

# Rational Points on Curves

MARK SAENGRUNGKONGKA

May 4, 2026

Throughout this article, let  $K$  be a number field and  $\mathcal{O}_K$  be its ring of integers. For any field  $F$ , let  $\text{Gal}_F = \text{Gal}(\overline{F}/F)$ . A curve (over  $K$ ) is said to be **nice** if it is smooth, projective, and geometrically integral.

## §1 Introduction

### §1.1 Faltings' Theorem

Determining rational points on curve over a number field  $K$  has been of a central interest in arithmetic geometry for the last century. The following result is fundamental.

 **Theorem 1.1** (Faltings).

Let  $X$  be a nice curve over  $K$  with genus at least 2. Then the set of  $K$ -points  $X(K)$  is finite.

There are three different proofs of this theorem, all very difficult.

- Faltings' original proof ([Fal83], or [Fal86] for translation), which proves the finiteness result that for any abelian variety  $A$  over  $K$ , there are finitely many abelian varieties  $B$  over  $K$  that is isogenous to  $A$ . The proof of this introduces height functions on the moduli space of abelian varieties and shows that it behaves well under isogenies.
- Vojta's approach based on diophantine approximation [Voj91], which is simplified by Bombieri [Bom90].
- Lawrence and Venkatesh's approach [LV20], which borrows some of the easier ideas from Faltings' proof but replaces the difficult argument with  $p$ -adic Hodge theory.

All three known proofs of Faltings' theorem are ineffective, in the sense that it does not give an algorithm for finding rational point on curves. In a recent preprint by Alpöge and Lawrence [AL24], they give a conditional algorithm.

 **Theorem 1.2** (Alpöge and Lawrence).

There exists a Turing machine  $T$  taking a nice curve  $X$  over  $K$  of genus at least 2 as an input such that

- if  $T$  terminates, then it outputs the complete list of  $K$ -points  $X(K)$ , and
- assuming the Hodge, Tate, and Fontaine-Mazur conjectures,  $T$  always terminates.

Although Alpöge and Lawrence give *some* algorithm, their algorithm is extremely impractical since it relies on brute force search for various objects. Alpöge even called it “literally the world’s worst algorithm”.<sup>1</sup> Regardless of how impractical the algorithm is, their result gives a strong evidence that finding rational points on a curve should be decidable. In contrast, the work by Davis, Matiyasevič, Putnam, and Robinson (negatively resolving the Hilbert’s tenth problem) shows that the problem of finding **integer** points on a **variety** is undecidable [DPR61; Mat70].

## §1.2 A Curious Family of Curves


The common thread of Faltings’ original proof of Faltings’ theorem, Lawrence and Venkatesh’s proof of Faltings’ theorem, and Alpöge and Lawrence’s algorithm is the use of a family of curves over  $X$ . More specifically, they construct a smooth morphism

$$Y \rightarrow X$$

defined over  $K$  such that for each  $x \in X$ , the fiber  $Y_x$  is a curve. This map should have the property that for each curve  $Z$ , there exists finitely many  $x \in X(K)$  such that  $Y_x \simeq Z$ .

Furthermore, we claim that  $Y_x$  has a good reduction outside  $S$  for some finite set of places  $S$  not depending on  $x$ . To see this, note that the morphism  $Y \rightarrow X$  of schemes over  $K$  spreads out to a smooth morphism  $\mathcal{Y} \rightarrow \mathcal{X}$  of schemes over some open dense subset of  $\text{Spec } \mathcal{O}_K$ . In particular, the morphism  $\mathcal{Y} \rightarrow \mathcal{X}$  is smooth over  $\mathcal{O}_{K,S}$ , the ring of  $S$ -integers, for some finite set  $S$  of places. Thus, the fiber  $\mathcal{Y}_x$  is smooth for any  $x \in X(K)$ , which implies that  $Y_x$  has a good reduction outside  $S$ .

Assuming the existence of such family, the above discussion allows us to reduce the Faltings’ theorem (Theorem 1.1) to the following conjecture, which Faltings proved en route to proving the Faltings’ theorem.

 **Theorem 1.3** (Shafarevich’s Conjecture, proved by Faltings).

Given a finite set  $S$  of primes in  $K$  and an integer  $g \geq 1$ , there exists finitely many curves  $X$  over  $K$  of genus  $g$  that has good reduction at every prime outside  $S$ .

Shafarevich’s Conjecture implies Faltings’ theorem because it tells that there are finitely many isomorphism classes of  $Y_x$ , and from our condition of a family, each isomorphism classes lead to finitely many possibilities of point  $x \in X(K)$ .

In Section 2, we will explain this construction in detail.

Faltings directly proved Theorem 1.3. On the other hand, Lawrence and Venkatesh [LV20] took a different approach by further transforming the curve into a Galois representation. In particular, we have a composition

$$X(K) \longrightarrow \{\text{curves}\} \longrightarrow \{\text{representation } \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GL}_n(\mathbb{Q}_\ell)\},$$

where the first map sends  $x$  to  $Y_x$ . The image of this map is a Galois representation unramified outside  $S$ . Using Hermite’s theorem, Faltings prove that the image of this map is finite (which we will explain the proof in Section 3). An argument involving  $p$ -adic Hodge theory, Gauss-Manin connection, and monodromy calculation shows that this map has finite fibers.

## §2 The Kodaira-Parshin Family

In this section, we will discuss the **Kodaira-Parshin family**, which allows us to transform a point in  $X(K)$  to a curve with good reduction outside  $S$ . To simplify the discussion, we will only discuss the

<sup>1</sup>quotation from <https://alpo.ge/>

construction in  $\mathbb{C}$ . One can use descent to show that it is defined over  $K$ , which we omit the details. The exposition in this section follows [Poo21, §3], and the missing proof can be found at [LV20, §7]

Let  $X$  be a nice curve over  $K$  of genus  $g \geq 2$ . Since  $X(\mathbb{C})$  is homeomorphic to a  $g$ -holed torus, an application of Seifert-van Kampen theorem gives the fundamental group of  $X(\mathbb{C})$  (at any base point).

$$\pi_1(X(\mathbb{C})) \simeq \langle a_1, \dots, a_g, b_1, \dots, b_g \mid [a_1, b_1] \cdots [a_g, b_g] = 1 \rangle$$

(here  $[a, b] = aba^{-1}b^{-1}$ ). For each point  $x \in X(\mathbb{C})$ , we have that

$$\pi_1(X(\mathbb{C}) \setminus \{x\}) \simeq \langle a_1, \dots, a_g, b_1, \dots, b_g, c \mid [a_1, b_1] \cdots [a_g, b_g]c = 1 \rangle,$$

where  $c$  is a class of a small loop around  $x$ .

We now fix a finite group  $G$ . Any surjective map  $\alpha : \pi_1(X(\mathbb{C}) \setminus \{x\}) \rightarrow G$  gives  $G$  a transitive  $\pi_1(X(\mathbb{C}) \setminus \{x\})$ -action, and thus produces a covering space  $Z \rightarrow X(\mathbb{C})$  ramified precisely at  $x$ . Riemann existence theorem then shows that  $Z = Y_{x,\alpha}(\mathbb{C})$  for some algebraic curve  $Y_{x,\alpha}$ , giving a map of algebraic curves  $Y_{x,\alpha} \rightarrow X$  ramified precisely at  $x$ .

We let  $Y_x = \coprod_{\alpha} Y_{x,\alpha}$  (which is a finite union)<sup>2</sup>, so we get a map  $Y_x \rightarrow X$  ramified precisely at  $x$ . As  $x$  vary continuously in  $X(\mathbb{C})$ , the curve  $Y_x(\mathbb{C})$  also vary continuously, so their union  $\coprod_x Y_x(\mathbb{C})$  is a 2-dimensional complex analytic manifold, producing a map  $\coprod_x Y_x(\mathbb{C}) \rightarrow X(\mathbb{C})$  whose fiber at  $x$  is  $Y_x(\mathbb{C})$ . It turns out that there exists a map of complex varieties  $Y \rightarrow X$  such that for any  $x \in X(\mathbb{C})$ , the fiber at  $x$  is actually isomorphic to our  $Y_x$ .

Even better, this construction is canonical enough to be defined over  $K$ . [LV20] proves this using a standard technique of Galois descent, although more algebraic and general constructions exist in literature.

We now have to show that for any curve  $Z$ , there exists finitely many  $x \in X(K)$  such that  $Y_x \simeq Z$ . To do this, we use the following result from algebraic geometry.

 **Theorem 2.1** (de Franchis).

Let  $X'$  and  $X$  be two curves over a field  $K$  such that  $X$  has genus at least 2. Then there are finitely many morphisms  $X' \rightarrow X$ .

► *Proof.* See, for example, [Mil08, Thm. IV.5.2] □

Since  $Y_x \rightarrow X$  ramified precisely at  $x$ , we get that  $Y_x \rightarrow X$  and  $Y_{x'} \rightarrow X$  are not the same for any distinct  $x, x' \in X(K)$ . Thus, the claim then follows from de Franchis' theorem.

**i Remark 2.2.**

Lawrence and Venkatesh [LV20] construct an additional family on top of  $Y \rightarrow X$ , giving a family

$$Z \rightarrow Y \rightarrow X$$


such that for each  $x \in X(K)$ , the fiber  $Z_x$  is an abelian variety. The construction is using the Prym variety out of the covering  $Y_x \rightarrow X$ .

By the same logic, as in the introduction, there exists a finite set of primes  $S$  such that for all  $x \in X(K)$ , the fiber  $Z_x$  has good reduction outside  $S$ .

<sup>2</sup>Lawrence and Venkatesh [LV20] gives a slightly different construction where  $G$  is center-free and the union is taken across conjugacy classes of  $\alpha$ 's.

### §3 Galois Representations

In what follows,  $\ell$  is a rational prime number.


 **Definition 3.1** (Galois Representation).

Let  $V$  be finite-dimensional  $\mathbb{Q}_\ell$ -vector space with dimension  $r$ . An  $\ell$ -adic **Galois representation** over  $K$  is a continuous map

$$\rho : \text{Gal}_K \longrightarrow \text{Aut } V \simeq \text{GL}_r(\mathbb{Q}_\ell).$$

Here we put a profinite topology on  $\text{Gal}_K$  and the  $\ell$ -adic topology on  $\text{GL}_r(\mathbb{Q}_\ell)$ .

The most important source of Galois representation is from torsion of abelian variety. In particular, given an abelian variety  $A$  of dimension  $g$  over  $K$ , recall that the  $m$ -torsion (over  $\bar{K}$ ) is  $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$ . The Galois group  $\text{Gal}_K$  acts on  $A[m]$ , providing a map  $\text{Gal}_K \rightarrow \text{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$ . We take the inverse limit of these maps when  $m = \ell^n$  for all  $n \geq 0$  to get the following.

 **Definition 3.2** (Tate Module).

Given an abelian variety  $A$  of dimension  $g$ , we define the **Tate module**  $T_\ell A$  by


$$T_\ell A = \varprojlim_{n \geq 0} A[\ell^n].$$

Notice that  $A[\ell^n] \simeq (\mathbb{Z}/\ell^n)^{\oplus 2g}$ , so  $T_\ell A \simeq \mathbb{Z}_\ell^{\oplus 2g}$ . Now, let

$$V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^{\oplus 2g}.$$

The action of  $\text{Gal}_K$  on  $V_\ell A$  gives a Galois representation  $\text{Gal}_K \rightarrow \text{GL}_{2g}(\mathbb{Q}_\ell)$ .

We now discuss some properties of Galois representations.

 **Definition 3.3.**

A Galois representation  $\text{Gal}_K$  acting on  $V$  is **unramified at  $\mathfrak{p}$**  if the action when restricted to the inertia group  $I_{\mathfrak{p}} \subseteq \text{Gal}_{K_{\mathfrak{p}}} \hookrightarrow \text{Gal}_K$  is trivial.

If  $A$  has a good reduction at prime  $p \neq \ell$ , then the reduction map  $A[\ell^n] \rightarrow \tilde{A}[\ell^n]$  is injective by injectivity of torsion lemma ([HS00, Thm. C.1.4]). Therefore,  $V_\ell A$  is unramified at  $p$ .

We now apply all our observations to study the Kodaira-Parshin family as constructed in the previous section. For each  $x \in X(K)$ , the fiber  $Y_x$  is a curve with good reduction outside  $S$ . Its Jacobian  $\text{Jac}(Y_x)$  has good reduction outside  $S$ . Therefore,  $V_\ell(\text{Jac}(Y_x))$  is an  $\ell$ -adic Galois representation unramified outside  $S$ .

The fact that our Galois representation is unramified outside  $S$  poses a severe restriction of all possible Galois representations. To illustrate this, we prove the following result due to Faltings.

 **Theorem 3.4.**

Fix a finite set of primes  $S$ , a prime  $\ell$ , and a positive integer  $d$ . Then there exists a finite set  $T = T_{S, \ell, d}$  consisting of primes in  $\mathcal{O}_K$  such that if  $\rho_1, \rho_2 : \text{Gal}_K \rightarrow \text{GL}_d(\mathbb{Q}_\ell)$  are  $d$ -dimensional

$\ell$ -adic Galois representation unramified outside  $S$  such that

$$\mathrm{tr} \rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr} \rho_2(\mathrm{Frob}_{\mathfrak{p}})$$

for all  $\mathfrak{p} \in T$ , then  $\mathrm{tr} \rho_1(g) = \mathrm{tr} \rho_2(g)$  for all  $g \in \mathrm{Gal}_K$ .

► *Proof.* Let  $n = \ell^{2d^2}$ . We first prove the following claim.

**Claim.** There exists a finite set  $T$  of primes in  $\mathcal{O}_K$  such that for any finite group  $G$  of order at most  $n$  and any continuous representation  $\chi : \mathrm{Gal}_K \rightarrow G$  unramified outside  $S$ , we have  $\mathrm{Im} \chi = \{\chi(\mathrm{Frob}_{\mathfrak{p}}) : \mathfrak{p} \in T\}$ .

*Proof.* Let  $L_\chi$  be a fixed field of  $\mathrm{Ker} \chi$ . Thus,  $\chi$  factors through  $\mathrm{Gal}(L_\chi/K)$ . Note that  $[L_\chi : K] \leq n$  and  $L_\chi/K$  is unramified outside  $S$ . By Hermite's theorem, there are finitely many number fields of degree at most  $n$  unramified outside  $S$ . Let  $L$  be their compositum, so  $L_\chi \subseteq L$  for all possible  $\chi$ . Thus, there exists  $L$  depending only on  $K$  and  $n$  such that  $\chi$  factors through  $\mathrm{Gal}(L/K)$ .


Now, by Chebotarev's density theorem, there exists a finite set  $T$  of primes in  $\mathcal{O}_K$  such that  $\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \in T\}$  contains every element in  $\mathrm{Gal}(L/K)$ . This set of  $T$  satisfies the required condition. ■

Back to the main proof. We claim that this set of  $T$  works. Without loss of generality, assume that  $\rho_1$  and  $\rho_2$  take values in  $\mathrm{GL}_d(\mathbb{Z}_\ell)$  (since by compactness of  $\mathrm{Gal}_K$ , the denominator of elements in  $\rho_1(\mathrm{Gal}_K)$  and  $\rho_2(\mathrm{Gal}_K)$  are bounded). Let  $R$  be the  $\mathbb{Z}_\ell$ -module generated by

$$\{(\rho_1(g), \rho_2(g)) : g \in \mathrm{Gal}_K\} \subseteq \mathrm{Mat}_{d \times d}(\mathbb{Q}_\ell) \times \mathrm{Mat}_{d \times d}(\mathbb{Q}_\ell).$$

This is a  $\mathbb{Z}_\ell$ -algebra. We let  $\chi$  be the composition  $\mathrm{Gal}_K \rightarrow R^\times \rightarrow (R/(\ell))^\times$ . Since  $(R/(\ell))^\times$  injects to  $\mathrm{GL}_d(\mathbb{F}_\ell)^2$ , we get that its cardinality is at most  $\ell^{2d^2}$ . Thus, by the claim, we get that  $\mathrm{Im} \chi = \{\chi(\mathrm{Frob}_{\mathfrak{p}}) : \mathfrak{p} \in T\}$ . In particular, we get that the set  $\{(\rho_1(\mathrm{Frob}_{\mathfrak{p}}), \rho_2(\mathrm{Frob}_{\mathfrak{p}})) : \mathfrak{p} \in T\}$  spans  $R/(\ell)$  as  $\mathbb{F}_\ell$ -vector space. Therefore, by Nakayama's lemma, we get that  $\{(\rho_1(\mathrm{Frob}_{\mathfrak{p}}), \rho_2(\mathrm{Frob}_{\mathfrak{p}})) : \mathfrak{p} \in T\}$  spans  $R$  (as  $\mathbb{Z}_\ell$ -module). Since  $\mathrm{tr} \rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr} \rho_2(\mathrm{Frob}_{\mathfrak{p}})$  for all  $\mathfrak{p} \in T$ , we get that  $R$  is contained in  $\{(A, B) : \mathrm{tr} A = \mathrm{tr} B\}$ , which implies that  $\mathrm{tr} \rho_1(g) = \mathrm{tr} \rho_2(g)$  for all  $g \in \mathrm{Gal}_K$ . □

Thus, knowing trace at finitely many primes is sufficient to determine the trace of the whole representation. It turns out that in a specific case of  $V_\ell A$  for abelian variety  $A$ , knowing the trace is sufficient to determine the abelian variety up to isogeny.

 **Theorem 3.5** (Traces determine abelian varieties up to isogeny).

Let  $A$  and  $B$  be two abelian varieties of dimension  $g$  over  $K$  such that for every prime  $\mathfrak{p} \in T_{S, \ell, 2g}$ , we have  $\mathrm{tr} \mathrm{Frob}_{\mathfrak{p}}|_{V_\ell A} = \mathrm{tr} \mathrm{Frob}_{\mathfrak{p}}|_{V_\ell B}$ . Then  $A$  and  $B$  are isogenous.

► *Proof.* By Theorem 3.4, we get that  $\mathrm{tr} \sigma|_{V_\ell A} = \mathrm{tr} \sigma|_{V_\ell B}$  for all  $\sigma \in \mathrm{Gal}_K$ . Now, the result follows from three famous facts about abelian varieties.

- **Semisimplicity.** The  $\mathrm{Gal}_K$ -representation  $V_\ell A$  is semisimple for all abelian varieties  $A$  [Mil08, Thm. IV.2.5].
- **Brauer-Nesbitt Theorem.** If  $V_1$  and  $V_2$  are  $d$ -dimensional  $\ell$ -adic semisimple Galois representations such that  $\mathrm{tr} \sigma|_{V_1} = \mathrm{tr} \sigma|_{V_2}$  for all  $\sigma \in \mathrm{Gal}_K$ , then  $V_1 \simeq V_2$ .
- **Tate's Isogeny Theorem.** If  $V_\ell A \simeq V_\ell B$  as  $\mathrm{Gal}_K$ -representations, then  $A$  and  $B$  are isogenous. □

In order to restrict the search space of Galois representation, we note the following result, which severely restricts the possibility of  $\mathrm{tr} \rho(\mathrm{Frob}_{\mathfrak{p}})$  from the entire  $\mathbb{Q}_\ell$  to finitely many values.

 **Theorem 3.6.**


Let  $A$  be an abelian variety with dimension  $g$ . Let  $\rho : \text{Gal}_K \rightarrow \text{GL}_{2g}(\mathbb{Q}_\ell)$  be the Galois representation of  $V_\ell A$ . We have that  $\text{tr } \rho(\text{Frob}_p) \in \mathbb{Z}$ . Moreover,  $|\text{tr } \rho(\text{Frob}_p)| \leq 2g\sqrt{|\mathcal{O}_K/\mathfrak{p}|}$ .

► *Proof.* Follows directly from the Riemann Hypothesis for abelian varieties [Mil08, Thm. II.1.1]. ◻

## §4 Conditional Algorithm to Find Rational Points

We can now flesh out Alpöge and Lawrence’s algorithm to find rational points on curves.

The main use of Hodge, Tate, and Fontaine-Mazur conjectures is to give the condition for a Galois representation to come from an abelian variety. More specifically, Alpöge and Lawrence prove the following theorem, which we state informally.

 **Theorem 4.1** (Alpöge and Lawrence, informally stated).

Let  $\rho : \text{Gal}_K \rightarrow \text{GL}_{2g}(\mathbb{Q}_\ell)$  be a Galois representation on  $V \simeq \mathbb{Q}_\ell^{\oplus 2g}$ . Then assuming Hodge, Tate, and Fontaine-Mazur conjecture, there exists a condition to determine whether  $V^{\oplus k} \simeq V_\ell A$  for some positive integer  $k$  and abelian variety  $A$ . This condition is computable in terms of  $\text{tr } \rho(g)$  for  $g \in \text{Gal}_K$ .

### §4.1 Finding Abelian Varieties with Good Reduction outside $S$

Using this, we now explain an algorithm to determine all abelian varieties of dimension  $g$  and has good reduction outside  $S$ .

The idea is as follows. Given an abelian variety  $A$  with good reduction outside  $S$ , note that  $V_\ell A$  is unramified outside  $S$ . Therefore, Theorem 3.4 and Theorem 3.6 tells that there are finitely many possibilities for trace function  $g \mapsto \text{tr } \rho(g)$ . For each such trace function, we alternate between doing the following.

- By day, search for obstruction that makes this trace function fails to come from an abelian variety.
- By night, search for an abelian variety to match it.

More specifically, given a positive integer  $g$  and a finite set  $S$  of primes in  $\mathcal{O}_K$ , we do the following.

1. Choose a prime  $\ell$  not divisible by any of the primes in  $S$ .
2. Find a finite set  $T = T_{S,\ell,g}$  of primes satisfying Theorem 3.4 (i.e., knowing traces at  $\mathfrak{p} \in T$  is sufficient to determine the traces of the whole Galois representation).
3. Initiate  $\mathcal{A} = \emptyset$ , which will be the set of resulting abelian varieties.
4. We consider each tuple  $(a_{\mathfrak{p}})_{\mathfrak{p} \in T}$  such that  $a_{\mathfrak{p}} \in \mathbb{Z}$  and  $|a_{\mathfrak{p}}| \leq 2g\sqrt{|\mathcal{O}_K/\mathfrak{p}|}$  for all  $\mathfrak{p} \in T$ .

For each such tuples, we do the following. We set the parameter  $H$  and  $N$ . In each loop, we increase  $H$  and  $N$  by 1 and do the following.

- (a) Let  $V$  be a Galois representation such that  $\text{tr } \text{Frob}_p|_V = a_p$  for all  $\mathfrak{p} \in T$ . Note that the trace  $\text{tr } \sigma|_V$  for all  $\sigma \in \text{Gal}_K$  can be computed in modulo  $\ell^N$  by following the proof of Theorem 3.4. We verify the condition in Theorem 4.1 up to modulo  $\ell^N$ . If this condition is violated modulo  $\ell^N$ , then we remove this tuple  $(a_{\mathfrak{p}})$  from  $\mathcal{C}$ .

- (b) We look at the  $H$ -th abelian variety  $A$  (under a fixed enumeration).
- i. If  $\dim B$  is not divisible by  $g$ , then we proceed to the next  $N$  and  $H$ .
  - ii. Otherwise,  $\dim B = gk$  for some positive integer  $k$ . We thus check whether  $V^{\times k}$  is isomorphic to  $V_\ell B$  by computing and comparing Frobenius traces at all primes  $\mathfrak{p} \in T_{S,\ell,k,g}$ . If they are not isomorphic, then we proceed to the next  $N$  and  $H$ .  
At this point, we know that if  $V \simeq V_\ell A$  for some abelian variety  $A$ , then  $A^{\times k}$  is isogenous to  $B$ .
  - iii. We now determine whether there exists an abelian variety  $A'$  such that  $(A')^{\times k} \simeq B$ . If not exists, proceed to the next  $N$  and  $H$ .
  - iv. If  $V \simeq V_\ell A$  for some abelian variety  $A$ , then  $A^{\times k}$  and  $(A')^{\times k}$  are isogenous, so by Poincaré irreducibility theorem,  $A$  and  $A'$  are isogenous.  
Thus, we find all abelian varieties isogenous to  $A'$  (this is done by bounding the degree of isogeny using Masser-Wüholtz isogeny estimate [MW93]) and add them to  $\mathcal{A}$ .
5. Return  $\mathcal{A}$ .

## §4.2 Finding Rational Points on Curves

Finally, we explain how to find rational points on curve.

1. First, compute the family  $Z \rightarrow X$  as in Remark 2.2 such that for all  $x \in X(k)$ , the fiber  $Z_x$  is an abelian variety with good reduction outside some finite set of primes  $S$ .
2. Let  $\mathcal{A}$  be the collection of abelian varieties over  $K$  of dimension equal to the genus of  $Z_x$  with good reduction outside  $S$ . This is enumerated using the algorithm in Section 4.1.
3. For each  $A \in \mathcal{A}$ , enumerate all point  $x \in X(K)$  such that  $\text{Jac } Y_x \simeq A$ . This is done by Mumford's explicit description of the moduli space of abelian varieties [Mum66].
4. Return the union of such  $x$  across all  $A \in \mathcal{A}$ .

## References

- [AL24] Levent Alpöge and Brian Lawrence. *Conditional algorithmic Mordell*. Preprint. Aug. 2024. URL: <https://arxiv.org/abs/2408.11653>.
- [Bom90] Enrico Bombieri. "The Mordell conjecture revisited". In: *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* 17.4 (1990), pp. 615–640. URL: [http://www.numdam.org/item?id=ASNSP\\_1990\\_4\\_17\\_4\\_615\\_0](http://www.numdam.org/item?id=ASNSP_1990_4_17_4_615_0).
- [DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. "The decision problem for exponential diophantine equations". In: *Ann. of Math. (2)* 74 (1961), pp. 425–436. URL: <https://doi.org/10.2307/1970289>.
- [Fal83] G. Faltings. "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". In: *Invent. Math.* 73.3 (1983), pp. 349–366. URL: <https://doi.org/10.1007/BF01388432>.
- [Fal86] Gerd Faltings. "Finiteness theorems for abelian varieties over number fields". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Translated from the German original [Invent. Math. 73 (1983), no. 3, 349–366; MR0718935; ibid. 75 (1984), no. 2, 381; MR0732554] by Edward Shipz. Springer, New York, 1986, pp. 9–27.
- [HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. URL: <https://doi.org/10.1007/978-1-4612-1210-2>.

- [LV20] Brian Lawrence and Akshay Venkatesh. “Diophantine problems and  $p$ -adic period mappings”. In: *Invent. Math.* 221.3 (2020), pp. 893–999. URL: <https://doi.org/10.1007/s00222-020-00966-7>.
- [MW93] David Masser and Gisbert Wüstholz. “Isogeny estimates for abelian varieties, and finiteness theorems”. In: *Ann. of Math. (2)* 137.3 (1993), pp. 459–472. URL: <https://doi.org/10.2307/2946529>.
- [Mat70] Ju.Ŧ. Matijasevič. “The Diophantineness of enumerable sets”. In: *Dokl. Akad. Nauk SSSR* 191 (1970), pp. 279–282.
- [Mil08] James S. Milne. *Abelian Varieties (v2.00)*. 2008. URL: [www.jmilne.org/math/CourseNotes/av.html](http://www.jmilne.org/math/CourseNotes/av.html).
- [Mum66] D. Mumford. “On the equations defining abelian varieties. I”. In: *Invent. Math.* 1 (1966), pp. 287–354. URL: <https://doi.org/10.1007/BF01389737>.
- [Poo21] Bjorn Poonen. “A  $p$ -adic approach to rational points on curves”. In: *Bull. Amer. Math. Soc. (N.S.)* 58.1 (2021), pp. 45–56. URL: <https://doi.org/10.1090/bull/1707>.
- [Voj91] Paul Vojta. “Siegel’s theorem in the compact case”. In: *Ann. of Math. (2)* 133.3 (1991), pp. 509–548. URL: <https://doi.org/10.2307/2944318>.