega^1)_{\mathrm{inv}} \otimes_{K,\tau} L_\mathfrak{P})$ and $P = (P_\tau)$ in $\mathcal{A}(\mathcal{O}_{L_\mathfrak{P}}) = \prod_\tau \mathcal{J}_\tau(\mathcal{O}_{L_\mathfrak{P}})$, we have

$$\int_0^P \omega = \sum_\tau \int_0^{P_\tau} \omega_\tau\,.$$

Similarly, p-adic integrals on $\mathcal{V}_{L_\mathfrak{P}}$ decompose as a sum of integrals on the multiplicands $\mathcal{C}_\tau$. If we choose local parameters $t_1,\dots,t_d$ near $P = (P_\tau)$ in $\mathcal{V}(\mathcal{O}_{L_\mathfrak{P}}) = \prod_\tau \mathcal{C}_\tau(\mathcal{O}_{L_\mathfrak{P}})$ which are local parameters on the multiplicands, then for P_1, P_2 in the

same (sufficiently small) residue disc, there exist functions $F_{\omega,i} \in L_{\mathfrak{P}}[[t_i]]$ such that

$$\int_{P_1}^{P_2} j^*\omega = \sum_{i=1}^{d} F_{\omega,i}(t_i(P_1)) - F_{\omega,i}(t_i(P_2))\,.$$

In particular,

$$j^{-1}(\overline{\mathcal{J}(\mathcal{O}_{K,S})}) \subset \prod_{\tau} \mathcal{C}_\tau(\mathcal{O}_{L_{\mathfrak{P}}})$$

is contained in the vanishing locus of a collection of power series of this form, which we can compute explicitly by linear algebra analogous to that in Remark 3.2.2. Such power series are said to be *pure* because the coefficients of any mixed terms are zero. In particular, these power series are sparse.

This sparse representation comes at some cost – computations over $L_{\mathfrak{P}}$ are significantly more expensive than computations over $\mathbb{Q}_p$ and the $\mathcal{O}_{L_{\mathfrak{P}}}$-valued vanishing set of our equations may be larger than the set computed when working over $\mathbb{Z}_p$. This latter cost can be mitigated by keeping track of the action of $\mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p)$. We expect that the savings allowed by the sparse power series will compensate for the former cost in practice. And as we show in Chapter 6, this sparse representation is certainly helpful when trying to reason about RoS Chabauty for many base changes of a curve simultaneously.

Chapter 5

RoS Chabauty and Genus 0 Descent: General Theory

In this section, we combine Chabauty's method and RoS Chabauty with the method of descent, which reduces the problem of computing $\mathcal{C}(\mathcal{O}_{K,S})$ to computing $\mathcal{D}(\mathcal{O}_{K,S})$ for a finite set of curves which map to $\mathcal{C}$. We will be particularly interested in the case where the $\mathcal{C}$ and $\mathcal{D}$ are all sound clearance hole curves such that the generic fiber is a punctured genus zero curve, and the $\mathcal{D}$ are $\mathcal{G}$-torsors over $\mathcal{C}$ for some finite Galois group $\mathcal{G}$. We prove that in most cases, classical Chabauty's method together with Galois descent by genus 0 covers *cannot* succeed in proving that $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ is finite. In contrast, so long as K does not contain a CM subfield, RoS Chabauty applied to a suitable set of genus zero covers of $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ has no strong base change obstruction. For each cover in this set, there exists an $\alpha \in \mathcal{O}_{K,S}$ and and a morphism to $\mathcal{D}'_\alpha := \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{x \in \overline{K} \smallsetminus K : \alpha x^q - 1 = 0\}$. The $\mathcal{D}'_\alpha$ for α not a qth power have no obstruction to RoS Chabauty coming solely from a combination of strong base change and full Prym obstructions.

The review of generalized Jacobians of genus zero curves in Section 2.2.5 and the review of descent in Section 2.3 (particularly the classification of genus 0 descent sets in Section 2.3.3) may be helpful as background.

5.1 Classical Chabauty and genus 0 descent.

Suppose that $\mathcal{C} = \mathcal{X} \smallsetminus \Gamma$ is a sound, genus 0 clearance hole curve over $\mathcal{O}_{K,S}$. Taking $\mathcal{J}$ to be the generalized Jacobian of $\mathcal{C}$, the classical Chabauty inequality (3.2.6) becomes

$$\operatorname{rank} \mathcal{J}(\mathcal{O}_{K,S}) \leq (\#\Gamma(\overline{K}) - 1) - 1 = \#\Gamma(\overline{K}) - 2\,. \tag{5.1.1}$$

in this case. We use Lemma 2.2.15 to study when (5.1.1) holds (or fails to hold) for $\mathcal{C}$.

As a warm up, note that the classical Chabauty inequality is satisfied for $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$ if and only if $\operatorname{rank} \mathcal{O}_{K,S}^\times < 1$, or equivalently $S = \emptyset$ and either $K = \mathbb{Q}$ or K is an imaginary quadratic field.

More generally, we note the following:

Proposition 5.1.2. *Let K be a number field with absolute Galois group $G = \operatorname{Gal}(\overline{K}/K)$. Suppose that $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma$ for some horizontal divisor Γ is a sound clearance hole curve. The classical Chabauty-Coleman inequality (5.1.1) for $\mathcal{C}$ fails if any of the following conditions hold:*

1. *$r_2(K) \geq 1$ and $r_1(K) + r_2(K) + \#S \geq 2$,*
2. *$r_1(K) \geq 3$ and $r_1(K) + \#S \geq 4$,*
3. *$r_1(K) = 2$ and $r_1(K) + \#S \geq 4$ and $\#(G\backslash\Gamma(\overline{K})) \geq 2$,*
4. *$r_1(K) = 3$ and $\Gamma(\overline{K})$ cannot be written as a disjoint union of G-orbits $\{P_i, P_i'\}$ which remain $G_\mathfrak{p}$ orbits for each real place $\mathfrak{p}$. (E.g. The condition on $\Gamma(\overline{K})$ is automatic if $\#\Gamma(\overline{K})$ is odd.)*

Of course, the classical Chabauty inequality (5.1.1) may also fail under many other conditions, especially when S is large. We sketch the proof.

Proof. We use Lemma 2.2.15 to express $\operatorname{rank} \mathcal{J}_\mathcal{C}(\mathcal{O}_{K,S})$ in terms of the action of $\operatorname{Gal}(\overline{K}/K)$ on $\Gamma(\overline{K})$.

The statement follows quickly from three observations:

1. If $\mathfrak{p} \in \Sigma_\infty$ is a complex place $G_\mathfrak{p} = \{1\}$, so $\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1 = \#\Gamma(\overline{K}) - 1$.

2. If $\mathfrak{p} \in \Sigma_\infty$ is a real place $G_\mathfrak{p} = \mathbb{Z}/2\mathbb{Z}$, so $\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1 \geq \left\lceil \frac{\#\Gamma(\overline{K})}{2} \right\rceil - 1$, with equality if and only if $\Gamma(\overline{K})$ decomposes into complex conjugate pairs over $K_\mathfrak{p}$.

3. $[\#(G\backslash\Gamma(\overline{K})) - 1] \leq \min_{\mathfrak{p}\in S\cup\Sigma_\infty}[\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1]$.

For example, if $r_2(K) \geq 1$ and $r_1(K) + r_2(K) + \#S \geq 2$, let ∞_1 be an infinite place and let $\mathfrak{p} \neq \infty_1$ be another place with $\#(G_\mathfrak{p}\backslash\Gamma(\overline{K}))$ minimal. By Lemma 2.2.15,

$$\begin{aligned}\operatorname{rank} \mathcal{J}_\mathcal{C}(\mathcal{O}_{K,S}) &\geq [\#(G_{\infty_1}\backslash\Gamma(\overline{K})) - 1] + [\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1] - [\#(G\backslash\Gamma(\overline{K})) - 1] \\ &\geq [\#(G_{\infty_1}\backslash\Gamma(\overline{K})) - 1] + [\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1] - [\#(G_\mathfrak{p}\backslash\Gamma(\overline{K})) - 1] \\ &= \#\Gamma(\overline{K}) - 1\,.\end{aligned}$$

The other cases are similar, hinging on the fact that the $-[\#(G\backslash\Gamma(\overline{K})) - 1]$ term in Lemma 2.2.15 can cancel *at most* the minimal positive term. □

Corollary 5.1.3. *Suppose that we are* not *in the following situations: (i) $K = \mathbb{Q}$, (ii) K a real quadratic field and $\#S \leq 1$, (iii) K an imaginary quadratic or totally real cubic field and $\#S = 0$.*

Then the classical Chabauty inequality (3.2.6) *is not satisfied by any descent set consisting of genus zero covers of $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$. Under Leopoldt's Conjecture, this implies that the combination of classical Chabauty and descent by genus zero covers is insufficient to prove that*

$$(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$$

is finite.

Remark 5.1.4. If $K = \mathbb{Q}$ the results of the next section show that $(\mathbb{Z}/q\mathbb{Z})$-descent and classical Chabauty suffice to prove finiteness of $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathbb{Z}_{S'})$ for any set S' of primes. Of course, when K is imaginary quadratic, classical Chabauty without descent trivially suffices to prove that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ is finite.

In the remaining cases, where K is a totally real quadratic or cubic field, one can check that $(\mathbb{Z}/q\mathbb{Z})$-descent and classical Chabauty *is not* sufficient to prove the desired finiteness result. It may be possible to prove a similar finiteness result in these cases using an *iterated* cyclic descent, or a descent-like procedure using covers which are not torsors over the base curve, but this would require a more careful analysis.

5.2 RoS Chabauty and genus 0 descent.

For the genus 0 sound clearance hole curve $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma$, the condition for RoS Chabauty to apply becomes

$$\operatorname{rank} \mathcal{J}_{\mathcal{C}}(\mathcal{O}_{K,S}) \leq d\left(\#\Gamma(\overline{K}) - 2\right) . \tag{5.2.1}$$

The main results of this section are the following two theorems.

Theorem 5.2.2. *The punctured curve $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$ has a descent set $\mathscr{D}$ consisting of genus 0 sound clearance hole curves $\mathcal{D} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma_{\mathcal{D}}$ (see Definition 2.1.1) such that*

I. the RoS Chabauty inequality

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{K,S}) \leq d(\#\Gamma_{\mathcal{D}}(\overline{K}) - 2). \tag{5.2.3}$$

holds for all $\mathcal{D} \in \mathscr{D}$.

II. Under the further assumption that K does not contain a CM field, $\mathscr{D}$ can be chosen so that there is no base change obstruction to RoS Chabauty for $(\mathcal{D}, \mathcal{O}_{K,S})$ for any $\mathcal{D} \in \mathscr{D}$.

Theorem 5.2.4. *Let K be a number field which does not contain a CM subfield and let q be a prime. Fix an $\alpha \in K$ which is not a qth power in K and let*

$$\mathcal{C} := \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{x \in K : x^q - \alpha = 0\} .$$

For q sufficiently large (depending only on K and S), there is no full Prym obstruction to RoS Chabauty for $\mathcal{C}$. Moreover, if $\mathcal{C}$ is the base change of some curve $\mathcal{D}$, there is no full Prym obstruction to RoS Chabauty for $\mathcal{D}$.

Also, there is no base change obstruction to RoS Chabauty for $\mathcal{C}$.

Remark 5.2.5. We saw in Section 5.1 that descent by genus 0 covers and classical Chabauty are very unlikely to prove finiteness of $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$, except in a few special cases with K of low degree.

In Remark 6.1.1, we will see that RoS Chabauty alone cannot prove finiteness of $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ unless every subfield $k \subseteq K$ has at most two real places.

In contrast, Theorems 5.2.2 and 5.2.4 suggest that descent and RoS Chabauty together are likely to be sufficient to prove that $(\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0,1,\infty\})(\mathcal{O}_{K,S})$ is finite, so long as K does not contain a CM subfield. Of course, there are many other ways to prove that this set is finite; the real value of Theorems 5.2.2 and 5.2.4 is not to prove this finiteness, but to provide evidence that Chabauty's method could be used to prove finiteness of integral points on a curve over a wide range of number fields.

Before we begin the proof, we note that if $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma_1$ and $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma_2$ are isomorphic, then there is some fractional linear transformation $\phi : x \mapsto \frac{ax+b}{cx+d}$ with $a, b, c, d \in K$ such that $\phi(\Gamma_1(\overline{K})) = \Gamma_2(\overline{K})$. To determine when RoS Chabauty applies, we will need to understand the number of real and complex embeddings of the fields generated by the Galois orbits in Γ_1 and Γ_2, as well as the splitting of the primes in S in these fields.

The following lemmas will be helpful in the proof of Theorem 5.2.2 and Theorem 5.2.4.

Lemma 5.2.6. *Let q be a prime. Suppose that K is a number field with $[K(\zeta_q) : K] = q - 1$. Let $a, b, c, d \in K$ be such that $ad - bc \neq 0$. Define a map $\phi : K \to K$ by $\phi(x) = \frac{ax+b}{cx+d}$. Suppose that $k \subset K$ is a subfield such that $[k(\phi(\zeta_q)) : k] = q - 1$. Let $r_1(k)$ be the number of real embeddings of k.*

a) If $[K : \mathbb{Q}]$ is odd, then,

$$r_1(k(\phi(\zeta_q))) \leq 2r_1(k)\,.$$

b) If K does not contain a CM subfield, then

$$r_1(k(\phi(\zeta_q))) \leq [k:\mathbb{Q}](q-1) - (q-3)\,.$$

For the proof, it will be convenient to have the following lemma.

Lemma 5.2.7. *Suppose that K is a number field and that γ is algebraic over K. Let $a, b, c, d \in K$ be such that $ad - bc \neq 0$. Define a map $\phi : K \to K$ by $\phi(x) = \frac{ax+b}{cx+d}$. Suppose that $k \subset K$ is a subfield such that $[k(\phi(\gamma)) : k] = [K(\gamma) : K]$.*

a) Fix an embedding $\iota : K \to \mathbb{C}$ and some $r \in \mathbb{R}_{>0}$. Suppose that for all embeddings $\iota' : K(a) \hookrightarrow \mathbb{C}$ extending ι, the image $\iota'(\gamma)$ lies on the circle $U_r := \{x \in \mathbb{C} : |x| = r\}$. If $\iota(K) \cap U_r$ is finite, then there are at most 2 real embeddings $k(\phi_\iota(\gamma)) \hookrightarrow \mathbb{R}$ extending $\iota|_k$.

b) For each $\iota : K \to \mathbb{C}$ fix some $r_\iota \in \mathbb{R}_{>0}$. Suppose that for all embeddings $\iota' : K(a) \hookrightarrow \mathbb{C}$ extending ι, the image $\iota'(\gamma)$ lies on the circle $U_{r_\iota} := \{x \in \mathbb{C} : |x| = r_\iota\}$. If $K_{bad} := \{x \in K : \iota(x) \in U_{r_\iota} \text{ for all } \iota\}$ is finite, then there exists some some ι such that there are at most 2 real embeddings $k(\phi_\iota(\gamma)) \hookrightarrow \mathbb{R}$ extending $\iota|_k$.

Proof of Lemma 5.2.7. Let $\phi_\iota : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ be the fractional linear transformation induced by ϕ and ι.

(a) Suppose for the sake of contradiction that three of the conjugates of $\phi_\iota(\gamma)$ (extending $\iota(K)$) lie in $\mathbb{R}$. Since fractional linear transformations take circles/lines to circles/lines, $\phi_\iota(U_r) = \mathbb{P}^1(\mathbb{R})$. For any $x \in \mathbb{Q}$, we have $\phi_\iota^{-1}(x) \in U_r \cap \iota(K)$. But ϕ_ι^{-1} is injective and $U_r \cap \iota(K)$ is finite, so this is clearly impossible.

So, $\phi_\iota(\gamma)$ is real in at most 2 of the embeddings $K(\phi_\iota(\gamma)) \hookrightarrow \mathbb{C}$ extending ι. Since $[k(\phi(\gamma)) : k] = [K(\gamma) : K]$, there are at most 2 real embeddings of $k(\phi_\iota(\gamma)) \hookrightarrow \mathbb{C}$ extending $k|_\iota$.

(b) Suppose for the sake of contradiction that three of the conjugates of $\phi_\iota(\gamma)$ (extending $\iota(K)$) lie in $\mathbb{R}$ *in every embedding* $\iota : K \hookrightarrow \mathbb{C}$. Then, for any $x \in \mathbb{Q}$,

we have $\phi^{-1}(x) \in K_{\text{bad}}$. But ϕ^{-1} is injective and K_{bad} is finite, so this is clearly impossible.

So, there is some ι such that $\phi_\iota(\gamma)$ is real in at most 2 of the embeddings $K(\phi_\iota(\gamma)) \hookrightarrow \mathbb{C}$ extending ι. Since $[k(\phi(\gamma)) : k] = [K(\gamma) : K]$, there are at most 2 real embeddings of $k(\phi_\iota(\gamma)) \hookrightarrow \mathbb{C}$ extending $k|_\iota$. □

Proof of Lemma 5.2.6. Let $\iota : K \to \mathbb{C}$ be a complex embedding of K. Let $|\cdot|$ be the corresponding complex absolute value. Let $U := \{x \in \mathbb{C} : |x| = 1\}$. Now, ι and ϕ induce a fractional linear transformation $\phi_\iota : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Any such map takes lines and circles to lines and circles.

(a) Suppose $[K : \mathbb{Q}]$ is odd. We claim that

$$U \cap \iota(K) = \{\pm 1\}\,.$$

Suppose for the sake of contradiction that $x \in \iota(K)$ with $|x| = 1$ and $x \neq \pm 1$, then the complex conjugate $\overline{x} = x^{-1} \in \iota(K)$ as well. In particular, the minimal polynomial of x over $\iota(K) \cap \mathbb{R}$ is $z^2 - (x + x^{-1})z + 1$. So, x has degree 2 over $\iota(K) \cap \mathbb{R}$, whence K has even degree. But K has odd degree, which gives the desired contradiction.

Then, Lemma 5.2.7 part (a) applies with $r = 1$ for each embedding ι. So,

$$r_1(k(\phi(\zeta_q))) \leq 2r_1(k)\,,$$

as desired.

(b) Now we consider the case that K does not contain a CM-subfield.

Suppose that $x \in K$ ($x \neq \pm 1$) lies on the unit circle in every complex embedding. Then, $\mathbb{Q}(x)$ is a degree 2, totally complex extension of the totally real field $\mathbb{Q}(x+x^{-1})$. But then $\mathbb{Q}(x)$ is a CM subfield of K, which is a contradiction.

Then, Lemma 5.2.7 part (b) applies with $r_\iota = 1$ for all ι. For some ι, the are at most 2 real places of $k(\phi_\iota(\zeta_q))$ extending $\iota|_k$. For each other place, there are at most

$q-1$ real places extending $\iota|_k$. So,

$$\begin{aligned} r_1(k(\phi(\zeta_q))) &\leq (r_1(k)+r_2(k)-1)(q-1)+2\,, \\ &\leq [K:\mathbb{Q}](q-1)-(q-3)\,, \end{aligned}$$

as desired. □

Lemma 5.2.8. *Suppose that K is a number field and $\alpha \in K$ with $[K(\sqrt[q]{\alpha}):K]=q$. Let $a,b,c,d \in K$ be such that $ad-bc\neq 0$. Define a map $\phi: K\to K$ by $\phi(x)=\frac{ax+b}{cx+d}$. Suppose that $k\subset K$ is a subfield such that $[k(\phi_M(\alpha)):k]=q$. Let $r_1(k)$ be the number of real embeddings of k.*

1. *If $[K:\mathbb{Q}]$ is odd, then,*
$$r_1(k(\phi(\sqrt[q]{\alpha}))) \leq 2r_1(k)\,.$$

2. *If K does not contain a CM subfield, then*
$$r_1(k(\phi(\sqrt[q]{\alpha}))) \leq [k:\mathbb{Q}]q-(q-2)\,.$$

Proof of Lemma 5.2.8. The proof of Lemma 5.2.8, is very similar to the proof of Lemma 5.2.6.

(a) Suppose $[K:\mathbb{Q}]$ is odd and fix $\iota: K\hookrightarrow\mathbb{C}$. Set $r_\iota=\sqrt[q]{|\iota(\alpha)|}$. For any embedding extending ι, we have $|\sqrt[q]{\alpha}|=r$. If there is some $\beta\in\iota(K)$ such that $|\iota(\beta)|=r$, then $|\iota(\beta^q/\alpha)|=1$. Since α is not a qth power, we have $\beta^q/\alpha\neq\pm1$. So, the existence of such a β implies the existence of an element on the unit circle in that embedding. From part (a) of the proof of Lemma 5.2.6, we see that β^q/α has even degree, which is a contradiction.

Then, part (a) of Lemma 5.2.7 implies that there are at most two real embeddings of $k(\phi(\sqrt[q]{\alpha}))$ extending $\iota|_k$. Since ι was arbitrary, we have

$$r_1(k(\phi(\sqrt[q]{\alpha}))) \leq 2r_1(k)\,.$$

(b) If there were some β such that $|\iota(\beta)| = \sqrt[q]{|\iota(\alpha)|}$ for all ι, then $\iota(\beta^q/\alpha)$ would lie on the unit circle in all embeddings $\iota : K \hookrightarrow \mathbb{C}$. As in the proof of part (b) of the proof of Lemma 5.2.6, this would imply that K contains a CM field, so it cannot be the case.

Apply part (b) of Lemma 5.2.7 with $r_\iota = \sqrt[q]{|\iota(\alpha)|}$. For some ι, the are at most 2 real places of $k(\phi_\iota(\sqrt[q]{\alpha}))$ extending $\iota|_k$. For each other place, there are at most $q-1$ real places extending $\iota|_k$. So,

$$\begin{aligned} k(\phi(\sqrt[q]{\alpha})) &\leq (r_1(k) + r_2(k) - 1)q + 2\,, \\ &\leq [K : \mathbb{Q}]q - (q-2)\,, \end{aligned}$$

as desired. □

Proof of Theorem 5.2.2. We construct an explicit set $\mathscr{D}$ consisting of covers of twists of the qth power map for any sufficiently large prime $q \notin S'$. We determine how large q needs to be later in the proof.

Choose a set U of coset representatives for $\mathcal{O}_{K,S}^\times / \mathcal{O}_{K,S}^{\times q}$ with $1 \in U$.

Let $\mathcal{D}_u$ be the curve $\mathbb{A}^1_{\mathcal{O}_{K,S}} \smallsetminus \{x(x^q - u^{-1}) = 0\}$. If we take Γ_u to be the divisor (defined over K) given by

$$\Gamma_u = \{0, \infty\} \cup \{x \in \overline{K} : ux^q - 1 = 0\}\,,$$

then $\mathcal{D}_u = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \Gamma_u$. The curve $\mathcal{D}_u$ maps to $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$ via

$$\begin{aligned} \mathbb{A}^1_{\mathcal{O}_{K,S}} \smallsetminus \{x(x^q - u^{-1}) = 0\} &\to \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\} \\ x &\mapsto ux^q\,. \end{aligned}$$

Let $\mathscr{D}$ be the set $\{\mathcal{D}_u : u \in U\}$. For each $u \in U$, the image of $\mathcal{D}_u(\mathcal{O}_{K,S})$ is in $u\mathcal{O}_{K,S}^{\times q} \cap (\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{K,S})$. As a result, $\mathscr{D}$ is a descent set for $\mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$.

Let $\mathcal{J}_u$ be the generalized Jacobian of $\mathcal{D}_u$. For each $u \in U$, the generic fiber of $\mathcal{D}_u$ is $\mathbb{P}^1$ with a reduced divisor of degree $q+2$ removed. Hence, $\dim \mathcal{J}_u = q + 1$.

Bounding $\operatorname{rank} \mathcal{J}_u$ will require more work. We break into two cases based on whether or not $u = 1$.

Case 1: $u = 1$

Part I: $(\mathcal{D}_1, \mathcal{O}_{K,S})$ satisfies the RoS Chabauty inequality.

Let G be the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ and let $G_{\mathfrak{p}}$ be the decomposition group at the place $\mathfrak{p}$. We use Lemma 2.2.15 to compute the rank of $\mathcal{J}_1$ in terms of the action of the $G_{\mathfrak{p}}$ on $\Gamma_1(\overline{K})$.

By construction,

$$\#(G\backslash\Gamma_1(\overline{K})) = 4\,.$$

Moreover,

$$\#(G_{\mathfrak{p}}\backslash\Gamma_1(\overline{K})) = \begin{cases} q+2 & \text{if } \mathfrak{p} \text{ is a complex place of } K\,, \\ 3+\frac{q-1}{2} & \text{if } \mathfrak{p} \text{ is a real place of } K\,, \\ 3+\#\{\text{primes } \mathfrak{P} \text{ of } K(\zeta_q) \text{ above } \mathfrak{p}\} & \text{if } \mathfrak{p} \text{ is a finite place of } K\,. \end{cases}$$

While an exact formula for the number of primes of $K(\zeta_q)$ above $\mathfrak{p}$ is complicated, we can bound it as follows when $\mathfrak{p}$ does not lie over q.

Let $\kappa_{\mathfrak{p}}$ be the residue field of $K_{\mathfrak{p}}$. Let $a_{\mathfrak{p}} = [\kappa_{\mathfrak{p}}(\zeta_q) : \kappa_{\mathfrak{p}}]$. Then, $a_{\mathfrak{p}}$ is the order of $\#\kappa_{\mathfrak{p}}$ in $(\mathbb{Z}/q\mathbb{Z})^\times$, so

$$a_{\mathfrak{p}} \geq \left\lceil \frac{\ln(q-1)}{\ln(\#\kappa_{\mathfrak{p}})} \right\rceil .$$

Also,

$$\#\{\text{primes } \mathfrak{P} \text{ of } K[\zeta_p] \text{ above } \mathfrak{p}\} = \frac{q-1}{a_{\mathfrak{p}}} \leq \frac{q-1}{\left\lceil \frac{\ln(q-1)}{\ln(\#\kappa_{\mathfrak{p}})} \right\rceil} .$$

Thus, given any $\varepsilon > 0$, we may choose q sufficiently large (depending on ε, K, and S) so that

$$\sum_{\mathfrak{p}\in S} \#\{\text{primes } \mathfrak{P} \text{ of } K[\zeta_p] \text{ above } \mathfrak{p}\} \leq \varepsilon(q-1)\,. \tag{5.2.9}$$

For such q, Lemma 2.2.15 implies that

$$\begin{aligned}\operatorname{rank} \mathcal{J}_1(\mathcal{O}_{K,S}) &\leq \left(\frac{q+3}{2}\right) r_1(K) + (q+1) r_2(K) + 2\#S + \varepsilon(q-1) - 3 \\ &= \left(\frac{r_1(K) + 2r_2(K)}{2} + \varepsilon\right) q + O(1)\,,\end{aligned}$$

where the $O(1)$ term depends only on K and S. In comparison,

$$[K:\mathbb{Q}](\dim \mathcal{J}_1 - 1) = (r_1(K) + 2r_2(K))q\,.$$

Hence, if q is sufficiently large,

$$\operatorname{rank} \mathcal{J}_1(\mathcal{O}_{K,S}) \leq [K:\mathbb{Q}](\dim \mathcal{J}_1 - 1)\,.$$

In other words, $(\mathcal{D}_1, \mathcal{O}_{K,S})$ satisfies the RoS Chabauty inequality (4.1.5).

Part II: $(\mathcal{D}_1, \mathcal{O}_{K,S})$ has no base change obstruction.
We claim that if K does not contain a CM subfield then for sufficiently large q the pair $(\mathcal{D}_1, \mathcal{O}_{K,S})$ has no base change obstruction to RoS Chabauty.

Let k be a subfield of K. Let S_k be the set of primes lying under primes in S. Let $H = \operatorname{Gal}(\overline{k}/k)$ be the absolute Galois group of k. Given a prime $\mathfrak{l}$ of $\mathcal{O}_k$, let $H_\mathfrak{l}$ be the decomposition group at $\mathfrak{l}$. Note that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ lying over $\mathfrak{l}$, we can identify $G_\mathfrak{p}$ with a subgroup of $H_\mathfrak{l}$.

Suppose that $\mathcal{D}'/\mathcal{O}_{k,S_k}$ is a curve with $\mathcal{D}'_{\mathcal{O}_{K,S}} \cong \mathcal{D}_1$. We know that the generic fiber $\mathcal{D}'_k$ of $\mathcal{D}'$ is a punctured genus 0 curve. A priori, the projective closure of $\mathcal{D}'_k$ could be a twisted form of $\mathbb{P}^1_k$. However, the set of punctures gives a reduced divisor, which has degree $q+2$. Since this degree is odd, the projective closure of $\mathcal{D}'_k$ must be $\mathbb{P}^1_k$.

In particular, there is some k-rational divisor so that $\mathcal{D}'_k \cong \mathbb{P}^1_k \smallsetminus \Gamma_{\mathcal{D}'_k}$. (Note that although there may be room to choose the integral structure of $\mathcal{D}'$, we have that $\operatorname{rank} \mathcal{J}_{\mathcal{D}'}(\mathcal{O}_{k,S_k})$ is independent of the choice.)

Let $\phi(x) = \frac{ax+b}{cx+d}$ define the isomorphism $(\mathcal{D}_1)_K \cong (\mathcal{D}')_K$. Then, $\Gamma_{\mathcal{D}'_k}(\overline{k}) = (\phi(\{0,\infty\} \cup \{x : x^q - 1 = 0\})$.

Since K does not contain a CM subfield, a slight generalization of (the proof of) Lemma 5.2.6 implies that there is some embedding $\iota : k \hookrightarrow \mathbb{C}$ such that $\#(\Gamma_{\mathcal{D}'_k}(\overline{k}) \cap \mathbb{R}) \leq 4$.

For the corresponding place $\mathfrak{l} \in \Sigma_{k,\infty}$, consider the action of $H_\mathfrak{l}$ on $\Gamma_{\mathcal{D}'_k}(\overline{k})$. Let M be the number of $H_\mathfrak{l}$ orbits of size 1 and let N be the number of $H_\mathfrak{l}$ orbits of size 2. We have $M + 2N = q + 2$ and $M \leq 4$, so $M + N \leq (q+6)/2$.

For all other infinite places of k, we use the trivial bound $\#(H_\mathfrak{l} \backslash \Gamma_{\mathcal{D}'}(\overline{k})) \leq \#\Gamma_{\mathcal{D}'}(\overline{k}) = q + 2$. So,

$$\begin{aligned}\sum_{\mathfrak{l} \in \Sigma_{k,\infty}} \#(H_\mathfrak{l} \backslash \Gamma_{\mathcal{D}'}(\overline{k})) &\leq (r_1(k) + r_2(k) - 1)(q+2) + \frac{q+6}{2} \\ &\leq \left([k:\mathbb{Q}] - \frac{1}{2}\right) q + O(1)\,.\end{aligned}$$

Since K has finitely many subfields k, the $O(1)$ term depends only on K.

For any place $\mathfrak{l}$ of k lying under a place $\mathfrak{p}$ of K, we have

$$\#(H_\mathfrak{l} \backslash \Gamma_{\mathcal{D}'}(\overline{k})) \leq \#(G_\mathfrak{p} \backslash \Gamma_{\mathcal{D}'}(\overline{K})) = \#(G_\mathfrak{p} \backslash \Gamma_1(\overline{K}))\,.$$

Applying (5.2.9), and accounting for the 3 additional rational points $\{0, 1, \infty\}$ we have

$$\sum_{\mathfrak{l} \in S_k} \#(H_\mathfrak{l} \backslash \Gamma_{\mathcal{D}'}(\overline{k})) \leq \sum_{\mathfrak{p} \in S} \#(G_\mathfrak{p} \backslash \Gamma_{\mathcal{D}'}(\overline{K})) = \sum_{\mathfrak{p} \in S} \#(G_\mathfrak{p} \backslash \Gamma_1(\overline{K})) \leq \varepsilon(q-1) + 3\#S\,.$$

By Lemma 2.2.15, we have

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}'}(\mathcal{O}_{k,S_k}) \left([k:\mathbb{Q}] - \frac{1}{2} + \varepsilon\right) q + O(1)\,.$$

Choosing $\varepsilon = 1/4$ and q sufficiently large (independent of the choice of $k \subset K$)

we may arrange that

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{k,S_k}) \leq [k:\mathbb{Q}] \cdot q = [k:\mathbb{Q}](\dim \mathcal{J}_{\mathcal{D}} - 1)\,.$$

Case 2: $u \notin \mathcal{O}_{K,S}^{\times q}$

Part I: $(\mathcal{D}_u, \mathcal{O}_{K,S})$ satisfies the RoS Chabauty inequality.

The proof in this case is very similar to the previous case. There is a slight difference in the treatment of the finite places.

$$\#(G_{\mathfrak{p}} \backslash \Gamma_u(\overline{K})) = \begin{cases} q+2 & \text{if } \mathfrak{p} \text{ is a complex place of } K\,, \\ 3 + \frac{q-1}{2} & \text{if } \mathfrak{p} \text{ is a real place of } K\,, \\ 2 + \#\{\text{primes } \mathfrak{P} \text{ of } K[\sqrt[q]{u}] \text{ above } \mathfrak{p}\} & \text{if } \mathfrak{p} \text{ is a finite place of } K\,. \end{cases}$$

With $a_{\mathfrak{p}}$ defined as in the previous case, for a finite place $\mathfrak{p}$ of K not lying over q,

$$\#\{\text{primes } \mathfrak{P} \text{ of } K[\sqrt[q]{u}] \text{ above } \mathfrak{p}\} = \begin{cases} 1, & \text{if } \overline{u} \notin \kappa_{\mathfrak{p}}^{\times q}\,, \\ 1 + (q-1)/a_{\mathfrak{p}}, & \text{otherwise}\ . \end{cases}$$

For ε as in Part 1, Lemma 2.2.15 gives

$$\operatorname{rank} \mathcal{J}_u(\mathcal{O}_{K,S}) \leq \left(\frac{q+3}{2}\right) r_1(K) + (q+1) r_2(K) + 2\#S + \varepsilon(q-1) - 2\,.$$

Again, in comparison,

$$[K:\mathbb{Q}](\dim \mathcal{J}_u - 1) = (r_1(K) + 2r_2(K))q\,.$$

Taking q large enough, we have

$$\operatorname{rank} \mathcal{J}_u(\mathcal{O}_{K,S}) \leq [K:\mathbb{Q}](\dim \mathcal{J}_u - 1)\,,$$

so that $(\mathcal{D}_u, \mathcal{O}_{K,S})$ satisfies the RoS Chabauty inequality (4.1.5).

Part II: $(\mathcal{D}_u, \mathcal{O}_{K,S})$ has no base change obstruction.

The proof that $\mathcal{D}_u$ has no base change obstruction so long as K does not contain a CM subfield is essentially identical to the proof for $\mathcal{D}_1$, except that it a mild generalization of Lemma 5.2.8 in place of the mild generalization of Lemma 5.2.6. Again, for any $\mathcal{D}'/\mathcal{O}_{k,S_k}$ with $\mathcal{D}'_{\mathcal{O}_{K,S}} \cong \mathcal{D}_u$, we find by Lemma 2.2.15 that

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}'}(\mathcal{O}_{k,S_k}) \left([k : \mathbb{Q}] - \frac{1}{2} + \varepsilon \right) q + O(1) \,. \tag{5.2.10}$$

Choosing $\varepsilon = 1/4$ and q sufficiently large we may arrange that

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{k,S_k}) \leq [k : \mathbb{Q}] \cdot q = [k : \mathbb{Q}](\dim \mathcal{J}_{\mathcal{D}} - 1) \,.$$

□

Remark 5.2.11. Retain the notation of Theorem 5.2.2 and its proof. In contrast to the situation where K does not contain a CM field, if K is a CM field, we will show that there *is* a base change obstruction to RoS Chabauty for $(\mathcal{D}_1, \mathcal{O}_{K,S})$ for any large q, at least when $\#S \geq 3$.

Suppose K is CM, with maximal totally real subfield k. Let $\alpha \in \mathcal{O}_K$ be such that $K = k(\alpha)$. Let $\overline{\alpha}$ be the Galois conjugate of α under the $\mathrm{Gal}(K/k)$ action. Then, $\overline{\alpha}$ is the complex conjugate of α for every embedding $K \hookrightarrow \mathbb{C}$. Define the fractional linear transformation:

$$\begin{aligned} f : \mathbb{P}^1 &\to \mathbb{P}^1 \,, \\ x &\mapsto \frac{\alpha x - \overline{\alpha}}{x - 1} \,. \end{aligned}$$

If $a \in \mathbb{C} \smallsetminus \mathbb{R}$, then

$$x \mapsto \frac{ax - \overline{a}}{x - 1}$$

maps $\{z \in \mathbb{C} : |z| = 1\}$ to $\mathbb{R} \cup \{\infty\}$. Applying this to $a = \alpha$ and $x = \zeta_q$ (under any embedding $K(\zeta_q) \hookrightarrow \mathbb{C}$) shows that $f(\zeta_q)$ is totally real. Thus, the minimal polynomial of $f(\zeta_q)$ over K has coefficients in k.

Also, $f(1) = \infty$ and $f(\{0, \infty\}) = \{\alpha, \overline{\alpha}\}$, so $\Gamma_{\mathcal{D}} := f(\{x : x^q - 1 = 0\} \cup \{0, \infty\})$ is defined over k.

Moreover, for each infinite place $\mathfrak{l}$ of k, we have

$$\#(H_{\mathfrak{l}} \backslash \Gamma_{\mathcal{D}}(\overline{k})) = q + 1\,.$$

The set $(H \backslash \Gamma_{\mathcal{D}}(\overline{k}))$ consists of the orbits $\{\infty\}, \{\alpha, \overline{\alpha}\}$, and at least one other orbit, so $\#(H \backslash \Gamma_{\mathcal{D}}(\overline{k})) \geq 3$. Thus, for any finite place $\mathfrak{l}$ of k,

$$\#(H_{\mathfrak{l}} \backslash \Gamma_{\mathcal{D}}(\overline{k})) \geq \#(H \backslash \Gamma_{\mathcal{D}}(\overline{k})) \geq 3\,.$$

Set $\mathcal{D} = \mathbb{P}^1_{\mathcal{O}_{k,S_k}} \smallsetminus \Gamma_{\mathcal{D}}$ and let $\mathcal{J}_{\mathcal{D}}$ be its Jacobian. When $S_k \neq \emptyset$, we can absorb the $\#(H \backslash \Gamma_{\mathcal{D}}(\overline{k})) - 1$ term of Lemma 2.2.15 into one of the finite places to get implies that

$$\begin{aligned} \operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{k,S_k}) &\geq [k : \mathbb{Q}]q + 2\#S_k - 2 \\ &> [k : \mathbb{Q}](\dim \mathcal{J}_{\mathcal{D}} - 1) + 2\#S_k - 3\,. \end{aligned}$$

In particular, if $\#S_K \geq 3$, then $\#S_k \geq 2$ so $(\mathcal{D}, \mathcal{O}_{k,S_k})$ is a base change obstruction to RoS Chabauty for $(\mathcal{D}_1, \mathcal{O}_{K,S})$.

Of course, if K is not CM, but contains a CM field, we may apply the same argument to the CM subfield to construct a base change obstruction.

Before proving Theorem 5.2.4, we state and prove one more technical lemma, which says roughly that full Prym obstructions to RoS Chabauty for a genus 0 sound clearance hole curve $\mathcal{C}$ over $\mathcal{O}_{K,S}$ only occur when the map 'forgets' a puncture or when the rank of the Jacobian is close to (more precisely, within approximately $\operatorname{rank} \mathcal{O}_{K,S}^{\times}$ of) the bound from the RoS Chabauty inequality.

Lemma 5.2.12. *Let $\mathcal{C}_1 := \mathbb{P}^1 \smallsetminus \Gamma_1$ and let $\mathcal{C}_2 := \mathbb{P}^1 \smallsetminus \Gamma_2$ be sound clearance hole curves over $\mathcal{O}_{K,S}$. Let $\mathcal{J}_1$ be the generalized Jacobian of $\mathcal{C}_1$ and suppose that*

$$\operatorname{rank} \mathcal{J}_1(\mathcal{O}_{K,S}) + \operatorname{rank} \mathbb{G}_m(\mathcal{O}_{K,S}) + 1 < [K : \mathbb{Q}] \cdot \#\Gamma_1(\overline{K})\,.$$

a) Suppose that $\Gamma_2(K)$ consists of a single Galois orbit and that we are given a morphism $\varphi : \mathcal{C}_1 \to \mathcal{C}_2$ such that the induced morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ maps $\Gamma_1(\overline{K})$ to $\Gamma_2(\overline{K})$ surjectively. Then, φ is not a full Prym obstruction to RoS Chabauty for $\mathcal{C}_1$.

b) Suppose that Γ_1 consists of a single Galois orbit. Then, there is no full Prym obstruction to RoS Chabauty for $\mathcal{C}_1$.

Proof. (a) Let $n = \#(G\backslash\Gamma_1(\overline{K}))$. Let $\delta = \#\Gamma_1(\overline{K})/\#\Gamma_2(\overline{K})$. Let $\mathcal{J}_2$ be the generalized Jacobian of $\mathcal{C}_2$. Then, adding $\operatorname{rank}\mathbb{G}_m(\mathcal{O}_{K,S}) = -1 + \sum_{\mathfrak{p}\in S\cup\Sigma_\infty} 1$ to the formula from Lemma 2.2.15 gives

$$\operatorname{rank}\mathcal{J}_1(\mathcal{O}_{K,S}) + \operatorname{rank}\mathbb{G}_m(\mathcal{O}_{K,S}) + n = \sum_{\mathfrak{p}\in S\cup\Sigma_\infty} \#(G_\mathfrak{p}\backslash\Gamma_1(\overline{K}))\,. \tag{5.2.13}$$

Similarly,

$$\operatorname{rank}\mathcal{J}_2(\mathcal{O}_{K,S}) + \operatorname{rank}\mathbb{G}_m(\mathcal{O}_{K,S}) + 1 = \sum_{\mathfrak{p}\in S\cup\Sigma_\infty} \#(G_\mathfrak{p}\backslash\Gamma_2(\overline{K}))\,.$$

Now, for each $\mathfrak{p} \in S \cup \Sigma_\infty$, we have $\#(G_\mathfrak{p}\backslash\Gamma_1(\overline{K})) \le \delta\#(G_\mathfrak{p}\backslash\Gamma_2(\overline{K}))$, so

$$\operatorname{rank}\mathcal{J}_1(\mathcal{O}_{K,S}) - \operatorname{rank}\mathcal{J}_2(\mathcal{O}_{K,S}) \le \frac{\delta-1}{\delta}\left(\operatorname{rank}\mathcal{J}_1(\mathcal{O}_{K,S}) + \operatorname{rank}\mathbb{G}_m(\mathcal{O}_{K,S}) + 1\right)\,.$$

On the other hand,

$$\dim\mathcal{J}_1 - \dim\mathcal{J}_2 = (\#\Gamma_1(\overline{K}) - 1) - (\#\Gamma_2(\overline{K}) - 1) = \frac{\delta-1}{\delta}\#\Gamma_1(\overline{K})\,.$$

Combining (5.2.13) with the previous two sentences shows that

$$\operatorname{rank}\mathcal{J}_1(\mathcal{O}_{K,S}) - \operatorname{rank}\mathcal{J}_2(\mathcal{O}_{K,S}) < \dim\mathcal{J}_1 - \dim\mathcal{J}_2\,.$$

Thus, $\mathcal{C}_1 \to \mathcal{C}_2$ is not a large Prym obstruction.

Part (b) follows immediately from part (a), since if Γ_1 consists of a single Galois orbit, $\phi(\Gamma_1)$ must also consist of a single Galois orbit. □

Theorem 5.2.4 is essentially a corollary of Lemma 5.2.12 and the rank bounds from the proof of Theorem 5.2.2.

Proof of Theorem 5.2.4. Suppose that k is a subfield of K and $\mathcal{D}$ is a sound clearance hole curve over $\mathcal{O}_{k,S_k}$ such that $\mathcal{D}_{\mathcal{O}_{K,S}} \cong \mathcal{C}$. Since $\mathcal{D}$ differs from the curves considered in (5.2.10) only by a finite set of punctures, the ranks will be the same up to an $O(1)$ term (depending on K and S, but not on q.) We get

$$\operatorname{rank} \mathcal{J}_{\mathcal{D}}(\mathcal{O}_{k,S_k}) + \operatorname{rank} \mathbb{G}_m(\mathcal{O}_{k,S_k}) + 1 \leq \left([k : \mathbb{Q}] - \frac{1}{2} + \varepsilon \right) \cdot q + O(1)\,.$$

Taking $\varepsilon = 1/4$ and q sufficiently large, this is strictly less that $[k : \mathbb{Q}] \cdot q = [k : \mathbb{Q}] \cdot \#\Gamma_{\mathcal{D}}(\overline{K})$. Applying Lemma 5.2.12 completes the proof. □

Chapter 6

RoS Chabauty and $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$: Computations

In this chapter, we study the application of restriction of scalars and Chabauty's method to compute solutions to the unit equation (without using descent). Most of the section is an extended series of examples of RoS Chabauty for $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$. The final subsection uses a slight variant of this setup to prove that if 3 splits completely in K and $3 \nmid [K : \mathbb{Q}]$ then $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K) = \emptyset$.

6.1 RoS Chabauty and $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$: Generalities

We make explicit the theory of RoS Chabauty from Sections 4.1 and 4.4 in the context of $\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$. Our notation is as in Section 4.4. From here on, we drop subscripts signifying the base ring to ease notation if we think it is unlikely to cause confusion.

Remark 6.1.1. If $\mathcal{C} = \mathbb{P}^1_{\mathcal{O}_{K,S}} \smallsetminus \{0, 1, \infty\}$ then $\mathcal{J}_\mathcal{C} \cong \mathbb{G}_{m,\mathcal{O}_{K,S}} \times \mathbb{G}_{m,\mathcal{O}_{K,S}}$. Let r_1 and r_2 be the number of real and complex embeddings of K, so $d = r_1 + 2r_2$. We have $\dim \mathcal{J}_\mathcal{C} = 2$ and

$$\operatorname{rank} \mathcal{J}(\mathcal{O}_{K,S}) = 2 \operatorname{rank} \mathcal{O}_{K,S}^\times = 2(r_1 + r_2 + \#S - 1)\,.$$

In this case, the RoS Chabauty inequality (4.1.5) becomes:

$$2(r_1 + r_2 + \#S - 1) \leq (r_1 + 2r_2)(2 - 1)\,,$$

or equivalently

$$r_1 + 2\#S \leq 2\,.$$

Hence, $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}, \mathcal{O}_{K,S})$ satisfies the RoS Chabauty inequality if and only if one of the following holds:

- $r_1 = 0$ and $\#S \leq 1$,
- $r_1 = 1$ and $\#S = 0$,
- $r_1 = 2$ and $\#S = 0$.

If $\#S > 0$, then $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}, \mathbb{Z}_{S'})$ violates the RoS Chabauty inequality and therefore is a base change obstruction to RoS Chabauty for $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\}, \mathcal{O}_{K,S})$. As a result, we do not lose much generality if we restrict to the case $S = \emptyset$. We will do so for the rest of this section to ease notation.

Throughout, we fix the Abel-Jacobi map:

$$\begin{aligned} j : \mathbb{P}^1 \smallsetminus \{0, 1, \infty\} &\hookrightarrow \mathbb{G}_m \times \mathbb{G}_m \\ x &\mapsto (x, x - 1)\,. \end{aligned}$$

The outside of the diagram (4.4.1) becomes

$$\begin{array}{ccc} (\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K) & \longhookrightarrow & (\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_{L_\mathfrak{P}})^d \\ \downarrow & & \downarrow \\ \mathbb{G}_m(\mathcal{O}_K) \times \mathbb{G}_m(\mathcal{O}_K) & \longhookrightarrow & \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d\,. \end{array} \tag{6.1.2}$$

Let $\sigma_1, \ldots, \sigma_d : K \to L_\mathfrak{P}$ be the embeddings of K into $L_\mathfrak{P}$. The bottom horizontal map in (6.1.2) is given by

$$(x, y) \mapsto ((\sigma_1(x), \ldots, \sigma_d(x)), (\sigma_1(y), \ldots, \sigma_d(y)))\,,$$

while the rightmost vertical map in (6.1.2) is given by

$$(u_1, \dots, u_d) \mapsto ((u_1, \dots, u_d), (u_1 - 1, \dots, u_d - 1)) .$$

Let $x_1, \dots, x_d, y_1, \dots, y_d$ be the local coordinates on $\mathbb{G}_m^d \times \mathbb{G}_m^d$. We have

$$H^0(\mathbb{G}_m^d \times \mathbb{G}_m^d, \Omega^1)_{\text{inv}} = \text{Span}\left\{ \frac{dx_1}{x_1}, \dots, \frac{dx_d}{x_d}, \frac{dy_1}{y_1}, \dots, \frac{dy_d}{y_d} \right\} .$$

In these coordinates, the p-adic integration theory has a particularly simple interpretation: For $i \in \{0, 1\}$ set

$$Q_i = ((x_1^{(i)}, \dots, x_d^{(i)}), (y_1^{(i)}, \dots, y_d^{(i)})) .$$

Let log denote the p-adic logarithm. Then,

$$\int_{Q_0}^{Q_1} \sum_{j=1}^{d} \left(a_j \frac{dx_j}{x_j} + b_j \frac{dy_j}{y_j} \right) = \sum_{j=1}^{d} \left(a_j \log \frac{x_j^{(1)}}{x_j^{(0)}} + b_j \log \frac{y_j^{(1)}}{y_j^{(0)}} \right) .$$

Since we will only ever evaluate at points where the $x_j^{(i)}$ and $y_j^{(i)}$ are units, we do not need to specify the value of $\log p$.

Now, we must gather information about the space of a_j and b_j such that for any

$$Q = ((x_1', \dots, x_d'), (y_1', \dots, y_d')) \in \mathbb{G}_m(\mathcal{O}_K) \times \mathbb{G}_m(\mathcal{O}_K) \subset \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d ,$$

we have

$$\int_{(1,1)}^{Q} \sum_{j=1}^{d} \left(a_j \frac{dx_j}{x_j} + b_j \frac{dy_j}{y_j} \right) = \sum_{j=1}^{d} \left(a_j \log x_j' + b_j \log y_j' = 0 \right) .$$

Let $\mathscr{A} \subset L_\mathfrak{P}^d$ be the subspace of $(a_1, \dots, a_d)$ such that

$$\sum_{j=1}^{d} a_j \log \sigma_j(x) = 0$$

for all $x \in \mathbb{G}_m(\mathcal{O}_K)$. Let $r = \operatorname{rank} \mathbb{G}_m(\mathcal{O}_K)$. Then $\dim \mathscr{A} \geq d - r$ with equality if

Leopoldt's conjecture holds.

For any $x \in \mathcal{O}_K$, we have $\prod_{j=1}^{d} \sigma(x) \in \mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$. In particular,

$$\sum_{j=1}^{d} \log \sigma_j(x) = 0\,,$$

so $(1, \ldots, 1) \in \mathscr{A}$ regardless of K.

Let $Z \subseteq \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d$ be the common vanishing locus of the (at least) $2(d-r)$-dimensional vector space of functions:

$$\mathcal{F} := \left\{ \sum_{j=1}^{d} a_j \log x_j : (a_1, \ldots, a_d) \in \mathscr{A} \right\} \oplus \left\{ \sum_{j=1}^{d} a_j \log y_j : (a_1, \ldots, a_d) \in \mathscr{A} \right\}. \tag{6.1.3}$$

By construction, we have $\mathbb{G}_m(\mathcal{O}_K) \times \mathbb{G}_m(\mathcal{O}_K) \subseteq Z$.

Roughly speaking, our strategy for proving finiteness of $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ is to prove finiteness of the intersection

$$Z \cap (\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})^d(\mathcal{O}_{L_\mathfrak{P}}) \subset \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d\,,$$

which contains the image of $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$.

Since the image of $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})^d(\mathcal{O}_{L_\mathfrak{P}})$ is cut out by the equations

$$\mathcal{G} := \{x_j - y_j = 1 : j \in [1, \ldots, d]\}\,, \tag{6.1.4}$$

this intersection is the common vanishing locus of at least $2d - 2r + d$ functions on the $2d$-dimensional $\mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d$. On sufficiently small closed compact neighborhoods U all of these functions can be written simultaneously as multivariate p-adic power series with $L_\mathfrak{P}$-coefficients which converge on an open neighborhood of U. In other words, the p-adic power series are *overconvergent* on U. When $2r+d \leq 2d$, we may hope that this intersection, the common vanishing locus of the functions in $\mathcal{F}$ and $\mathcal{G}$, consists of a finite set of isolated points.

In subsection 6.2.4, we need a slight variant of this high-level strategy. To explain our approach, we first recall a few facts from the theory of rigid analytic geometry as they apply to our setup.

Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$. Given any U as above, we may assume that there exist $a_1, \ldots, a_{2d} \in \mathbb{R}$ such that U is (isomorphic to)

$$\{ (t_1, \ldots, t_{2d}) \in L_{\mathfrak{P}}^{2d} : |t_i| \leq a_i \text{ for all } i \in \{1, \ldots, 2d\} \}.$$

Choosing linearly independent functions $F_1, \ldots, F_{2d-2r} \in \mathcal{F}$ and $G_1, \ldots, G_d \in \mathcal{G}$ and expressing them as overconvergent power series in the local coordinates for U, we may assume that they converge for all $t_i \in \mathbb{C}_p$ with $|t_i| < a_i + \epsilon$ on U.

Let $\|(u_1, \ldots, u_{2d})\| = \sum_{i=1}^{2d} u_i$ for $u \in \mathbb{Z}_{\geq 0}^{2d}$. After rescaling the local coordinates so that all of the a_i are 0, the set of common zeros $\mathbb{C}_p$-valued zeros of these power series in $\mathcal{O}_{\mathbb{C}_p}$ is the MaxSpec of the affinoid algebra

$$A := \left\{ \sum_u b_u t^u \in \mathbb{C}_p[[t_1, \ldots, t_{2d}]] \colon |b_u| \to \infty \text{ as } \|u\| \to \infty \right\} / \langle F_1, \ldots, F_{2d-2r}, G_1, \ldots, G_d \rangle ,$$

This gives the common vanishing set of our power series (on each disc) the structure of an (affinoid) rigid analytic space. The ring A is noetherian and irreducible components of MaxSpec(A) correspond to the finitely many minimal prime ideals of A. (See for instance [Con99], where this theory is developed in significantly greater generality.)

Since any isolated common zeros of $F_1, \ldots, F_{2d-2r}, G_1, \ldots, G_d$ are irreducible components of MaxSpec(A), this implies that our power series have finitely many common zeros which are isolated among their $\mathcal{O}_{\mathbb{C}_p}$-valued common zeros.

In the next section, we will use tangent space computations to prove in several particular cases that if $P \in U$ is in the image of $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$, then P is isolated among $\mathcal{O}_{\mathbb{C}_p}$-valued common zeros of the F_i and G_i. It then follows immediately from the discussion above that $(\mathbb{P}^1 \smallsetminus \{0, 1, \infty\})(\mathcal{O}_K)$ is finite.

6.2 Finiteness of the Chabauty set: Examples

In the upcoming subsections, K will be a quadratic field, mixed cubic field, or a complex quartic field. In the final subsection, K will be a mixed quartic field with a totally real quadratic subfield. We always take p to be a prime which is unramified in K and let $L_{\mathfrak{P}}$ be a finite extension of $\mathbb{Q}_p$ which is a splitting field for K.

Following the strategy and notation of section 6.1, we will show that with finitely many exceptions, for $P \in (\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K)$ the intersection of the tangent spaces of the $F_1, \ldots, F_{2d-2r}, G_1, \ldots, G_d$ at $j(P)$ is zero-dimensional. Hence, $j(P)$ is isolated among $\mathcal{O}_{\mathbb{C}_p}$-valued common zeros of the F_i and G_i. By the discussion at the end of section 6.1, this implies that $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K)$ is finite.

6.2.1 Real quadratic fields

Proposition 6.2.1. *Let K be a real quadratic field. Let*

$$\begin{aligned} j : \mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0,1,\infty\} &\hookrightarrow \mathbb{G}_{m,\mathcal{O}_K} \times \mathbb{G}_{m,\mathcal{O}_K} \\ x &\mapsto (x, x-1)\,. \end{aligned}$$

Also use j to refer to the corresponding map on the restriction of scalars to $\mathbb{Z}$. Then, inside $(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z}_p)$, the intersection

$$j((\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}\,\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathbb{Z}_p)) \cap \overline{(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z})}$$

consists of finitely many isolated points. It follows that $\#(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) < \infty$.

Proof. Suppose that K is a real quadratic field. In this case, $\operatorname{rank} \mathcal{O}_K^\times = 1$ and $[K:\mathbb{Q}] = 2$, so $\mathscr{A}$ is 1-dimensional. Thus, $\mathscr{A}$ is spanned by $(1,1)$.

We may take F_1, F_2, G_1, G_2 to be the equations

$$\begin{aligned} F_1 &: \log x_1 + \log x_2 = 0\,, \\ F_2 &: \log y_1 + \log y_2 = 0\,, \\ G_1 &: x_1 - y_1 - 1 = 0\,, \\ G_2 &: x_2 - y_2 - 1 = 0\,. \end{aligned}$$

After accounting for finitely many exceptions, we show that if $x \in \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})$ solves these equations then the intersection of the tangent spaces of the zero sets of F_1, F_2, G_1, and G_2 at x is zero-dimensional. Equivalently, we will show that the matrix of derivatives at $x = (x_1, x_2, y_1, y_2)$

$$M_x := \begin{pmatrix} \frac{1}{x_1} & \frac{1}{x_2} & 0 & 0 \\ 0 & 0 & \frac{1}{y_1} & \frac{1}{y_2} \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

has rank 4. After some elementary column/row operations and substituting $y_j = x_j - 1$, the condition $\operatorname{rank} M_x = 4$ is equivalent to

$$\operatorname{rank} \begin{pmatrix} x_1 - 1 & x_2 - 1 \\ x_1 & x_2 \end{pmatrix} = 2\,.$$

This holds unless $x_1 = x_2$. In that case, $\log x_1 = \log x_2 = 0$, which only holds for finitely many $x_1, x_2 \in \mathcal{O}_{L_\mathfrak{P}}$. Hence, the set of points where the rank drops is finite.

On residue discs where F_1, F_2, G_1 and G_2 can be expressed as overconvergent power series, this implies that all common zeros are isolated (even among the $\mathcal{O}_{\mathbb{C}_p}$-valued zeros.)

In particular, the set of $\mathcal{O}_{L_\mathfrak{P}}$-valued common zeros of F_1, F_2, G_1, G_2 is finite, which proves the claim. □

In fact, since the equations used in the proof of Proposition 6.2.1 do not depend

on the choice of field, the proof is uniform in the field in the following sense. We have:

Corollary 6.2.2.

$$\bigcup_{K:[K:\mathbb{Q}]=2} (\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) < \infty.$$

In fact, the only solutions to the unit equation in real quadratic fields are

$$\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}, \frac{3+\sqrt{5}}{2}, \frac{-1-\sqrt{5}}{2}, \frac{3-\sqrt{5}}{2}, \text{ and } \frac{-1+\sqrt{5}}{2}.$$

As an amusing digression, we note a quick geometric proof of this result.

$$\begin{aligned} \mathrm{Sym}^2(\mathbb{P}^1 \smallsetminus \{0,1,\infty\}) &\cong \mathbb{G}_m \times \mathbb{G}_m, \\ \{x,y\} &\mapsto (xy, (x-1)(y-1)). \end{aligned}$$

Since $\#(\mathbb{G}_m \times \mathbb{G}_m)(\mathbb{Z}) = 4$ and each element corresponds to an unordered pair of solutions, there are exactly 8 solutions to the unit equation in quadratic fields.

In [DCW15], Dan-Cohen and Wewers develop an explicit version Kim's of non-abelian Chabauty to study points on $(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K)$. Their computation cuts out solutions using single-variable polylogarithms instead of sums of logarithms in different variables. In the case where K is a quadratic field, their method is *also* uniform in the field, giving another proof that these are the only solutions to the unit equation in quadratic fields where 11 splits.

6.2.2 Complex cubic fields

Proposition 6.2.3. *Let K be a complex cubic field. Let*

$$\begin{aligned} j : \mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0,1,\infty\} &\hookrightarrow \mathbb{G}_{m,\mathcal{O}_K} \times \mathbb{G}_{m,\mathcal{O}_K} \\ x &\mapsto (x, x-1). \end{aligned}$$

Also use j to refer to the corresponding map on the restriction of scalars to $\mathbb{Z}$. Then, inside $(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z}_p)$, the intersection

$$j((\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}\,\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathbb{Z}_p)) \cap \overline{(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z})}$$

consists of finitely many isolated points. It follows that $\#(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) < \infty$.

Proof. Suppose now that K is a complex cubic field. In this case, $\operatorname{rank}\mathcal{O}_K^\times = 1$ and $[K:\mathbb{Q}] = 3$, so $\mathscr{A}$ is 2-dimensional. Thus, $\mathscr{A}$ is spanned by $(1,1,1)$ and one other vector, call it (a_1,a_2,a_3).

We wish to show that the any common zero in $(\mathcal{O}_{L_\mathfrak{P}}^\times)^6$ to the equations

$$\begin{aligned}
F_1&\colon \log x_1 + \log x_2 + \log x_3 = 0\,,\\
F_2&\colon a_1\log x_1 + a_2\log x_2 + a_3\log x_3 = 0\,,\\
F_3&\colon \log y_1 + \log y_2 + \log y_3 = 0\,,\\
F_4&\colon a_1\log y_1 + a_2\log y_2 + a_3\log y_3 = 0\,,\\
G_1&\colon x_1 - y_1 - 1 = 0\,,\\
G_2&\colon x_2 - y_2 - 1 = 0\,,\\
G_3&\colon x_3 - y_3 - 1 = 0\,,
\end{aligned}$$

consists of points which are isolated inside the set of $\mathcal{O}_{\mathbb{C}_p}$-valued solutions. Let X be the set $\mathcal{O}_{L_\mathfrak{P}}$-valued common solutions of the F_i and G_j.

To do this, we will check that with finitely many exceptions, the intersection of the tangent spaces of the equations $F_1,F_2,F_3,F_4,G_1,G_2,G_3$ at $x \in X$ is zero-dimensional. To do this, we will show that the matrix of derivatives at $x = (x_1,x_2,x_3,y_1,y_2,y_3) \in$

X, namely

$$M_x := \begin{pmatrix} \frac{1}{x_1} & \frac{1}{x_2} & \frac{1}{x_3} & 0 & 0 & 0 \\ \frac{a_1}{x_1} & \frac{a_2}{x_2} & \frac{a_3}{x_3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{y_1} & \frac{1}{y_2} & \frac{1}{y_3} \\ 0 & 0 & 0 & \frac{a_1}{y_1} & \frac{a_1}{y_2} & \frac{a_1}{y_3} \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

has rank 6 except for a finite subset of X consisting of isolated points. We may assume without loss of generality that $a_1 = 0$. Substituting $y_j = x_j - 1$ and applying elementary row and column operations, the condition $\operatorname{rank} M_x \neq 6$ is equivalent to

$$\operatorname{rank} \begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ 0 & a_2 & a_3 \\ 0 & a_2 x_2 & a_3 x_3 \end{pmatrix} = 3\,.$$

If this fails, then $(0, a_2, a_3)$ is proportional to $(0, a_2 x_2, a_3 x_3)$. If these vectors are proportional, then either (i) $a_2 = 0$, (ii) $a_3 = 0$, or (iii) $x_2 = x_3$.

If we are in case (i), we may replace $(0, 0, a_3)$ with $(-a_3, -a_3, 0)$ and $(0, 0, a_3 x_3)$ with $(-a_3 x_1, -a_3 x_2, 0)$ and reindex the variables to reduce to case (iii). We can do the same in case (ii). Making a similar transformation, we may assume that $a_2 + a_3 \neq 0$. So, when $\operatorname{rank} M_x \neq 6$, we must have $x_2 = x_3$ and $y_2 = y_3$.

When we plug this into the F_i and G_i, we get $(a_2 + a_3) \log x_2 = 0$. So, if $\operatorname{rank} M_x \neq 6$, then $\log x_2 = 0$. It follows that if $\operatorname{rank} M_x \neq 6$,

$$\log x_1 = \log x_2 = \log x_3 = \log y_1 = \log y_2 = \log y_3 = 0\,.$$

The solutions to this equation are isolated in $(\mathcal{O}_{\mathbb{C}_p}^{\times})^6$, so we have shown that the dimension of the the intersection of the tangent spaces of the F_i and G_i is zero-dimensional for $x \in X$ except perhaps at a finite set of isolated points. We have seen

that the points of X are all isolated among the $\mathbb{C}_p$ solutions to the F_i and G_i in their residue disc. Therefore, X is finite. The conclusion follows immediately. $\square$

6.2.3 Totally complex quartic fields

Let K be a totally complex quartic field. In this case, $\operatorname{rank} \mathcal{O}_K^\times = 1$ and $[K : \mathbb{Q}] = 4$, so $\mathscr{A}$ is 3-dimensional. Thus, $\mathscr{A}$ is spanned by $v_1 := (1, 1, 1, 1)$ and two other vectors, which we may assume have the form $v_2 := (0, 1, a_3, a_4)$ and $v_3 := (0, 0, 1, b_4)$ after possibly reindexing. Let $v^{(i)}$ denote the ith component of the vector v.

As in the previous cases, for $i \in \{1, 2, 3\}$ and $j \in \{1, 2, 3, 4\}$ we can set

$$\begin{aligned} F_i &\colon v_i^{(1)} \log x_1 + v_i^{(2)} \log x_2 + v_i^{(3)} \log x_3 + v_i^{(4)} \log x_4 \,, \\ F_{i+3} &\colon v_i^{(1)} \log y_1 + v_i^{(2)} \log y_2 + v_i^{(3)} \log y_3 + v_i^{(4)} \log y_4 \,, \\ G_j &\colon x_j - y_j - 1 = 0 \,. \end{aligned}$$

Let X be the set of solutions to the F_i and G_j in $(\mathcal{O}_{L_\mathfrak{P}}^\times)^8$. As in previous cases, we claim that each $x \in X$ is isolated among the $\mathcal{O}_{\mathbb{C}_p}$-valued solutions to the F_i and G_j in any residue disc about x.

We check that at $x \in X$, the intersection of the tangent spaces of the F_i and G_j is zero-dimensional except possibly on a finite subset of X consisting of isolated points. This is equivalent to checking that the matrix

$$M_x := \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ 0 & 1 & a_3 & a_4 \\ 0 & x_2 & a_3 x_3 & a_4 x_4 \\ 0 & 0 & 1 & b_4 \\ 0 & 0 & x_3 & b_4 x_4 \end{pmatrix}$$

has rank 4. If this fails, then either (i) $x_3 = x_4$ or (ii) $b_4 = 0$. If $x_3 = x_4$ and

$\operatorname{rank} M_x < 4$, we must have

$$\operatorname{rank} \begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_4 \\ 0 & 1 & (a_3+a_4)/2 \\ 0 & x_2 & x_4(a_3+a_4)/2 \end{pmatrix} < 3\,.$$

If $b_4 = 0$ and $\operatorname{rank} M_x < 4$, we must have

$$\operatorname{rank} \begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_4 \\ 0 & 1 & a_4 \\ 0 & x_2 & a_4 x_4 \end{pmatrix} < 3\,.$$

In both cases, the proof that the rank drops at points x in a subset of X consisting of isolated points is essentially the same as in the cubic field case, so we omit it. We conclude:

Proposition 6.2.4. *If K is a totally complex quartic field, then the intersection*

$$(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_{L_\mathfrak{P}})^d \cap \overline{\mathbb{G}_m(\mathcal{O}_K) \times \mathbb{G}_m(\mathcal{O}_K)} \subset \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d$$

consists of finitely many isolated points. Thus,

$$\#(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) < \infty$$

6.2.4 Mixed quartic fields with a totally real subfield

Suppose now that K is a mixed quartic field, i.e. that $r_1(K) = 2$ and $r_2(K) = 1$. In this case, $\operatorname{rank} \mathcal{O}_K^\times = 2$ and $[K : \mathbb{Q}] = 4$, so $\mathscr{A}$ is 2-dimensional. Thus, $\mathscr{A}$ is spanned by $(1,1,1,1)$ and one other vector, call it (a_1, a_2, a_3, a_4).

We claim:

Proposition 6.2.5. *If K is a mixed quartic field with a totally real quadratic sub-*

field, then for any p, the image $j((\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K))$ *in* $\mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d \times \mathbb{G}_m(\mathcal{O}_{L_\mathfrak{P}})^d$ *is contained in the (finite) subset of* $\mathcal{O}_{L_\mathfrak{P}}^\times$*-valued common solutions to the equations*

$$\begin{aligned}
F_1 &: \log x_1 + \log x_2 + \log x_3 + \log x_4 = 0\,,\\
F_2 &: a_1 \log x_1 + a_2 \log x_2 + a_3 \log x_3 + a_4 \log x_4 = 0\,,\\
F_3 &: \log y_1 + \log y_2 + \log y_3 + \log y_4 = 0\,,\\
F_4 &: a_1 \log y_1 + a_2 \log y_2 + a_3 \log y_3 + a_4 \log y_4 = 0\,,\\
G_j &: x_j - y_j - 1 = 0 \quad \textit{for} \quad j \in \{1,2,3,4\}\,,
\end{aligned}$$

which are isolated among the $\mathcal{O}_{\mathbb{C}_p}^\times$*-valued common solutions.*

In particular,

$$\#(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) < \infty\,.$$

Let k be the totally real subfield of K. The field k has two embeddings $\tau_1, \tau_2 \hookrightarrow L_\mathfrak{P}$. Say that σ_1 and σ_2 extend τ_1 and that σ_3 and σ_4 extend τ_2.

In our chosen coordinates, we can identify $\left(\mathrm{Res}_{\mathcal{O}_k/\mathbb{Z}}\mathbb{G}_m\right)_{L_\mathfrak{P}}$ inside of $\left(\mathrm{Res}_{\mathcal{O}_k/\mathbb{Z}}\mathbb{G}_m\right)_{L_\mathfrak{P}}$ as the space $x_1 = x_2$, $x_3 = x_4$.

If we restrict F_1 and F_2 to this subspace, then they must vanish on the points corresponding to elements of $\mathcal{O}_k^\times$. Taking parameters x_1 and x_3, the space of functions of the form $b_1 \log x_1 + b_3 \log x_3$ on

$$\left(\mathrm{Res}_{\mathcal{O}_k/\mathbb{Z}}\mathbb{G}_m\right)_{L_\mathfrak{P}}(L_\mathfrak{P})$$

which vanish on the image of $\mathbb{G}_m(\mathcal{O}_k)$ is one-dimensional vector space spanned by $\log x_1 + \log x_3$. This implies that $a_1 + a_2 = a_3 + a_4$. So, we may assume that

$$a_1 = 0, a_2 = 1, a_3 = b, a_4 = 1 - b\,.$$

Substituting for the y_i using the G_i, if we followed the pattern from the previous subsections we would now show that the set $X \subset (\mathcal{O}_{L_\mathfrak{P}}^\times \cap (\mathcal{O}_{L_\mathfrak{P}}^\times - 1))^4$ of common

solutions of the equations

$$\begin{aligned}
\log x_1 + \log x_2 + \log x_3 + \log x_4 &= 0\,,\\
\log x_2 + b\log x_3 + (1-b)\log x_4 &= 0\,,\\
\log(1-x_1) + \log(1-x_2) + \log(1-x_3) + \log(1-x_4) &= 0\,,\\
\log(1-x_2) + b\log(1-x_3) + (1-b)\log(1-x_4) &= 0\,.
\end{aligned}$$

consists of isolated points inside the $\mathcal{O}_{\mathbb{C}_p}$-valued solutions. Instead, we will show that if $x \in X$ is not an isolated inside the $\mathcal{O}_{\mathbb{C}_p}$-valued solutions then $x \notin (\mathbb{P}^1_{\mathcal{O}_K} \smallsetminus \{0,1,\infty\})(\mathcal{O}_K)$.

For $x = (x_1, \ldots, x_4) \in X$, let

$$M_x := \begin{pmatrix} \frac{1}{x_1} & \frac{1}{x_2} & \frac{1}{x_3} & \frac{1}{x_4} \\ 0 & \frac{1}{x_2} & \frac{b}{x_3} & \frac{1-b}{x_4} \\ \frac{1}{x_1-1} & \frac{1}{x_2-1} & \frac{1}{x_3-1} & \frac{1}{x_4-1} \\ 0 & \frac{1}{x_2-1} & \frac{b}{x_3-1} & \frac{1-b}{x_4-1} \end{pmatrix}.$$

If $\operatorname{rank}(M_x) < 4$, then

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ 0 & 1 & b & 1-b \\ 0 & x_2 & bx_3 & (1-b)x_4 \end{pmatrix} = 0\,.$$

So, $\operatorname{rank}(M_x) < 4$ if and only if

$$\frac{(x_1-x_3)(x_2-x_4)}{(x_2-x_3)(x_1-x_4)} = \frac{(0-b)(1-(1-b))}{(1-b)(0-(1-b))} = \frac{b^2}{(1-b)^2}\,.$$

In particular, if some point $x \in (\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) \subset X$ is not isolated then b must be algebraic.

We will prove by contradiction that b cannot be algebraic. The key tool is a p-adic analogue due to Brumer [Bru67] of Baker's Theorem on the linear independence of logarithms of algebraic numbers.

Theorem 6.2.6 (Brumer, [Bru67]). *Let $\alpha_1, \ldots, \alpha_n$ be elements of the completion of the algebraic closure of $\mathbb{Q}_p$ which are algebraic over the rationals $\mathbb{Q}$ and whose p-adic logarithms are linearly independent over $\mathbb{Q}$. These logarithms are then linearly independent over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{Q}_p$.*

Choose generators u_1, u_2 for a finite index subgroup of $\mathcal{O}_K^\times$ with $u_1 \in \mathcal{O}_k^\times$.

If b is algebraic, the contrapositive of Brumer's theorem implies that there are integers $c_2', c_3', c_4' \in \mathbb{Z}$, not all zero, such that

$$c_2' \log \sigma_2(u_2) + c_3' \log \sigma_3(u_2) + c_4' \log \sigma_4(u_2) = 0\,,$$

or equivalently that there are $c_2, c_3, c_4 \in \mathbb{Z}$, not all zero, such that

$$\sigma_2(u_2)^{c_2} \sigma_3(u_2)^{c_3} \sigma_4(u_2)^{c_4} = 1\,.$$

Since k is a quadratic field, $\tau_1(k) = \tau_2(k) \subset L_\mathfrak{P}$ *as subsets* of $L_\mathfrak{P}$. Moreover, since K is a quadratic extension of k, we have $\sigma_1(K) = \sigma_2(K) \subset L_\mathfrak{P}$ and $\sigma_3(K) = \sigma_4(K) \subset L_\mathfrak{P}$ as subsets of $L_\mathfrak{P}$. On the other hand, $\sigma_2(K) \cap \sigma_3(K) = \tau_1(k)$ as subsets of $L_\mathfrak{P}$.

Then, if $\sigma_2(u_2)^{c_2} \sigma_3(u_2)^{c_3} \sigma_4(u_2)^{c_4} = 1$, we must have $\sigma_2(u_2)^{c_2} \in \tau_1(k) \subset L_\mathfrak{P}$. Hence, there are nonzero $c, d \in \mathbb{Z}$ such that $\sigma_2(u_2)^{c \cdot c_2} = \sigma_2(u_1)^d$. But this is only possible if $c_2 = 0$, since u_1 and u_2 generate a rank 2 group and are therefore multiplicatively independent.

Hence, we have

$$\sigma_3(u_2)^{c_3} \sigma_4(u_2)^{c_4} = 1\,.$$

By the same argument applied to $u_1 u_2$ in place of u_2, there are non-zero $d_3, d_4 \in \mathbb{Z}$ such that

$$\sigma_3(u_2 u_1)^{d_3} \sigma_4(u_2 u_1)^{d_4} = 1\,. \tag{6.2.7}$$

So, we have

$$\sigma_3(u_2)^{c_3d_3}\sigma_4(u_2)^{c_4d_3} = 1\,,$$
$$\sigma_3(u_2u_1)^{c_3d_3}\sigma_4(u_2u_1)^{c_3d_4} = 1\,.$$

This implies that $\sigma_4(u_2)^{c_4d_3-c_3d_4} = \sigma_3(u_1)^{c_3d_3}\sigma_4(u_1)^{c_3d_4} \in \tau_2(k)$. So, $c_4d_3 = c_3d_4$. Then,

$$(\sigma_3(u_1)^{d_3}\sigma_4(u_1)^{d_4})^{c_3} = 1\,,$$

so $\sigma_3(u_1)^{d_3}\sigma_4(u_1)^{d_4} = \tau_2(u_1)^{d_3+d_4}$ is a root of unity. But if $u_1^{d_3+d_4}$ is a root of unity, $d_3 = -d_4$, since u_1 generates the free part of $\mathcal{O}_k$.

Then, 6.2.7 becomes $\sigma_3(u_2)^{d_3} = \sigma_4(u_2)^{d_3}$, which implies that $\sigma_3(u_2)^{d_3} \in \tau_2(k)$. Since d_3 and d_4 are non-zero and $u_2 \notin k$, this is a contradiction. This proves that b cannot be algebraic.

As a consequence, if some point $x \in X$ is not isolated in the $\mathcal{O}_{\mathbb{C}_p}$ solutions to our equations on its residue disc, then $x \notin (\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K)$.

This completes the proof.

6.3 Fields where 3 splits completely

Theorem 6.3.1. *Suppose that $[K:\mathbb{Q}]$ is not divisible by 3 and that 3 splits completely in K. Then there is no pair $x, y \in \mathcal{O}_K^\times$ such that $x + y = 1$. Equivalently,*

$$(\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathcal{O}_K) = \emptyset.$$

Remark 6.3.2. Before we begin the proof, we note that the corresponding result for 2 is trivial. In fact, if there is *any* prime $\mathfrak{p}$ above 2 such that $K_\mathfrak{p}$ is a totally ramified extension of $\mathbb{Z}_2$ and $\mathfrak{p} \notin S$ then there are no $x, y \in \mathcal{O}_{K,S}^\times$ such that $x + y = 1$. In that setup, the proof is very short; there is a local obstruction at $\mathfrak{p}$. Solutions to the unit equation cannot be congruent to 0 or 1 modulo $\mathfrak{p}$. On the other hand, if $K_\mathfrak{p}$ is totally ramified over $\mathbb{Z}_2$, then every element of $\mathcal{O}_{K,S}$ is either congruent to 0 or 1 modulo $\mathfrak{p}$.

Proof. Although it is disguised in our argument, the main idea of the proof is to use a variant of Chabauty's method to prove that for any unit $u \in \mathcal{O}_K^\times$, the intersection

$$(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}\,\mathbb{P}^1 \smallsetminus \{0,1,\infty\})(\mathbb{Z}_3) \cap \overline{\{u^n : n \in \mathbb{Z}\} \times \mathcal{O}_K^\times}$$

inside $(\mathrm{Res}_{\mathcal{O}_K/\mathbb{Z}}(\mathbb{G}_m \times \mathbb{G}_m))(\mathbb{Z}_3)$ is empty.

Suppose that 3 splits completely in K and choose any $u \in \mathcal{O}_K^\times$. The splitting gives d different maps $\mathcal{O}_K \to \mathbb{Z}_3$. Let $u_1, \ldots, u_d$ be the images of u in $\mathbb{Z}_3$ under these maps. Since u is a unit,

$$\prod_{i=1}^{d} u_i = \mathrm{Nm}_{K/\mathbb{Q}}\, u \in \mathbb{Z}^\times = \{\pm 1\}\,.$$

Now, suppose further that $-u$ is a solution to the unit equation, so that there exists some $v \in \mathcal{O}_K^\times$ with $-u - v = 1$. Since u and v are units, we must have $u_i \in 1 + 3\mathbb{Z}_3$ for all $i \in \{1, \ldots, d\}$. Moreover, we have

$$\prod_{i=1}^{d}(1 + u_i) = \mathrm{Nm}_{K/\mathbb{Q}}\, -v = (-1)^d\,.$$

In particular, this says that $n = 1$ is a solution to the p-adic analytic equation

$$f(n) := (1 + u_1^n) \cdots (1 + u_d^n) - (-1)^d = 0\,.$$

Now, $\prod_{i=1}^{d} u_i = 1$ by the norm equation, so

$$\begin{aligned} f(-n) &= \prod_{i=1}^{d}(1 + u_i^{-n}) - (-1)^d \\ &= \prod_{i=1}^{d} u_i^{-n} \prod_{i=1}^{d}(1 + u_i^n) - (-1)^d \\ &= \prod_{i=1}^{d}(1 + u_i^n) - (-1)^d \\ &= f(n)\,, \end{aligned}$$

so f is an even function. In particular, if we expand f as a p-adic power series, only even-degree terms will have non-zero coefficients. Now, we can rewrite f as

$$f(n) = -(-1)^d + \prod_{i=1}^{d}(1 + \exp(n \log u_i)),.$$

Since $\log u_i$ has 3-adic valuation ≥ 1 and exp converges so long as the 3-adic valuation of $(n \log u_i)$ is $> 1/2$, this power series converges on an open neighborhood of $\mathcal{O}_{\mathbb{C}_3} \subset \mathbb{C}_3$.

Expanding f as a power series,

$$f(n) = -(-1)^d + \prod_{i=1}^{d}(2 + n \log u_i + \frac{n^2}{2}(\log u_i)^2 + \frac{n^3}{3!}(\log u_i)^3 + \cdots).$$

So, writing $f(n) = \sum_{j=0}^{\infty} a_n n^j$ and using the identity $\sum_{i=1}^{d} \log u_i = 0$ gives

$$\begin{aligned} a_0 &= 2^d - (-1)^d, \\ a_1 &= 0, \\ a_2 &= 2^{d-3} \sum_{i=1}^{d} (\log u_i)^2, \\ a_3 &= 0, \\ v_3(a_j) &\geq 3 \qquad \text{for all } j \geq 4. \end{aligned}$$

We have $v(a_2) \geq 2$, so $f(n)$ has no solution in $\mathbb{Z}_3$ when a_0 is not divisible by 9. But a_0 is divisible by 9 if and only if d is divisible by 3, which completes the proof. $\square$

Remark 6.3.3. Unfortunately, it seems unlikely that we can do any better in general by these methods.

Consider the number field $K := \mathbb{Q}[z]/(z^3 + 3z^2 + 2z + 3)$. It is easy to check that 3 splits completely in K. A computation in Magma shows that $\mathcal{O}_K^\times$ is generated by $z^2 + 1$ and -1.

Set $u = -(z^2 + 1)^2 = -(9z^2 + 3z + 10) = -3(3z^2 + z + 3) - 1$.

Computing in Magma gives

$$\log(u_1) = 0 \cdot 3^1 + 2 \cdot 3^2 + O(3^3)\,,$$
$$\log(u_2) = 2 \cdot 3^1 + 2 \cdot 3^2 + O(3^3)\,,$$
$$\log(u_3) = 1 \cdot 3^1 + 1 \cdot 3^2 + O(3^3)\,.$$

In this case, it is clear that $v_3(\log(u_1)^2+\log(u_2)^2+\log(u_3)^2) = 2$ exactly. Write $f(n) = \sum_{j=0}^{\infty} a_n n^j$ as in the proof of theorem 6.3.1. Then, we see that $v_3(a_0) = v_3(a_2) = 2$, and all other coefficients have larger valuation. Moreover, $\frac{f(n)}{9} \equiv 1 - n^2 \pmod 3$. It follows by Hensel's Lemma that f will have exactly two solutions in $\mathbb{Z}_3$.

Bibliography

[AKM+18] Alejandra Alvarado, Angelos Koutsianas, Beth Malmskog, Chris Rasmussen, Christelle Vincent, and Mckenzie West. Solving S-unit equations over number fields. https://trac.sagemath.org/ticket/22148, 2018.

[Bak67] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[BD17] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *ArXiv e-prints*, April 2017.

[BD18a] J. Balakrishnan and N. Dogra. An effective Chabauty-Kim theorem. *ArXiv e-prints*, March 2018.

[BD18b] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018.

[BDS+17] J. S. Balakrishnan, N. Dogra, J. Steffen Müller, J. Tuitman, and J. Vonk. Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13. *ArXiv e-prints*, November 2017.

[BG13] Manjul Bhargava and Benedict H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of

Tata Inst. Fundam. Res. Stud. Math., pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[BKSW19] Irene I Bouw, Angelos Koutsianas, Jeroen Sijsling, and Stefan Wewers. Conductor and discriminant of picard curves. *arXiv preprint arXiv:1902.09624*, 2019.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Bou98] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Bru67] Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[Bru03] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[CGP15] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015.

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[CK10] John Coates and Minhyong Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Con99] Brian Conrad. Irreducible components of rigid spaces. *Ann. Inst. Fourier (Grenoble)*, 49(2):473–541, 1999.

[DCW15] Ishai Dan-Cohen and Stefan Wewers. Explicit Chabauty-Kim theory for the thrice punctured line in depth 2. *Proc. Lond. Math. Soc. (3)*, 110(1):133–171, 2015.

[Dog19] Netan Dogra. Unlikely intersections and the chabauty-kim method over number fields. *arXiv preprint arXiv:1903.05032v2*, 2019.

[EH17] J. S. Ellenberg and D. R. Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty. *ArXiv e-prints*, June 2017.

[Eis03] Kirsten Eisenträger. *Hilbert's Tenth Problem and Arithmetic Geometry.* PhD thesis, University of California at Berkeley, 2003.

[EST88] P. Erdös, C. L. Stewart, and R. Tijdeman. Some Diophantine equations with many solutions. *Compositio Math.*, 66(1):37–56, 1988.

[Eve84] J.-H. Evertse. On equations in S-units and the Thue-Mahler equation. *Invent. Math.*, 75(3):561–584, 1984.

[FT15] E. V. Flynn and D. Testa. Finite Weil restriction of curves. *Monatsh. Math.*, 176(2):197–218, 2015.

[FW99] E. Victor Flynn and Joseph L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, 100(4):519–533, 1999.

[GG93] Daniel M. Gordon and David Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus two. *Trans. Amer. Math. Soc.*, 337(2):807–824, 1993.

[GM17] J. Gunther and J. S. Morrow. Irrational points on random hyperelliptic curves. *ArXiv e-prints*, September 2017.

[Gra96] David Grant. Sequences of fields with many solutions to the unit equation. *Rocky Mountain J. Math.*, 26(3):1017–1029, 1996. Symposium on Diophantine Problems (Boulder, CO, 1994).

[Győ19] Kálmán Győry. Bounds for the solutions of s-unit equations and decomposable form equations ii. *arXiv preprint arXiv:1901.11289*, 2019.

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

[Kla93] Matthew James Klassen. *Algebraic points of low degree on curves of low rank*. PhD thesis, The University of Arizona, 1993.

[KRZB16] Eric Katz, Joseph Rabinoff, and David Zureick-Brown. Uniform bounds for the number of rational points on curves of small Mordell-Weil rank. *Duke Math. J.*, 165(16):3189–3240, 2016.

[Lan60] Serge Lang. Integral points on curves. *Inst. Hautes Études Sci. Publ. Math.*, (6):27–43, 1960.

[LT02] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Chabauty-Coleman. *Invent. Math.*, 148(1):47–77, 2002.

[LV18] B. Lawrence and A. Venkatesh. Diophantine problems and p-adic period mappings. *ArXiv e-prints*, July 2018.

[Mah33] K. Mahler. Zur approximation algebraischer zahlen. i. *Math. Ann.*, 1(107):691–730, 1933.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[MP13] M. Ram Murty and Hector Pasten. Modular forms and effective Diophantine approximation. *J. Number Theory*, 133(11):3739–3754, 2013.

[MS93] J. R. Merriman and N. P. Smart. Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point. *Math. Proc. Cambridge Philos. Soc.*, 114(2):203–214, 1993.

[Nag64] Trygve Nagell. Sur une propriété des unités d'un corps algébrique. *Ark. Mat.*, 5:343–356 (1964), 1964.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Ove16] O. Overkamp. Finite descent obstruction and non-abelian reciprocity. *ArXiv e-prints*, November 2016.

[Par14] Jennifer Mun Young Park. *Effective Chabauty for symmetric powers of curves*. PhD thesis, Massachusetts Institute of Technology, June 2014.

[Par16] Jennifer Park. Effective Chabauty for symmetric powers of curves. *ArXiv e-prints*, June 2016.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[PS14] Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.

[Ser65] Jean-Pierre Serre. Classification des variétés analytiques p-adiques compactes. *Topology*, 3:409–412, 1965.

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[Ser06] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

[Sik09] Samir Siksek. Chabauty for symmetric powers of curves. *Algebra Number Theory*, 3(2):209–236, 2009.

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

[Sik15] Samir Siksek. Chabauty and the Mordell-Weil sieve. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 194–224. IOS, Amsterdam, 2015.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sko01] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[Sma99] N. P. Smart. Determining the small solutions to S-unit equations. *Math. Comp.*, 68(228):1687–1699, 1999.

[Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006.

[Sto09] Michael Stoll. On the average number of rational points on curves of genus 2. *arXiv preprint arXiv:0902.4165*, 2009.

[Sto17] Michael Stoll. Chabauty without the Mordell-Weil group. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 623–663. Springer, Cham, 2017.

[Sto19] Michael Stoll. Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell–Weil rank. *J. Eur. Math. Soc. (JEMS)*, 21(3):923–956, 2019.

[Š63] I. R. Šafarevič. Algebraic number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 163–176. Inst. Mittag-Leffler, Djursholm, 1963.

[Wet00] Joseph Wetherell. Chabauty and covers for curves with an automorphism. MSRI Workshop on Arithmetic Geometry, 2000.

[Yu89] Kun Rui Yu. Linear forms in p-adic logarithms. *Acta Arith.*, 53(2):107–186, 1989.