Two recent p-adic approaches towards the (effective) Mordell conjecture

Balakrishnan, Jennifer S.; Best, Alex J.; Bianchi, Francesca; Lawrence, Brian; Müller, J. Steffen; Triantafillou, Nicholas; Vonk, Jan

Published in:
ArXiv

Publication date:
2019

TWO RECENT p-ADIC APPROACHES TOWARDS THE (EFFECTIVE) MORDELL CONJECTURE

JENNIFER S. BALAKRISHNAN, ALEX J. BEST, FRANCESCA BIANCHI, BRIAN LAWRENCE, J. STEFFEN MÜLLER, NICHOLAS TRIANTAFILLOU, AND JAN VONK

Contents

1. Introduction 1
2. The method of Lawrence–Venkatesh: Finiteness 6
3. The method of Lawrence–Venkatesh: Effectivity 11
4. The method of Chabauty–Kim: Finiteness 15
5. The method of Chabauty–Kim: Effectivity 19
6. Examples 24
References 31

1. Introduction

1.1. **The Mordell conjecture.** Many important developments in arithmetic geometry were motivated by the Mordell conjecture, stated nearly a century ago. Let X be a smooth projective curve, defined over the field of rational numbers $\mathbf{Q}$. Its set of rational points $X(\mathbf{Q})$, which consists of all the projective solutions with rational coordinates to a finite set of equations defining X in some projective space, is an interesting arithmetic quantity. In 1922, Mordell [Mor22] made the following conjecture:

Conjecture 1.1 (Mordell)**.** *Suppose that X is of genus at least two. Then $X(\mathbf{Q})$ is finite.*

In a monumental paper, Faltings [Fal83] proved this conjecture. The method of Faltings is ingenious, and merits a thorough treatment on its own. Indeed, many such are available in the literature, see for instance [CS86] for an early account. In this paper, we wish to give an introductory account of two recent alternative approaches towards this conjecture, due to Lawrence–Venkatesh [LV18] and Kim [Kim05, Kim09, Kim10]. The latter method, which is usually called the method of *Chabauty–Kim* or *non-abelian Chabauty* in the literature, has the advantage that in some cases it has been turned into an effective method to *determine* the set of rational points $X(\mathbf{Q})$, and we illustrate this by presenting three new examples of modular curves where this set can be determined, due to Best, Bianchi, and Triantafillou.

Remark 1.2. Mordell's conjecture, as well as many of the results discussed below, admit analogues where X is replaced by a smooth *hyperbolic curve*, including also the cases of a punctured elliptic curve and

$\mathbf{P}^1 \setminus \{0,1,\infty\}$, when the set of rational points $X(\mathbf{Q})$ is replaced by the set of S-integral points, where S is a finite set of primes. See also our discussion of the S-unit equation below.

Remark 1.3. For the purpose of exposition, we only consider the base field $\mathbf{Q}$. It should be noted that many results admit appropriate generalizations to number fields [Sik13, Dog19, BBBM19]. The only exception is our discussion of the method of Lawrence–Venkatesh, where field extensions play an essential role.

1.2. **Two recent approaches.** After Faltings' proof, two notable new methods for proving finiteness of $X(\mathbf{Q})$ for X of genus $g \geq 2$ have emerged. In broad strokes, they follow a similar strategy: We start by choosing a prime p at which the curve X has good reduction, and we study the set of rational points through the inclusion

$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p). \tag{1}$$

For any field K, we write $G_K = \mathrm{Gal}(\overline{K}/K)$ for its absolute Galois group. The starting point of both the methods of Chabauty–Kim and Lawrence–Venkatesh is the association of a certain finite-dimensional Galois representation over $\mathbf{Q}_p$ to every point on the curve, giving maps

$$\rho : X(K) \longrightarrow \mathrm{Rep}(G_K), \tag{2}$$

for K equal to $\mathbf{Q}$ or $\mathbf{Q}_p$. In both the approaches of Lawrence–Venkatesh and Chabauty–Kim, finiteness of the set $X(\mathbf{Q})$ is obtained from the consideration of a commutative diagram of the following shape:

(3)
$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r] \arrow[d, "\rho"'] & X(\mathbf{Q}_p) \arrow[d, "\rho"'] \arrow[rd, dashed, bend left, "\mathrm{per}_p"] & \\
\mathrm{Rep}(G_{\mathbf{Q}}) \arrow[r, "\mathrm{res}_p"] & \mathrm{Rep}(G_{\mathbf{Q}_p}) \arrow[r, "\mathrm{D}_{\mathrm{cris}}"] & \mathrm{MF}^{\phi}/\simeq.
\end{tikzcd}$$

While the nature of ρ is very different in the two approaches, the horizontal maps are the same. First of all, the map from $X(\mathbf{Q})$ to $X(\mathbf{Q}_p)$ is simply the natural inclusion, and res_p is the restriction of Galois representations, making the diagram commutative in both approaches. The map $\mathrm{D}_{\mathrm{cris}}$ is defined using p-adic Hodge theory. More precisely, it is Fontaine's crystalline Dieudonné functor from p-adic Galois representations to filtered ϕ-modules. Finally, per_p is defined to be the composite of this map with ρ, and will be referred to as the (p-adic) *period map*.

As mentioned above, the maps ρ which feature in the methods of Lawrence–Venkatesh and Chabauty–Kim are of a very different nature, and are responsible for the drastic differences between the two approaches. They may roughly be described as follows:

- The method of Lawrence–Venkatesh starts by considering a family of curves $\mathcal{C} \longrightarrow X$. This is a so-called *Parshin family*, where the fibre $\mathcal{C}_x$ of a point x in $X(K)$ is itself a disjoint union of finite coverings of X, unramified away from the point x. The association ρ is then simply

  $$\rho : \ x \longmapsto \mathrm{H}^1_{\text{ét}}(\overline{\mathcal{C}}_x, \mathbf{Q}_p).$$

  A lemma of Faltings can be used to show that the number of global representations in $\rho(X(\mathbf{Q}_p))$ is finite. The main part of the argument of Lawrence–Venkatesh is to establish that the map per_p is finite-to-one. The argument starts by realizing per_p as the quotient of the Hodge filtration map $\Phi_p : X(\mathbf{Q}_p) \longrightarrow \mathrm{Gr}(g,2g)$ by the Frobenius centralizer, and showing that on every residue disk
  (1) every orbit of the Frobenius centralizer has positive codimension in $\mathrm{Gr}(g,2g)$, and
  (2) the image of Φ_p is Zariski dense.

The former is established via carefully extending the base field and exploiting the semi-linearity of the Frobenius operator, whereas the latter is established using a monodromy calculation for the family $\mathcal{C}$. The finiteness of $X(\mathbf{Q})$ follows easily from the above commutative diagram.

- In the method of Chabauty–Kim, one chooses a rational base point $b \in X(\mathbf{Q})$ and obtains the association ρ by considering certain well-chosen *unipotent* quotients $\mathrm{U}(b)$ of the algebraic fundamental group $\pi_1^{\text{ét}}(\overline{X}; b)$. This choice of quotient typically depends on the specifics of the curve X under consideration. The association ρ in the method of Chabauty–Kim is then of the form

$$\rho : \; x \longmapsto \mathrm{U}(b, x)$$

where $\mathrm{U}(b,x)$ is obtained by twisting the unipotent quotient $\mathrm{U}(b)$ by the path torsor $\pi_1^{\text{ét}}(\overline{X}; b, x)$. This carries the structure of a $\mathbf{Q}_p$-representation of G_K whenever x is in $X(K)$. All these Galois representations are twists of $\mathrm{U}(b)$, whose unipotence provides a certain rigidity that is crucial for arithmetic applications. More precisely, Kim shows that the image of ρ is contained in a set that naturally carries the structure of an algebraic variety, which is usually referred to as a *Selmer variety*, such that the map res_p between the global and local Selmer varieties is algebraic.

This rigidity provides us with a clear strategy to prove finiteness, in the style of the classical method of Chabauty (see below). Indeed, if we can establish that

(1) the global Selmer variety has positive codimension in the local Selmer variety, and
(2) the image of $X(\mathbf{Q}_p)$ is Zariski dense,

then the intersection of the two sets (which contains the set of rational points) must be finite. Property (2) is true in great generality, whereas (1) typically requires additional information. Note the amusing similarity with the two steps in the proof of Lawrence–Venkatesh discussed above.

In spite of the apparent similarity of the two strategies, the different nature of the maps ρ already lays bare a crucial difference: In contrast with the unconditional proof of Lawrence–Venkatesh, an additional piece of information is needed to deduce finiteness from the method of Chabauty–Kim. Typically this either takes the form of a *geometric* assumption, such as having a large Néron–Severi rank [BD18, BD19a], or the assumption of a geometric conjecture, such as the Bloch–Kato conjecture, see [Kim09].

1.3. **Finding rational points explicitly.** At first glance, it may seem from the above comments that the conditional nature of the proof of finiteness obtained from the method of Chabauty–Kim puts the method at a significant disadvantage, especially when compared to the unconditional proof of Lawrence–Venkatesh. However, recent developments [BD18, BD19a, BDM+19] have shown that in certain examples where additional geometric information is known, the method for proving finiteness can in fact be turned into a method to *explicitly determine* the finite set $X(\mathbf{Q})$.

To explain the ideas, we briefly remind the reader of the method of Chabauty–Coleman [Cha41, Col85], of which an excellent exposition may be found in McCallum–Poonen [MP12]. In this method, one chooses a rational base point b in $X(\mathbf{Q})$ and attaches to every other point a torsor of the p-adic Tate module V of the Jacobian J. More precisely, if K is either $\mathbf{Q}$ or $\mathbf{Q}_p$, this torsor is obtained by the composition

$$\rho \;:\; X(K) \longrightarrow J(K) \longrightarrow \mathrm{H}^1_f(G_K, V) \tag{4}$$

where the first map is the Abel–Jacobi embedding attached to the choice of base point b, and the second map attaches to a point x in $J(K)$ the torsor of V obtained from the inverse limit of the preimages of x

under the multiplication-by-p^n map on the Jacobian, i.e.

$$\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \left(\varprojlim_n \, [p^n]^{-1}(x) \right). \tag{5}$$

Such torsors are classified by the cohomology group $\mathrm{H}^1(G_K, V)$ and satisfy certain *Selmer conditions*[1] which are denoted by the subscript f. This association ρ is familiar from the context of the classical method of descent, used to compute the Mordell–Weil group of the Jacobian.

We now obtain the commutative diagram:

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r] \arrow[d, "\rho"'] & X(\mathbf{Q}_p) \arrow[d, "\rho"'] \arrow[dr, dashed, bend left, "\mathrm{per}_p"] & \\ \mathrm{H}^1_f(G_{\mathbf{Q}}, V) \arrow[r, "\mathrm{res}_p"] & \mathrm{H}^1_f(G_{\mathbf{Q}_p}, V) \arrow[r, "\sim"] & \mathrm{H}^0(X, \Omega^1_X)^\vee \end{tikzcd} \tag{6}$$

representing perhaps the simplest instance of the Chabauty–Kim strategy towards the Mordell conjecture discussed above, where U is taken to be the *abelianization* V of the fundamental group. In this situation, the relevant filtered ϕ-modules are classified by the dual to the space of holomorphic differentials on X, which is of dimension g, and the isomorphism is provided by the Bloch–Kato logarithm. With suitable finiteness conditions f, the dimension of $\mathrm{H}^1_f(G_{\mathbf{Q}}, V)$ can be bounded above by the rank r of the $\mathbf{Q}$-rational points of the Jacobian of X. The discussion of how to prove finiteness of $X(\mathbf{Q})$ using the method of Chabauty–Kim then specializes to the classical argument of Chabauty, who deduces finiteness under the assumption that $r < g$.

Going one step further, we note that the p-adic period map per_p has the following concrete description:

$$\mathrm{per}_p(x) = \left(\omega \longmapsto \int_b^x \omega \right) \tag{7}$$

where the integration is taken in the sense of Coleman [Col85]. Our ability to compute Coleman integrals [BBK10, Bal15, BT19] often results in an explicit determination of the set $X(\mathbf{Q})$. Since there already exist several excellent expositions of this method [MP12], we will simply explain the method by showing it in action for a single example.

Example. Let X be the genus 3 hyperelliptic curve with minimal model[2]

$$w^2 + (z^4 + z^2 + z + 1)w = -z^5 - z^2.$$

A search for points with small coordinates gives that

$$\{\infty^\pm, (-1,-2), (-1,0), (0,-1), (0,0)\} \subseteq X(\mathbf{Q}), \tag{8}$$

where $\infty^+ = (1:0:0)$ and $\infty^- = (1:-1:0)$ are the points at infinity. In order to determine the full set of rational points $X(\mathbf{Q})$, we apply the Chabauty–Coleman method with $p = 3$; for convenience, we work with the following model for X:

$$X' \colon w^2 = z^8 + 2z^6 - 2z^5 + 3z^4 + 2z^3 - z^2 + 2z + 1.$$

We embed X' into its Jacobian J via the Abel–Jacobi map corresponding to the base point $b = (0,1)$ in $X'(\mathbf{Q})$. A computation in `Magma` [BCP97] shows that the Mordell–Weil rank of J is equal to 1, and the

[1] We are deliberately vague about these finiteness conditions here, but mention that the discussion below can be made unconditional on the finiteness of the Tate–Shafarevich group of the Jacobian.

[2] Here X is the curve of absolute discriminant and conductor both equal to $60329 = 23 \cdot 43 \cdot 61$ from the database [BPSS].

above discussion then implies that the codimension of the image of res_3 is at least 2. In fact, it is precisely equal to 2: the set $\left\{\omega_i = z^i \frac{dz}{w} : 0 \leq i \leq 2\right\}$ is a basis for $\mathrm{H}^0(X', \Omega^1_{X'})$ and we have

$$\begin{aligned} \mathrm{per}_3(0,-1)(\omega_0) &\equiv 3(3 + 3^3 + 2\cdot 3^4) && \bmod 3^6 \\ \mathrm{per}_3(0,-1)(\omega_1) &\equiv 3(1 + 3^3 + 3^4) && \bmod 3^6 \\ \mathrm{per}_3(0,-1)(\omega_2) &\equiv 3(1 + 3^2 + 2\cdot 3^3 + 2\cdot 3^4) && \bmod 3^6. \end{aligned}$$

Thus, we may choose generators $\alpha = a_0\omega_0 - a_1\omega_1$ and $\beta = b_0\omega_0 - b_2\omega_2$ for the $\mathbf{Q}_3$-vector space

$$\left\{\omega \in \mathrm{H}^0(X', \Omega^1_{X'}) : \mathrm{res}_3(c)(\omega) = 0 \text{ for all } c \in \mathrm{H}^1_f(G_{\mathbf{Q}}, V)\right\}$$

such that

$$\begin{array}{lllllll} a_0 & \equiv & 1 + 3^3 + 3^4 & \bmod 3^5 & a_1 & \equiv & 3 + 3^3 + 2\cdot 3^4 \quad \bmod 3^5 \\ b_0 & \equiv & 1 + 3^2 + 2\cdot 3^3 + 2\cdot 3^4 & \bmod 3^5 & b_2 & \equiv & 3 + 3^3 + 2\cdot 3^4 \quad \bmod 3^5. \end{array} \tag{9}$$

By construction, we have

$$X'(\mathbf{Q}) \subseteq \{x \in X'(\mathbf{Q}_3) : \mathrm{per}_3(x)(\alpha) = 0 \text{ and } \mathrm{per}_3(x)(\beta) = 0\} =: \mathcal{T}; \tag{10}$$

a computation shows that $\mathcal{T}$ contains precisely 6 points and hence that the inclusion in (8) is in fact an equality. Explicitly, suppose for instance that we want to compute all $x \in \mathcal{T}$ which reduce to the point $(1:1:0)$ in $X'(\mathbf{F}_3)$. For $\gamma \in \{\alpha, \beta\}$ we have

$$\mathrm{per}_3(x)(\gamma) = \mathrm{per}_3(1:1:0)(\gamma) + \int_{(1:1:0)}^{x} \gamma = \int_{(1:1:0)}^{x} \gamma;$$

expanding in terms of the local parameter $t = z(x)^{-1}$ and formally integrating yields

$$\begin{aligned} \mathrm{per}_3(x)(\alpha) &= (2\cdot 3 + 3^2)\cdot t^2 + (2\cdot 3^{-1} + 2 + 2\cdot 3 + 3^2)\cdot t^3 && \bmod (3^3, t^4) \\ \mathrm{per}_3(x)(\beta) &= 3\cdot t + (2\cdot 3^{-1} + 1 + 3 + 2\cdot 3^2)\cdot t^3 && \bmod (3^3, t^4). \end{aligned}$$

The i-th coefficient of the local expansion of $\mathrm{per}_3(x)(\alpha)$ or $\mathrm{per}_3(x)(\beta)$ has valuation bounded from below by $-\mathrm{ord}_3(i)$; from Newton polygon considerations, we deduce that

- $\mathrm{per}_3(x)(\alpha)$ has a double zero at $t = 0$, a simple zero at some $t \in \mathbf{Z}_3$ which satisfies $t \equiv 2\cdot 3^2 \bmod 3^3$, and no other zero in $3\,\mathbf{Z}_3$;
- $\mathrm{per}_3(x)(\beta)$ has a simple zero at $t = 0$, two simple zeros congruent modulo 3^2 to $2\cdot 3$ and 3, respectively, and no other zero in $3\,\mathbf{Z}_3$.

Therefore, the intersection of the zero sets of $\mathrm{per}_3(x)(\alpha)$ and $\mathrm{per}_3(x)(\beta)$ in the residue disk of the point $(1:1:0)$ in $X'(\mathbf{F}_3)$ is precisely $\{(1:1:0)\} \subset X'(\mathbf{Q})$.

We emphasize that neither α nor β on their own would have sufficed to determine $X(\mathbf{Q})$, as each of $\mathrm{per}_3(x)(\alpha)$ and $\mathrm{per}_3(x)(\beta)$ vanishes at some points $x \in X'(\mathbf{Q}_3) \setminus X'(\mathbf{Q})$ which we can only compute modulo 3^n for a choice of n. More generally, for curves X of genus g with rank $g-1$ Jacobians, the Chabauty–Coleman method typically provides us with only one locally analytic function whose zero set $\mathcal{T}$ contains $X(\mathbf{Q})$. It is then often the case that $\mathcal{T}$ contains some points that we cannot recognize as points in $X(\mathbf{Q})$. In such situations, the Mordell–Weil sieve (see §6.7 for a discussion) can often be used to prove that the p-adic approximations of these points that we have computed cannot be approximations of points in $X(\mathbf{Q})$.

2. The method of Lawrence–Venkatesh: Finiteness

In this section, we will discuss the main ideas of the approach towards Mordell's conjecture due to Lawrence and Venkatesh. For simplicity, our main focus will be to explain the method in the case of $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ where the proof is especially simple. Finally, we make some comments about the obstacles one faces in making this approach effective, in the example of the 2-unit equation.

Recall from the introduction that we start by constructing a map ρ which attaches a Galois representation to any point on X. In the method of Lawrence–Venkatesh, the map ρ arises from the cohomology of the fibres of a certain Parshin family $\mathcal{C} \longrightarrow X$, see §2.2. In the case of $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$, which we discuss first, this family is a simple modification of the classical *Legendre family* of elliptic curves.

2.1. **The S-unit equation.** To explain some of the ideas in the proof, we discuss the case of the S-unit equation in more detail. This has the benefit of being substantially simpler, while still containing many of the main ideas that go into the proof of the Mordell conjecture. To illustrate the ideas of the proof, we will start with a version of the Parshin family for which the period map per_p fails to be finite-to-one. Then we will give a correct argument, in which a nontrivial Galois action on H^0 of the fibers supplies the key missing ingredient.

Take $K = \mathbf{Q}$ and S a finite set of primes. We denote the set of S-units by $\mathcal{O}_S^\times$ and will consider the *S-unit equation* given by

$$x + y = 1, \qquad x, y \in \mathcal{O}_S^\times, \tag{11}$$

whose solution set is finite by Siegel's theorem. This statement represents an attractive toy case for the Mordell conjecture; its geometric proof along the lines sketched above takes place on $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$. Note that we may enlarge S without loss of generality, so that we may as well assume that S contains 2.

The role of the Parshin family is played by the *Legendre family* over $\mathcal{O}_S$. Denoting x for the coordinate on $\mathcal{X} = \mathbf{P}^1_{\mathcal{O}_S} \setminus \{0, 1, \infty\}$, this family $\mathcal{C} \longrightarrow \mathcal{X}$ is given by the equation

$$\mathcal{C} \;:\; w^2 = z(z-1)(z-x). \tag{12}$$

This family gives us a Galois representation $\rho(x)$ on the étale cohomology group $\mathrm{H}^1_{\text{ét}}(\mathcal{C}_{\overline{x}}, \mathbf{Q}_p)$, where p is a prime not below any places in S, which is unramified in K. This gives the following diagram:

$$\begin{tikzcd}
\mathcal{X}(\mathcal{O}_S) \arrow[r] \arrow[d, "\rho"'] & \mathcal{X}(\mathcal{O}_v) \arrow[d, "\rho"'] \arrow[dr, dashed, "\mathrm{per}_p"] & \\
\{\text{Iso classes } \rho\} \arrow[r] & \{\text{Iso classes } \rho_v\} \arrow[r, "\mathrm{D_{cris}}"] & \mathrm{MF}^{\phi}/\simeq \; .
\end{tikzcd} \tag{13}$$

Let us now make a first attempt to deduce finiteness from the above diagram. There are two major considerations to the strategy, corresponding to *global* and *local* aspects. The local considerations revolve around a careful analysis of the period map, via a monodromy calculation.

a. Global representations. The Mordell conjecture will ultimately be reduced to a finiteness statement about a certain set of global Galois representations, due to Faltings. More precisely, the proof of [Fal83, Satz 5] deduces the following consequence from the classical theorem of Hermite–Minkowski:

Lemma 2.1. *Fix integers $w, d \geqslant 0$, and fix a number field K and a finite set S of primes of $\mathcal{O}_K$. There are, up to conjugation, only finitely many semisimple Galois representations $\rho : G_K \to \mathrm{GL}_d(\mathbf{Q}_p)$ such that*

(a) *ρ is unramified outside S, and*
(b) *ρ is pure of weight w, i.e. for every prime $\mathfrak{p} \notin S$ all the eigenvalues of Frobenius at $\mathfrak{p}$ are algebraic integers, all of whose conjugates have complex absolute value $|\mathcal{O}_K/\mathfrak{p}|^{w/2}$.*

It should be noted that this does not make the approach of Lawrence–Venkatesh depend on the work of Faltings in an essential way, as this lemma is comparatively simple in Faltings' overall argument.

The semisimplicity hypothesis in Faltings' lemma is essential: there can be infinitely many nontrivial extensions between Galois representations. [3] In fact, Faltings shows that all the representations we consider—which arise as subquotients of the étale cohomology of a curve—are semisimple. This fact requires the full weight of Faltings' argument in [Fal83]. In order to give an independent proof of Mordell's conjecture, it is necessary to contemplate the possibility that some of these representations might not be semisimple. In potential algorithmic applications, we know this situation cannot arise, so we will content ourselves here with mentioning that in [LV18] this is addressed by showing that all but finitely many representations in our family must be simple. This is a consequence of results of the following form:

(1) If the global representation $\rho(x)$ has a (global) subrepresentation, then the local representation must be of a particularly special form.
(2) There are finitely many x in $X(\mathbf{Q}_p)$ where the local representation $\rho(x)$ takes this special form.

b. The period map. The more subtle points of the argument of Lawrence–Venkatesh lie in the study of the period map per_p, where one systematically enlarges the base field to gain control over the Frobenius centralizers. Let us explain the need for this step, by first approaching the problem naively using the unadjusted Legendre family above.

Recall that we want to show finiteness of the set of solutions to the S-unit equation. Since we already established the finiteness of the set of isomorphism classes of global representations $\rho(x)$ that can arise, it is tempting to try and show that the fibres of the period map per_p are finite. However, this is **not** true: The filtered ϕ-modules that arise in the image of per_p necessarily are of the form $\mathrm{H}^1_{\mathrm{dR}}(\mathcal{C}_x, \mathbf{Q}_p)$, and on every good residue disk of $X(\mathbf{Q}_p)$ the Frobenius operator ϕ has a constant characteristic polynomial

$$f = aT^2 + bT + c \quad \in \mathbf{Z}_p[T] \tag{14}$$

which has two roots in $\mathbf{C}_p$ whose valuations sum up to 1. The number of residue disks is finite, and for each of these finitely many polynomials f, the filtered ϕ-module belongs to a finite number of possible isomorphism classes, which is most easily seen with a simple case-by-case analysis:

- If f is irreducible, then we may pick a basis e_1 for Fil^1 and set $e_2 = \phi(e_1)$. Then $\{e_1, e_2\}$ is a basis for $\mathrm{H}^1_{\mathrm{dR}}$. With respect to this basis, we have $\mathrm{Fil}^1 = \langle e_1 \rangle$ and
$$\phi = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}.$$
- If f is reducible, then it must have distinct roots of valuations 0 and 1, corresponding to eigenvectors e_1, e_2 which necessarily span $\mathrm{H}^1_{\mathrm{dR}}$. Then we either have $\mathrm{Fil}^1 = \langle e_1 \rangle$ or $\langle e_2 \rangle$, or we can rescale the eigenvectors to obtain $\mathrm{Fil}^1 = \langle e_1 + e_2 \rangle$.

[3] As we will see in the next section, the existence of families of non-trivial extensions of a fixed set of Galois representations is precisely what underlies the method of Chabauty–Kim.

In conclusion, we see that there is only a *finite number* of possible isomorphism classes of filtered ϕ-modules attached to the representations $\rho(x)$, and therefore the period map appearing in (13) cannot possibly have finite fibres! Furthermore, we see from this discussion exactly what the problem is, since we had in each case so much freedom in choosing our basis, so as to move around the Hodge filtration Fil^1 while respecting the Frobenius operator.

We can rephrase the problem as follows. Fix a pair (V, ϕ) of a two-dimensional vector space and linear endomorphism; in our situation, (V, ϕ) will arise as the crystalline cohomology $\mathrm{H}^1_{\text{cris}}(\mathcal{C}_x \,/\, \mathbf{Z}_p)$, which only depends on the reduction of x modulo p. The possible filtrations $\mathrm{Fil}^1 \subseteq V$ are classified by the Grassmannian $\mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$. The centralizer $Z(\phi)$ acts on $\mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$, and the orbits of this action are in bijection with isomorphism classes $(V, \phi, \mathrm{Fil}^1)$ of filtered ϕ-module with underlying ϕ-module (V, ϕ). In the setting just described, $Z(\phi)$ has a Zariski-dense orbit on $\mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$, so most such filtered ϕ-modules belong to a single isomorphism class.

Interlude: Semilinearity. Let us take a short break to recall some crystalline theory. So far we have been applying p-adic Hodge theory, in particular the crystalline comparison theorem, to schemes $\mathcal{C}_x$ over $\mathbf{Q}_p$. In general, suppose L_p is an unramified extension of $\mathbf{Q}_p$, and $\mathcal{C}_x$ is a scheme over L_p, admitting a smooth model over $\mathcal{O}_{L_p}$. Then L_p is Galois over $\mathbf{Q}_p$, with cyclic Galois group generated by a Frobenius element Fr that acts as the p-th power map on the residue field. The crystalline-de Rham cohomology $\mathrm{H}^1_{\text{dR}}(\mathcal{C}_x \,/ L_p)$ has the structure of a filtered ϕ-module, where ϕ is now a *semilinear* operator: it satisfies

$$\phi(\lambda v) = \mathrm{Fr}(\lambda)\phi(v). \tag{15}$$

This is important because semilinear automorphisms have small centralizers: it's not easy for an automorphism of V to both respect the action of L_p and commute with ϕ. This is made precise in the following lemma, which was proved in Lawrence–Venkatesh [LV18, Lemma 2.1].

Lemma 2.2. *Let L_p be an unramified extension of $\mathbf{Q}_p$ of degree e, and let $\mathrm{Fr} : L_p \to L_p$ be the Frobenius endomorphism that acts as the p-th power map on the residue field. Let V be an L_p-vector space of dimension d, and $\phi : V \to V$ a Fr-semilinear automorphism. Define the centralizer $\mathrm{Z}(\phi)$ of ϕ in the ring of L_p-linear endomorphisms of V via*

$$\mathrm{Z}(\phi) = \{f : V \longrightarrow V \text{ an } L_p\text{-linear map}, \quad f\phi = \phi f\};$$

it is a $\mathbf{Q}_p$-vector space. Then

$$\dim_{\mathbf{Q}_p} \mathrm{Z}(\phi) = \dim_{L_p} \mathrm{Z}(\phi^e),$$

where $\phi^e : V \to V$ is now L_p-linear. In particular, $\dim_{\mathbf{Q}_p} \mathrm{Z}(\phi) \leqslant (\dim_{L_p} V)^2$.

c. Finiteness. Armed with this tool, we now return to the failed finiteness argument above, and take advantage of semilinearity to resolve the issues we were having. More precisely, we bound the size of Frobenius centralizers by considering instead the modified Parshin family

$$E : w^2 = z(z-1)(z-t), \qquad t^8 = x. \tag{16}$$

For every field K and x in $X(K)$, the fiber E_x is a geometrically disconnected curve whose H^0 is the algebra $K[t]/(t^8 - x)$. Suppose $K = \mathbf{Q}_p$ and x is a unit in $\mathbf{Q}_p$ which is not a square[4]. Then E_x is a curve defined

[4] It is enough to consider x of this form by an elementary argument based on the fact that, if x is both a square and a solution to the S-unit equation in some number field K, then $\pm\sqrt{x}$ satisfy the S-unit equation as well. However, this does necessitate some care in the choice of p.

over $L_p = \mathbf{Q}_p[x^{1/8}]$, the degree-8 unramified extension of $\mathbf{Q}_p$. We want to show that the map

$$\mathrm{per}_p : \mathcal{X}(\mathcal{O}_v) \longrightarrow (\mathrm{MF}^\phi / \simeq)$$

is finite-to-one. On each p-adic residue disk $\Omega_v \subseteq \mathcal{X}(\mathcal{O}_v)$, the ϕ-module $(V, \phi) = \mathrm{H}^1_{\text{cris}}(E_x)$ is constant; only the filtration varies. Thus we can regard per_p as a map

$$\mathrm{per}_p : \Omega_v \longrightarrow \mathrm{Gr}(\mathrm{Fil}^1 \subseteq V) \longrightarrow \mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)/Z(\phi)\,.$$

Since per_p is an analytic map from a one-dimensional source, to show it is finite-to-one, we need only show that it is not constant; in other words, that the image of $\Phi_p \colon \Omega_v \to \mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$ is not contained in a single orbit of $Z(\phi)$. This follows from the following two results:

(1) Every orbit of $Z(\phi)$ has positive codimension in $\mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$.
(2) The image of Φ_p is Zariski dense.

The first of these two follows from the bound in Lemma 2.2; the second, from a complex monodromy calculation. It is essential that L_p have large degree over $\mathbf{Q}_p$, which comes from the assumption that x is not a square in $\mathbf{Q}_p$.

The Zariski density of the image of Φ_p is obtained by comparing it with the complex period map $\Phi_{\mathbf{C}}$. Let's recall the construction of $\Phi_{\mathbf{C}}$. The family E of elliptic curves over X gives rise to a variation of Hodge structure on X. Let $\Omega_{\mathbf{C}}$ be a contractible open subset of X^{an}, containing some basepoint x_0 in $X(K)$, for K a number field. Over $\Omega_{\mathbf{C}}$, the family E splits as the disjoint union of eight families of elliptic curves $E^{(1)}, \ldots, E^{(8)}$. (The monodromy action of $\pi_1(X)$ preserves the splitting but permutes the eight components.) Choose an integral basis $\mathbf{B}$ for the fiberwise Betti cohomology of each elliptic curve $V_{\mathbf{C}}^{(i)} = \mathrm{H}^1_B(E^{(i)}_{x_0})$ over x_0. With respect to this basis, the Hodge filtration is described by a map

$$\Phi_{\mathbf{C}} \colon \Omega_{\mathbf{C}} \longrightarrow \prod_{i=1}^{8} \mathrm{Gr}(\mathrm{Fil}^1 \subseteq V^{(i)}),$$

where the Grassmannian classifies one-dimensional subspaces of the two-dimensional $V^{(i)}$.

The importance of $\Phi_{\mathbf{C}}$ to us comes from the fact that $\Phi_{\mathbf{C}}$ and Φ_p are, in a suitable sense, the same. (See [LV18, Section 3.4] for details.) Both period maps satisfy the same algebraic differential equation, coming from the Gauss–Manin connection. It follows that in suitable local coordinates, the (complex) power series representation of $\Phi_{\mathbf{C}}$ and the (p-adic) power series representation of Φ_p both have all their coefficients in the number field K, and the two power series agree. This means we can compare the images of the two period maps, and Lemmas 3.1 and 3.2 of [LV18] yield the following result:

Lemma 2.3. *The image of $\Phi_{\mathbf{C}}$ is Zariski dense if and only if the image of Φ_p is Zariski dense.*

The advantage of this result is that establishing the Zariski-density of the map $\Phi_{\mathbf{C}}$ boils down to an explicit monodromy calculation, see [LV18, Eqn. 3.11].

Lemma 2.4. *If the image of the monodromy representation of E contains a Zariski-dense subset of Sp_2^d, then the image of $\Phi_{\mathbf{C}}$ is Zariski dense in $\mathrm{Gr}(\mathrm{Fil}^1 \subseteq V)$.*

Proof. Let $\widetilde{X}$ be the universal cover of X, and extend $\Phi_{\mathbf{C}}$ to a map

$$\Phi_{\mathbf{C}} \colon \widetilde{X} \longrightarrow \mathrm{Gr}(\mathrm{Fil}^1 \subseteq V).$$

This map $\Phi_{\mathbf{C}}$ is $\pi_1(X)$-equivariant, where $\pi_1(X)$ acts on the Grassmannian through the monodromy representation. Since the image of monodromy is Zariski dense, the extended $\Phi_{\mathbf{C}}$ has Zariski-dense image. By analytic continuation, the restriction of $\Phi_{\mathbf{C}}$ to $\Omega_{\mathbf{C}}$ has Zariski-dense image as well. □

Lemma 2.5. *The image of the monodromy representation*

$$\pi_1(X, x_0) \longrightarrow \operatorname{Aut}\left(\prod_{i=1}^{8} \mathrm{H}^1_B(E^{(i)}_{x_0})\right)$$

contains a Zariski-dense subset of $\mathrm{Sp}_2(\mathbf{Z})^8$.

Proof. This is a calculation in classical topology, see [LV18, Lemma 4.3]. □

2.2. **The Mordell conjecture over general K.** After our discussion of the S-unit equation, we now make a brief foray into the general case, and outline how to adapt this argument to prove Mordell's conjecture. Suppose X is a smooth projective curve of genus at least 2 over K. We will define the *Parshin family* over X, implicitly dependent on a parameter q. It will replace the Legendre family in the S-unit argument.

Let $q \geq 3$ be a prime number, and let $\mathrm{Aff}(q)$ be the non-abelian group of affine-linear transformations $x \mapsto ax + b$ over $\mathbf{F}_q$. The action of $\mathrm{Aff}(q)$ on $\mathbf{F}_q$ realizes $\mathrm{Aff}(q)$ as a subgroup of the symmetric group S_q. Note also that $\mathrm{Aff}(q)$ surjects onto $\mathbf{F}_q^\times$.

Definition 2.6. *Let X be a curve over K, and $x \in X(K)$ a point of X. An $\mathrm{Aff}(q)$-cover of X, branched at x, is a curve Z and a map $Z \to X$, satisfying the following properties.*

- *$Z \to X$ is étale over $X - \{x\}$, but not étale over x.*
- *$Z \to X$ is of degree q.*
- *For any choice of basepoint x_0, and for an appropriate identification of the fiber over x_0 with $\mathbf{F}_q$, the monodromy map $\pi_1(X, x_0) \to S_q$ corresponding to the cover Z has image $\mathrm{Aff}(q)$.*

For every x in $X(K)$, there are finitely many isomorphism classes of $\mathrm{Aff}(q)$-covers $Z \to X$ branched at x. The Parshin family $Y \to X$ is characterized by the property that the fiber Y_x is geometrically the disjoint union of these finitely many curves.

In the S-unit argument, the key semilinearity bound came from taking an 8-th root of x (along with the elementary assumption that x is not a square). Here the corresponding bound comes from the torsion on the Jacobian J of X, which is guaranteed to have a nontrivial Galois structure. Specifically, for any $\mathrm{Aff}(q)$-cover of X, the composed map

$$\pi_1(X - \{x\}) \longrightarrow \mathrm{Aff}(q) \longrightarrow \mathbf{F}_q^\times$$

gives a degree-$(q-1)$ cover of X that turns out to be unramified everywhere, even over x. This cover in turn corresponds to a $(q-1)$-torsion point on the dual of the Jacobian. We choose q and p so that the Frobenius at p acts with sufficiently large orbits on $J[q-1]$; this in turn guarantees that the components of each fiber Y_x are defined over large p-adic fields, so we can leverage the semilinearity lemma 2.2.

As with the S-unit equation, a calculation in the classical topology is needed to show that the Parshin family has big monodromy. Fix X and x, and let $Z_1, \ldots, Z_N$ be the $\mathrm{Aff}(q)$-covers of X branched at x. We want to determine the image of the monodromy action

$$\mathrm{Mon}\colon \pi_1(X, x) \longrightarrow \operatorname{Aut}\left(\prod_i \mathrm{H}^1_B(Z_i)\right)$$

as an algebraic group. The cohomology of each Z_i contains a copy of $\mathrm{H}^1_B(X)$; define[5]

$$\mathrm{H}^1_{\mathrm{Pr}}(Z_i) = \mathrm{H}^1_B(Z_i)/\, \mathrm{H}^1_B(X).$$

The map Mon descends to an automorphism of $\prod_i \mathrm{H}^1_{\mathrm{Pr}}(Z_i)$. We need the following big monodromy result.

Theorem 2.7. *The Zariski closure of the image of*

$$\mathrm{Mon}\colon \pi_1(X, x) \longrightarrow \mathrm{Aut}\left(\prod_i \mathrm{H}^1_{\mathrm{Pr}}(Z_i)\right)$$

contains the group

$$\prod_i \mathrm{Sp}(\mathrm{H}^1_{\mathrm{Pr}}(Z_i)).$$

This theorem is really saying that the image of monodromy is as big as possible: we know for abstract reasons that the identity component of the Zariski closure of the image is no larger than the product of symplectic groups. We say a few words about the main ideas that go into the proof:

The monodromy action of $\pi_1(X, x)$ on the covers Z_i extends to an action of the full mapping class group[6] $\mathrm{MCG}(X - \{x\})$. By the Birman exact sequence, $\pi_1(X, x)$ is a normal subgroup of $\mathrm{MCG}(X - \{x\})$. Since the symplectic group is simple modulo center, we can deduce Theorem 2.7 if we know that the Zariski closure of the image of

$$\mathrm{Mon}\colon \mathrm{MCG}(X - \{x\}) \longrightarrow \mathrm{Aut}\left(\prod_i \mathrm{H}^1_{\mathrm{Pr}}(Z_i)\right)$$

contains said product of symplectic groups. The benefit to working with the full mapping class group is that we now have access to Dehn twists, a particularly simple class of automorphism that is amenable to explicit calculation. Dehn twists map to unipotent automorphisms via Mon, and the proof concludes by producing a collection of unipotent automorphisms that generates the full symplectic group.

The study of mapping class group representations like Mon is a big subject in geometric topology. Looijenga [Loo97] studied the analogous question for abelian covers. Grunewald, Larsen, Lubotzky, and Malestein [GLLM15] study (unramified) covers of *compact* surfaces, and in a recent paper [ST18] Salter and Tshishiku study covers whose covering group is the Heisenberg group. These results are stronger than ours: they all show that the image of the representation has finite index in an appropriate arithmetic group, rather than merely being Zariski dense.

3. The method of Lawrence–Venkatesh: Effectivity

We now discuss the extent to which we expect the work of Lawrence–Venkatesh to yield a method for *explicitly determining* the set $X(K)$ in examples. Since it is so recent, it is unsurprising that this aspect of the method of Lawrence–Venkatesh does not yet seem to be addressed in the literature. In this section we adopt a more speculative tone, merely making some brief comments about various ingredients that would likely be needed to parlay this method into an algorithm for bounding the number of rational points on a curve over a number field; which would yield, in a weak sense, a form of "algorithmic Mordell."

Roughly speaking, a potential form of such a hoped-for algorithm is as follows.

[5] The symbol "Pr" stands for "primitive."

[6] The mapping class group is the group of *topological* automorphisms of the topological surface X fixing the point x, up to isotopy fixing x. The book of Farb and Margalit [FM12] is an excellent introduction and reference on mapping class groups.

Algorithm 3.1. Take as input a number field K, a smooth projective curve X over K, and a power v^n of a good[7] prime ideal v of $\mathcal{O}_K$. Return as output a finite list of points[8] in $\mathcal{X}(\mathcal{O}_v)$, to any desired finite precision which is guaranteed to include all the rational points of X.

It should be mentioned that such an algorithm, until an efficient implementation proves the contrary, is at risk of being prohibitively slow so as to be useless from a practical standpoint. The essential difficulty lies in enumerating Galois representations with prescribed ramification; modularity results for the representations in question, if known, could speed up the algorithms significantly. One possible approach to the calculation is proposed in what follows. It has four essential components, each of which we briefly discuss below. It should be noted that whereas many of the separate ingredients have been extensively studied in the literature, the method of Lawrence–Venkatesh has so far not been made effective, and therefore the ideas in this section are tentative. It would be very interesting to explore the effectivity of this method further, and make a serious attempt at a computational version of this method.

Remark 3.2. An algorithm of the above form may return extraneous points, not corresponding to a rational point. This phenomenon arises also in Chabauty's method, though in the example in §1 it was circumvented by exhibiting two independent analytic sets, which was possible since $g - r = 2$. Likewise, it is conceivable that one can circumvent in the method of Lawrence–Venkatesh by varying the choice of q in the covering group $\mathrm{Aff}(q)$. Alternatively, one could attempt to apply the Mordell–Weil sieve, see §6.7.

3.1. **Enumerating global Galois representations.**

Faltings's finiteness lemma for Galois representations (Lemma 2.1) can be made effective; we expect this to be the most computation-intensive part of the algorithm. Recall that we want to enumerate all global Galois representations

$$\rho : G_K \longrightarrow \mathrm{GL}_d(\mathbf{Z}_p)$$

that could arise from our family, in the sense of Lemma 2.1. We know the following about ρ:

- We are given a finite set S of places of K, outside of which ρ is unramified.
- For every prime $\mathfrak{p} \notin S$, all the eigenvalues of Frobenius at $\mathfrak{p}$ are Weil numbers of weight 1/2.
- The representation ρ is semisimple.

On the one hand, we can list all possible mod-p^n representations for any n. First, one enumerates all possible residual representations

$$\rho_1 : G_K \longrightarrow \mathrm{GL}_d(\mathbf{F}_p).$$

This is a straightforward application of Hermite–Minkowski finiteness. The residual representation has finite image, so it corresponds to an extension L_1 of K of degree at most $|\mathrm{GL}_d(\mathbf{F}_p)|$. The ramification condition translates to a bound on the discriminant of L_1. One can find all possible number fields L_1 by a targeted Hunter search [Coh00, §9.3]. However, the time complexity of such a search (for fixed K and S) is doubly exponential in the degree $[L_1 : K]$, so it may be necessary to further refine the search using more specifics of the situation at hand.

Second, for each residual representation, one lifts successively to mod-p^n representations

$$\rho_n : G_K \longrightarrow \mathrm{GL}_d(\mathbf{Z}/p^n),$$

[7] The method of LV requires p to satisfy a certain Galois-theoretic condition; here we will simply call primes satisfying that condition "good" primes. The condition is needed to guarantee that a certain extension of K_p is of large degree, and is analogous to the requirement in the S-unit equation above that x not be a square in $\mathbf{Q}_p$. Choosing a good p presents no algorithmic difficulty.

[8] possibly with multiplicities

which correspond to a tower of fields L_n. The successive extensions L_{n+1}/L_n are abelian, so they can be found by class field theory. (Everything we need from class field theory can be done algorithmically; see [Coh00].) To do this, we need to compute ideal class groups and unit groups of number fields whose degrees grow exponentially in n; this is again a computationally expensive task.

On the other hand, given the residual representation ρ_1, the Faltings–Serre method (see for example [Del85]) allows one to compute effectively a finite set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ such that for any semisimple ρ lifting ρ_0, the *rational* representation

$$G_K \longrightarrow \mathrm{GL}_d(\mathbf{Q}_p)$$

is determined by the Frobenius traces

$$\mathrm{Tr}(\mathrm{Fr}_{\mathfrak{p}_i} | \rho)$$

at these finitely many primes. (In general, there may be multiple isomorphism classes of *integral* representation, as the rational representation may have more than one stable $\mathbf{Z}_p$-lattice.) The condition on Frobenius eigenvalues guarantees that there are only finitely many possible values for $\mathrm{Tr}(\mathrm{Fr}_{\mathfrak{p}_i} | \rho)$, for each i. We can choose n_0 large enough that, for each fixed $i \in \{1, \dots, s\}$, no two of these possible values are congruent modulo p^{n_0}. Then any mod-p^{n_0} representation ρ_{n_0} can lift to at most one semisimple p-adic representation.

The strategy, then, is as follows. First, make a list of all (finitely many) possible tuples

$$(\mathrm{Tr}(\mathrm{Fr}_{\mathfrak{p}_i} | \rho))_{i \in \{1,\dots,s\}};$$

we'll call such a tuple a *candidate*. As described above, we can enumerate all mod-p^n representations for some $n \geq n_0$. We compute their Frobenius traces and match them with candidates, discarding candidates that don't match any representation, and vice-versa. We can repeat this procedure for any desired n; the list of candidates will get shorter, as spurious candidates are deleted.

3.2. **Computing the Parshin family.** Before we get to the purely local part of the computation, which consists of describing the p-adic period map per_p, we are faced with the problem of finding an explicit set of algebraic equations defining the Parshin family

$$\mathcal{C} \longrightarrow X,$$

whose fibres are finite covers of X branched over the variable point x. This is an instance of the Riemann–Hurwitz problem. Computational work on branched covers of curves is particularly well-developed in the case of Belyĭ covers of $\mathbf{P}^1$; see [SV14] for an overview. The covers appearing in our setting are solvable, and we expect that explicit calculations on the Jacobian could provide a fruitful approach.

The solvability of the covering group $\mathrm{Aff}(q)$ has the following geometric interpretation. Suppose $Z \to X$ is an $\mathrm{Aff}(q)$-cover, branched at x. Let Z^{Gal} be the Galois closure of Z; this is a cover of X of degree $q(q-1)$, ramified only above x and having Galois group $\mathrm{Aff}(q)$. The quotient map $\mathrm{Aff}(q) \to \mathbf{F}_q^\times$ gives a curve Z^{ab}, corresponding by the Galois correspondence to $\mathbf{F}_q^\times$. Thus we have the tower of covers

$$Z^{\mathrm{Gal}} \longrightarrow Z^{\mathrm{ab}} \xrightarrow{\pi} X.$$

In this tower, Z^{ab} is an unramified abelian cover of X of degree $q-1$, and Z^{Gal} is an abelian cover of Z^{ab} of degree q, ramified at exactly the points of $\pi^{-1}(x)$. The curve Z can be recovered as a quotient of Z^{Gal}.

This suggests the following strategy to compute the Parshin family Y, each of whose fibers is a union of $\mathrm{Aff}(q)$-covers Z. First, we attempt to compute abelian covers (both unbranched and branched) of arbitrary curves, by finding torsion points on algebraic generalized Jacobians. To describe one strategy[9], we will

[9] An alternative approach to computing covers of curves is by Hensel lifting from a finite field, as in [Mas19].

restrict attention to unramified covers and the (ungeneralized) Jacobian. In this setting, we want to find a divisor D on the curve X, along with a meromorphic function f on X such that

$$\operatorname{div}(f) = rD,$$

which amounts to looking for r-torsion on the Jacobian of X. The Jacobian has an algebraic incarnation as a variety classifying divisor classes on X and an analytic incarnation as a complex torus. It is of course trivial to identify torsion points on the *analytic* Jacobian; what we need is to describe them as points on the algebraic Jacobian.

Fix a basepoint $b \in X(\mathbf{C})$. By integration we can compute coordinates on the analytic torus $\operatorname{Jac} X$, along with the analytic Abel–Jacobi map

$$X \longrightarrow \operatorname{Jac} X.$$

In the other direction, let g be the genus of X. We want to invert the map

$$\operatorname{Sym}^g X \longrightarrow \operatorname{Jac} X, \tag{17}$$

to realize a point of the analytic Jacobian as a divisor on X. This map is a birational equivalence, but not an isomorphism. On a Zariski-dense subset of $\operatorname{Jac} X$, the map can be inverted, for example, by theta function methods [Mum83, Theorem II.3.1], by Puiseux series methods [CMSV19], or by computations in Grassmannians arising from Riemann-Roch theory [KM04, CMSV19]. A general algorithm appears in [CMSV19, §3.3].

If we can compute arbitrary abelian covers, we could try to determine all the covers Z^{Gal} for any fixed point x; from there one computes Z by Galois theory on the function field. In other words, we can compute the fiber Y_x of the Parshin family over any given point $x \in X$. To compute the Parshin family as an algebraic family, we are faced with the need to interpolate these fibers, perhaps by Puiseux series methods.

3.3. Computing the p-adic period map.

We now come to the local part of the computation, where a description of the p-adic period map per_p reduces to a computation with p-adic cohomology in families. There is a vast literature on this subject, and this step is therefore likely to be more accessible and efficient than the others[10]. We give a brief overview of some results in the literature, for more detailed treatments that address also the history of the subject, see Kedlaya [Ked09, Ked07].

The basic problem is the following: Suppose we are given a curve $\mathcal{C}_x$ over a p-adic field K_v and want to compute the filtered ϕ-module structure of $\mathrm{H}^1_{\mathrm{dR}}(\mathcal{C}_x/K_v)$. Representing this space by differentials of the second kind, the Hodge filtration is easily worked out, and it is the Frobenius operator ϕ that forms the essence of this problem. When $\mathcal{C}_x$ is hyperelliptic, Kedlaya [Ked01] introduced an efficient algorithm, a variant of which we will see in action for the examples of the genus 2 curves in §6. There are two main ingredients for the computation:

- An appropriate lift of Frobenius on the functions in a (p-adic analytic) open subset of $\mathcal{C}_x$,
- A reduction algorithm in de Rham cohomology, that writes an arbitrary differential as the sum of an exact differential and a linear combination of our basis differentials.

By applying the reduction in cohomology to the image of a set of basis differentials under this Frobenius lift, we may obtain a matrix of the Frobenius operator ϕ, up to some precision v^n.

[10] Indeed, the algorithms mentioned here are crucial ingredients for the effective method of Chabauty–Kim, as we will see in §6.

This method has seen extensive developments since [Ked01], notably by Lauder [Lau04, Lau06] who introduced the *fibration method*. This method makes use of the Frobenius structure on the sheaf of relative q-th de Rham cohomology $\mathcal{H}^q_{\mathrm{dR}}(X/S)$ of a smooth morphism $X \longrightarrow S$ between smooth varieties over K_v. The variation of the de Rham cohomology of the fibres in this family is described by the Gauß–Manin connection

$$\nabla_{\mathrm{GM}} : \mathcal{H}^q_{\mathrm{dR}}(X/S) \longrightarrow \Omega^1_{X/S} \otimes \mathcal{H}^q_{\mathrm{dR}}(X/S),$$

which gives a system of differential equations known as the *Picard–Fuchs equations*, whose study was taken up in the 19th century. Suppose we find a local lift of Frobenius ϕ on S, then the pullback of the relative de Rham cohomology $\mathcal{H}^q_{\mathrm{dR}}(X/S)$ by ϕ is isomorphic *as a vector bundle with connection* to the original one. In concrete terms, let us suppose that S is a curve, then we may express this in matrix form as

$$NFdt + \frac{\partial}{\partial t}F = \left(\frac{\partial}{\partial t}\phi(t)\right) F\phi(N)dt \tag{18}$$

by choosing a local coordinate t on S, and a basis of the relative de Rham cohomology, with respect to which we obtain a matrix $F(t)$ describing the Frobenius operator on the fibres, and $N(t)dt$ describing the Gauß–Manin connection. This equation is very useful. For instance, if $F(t)$ can be computed for a single value of $t = t_0$, then we may solve these p-adic differential equation using $F(t_0)$ as an initial condition. Lauder [Lau04, Lau06] uses this idea to compute the Frobenius action in families. It is surprisingly versatile, applying both to individual curves with a map to $\mathbf{P}^1$ as well as families of curves. It has been developed in many subsequent papers of which we mention the recent algorithms of Tuitman [Tui16, Tui17], and the references contained therein, which vastly extend the range of applicability of these ideas.

3.4. **Compare the global Galois representations with the p-adic periods.** We suggest two approaches. The first is to use p-adic Hodge theory, along the lines of Fontaine–Laffaille theory [FL82]. We are given a mod-p^n global Galois representation, presented as a polynomial whose splitting field is its kernel. We can determine the corresponding local representation at p, in terms of extensions of $\mathbf{Q}_p$. Fontaine and Laffaille define a functor $\underline{U}_S$ from a certain category of finite-length filtered ϕ-modules to the category of Galois representations [FL82, §0.6]. One expects that Fontaine–Laffaille theory can be made algorithmic: given a mod-p^n Galois representation, we should be able to determine whether it is in the image of this functor, and if so, describe the underlying filtered ϕ-module. We can then compare these ϕ-modules with the ϕ-modules arising from the p-adic period map, to determine a list of candidate points.

Our second approach avoids filtered ϕ-modules entirely, by working directly with Galois representations. It is a consequence of Fontaine–Laffaille theory that the mod-p^n local Galois representation ρ_x depends only on the reduction of x modulo v^{n+1}. Using this, we can compute explicitly all the possibilities for the local Galois representation at p, and match them explicitly with the list of "candidates" from the global Galois calculation. In other words, for each candidate ρ, we obtain a list of mod-v^{n+1} points of X, the local representations at which agree modulo p^n with ρ. For each of these mod-v^{n+1} residue classes, we then use the period map per_p to compute a bound on the number of rational points in the class.

4. The method of Chabauty–Kim: Finiteness

In this section, we discuss the approach to Mordell's conjecture due to Minhyong Kim. It follows the same pattern as the method of Chabauty–Coleman discussed in the introduction, and as such it depends on some geometric input, replacing the condition $r < g$ by something weaker, which may be done at the cost of replacing the p-adic Tate module V by a more sophisticated quotient of the fundamental group. We discuss in some detail the particular case of a quotient arising from a geometric correspondence [BD18, BD19a, BDM$^+$19] using the geometric language of Edixhoven–Lido [EL19].

4.1. **Quotients of the fundamental group.** To motivate an interest in unipotent quotients of the algebraic fundamental group for Diophantine applications, it is instructive to first recall the *section conjecture* of Grothendieck [Gro97], which states that the map

$$\begin{array}{rccc} \rho \ : & X(\mathbf{Q}) & \longrightarrow & \mathrm{H}^1\big(G_{\mathbf{Q}}, \pi_1^{\text{ét}}(\overline{X}, b)\big)\,, \\ & x & \longmapsto & [\, \pi_1^{\text{ét}}(\overline{X}; b, x)\,] \end{array}$$

which attaches to every rational point the class of the Galois representation defined by the corresponding *path torsor* of the algebraic fundamental group, should be an isomorphism. In other words, every torsor of the fundamental group should necessarily arise from a rational point. This provides us with the tantalizing possibility of studying the set of such torsors in lieu of the set $X(\mathbf{Q})$. Unfortunately, the cohomology set that classifies these torsors does not seem to have much structure with which we can work.

On the other end of the spectrum, we already saw that the twists of the p-adic Tate module V of the Jacobian J of X, which is essentially the abelianization of the fundamental group, are classified by an object which is very closely related to J, and which therefore has a tremendous amount of structure. That said, this association only gives us enough information under the additional assumption that $r < g$.

In summary, we could roughly describe the situation by saying that the association

$$\rho \ : \ X(\mathbf{Q}) \longrightarrow \mathrm{H}^1\big(G_{\mathbf{Q}}, \pi_1^{\text{ét}}(\overline{X}, b)\big) \tag{19}$$

in the section conjecture has a target with *too little* structure, whereas the association

$$\rho \ : \ X(\mathbf{Q}) \longrightarrow \mathrm{H}^1_f(G_{\mathbf{Q}}, V) \tag{20}$$

appearing in the method of Chabauty–Coleman has a target with *too much* structure. The latter statement is meant in the sense that ρ factors through the Jacobian, and in situations where $r \geq g$ this kills some crucial non-abelian information needed to understand $X(\mathbf{Q})$. In the method of Chabauty–Kim, we allay the difficulties inherent to both settings by working with a suitable intermediate quotient, balancing the availability of structure on the sets H^1 against our ability to explicitly describe the target. We consider quotients of the fundamental group that are unipotent.[11]

The strategy for proving finiteness follows the same pattern as our discussion of the method of Lawrence–Venkatesh. First, one attempts to gain sufficient control over the set of global representations involved, and second, one studies the local representations via the analytic properties of an associated period map.

a. Global representations. A general theorem of Kim ([Kim05, Proposition 2] and [Kim09, p. 118]) states that if U is a unipotent quotient satisfying certain technical assumptions which we will not state here, the set $\mathrm{H}^1_f(G_K, \mathrm{U})$ carries the structure of an algebraic variety, dubbed *Selmer variety*, such that the localization map

$$\mathrm{H}^1_f(G_{\mathbf{Q}}, \mathrm{U}) \longrightarrow \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathrm{U}) \tag{21}$$

between the global and local Selmer varieties is algebraic. The algebraic nature of this map allows us to gain control over the image of the global Selmer variety, typically by showing that the global Selmer variety is of lower dimension than the local Selmer variety, so that the image cannot be Zariski dense.

[11] Strictly speaking, quotients of the $\mathbf{Q}_p$-unipotent étale fundamental group studied in Deligne [Del89].

b. The period map. As was the case in the method of Lawrence–Venkatesh, the control of global representations can be turned into a proof of finiteness by controlling a p-adic period map. In the method of Chabauty–Kim, this means concretely that one establishes that the association

$$\rho \;:\; X(\mathbf{Q}_p) \longrightarrow \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathrm{U}), \tag{22}$$

of the path torsor of U attached to a point, has an image which is Zariski dense. Typically, the quotient U is of a "motivic" nature, in which case the association ρ in (22) has a de Rham realisation

$$\mathrm{per}_p \;:\; X(\mathbf{Q}_p) \longrightarrow \mathrm{MF}^{\phi} \tag{23}$$

which can be expressed as a linear combination of iterated Coleman integrals of differentials. A general theorem of Kim [Kim09, Theorem 1] establishes the linear independence of such iterated integrals, which often implies the Zariski density of the image of (22) by p-adic Hodge theory.

c. Finiteness. In conclusion, we are left with the following attractive strategy to study the set of rational points $X(\mathbf{Q})$: Suppose that we can construct a specific finite-dimensional unipotent quotient U satisfying the technical hypotheses required for the representability of the Selmer varieties, such that furthermore

(1) we can prove that $\dim \mathrm{H}^1_f(G_{\mathbf{Q}}, \mathrm{U}) < \dim \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathrm{U})$,
(2) the quotient is "motivic", so that we have a p-adic period map

$$\mathrm{per}_p \;:\; X(\mathbf{Q}_p) \longrightarrow \mathrm{MF}^{\phi}$$

which is a linear combination of iterated integrals of differentials on X, and
(3) we can find a *computable* condition on elements of the image of per_p to come from a point in $X(\mathbf{Q})$.

Once we manage to find a quotient U satisfying these conditions, we consider the diagram

$$\begin{tikzcd} X(\mathbf{Q}) \arrow[r] \arrow[d, "\rho"'] & X(\mathbf{Q}_p) \arrow[d, "\rho"'] \arrow[dr, dashed, "\mathrm{per}_p"] & \\ \mathrm{H}^1_f(G_{\mathbf{Q}}, \mathrm{U}) \arrow[r] & \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathrm{U}) \arrow[r, "\mathbf{D}_{\mathrm{cris}}"] & \mathrm{MF}^{\phi}. \end{tikzcd} \tag{24}$$

The first two conditions on U are the active ingredients for deducing finiteness. The first condition is the analogue of the condition "$r < g$" appearing in the method of Chabauty–Coleman, and allows us to control the image of the global Selmer variety. When combined with a concrete understanding of the period map per_p provided by the second condition (for instance, enough to show Zariski-density of (22), see [Kim09, Theorem 1]) the above commutative diagram implies that $X(\mathbf{Q}_p)$ intersects the image of the global Selmer variety in a finite set of points. In particular, this shows that $X(\mathbf{Q})$ is finite.

Finding suitable quotients that satisfy the first two conditions is the subject of many works, and is typically done by considering quotients U arising from powers of the augmentation ideal, see for instance Kim [Kim05, Kim09], Coates–Kim [CK10] and Ellenberg–Hast [EH]. The third condition is relevant for the *explicit determination* of $X(\mathbf{Q})$ and will reappear later.

4.2. **Geometric correspondences on X.** We now discuss one instance where such a quotient can be constructed, under the additional assumption that the Jacobian J of X has non-trivial Néron–Severi rank, following [BD18, BDM$^+$19]. To offer a different perspective on the constructions in *loc. cit.* we opt for the more geometric reformulation of this theory following the beautiful work of Edixhoven–Lido [EL19]. It should be noted that in [EL19] this geometric viewpoint is retained to find a method for the effective determination of $X(\mathbf{Q})$, but in §5 we instead opt for the cohomological language of [BD18, BDM$^+$19].

Recall that the Néron–Severi group of a smooth proper variety is the group of components of its Picard scheme. In the situation at hand, we have chosen a base point b in $X(\mathbf{Q})$, which gives us an associated Abel–Jacobi map $X \longrightarrow J$. By functoriality, we obtain the following diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Pic}^0(J) \arrow[r] \arrow[d, equal] & \mathrm{Pic}(J) \arrow[r] \arrow[d] & \mathrm{NS}(J) \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & \mathrm{Pic}^0(X) \arrow[r] & \mathrm{Pic}(X) \arrow[r] & \mathbf{Z} \arrow[r] & 0.
\end{tikzcd} \tag{25}$$

The Néron–Severi group $\mathrm{NS}(J)$ is a finitely generated group, of rank $\mathrm{rk}_{\mathrm{NS}}$ which is called the *Néron–Severi rank* of J. Now suppose that we have a non-trivial class Z in $\mathrm{NS}(J)$ which maps to zero in $\mathbf{Z} \simeq \mathrm{NS}(X)$ in the above diagram[12]. Then, by the identification of $\mathrm{Pic}^0(J)$ with $\mathrm{Pic}^0(X)$ there is a unique lift of Z to an element of $\mathrm{Pic}(J)$ which is trivial when restricted to X. In other words, Z uniquely determines a (non-trivial) line bundle $\mathscr{L}_Z$ on J which is trivial when restricted to X, and hence we obtain a lift of the Abel–Jacobi map

$$\begin{tikzcd}
 & \mathscr{L}_Z \arrow[d] \\
X \arrow[r] \arrow[ru, dashed, bend left] & J.
\end{tikzcd} \tag{26}$$

This lifting of the Abel–Jacobi map, or equivalently this trivialization of the line bundle $\mathscr{L}_Z$ restricted to X, is a priori uniquely determined up to multiplication by elements of $\mathbf{Q}^\times$. As explained in Edixhoven–Lido [EL19], one can determine it up to $\mathbf{Z}^\times = \{\pm 1\}$, and hence essentially uniquely, at the cost of taking a small[13] tensor power of $\mathscr{L}_Z$ by spreading out the geometry over $\mathbf{Z}$ and working with the Néron model of J. In conclusion, we obtain an essentially unique lift

$$X \longrightarrow \mathscr{L}_Z^\times := \mathbf{Isom}_J(\mathcal{O}, \mathscr{L}_Z). \tag{27}$$

The scheme $\mathscr{L}_Z^\times$ is a $\mathbf{G}_m$-torsor[14] over the Jacobian J. We define U to be the $\mathbf{Q}_p$-étale fundamental group of $\mathscr{L}_Z^\times$. This group is non-abelian, and may be understood geometrically as follows. One can show (see for instance Bertrand–Edixhoven [BE, § 4] for the arguments in the $\mathbf{C}$-analytic setting) that there is a co-final system of étale coverings

$$\pi_n : (\mathscr{L}_Z^\times)^{\otimes n} \longrightarrow \mathscr{L}_Z^\times$$

obtained by composing the pullback of the map $[n]$ on the Jacobian with the n^{th} power map on fibres. The Galois group U_n of this étale cover is a central extension

$$1 \longrightarrow \mu_n \longrightarrow \mathrm{U}_n \longrightarrow J[n] \longrightarrow 0,$$

so that U is a Heisenberg group, and as a Galois representation it is an extension of V by $\mathbf{Q}_p(1)$. Suppose that x is a point in $X(K)$ for K equal to $\mathbf{Q}$ or $\mathbf{Q}_p$. Then in analogy with (5) we obtain a torsor of U from the inverse limit of the preimages of x under the maps π_n, i.e.

$$\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \left(\varprojlim_n \pi_n^{-1}(x) \right), \qquad \pi_n \; : \; (\mathscr{L}_Z^\times)^{\otimes n} \longrightarrow \mathscr{L}_Z^\times. \tag{28}$$

[12] Such a class always exists when $\mathrm{rk}_{\mathrm{NS}} > 1$, which is true for many examples of interest, including modular curves.

[13] It suffices to take the least common multiple of the exponents of the Néron component groups at all primes of bad reduction.

[14] Since the class of its line bundle in $\mathrm{Pic}(J)$ maps to a non-zero element of $\mathrm{NS}(J)$, this $\mathbf{G}_m$-torsor is not a group.

Such torsors are classified by the cohomology group $\mathrm{H}^1(G_K, \mathrm{U})$ and satisfy certain local conditions which we will not make explicit here. In conclusion, we obtain an association ρ analogous to (4):

$$\rho \;:\; X(K) \longrightarrow \mathscr{L}_Z^{\times}(K) \longrightarrow \mathrm{H}^1_f(G_K, \mathrm{U}). \tag{29}$$

4.3. **Finiteness of $X(\mathbf{Q})$.** The quotient U attached to a Néron–Severi class Z as above has dimension $2g+1$ as a $\mathbf{Q}_p$-vector space. More precisely, as a Galois representation, it is an extension of the form

$$0 \longrightarrow \mathbf{Q}_p(1) \longrightarrow \mathrm{U} \longrightarrow V \longrightarrow 0, \tag{30}$$

where $\mathbf{Q}_p(1)$ is the one-dimensional representation given by the cyclotomic character. The simple nature of this one-dimensional graded piece is responsible for the proof that the quotient U satisfies the first condition on our wish list in §4.1. Indeed, this can be deduced from the statements

$$\begin{array}{rcccl} \mathrm{H}^1_f(G_{\mathbf{Q}}\;, \mathbf{Q}_p(1)) & = & \mathbf{Z}^{\times} \widehat{\otimes}\, \mathbf{Q}_p & = & 0, \\ \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathbf{Q}_p(1)) & = & \mathbf{Z}_p^{\times} \widehat{\otimes}\, \mathbf{Q}_p & = & \mathbf{Q}_p \end{array} \tag{31}$$

which result, via the simple argument in [BD18, Lemma 3.1], in the statements

$$\begin{array}{rcl} \dim \mathrm{H}^1_f(G_{\mathbf{Q}}\;, \mathrm{U}) & \leq & r, \\ \dim \mathrm{H}^1_f(G_{\mathbf{Q}_p}, \mathrm{U}) & = & g+1. \end{array} \tag{32}$$

The quotient U is also *motivic* in nature, as its geometric definition via the $\mathbf{G}_m$-torsor $\mathscr{L}_Z^{\times}$ shows. In particular, besides the Galois representation U, there is also a de Rham realisation U^{dR}, which is a quotient of the de Rham fundamental group of X, see [Kim05, Kim09] for more precise definitions. The theorem of Kim [Kim09, Theorem 1] discussed in §4.1 then implies that the image of $X(\mathbf{Q}_p)$ under ρ is Zariski dense.

This allows us to deduce finiteness of $X(\mathbf{Q})$ for certain curves X. Suppose that $r = g$, so that we are just outside of the range where the method of Chabauty–Coleman applies, and assume furthermore that the Néron–Severi rank $\mathrm{rk}_{\mathrm{NS}}$ of J is at least 2, so that there exists a quotient U as above. The diagram (25) implies, via the two properties we just discussed, that the intersection of $X(\mathbf{Q}_p)$ with the global Selmer variety is finite. Since this set contains $X(\mathbf{Q})$, finiteness of the latter set follows.

In fact, one can refine the above discussion by constructing a quotient which is an extension of V by the direct sum of characters $\mathbf{Q}_p(1)^{\oplus(\mathrm{rk}_{\mathrm{NS}}-1)}$, resulting via the same reasoning in the following finiteness statement, which is a special case of Balakrishnan–Dogra [BD18, Lemma 3.2].

Theorem 4.1. *Suppose that X is a smooth projective curve over $\mathbf{Q}$. Then $X(\mathbf{Q})$ is finite whenever*

$$r \;<\; g + \mathrm{rk}_{\mathrm{NS}} - 1. \tag{33}$$

Many other instances of finiteness are known to follow from the method of Chabauty–Kim, and in general finiteness was proved by Kim [Kim09] under the assumption of the Bloch–Kato conjecture. We will not discuss these results here, but rather turn to the question of how to explicitly determine the set $X(\mathbf{Q})$.

5. The method of Chabauty–Kim: Effectivity

In this section, we discuss how to use the method of Chabauty–Kim to compute the rational points on X in the simplest instance of Theorem 4.1: the case $r = g$ and $\mathrm{rk}_{\mathrm{NS}} > 1$. Whereas the method of Chabauty–Coleman relies on detecting global points via *linear* relations in the image of per_p, we will provide a computable condition on filtered ϕ-modules in the image of per_p to come from a point in $X(\mathbf{Q})$ via *bilinear* relations, thereby addressing the third item in our wish list in §4.1.

5.1. **Heights on Selmer varieties.** Looking for bilinear relations, one is naturally led to p-adic heights. Classically, these were defined as bilinear pairings on $J(\mathbf{Q})$ but since it is crucial that the non-abelian method of Chabauty–Kim factors through a non-abelian Selmer variety rather than the abelian variety J, we instead prefer to utilize a more general approach due to Nekovář [Nek93, §2]. Namely, he constructs a continuous bilinear pairing

$$h\colon \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, V) \times \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, V^*(1)) \longrightarrow \mathbf{Q}_p, \tag{34}$$

depending on some auxiliary choices, including the choice of a splitting of the Hodge filtration

$$s\colon V_{\mathrm{dR}}/\operatorname{Fil}^0 V_{\mathrm{dR}} \longrightarrow V_{\mathrm{dR}}\,. \tag{35}$$

The global height h decomposes as a sum of local heights h_v, where v runs through the finite primes of $\mathbf{Q}$. Briefly, the idea is to lift a pair in $\mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, V) \times \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, V^*(1))$ to a mixed extension of p-adic Galois representations with graded pieces $\mathbf{Q}_p, V$ and $\mathbf{Q}_p(1)$ and to define h_v on it. As explained in [BD18, Section 5], we can construct such a representation from a torsor $P \in \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, \mathrm{U})$, where U is attached to a Néron–Severi class as in §4.2, by twisting a certain quotient of the universal enveloping algebra of the $\mathbf{Q}_p$-unipotent étale fundamental group by P. There is an analogous local construction for $P \in \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}_v}, \mathrm{U})$.

We will assume throughout that $r = g$ and that the p-adic closure of $J(\mathbf{Q})$ has finite index in $J(\mathbf{Q}_p)$. [15] Then there are isomorphisms

$$\mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, V) \xrightarrow{\mathrm{res}_p} \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}_p}, V) \xrightarrow{\log} \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee.$$

By Poincaré duality we obtain maps

$$\pi\colon\ \mathrm{H}^1_{\mathrm{f}}(G_K, \mathrm{U}) \longrightarrow \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$$

for $K \in \{\mathbf{Q}, \mathbf{Q}_p\}$.

For ease of exposition, we shall assume for all $v \neq p$ that $h_v = 0$ for torsors coming from $X(\mathbf{Q}_v)$. The local height h_p will be discussed in more detail below. The main point is that it factors through $\mathrm{D}_{\mathrm{cris}}$, so we obtain the following refinement of diagram (24):

$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r] \arrow[d, "\rho"'] & X(\mathbf{Q}_p) \arrow[d, "\rho"'] \arrow[dr, dashed, bend left, "\mathrm{per}_p"] & \\
\mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}}, \mathrm{U}) \arrow[r, "\mathrm{res}"] \arrow[dr, "\pi"'] & \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}_p}, \mathrm{U}) \arrow[r, "\mathrm{D}_{\mathrm{cris}}"] \arrow[d, "\pi"'] & \mathrm{MF}^\phi \arrow[d, "h_p"'] \\
 & \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \arrow[r, "h"'] & \mathbf{Q}_p\,,
\end{tikzcd} \tag{36}$$

where h_p is now defined on the image of $\mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}_p}, \mathrm{U})$.

If (ψ_i) is a basis of the dual space of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$, then there are constants $\alpha_i \in \mathbf{Q}_p$ such that $h = \sum_i \alpha_i \psi_i$. We deduce that the locally analytic function

$$Q\,:\ X(\mathbf{Q}_p) \longrightarrow \mathbf{Q}_p\,; \qquad x \mapsto \sum_i \alpha_i \psi_i(\pi(\rho(x))) - h_p(\mathrm{per}_p(x)) \tag{37}$$

vanishes along $X(\mathbf{Q})$; furthermore, one can show that it has only finitely many zeroes (see [BD19a]). We can use this function for the explicit computation of $X(\mathbf{Q})$ if we have algorithms to

[15] If the latter condition fails, we may apply classical Chabauty as in §1.3.

(i) compute the α_i for a suitable explicitly computable basis ψ_i.
(ii) expand the function $x \mapsto h_p(\mathrm{per}_p(x))$ into convergent power series on residue disks.

We can easily solve (i) given $x_1, \dots, x_m \in X(\mathbf{Q})$ such that

$$\{\pi(\rho(x_i))\}_{i=1,\dots,m} \text{ is a basis for } \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee;$$

in this case we only need to compute $h_p(\mathrm{per}_p(x_i))$ and $\pi(\rho(x_i))$. If we choose an $\mathrm{End}_0(J)$-equivariant splitting in (35), then the global height is also $\mathrm{End}_0(J)$-equivariant, thus reducing the number of points x_i required. Nevertheless, there need not exist enough points x_i, in which case we can solve (i) using generators of $J(\mathbf{Q}) \otimes \mathbf{Q}$ and a construction of p-adic heights on J due to Coleman and Gross [CG89].

Remark 5.1. It is possible to write down functions vanishing in $X(\mathbf{Q})$ with finitely many zeroes when $r < g + \mathrm{rk}_{\mathrm{NS}} - 1$ using p-adic heights [BD18, Proposition 5.9]. More generally, one can extend Nekovář's construction to construct such functions when $r < g^2$, conditional on the conjecture of Bloch–Kato, see [BD19a, §4]. This has only been made explicit in the special case of the Kulesz–Matera–Schost family of bielliptic genus 2 curves, see the (unconditional) Theorem 1.2 of [BD19a].

5.2. **Local heights.** In the remainder of this section we focus on (ii). We first discuss in more detail the local height h_p, following [Nek93, §4]. Let $P \in \mathrm{H}^1_{\mathrm{f}}(G_{\mathbf{Q}_v}, \mathrm{U})$ and denote by M_P the mixed extension of $\pi(P)$ mentioned above. Then $h_p(M_P)$ is constructed using $\mathrm{D}_{\mathrm{cris}}(M_P)$, which is a mixed extension of filtered ϕ-modules with graded pieces $\mathbf{Q}_p$, $V_{\mathrm{dR}} := \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^\vee = \mathrm{D}_{\mathrm{cris}}(V)$ and $\mathbf{Q}_p(1)$.

For simplicity, we only describe h_p on the image of $X(\mathbf{Q}_p)$. The family $(\mathrm{D}_{\mathrm{cris}}(M_{\rho(x)}))_x$ interpolates in the following sense: There is a filtered connection $\mathcal{A}_Z = \mathcal{A}_Z(b)$ with Frobenius structure such that we have

$$\mathrm{D}_{\mathrm{cris}}(M_{\rho(x)}) \simeq x^*\mathcal{A}_Z \quad \text{for all } x \in X(\mathbf{Q}_p). \tag{38}$$

Suppose that we have isomorphisms

$$\begin{array}{rcl} s^\phi(b,x) & : & \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} x^*\mathcal{A}_Z \\ s^{\mathrm{Fil}}(b,x) & : & \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} x^*\mathcal{A}_Z \end{array}$$

where s^ϕ is Frobenius-equivariant, and s^{Fil} respects the filtrations, and suppose we can write them as

$$s^\phi(b,x) = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b,x) & 1 & 0 \\ \gamma_\phi(b,x) & \boldsymbol{\beta}_\phi^{\mathsf{T}}(b,x) & 1 \end{pmatrix} \qquad s^{\mathrm{Fil}}(b,x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \gamma_{\mathrm{Fil}}(b,x) & \boldsymbol{\beta}_{\mathrm{Fil}}^{\mathsf{T}}(b) & 1 \end{pmatrix}. \tag{39}$$

Note that we make a choice of basis differentials on the affine open Y (see § 5.3) so that $s^\phi(b,x)$ and $s^{\mathrm{Fil}}(b,x)$ are of this form. The splitting s in (35) induces idempotents

$$\begin{array}{rcl} s_1 & : & V_{\mathrm{dR}} \longrightarrow s(V_{\mathrm{dR}}/\,\mathrm{Fil}^0 V_{\mathrm{dR}}) \\ s_2 & : & V_{\mathrm{dR}} \longrightarrow \mathrm{Fil}^0 V_{\mathrm{dR}}. \end{array}$$

With respect to our choices, Nekovář's local height at p is

$$h_p(\mathrm{per}_p(x)) = \gamma_\phi(b,x) - \gamma_{\mathrm{Fil}}(b,x) - \boldsymbol{\beta}_\phi^{\mathsf{T}}(b,x) \cdot s_1(\boldsymbol{\alpha}_\phi)(b,x) - \boldsymbol{\beta}_{\mathrm{Fil}}^{\mathsf{T}}(b) \cdot s_2(\boldsymbol{\alpha}_\phi)(b,x). \tag{40}$$

So in order to solve (ii) we need to compute the entries of (39), which means computing the Hodge filtration and the Frobenius structure on $\mathcal{A}_Z$. For (i), we also need to explicitly compute the composition

$\pi \circ \rho$. With respect to the dual basis of our chosen basis differentials on Y, the map $\pi \circ \rho$ is given by

$$\begin{aligned} \pi \circ \rho : Y(\mathbf{Q}_p) &\to H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \\ x &\mapsto \boldsymbol{\alpha}_\phi(b,x)^\intercal \cdot \left(\frac{I_g}{0_g}\right) \otimes (\boldsymbol{\beta}_\phi^\intercal(b,x) - \boldsymbol{\beta}_{\mathrm{Fil}}^\intercal(b)) \cdot \left(\frac{0_g}{I_g}\right). \end{aligned} \tag{41}$$

Note in particular that the first factor is the Abel-Jacobi map $\mathrm{AJ_b}(x)$, sending x to the functional $\omega \mapsto \int_b^x \omega$.

5.3. **Computing the Hodge filtration.** We work in an affine open subset Y of X. Suppose that we have $\#(X \setminus Y)(\overline{\mathbf{Q}}) = d$ and choose differentials $\omega_0, \dots, \omega_{2g+d-2} \in H^0(Y_{\overline{\mathbf{Q}}}, \Omega^1)$ on Y such that the following conditions are satisfied:

(1) The differentials $\omega_0, \dots \omega_{2g-1}$ are of the second kind (residue zero) on X and form a symplectic basis of $H^1_{\mathrm{dR}}(X_{\mathbf{Q}})$ with respect to the cup product pairing. We let $\boldsymbol{\omega}$ denote the column vector $(\omega_0, \dots \omega_{2g-1})^\intercal$.
(2) The differentials $\omega_{2g}, \dots, \omega_{2g+d-2}$ are of the third kind (all poles have order one) on X.

Universal properties give that the rank $2g+2$ vector bundle $\mathcal{A}_Z$ has a connection, a Hodge filtration, and a Frobenius structure, as discussed in [BDM+19, §4,5]. Here, we give algorithms that describe these objects.

Recall that we have a non-trivial class Z in $\mathrm{NS}(J)$ mapping to 0 in $\mathrm{NS}(X)$. This is equivalent to the choice of an endomorphism of $\mathrm{H}^1_{\mathrm{dR}}(X)$ satisfying several conditions (see [BDM+19, §4.4]), and we describe a method to compute this in the case of modular curves in Section 6. We denote the matrix of the correspondence Z on $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q})$ also by Z, where we act on column vectors.

Choose a trivialization

$$s_0 : \mathcal{O}_Y \otimes (\mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1)) \to \mathcal{A}_Z|_Y$$

such that, with respect to this trivialization, the connection ∇ on $\mathcal{A}_X$ is given by

$$\nabla = d + \Lambda,$$

where

$$\Lambda = -\begin{pmatrix} 0 & 0 & 0 \\ \boldsymbol{\omega} & 0 & 0 \\ \eta & \boldsymbol{\omega}^\intercal Z & 0 \end{pmatrix},$$

where η is a differential of the third kind on X that is uniquely determined by the following two properties:

(1) It is in the space spanned by $\omega_{2g}, \dots, \omega_{2g+d-2}$, and
(2) The connection ∇ extends to a holomorphic connection on all of X.

The Hodge filtration on $\mathcal{A}_Z$ is determined completely from the Hodge filtration on its graded pieces, via universal properties. Here is an algorithm to compute the Hodge filtration:

Algorithm 5.2 (Computing the Hodge filtration on $\mathcal{A}_Z$).

(1) Let $L/\mathbf{Q}$ denote a finite extension over which all the points of $X \setminus Y$ are defined. Compute local coordinates at each $x \in (X \setminus Y)(L)$.
(2) For each $x \in (X \setminus Y)(L)$, compute power series for $\boldsymbol{\omega}_x$, the expansion of the vector of differentials $\boldsymbol{\omega}$ at x to large enough precision, which means at least mod $t_x^{d_x}$, where d_x is the order of the largest pole occurring.

(3) Compute the vector $\mathbf{\Omega}_x$, defined by

$$d\mathbf{\Omega}_x = -\boldsymbol{\omega}_x.$$

(4) Compute η as the unique linear combination of $\omega_{2g}, \dots, \omega_{2g+d-2}$ such that

$$d\mathbf{\Omega}_x^{\intercal} Z \mathbf{\Omega}_x - \eta$$

has residue zero at all $x \in (X \backslash Y)(L)$. To do this, carry out the following:
   (a) Using local coordinates at each $x \in (X \backslash Y)(L)$, rewrite $\omega_{2g}, \dots, \omega_{2g+d-2}$.
   (b) Solve for η by comparing residues.

(5) Solve the system of equations for g_x in $L(\!(t_x)\!)/L[\![t_x]\!]$ such that

$$dg_x = \mathbf{\Omega}_x^{\intercal} Z d\mathbf{\Omega}_x - \eta.$$

(6) Compute the vector of constants $\mathbf{b}_{\mathrm{Fil}} = (b_g, \dots, b_{2g-1}) \in \mathbf{Q}^g$ and the function γ_{Fil} characterized by $\gamma_{\mathrm{Fil}}(b) = 0$ and

$$g_x + \gamma_{\mathrm{Fil}} - \mathbf{b}_{\mathrm{Fil}}^{\intercal} N^{\intercal} \mathbf{\Omega}_x - \mathbf{\Omega}_x^{\intercal} Z N N^{\intercal} \mathbf{\Omega}_x \in L[\![t_x]\!] \tag{42}$$

where N is the $2g \times g$ matrix which has the zero matrix of dimension g and the identity matrix of dimension g as blocks. Set $\boldsymbol{\beta}_{\mathrm{Fil}} = \boldsymbol{\beta}_{\mathrm{Fil}}(b) = (0, \dots, 0, b_g, \dots, b_{2g-1})^{\intercal}$.

Remark 5.3. We note that [BD19a, Lemma 6.5] simplifies some of the calculations in the case of a hyperelliptic curve X: in this case, we have that $\eta = 0$ and $\boldsymbol{\beta}_{\mathrm{Fil}} = (0, \dots, 0)^{\intercal}$.

5.4. **Computing the Frobenius structure.** The Frobenius structure on $\mathcal{A}_Z$ can be determined explicitly in terms of double Coleman integrals, as discussed in [BDM$^+$19, §5]. Here is an algorithm to compute it:

Algorithm 5.4 (Computing the Frobenius structure on $\mathcal{A}_Z$).

(1) Use Tuitman's algorithm [Tui16, Tui17] to compute the matrix of Frobenius F and a vector $\boldsymbol{f}$ of overconvergent functions such that

$$\phi^* \boldsymbol{\omega} = d\boldsymbol{f} + F \boldsymbol{\omega},$$

where ϕ is a certain lift of Frobenius.

(2) Let b_0, x_0 be Teichmüller representatives of b, x respectively. Compute the matrix

$$\mathrm{A} = \mathrm{I}(x, x_0)^+ \cdot \mathrm{I}(b_0, b)^-,$$

where we define for any pair $x_1, x_2 \in X(\mathbf{Q}_p)$ the parallel transport matrices

$$\mathrm{I}^{\pm}(x_1, x_2) = \begin{pmatrix} 1 & 0 & 0 \\ \int_{x_1}^{x_2} \boldsymbol{\omega} & 1 & 0 \\ \int_{x_1}^{x_2} \eta + \int_{x_1}^{x_2} \boldsymbol{\omega}^{\intercal} Z \boldsymbol{\omega} & \pm \int_{x_1}^{x_2} \boldsymbol{\omega}^{\intercal} Z & 1 \end{pmatrix},$$

where η is as computed in Algorithm 5.2 (see also Remark 5.3).

(3) Explicitly solve the system

$$\begin{cases} d\mathbf{g}^{\intercal} &= d\mathbf{f}^{\intercal} Z F, \\ dh &= \boldsymbol{\omega}^{\intercal} F^{\intercal} Z \mathbf{f} + d\mathbf{f}^{\intercal} Z \mathbf{f} - \mathbf{g}^{\intercal} \boldsymbol{\omega} + \phi^* \eta - p\eta, \\ h(b) &= 0. \end{cases}$$

Then compute the matrix

$$\mathrm{M}(b_0, x_0) = \begin{pmatrix} 1 & 0 & 0 \\ (I-F)^{-1}\mathbf{f} & 1 & 0 \\ \frac{1}{1-p}\left(\mathbf{g}^\intercal (I-F)^{-1}\mathbf{f} + h\right) & \mathbf{g}^\intercal (F-p)^{-1} & 1 \end{pmatrix} (x_0).$$

(4) Finally, compute the matrix

$$s_0^{-1}(b,x) \circ s^{\phi}(b,x) = \mathrm{A} \cdot \mathrm{M}(b_0, x_0) = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi(b,x) & 1 & 0 \\ \gamma_\phi(b,x) & \boldsymbol{\beta}^\intercal_\phi(b,x) & 1 \end{pmatrix}.$$

Remark 5.5. If X is a hyperelliptic curve, say the smooth projective model of the affine curve $Y\colon\, y^2 = f(x)$, where f is monic and has no repeated roots, then we can use Kedlaya's algorithm [Ked01] or Harrison's generalization [Har12] in Step (1) above. In fact, Tuitman's approach generalizes the approach of Kedlaya and Harrison. Note that the `SageMath` implementation of Kedlaya's algorithm takes the convention that Frobenius acts on columns, while the `Magma` implementation of Tuitman's algorithm as used here takes the convention that Frobenius acts on rows and thus differs by a transpose.

Remark 5.6. Computing the action of Frobenius in Step (1) gives us a way to compute Coleman integrals: in particular, if $b_0 = \phi(b_0)$ and $x_0 = \phi(x_0)$ are Teichmüller points, we compute the Coleman integral as

$$\int_{b_0}^{x_0} \boldsymbol{\omega} = (1-F)^{-1}\left(\boldsymbol{f}(x_0) - \boldsymbol{f}(b_0)\right).$$

6. Examples

We illustrate the practicality of the method of Chabauty–Kim discussed in Section 5 by applying it to three new examples of curves whose rational points were previously unknown. They are all curves of the form

$$X_0(N)^+ := X_0(N)/w_N \tag{43}$$

where N is prime and w_N is the Atkin–Lehner involution, and therefore they have a unique rational cusp, and their non-cuspidal rational points classify unordered pairs of elliptic curves that are related by an N-isogeny. We consider the cases $N = 67$, 73, and 103. For each value of N, the curve $X_0(N)^+$ is of genus 2 and its Jacobian has real multiplication. Thus, the rank of the Néron–Severi group is equal to 2, and the method outlined in Section 5 produces exactly one non-trivial locally analytic function on $X_0(N)^+(\mathbf{Q}_p)$ vanishing on the set of rational points $X_0(N)^+(\mathbf{Q})$. Hence, unlike in the Chabauty–Coleman example at the end of Section 1, we need in addition the Mordell–Weil sieve (see §6.7) to extract the set of rational points from the larger quadratic Chabauty set.

We discuss the computation for $N = 67$ in some detail and briefly summarize the cases $N = 73$ and $N = 103$. These computations use the computer algebra system `Magma` [BCP97] and were done by Best, Bianchi, and Triantafillou, mostly at the workshop "Arithmetic Statistics and Diophantine Stability" at the Fondation des Treilles in July 2018.

Remark 6.1. In [BGX19], the authors apply a combination of elliptic curve Chabauty with covering techniques to determine the rational points on $X_0(N)^+$ for several composite squarefree values of N such that $X_0(N)+$ has genus 2. It would be interesting to determine the rational points on the 13 remaining hyperelliptic curves $X_0(N)+$ for squarefree N; all of them have genus 2.

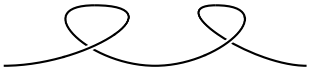

FIGURE 1. The reduction of $\mathcal{X}_0(N)^+$ at N.

6.1. **An explicit model for $X_0(67)^+$.** As is explained in [Mur92, Gal96], an affine model for the genus 2 curve $X_0(67)^+$ can be found explicitly as follows. Let f be the unique, up to conjugation, newform of level 67, weight 2, which is furthermore invariant under the Atkin–Lehner involution w_{67}. The complex vector space spanned by f and its Galois conjugate f^c is isomorphic to the space of regular differentials on $X_0(67)^+$, and we may choose a basis g_1 and g_2 for this space such that $g_1 = q + \cdots$ and $g_2 = q^2 + \cdots$. Note that f and f^c can be computed up to arbitrary q-adic precision using Magma [BCP97]. Then $x = \frac{g_1}{g_2}$ and $y = \frac{q}{g_2}\frac{dx}{dq}$ are related by an equation of the form $y^2 = p(x)$, for some monic polynomial $p(x)$ of degree 6 whose coefficients can be determined from the q-expansions. Such an equation gives a model for $X_0(67)^+$; while g_2 is unique, a certain choice of g_1 yields

$$Y\colon y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1 \qquad [=: f_{67}(x)\,]\,.$$

See [Mur92] for more details; for other examples of computations of models of higher genus modular curves, see [Gal96]. The projective closure X adds two points at infinity, ∞^+ and ∞^-, corresponding to $(1:1:0)$ and $(1:-1:0)$ respectively. By an explicit search, we quickly find several points in $X(\mathbf{Q})$. Indeed,

$$X(\mathbf{Q}) \supset \{\infty^+, \infty^-, (0,\pm 1), (-1,\pm 3), (1,\pm 1), (-2,\pm 7)\}\,. \tag{44}$$

Our goal is to use the machinery set up in Section 5, combined with the Mordell–Weil sieve, to show that $X(\mathbf{Q})$ consists precisely of these 10 points.

Using the explicit model Y, several arithmetic properties of $X_0(67)^+$ can be deduced. For instance, Magma's implementation of 2-descent shows that that the rank[16] of $J_0(N)^+(\mathbf{Q})$ is exactly 2. Alternatively, one can avoid the use of a model and draw the same conclusion from the Gross–Zagier–Kolyvagin–Logachev theorem [GZ86, KL89], by computing that (provably [Ste00, Chapter 3]) $L(f,1) = 0$ and (numerically [Cre97, Dok04]) $L'(f,1) \neq 0$.

6.2. **The reduction of $X_0(N)^+$.** Recall that the method outlined in Section 5 uses some global and local p-adic heights in the sense of Nekovář. Although these depend on some auxiliary choices that we have not made yet at this stage, we have already remarked that we can always ignore all the local heights at primes $v \neq p$ of potential good reduction. More generally, by work of Betts–Dogra [BD19b, Corollary 1.2.2], the map $X(\mathbf{Q}_v) \to \mathbf{Q}_p$ induced by the local height at $v \neq p$ takes at most as many values as the number of irreducible components of a regular semi-stable model at v. Note that $X_0(N)^+$ has good reduction at all primes away from N. Using an argument analogous to [BDM+19, Theorem 6.6], we can show that for all primes $N > 2$ there is a regular semi-stable model $\mathcal{X}_0(N)^+$ of $X_0(N)^+$ whose special fibre is isomorphic to a projective line intersecting itself g times, where g is the genus of $X_0(N)^+$ (see Figure 1). The self-intersections correspond to conjugate pairs of supersingular j-invariants in $\mathbf{F}_{N^2} \setminus \mathbf{F}_N$ (see [DR73, V, §1] and [Ogg75, §3]). In particular, the special fibre of $\mathcal{X}_0(N)^+$ consists of only one component, so the work of Betts–Dogra implies that there are no non-trivial contributions at $v \neq p$.

6.3. **Preliminary choices.**

[16] Since the Jacobian $J_0(N)^+$ has real multiplication over $\mathbf{Q}$ for every prime $N > 2$, its Mordell-Weil rank over $\mathbf{Q}$ is necessarily a multiple of the genus.

A prime p and a base point b. Since by §6.2 the curve $X_0(N)^+$ has good reduction at all primes away from N, we could let our fixed p be any prime different from N; we pick $p = 11$. This choice may seem slightly peculiar to the reader familiar with the classical Chabauty–Coleman method, where it is often advantageous to choose the smallest possible prime of good reduction. The prime 11 has two main advantages for our purposes. First, the polynomial f_{67} has no linear factors over $\mathbf{Q}_{11}$ and, as a result, the lift of Frobenius that we use in §6.5 extends to all of $X(\mathbf{Q}_{11})$. While it is possible to deal with disks containing a point with zero y-coordinate by working with a different lift of Frobenius or by using the trick discussed in [BDM$^+$19, §5.5], our choice of p makes both the exposition and the computation significantly shorter. The second advantage of the prime 11 is somewhat post-hoc, coming from the final Mordell-Weil sieve step. Indeed, it turns out that $J_0(N)^+(\mathbf{F}_q)$ has order divisible by 11^2 for several small primes q (including $q = 31$ and $q = 137$), which makes the Mordell-Weil sieve particularly efficient for proving that points of $X(\mathbf{Q}_{11})$ are *not* in $X(\mathbf{Q})$.

We choose $b = (1, 1)$ for the base point. Note that b lies in both our affine patch and in the affine patch at infinity. One advantage of b over other possible base points is that b will be a Teichmüller point for a convenient lift of Frobenius.

A basis for the de Rham cohomology of $X_0(67)^+$. It is well known that $\mathrm{H}^0(Y_{\overline{\mathbf{Q}}}, \Omega^1)$ has basis given by (the classes of) the differentials

$$\left\{ \frac{dx}{y}, \frac{x\,dx}{y}, \frac{x^2\,dx}{y}, \frac{x^3\,dx}{y}, \frac{x^4\,dx}{y} \right\} \tag{45}$$

and that, inside of $\mathrm{H}^0(Y_{\overline{\mathbf{Q}}}, \Omega^1)$, we can identify $\mathrm{H}^1_{\mathrm{dR}}(X)$ with those differentials which have residue 0 at both points of $X \smallsetminus Y = \{\infty^+, \infty^-\}$. By working with the expansion of each differential in (45) in terms of the uniformizer $t_{\infty^\pm} = x^{-1}$ at $\infty^\pm$, we construct a new basis $\omega_0, \dots, \omega_4$ satisfying the properties (1) and (2) of §5.3. In particular, we may take

$$\omega_0 = -\frac{dx}{y}, \quad \omega_1 = (-1 - x) \cdot \frac{dx}{y}, \quad \omega_2 = (-2 + x - x^3 - x^4) \cdot \frac{dx}{y},$$
$$\omega_3 = \frac{1}{2}\left(1 - x^2 - x^3\right) \cdot \frac{dx}{y}, \quad \omega_4 = (-x - x^2) \cdot \frac{dx}{y}\,.$$

From now on, $\boldsymbol{\omega}$ will denote the column vector $(\omega_0, \dots, \omega_3)^\intercal$.

6.3.1. *A Néron–Severi class.* The choice of a Néron–Severi class Z as in Section 4 is equivalent to the choice of an endomorphism of $\mathrm{H}^1_{\mathrm{dR}}(X)$, satisfying a list of conditions (see [BDM$^+$19, §4.4]). Let ℓ be a prime of good reduction for X. In order to compute the action of the Hecke operator $T_\ell \in \mathrm{End}(\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbf{Q}_\ell))$ on the whole of $\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbf{Q}_\ell)$, rather than just on $\mathrm{Fil}^0\,\mathrm{H}^1_{\mathrm{dR}}(X/\,\mathbf{Q}_\ell)$, we use the Eichler–Shimura formula

$$T_\ell = \mathrm{Fr}_\ell^\intercal + \ell \cdot (\mathrm{Fr}_\ell^\intercal)^{-1}\,.$$

The matrix of Frobenius Fr_ℓ with respect to the basis $\boldsymbol{\omega}$ may be computed using Tuitman's algorithm (we briefly postpone a discussion of this to Step (1) of §6.5, since this matrix for $\ell = p$, as well as one additional output of Tuitman's algorithm, are both needed at that step), and we identify the operator T_ℓ with its matrix representation with respect to $\boldsymbol{\omega}$. Note that the Eichler–Shimura formula holds for $X_0(67)$ and thus for $X_0(67)^+$, since the Atkin–Lehner involution commutes with T_ℓ at all $\ell \neq 67$.

To obtain from T_ℓ an endomorphism corresponding to a class $Z \in \mathrm{NS}(J)$ which maps to zero in $\mathrm{NS}(X)$, we first consider $\mathrm{Tr}(T_\ell) \cdot I_4 - 4T_\ell$, which has trace zero, and then multiply on the right by the inverse of the cup product matrix on $\boldsymbol{\omega}$. For example, choosing $\ell = 11$, we obtain the non-trivial endomorphism with matrix representation

$$Z = \begin{pmatrix} 0 & -8 & 12 & 8 \\ 8 & 0 & -8 & -12 \\ -12 & 8 & 0 & 0 \\ -8 & 12 & 0 & 0 \end{pmatrix}.$$

Since the Néron–Severi group has rank 2, choosing a different Hecke operator would only change the matrix Z by a multiplicative constant factor.

Remark 6.2. Using Tuitman's algorithm, we can compute the entries of T_ℓ only up to some ℓ-adic precision. In our case, this would suffice to carry out the steps of the quadratic Chabauty computation, since we have chosen $\ell = p$. It should however be possible to prove that Z is given exactly by the above matrix, and we may assume that this is the case, as doing so does not affect the computation in any crucial way.

6.4. **Hodge Filtration on $\mathcal{A}_Z$.** We now compute the Hodge filtration of the vector bundle $\mathcal{A}_Z$ attached to our choice of Néron–Severi class Z and base point b. Since the curve X is hyperelliptic, by Remark 5.3 we only need to compute γ_{Fil}, and we can do so using a simplified version of Algorithm 5.2. In particular, for each point at infinity $\infty^{\pm}$, we can compute $\boldsymbol{\Omega}_{\infty^\pm}$ and $g_{\infty^\pm}$ by formal integration of Laurent series in the uniformizer $t_{\infty^\pm}$. Following the steps, we then find that γ_{Fil} has a pole of exact order 1 at $\infty^{\pm}$ with residue -8. Since γ_{Fil} must vanish at b, we conclude that

$$\gamma_{\mathrm{Fil}} = -8x + 8.$$

6.5. **Frobenius structure on $\mathcal{A}_Z$.** We compute the Frobenius structure on $\mathcal{A}_Z$ using Algorithm 5.4.

Step (1): We first fix a lift of Frobenius ϕ. We take $\phi(x) = x^p$, and extend to $\mathbf{Q}_{11}[x]$ by linearity. Since f_{67} has no zeros over $\mathbf{F}_{11}$, we extend this lift to a strict open neighborhood of the tube $]Y_{\mathbf{F}_p}[$[17] by expanding

$$\phi(y) = \sqrt{\phi(f_{67}(x))} = y^p \cdot \left(1 + \frac{\phi(f_{67}(x)) - f_{67}(x)^p}{y^{2p}}\right)^{1/2}.$$

as an *overconvergent* Laurent series in $\mathbf{Q}_p[\![x, y, y^{-1}]\!]$. This lift naturally extends to one-forms.

Next, we compute p-adic approximations of F and $\boldsymbol{f}$ using Tuitman's algorithm [Tui16, Tui17], a generalization of Kedlaya's algorithm which incorporates Lauder's fibration method [Lau06]. Roughly speaking, we first compute $\phi^*\omega_i$. Then, we reduce pole orders by iteratively subtracting differentials of overconvergent functions (constructed by solving linear systems) until $\phi^*\omega_i$ has been reduced to a cohomologous linear combination of basis differentials $\sum_j F_{ji}\omega_j$. The sum f_i of the functions from each step satisfies

$$\phi^*\omega_i = \sum_j F_{ij}\omega_j + df_i\,.$$

Note that in our working example, this F is the matrix Fr_ℓ that was computed in §6.3.1 since ℓ was chosen there to be $p = 11$ as well.

Step (2): Since $b = (1,1)$ is a Teichmüller point for ϕ, $I(b_0, b)^- = I(b, b)^-$ is an identity matrix. To compute the $I(x, x_0)^+$ on each residue disk, we expand the ω_i in terms of a uniformizer near each Teichmüller point x_0 and integrate formally. To compute $\int_{x_0}^{x} \boldsymbol{\omega}^\intercal Z \boldsymbol{\omega}$, we expand, formally integrate, multiply terms, and formally integrate again, as in steps (3) and (5) of Algorithm 5.2.

[17] the tube consists of all points reducing to $Y_{\mathbf{F}_p}$

Step (3): The matrices Z and F are constants, so $\boldsymbol{g}^\intercal = \boldsymbol{f}^\intercal ZF$. We approximate h by iteratively "reducing" a p-adic approximation $(dh)_\sim$ to $dh = \boldsymbol{\omega}^\intercal F^\intercal Z\boldsymbol{f} + d\boldsymbol{f}Z\boldsymbol{f} - \boldsymbol{g}^\intercal\boldsymbol{\omega} + \phi^*\eta - p\eta$ as in Tuitman's algorithm until we find $a_j \in \mathbf{Q}_{11}$ and an overconvergent function $h_\sim(x)$ so that

$$(dh)_\sim = \sum_j a_j\omega_j + d(h_\sim)\,.$$

Then $h_\sim(x) - h_\sim(b)$ approximates $h(x)$. The remainder of Steps (3) and (4) are straightforward. The terms $\boldsymbol{\alpha}_\phi(b,x), \boldsymbol{\beta}_\phi(b,x), \gamma_\phi(b,x)$ cannot be expressed compactly, so we omit them here.

6.6. **The local p-adic height and a finite set of p-adic points containing $X(\mathbf{Q})$.** We have now assembled all ingredients to compute the quadratic Chabauty function from (37), whose finite set of zeroes contains $X(\mathbf{Q})$. To find the constants a_i in (37), we use the discussion at the end of §5.1.

Set $K := \mathbf{Q}(\sqrt{5}) = \mathrm{End}_0(J_0(67)^+)$ and $K_p = K \otimes_{\mathbf{Q}} \mathbf{Q}_p$. If we pick a K-equivariant splitting s of the Hodge filtration in formula (40), then the global height h factors through the tensor product $H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes_{K_p} H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$. We now choose auxiliary points $x_1 = (-2,7), x_2 = (-1,3) \in X(\mathbf{Q})$. Since $\mathrm{AJ}_\mathrm{b}(x_1) = [\omega \mapsto \int_b^{x_1}\omega]$ is nonzero, $\mathrm{AJ}_\mathrm{b}(x_1)$ is a K_p-basis for $H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$. Using (41), we compute $(\pi \circ \rho)(x_i)$ in this basis.

We compute $h(\pi(\rho(x_i))) = h_p(\mathrm{per}_p(x_i))$ using (40), the results of §6.4, §6.5 and the splitting s associated to the K-equivariant basis $(\omega_0, \omega_1, \omega_2, \omega_3 - \omega_1)$. Writing ψ_1 for the projection onto the "rational part" and ψ_2 for the projection onto the "$\sqrt{5}$ part," we find that the function sending $x \in X(\mathbf{Q}_p)$ to

$$\begin{aligned} Q(x) := h_p(\mathrm{per}_p(x)) &- (5\cdot 11 + 2\cdot 11^2 + 5\cdot 11^3 + 0\cdot 11^4 + \cdots)\cdot\psi_1(\pi(\rho(x))) \\ &+ (4\cdot 11 + 0\cdot 11^2 + 4\cdot 11^3 + 0\cdot 11^4 + \cdots)\cdot\psi_2(\pi(\rho(x))) \end{aligned} \tag{46}$$

vanishes for all $x \in X(\mathbf{Q})$.

We expand Q as a power series on each residue disk, find the roots, and repeat the computation on an affine patch containing the points at infinity to find a finite subset of $X(\mathbf{Q}_{11})$ which contains $X(\mathbf{Q})$. Using a Newton polygon argument, we find that every root of Q is simple. In addition to the 10 known rational points, we find 14 additional 11-adic zeros of Q (listed in Table 1). To show that these points are not rational, we turn to the Mordell-Weil sieve, described in the following subsection.

6.7. **The Mordell–Weil sieve.** We assume we are given a smooth projective curve $X/\mathbf{Q}$, p a prime of good reduction, a set $X_{\text{known}} \subseteq X(\mathbf{Q})$ and a set $X_{\text{extra}} \subseteq X(\mathbf{Q}_p)$ known to some finite p-adic precision, distinct from any of the X_{known} to that precision. The goal of the Mordell–Weil sieve, which we describe in this section, is to describe extra conditions that the points of $X(\mathbf{Q})$ satisfy that the points in X_{extra} do not. See also [Sik15, BS10, BBM17].

We will show that any rational point must be sufficiently close p-adically to an element of X_{known}. To do this, one proves that for each $x \in X(\mathbf{Q})$, there is some $y \in X_{\text{known}}$ such that $[x-y] \in J(\mathbf{Q})$ is p-adically close to the identity in $J(\mathbf{Q})$. We can get a handle on being p-adically close to $0 \in J(\mathbf{Q})$ using the p-adic filtration of $J(\mathbf{Q}_p)$ by

$$J_i = \left\{x \in J(\mathbf{Q}_p) \colon x \equiv 0 \pmod{p^i}\right\}.$$

The important property of this filtration that we will make use of is that

$$J_0/J_1 \simeq J(\mathbf{F}_p),\ \ J_i/J_{i+1} \simeq \mathbf{F}_p^{\dim J}\,,$$

Disks	x-coordinates of candidate points
$](0,\pm 1)[$	0 $0+7\cdot 11+0\cdot 11^2+3\cdot 11^3+3\cdot 11^4+\cdots$
$](1,\pm 1)[$	1 $1+6\cdot 11+6\cdot 11^2+8\cdot 11^3+7\cdot 11^4+\cdots$
$](6,\pm 5)[$	$6+5\cdot 11+8\cdot 11^2+2\cdot 11^3+4\cdot 11^4+\cdots$ $6+7\cdot 11+0\cdot 11^2+5\cdot 11^3+1\cdot 11^4+\cdots$
$](-2,\pm 7)[$	-2 $9+10\cdot 11+1\cdot 11^2+8\cdot 11^3+0\cdot 11^4+\cdots$
$](-1,\pm 3)[$	-1 $10+3\cdot 11+9\cdot 11^2+10\cdot 11^3+1\cdot 11^4+\cdots$
$]\infty^{\pm}[$	∞ $2\cdot 11^{-1}+4+10\cdot 11+9\cdot 11^2+8\cdot 11^3+7\cdot 11^4+\cdots$

TABLE 1. A set of 24 points of $X_0(67)^+(\mathbf{Q}_{11})$ containing $X_0(67)^+(\mathbf{Q})$.

so that p-adically close rational points must have difference in the Jacobian divisible by a large power of p. Then for any $D \in J(\mathbf{Q})$ we have $\#J(\mathbf{F}_p)\cdot p^i \cdot D \in J_{i+1}$.

The Mordell–Weil sieve locates small cosets within $J(\mathbf{Q})$ (that is, cosets of large index), that contain the image of $X(\mathbf{Q})$ under the Abel-Jacobi map $i_b\colon X \to J$ sending x to $[x-b]$. The sieve plays off local information at a finite set of primes v against the global Mordell–Weil group structure to find restrictions on $i_b(X(\mathbf{Q}))$. First we fix a prime v of good reduction and consider the following commutative diagram:

(47)
$$\begin{tikzcd}
X(\mathbf{Q}) \arrow[r, "i_b"] \arrow[d, "\mathrm{red}_{X,v}"'] & J(\mathbf{Q}) \arrow[d, "\mathrm{red}_{J,v}"] \\
X(\mathbf{F}_v) \arrow[r, "i_{b,v}"'] & J(\mathbf{F}_v)
\end{tikzcd}$$

The commutativity of the diagram implies that the image of $X(\mathbf{Q})$ along $\mathrm{red}_{J,v}\circ i_b$ is contained in the image of $i_{b,v}$. The advantage of this observation is that the bottom row of the diagram deals with finite objects and information about these may be computed effectively. In particular we can find $\operatorname{im} i_{b,v}$ given equations for X. In our setting of a hyperelliptic curve, algorithms for this go back to [Can87], and in general one can make use of work of Khuri-Makdisi [KM07]. Pulling the computed image $\operatorname{im} i_{b,v}$ back to $J(\mathbf{Q})$ gives a union of cosets for the kernel of $\mathrm{red}_{J,v}$ that contains the image of $X(\mathbf{Q})$. We will want to pick v so that the kernel of this map provides non-trivial information about cosets of the target subgroup, which means that the index of the kernel is divisible by p. The Mordell–Weil sieve diagram can be amended by using several primes v of good reduction or working with residue classes of $J(\mathbf{Q})$; it is also possible to make use of primes of bad reduction and to go deeper into the filtration $(J_i)_i$.

For simplicity, we suppose that $r=g$ and we fix a basis $D_1,\dots,D_g$ of $J(\mathbf{Q})/J(\mathbf{Q})_{\text{torsion}}$. If $x\in X(\mathbf{Q}_p)$ were to be rational, and we expressed

$$i_b(x)=\sum_{j=1}^{g} m_j D_j,\ m_j\in\mathbf{Z}\,,$$

then we would have, via the linearity of the Coleman integral of regular 1-forms on the Jacobian,

$$\int_b^x \omega_i = \sum_{j=1}^g m_j \int_0^{D_j} \omega_i, \text{ for each } i \in \{1, \dots, g\} \tag{48}$$

where we identify ω_i with the holomorphic differential it induces on J via ι_b. This can be used to determine the m_j for given $x \in X(\mathbf{Q}_p)$ modulo p^n for any n. We are done if we can show for every $x \in X_{\text{extra}}$ that the resulting coset of $J(\mathbf{Q})/p^n J(\mathbf{Q})$ does not meet the pullback of $i_{b,v}$ under $\text{red}_{J,v}$ for some v.

6.7.1. $X_0(67)^+$. We now give some details of this computation for $X_0(67)^+$, using the model

$$y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1\,;$$

we have for X_{known} the 10 points found in (44). The quadratic Chabauty computation described above also results in a set X_{extra} of 11-adic points of cardinality 14, known to finite precision, whose elements are roots of the function Q in (46), but which do not appear to be rational. See Table 1 for their x-coordinates.

As above, we take $b = (1, 1)$; with this choice $D_1 = i_b(\infty^-)$ and $D_2 = i_b(\infty^+)$ are generators for $J(\mathbf{Q})$. In terms of this basis, we find that $i_b(X_{\text{known}})$ is given by pairs

$$(m_1, m_2) \in \{(1,0), (0,1), (-6,4), (7,-3), (3,-1), (-2,2), (1,1), (0,0), (8,-5), (-7,6)\}\,.$$

Since we are working with $p = 11$, we look for primes v such that $\text{ord}_{11}(\#J(\mathbf{F}_v))$ is large.

We find that

$$J(\mathbf{F}_{31}) \simeq (\mathbf{Z}/(3\cdot 11))^2 \text{ and } J(\mathbf{F}_{137}) \simeq \mathbf{Z}/3 \oplus \mathbf{Z}/(3\cdot 11^2\cdot 19)$$

and the image of $J(\mathbf{Q})/11^2 J(\mathbf{Q})$ inside these groups surjects onto the 11-parts. We pull back the images of $i_{b,31}$ and $i_{b,137}$ to cosets for $J(\mathbf{Q})/11^2 J(\mathbf{Q})$. Using (48) we compute $i_b(x)$ modulo 11^2 for all $x \in X_{\text{extra}}$, assuming x is rational, and we find that this does not meet our cosets for 31 or 137.

6.7.2. *Further examples.* In the case of $N = 73$ we run computations analogous to the ones described above, using the prime $p = 5$ for the quadratic Chabauty procedure. This gives 6 "extra" points, which can be shown to be non-rational by applying the Mordell–Weil sieve using the primes 43 and 499. Likewise for $N = 103$ we can perform quadratic Chabauty at $p = 17$, and we can once again apply the Mordell–Weil sieve with the single prime 1093 to rule out the extra 17-adic points.

6.7.3. *Conclusion.* In summary, we have shown:

Theorem 6.3. *The number of rational points on the Atkin–Lehner quotient modular curves $X_0(N)^+$ for $N \in \{67, 73, 103\}$ are as follows:*

$$\#X_0(67)^+(\mathbf{Q}) = 10\,, \quad \#X_0(73)^+(\mathbf{Q}) = 8\,, \quad \#X_0(103)^+(\mathbf{Q}) = 8\,.$$

According to [Gal96], this shows that $X_0(67)^+(\mathbf{Q})$ contains no exceptional points and that $X_0(73)^+(\mathbf{Q})$ and $X_0(103)^+(\mathbf{Q})$ contain precisely one exceptional point each, up to the hyperelliptic involution. Here an exceptional point is a rational point that is neither a cusp nor a CM point.

Furthermore, we may conclude that the table in [Box19, § 4.6] contains all quadratic points on $X_0(67)$ and the table in [Box19, § 4.7] contains all quadratic points on $X_0(73)$, complementing [Box19, Theorem 1.1].

Finally, our theorem implies that the list of j-invariants of $\mathbf{Q}$-curves attached to non-cuspidal rational points on $X_0(N)^+$ given in [BGX19, §4.1] is complete for $N \in \{67, 73, 103\}$.

Acknowledgements. We would like to thank Barry Mazur, whose kind enthusiasm and encouragement were a great motivation for the writing of this paper. We thank Netan Dogra, Kiran Kedlaya, Minhyong Kim, Bjorn Poonen, Michael Stoll, Akshay Venkatesh, and John Voight for many useful conversations and suggestions relating to the material in this article, and Bas Edixhoven and Guido Lido for sharing an early version of their preprint [EL19] with us and for providing several useful suggestions and corrections on an earlier version of this article. Most of the computations described in Section 6 were done at the Workshop "Arithmetic Statistics and Diophantine Stability" at the Fondation des Treilles in July 2018. We are grateful to Barry Mazur and Karl Rubin for organizing this event.

JB was supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023. AB was supported by Simons Foundation grant #550023. FB was supported by EPSRC and by Balliol College through a Balliol Dervorguilla scholarship. BL was supported by an NSF postdoctoral fellowship. SM was partially supported by DFG grant MU 4110/1-1. NT was supported by an NSF Graduate Research Fellowship under grant #1122374, by Simons Foundation grant #550033, and by the Research and Training Group in Algebra, Algebraic Geometry, and Number Theory at the University of Georgia during various stages of this project. JV was supported by Francis Brown and ERC-COG 724638 'GALOP', the Carolyn and Franco Gianturco Fellowship at Linacre College (Oxford), and NSF Grant No. DMS-1638352, during various stages of this project.

References

[Bal15] J. Balakrishnan. Coleman integration for even-degree models of hyperelliptic curves. *LMS J. Comput. Math.*, 18(1):258–265, 2015. ↑4.

[BBBM19] J.S. Balakrishnan, A. Besser, F. Bianchi, and J.S. Müller. Explicit quadratic Chabauty over number fields. *ArXiv preprint*, arXiv:1910.04653, 2019. ↑2.

[BBK10] J. Balakrishnan, R. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory (ANTS-IX)*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. ↑4.

[BBM17] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86(305):1403–1434, 2017. ↑28.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp*, 24(3-4):235–265, 1997. ↑4, 24, 25.

[BD18] J. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. ↑3, 16, 17, 19, 20, 21.

[BD19a] J. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *Arxiv preprint*, arXiv:1705.00401v2, 2019. ↑3, 16, 20, 21, 23.

[BD19b] A. Betts and N. Dogra. Ramification of étale path torsors and harmonic analysis on graphs. *ArXiv preprint*, arXiv:1909.05734, 2019. ↑25.

[BDM$^+$19] J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Annals of Math.*, 189(3), 2019. ↑3, 16, 17, 22, 23, 25, 26.

[BE] D. Bertrand and B. Edixhoven. Pink's conjecture on unlikely intersections and families of semi-abelian varieties. *ArXiv Preprint*, arXiv:1904.01788. ↑18.

[BGX19] F. Bars, J. González and X. Xarles Hyperelliptic parametrizations of $\mathbb{Q}$-curves. *ArXiv Preprint*, arXiv:1910.10545. ↑24, 30.

[Box19] J. Box. Quadratic points on modular curves with infinite Mordell–Weil group. *ArXiv Preprint*, arXiv:1906.05206, 2019. ↑30.

[BPSS] A. Booker, D. Platt, J. Sijsling, and A. Sutherland. Genus 3 hyperelliptic curves. http://math.mit.edu/~drew/lmfdb_genus3_hyperelliptic.txt. ↑4.

[BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. ↑28.

[BT19] J. Balakrishnan and J. Tuitman. Explicit Coleman integration for curves. *ArXiv Preprint*, arXiv:1710.01673, 2019. ↑4.

[Can87] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987. ↑29.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑21.

[Cha41] C. Chabauty. Sur les points rationels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci.*, 212:882–884, 1941. ↑3.

[CK10] J. Coates and M. Kim. Selmer varieties for curves with CM jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010. ↑17.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019. ↑14.

[Coh00] H. Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Texts in Mathematics*. Springer, 2000. ↑12, 13.

[Col85] R. Coleman. Torsion points on curves and p-adic abelian integrals. *Annals of Math.*, 121:111–168, 1985. ↑3, 4.

[Cre97] J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. ↑25.

[CS86] G. Cornell and J. Silverman. *Arithmetic Geometry*. Springer-Verlag, New York, 1986. ↑1.

[Del85] Pierre Deligne. Représentations ℓ-adiques. In *Astérisque 124*. 1985. ↑13.

[Del89] P. Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$, volume 16 of *Math. Inst. Res. Inst. Publ.*, pages 79–297. Springer-Verlag, 1989. ↑16.

[Dog19] N. Dogra. Unlikely intersections and the Chabauty–Kim method over number fields. *ArXiv preprint*, arXiv:1903.05032v2, 2019. ↑2.

[Dok04] Tim Dokchitser. Computing special values of motivic L-functions. *Experiment. Math.*, 13(2):137–149, 2004. ↑25.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In W. Kuyk, editor, *Modular forms in one variable II*, volume 349 of *LNM*, pages 143–316. Springer-Verlag, 1973. ↑25.

[EH] J. Ellenberg and D. Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty. *ArXiv preprint*, arXiv:1706.00525. ↑17.

[EL19] B. Edixhoven and G. Lido. Geometric quadratic Chabauty. *ArXiv Preprint*, arXiv:1910.10752, 2019. ↑16, 17, 18, 31.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ↑1, 6, 7.

[FL82] Jean-Marc Fontaine and Guy Laffaille. Construction de représentations p-adiques. *Annales scientifiques de l'É.N.S.*, 14(4):547–608, 1982. ↑15.

[FM12] Benson Farb and Dan Margalit. *A Primer on Mapping Class Groups*. Princeton University Press, 2012. ↑11.

[Gal96] S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. ↑25, 30.

[GLLM15] Fritz Grunewald, Michael Larsen, Alexander Lubotzky, and Justin Malestein. Arithmetic quotients of the mapping class group. *Geometric and Functional Analysis*, 25:1493–1542, 2015. ↑11.

[Gro97] Alexander Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge University Press, 1997. ↑16.

[GZ86] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ↑25.

[Har12] M. C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *J. Symb. Comp.*, 47(1):89 – 101, 2012. ↑24.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001. ↑14, 15, 24.

[Ked07] K. Kedlaya. p-adic cohomology: from theory to practice. *Arizona Winter School Notes*, 2007. ↑14.

[Ked09] Kiran S. Kedlaya. p-adic cohomology. In *Algebraic geometry—Seattle 2005. Part 2*, volume 80 of *Proc. Sympos. Pure Math.*, pages 667–684. Amer. Math. Soc., Providence, RI, 2009. ↑14.

[Kim05] M. Kim. The motivic fundamental group of $\mathbf{P}^1\setminus\{0,1,\infty\}$ and the theorem of Siegel. *Invent. Math.*, 161:629–656, 2005. ↑1, 16, 17, 19.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑1, 3, 16, 17, 19.

[Kim10] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑1.

[KL89] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989. ↑25.

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73:333–357, 2004. ↑14.

[KM07] Kamal Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239, 2007. ↑29.

[Lau04] Alan G. B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc. (3)*, 88(3):565–602, 2004. ↑15.

[Lau06] Alan G. B. Lauder. A recursive method for computing zeta functions of varieties. *LMS J. Comput. Math.*, 9:222–269, 2006. ↑15, 27.

[Loo97] Eduard Looijenga. Prym representations of mapping class groups. *Geom. Dedicata*, 64(1):69–83, 1997. ↑11.

[LV18] B. Lawrence and A. Venkatesh. Diophantine problems and p-adic period mappings. *ArXiv preprint*, arXiv:1807.02721v1, 2018. ↑1, 7, 8, 9, 10.

[Mas19] Nicolas Mascot. Hensel-lifting torsion points on Jacobians and Galois representations. *ArXiv preprint*, arXiv:1808.03939, 2019. ↑13.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Phil. Soc.*, 21:179–192, 1922. ↑1.

[MP12] W. McCallum and B. Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012. ↑3, 4.

[Mum83] David Mumford. *Tata lectures on theta*. Birkhäuser, 1983. ↑14.

[Mur92] Naoki Murabayashi. On normal forms of modular curves of genus 2. *Osaka J. Math.*, 29(2):405–418, 1992. ↑25.

[Nek93] J. Nekovar. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. ↑20, 21.

[Ogg75] A. P. Ogg. Automorphismes de courbes modulaires. In *Séminaire Delange-PisotPoitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 7*, page 8. 1975. ↑25.

[Sik13] Samir Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013. ↑2.

[Sik15] Samir Siksek. Chabauty and the Mordell-Weil sieve. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 194–224. IOS, Amsterdam, 2015. ↑28.

[ST18] Nick Salter and Bena Tshishiku. Arithmeticity of the monodromy of some Kodaira fibrations. *ArXiv Preprint*, arXiv:1805.06789, 2018. ↑11.

[Ste00] W. Stein. *Explicit approaches to modular abelian varieties*. ProQuest LLC, Ann Arbor, MI, 2000. Thesis (Ph.D.)–University of California, Berkeley. ↑25.

[SV14] J. Sijsling and J. Voight. On computing Belyĭ maps. *Publications mathématiques de Besançon*, (1):73–131, 2014. ↑13.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016. ↑15, 23, 27.

[Tui17] J. Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. ↑15, 23, 27.

J. S. Balakrishnan, Department of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

E-mail address: jbala@bu.edu

A. J. Best, Department of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

E-mail address: alex.j.best@gmail.com

F. Bianchi, Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

E-mail address: francescabianchi25@gmail.com

B. Lawrence, Department of Mathematics, University of Chicago, 5734 S University Ave, Chicago, IL 60637, USA

E-mail address: brianrl@math.uchicago.edu

J. S. Müller, Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

E-mail address: steffen.muller@rug.nl

N. Triantafillou, Department of Mathematics, University of Georgia, Athens, GA 30602, USA

E-mail address: nicholas.triantafillou@uga.edu

J. Vonk, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ 08540, USA

E-mail address: vonk@ias.edu