Rational points and unipotent fundamental groups

By

Daniel Rayor Hast

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2018

Date of final oral examination: 1 June 2018

The dissertation is approved by the following members of the Final Oral Committee:

Jordan S. Ellenberg, Professor, Mathematics (dissertation advisor)

Melanie Matchett Wood, Professor, Mathematics

Nigel Boston, Professor, Mathematics and Electrical & Computer Engineering

Autumn Exum Kent, Associate Professor, Mathematics

Abstract

We investigate rational points on higher genus curves over number fields using Kim's non-abelian Chabauty method. We provide an exposition of this method, including a brief survey of the literature in the area. In joint work with Ellenberg, we then study the Selmer varieties of smooth projective curves of genus at least two defined over $\mathbb{Q}$ which geometrically dominate a curve with CM Jacobian. We extend a result of Coates and Kim to show that the non-abelian Chabauty method applies to such a curve. By combining this with results of Bogomolov–Tschinkel and Poonen on unramified correspondences, we deduce that any cover of $\mathbf{P}^1$ with solvable Galois group, and in particular any superelliptic curve over $\mathbb{Q}$, has only finitely many rational points over $\mathbb{Q}$.

We also present a strategy for generalizing the non-abelian Chabauty method to real number fields: A conjecture on certain transcendence properties of the unipotent Albanese map is formulated in the final two chapters of this thesis, together with a proof that this conjecture allows a generalization of several major results in the non-abelian Chabauty method to curves over a real number field.

Acknowledgements

I am deeply grateful to Prof. Jordan Ellenberg for helping me become a better mathematician with his advice and mentorship throughout my graduate studies, and for his role in our collaboration that produced part of this thesis. I also thank Prof. Minhyong Kim, Jackson Morrow, Isabel Vogt, and several anonymous reviewers for their comments on some of the material in this work, and Prof. David Zureick-Brown for our productive conversations on Chabauty's method.

Thanks as well to Prof. Melanie Matchett Wood, Prof. Nigel Boston, Prof. Autumn Kent, and Prof. Daniel Erman for many helpful conversations and words of advice during my graduate career. I sincerely appreciate the time that Prof. Fedor Bogomolov took to talk with me about interactions between my research and unramified correspondences. I am especially grateful to Prof. Karen Smith for sparking my initial interest in algebraic geometry as an undergraduate at University of Michigan.

I was fortunate to have several enlightening conversations on new developments and possible future directions in the non-abelian Chabauty method at a conference at the International Centre for Theoretical Physics in Trieste in September 2017. The many mathematical conversations I have had with my fellow mathematics graduate students at UW–Madison have also contributed greatly to my understanding.

I would also like to thank my fellow graduate workers in the Teaching Assistants' Association of UW–Madison, with whom I was proud to organize for better wages and working conditions during my time here. The University Works Because We Do!

Finally, I thank my family—especially my parents, Diane Rayor and David Hast—for their continual support and encouragement throughout my studies.

I was partially supported by NSF Grant RTG-1502553 during work on this thesis.

Contents

Chapter 1

Introduction

1.1 The big picture

Here is one of the central problems of number theory: Given a finite list of polynomial equations, what can we say about the set of all integer or rational solutions to the equations? More specifically:

(1) Are there any integer or rational solutions at all?

(2) Are there finitely or infinitely many?

(3) If finitely many, how many? (Related: How big can the solutions be?)

(4) Can we find all solutions, and prove that we've found all solutions? (You can start searching, but how do you know when to stop searching for more?)

This problem has a geometric interpretation: If we consider not just integer or rational solutions, but solutions valued in some larger set of numbers with more geometric structure (real numbers, complex numbers, p-adic numbers, and so on), then the set of solutions can itself be given geometric structure—a set of points, a curve, a surface, or a higher-dimensional object. The integer or rational solutions then correspond to *integral* or *rational points*, that is, points with integer or rational coordinates.

In the present work, we'll mostly look at the case of rational points on curves. A remarkable theorem conjectured by Mordell in 1922 and proved by Faltings in 1983 tells us that there are only finitely many rational points on any curve whose *genus* is at least 2. (For non-experts, you can picture the genus as the "number of holes" of the curve. Taking into consideration all points with coordinates in the complex numbers, the "curve" becomes two-dimensional over the real numbers—because the complex plane is a two-dimensional *plane*—so it might look like a sphere (genus zero), or a torus (genus one), or something like a torus but with multiple holes or handles.)

This still leaves some big open questions: How many rational points does any given curve have? Is there some upper bound on the number of rational points that only depends on the genus? Given equations for a curve, how can we provably find all the rational points?

To give a sense of how hard this can be, here are a couple examples:

(1) Fermat's famous "last theorem", first conjectured in 1637, is equivalent to showing that all curves of the form $x^n + y^n = 1$ with $n > 3$ have no rational solutions, excluding the obvious ones where x or y is zero. It wasn't proven until 1994, and Wiles and Taylor's proof requires techniques of algebraic geometry, number theory, and representation theory that were totally unknown to Fermat.

(2) Diophantus' *Arithmetica*, an Ancient Greek text on mathematics, poses a problem that's equivalent to finding rational points (x, y) on the curve $y^2 = x^6 + x^2 + 1$. One pair, $(0, \pm 1)$, is easy to see. Diophantus gave four less obvious points: $(\pm 1/2, \pm 9/8)$. But it wasn't until Wetherell's 1997 thesis that this was proven to be a complete list of the rational points!

Many different methods have been developed to investigate rational points on curves; as of yet, we still don't have a method that's guaranteed to work for all curves. My research is concerned with one particular method for studying rational points on curves—called the *non-abelian Chabauty method*, or the *Chabauty–Coleman–Kim method*—which we hope can be used to create such an algorithm, along with answers to some of the other major questions about rational points.

So far, this method has had some notable successes, including provably computing the set of rational points on some interesting curves where this hadn't been done before. The non-abelian Chabauty method has also yielded new proofs of Faltings' theorem for certain classes of curves; I recently proved one such result in joint work with Jordan Ellenberg, and that result is one of the main topics of this thesis.

1.2 Technical introduction

Let F be a number field, let S be a finite set of primes of F, and let $\mathcal{O} = \mathcal{O}_{F,S}$ be the ring of S-integers of F. Let Y be a smooth, geometrically integral, hyperbolic curve of genus g over a number field F, and let $\mathcal{Y}$ be a smooth model of Y over $\mathcal{O}$ that admits a smooth compactification over $\mathcal{O}$. (Note that Y is hyperbolic if and only if one of the following is true: $g \geq 2$, or $g = 1$ and Y is affine, or $g = 0$ and the complement of Y in its smooth proper model contains at least 3 points.) Our main object of study is the set $\mathcal{Y}(\mathcal{O})$ of S-integral F-points of $\mathcal{Y}$.

By Siegel's theorem in the affine case, and Faltings' theorem [Fal83] (formerly Mordell's conjecture) in the proper case, $\mathcal{Y}(\mathcal{O})$ is a finite set. Note that if Y is proper, then $\mathcal{Y}(\mathcal{O}) = Y(F)$ by the valuative criterion for properness; we will focus mostly on this case.

Even before Faltings, one knew finiteness of $Y(F)$ under certain conditions. One early strategy, developed by Chabauty [Cha41], shows that $Y(F)$ is finite whenever the Mordell–Weil rank of the Jacobian $J_Y = \mathrm{Jac}(Y)$ is strictly smaller than g. More recently, Kim [Kim05; Kim09; Kim12b; CK10] developed a non-abelian version of the Chabauty method, in which the role of the Mordell–Weil group of the Jacobian is played by a p-adic manifold called the *Selmer variety*, which we describe in §1.3 below. If this Selmer variety has small enough dimension, one can conclude that $\mathcal{Y}(\mathcal{O})$ is finite. This "dimension hypothesis" is the nonabelian analogue of the Chabauty condition

$$\mathrm{rank}\, J_Y(F) < g.$$

While there are many curves that fail to satisfy the Chabauty condition, it is at least plausible to hope that every curve over every number field satisfies Kim's dimension hypothesis.

However, verifying the dimension hypothesis has been difficult, apart from certain special classes of curves. Here are several classes for which the dimension hypothesis is known:

(1) For arbitrary hyperbolic curves, conditional on either the Fontaine–Mazur conjecture or the Bloch–Kato conjecture [Kim09];

(2) When $g = 0$ and $F = \mathbb{Q}$ [Kim05];

(3) When $g = 0$ and F is a totally real field [Kim12c];

(4) When Y is a CM elliptic curve minus the origin [Kim09, §4];

(5) When $g \geq 2$, $F = \mathbb{Q}$, the rank of $J_Y(\mathbb{Q})$ is equal to g, the Neron–Severi group of

J_Y has rank at least 2, and the p-adic closure of $J_Y(\mathbb{Q})$ has finite index in $J_Y(\mathbb{Q}_p)$ [BDMTV17];

(6) When $g \geq 2$, $F = \mathbb{Q}$, and Y is a curve whose Jacobian has CM [CK10];

(7) When $g \geq 2$, $F = \mathbb{Q}$, and Y admits a dominant morphism, defined over $\bar{\mathbb{Q}}$, to curve whose Jacobian has CM [EH18].

This last result, due to myself and Ellenberg, is one of the primary topics of this thesis. To lay the groundwork for our theorem, let us first state the main theorem of [CK10].

Theorem 1.1 ([CK10])**.** *Let Y be a smooth projective curve over $\mathbb{Q}$ of genus at least 2 whose Jacobian is a CM abelian variety. Then Y satisfies the dimension hypothesis, and in particular, $Y(\mathbb{Q})$ is finite.*

The central result of [EH18] is to generalize Theorem 1.1 to make it apply in slightly greater generality, and to show how this change can be used to substantially expand the class of curves over $\mathbb{Q}$ whose rational points can be proven finite via Kim's method. The following result is a corollary of Theorem 1.3, the main result of [EH18].

Corollary 1.2. *Let $Y/\mathbb{Q}$ be a smooth superelliptic curve $y^d = f(x)$ of genus at least 2. Then $Y(\mathbb{Q})$ is finite.*

Of course, this result is a special case of Faltings' theorem. However, the non-abelian Chabauty method is a fundamentally different way of proving finiteness, whose full scope one would like to understand. In particular, Chabauty methods are more amenable than others to providing explicit upper bounds on the number of rational points (cf. [Col85; KRZ16; BD18a]).

The above theorem is called a corollary because it follows from the main theorem of our paper, which modestly generalizes Theorem 1.1.

Theorem 1.3. *Let Y and X be smooth projective curves over $\mathbb{Q}$ of genus at least 2. Suppose there is a dominant map $f_K\colon Y_K \to X_K$ for some finite Galois extension $K/\mathbb{Q}$, and suppose the Jacobian J_X of X is a CM abelian variety. Then $Y(\mathbb{Q})$ is finite.*

Remark 1.4. We do not quite prove the dimension hypothesis for Y itself, but rather for what one might call a "relative Selmer variety" attached to f_K. Our method is in some sense the non-abelian analogue of a method used in a paper of Flynn and Wetherell [FW99]. In that paper, the authors study certain genus 5 curves $Y/\mathbb{Q}$ which admit a dominant map f to an elliptic curve E; however, the elliptic curve, whence also the map, is defined over a cubic extension K. The proof then proceeds by considering the map from Y to the Weil restriction of scalars $\operatorname{Res}_{\mathbb{Q}}^{K} E$, which is an abelian 3-fold defined over $\mathbb{Q}$; since the rank of $E(K)$ is the same as that of $(\operatorname{Res}_{\mathbb{Q}}^{K} E)(\mathbb{Q})$, it suffices to show that $E(K)$ has rank less than 3. Our argument has a similar structure, utilizing the map afforded by f from Y to the variety $\operatorname{Res}_{\mathbb{Q}}^{K} X$. We will state the "real version" of our theorem, a bound on the dimension of local Selmer varieties, as Theorem 1.5 in §1.3 below, once we've set up the necessary definitions.

The interest of Theorem 1.3 would be limited without a supply of curves satisfying its conditions. Fortunately, such a fund of examples is supplied by a theorem of Bogomolov and Tschinkel [BT02] (see also [BQ17]) which shows that every hyperelliptic curve has an étale cover which geometrically dominates a curve over $\mathbb{Q}$ with CM Jacobian. Poonen [Poo05] generalized this theorem to a more general class of curves, including all superelliptic curves.[1] By now it is well-understood that one can control the rational points of a variety Y by controlling the rational points of the twists of an étale cover of Y. This circle of ideas will allow us to derive Corollary 1.2 from Theorem 1.3.

In §1.3, we briefly sketch Kim's nonabelian Chabauty method. In §2, we define certain quotients of the étale and de Rham fundamental groups. In §2.4, we prove surjectivity of certain maps between fundamental groups. In §2.5, we define Selmer varieties and unipotent Albanese maps associated to the algebraic groups of §2, and we present the key diagram involving Selmer varieties. In §3.1 and §3.2, we prove the bounds needed for the dimension hypothesis, which we prove in §3.3. Finally, in §3.5, we combine our results with a theorem of Poonen [Poo05] to deduce finiteness of $Y(\mathbb{Q})$ for several classes of curves, including hyperelliptic and superelliptic curves.

Note that the above method, along with most of the known Diophantine finiteness results deduced from the non-abelian Chabauty method, only apply to $\mathbb{Q}$-points. This might seem surprising, since the (abelian) method of Chabauty and Coleman applies to curves over arbitrary number fields. In contrast, there seem to be more serious difficulties in generalizing the non-abelian case to arbitrary number fields. We will discuss these difficulties in chapter 4, including an apparent dichotomy between the real and totally imaginary cases.

In chapter 5, we propose a conjecture on the unipotent Albanese map, reminiscent of the Ax–Schanuel conjecture. We show that, conditional on this conjecture, several finiteness results for $\mathbb{Q}$-points using the non-abelian Chabauty method can be generalized to F-points for any real number field F.

[1] Thanks to Isabel Vogt for informing us of this result.

1.3 A sketch of Kim's method

The fundamental idea of the Chabauty [Cha41] method is to embed Y in its Jacobian variety J_Y by the Abel–Jacobi map associated to a rational point $b \in Y(F)$, then study how the $F_\mathfrak{p}$-points of Y (where $\mathfrak{p}$ is a prime of F) interact with the F-points of J_Y. This is illustrated by the commutative diagram

$$\begin{array}{ccc} Y(F) & \hookrightarrow & Y(F_\mathfrak{p}) \\ \downarrow & & \downarrow \\ J_Y(F) & \hookrightarrow & J_Y(F_\mathfrak{p}). \end{array} \tag{1.1}$$

By the Mordell–Weil theorem, $J_Y(F)$ is a finitely-generated abelian group of some rank r. In the case where $r < g$ and $\mathfrak{p}$ is an unramified prime of F of good reduction for Y, Chabauty proved that the image of $Y(F_\mathfrak{p})$ in the $\mathbb{Q}_p$-vector space $J_Y(F_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q}_p$ is dense, while the image of $J_Y(F)$ in $J_Y(F_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q}_p$ is contained in the vanishing of some nonzero form f; thus $Y(F)$ lies in the vanishing locus of f in $Y(F_\mathfrak{p})$. By the Zariski-density, $f|Y(F_\mathfrak{p})$ is nonzero, so its vanishing locus, whence also $Y(F)$, is finite.

Although Faltings' result subsumes Chabauty's, this method is still of interest: Coleman [Col85] refined Chabauty's method to show that, when $r < g$ as above, if $\mathfrak{p}$ is an unramified prime of good reduction for Y, of residue characteristic at least $2g$, then

$$\#Y(F) \leq N\mathfrak{p} + 2g(\sqrt{N\mathfrak{p}} + 1) - 1.$$

In the case where $r \leq g - 3$, Stoll [Sto15], Katz, Rabinoff, and Zureick-Brown [KRZ16] extended Coleman's method to primes of bad reduction, obtaining a *uniform* bound (depending only on g and $[F : \mathbb{Q}]$) on the cardinality of $Y(F)$ for such curves. This bound is very explicit; for example, when $F = \mathbb{Q}$, the bound is $\#Y(\mathbb{Q}) \leq 84g^2 - 98g + 28$.

Unfortunately, Chabauty's method does not apply when $r \geq g$. Minhyong Kim's idea (see [Kim05], [Kim09], [Kim12b], [CK10]), motivated in large part by Grothendieck's anabelian philosophy and the section conjecture, was to develop a "non-abelian Chabauty" method, in which the Jacobian of Y is replaced by a geometric object capturing a larger piece of the fundamental group, allowing a version of Chabauty's argument to go through even when the rank of $J_Y(F)$ is large.

The description of Kim's method that follows is largely drawn from [Kim09].

Remaining in the abelian context for a moment, we have a cohomological version of the commutative diagram (1.1):

$$\begin{array}{ccccc} Y(F) & \hookrightarrow & Y(F_{\mathfrak{p}}) & & \\ \downarrow & & \downarrow & \searrow & \\ H^1_f(G_F, V_p) & \longrightarrow & H^1_f(G_{\mathfrak{p}}, V_p) & \longrightarrow & \mathrm{Lie}(J_Y) \otimes_{\mathbb{Q}_p} F_{\mathfrak{p}}, \end{array}$$

where G_F and $G_{\mathfrak{p}}$ are the absolute Galois groups of F and $F_{\mathfrak{p}}$, respectively; V_p is the $\mathbb{Q}_p$-Tate module of J_Y; and H^1_f denotes the pro-p-Selmer group, i.e., the space of G_F-torsors of V_p that are unramified at the good primes of Y and crystalline at $\mathfrak{p}$.

Kim's non-abelian Chabauty method replaces V_p, which is essentially equivalent to the *abelianization* of the geometric (étale) fundamental group of Y, with the $\mathbb{Q}_p$-pro-unipotent completion (i.e., Malcev completion) Π_Y of the geometric fundamental group of Y. In order to work with schemes of finite type, we truncate after finitely many steps of the lower central series, and denote by $\Pi_{Y,n}$ the quotient of Π_Y by the $(n+1)$-st level of the lower central series of Π_Y. Kim [Kim09] showed that, for each $n \geq 1$, the spaces of torsors $H^1_f(G_F, \Pi_{Y,n})$ and $H^1_f(G_{\mathfrak{p}}, \Pi_{Y,n})$ are represented by algebraic varieties over $\mathbb{Q}_p$, called the (global and local) *Selmer varieties* of Y.

Likewise, $\mathrm{Lie}(J_Y) \otimes_{\mathbb{Q}_p} F_{\mathfrak{p}}$ is replaced with

$$\Pi_Y^{\mathrm{dR}} / F^0 \Pi_Y^{\mathrm{dR}}.$$

Here, Π_Y^{dR} is the de Rham fundamental group of Y, classifying unipotent vector bundles with integrable connection [Del89], and the de Rham realization $\Pi_Y^{\mathrm{dR}}/F^0\Pi_Y^{\mathrm{dR}}$ is the moduli space of "admissible" torsors for Π_Y^{dR} with separately trivializable Hodge structure and Frobenius action [Kim09, Prop. 1]. Restricting to the Tannakian subcategory generated by bundles of unipotency class at most n, we obtain finite-level versions

$$\Pi_{Y,n}^{\mathrm{dR}}/F^0\Pi_{Y,n}^{\mathrm{dR}},$$

which are represented by algebraic varieties over $\mathbb{Q}_p$.

As in the abelian case, there are analogues of the Abel–Jacobi map — which Kim calls the (local and global) *unipotent Albanese maps* — fitting into a commutative diagram

$$\begin{array}{ccccc} Y(F) & \hookrightarrow & Y(F_{\mathfrak{p}}) & & \\ \downarrow & & \downarrow & \searrow & \\ H^1_f(G_F, \Pi_{Y,n}) & \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} & H^1_f(G_{\mathfrak{p}}, \Pi_{Y,n}) & \xrightarrow{D} & \mathrm{Res}^{F_{\mathfrak{p}}}_{\mathbb{Q}_p}(\Pi_{Y,n}^{\mathrm{dR}}/F^0\Pi_{Y,n}^{\mathrm{dR}}) \end{array}$$

Kim showed that the image of $Y(F_{\mathfrak{p}})$ under the unipotent de Rham Albanese map is Zariski-dense in the de Rham local Selmer variety. Suppose the image of the localization map $\log_{\mathfrak{p}} := D \circ \mathrm{loc}_{\mathfrak{p}}$ is non-Zariski-dense; equivalently, there is an algebraic function F on $\mathrm{Res}^{F_{\mathfrak{p}}}_{\mathbb{Q}_p}(\Pi_{Y,n}^{\mathrm{dR}}/F^0\Pi_{Y,n}^{\mathrm{dR}})$ which vanishes on the image of $\log_{\mathfrak{p}}$. Since the image of $Y(F_{\mathfrak{p}})$ is Zariski dense, the pullback f of F to $Y(F_{\mathfrak{p}})$ is nonzero. But the image of $Y(F)$ in $Y(F_{\mathfrak{p}})$ lies in the vanishing of f, which is necessarily finite; so $Y(F)$ is finite as well.

Since $\log_{\mathfrak{p}}$ is algebraic, it suffices for the desired non-Zariski-density to prove the following "dimension hypothesis" for $n \gg 0$:

$$\dim H^1_f(G_F, \Pi_{Y,n}) < \dim \mathrm{Res}^{F_{\mathfrak{p}}}_{\mathbb{Q}_p}(\Pi_{Y,n}^{\mathrm{dR}}/F^0\Pi_{Y,n}^{\mathrm{dR}}) \qquad (\mathrm{DH}_{n,p})$$

More generally, it will suffice in our work to prove this for a certain quotient Ψ_n of $\Pi_{Y,n}$:

$$\dim H^1_f(G_F, \Psi_n) < \dim \mathrm{Res}^{F_{\mathfrak{p}}}_{\mathbb{Q}_p}(\Psi_n^{\mathrm{dR}}/F^0\Psi_n^{\mathrm{dR}}) \qquad (\mathrm{DH}_{\Psi_n,p})$$

Such a statement has been proved in several special cases; most relevant to us is the case [CK10] where Y is projective of genus at least two, $F = \mathbb{Q}$, and the Jacobian of Y is isogenous over $\bar{\mathbb{Q}}$ to a product of CM abelian varieties. (See [Kim12b] for an overview of some contexts where the method has been carried through successfully.)

In the present work, we weaken one hypothesis on Y: instead of requiring that Y itself have CM Jacobian, we require only that Y admit a dominant map onto such a curve after extension of the base number field. By combining this with theorems of Poonen [Poo05] and Bogomolov and Tschinkel [BT02] on the existence of certain unramified correspondences, we deduce that any curve admitting a map to $\mathbf{P}^1$ with solvable Galois group has only finitely many $\mathbb{Q}$-points. (See §3.5 for the precise statement.)

Theorem 1.5. *Let Y and X be smooth projective curves over $\mathbb{Q}$ of genus at least 2. Suppose there is a dominant map $f_K\colon Y_K \to X_K$ for some finite Galois extension $K/\mathbb{Q}$ of degree d. Let p be a prime of good reduction for both Y and X. Let S be a set of primes such that Y and X both have good reduction outside $T = S \cup \{p\}$. Suppose also that there is a number field L/K and a constant $B > 0$ (depending on X and T) such that for all $n \geq 1$,*

$$\sum_{i=1}^{n} \dim H^2(G_{L,T}, U_X^n/U_X^{n+1}) \leq Bn^{2g-1},$$

where U_X is the quotient of Π_X by the third level of its derived series. Then for $n \gg 0$,

$$\dim H^1_f(G_{\mathbb{Q}}, W_{[n]}) < \dim W_{[n]}^{\mathrm{dR}}/F^0 W_{[n]}^{\mathrm{dR}}, \qquad (\mathrm{DH}_{W_{[n]},p})$$

where $W_{[n]}$ is the quotient of Π_Y defined in §2.3. In particular, the image of $\log_p$ is non-Zariski-dense, so $Y(\mathbb{Q})$ is finite.

Remark 1.6. By [CK10, Thm. 0.1], the hypotheses of Theorem 1.5 are satisfied whenever the Jacobian J_X of X is isogenous over $\bar{\mathbb{Q}}$ to a product of CM abelian varieties.

1.4 A survey of the literature

Now that we have set up the notation and described the non-abelian Chabauty method, we provide a brief survey of some major results proved thus far. We do not attempt to comprehensively mention all results in the area, only some selected highlights that provide a sense of the big picture and active directions of research.

1.4.1 Chabauty's method

As previously mentioned, Chabauty's method started with the 1941 work of Chabauty [Cha41], and gained renewed attention with Coleman's 1985 paper [Col85] making the method explicit using p-adic analysis at a prime p of good reduction for the curve.

Theorem 1.7 ([Cha41])**.** *Let C be a smooth projective curve of genus g over a number field F. Let J be the Jacobian of C, and let $j\colon C \to J$ be the Abel–Jacobi map (a.k.a. the Albanese map) associated to a rational point $b \in C(F)$. Let v be a finite prime of F of good reduction for C. Suppose the rank r of the Mordell–Weil group $J(F)$ is less than g. Then the intersection*

$$j(C(F_v)) \cap \overline{J(F)}$$

is finite, where $\overline{J(F)}$ denotes the p-adic closure in $J(F_v)$. In particular, the subset $C(F)$ is finite.

Theorem 1.8 ([Col85])**.** *Under the hypotheses of Theorem 1.7, assuming the residue characteristic of v is at least $2g$, we have*

$$\#C(F) \leq Nv + 2g(\sqrt{Nv} + 1) - 1.$$

By extending to primes of bad reduction and using tropical geometry to handle the combinatorics of the reductions mod p, one can refine this further to a *uniform* bound on the number of rational points of low rank:

Theorem 1.9 ([KRZ16, Thm. 1.1]). *Let $d \geq 1$ and $g \geq 3$ be integers. There exists an explicit constant $N(g,d)$ such that for any number field F of degree d and any smooth, proper, geometrically connected genus g curve X/F of Mordell–Weil rank at most $g-3$, we have*

$$\#X(F) \leq N(g,d).$$

In particular, one can take $N(g,1) = 84g^2 - 98g + 28$.

An inherent restriction of this method is that $J(F)$ must be p-adically non-dense in $J(F_v)$. This does hold in some cases where $r \geq g$, for example as in [FW99], which deals with rational points on bielliptic genus 2 curves using a variant of Chabauty's method. However, this condition on $J(F)$ simply fails for some curves.

1.4.2 Kim's non-abelian generalization

See [Kim12b] for an expository overview and discussion of the motivation for Kim's method. (I found this to be a good introduction to this area of research.)

A promising approach to overcoming the restriction on the rank in Chabauty's method came with Kim's 2005 paper [Kim05], which replaces the Jacobian with a space constructed from a larger, non-abelian piece of the fundamental group to give a new proof of Siegel's S-unit theorem.

Theorem 1.10 ([Kim05]). *Let $C = \mathbf{P}^1 \setminus \{0,1,\infty\}$. Let S be a finite set of rational* *primes, and* $p \notin S$ *another prime. Then* $C(\mathbb{Z}_S)$ *is finite, where* $\mathbb{Z}_S \subset \mathbb{Q}$ *is the ring of* S*-integers.*

Kim put this into the general framework described above in 2009 [Kim09], formulating a *dimension hypothesis* at each index of unipotency n (with $n = 1$ being equivalent to Chabauty's method) sufficient for the method to work in general, and proved this dimension hypothesis conditional on one of several conjectures in Galois cohomology.

Theorem 1.11 ([Kim09, §3])**.** *Let* C *be a smooth connected hyperbolic curve over* $\mathbb{Q}$*. Assume one of the following conjectures: the Fontaine–Mazur conjecture, the Bloch–Kato conjecture, or (in the affine case) the weak Jannsen conjecture. Then the dimension hypothesis holds for* C *at sufficiently large index of unipotency* n*. In particular, the set of integral points of* C *is finite.*

In principle, conditional on some more conjectures, this can be turned into an effective algorithm for computing integral or rational points [Kim12a]. Such conjectures imply that the method determines the set of rational points exactly—i.e., a unipotent analogue of Grothendieck's section conjecture—and this is investigated further, and verified in some special cases, in [BDCKW17].

Much of the work on Kim's method has been in proving the dimension hypothesis unconditionally for larger classes of curves, and making the method more explicit in various ways (for example, by bounding the number or height of points identified by the method, or using the method to construct and implement practical algorithms for finding integral/rational points). The same paper included one such result of the former type:

Theorem 1.12 ([Kim09, §3])**.** *Let* C *be a CM elliptic curve of rank* 1 *minus the origin over* $\mathbb{Q}$*. Then the dimension hypothesis holds for* C *at index of unipotency* $n = 2$*. In* *particular, the set of integral points of C is finite.*

This was generalized to higher genus—with no assumption on the rank—shortly thereafter by Coates and Kim.

Theorem 1.13 ([CK10]). *Let C be a smooth projective curve over $\mathbb{Q}$ of genus at least 2 whose Jacobian has CM over $\bar{\mathbb{Q}}$. Then the dimension hypothesis holds for C at sufficiently large index of unipotency n. Hence, the set of rational points of C is finite.*

The CM hypothesis in the above theorems is useful because it ensures that the p-adic Tate module decomposes as a direct sum of Galois characters. In all cases mentioned so far, the strategy for proving the dimension hypothesis involves using the Euler characteristic formula to reduce the problem to bounding the dimension of an H^2 group in Galois cohomology, a Hodge filtered piece of the de Rham fundamental group, and an Archimedean piece related to the action of complex conjugation. The dimension of the H^2 piece can be reduced by various duality theorems to a problem in Iwasawa theory (see [CK10, §3] for details); the Tate module decomposing as a direct sum of characters ensures the relevant Iwasawa module is commutative, thus avoiding problems in noncommutative Iwasawa theory beyond the reach of currently known techniques.

The latest development I am aware of in this direction is Theorem 1.5, exposited in this thesis, which extends Theorem 1.13 to curves that geometrically dominate a CM curve over $\mathbb{Q}$. In combination with the work of Bogomolov, Tschinkel, and Poonen on unramified correspondences (see sections 3.4 and 3.5), this yields a new proof of finiteness of $\mathbb{Q}$-points on solvable curves (a class that includes hyperelliptic and superelliptic curves). This is still relying on the CM hypothesis: the dominant morphism provides a piece of the Jacobian that has CM, and this is sufficient to essentially lift the dimension estimates of [CK10] (up to some asymptotically negligible factors) to the Selmer varieties of the dominating curve.

1.4.3 Explicit bounds and algorithms

Another major direction of research is in making the method more explicit in various ways. In the more computational work in the literature, the class of curves is often much more restricted; most of the work is for the case $n = 2$, where the computations are more tractable, and this leads to conditions on the rank of the Jacobian, as well as some other technical hypotheses.

One example of such a result is in [BDMTV17], which provides an algorithm for provably computing a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$ under the following conditions:

(1) The Mordell–Weil rank r of the Jacobian $J = \mathrm{Jac}(C)$ is equal to the genus g;

(2) The rank ρ of the Néron–Severi group $\mathrm{NS}(J)$ is greater than 1;

(3) The p-adic closure of $J(\mathbb{Q})$ has finite index in $J(\mathbb{Q}_p)$; and

(4) There are enough rational points in $C(\mathbb{Q})$ to satisfy a technical hypothesis (which we won't explain here, but which is satisfied for many curves of interest).

As an application, they prove that the seven known rational points of $X_s(13)$, the split Cartan modular curve of level 13, are all the rational points, which was not previously known.

In a related work [BD18b], a similar approach is used to prove finiteness of $C(F)$ for any imaginary quadratic field F under the same hypotheses $r = g$, $\rho > 1$, and

$[J(\mathbb{Q}_p) : \overline{J(\mathbb{Q})}] < \infty$ (where r and ρ are now the Mordell–Weil rank and Néron–Severi rank over F, not $\mathbb{Q}$).

In the direction of explicit bounds on the number of rational points, Balakrishnan and Dogra [BD18a] have used the non-abelian Chabauty method at $n = 2$ to provide such a bound for $\mathbb{Q}$-points when $r = g$, under the assumption of a technical hypothesis (which is always true conditionally on a conjecture of Bloch and Kato). The bound depends only on the prime p, the genus g, and local constants n_v defined in terms of the reduction data of the curve at bad primes.

1.4.4 Alternate frameworks and generalizations

A few authors have reformulated the non-abelian Chabauty method in ways that may be useful for future applications and generalizations. One recent reformulation is due to Betts [Bet17], who uses cosimplicial groups and techniques of homotopical algebra to construct local Selmer varieties and a unipotent Albanese map for any variety at any prime, including primes of bad reduction and Archimedean places.

This raises the prospect of studying global Selmer varieties at primes of bad reduction, which one hopes could lead to a non-abelian analogue of results such as those of [KRZ16]. (Of course, there are significant technical obstacles to such a generalization, but it is reassuring to know that the main objects of the theory can at least be constructed.)

Another recent paper, due to Brown [Bro17], reformulates the non-abelian Chabauty method in terms of motivic periods. This leads to more concrete descriptions of some of the objects of the theory, while also highlighting how some of the main results of [Kim09] and related papers can be recast in terms of an elementary lemma in linear algebra and the comparison between de Rham and Betti cohomology.

Finally, in a recent paper [Kim17], Kim draws an analogy between Selmer varieties and the moduli spaces of gauge fields (principal bundles with connection) arising in quantum field theory. Under this analogy, Selmer varieties can be thought of as parametrizing *arithmetic gauge fields*, with rational points mapping under the unipotent Albanese map to *rational gauge fields*. Kim speculates on, and provides some heuristic evidence for, a "least action principle" for arithmetic gauge fields that should identify rational gauge fields in the same way the equations of motion in mechanics are identified by minimizing a certain "action" functional. This analogy to physics, if formalized, might lead to new methods for efficiently finding rational points on curves.

Chapter 2

Fundamental groups and Selmer varieties

The Selmer varieties that play a central role in the non-abelian Chabauty method are constructed as moduli spaces of torsors for various fundamental groups attached to the curve. The two main fundamental groups that appear are:

(1) The $\mathbb{Q}_p$-unipotent étale fundamental group, which carries a $\mathrm{Gal}(\bar{F}/F)$-action induced by the usual Galois action on the geometric étale fundamental group.

(2) The de Rham fundamental group, which carries a Frobenius action (induced by comparison with a *crystalline* fundamental group defined via lifting from the residue field) and a Hodge structure.

The Galois action on the unipotent étale fundamental group provides information about rational points on the curve, while the de Rham fundamental group is more suitable for certain dimension computations; a comparison theorem allows us to relate torsors over the two.

In this chapter, we outline the constructions of these fundamental groups and the notation that will be used in the rest of the paper. In section 2.3, we also construct some quotients and subquotients of these fundamental groups attached to a map between curves; these will be used in later chapters to prove certain cases of the dimension hypothesis.

Finally, in section 2.4, we prove a lemma about functorially induced maps between the unipotent étale and de Rham fundamental groups that will be useful later on.

2.1 Étale realizations

This section and the one that follows are essentially review of the objects constructed in [Kim09].

We briefly recall the definition of the $\mathbb{Q}_p$-pro-unipotent étale fundamental group. Let S be a scheme over a field F of characteristic zero, and let $\bar{S} := S \times_{\operatorname{Spec} F} \operatorname{Spec} \bar{F}$. Let $b \in S(F)$ be a point. Denote by Π_S the p-adic unipotent completion [HM03, Appendix A.2] of the geometric étale fundamental group $\pi_1^{\text{ét}}(\bar{S}, b)$. Then Π_S is a pro-unipotent group scheme over the field $\mathbb{Q}_p$, with an action of $G_F := \operatorname{Gal}(\bar{F}/F)$ induced by the action of G_F on $\bar{S}$.

One can also interpret Π_S as the fundamental group of the Tannakian category $\operatorname{Un}_p^{\text{ét}}(\bar{S})$ of unipotent $\mathbb{Q}_p$-smooth sheaves on the étale site of $\bar{S}$ with fiber functor e_b given by the fiber at b. Indeed, $\operatorname{Un}_p^{\text{ét}}(\bar{S})$ is equivalent to the category of unipotent $\mathbb{Q}_p$-representations of $\pi_1^{\text{ét}}(\bar{S}, b)$, which is equivalent to the category of $\mathbb{Q}_p$-representations of Π_S by the universal property of unipotent completion.

Given a geometric point $s \in S(\bar{F})$, we have the path torsor

$$P_S^{\text{ét}}(s) = \operatorname{Iso}^{\otimes}(e_b, e_s).$$

If $s \in S(F)$, then $P_S^{\text{ét}}(s)$ also has an action of G_F.

Given a pro-unipotent algebraic group U, we denote the lower central series $U^1 = U$ and $U^{n+1} = [U, U^n]$, and the derived series by $U^{(1)} = U$ and $U^{(n+1)} = [U^{(n)}, U^{(n)}]$. Also denote $U_n = U/U^{n+1}$.

Let

$$U_S := \Pi_S / \Pi_S^{(3)}$$

be the metabelianization of Π_S. This is again a pro-unipotent $\mathbb{Q}_p$-group scheme with G_F-action.

2.2 De Rham realizations

We will also need the "de Rham realizations" of the above algebraic groups, whose definitions we now recall. Let L be a field of characteristic zero and let X be a smooth L-scheme. As in [Kim09, §1], let $\mathrm{Un}(X)$ be the Tannakian category of unipotent vector bundles with integrable connection on X.

For each $n \geq 1$, let $\langle \mathrm{Un}_n(X) \rangle$ be the full Tannakian subcategory of $\mathrm{Un}(X)$ generated by bundles with connection $(\mathcal{V}, \nabla_{\mathcal{V}} \colon \mathcal{V} \to \Omega_{X/L} \otimes \mathcal{V})$ with index of unipotency at most n, i.e., such that there exists a filtration

$$\mathcal{V} = \mathcal{V}_n \supseteq \mathcal{V}_{n-1} \supseteq \cdots \supseteq \mathcal{V}_1 \supseteq \mathcal{V}_0 = 0$$

stabilized by the connection $\nabla_{\mathcal{V}}$ and such that each $(\mathcal{V}_i/\mathcal{V}_{i-1}, \nabla_{\mathcal{V}})$ is a trivial bundle with connection (i.e., given by pullback of a bundle with connection on $\operatorname{Spec} L$).

Given an L-scheme S and a base point $b \in X(L)$, we have a morphism $b_S \colon S \to X_S$ and hence fiber functors

$$e_b^n(S) \colon \mathrm{Un}_n(X \times_L S) \to \mathrm{Vect}_S$$

sending each bundle $\mathcal{V}$ in $\mathrm{Un}_n(X \times_L S)$ to the fiber $\mathcal{V}_{b_S}$. Let $\Pi^{\mathrm{dR}}_{X,n}$ be the unipotent algebraic group over L representing the functor given on L-schemes S by

$$S \mapsto \mathrm{Aut}^{\otimes}(e^n_b(S)),$$

the group of tensor-compatible automorphisms of the functor $e^n_b(S)$. Likewise define Π^{dR}_X as the pro-unipotent algebraic group representing the functor $S \mapsto \mathrm{Aut}^{\otimes}(e_b(S))$, where $e_b(S)\colon \mathrm{Un}(X \times_L S) \to \mathrm{Vect}_S$ is the fiber functor at b_S.

Given another point $x \in X(L)$, we have path torsors

$$P^{\mathrm{dR}}_{X,n}(x) = \mathrm{Iso}^{\otimes}(e^n_b, e^n_x).$$

Now suppose $L = F_{\mathfrak{p}}$ is the completion of a number field F at a prime $\mathfrak{p}$ of good reduction for X. As explained in [Kim09, §1], via comparison with the crystalline fundamental group, $\Pi^{\mathrm{dR}}_{X,n}$ can be equipped with a compatible Hodge structure and Frobenius action; we will always consider $\Pi^{\mathrm{dR}}_{X,n}$ with these extra structures.

As in the previous section, let

$$U^{\mathrm{dR}}_{X,n} := \Pi^{\mathrm{dR}}_{X,n}/(\Pi^{\mathrm{dR}}_{X,n})^{(3)}$$

be the metabelianization of $\Pi^{\mathrm{dR}}_{X,n}$.

2.3 Restriction of scalars

Now we come to the main new construction in our paper.

Suppose we are given quasiprojective F-varieties Y and X, a finite Galois extension K/F of degree d, and a K-morphism $f_K\colon Y_K \to X_K$. Then the restriction of scalars $\mathrm{Res}^K_F X_K$ is represented by a quasiprojective variety [BLR90, Thm. 7.6.4]. By the universal property of restriction of scalars, f_K corresponds to an F-morphism $f\colon Y \to R := \operatorname{Res}^K_F X_K$. Unipotent completion is functorial, so f induces a map

$$U_f\colon U_Y \to U_R$$

equivariant for the G_F-actions on U_Y and U_R.

Remark 2.1. Unipotent completion commutes with finite products, so since $R_K \cong X_K^{\times d}$ (the d-fold direct product of X_K with itself), we have a G_K-equivariant (but not necessarily G_F-equivariant) isomorphism $U_R \cong (U_X)^{\times d}$. Similarly, we have a G_K-equivariant isomorphism $U_R^{\mathrm{dR}} \cong (U_X^{\mathrm{dR}})^{\times d}$ that preserves the Hodge structure and Frobenius action.

Let $W \subseteq U_R$ be the image of U_f, i.e., the smallest subgroup scheme of U_R through which the morphism U_f factors. (This is well-defined by [Mil17, Thm. 5.39].) We expect that in many cases, W is the whole of U_R, but we won't need this for our argument.

For each $n \geq 1$, let $W^{[n]} := W \cap U_R^n$ (where U_R^n is the n-th level of the lower central series of U_R, and the intersection is as subgroup schemes of U_R), and

$$W_{[n]} := W/W^{[n+1]}.$$

(We use square brackets to avoid confusion with the lower central series of W itself.) By construction, this induces surjections

$$\pi_n\colon U_{Y,n} \to W_{[n]}$$

of unipotent $\mathbb{Q}_p$-algebraic groups equivariant for the G_F-actions on $U_{Y,n}$ and $W_{[n]}$.

Similarly, for the de Rham realization, f induces a map $U_f^{\mathrm{dR}}\colon U_Y^{\mathrm{dR}} \to U_R^{\mathrm{dR}}$ whose image we denote W^{dR}. For each $n \geq 1$, let $(W^{\mathrm{dR}})^{[n]} := W^{\mathrm{dR}} \cap (U_R^{\mathrm{dR}})^n$ and $W_{[n]}^{\mathrm{dR}} := W^{\mathrm{dR}}/(W^{\mathrm{dR}})^{[n+1]}$, and let $\pi_n^{\mathrm{dR}}\colon U_{Y,n}^{\mathrm{dR}} \to W_{[n]}^{\mathrm{dR}}$ be the induced surjection. These maps are compatible with the Hodge filtration and Frobenius action.

2.4 Functorial properties of fundamental groups

The following lemma about functorially induced morphisms of unipotent fundamental groups will be useful later on.

Lemma 2.2. *Let $L/\mathbb{Q}_p$ be an unramified extension. Let $f\colon Y \to X$ be a morphism of smooth irreducible varieties over L such that, for some dense open $X' \subseteq X$, the restriction $f|_{f^{-1}(X')}\colon f^{-1}(X') \to X'$ is finite étale. Then the induced maps $\Pi_Y \to \Pi_X$ and $\Pi_Y^{\mathrm{dR}} \to \Pi_X^{\mathrm{dR}}$ of $\mathbb{Q}_p$-unipotent étale and de Rham fundamental groups are surjective.*

Proof. We proceed by comparison between the étale fundamental groups over an algebraic closure of L, the $\mathbb{Q}_p$-pro-unipotent fundamental groups, and the de Rham fundamental groups.

Let $y_0 \in Y$ and $x_0 \in X'$ be points such that $f(y_0) = x_0$, and let $\bar{y}_0$ and $\bar{x}_0$ be geometric points over y_0 and x_0, respectively. Let $\bar{Y}, \bar{X}, \bar{X}'$ be the base changes to $\bar{L}$. By functoriality, we have a commutative diagram of étale fundamental groups

$$\begin{array}{ccc} \pi_1^{\text{ét}}(f^{-1}(\bar{X}'), \bar{y}_0) & \xhookrightarrow{f_*} & \pi_1^{\text{ét}}(\bar{X}', \bar{x}_0) \\ \downarrow & & \downarrow \\ \pi_1^{\text{ét}}(\bar{Y}, \bar{y}_0) & \xrightarrow{f_*} & \pi_1^{\text{ét}}(\bar{X}, \bar{x}_0) \end{array}$$

in which the vertical maps are induced by restriction of étale covers to dense open subschemes. An étale cover of a smooth scheme is smooth, hence connected étale covers of smooth schemes are irreducible. Thus, the restriction of a connected cover to an dense open subscheme is connected, which implies surjectivity of the vertical maps by [Stacks, Lemma 0BN6]. By Grothendieck's Galois theory, the image of the top horizontal map has finite index, hence the bottom horizontal map also has finite index.

Taking $\mathbb{Q}_p$-pro-unipotent completions [HM03, Appendix A] gives the morphism of $\mathbb{Q}_p$-unipotent étale fundamental groups $\pi_1^{\mathbb{Q}_p}(f)\colon \Pi_Y \to \Pi_X$, where $\Pi_Y := \pi_1^{\mathbb{Q}_p}(\bar{Y}, \bar{y}_0)$ and $\Pi_X := \pi_1^{\mathbb{Q}_p}(\bar{X}, \bar{x}_0)$. Now we need another lemma.

Lemma 2.3. *Let $\varphi\colon H \to \Gamma$ be a morphism of topological groups whose image has finite index in Γ. Let k be a topological field of characteristic zero. Then continuous k-unipotent completion induces a surjective morphism of k-pro-unipotent groups $\varphi^{\mathrm{un}}\colon H^{\mathrm{un}} \twoheadrightarrow \Gamma^{\mathrm{un}}$.*

Proof. Let $\gamma_1, \ldots, \gamma_n \in \Gamma$ be representatives of the left H-cosets of Γ. By construction, the image of Γ in $\Gamma^{\mathrm{un}}(k)$ is Zariski-dense in Γ^{un}. Since $\Gamma = \bigcup_{i=1}^n \gamma_i \cdot \varphi(H)$, taking Zariski closures, we obtain

$$\Gamma^{\mathrm{un}} = \bigcup_{i=1}^{n} \gamma_i \cdot \overline{\varphi(H)}.$$

Since k has characteristic zero, Γ^{un} is connected, so in fact $\overline{\varphi(H)} = \Gamma^{\mathrm{un}}$. The image of a homomorphism of group schemes is closed, so

$$\Gamma^{\mathrm{un}} = \overline{\varphi(H)} = \overline{\varphi^{\mathrm{un}}(H^{\mathrm{un}})} = \varphi^{\mathrm{un}}(H^{\mathrm{un}}),$$

proving surjectivity of φ^{un}. □

Returning to the proof of Lemma 2.2: The image of f_* has finite index, so Lemma 2.3 implies $\pi_1^{\mathbb{Q}_p}(f)$ is surjective, proving the first claim.

By Olsson's non-abelian p-adic Hodge theory [Ols11, Thm. 1.8], there is a comparison isomorphism

$$\Pi_Y^{\mathrm{dR}} \otimes_L B_{\mathrm{cr}} \cong \Pi_Y \otimes_{\mathbb{Q}_p} B_{\mathrm{cr}},$$

and likewise for X in place of Y. Since B_{cr} is faithfully flat over $\mathbb{Q}_p$ and L, surjectivity of $\Pi_Y \to \Pi_X$ implies surjectivity of the map of de Rham fundamental groups

$$\pi_1^{\mathrm{dR}}(f)\colon \Pi_Y^{\mathrm{dR}} \twoheadrightarrow \Pi_X^{\mathrm{dR}}.$$

This completes the proof of Lemma 2.2. □

This same map $\pi_1^{\mathrm{dR}}(f)$ is also given by taking de Rham fundamental groups of the pullback functor $f^*\colon \mathrm{Un}(X) \to \mathrm{Un}(Y)$ of categories of unipotent vector bundles with integrable connection.

2.5 Selmer varieties and unipotent Albanese maps

Here, we describe the étale and de Rham realizations of the Selmer varieties, summarizing the relevant parts of [Kim09]. We also describe the unipotent Albanese maps that act as replacements for the Abel–Jacobi map.

For the remainder of the paper, Y and X are smooth projective curves of genus $g \geq 2$ defined over $\mathbb{Q}$, and there is a dominant map $f_K\colon Y_K \to X_K$ defined over K. Let g be the genus of X, and fix a rational prime p that splits completely in K and is of good reduction for Y and X. Let $V_p := T_p J_X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ be the $\mathbb{Q}_p$-Tate module of J_X. Let S be a set of rational primes such that X and Y both have good reduction away from S, and let $T = S \cup \{p\}$. Denote the absolute Galois group of any number field L by G_L; let G_T be the Galois group $\mathrm{Gal}(\mathbb{Q}_T/\mathbb{Q})$, where $\mathbb{Q}_T$ is the maximal subfield of $\bar{\mathbb{Q}}$ unramified outside T; and fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, which determines an injection $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow G_{\mathbb{Q}}$.

The étale realization $H^1_f(G_T, U_{Y,n})$ is the moduli space of G-torsors for $U_{Y,n}$ that are unramified away from T and crystalline at p, and likewise for $H^1_f(G_p, U_{Y,n})$ with G_p-torsors replacing G-torsors.

The de Rham realization $U^{\mathrm{dR}}_{Y,n}/F^0U^{\mathrm{dR}}_{Y,n}$ is the moduli space of torsors for $U^{\mathrm{dR}}_{Y,n}$ with Frobenius structure and Hodge filtration that are *admissible*, i.e., separately trivializable for the Frobenius structure and the Hodge filtration [Kim09, Prop. 1].

For each $n \geq 1$, let $j_n^{\text{ét,glob}}, j_n^{\text{ét,loc}}, j_n^{\text{dR}}$ be the unipotent Albanese maps defined in [Kim09] as follows: Fix a base point $b \in Y(\mathbb{Q})$. Then $j_n^{\text{ét,glob}}$ (resp. $j_n^{\text{ét,loc}}$) sends each $y \in Y(\mathbb{Q})$ (resp. $y \in Y(\mathbb{Q}_p)$) to the class of the path torsor $[P_Y^{\text{ét}}(y)]$ in $H^1_f(G_T, U_{Y,n})$ (resp. $H^1_f(G_p, U_{Y,n})$). Likewise, j_n^{dR} sends each $y \in Y(\mathbb{Q}_p)$ to the class of the path torsor $[P_{Y,n}^{\text{dR}}(y)]$ in $U_{Y,n}^{\text{dR}}/F^0U_{Y,n}^{\text{dR}}$.

We have the following commutative diagram:

$$\begin{array}{ccccc}
Y(\mathbb{Q}) & \hookrightarrow & Y(\mathbb{Q}_p) & & \\
\downarrow{\scriptstyle j_n^{\text{ét,glob}}} & & \downarrow{\scriptstyle j_n^{\text{ét,loc}}} & \searrow{\scriptstyle j_n^{\text{dR}}} & \\
H^1_f(G_T, U_{Y,n}) & \xrightarrow{\text{loc}_p} & H^1_f(G_p, U_{Y,n}) & \xrightarrow{D} & U_{Y,n}^{\text{dR}}/F^0U_{Y,n}^{\text{dR}} \\
\downarrow{\scriptstyle \pi_n^{\text{ét,glob}}} & & \downarrow{\scriptstyle \pi_n^{\text{ét,loc}}} & & \downarrow{\scriptstyle \pi_n^{\text{dR}}} \\
H^1_f(G_T, W_{[n]}) & \xrightarrow{\text{loc}_{p,W}} & H^1_f(G_p, W_{[n]}) & \xrightarrow{D} & W_{[n]}^{\text{dR}}/F^0W_{[n]}^{\text{dR}}
\end{array}$$

Here, the vertical maps $\pi_n^{\text{ét,glob}}$, $\pi_n^{\text{ét,loc}}$, and π_n^{dR} are functorially induced by π_n. As proved in [Kim09], if the image of the algebraic map $\log_{p,W} := D \circ \text{loc}_{p,W}$ — and hence the image of $\log_p := D \circ \text{loc}_p$ — is not Zariski-dense, then $Y(\mathbb{Q})$ is finite.

Chapter 3

Rational points on solvable curves

3.1 Bounds for local and global Selmer varieties

With the basic setup now in place, we turn to our main goal, which is to show that the image of the global Selmer variety in the de Rham local Selmer variety is not Zariski dense. This has two parts: giving an upper bound for the dimension of the global Selmer variety (filling the role played by the Mordell–Weil group in classical Chabauty) and giving a lower bound for the dimension of the de Rham local Selmer variety (filling the role classically played by the genus.)

We begin with a few remarks about the structure of W. As mentioned in Remark 2.1, there is a G_K-equivariant isomorphism of $\mathbb{Q}_p$-algebraic groups

$$U_{R,n} \cong U_{X,n}^{\times d}.$$

Composing the map $W_{[n]} \hookrightarrow U_{R,n}$ with projection onto the first coordinate $U_{X,n}$ under the above isomorphism yields a G_K-equivariant map

$$W_{[n]} \to U_{X,n}$$

which is functorially induced by $f_K \colon Y_K \to X_K$, hence is surjective by Lemma 2.2. Counting dimension, we obtain

$$\dim U_{X,n} \leq \dim W_{[n]} \leq \dim U_{R,n} = d \cdot \dim U_{X,n}.$$

We can also take graded pieces: define $Z_{[n]} := W^{[n]}/W^{[n+1]}$, which fits into an exact sequence

$$0 \to Z_{[n]} \to W_{[n]} \to W_{[n-1]} \to 0$$

of $\mathbb{Q}_p[G_{\mathbb{Q}}]$-modules. Similarly, write $Z_n(U_R)$, $Z_n(U_Y)$, and $Z_n(U_X)$ for the n-th graded pieces (with respect to the lower central series) of the other algebraic groups. By construction of $W_{[n]}$, we obtain as above a $G_{\mathbb{Q}}$-equivariant injection

$$Z_{[n]} \hookrightarrow Z_n(U_R)$$

and a G_K-equivariant surjection

$$Z_{[n]} \twoheadrightarrow Z_n(U_X).$$

3.1.1 Lower bounds for the de Rham local Selmer variety

In order to obtain lower bounds for the dimension of $W^{\mathrm{dR}}_{[n]}/F^0W^{\mathrm{dR}}_{[n]}$, we will need upper bounds for the dimension of the filtered piece $F^0W^{\mathrm{dR}}_{[n]}$.

Lemma 3.1. *There is a constant A (depending only on X, T, and d) such that, for all $n \geq 1$,*

$$\dim F^0W^{\mathrm{dR}}_{[n]} \leq An^g.$$

Proof. The G_K-equivariant inclusion

$$W^{\mathrm{dR}}_{[n]} \hookrightarrow (U^{\mathrm{dR}}_{X,n})^{\times d}$$

is compatible with the Hodge structures, hence induces an inclusion of Hodge filtered pieces

$$F^0W^{\mathrm{dR}}_{[n]} \hookrightarrow F^0(U^{\mathrm{dR}}_{X,n})^{\times d} = (F^0U^{\mathrm{dR}}_{X,n})^{\times d}.$$

By the proof of [CK10, Thm. 2], there is a constant A' such that $\dim F^0 U^{\mathrm{dR}}_{X,n} \leq A' n^g$ for all $n \geq 1$. Thus,

$$\dim F^0 W^{\mathrm{dR}}_{[n]} \leq d \cdot \dim F^0 U^{\mathrm{dR}}_{X,n} \leq dA' n^g. \qquad \square$$

3.1.2 Upper bounds for the global Selmer variety

In this section, we show that the dimension of the global cohomology space $H^1(G_T, W_{[n]})$ can be bounded by the dimension of "abelianizations" coming from the graded pieces $Z_{[n]}$, which can in turn be studied using the Euler characteristic formula.

Lemma 3.2. *For all* $n \geq 1$, $H^0(G_T, Z_{[n]}) = 0$.

Proof. The injection $Z_{[n]} \hookrightarrow Z_n(U_R)$ induces an injection

$$H^0(G_T, Z_{[n]}) \hookrightarrow H^0(G_T, Z_n(U_R)).$$

Since $Z_n(U_R)$ is a quotient of $U_{R,1}^{\otimes n} = H_1(R, \mathbb{Q}_p)^{\otimes n}$, $Z_n(U_R)$ has Frobenius weight n, so $H^0(G_T, Z_n(U_R)) = 0$. $\square$

Lemma 3.3. *For all* $n \geq 1$,

$$\dim H^1(G_T, W_{[n]}) \leq \sum_{i=1}^{n} \dim H^1(G_T, Z_{[i]}).$$

Proof. By Lemma 3.2, $H^0(G_T, W_{[n]}) \subseteq H^0(G_T, W_{[n-1]})$ for each $n \geq 2$, so

$$H^0(G_T, W_{[n]}) \subseteq H^0(G_T, W_{[1]}) = H^0(G_T, Z_{[1]}) = 0.$$

By the claim in the proof of [Kim05, Prop. 2] (noting that the proof works without modification for the filtration $W^{[n]}$, not just for the lower central series), the exact sequence

$$0 \to Z_{[n]} \to W_{[n]} \to W_{[n-1]} \to 0$$

induces an exact sequence

$$0 = H^0(G_T, W_{[n-1]}) \to H^1(G_T, Z_{[n]}) \to H^1(G_T, W_{[n]}) \\ \to H^1(G_T, W_{[n-1]}) \xrightarrow{\delta} H^2(G_T, Z_{[n]}),$$

by which we mean that $H^1(G_T, W_{[n]})$ is a $H^1(G_T, Z_{[n]})$-torsor over the subvariety of $H^1(G_T, W_{[n-1]})$ given by the kernel of the boundary map δ. Thus,

$$\dim H^1(G_T, W_{[n]}) \leq \dim H^1(G_T, W_{[n-1]}) + \dim H^1(G_T, Z_{[n]}),$$

and the result follows by induction. □

Using Lemma 3.2, the Euler characteristic formula [Mil06, Thm. I.5.1] implies that for each $n \geq 1$,

$$\dim H^1(G_T, Z_{[n]}) = \dim H^2(G_T, Z_{[n]}) + \dim Z_{[n]} - \dim Z^+_{[n]},$$

where $Z^+_{[n]}$ denotes the positive eigenspace of the action of complex conjugation on $Z_{[n]}$. So to bound $H^1(G_T, Z_{[n]})$, we can work instead with $H^2(G_T, Z_{[n]})$ and $Z^+_{[n]}$.

We now turn to the problem of bounding the dimension of $H^2(G_T, Z_{[n]})$.

Lemma 3.4. *Suppose there is a number field L/K and a constant B (depending only on X and T) such that, for all $n \neq 1$,*

$$\sum_{i=1}^{n} \dim H^2(G_{L,T}, Z_i(U_X)) \leq Bn^{2g-1}.$$

Then for all $n \geq 1$,

$$\sum_{i=1}^{n} \dim H^2(G_T, Z_{[i]}) \leq dBn^{2g-1},$$

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

Proof. Since $G_{L,T} \leq G_T$ is a subgroup of some finite index m, we have a corestriction map

$$H^2(G_{L,T}, Z_{[i]}) \to H^2(G_T, Z_{[i]})$$

for each i. Precomposing corestriction with restriction yields multiplication by m. Since $Z_{[i]}$ is a divisible abelian group, multiplication by m is an automorphism, so the above corestriction map is surjective, and it suffices to bound $\dim H^2(G_{L,T}, Z_{[i]})$.

By the semisimplicity theorem of Faltings and Tate, the $\mathbb{Q}_p$-Tate module $Z_1(U_X) = V_p = T_p J_X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a semisimple G_L-representation. Hence, $(V_p^{\otimes i})^{\oplus d}$ is semisimple. As in [CK10], we have a surjection $V_p^{\otimes i} \twoheadrightarrow Z_i(U_X)$ which splits, realizing $Z_i(U_X)$ as a direct summand of $V_p^{\otimes i}$.

We also have an inclusion of $\mathbb{Q}_p[G_{L,T}]$-modules

$$Z_{[i]} \hookrightarrow Z_i(U_X)^{\oplus d}.$$

But $Z_i(U_X)^{\oplus d}$ is semisimple, so $Z_{[i]}$ is in fact a direct summand. Since cohomology preserves direct summands, it follows that

$$\dim H^2(G_{L,T}, Z_{[i]}) \leq d \cdot \dim H^2(G_{L,T}, Z_i(U_X)).$$

Summing the above over all $1 \leq i \leq n$, we are done. □

Remark 3.5. Suppose the Jacobian J_X of X is isogenous over $\bar{\mathbb{Q}}$ to a product of CM abelian varieties. Then there is a number field L/K such that:

- The complex multiplication and decomposition of J_X are defined over L;
- $K(J_X[p]) \subseteq L$; and

- the image Γ of the associated Galois representation

$$\rho_L : \mathrm{Gal}(\bar{L}/L) \to \mathrm{GL}(V_p)$$

is isomorphic to $\mathbb{Z}_p^r$ for some integer r.

By [CK10, Thm. 1], there is a constant B (depending on X and T) such that

$$\sum_{i=1}^{n} \dim H^2(G_{L,T}, Z_i(U_X)) \leq Bn^{2g-1},$$

so the conclusion of Lemma 3.4 holds. In this case, V_p is isomorphic as a G_L-representation to a direct sum of characters, so we also do not need to appeal to the semisimplicity theorem in the proof of Lemma 3.4. (In particular, the results of §3.5 do not rely on the semisimplicity theorem.)

3.2 Bounding the invariants of complex conjugation

We need a lower bound on the dimension $Z_{[i]}^+$, the subgroup of $Z_{[i]}$ on which complex conjugation acts as the identity. We begin with a combinatorial lemma.

Lemma 3.6. *Let k be a field not of characteristic 2. Let V be a k-vector space of finite dimension m. Let $c\colon V \to V$ be a linear involution which is not multiplication by ± 1. Then*

$$\lim_{n\to\infty} \frac{\dim \mathrm{Sym}^n(V)^+}{\dim \mathrm{Sym}^n(V)} = \frac{1}{2}.$$

Proof. Define $a_n = \dim \mathrm{Sym}^n(V)^+ - \dim \mathrm{Sym}^n(V)^-$. Since $\dim \mathrm{Sym}^n(V) = \binom{n+m-1}{m-1}$, which is a polynomial in n of degree $m-1$, it suffices to show that to show that $a_n = O(n^{m-2})$. Write m^+, m^- for the dimension of the $+1$ and -1 eigenspaces of c on V.

Then we have a generating function identity

$$\sum_{n=0}^{\infty} a_n t^n = (1-t)^{-m^+}(1+t)^{-m^-} = \sum_{i=1}^{m^+} \frac{A_i}{(1-t)^i} + \sum_{i=1}^{m^-} \frac{B_i}{(1+t)^i},$$

where $A_i, B_i \in \mathbb{Q}$ are given by partial fraction decomposition. The power series coefficients of $(1 \pm t)^{-i}$ are of order $O(n^{i-1})$, so $a_n = O(n^{\max\{m^+,m^-\}-1})$. Since $\max\{m^+, m^-\} < m$, we have $a_n = O(n^{m-2})$, completing the proof. □

Remark 3.7. Lemma 3.6 is equivalent to the following combinatorial statement: Suppose we have $a \geq 1$ labelled bins colored blue, $b \geq 1$ labelled bins colored green, and n indistinguishable balls. Then for $n \gg 0$, out of all the ways to place the n balls into the $a + b$ bins, approximately half result in the total number of balls in *green* bins being even.

Coates and Kim [CK10, proof of Cor. 0.2, pp. 847–848] prove the special case of Lemma 3.6 where $a = b$, in which case there are additional symmetries that simplify the problem.

Lemma 3.8. *There is a constant $C > 0$ (depending only on X and T) such that, for all $n \geq 1$,*

$$\sum_{i=1}^{n} \dim Z^+_{[i]} \geq Cn^{2g}.$$

Proof. Let $c \in G_{\mathbb{Q}}$ be a complex conjugation. We may choose a $\mathbb{Q}_p$-basis $\bar{f}_1, \ldots, \bar{f}_{2g(Y)}$ of $Z_1(U_Y)$ (in other words, of the $\mathbb{Q}_p$-Tate module of Y) such that $c(\bar{f}_i) = \pm \bar{f}_i$ for each $i = 1, \ldots, 2g(Y)$. Let $\tilde{f}_i$ be lifts of $\bar{f}_i$ to U_Y. Recall the $G_{\mathbb{Q}}$-equivariant map

$$U_f : U_Y \to W.$$

Let $f_i := U_f(\tilde{f}_i)$.

We also have a surjective homomorphism $W \twoheadrightarrow U_X$. Recall that the Galois action on W was defined to be the one inherited from the Galois action on U_Y; since the map

$Y \to X$ is defined only over K, the map $U_Y \to U_X$, whence the map $W \to U_X$, is equivariant only for the Galois group G_K, not the whole of $G_{\mathbb{Q}}$. In particular, if K is not totally real, the map from W to U_X is not equivariant for complex conjugation. We will see that this doesn't matter; using the purely combinatorial Lemma 3.6, we can lower-bound the conjugation-invariant part of $Z_{[i]}$ using only the group structure of W, no matter what the action of c is, as we now explain.

After reordering $f_1, \ldots, f_{2g(Y)}$ if necessary, we may assume that $f_1, \ldots, f_{2g}$ project to a basis $a_1, \ldots, a_{2g}$ of $Z_1(U_X)$. The projection of f_i to $Z_1(W)$ is an eigenvector for c; again reordering if necessary, we may assume the eigenvalue is $+1$ for $i = 1, \ldots, s$ and -1 for $i = s+1, \ldots, 2g$.

Let $L \subseteq \mathrm{Lie}(W)$ be the Lie subalgebra generated by $f_1, \ldots, f_{2g}$, and let L^n denote the n-th level of the lower central series of L. Let $L_{[n]}$ be the subspace of $Z_{[n]}$ generated by L^n. The homomorphism $W \twoheadrightarrow U_X$ induces a homomorphism $L_{[n]} \twoheadrightarrow Z_n(U_X)$. By [CK10, proof of Cor. 0.2, p. 847], a basis for $Z_n(U_X)$ when $n \geq 2$ is given by elements of the form

$$[\ldots[a_{i_1}, a_{i_2}], a_{i_3}], \ldots], a_{i_n}]$$

with $i_1 < i_2$ and $i_2 \geq i_3 \geq \ldots \geq i_n$. In particular, this means the elements

$$[\ldots[f_{i_1}, f_{i_2}], f_{i_3}], \ldots], f_{i_n}]$$

are linearly independent in $L_{[n]}$. Note that c acts on such an element by ± 1; more precisely, it acts as $(-1)^k$ where k is the number of the $i_1, \ldots, i_n$ which are greater than s. Write $V_n < L_{[n]}$ for the space spanned by the elements above.

We now consider three cases.

If $s = 2g$, then c acts as 1 on V_n. So $\dim V_n^+ = \dim L_{[n]}$, which is bounded below by Cn^{2g-1} for all n. This proves the lemma in this case.

If $s = 0$, then c acts as -1 on V_n. So $\dim V_n^+ = \dim L_{[n]}$ for all even n, and the lemma follows again.

Now suppose $0 < s < 2g$. Consider the space $V_{1,n} < V_n$ spanned by

$$[\dots[f_1, f_{i_2}], f_{i_3}], \dots], f_{i_n}].$$

This basis for $V_{1,n}$ is naturally in bijection with the set of monomials $x_{i_2} \dots x_{i_n}$ of degree $n-1$ in the variables $x_1, x_2, \dots, x_{2g}$; thus $\dim V_{1,n}$ is on order n^{2g-1} as n grows. A basis for $V_{1,n}^+$ is given by those monomials whose total degree in $x_1, \dots, x_s$ is even. Lemma 3.6 tells us precisely that

$$\dim V_{1,n}^+ = (1/2) \dim V_{1,n} + o(\dim V_{1,n}) \geq C n^{2g-1}$$

Once again, the lemma follows. □

3.3 Proof of Theorem 1.5

Our goal is to prove that, for n sufficiently large,

$$\dim H^1_f(G_T, W_{[n]}) < \dim W_{[n]}^{\mathrm{dR}} / F^0 W_{[n]}^{\mathrm{dR}}.$$

Recall that $H^1_f(G_T, W_{[n]})$ is a subvariety of $H^1(G_T, W_{[n]})$; it thus suffices to bound the dimension of the latter variety, which by Lemma 3.3 and the Euler characteristic formula is bounded above as follows:

$$\begin{aligned}\dim H^1(G_T, W_{[n]}) &\leq \sum_{i=1}^{n} \left(\dim Z_{[i]} + \dim H^2(G_T, Z_{[i]}) - \dim Z_{[i]}^+\right) \\ &= \dim W_{[n]} + \sum_{i=1}^{n} \dim H^2(G_T, Z_{[i]}) - \sum_{i=1}^{n} \dim Z_{[i]}^+.\end{aligned}$$

By Lemma 3.4, the contribution of $\sum_{i=1}^{n} \dim H^2(G_T, Z_{[i]})$ is $O(n^{2g-1})$. By Lemma 3.8, we know $\sum_{i=1}^{n} \dim Z_{[i]}^{+}$ is bounded below by a multiple of n^{2g}. Putting these facts together, we have

$$\dim H^1(G_T, W_{[n]}) \leq \dim W_{[n]} - Cn^{2g}$$

for some $C > 0$.

On the other hand, by Lemma 3.1, we have

$$\dim F^0 W_{[n]}^{\mathrm{dR}} = O(n^g)$$

Thus, for n large enough, we have

$$\dim H_f^1(G_T, W_{[n]}) \leq \dim H^1(G_T, W_{[n]}) < \dim W_{[n]} - \dim F^0 W_{[n]}^{\mathrm{dR}} = \dim W_{[n]}^{\mathrm{dR}} / F^0 W_{[n]}^{\mathrm{dR}}$$

which is the desired result.

Remark 3.9. The difficulty in applying the same technique over a number field F other than $\mathbb{Q}$ is that

$$\dim Z_{[n]} - \dim Z_{[n]}^{+}$$

in the Euler characteristic formula is replaced with

$$\sum_{v \text{ real}} (\dim Z_{[n]} - \dim Z_{[n]}^{+,v}) + \sum_{v \text{ complex}} \dim Z_{[n]},$$

where the sums are over the real and complex places of F, and $Z_{[n]}^{+,v}$ is the 1-eigenspace of the complex conjugation associated to a real place v. For our argument to go through, this sum needs to be strictly smaller than $\dim Z_{[n]}$. Obviously this is impossible if F has a complex place, and even if F is totally real, the summands corresponding to real places should have size about $(1/2) \dim Z_{[n]}$ for large n, which blocks the method from working when F is larger than $\mathbb{Q}$. It would be interesting to see if there were any hope of making the method work in the “boundary case” where F is a real quadratic extension of $\mathbb{Q}$.

This is not merely an artefact of the “abelianization” that replaces W with its graded pieces; the long exact sequence in the proof of Lemma 3.3 shows that this abelianization can add at most $\sum_{i=1}^{n} \dim H^2(G_{F,T}, Z_{[n]})$ to the dimension, so $\dim H^1(G_{F,T}, W_{[n]})$ is still too large.

In chapter 4, we discuss an approach to overcoming this obstacle: By choosing p to be inert (rather than completely split) in $F/\mathbb{Q}$, the leading term in the dimension count is enlarged by exactly the factor $[F : \mathbb{Q}]$ needed for the argument to go through with only minor modifications, provided F has a real embedding. This comes at a cost: the dimension of $C(F_p)$ as a $\mathbb{Q}_p$-analytic space becomes $[F : \mathbb{Q}]$ instead of 1, so the dimension hypothesis no longer automatically implies finiteness. In chapter 5, we motivate and pose a conjecture that refines [Kim09, Thm. 1] and implies finiteness in this more general setting.

3.4 Unramified correspondences

One of the main tools used in [EH18] to prove finiteness of $\mathbb{Q}$-points of solvable curves is the notion of *unramified correspondences*, due to Bogomolov and Tschinkel [BT02]. In this chapter, we give an overview of the main results and conjectures on unramified correspondences and relate it to finiteness questions for points on hyperbolic curves.

Definition 3.10. Let V and W be irreducible algebraic varieties over a field k. An *unramified correspondence* from V to W is a triple (Z, f, g), where Z is an irreducible algebraic variety, $f\colon Z \to V$ is an étale k-morphism, and $g\colon Z \to W$ is a dominant

k-morphism.

We write $V \Rightarrow W$ if there exists an unramified correspondence from $V_{\bar{k}}$ to $W_{\bar{k}}$.

Conjecture 3.11 ([BT07, Conj. 3.1]). *Let C and C' be smooth projective curves of genus at least 2 over $\bar{\mathbb{Q}}$. Then $C \Rightarrow C'$.*

In other words, the fundamental group of a hyperbolic curve is so big that the set of the curve's étale covers dominates any other curve.

This conjecture is very far from being proven, but some special cases are known.

Definition 3.12. Let C_n be the hyperelliptic curve with affine model $y^2 = x^n - 1$.

Note that $C_{mn} \Rightarrow C_m$ for all m, n. One can deduce [BT02] from Belyi's theorem [Bel79] that for every curve $C'/\bar{\mathbb{Q}}$, there exists n such that $C_n \Rightarrow C'$.

Theorem 3.13 ([BT04, Prop. 2.4]). *Let H be a hyperelliptic curve over $\bar{\mathbb{Q}}$. Then $H \Rightarrow C_6$ and $H \Rightarrow C_8$.*

Theorem 3.14 ([BT04, Thm. 1.2]). *Let $k = \bar{\mathbb{Q}}$, $m \geq 6$, and $n \in \{2, 3, 5\}$. Then $C_m \Rightarrow C_{mn}$.*

Theorem 3.15 ([Poo05, Thm. 1.7]). *Let C be a curve of genus $g(C) \geq 2$ over an algebraically closed field of characteristic zero. Let G be a subgroup of $\mathrm{Aut}(C)$. Let $D = C/G$, and assume D is of genus $g(D) \leq 2$. Suppose also that at least one of the following holds:*

(1) $g(D) \in \{1, 2\}$.

(2) G is solvable.

(3) There are two distinct points of D above which the ramification indices are not coprime.

(4) There are three points of C above which the ramification indices are divisible by $2, 3, \ell$, respectively, where ℓ is a prime with either $\ell \leq 89$ or

$$\ell \in \{101, 103, 107, 131, 167, 191\}.$$

Then there exists a hyperbolic hyperelliptic curve H such that $C \Rightarrow H$.

Corollary 3.16 ([Poo05, Cor. 1.8])**.** *Let C satisfy the hypotheses of Theorem 3.15. (In particular, C could be any projective hyperbolic curve over $\bar{\mathbb{Q}}$ such that there exists a Galois morphism $C \to \mathbf{P}^1$ with solvable Galois group.) Then there exists a hyperelliptic hyperbolic curve H such that $C \Rightarrow H$.*

Remark 3.17. Since the relation $\Rightarrow$ is transitive, to prove Conjecture 3.11, it would suffice to do the following:

(1) Generalize Theorem 3.14 to allow n to be any prime (instead of just 2, 3, or 5); and

(2) Generalize Theorem 3.15 to allow C to be any projective hyperbolic curve.

3.5 Application to superelliptic curves

We now combine Theorem 1.5 with results of Poonen [Poo05] and Bogomolov and Tschinkel [BT02] to prove finiteness of $C(\mathbb{Q})$ whenever C is a smooth proper curve over $\mathbb{Q}$ of genus at least 2 such that there exists a map $C \to \mathbf{P}^1$ with solvable automorphism group (e.g., when C is superelliptic).

Theorem 3.18. *Let C be a smooth proper curve over $\mathbb{Q}$ such that $C \Rightarrow X$ for some curve X over $\mathbb{Q}$ such that the Jacobian of X has potential CM. Then $C(\mathbb{Q})$ is finite.*

Proof. Since $C \Rightarrow X$, there exists an étale cover $\pi\colon Y \to C$ and a dominant morphism $f\colon Y \to X$ defined over $\bar{\mathbb{Q}}$, and hence over some Galois extension $L/\mathbb{Q}$ of finite degree m. Let $Y_1, \ldots, Y_m$ be the Galois conjugates of Y, and let Z be a connected component of the $\mathbb{Q}$-scheme $\mathrm{Gal}(L/\mathbb{Q})\backslash(Y_1 \sqcup \cdots \sqcup Y_m)$. Then Z is a connected (but not necessarily geometrically connected) finite étale cover of C defined over $\mathbb{Q}$. Let $\tilde{Z} \to Z \to C$ be the Galois closure of the connected étale cover $Z \to C$.

By the Chevalley–Weil theorem [Ser89, §4.2] there is a finite set of twists $\tilde{Z}^\tau/\mathbb{Q}$, each with a $\mathbb{Q}$-rational map π^τ to C, such that $C(\mathbb{Q})$ is covered by $\pi^\tau(\tilde{Z}^\tau(\mathbb{Q}))$. (See e.g. [Vol12, p. 2].) Let $\{W_1, \ldots, W_\nu\}$ be the set of all connected components of the twists $\tilde{Z}^\tau$ such that $W_i(\mathbb{Q})$ is nonempty. By [Stacks, Tag 04KV], each W_i is geometrically connected.

Each W_i is a smooth, proper, geometrically connected curve over $\mathbb{Q}$ with a dominant $\bar{\mathbb{Q}}$-morphism to X. Because X has potential CM, the theorem of Coates–Kim [CK10, Thm. 0.1]) implies that the hypotheses of Theorem 1.5 hold for each W_i. Hence, W_i is finite for all i, so $C(\mathbb{Q}) \subseteq \bigcup_{i=1}^{\nu} \pi^\tau(W_i(\mathbb{Q}))$ is also finite. □

As in the previous section, let C_6 be the smooth projective model of the curve with affine equation $y^2 = x^6 - 1$.

Corollary 3.19. *Let C be a smooth projective curve over $\mathbb{Q}$ of genus at least 2. Suppose $C_{\bar{\mathbb{Q}}}$ satisfies the hypotheses of Theorem 3.15. Then $C(\mathbb{Q})$ is finite. In particular, if C is a smooth superelliptic curve $y^d = f(x)$ of genus at least two, $C(\mathbb{Q})$ is finite.*

Proof. Immediate from Theorem 3.18, Corollary 3.16, and the fact that the Jacobian of C_6 is isogenous to the product of elliptic curves $y^2 = x^3 - 1$ and $y^2 = x^3 + 1$, which both have CM by the ring of integers of $\mathbb{Q}(\sqrt{-3})$. □

Remark 3.20. In [BT07, Conj. 3.1], Bogomolov and Tschinkel conjecture that $C \Rightarrow C'$ for *any* smooth projective curves C and C' over $\bar{\mathbb{Q}}$ of genus at least 2. If this conjecture is true, our method applies to show finiteness of $C(\mathbb{Q})$ for every such curve C over $\mathbb{Q}$.

Chapter 4

Generalization to real number fields

In much of the existing literature on the Chabauty–Kim method — including [Kim09], [CK10], and [EH18] — the so-called “dimension hypothesis” that is central to the theory is only proved for curves defined over $\mathbb{Q}$, and the conclusions are about $\mathbb{Q}$-points of the curves. This assumption on the base field is because of substantive difficulties in generalizing to arbitrary number fields, not merely out of convenience.

In this chapter, we show that for any number field F with a real embedding $F \hookrightarrow \mathbb{R}$, assuming the prime p is inert in $F/\mathbb{Q}$, the difficulty is only in controlling the simultaneous vanishing of multiple p-adic analytic functions on the curve, and not in producing such functions that vanish on the set of F-points. In particular, we prove that the dimension hypothesis over F holds for sufficiently large n in three major cases where it has already been proved over $\mathbb{Q}$: for arbitrary curves conditional on one of several conjectures [Kim09], for curves with CM Jacobian [CK10], and for curves geometrically dominating a curve with CM Jacobian [EH18].

We conclude in each of these cases that finiteness of F-points on the curve follows from a certain transcendence conjecture on the unipotent Albanese map that gives exactly the required control over the simultaneous vanishing of the p-adic analytic functions produced by this method. We motivate and give a precise formulation of this conjecture in chapter 5. In summary, we prove the following:

Theorem 4.1. *Assume Conjecture 5.1. Let F be a number field with a real embedding $F \hookrightarrow \mathbb{R}$. Let C be a smooth projective curve over F of genus $g \geq 2$. Let p be a rational prime that is inert in $F/\mathbb{Q}$ and is of good reduction for C. Suppose one of the following is true:*

(1) Conjecture 2 of [Kim09] is true for C. (By [Kim09, §3], this follows from either the Fontaine–Mazur or Bloch–Kato conjectures.)

(2) There is a smooth projective curve X/F of genus ≥ 2 such that the Jacobian of X has CM and there exists a dominant morphism $C \to X$ defined over $\bar{\mathbb{Q}}$.

Then for all sufficiently large n, the intersection

$$C(F_p) \cap H^1_f(G_T, U_n)$$

inside $H^1_f(G_p, U_n)$ is a finite set. (Note that $C(F)$ is a subset of the above set.)

The non-abelian Chabauty method over a number field F requires an inequality of dimensions

$$\dim H^1_f(G_T, U_n) < \dim \mathrm{Res}^{F_v}_{\mathbb{Q}_p}(U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}}),$$

of $\mathbb{Q}_p$-varieties called *Selmer varieties*. (Here, v is a prime of F above p; we will define the rest of the notation shortly.) An Euler characteristic argument on graded pieces Z_n of the unipotent group U reduces the problem to an inequality

$$[F : \mathbb{Q}] \dim Z_n - \sum_{\iota\colon F \hookrightarrow \mathbb{R}} \dim Z_n^{\iota,+} + \dim H^2(G_T, Z_n) < [F_v : \mathbb{Q}_p] \dim Z_n - [F_v : \mathbb{Q}_p] \dim F^0 Z_n^{\mathrm{dR}},$$

which has been proved when $F = \mathbb{Q}$ in each of the aforementioned cases. Note that $[F_v : \mathbb{Q}_p] \leq [F : \mathbb{Q}]$, with equality if and only if p is inert in $F/\mathbb{Q}$. The highest order term on each side comes from $\dim Z_n$, so the above inequality will fail for sufficiently large n unless p is inert.

Now suppose p is inert in $F/\mathbb{Q}$. Then the inequality reduces to

$$\dim H^2(G_T, Z_n) + [F : \mathbb{Q}] \dim F^0 Z_n^{\mathrm{dR}} < \sum_{\iota\colon F \hookrightarrow \mathbb{R}} \dim Z_n^{\iota,+},$$

which is clearly only possible if there exists a real embedding $\iota\colon F \hookrightarrow \mathbb{R}$. (Over a totally imaginary number field, non-Zariski-density of the image of the localization map—if it is true at all—must follow from something other than this dimension-counting argument.) This observation motivates the remainder of the paper, where we show that, under these circumstances, the arguments of [Kim09], [CK10], and [EH18] for the most part still carry through for higher genus curves over F; we provide the necessary modifications for the arguments that need to be changed.

Let F be a number field with an embedding $\iota\colon F \hookrightarrow \mathbb{R}$. Let C be a smooth projective curve over F of genus $g \geq 2$. Let p be a rational prime which is inert in F and such that C has good reduction at p. Our goal is to apply the Chabauty–Kim method to C at the prime p for the same classes of curves for which this method can be applied when $F = \mathbb{Q}$.

We first recall the setup of [Kim09]: Let S be a finite set of primes of F containing all archimedean primes and all primes of bad reduction for C, and let $T = S \cup \{p\}$. Let F_T be the maximal subfield of $\bar{F}$ unramified outside T. Let $G_T = \mathrm{Gal}(F_T/F)$. Let $G_p = \mathrm{Gal}(\bar{F}_p/F_p)$, and choose an embedding $F_T \hookrightarrow \bar{F}_p$, inducing an inclusion $G_p \hookrightarrow G_T$.

Let $b \in C(F)$ be an F-rational point, and let $\bar{b}$ be a geometric point lying over b. Let $\bar{C} := C \times_{\operatorname{Spec} F} \operatorname{Spec} \bar{F}$. Let Π be the $\mathbb{Q}_p$-pro-unipotent completion of the étale fundamental group $\pi_1^{\text{ét}}(\bar{C}, \bar{b})$. (Equivalently, Π is the fundamental group of the Tannakian category of unipotent smooth $\mathbb{Q}_p$-sheaves on $\bar{C}$ with fiber functor given by the fiber at *b.*) Note that G_T and G_p act on Π.

Given a $\mathbb{Q}_p$-pro-unipotent group U with an action of a profinite group G, define the functor $H^1(G, U)$ for each $\mathbb{Q}_p$-algebra R by

$$H^1(G,U)\colon \mathbb{Q}_p\text{-}\mathbf{Alg} \to \mathbf{Set}_*,$$
$$R \mapsto H^1(G, U(R)).$$

Also let $H^1_f(G, U)$ be the subfunctor of crystalline torsors, i.e., those that trivialize after base change to $U \otimes_{\mathbb{Q}_p} B_{cr}$.

For each $n \geq 1$, let U^n be the n-th level of the lower central series of U (so $U^1 = U$ and $U^{n+1} = [U, U^n]$), and let $U_n := U/U^{n+1}$.

By [Kim09] and [CK10], for each $n \geq 1$, we have that $H^1_f(G, \Psi)$ is representable by an algebraic variety, where G is either G_T or G_p, and Ψ is either Π_n or the metabelianization $U_n = \Pi_n/\Pi_n^{(3)}$ (where the superscript denotes the derived series).

Just as in [Kim09] and [CK10] (see also [EH18, §2] for a brief exposition), our aim is to prove the asymptotic dimension hypothesis

$$\dim H^1_f(G_T, \Psi_n) \ll \dim \operatorname{Res}^{F_p}_{\mathbb{Q}_p}(\Psi_n^{\mathrm{dR}}/F^0\Psi_n^{\mathrm{dR}})$$

for a quotient Ψ_n of Π_n (usually something like the metabelianization of Π_n).

Remark 4.2. Unlike over $\mathbb{Q}$ (or more generally, when p is totally split in $F/\mathbb{Q}$), the dimension hypothesis does *not* directly imply finiteness of $Y(F)$; the output of the argument is a nonzero $\mathbb{Q}_p$-analytic function on $Y(F_p)$ that vanishes on $Y(F)$, and $Y(F_p)$ is $[F_p : \mathbb{Q}_p]$-dimensional as a $\mathbb{Q}_p$-analytic space.

The situation isn't hopeless, though, because the difference in dimensions between the global and local Selmer varieties grows arbitrarily large with n. This gives us arbitrarily many algebraically independent functions on $\mathrm{Res}^{F_p}_{\mathbb{Q}_p}(U_n^{\mathrm{dR}}/F^0U_n^{\mathrm{dR}})$ that vanish on the image of the global Selmer variety.

One might hope that any $[F:\mathbb{Q}]$ of these functions pull back to $\mathbb{Q}_p$-analytic functions on $Y(F_p)$ whose simultaneous vanishing is zero-dimensional. In chapter 5, we explore this question further and pose a conjecture that implies this (and hence gives a new conditional proof of finiteness of $C(F)$).

4.1 Arbitrary hyperbolic curves, conditionally

In [Kim09], Kim proves the dimension hypothesis for an arbitrary curve X over $\mathbb{Q}$ of genus $g \geq 2$, conditional on either the Bloch–Kato conjecture or the Fontaine–Mazur conjecture. We generalize this to number fields F with a real place by proving [Kim09, Prop. 2] over such a number field.

Theorem 4.3. *Let F be a number field with a real embedding. Let X be a smooth hyperbolic curve over F. Let p be a rational prime, inert in $F/\mathbb{Q}$ and of good reduction for X. Let $V_n = H^1_{\text{ét}}(\bar{X}, \mathbb{Q}_p)^{\otimes n}(1)$. Define*

$$\mathrm{Sel}^0_T(V_n) := \ker\Big(H^1(G_T, V_n) \to \bigoplus_{w \in T} H^1(G_w, V_n)\Big),$$

and suppose $\mathrm{Sel}^0_T(V_n) = 0$. (Note that this follows from either the Bloch–Kato or the Fontaine–Mazur conjecture, as shown in [Kim09, §3].) Then there exists $c < 1$ such that, for all sufficiently large n,

$$\dim H^1_f(G_T, \Pi_n) < c \cdot \dim \mathrm{Res}^{F_p}_{\mathbb{Q}_p}(\Pi_n^{\mathrm{dR}}/F^0\Pi_n^{\mathrm{dR}}).$$

Proof. The argument is essentially the same as for [Kim09, Prop. 2], with some modifications. The Euler characteristic formula becomes

$$\dim H^1(G_T, Z^n/Z^{n+1}) - \dim H^2(G_T, Z^n/Z^{n+1}) \\ = [F:\mathbb{Q}]\dim(Z^n/Z^{n+1}) - \sum_{\iota\colon F\hookrightarrow\mathbb{R}} \dim(Z^n/Z^{n+1})^{\iota,+},$$

where the latter superscript refers to the 1-eigenspace of the complex conjugation corresponding to ι. Since p is inert in F, we have $[F_p : \mathbb{Q}_p] = [F : \mathbb{Q}]$, so

$$\dim_{\mathbb{Q}_p}(Z^n/Z^{n+1} \otimes_{\mathbb{Q}_p} F_p) = [F:\mathbb{Q}]\dim_{\mathbb{Q}_p}(Z^n/Z^{n+1}).$$

There is at least one embedding $\iota\colon F \hookrightarrow \mathbb{R}$, and the corresponding term $\dim(Z^n/Z^{n+1})^{\iota,+}$ has dimension $\frac{1}{2}\dim(Z^n/Z^{n+1})$ (by the same comparison with complex Hodge theory as in the proof of [Kim09, Prop. 2]). Hence, it suffices to show that $\dim H^2(G_T, Z^n/Z^{n+1})$ does not contribute to the asymptotic, which is shown in [Kim09, Lemma 6], the proof of which works over any number field. □

4.2 Curves with CM Jacobian

In this section, we provide the necessary modifications to [CK10] to generalize the main result to real number fields.

For the remainder of this section, assume Jac(C) is isogenous over $\bar{F}$ to a product of CM abelian varieties. Let K be the compositum of the CM fields K_i of the simple factors of Jac(C). As in [CK10], the quotient we use to prove the dimension hypothesis is $\Psi = U_n$, the metabelianization of $\Pi_{C,n}$, for $n \gg 0$. We follow the same strategy as [CK10], modified in certain places to account for the fact that C is over F instead of

$\mathbb{Q}$ and that we do not have control over the splitting behavior of p in K (because p is assumed to be inert in F).

For each $n \geq 1$, we have the short exact sequence

$$0 \to Z_n \to U_n \to U_{n-1} \to 0.$$

Since $U_1 = V_p \operatorname{Jac}(C)$ is a quotient of U_{n-1} and has trivial stabilizer under a lift of Frobenius, we have $H^0(G_T, U_{n-1}) = 0$. Hence, we obtain an exact sequence

$$0 = H^0(G_T, U_{n-1}) \to H^1(G_T, Z_n) \to H^1(G_T, U_n) \to H^1(G_T, U_{n-1}).$$

So

$$\dim H^1_f(G_T, U_n) \leq \dim H^1(G_T, U_n) \leq \sum_{i=1}^{n} \dim H^1(G_T, Z_i).$$

By the global Poincaré–Euler characteristic formula (noting that $H^0(G_T, Z_i) = 0$),

$$\dim H^1(G_T, Z_i) = [F : \mathbb{Q}] \dim Z_i - \sum_{\iota \colon F \hookrightarrow \mathbb{R}} \dim Z_i^{\iota,+} + \dim H^2(G_T, Z_i),$$

where ι ranges over real places of F, and $Z_i^{\iota,+}$ is the 1-eigenspace of the action of the complex conjugation associated to ι on Z_i. So

$$\sum_{i=1}^{n} \dim H^1(G_T, Z_i) = [F : \mathbb{Q}] \dim U_n - \sum_{i=1}^{n} \sum_{\iota \colon F \hookrightarrow \mathbb{R}} \dim Z_i^{\iota,+} + \sum_{i=1}^{n} \dim H^2(G_T, Z_i).$$

We compare this to

$$\begin{aligned} \dim \operatorname{Res}^{F_p}_{\mathbb{Q}_p}(U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}}) &= [F_p : \mathbb{Q}_p] \dim U_n^{\mathrm{dR}} - [F_p : \mathbb{Q}_p] \dim F^0 U_n^{\mathrm{dR}} \\ &= [F : \mathbb{Q}] \dim U_n - [F : \mathbb{Q}] \dim F^0 U_n^{\mathrm{dR}}. \end{aligned}$$

We will see that, as in [CK10], the highest-order term in both the above formulas is $\dim U_n$. This motivates our assumption that p is inert in F: comparison of leading coefficients shows the dimension hypothesis is impossible unless $[F_p : \mathbb{Q}_p] = [F : \mathbb{Q}]$, which means p cannot split in F. (This does not rule out the possibility of p being ramified rather than inert; the generalization to the ramified setting poses additional technical difficulties which the author hopes to investigate in future research.)

The proof of the bound

$$\dim F^0 U_n^{\mathrm{dR}} = O(n^g)$$

from [CK10, Proof of Corollary 0.2] holds without modification in our setting. Indeed, the only non-combinatorial input to that argument is that $F^0 U_1^{\mathrm{dR}}$ is g-dimensional, which is still true when the base field is F_p instead of $\mathbb{Q}_p$.

Similarly, the bound

$$\dim Z_i^{\iota,+} \geq C n^{2g-1}$$

for some constant $C > 0$ can be proved exactly as in [CK10]; their proof is purely combinatorial and can be applied to the complex conjugation associated to each ι.

To complete the strategy of [CK10], it remains to prove

$$\dim H^2(G_T, Z_n) = O(n^{2g-2}).$$

This is the part that requires modification: [CK10, Proof of Theorem 0.1] relies on the decomposition of U_1 as a direct sum of characters, but as one can see from [CK10, §1], this relies on the splitting of p in K; in general,

$$\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m) \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

is a torus, but not necessarily a *split* torus over $\mathbb{Q}_p$. However,

$$\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m) \otimes_{\mathbb{Q}} L$$

is a split torus over some finite Galois extension $L/\mathbb{Q}_p$, so $U_1 \otimes_{\mathbb{Q}_p} L$ is a direct sum of L-valued Galois characters $\chi_1, \ldots, \chi_{2g}$. To use this fact, we need a lemma in Galois cohomology.

Lemma 4.4. *Let K be a p-adic field. Let V be a $K[G_T]$-module such that $H^0(G_T, V) = 0$ and $\dim_K V < \infty$. Let L be a Galois extension of K. Let $V_L = V \otimes_K L$ with G_T acting trivially on L. Then*

$$\dim_K H^2(G_T, V) = \dim_L H^2(G_T, V_L).$$

Proof. The actions of G_T and $\Gamma = \mathrm{Gal}(L/K)$ on V_L commute, so

$$0 = H^0(G_T, V) = H^0(G_T \times \Gamma, V_L) = H^0(G_T, V_L)^{\Gamma},$$

so by Galois descent, $H^0(G_T, V_L) = 0$. Part of the inflation-restriction exact sequence for $G_T \subseteq G_T \times \Gamma$ acting on V_L is

$$H^1(\Gamma, V_L^{G_T}) \to H^1(G_T \times \Gamma, V_L) \to H^1(G_T, V_L)^{\Gamma} \to H^2(\Gamma, V_L^{G_T}),$$

and since $V_L^{G_T} = 0$, we obtain

$$H^1(G_T \times \Gamma, V_L) \cong H^1(G_T, V_L)^{\Gamma}.$$

The inflation-restriction exact sequence for $\Gamma \subseteq G_T \times \Gamma$ acting on V_L gives exactness of

$$0 \to H^1(G_T, V) \to H^1(G_T \times \Gamma, V_L) \to H^1(\Gamma, V_L)^{G_T},$$

but $V_L \cong L^{\dim_K V}$ as a Γ-module, so $H^1(\Gamma, V_L) = 0$. Thus,

$$H^1(G_T, V) \cong H^1(G_T \times \Gamma, V_L) \cong H^1(G_T, V_L)^{\Gamma},$$

so $\dim_K H^1(G_T, V) = \dim_L H^1(G_T, V_L)$ by Galois descent.

By the Euler characteristic formula [Mil06, I, Thm. 5.1] and the fact that involutions are diagonalizable over any field, $\chi(G_T, V) = \chi(G_T, V_L)$. Since we have already shown equality of dimensions for the H^0 and H^1 terms, we are done. □

In particular,

$$\dim_{\mathbb{Q}_p} H^2(G_T, Z_n) = \dim_L H^2(G_T, Z_n \otimes_{\mathbb{Q}_p} L),$$

and the proof of [CK10, Thm. 0.1] applies without modification to the latter: the same weight argument reduces the problem to Iwasawa theory, and the remainder of the proof is the same. (We verify below that the setup in [CK10, §1] encounters no difficulties when the representations are allowed to take values in extensions of $\mathbb{Q}_p$.)

We have now proven all the necessary bounds to carry out the argument of [CK10, Proof of Cor. 0.2].

Theorem 4.5. *Let F be a number field with an embedding $F \hookrightarrow \mathbb{R}$. Let C be a smooth projective curve over F of genus $g \geq 2$ such that* $\mathrm{Jac}(C)$ *has potential CM. There exists $c < 1$ such that, for all n sufficiently large,*

$$\dim H^1_f(G_T, U_n) < c \cdot \dim \mathrm{Res}^{F_p}_{\mathbb{Q}_p}(U_n^{\mathrm{dR}}/F^0 U_n^{\mathrm{dR}}).$$

4.2.1 “Preliminaries on complex multiplication”

In this subsection, we fully replicate the contents of [CK10, §1], adapted to our level of generality and notation. The author claims no originality in what follows; this is purely to ensure that nothing goes wrong when we generalize to an inert prime in a real number field.

Let L/F be a finite extension with the property that the isogeny decomposition

$$J := \mathrm{Jac}(C) \sim \prod_i A_i$$

as well as the complex multiplication on each A_i are defined over L. We assume further that $L \supset F(J[p])$, so that $L_\infty := L(J[p^\infty])$ has Galois group $\Gamma \cong \mathbb{Z}_p^r$ over L. Denote by $G_{L,T}$ the Galois group $\mathrm{Gal}(L_T/L)$, where L_T is the maximal extension of L unramified outside the primes dividing those in T.

As a representation of $G_{L,T}$, we have

$$V := T_pJ \otimes \mathbb{Q}_p \cong \bigoplus_i V_i,$$

where $V_i := T_pA_i \otimes \mathbb{Q}_p$.

Let m be a modulus of L that is divisible by the conductor of all the representations V_i. Each factor representation

$$\rho_i \colon G_{L,T} \to (K_i \otimes \mathbb{Q}_p)^* \subset \mathrm{Aut}(V_i)$$

corresponds to an algebraic map

$$f_i \colon S_m \to \mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m),$$

where S_m is the Serre group of L with modulus m, and $\mathrm{Res}_{\mathbb{Q}}^{K_i}$ is the restriction of scalars from K_i to $\mathbb{Q}$. That is, there is a universal representation

$$\epsilon_p \colon G_{L,T} \to S_m(\mathbb{Q}_p)$$

such that

$$\rho_i = f_i \circ \epsilon_p \colon G_{L,T} \to S_m(\mathbb{Q}_p) \to \mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m)(\mathbb{Q}_p) = (K_i \otimes \mathbb{Q}_p)^*.$$

Since we have made no assumptions about the splitting type of p in K_i, the algebraic torus

$$\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m) \otimes \mathbb{Q}_p$$

might be non-split. However, for some finite extension $k/\mathbb{Q}_p$, we have

$$\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m) \otimes k \cong \prod_j [\mathbb{G}_m]_k.$$

Thus, extending scalars to k, each of the algebraic characters

$$f_{ij} = \mathrm{pr}_j \circ \rho_i \colon [S_m]_k \to [\mathrm{Res}_{\mathbb{Q}}^{K_i}(\mathbb{G}_m)]_k \cong \prod_j [\mathbb{G}_m]_k \stackrel{\mathrm{pr}_j}{\to} [\mathbb{G}_m]_k$$

correspond to Galois characters

$$\chi_{ij} = f_{ij} \circ \epsilon_p \colon G_{L,T} \to k^*$$

in such a way that

$$\rho_i \cong \bigoplus_j \chi_{ij}$$

after extension of scalars to k.

Recall that S_m fits into an exact sequence

$$0 \to T_m \to S_m \to C_m \to 0$$

with C_m finite and T_m an algebraic torus. Hence, there is an integer N such that the kernel of the restriction map on characters

$$X^*([S_m]_k) \to X^*([T_m]_k)$$

is killed by N. Since $X^*([T_m]_k)$ is a finitely-generated torsion-free abelian group, so is the image of $X^*([S_m]_k)$. Let $\{\beta_1', \dots, \beta_d'\}$ be a basis for the subgroup of $X^*([T_m]_k)$ generated by the restrictions $f_{ij}|[T_m]_k$ as we run over all i and j. Then the set $\{\beta'_1, \dots, \beta'_d\}$ can be lifted to characters $\{\beta_1, \dots, \beta_d\}$ of $[S_m]_k$ so that each f_{ij}^N is a product

$$f_{ij}^N = \prod_{\kappa} \beta_{\kappa}^{n_{ij\kappa}}$$

for integers $n_{ij\kappa}$. For ease of notation, we now change the indexing and write $\{f_1, \dots, f_{2g}\}$ for the set of f_{ij} and $\{\chi_i\}_{i=1}^{2g}$ for the characters of $G_{L,T}$ that they induce. We have shown that there are integers n_{ij} such that

$$f_i^N = \prod_j \beta_j^{n_{ij}}.$$

Thus, if we denote by ξ_i the character

$$\beta_i \circ \epsilon_p \colon G_{L,T} \to k^*,$$

then

$$\chi_i^N = \prod_j \xi_j^{n_{ij}}.$$

Lemma 4.6. *The characters ξ_i are $\mathbb{Z}_p$-linearly independent.*

Proof. Suppose

$$\prod_i \xi_i^{a_i} = 1$$

for some $a_i \in \mathbb{Z}_p$ as a function on $G_{L,T}$ (and the choice of p-adic log such that $\log(p) = 0$). Then

$$\prod_i \beta_i^{a_i} = 1$$

as a (k^*-valued) character on $\epsilon_p(G_{L,T})$. As noted in [Ser68, II.2.3, Remark], the image of the map $\epsilon_p \colon G_{L,T} \to S_m(\mathbb{Q}_p)$ is Zariski-dense, so in fact the above equation holds everywhere on T_m. Since the $\beta_i|[T_m]_k = (\beta_i')^N$ are $\mathbb{Z}$-linearly independent, for each j there exists a cocharacter

$$c_j \colon [\mathbb{G}_m]_k \to [T_m]_k$$

such that $\beta_i \circ c_j = 1$ for $i \neq j$ and

$$\beta_j \circ c_j \colon [\mathbb{G}_m]_k \to [\mathbb{G}_m]_k$$

is nontrivial and hence an isogeny. So for all $x \in k^\times$, we have

$$\beta_j(c_j(x))^{a_j} = 1.$$

Since p-adic exponentiation is injective within its radius of convergence, if $c^{a_j} = 1$, then either $a_j = 0$ or $\log_p(c) = 0$. But $\log_p(c) = 0$ if and only if c is a rational power of p times a root of unity, so if $c^{a_j} = 1$ for uncountably many c, then $a_j = 0$. Combining this observation with the above, we obtain $a_j = 0$ and are done. □

4.3 Unramified correspondences and solvable curves

In this section, we provide the necessary modifications to [EH18] to generalize the main result to real number fields.

Let Y and X be smooth projective curves over F of genus at least 2. Suppose there is a dominant map $f_K \colon Y_K \to X_K$ for some finite Galois extension K/F, and suppose that $\mathrm{Jac}(X)$ is a CM abelian variety. Let p be a rational prime, inert in $F/\mathbb{Q}$, such that Y and X both have good reduction at p. Let W be the image of the induced map $U_Y \to U_R$, where $R = \mathrm{Res}_F^K(X_K)$, and let $W_{[n]}$ be the quotient defined as in [EH18, §3.3].

We assume also that p is unramified in $K/\mathbb{Q}$, which is only needed to use Olsson's comparison isomorphism in the proof of [EH18, Lemma 4.1]. This assumption could be dropped if we instead use the comparison isomorphism

$$\Pi_Y^{\mathrm{dR}} \otimes_L B_{\mathrm{dR}} \cong \Pi_Y \otimes_{\mathbb{Q}_p} B_{\mathrm{dR}},$$

which should hold for any local field $L/\mathbb{Q}_p$, not just unramified extensions (and, for that matter, regardless of the reduction type of Y at p). However, to my knowledge, a proof of this comparison isomorphism is not present in the published literature at this time; it seems to be "folklore" that it could be extracted from Beilinson and Bhatt's work on derived p-adic Hodge theory (perhaps by reconstructing the fundamental groups from the corresponding E_∞-algebras).

Requiring p to be inert in F and applying the same modifications to the Euler characteristic formula as in the previous section, all the arguments needed for the main result of [EH18] can still be carried out in this level of generality.

(There are two arguments in [EH18], namely the proofs of Lemmas 6.1 and 6.2, that use that p splits completely in K, but both of these assumptions are unnecessary. For Lemma 6.1, the Hodge filtration is compatible with extending the base field (and this does not change the dimensions), so we can carry out the same argument using the de Rham fundamental group over $\bar{F}_p$. For Lemma 6.2, the vanishing of H^0 follows by examining the Frobenius weights, just as in the case $F = \mathbb{Q}$. See Lemmas 3.1 and 3.2 of this thesis for the appropriately modified proofs.)

Theorem 4.7. *Let S be a finite set of primes of F such that both Y and X have good reduction outside $T = S \cup \{p\}$. Suppose there is a number field L/K and a constant $B > 0$ (depending on X and T) such that for all $n \geq 1$,*

$$\sum_{i=1}^{n} \dim H^2(G_{L,T}, U_X^n/U_X^{n+1}) \leq Bn^{2g-1}.$$

Then there exists $c < 1$ *such that, for all sufficiently large* n*,*

$$\dim H^1_f(G_T, W_{[n]}) < c \cdot \mathrm{Res}^{F_p}_{\mathbb{Q}_p}(\dim W^{\mathrm{dR}}_{[n]}/F^0 W^{\mathrm{dR}}_{[n]}).$$

Chapter 5

Transcendence properties of the unipotent Albanese map

In this chapter, we discuss transcendence properties of the unipotent Albanese map

$$j_n^{\mathrm{dR}} \colon \mathcal{X}(\mathcal{O}_{F_v}) \to \mathrm{Sel}_n^{\mathrm{dR}}(X/F_v) := \mathrm{Res}_{\mathbb{Q}_p}^{F_v}(U_{X,n}^{\mathrm{dR}}/F^0U_{X,n}^{\mathrm{dR}}).$$

This is a p-adic analytic map given in coordinates by iterated p-adic integration in the sense of [Bes02]. By [Kim09, Thm. 1], the image of j_n^{dR} is Zariski-dense. As a consequence, any nonzero algebraic function on $\mathrm{Sel}_n^{\mathrm{dR}}(X/F_v)$ pulls back to a nonzero p-adic analytic function on $\mathcal{X}(\mathcal{O}_{F_v})$.

As discussed in Remark 4.2, this is insufficient to deduce finiteness of $\mathcal{X}(\mathcal{O}_{F_v})$ when p does not split completely in $F/\mathbb{Q}$, because $\mathcal{X}(\mathcal{O}_{F_v})$ is $[F_v : \mathbb{Q}_p]$-dimensional as a $\mathbb{Q}_p$-manifold. We propose a stronger conjecture that is sufficient to deduce finiteness.

Conjecture 5.1. *Let X be a smooth hyperbolic curve with integral model $\mathcal{X}$ over a number field F. Let v be an unramified finite prime of F such that X has good reduction at v. Let $\delta \le d = [F_v : \mathbb{Q}_p]$. Let $Z \subseteq \mathrm{Sel}_n^{\mathrm{dR}}(X/F_v)$ be a closed algebraic subvariety such that, for each intermediate subfield $\mathbb{Q}_p \subseteq K \subseteq F_v$ and each curve X'/K such that $X'_{F_v} \cong X$, the codimension of $Z \cap \mathrm{Sel}_n^{\mathrm{dR}}(X'/K)$ in $\mathrm{Sel}_n^{\mathrm{dR}}(X'/K)$ is at least* $\min\{\delta, [K : \mathbb{Q}_p]\}$. *(We* *identify* $\mathrm{Sel}_n^{\mathrm{dR}}(X'/K)$ *with the subvariety of* $\mathrm{Sel}_n^{\mathrm{dR}}(X/F_v)$ *fixed by* $\mathrm{Gal}(F_v/K)$*.) Then*

$$\dim_{\mathbb{Q}_p}(j_n^{\mathrm{dR}}(\mathcal{X}(\mathcal{O}_{F_v})) \cap Z) \leq d - \delta.$$

Remark 5.2. One might initially conjecture (and by this I mean I did initially conjecture) that Z merely has to be of codimension δ. However, this is false: if X is defined over $\mathbb{Q}_p$ and $Z = \mathrm{Sel}_n^{\mathrm{dR}}(X/\mathbb{Q}_p)$ is embedded "diagonally" as $\mathrm{Sel}_n^{\mathrm{dR}}(X/F_v)^{\mathrm{Gal}(F_v/\mathbb{Q}_p)}$, then the dimension of Z is $(1/d) \cdot \dim \mathrm{Sel}_n^{\mathrm{dR}}(X/F_v)$, but $\mathcal{X}(\mathbb{Z}_p) \subseteq Z \cap \mathcal{X}(\mathcal{O}_{F_v})$.

Assuming Conjecture 5.1, we can apply the results of chapter 4 to deduce finiteness of $X(F)$ for real number fields F under certain conditions on X (namely, X dominates a curve with CM Jacobian, or X is arbitrary if we assume one of several conjectures in Galois cohomology).

Corollary 5.3. *Let $F/\mathbb{Q}$ be a number field of degree d. Let X be a smooth projective hyperbolic curve over a number field F. Let v be an unramified finite prime of F such that X has good reduction at v. Suppose that for each subfield $K \subseteq F$ and each curve X'/K such that $X'_F \cong X$, we have*

$$\dim H^1_f(G_{K,T}, U_{X,n}) \leq \dim \mathrm{Res}^K_{\mathbb{Q}_p}(U^{\mathrm{dR}}_{X,n}/F^0 U^{\mathrm{dR}}_{X,n}) - [K : \mathbb{Q}_p]$$

for all sufficiently large n. Suppose also that Conjecture 5.1 holds for X whenever $\delta \leq d$. Then $X(F)$ is finite.

Proof. By Conjecture 5.1 and the main commutative diagram, $j_n^{\mathrm{dR}}(X(F))$ is zero-dimensional and compact, hence finite. □

In the remainder of this chapter, we motivate and provide evidence for Conjecture 5.1. A few preliminary remarks:

(1) Intuitively, the conjecture says that j_n^{dR} is "purely transcendental", in the sense that it remains non-algebraic even after restricting to an algebraic subvariety of the target (assuming the restriction is still positive-dimensional).

(2) The conjecture in codimension 1 is a reformulation of [Kim09, Thm. 1], which underlies the existing results over $\mathbb{Q}$.

(3) This conjecture is formally similar to the Ax–Schanuel theorem, conjectured for variations of Hodge structure in [Kli17] and proved in [BT17]. However, while the period map for so-called "Hodge varieties" is surjective, the unipotent Albanese map j_n^{dR} is not, necessitating the restriction $\delta \leq d$ on codimension.

5.1 The Ax–Schanuel theorem

The classical Ax–Schanuel theorem, conjectured by Schanuel and proved by Ax, is as follows.

Theorem 5.4 ([Ax71]). *Let $f_1, \ldots, f_n \in t\mathbb{C}[[t]]$ be linearly independent over $\mathbb{Q}$. Then the field extension*

$$\mathbb{C}(t) \subset \mathbb{C}(t, f_1, \ldots, f_n, e^{f_1}, \ldots, e^{f_n})$$

has transcendence degree at least n.

This has a geometric reformulation:

Theorem 5.5 ([Tsi15]). *Let $W \subset \mathbb{C}^n \times (\mathbb{C}^\times)^n$ be an algebraic subvariety. Let $D \subset \mathbb{C}^n \times (\mathbb{C}^\times)^n$ be the graph of the complex exponential map* $\exp\colon \mathbb{C}^n \to (\mathbb{C}^\times)^n$*. Let U be an irreducible component of $W \cap D$ of larger than expected dimension, i.e., such that*

$$\operatorname{codim} U < \operatorname{codim} W + \operatorname{codim} D,$$

where the codimensions are relative to $\mathbb{C}^n \times (\mathbb{C}^\times)^n$*. Then the projection of* U *to* $(\mathbb{C}^\times)^n$ *is contained in a coset of a proper subtorus of* $(\mathbb{C}^\times)^n$*.*

In this formulation, generalizations to Shimura varieties [MPT17] and Hodge varieties [BT17] have been formulated and proved. The most general version I am currently aware of is the following:

Theorem 5.6 (Ax–Schanuel for variations of Hodge structures, [BT17])**.** *Let* X *be a smooth algebraic variety over* $\mathbb{C}$ *supporting a pure polarized integral variation of Hodge structures. Let* D *be the weak Mumford–Tate domain associated to this variation of Hodge structures, and let*

$$\phi \colon X \to \Gamma \backslash D$$

be the period map, where Γ *is the image of monodromy acting on* D*. Let* $\check{D}$ *be the compact dual of* D*, which is a projective variety containing* D *in the Archimedean topology. Let* $W = X \times_{\Gamma\backslash D} D$*. Let* $V \subset X \times \check{D}$ *be an algebraic subvariety. Let* U *be an irreducible analytic component of* $V \cap W$ *of larger than expected dimension, i.e., such that*

$$\operatorname{codim} U < \operatorname{codim} V + \operatorname{codim} W,$$

where the codimensions are relative to $X \times \check{D}$*. Then the projection of* U *to* X *is contained in a proper weak Mumford–Tate subvariety (in the sense defined in [BT17]).*

Note that in each case, there is some class of "special subvarieties": cosets of subtori for $(\mathbb{C}^\times)^n$, weakly special subvarieties for Shimura varieties, weak Mumford–Tate subvarieties for Hodge varieties, etc. The various Ax–Schanuel theorems are all to the effect that intersections of larger than expected dimension must be "explained" by containment in a proper special subvariety.

In our setting, we are concerned with rational points on certain varieties—in particular, restrictions of scalars of curves, which become Cartesian powers of curves after base change—and there is another notion of "special subvariety": those subvarieties which are not of general type. This is motivated by the geometric Lang conjecture:

Conjecture 5.7. *Let X be a variety of general type. Then the union of all irreducible, positive-dimensional subvarieties of X not of general type is a proper closed subvariety of X.*

Caporaso, Harris, and Mazur [CHM97] show that, in combination with the weak Lang conjecture, this implies a strong uniformity statement on the number of rational points of higher genus curves over number fields.

Anyway, one cannot hope for a statement such as Conjecture 5.1 to hold for arbitrary varieties because of the presence of such positive-dimensional exceptional subvarieties. For example, the symmetric square of a hyperelliptic curve contains a copy of $\mathbf{P}^1$. (Nonetheless, Chabauty's method has been applied to count rational points outside the "exceptional set" for symmetric powers of curves; see, for example, [Par16] and [GM17]. It would be very interesting to see an application of non-abelian Chabauty to symmetric powers of curves.)

Fortunately, for a Cartesian power of a curve, which is what arises in our application, there are no positive-dimension subvarieties not of general type, which is why Conjecture 5.1 is formulated without any provision for special subvarieties analogous to those occurring in various versions of the Ax–Schanuel theorem.

Bibliography

[Ax71] J. Ax. "On Schanuel's conjectures". *Ann. of Math.* 93 (1971), pp. 252–268.

[BT17] B. Bakker and J. Tsimerman. "The Ax–Schanuel conjecture for variations of Hodge structures". *ArXiv e-prints* (2017). arXiv: `1712.05088 [math.AG]`.

[BDCKW17] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. "A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves". *ArXiv e-prints* (2017). arXiv: `1209.0640 [math.NT]`.

[BD18a] J. S. Balakrishnan and N. Dogra. "An effective Chabauty–Kim theorem". *ArXiv e-prints* (2018). arXiv: `1803.10102 [math.NT]`.

[BD18b] J. S. Balakrishnan and N. Dogra. "Quadratic Chabauty and rational points I: p-adic heights". *ArXiv e-prints* (2018). arXiv: `1601.00388 [math.NT]`.

[BDMTV17] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuiman, and J. Vonk. "Explicit Chabauty–Kim for the split Cartan modular curve of level 3". *ArXiv e-prints* (2017). arXiv: `1711.05846 [math.NT]`.

[Bel79] G. V. Belyi. "Galois extensions of a maximal cyclotomic field". *Izv. Akad. Nauk SSSR Ser. Mat.* 43.2 (1979), pp. 267–276, 479.

[Bes02] A. Besser. "Coleman integration using the Tannakian formalism". *Math. Ann.* 322.1 (2002), pp. 19–48.

[Bet17] L. A. Betts. "The motivic anabelian geometry of local heights on abelian varieties". *ArXiv e-prints* (2017). arXiv: `1706.04850 [math.NT]`.

[BQ17] F. Bogomolov and J. Qian. “On Contraction of Algebraic Points”. *ArXiv e-prints* (2017). arXiv: `1607.01832 [math.AG]`.

[BT02] F. Bogomolov and Y. Tschinkel. “Unramified correspondences”. *Algebraic Number Theory and Algebraic Geometry*. Ed. by S. Vostovok and Y. Zarhin. Vol. 300. Contemporary Mathematics. 2002, pp. 17–26.

[BT04] F. Bogomolov and Y. Tschinkel. “Couniformization of curves over number fields”. *Geometric methods in algebra and number theory*. Vol. 235. Progress in Math. Birkhäuser, 2004, pp. 43–57.

[BT07] F. Bogomolov and Y. Tschinkel. “Algebraic varieties over small fields”. *Diophantine Geometry*. Vol. 4. CRM Series. Scuola Normale Superiore di Pisa, 2007, pp. 73–91.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron Models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer, Berlin, Heidelberg, 1990.

[Bro17] F. Brown. “Integral points on curves, the unit equation, and motivic periods”. *ArXiv e-prints* (2017). arXiv: `1704.00555 [math.NT]`.

[CHM97] L. Caporaso, J. Harris, and B. Mazur. “Uniformity of rational points”. *J. Amer. Math. Soc.* 10 (1997), pp. 1–35.

[Cha41] C. Chabauty. “Sur les points rationels des courbes algébriques de genre supérieur à l’unité”. *C. R. Acad. Sci* 212 (1941), pp. 882–884.

[CK10] J. Coates and M. Kim. “Selmer varieties for curves with CM Jacobians”. *Kyoto J. Math.* 50.4 (2010), pp. 827–852.

[Col85] R. F. Coleman. "Effective Chabauty". *Duke Math. J.* 52.3 (1985), pp. 765–770.

[Del89] P. Deligne. "Le groupe fondamental de la droite projective moins trois points". *Galois groups over* $\mathbb{Q}$. Ed. by Y. Ihara, K. Ribet, and J.-P. Serre. Vol. 16. Mathematical Sciences Research Institute Publications. 1989, pp. 79–297.

[EH18] J. S. Ellenberg and D. R. Hast. "Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty". *ArXiv e-prints* (2018). arXiv: `1706.00525 [math.NT]`.

[Fal83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". *Invent. Math.* 73.3 (1983), pp. 349–366.

[FW99] E. V. Flynn and J. L. Wetherell. "Finding rational points on bielliptic genus 2 curves". *Manuscripta Mathematica* 100 (1999), pp. 519–533.

[GM17] J. Gunther and J. S. Morrow. "A positive proportion of odd degree hyperelliptic curves over $\mathbb{Q}$ have at most 12 pairs of unexpected quadratic points". *ArXiv e-prints* (2017). arXiv: `1709.02041 [math.NT]`.

[HM03] R. Hain and M. Matsumoto. "Weighted Completion of Galois Groups and Galois Actions on the Fundamental Group of $\mathbb{P}^1 - \{0, 1, \infty\}$". *Compositio Math.* 139 (2003), pp. 119–167.

[KRZ16] E. Katz, J. Rabinoff, and D. Zureick-Brown. "Uniform bounds for the number of rational points on curves of small Mordell–Weil rank". *Duke Math. J.* 165.16 (2016), pp. 3189–3240.

[Kim05] M. Kim. "The motivic fundamental group of the projective line minus three points and the theorem of Siegel". *Invent. Math.* 161.3 (2005), pp. 629–656.

[Kim09] M. Kim. "The unipotent Albanese map and Selmer varieties for curves". *Publ. Res. Inst. Math. Sci.* 45.1 (2009), pp. 89–133.

[Kim12a] M. Kim. "A remark on fundamental groups and effective Diophantine methods for hyperbolic curves". *Number Theory, Analysis, and Geometry. In memory of Serge Lang.* Springer-Verlag, 2012.

[Kim12b] M. Kim. "Galois Theory and Diophantine Geometry". *Non-abelian Fundamental Groups and Iwasawa Theory.* Ed. by J. Coates, M. Kim, F. Pop, M. Saïdi, and P. Schneider. Vol. 393. London Mathematical Society Lecture Note Series. Cambridge University Press, 2012, pp. 162–187.

[Kim12c] M. Kim. "Tangential localization for Selmer varieties". *Duke Math. J.* 161.2 (2012), pp. 173–199.

[Kim17] M. Kim. "Arithmetic gauge theory: A brief introduction". *ArXiv e-prints* (2017). arXiv: `1712.07602 [math.NT]`.

[Kli17] B. Klingler. "Hodge loci and atypical intersections: conjectures". *ArXiv e-prints* (2017). arXiv: `1711.09387 [math.AG]`. To appear in the proceedings of the conference "Motives and Complex Multiplication", held in Monte-Verita, August 2016.

[Mil06] J. S. Milne. *Arithmetic Duality Theorems.* 2nd. BookSurge Publishing, 2006.

[Mil17] J. S. Milne. *Algebraic Groups*. Vol. 170. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2017.

[MPT17] N. Mok, J. Pila, and J. Tsimerman. "Ax–Schanuel for Shimura varieties". *ArXiv e-prints* (2017). arXiv: `1711.02189 [math.NT]`.

[Ols11] M. Olsson. *Towards Non-Abelian p-adic Hodge Theory in the Good Reduction Case*. Vol. 210. Memoirs of the American Mathematical Society. 2011.

[Par16] J. Park. "Effective Chabauty for symmetric powers of curves". *ArXiv e-prints* (2016). arXiv: `1606.05195 [math.NT]`.

[Poo05] B. Poonen. "Unramified covers of Galois covers of low genus curves". *Mathematical Research Letters* 12.4 (2005), pp. 475–481.

[Ser68] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968, xvi+177 pp. (not consecutively paged).

[Ser89] J.-P. Serre. *Lectures on the Mordell–Weil Theorem*. Vol. 15. Aspects of Mathematics. 1989.

[Sto15] M. Stoll. "Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell–Weil rank". *ArXiv e-prints* (2015). arXiv: `1307.1773 [math.NT]`. To appear in *J. Eur. Math. Soc.*

[Stacks] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`. 2017.

[Tsi15] J. Tsimerman. “Ax–Schanuel and o-minimality”. *O-minimality and Diophantine geometry*. Vol. 421. LMS Lecture Note Series. Cambridge University Press, 2015, pp. 216–221.

[Vol12] J. F. Voloch. “Finite descent obstruction for curves over function fields”. *Bull. Braz. Math. Soc.* 43.1 (2012), pp. 1–6.