Deciding if a Genus 1 Curve has a Rational Point

Nicolas J. Swanson

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Travis Morrison, Chair
Jason LeGrow
Gretchen Matthews
Jamie Sikora

April 29, 2024
Blacksburg, Virginia

Keywords: Elliptic curves, decisional algorithms, local solubility

Deciding if a Genus 1 Curve has a Rational Point

Nicolas J. Swanson

(ABSTRACT)

Many sources suggest a folklore procedure to determine if a smooth curve of genus 1 has a rational point. This procedure terminates conditionally on the Tate-Shafarevich conjecture. In this thesis, we provide an exposition for this procedure, making several steps explicit. In some instances, we also provide MAGMA implementations of the subroutines. In particular, we give an algorithm to determine if a smooth, genus 1 curve of arbitrary degree is locally soluble, we compute its Jacobian, and we give an exposition for descent in our context. Additionally, we prove there exists an algorithm to decide if smooth, genus 1 curve has a rational point if and only if there exists an algorithm to compute the Mordeil-Weil group of an elliptic curve.

Deciding if a Genus 1 Curve has a Rational Point

Nicolas J. Swanson

(GENERAL AUDIENCE ABSTRACT)

It is unknown whether an algorithm can determine if an equation with rational coefficients has a solution in the rational numbers. This thesis examines the simplest class of such equations: those representing so called smooth curves of genus 1. We demonstrate that an algorithm can decide if these equations have a rational solution if and only if there is an algorithm that can compute all rational solutions given a single rational solution. A procedure exists for the latter, but its success relies on a conjecture. Assuming this conjecture, we explicitly construct the corresponding algorithm to decide if an equation representing a smooth curve of genus 1 has a rational solution.

Dedication

I dedicate this to my family, friends, and mentors.

Acknowledgments

I wish to extend my gratitude to Travis Morrison for his guidance and support throughout this project. Originating as a joint project for a course, I also wish to acknowledge my collaborator, Fredrick Mooers, for his assistance and camaraderie.

Contents

Chapter 1

Introduction

An elliptic curve over $\mathbb{Q}$ is a smooth, projective, genus 1 curve with a point over $\mathbb{Q}$ and is a particular object of interest in number theory and cryptography. However, some genus 1 curves have no rational points, and despite best efforts, there is no known algorithm that can distinguish elliptic curves from smooth, genus 1 curves without a rational point. This easily stated open problem makes pointless curves particularly interesting. In this thesis, we study the following question:

Given a smooth, projective, genus 1 curve C defined over $\mathbb{Q}$, is there an algorithm to decide if C has a point in $\mathbb{Q}$?

Deciding if C is an elliptic curve over $\mathbb{Q}$ is a restriction of Hilbert's 10th problem over $\mathbb{Q}$ to a subset of curves, making it an essential question in number theory and decidability. A common method of finding points on curves over $\mathbb{Q}$ is to look at local completions of $\mathbb{Q}$, which are fields with a nicer structure than $\mathbb{Q}$. The local-global principle states that a curve having a rational point over every local completion of $\mathbb{Q}$ must also have a rational point over $\mathbb{Q}$. The Hasse-Minkowski theorem states that genus 0 curves satisfy the local-global principle; however, for genus 1 curves this property dramatically fails. The Tate-Shafarevich group associated with the Jacobian, an elliptic curve that is isomorphic to C over a small extension of $\mathbb{Q}$, attempts to quantify this failure. The starting curve C represents a class inside this group and its order tells us if C has a rational point. Unfortunately, it is unknown if the Tate-Shafarevich group is finite, so we do not know if we can always identify the original curve as an element in the group in finite time. The Tate-Shafarevich conjecture states that the Tate-Shafarevich group is always finite, giving us a proof that our procedure always terminates.

A rough outline of a procedure to decide if a genus 1 curve C has a point over $\mathbb{Q}$ is as follows:

1. Decide if $C(\mathbb{R}) \neq \emptyset$. If not, then $C(\mathbb{Q}) = \emptyset$.

2. Decide if $C(\mathbb{Q}_p) \neq \emptyset$ for every completion $\mathbb{Q}_p$. If $C(\mathbb{Q}_p) = \emptyset$ for some completion, then $C(\mathbb{Q}) = \emptyset$.

3. Compute the Jacobian of C, denoted J.

4. Compute $J(\mathbb{Q})/nJ(\mathbb{Q})$ for a certain n depending on C.

5. Determine if C represents a trivial element in $Ш(J/\mathbb{Q})$, the Tate-Shafarevich group.

6. If C represents a trivial element in $Ш(J/\mathbb{Q})$, then $C(\mathbb{Q}) \neq \emptyset$. Otherwise, $C(\mathbb{Q}) = \emptyset$.

In Theorem 4.45, we prove that computing $J(\mathbb{Q})/nJ(\mathbb{Q})$ is Turing equivalent to deciding if a genus 1 curve has a rational point without the assumption of a conjecture. The primary tool used for computing $J(\mathbb{Q})/nJ(\mathbb{Q})$ is called n-descent and we will use this tool in our algorithm. It is exactly this step that requires the Tate-Shafarevich conjecture. We will not be concerned with the algorithm's runtime, as long as it terminates in a finite number of steps. The procedure we present is highly inefficient and the subroutines we have implemented in MAGMA take significant time even on small inputs. Even so, any algorithm is better than no algorithm.

1.1 Preliminaries

We recommend the reader be familiar with abstract algebra, but it is only mildly required until Chapter 3. If the reader is unfamiliar with algebraic number theory, then they should proceed with the assumption that $K = \mathbb{Q}$ and see Example 1.3. In this section, we provide a brief exposition on the prerequisite knowledge recommended.

1.1.1 Number Theory

For a detailed exposition, we refer the reader to Serre [20], Marcus [17], and Cohen [4].

A number field is a finite algebraic extension of $\mathbb{Q}$; i.e., a field $K = \mathbb{Q}(\theta)$ where θ is a root of a polynomial in $\mathbb{Q}$. There is a unique maximal order of K which we denote by O_K called the *ring of integers of* K. The ring O_K is defined as the set of all elements in K that are roots of monic polynomials in $\mathbb{Z}$.

Definition 1.1. A place of K, denoted v, is an equivalence class of absolute values. That is, v is represented by a function $|\cdot|_v \colon K \to \mathbb{R}$ satisfying

- $|a|_v \geq 0$ and $|a| = 0$ if and only if $a = 0$;
- $|ab|_v = |a|_v|b|_v$;
- $|a+b|_v \leq |a|_v + |b|_v$,

under the equivalence relation $|\cdot|_v \sim |\cdot|_w$ if and only if there exists some $\lambda \in \mathbb{R}_{>0}$ such that $|\cdot|_v = |\cdot|_w^\lambda$.

Number field places are divided into archimedean places and non-archimedean places. To be a non-archimedean place, $|\cdot|_v$ must satisfy $|a+b|_v \leq \max\{|a|_v, |b|_v\}$. An equivalent definition of the ring of integers is

$$O_K = \{x \in K \colon |x|_v \leq 1 \text{ for all non-archimedean } v\}.$$

For every place v, we can complete the field K with respect to v by taking the set of Cauchy sequences in K and modding out by the Cauchy sequences which tend to zero with respect to $|\cdot|_v$. We denote this complete field K_v and call it *the (local) completion of K at v*. These completions are examples of *local fields* and are useful when trying to find K-rational points over the *global field* K.

Example 1.2. The place $|\cdot|_0 \colon K \to \{0,1\}$ defined by $|a|_0 = 1$ for all $a \neq 0$ and $|0|_0 = 0$ is called the trivial place. It is non-archimedean and satisfies $K_v = K$.

Example 1.3. For $K = \mathbb{Q}$, there is a single archimedean place which is the typical absolute value map $|\cdot|_\infty \colon \mathbb{Q} \to \mathbb{R}$. The non-archimedean places of $\mathbb{Q}$ are the p-adic absolute values $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}$ defined by $|a|_p = p^{-r}$ where $a = p^r \frac{a'}{a''}$ and p does not divide a' nor a''. Ostrowksi's theorem tells us that these are the only the places of $\mathbb{Q}$. See [18, Theorem 1, Section 1.3] for a proof of this fact. The ring of integers of $\mathbb{Q}$ is $O_{\mathbb{Q}} = \mathbb{Z}$. The completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$ and the completion of $\mathbb{Q}$ with respect to a prime $|\cdot|_p$ is $\mathbb{Q}_p$, the p-adic numbers. Nonzero elements $\alpha \in \mathbb{Q}_p$ have a unique expansion of the form $\alpha = \sum_{n=n_0}^{\infty} a_n p^n$ where $n_0 \in \mathbb{Z}$, $a_n \in \{0, \ldots, p-1\}$ and $|\alpha|_p = p^{-n_0}$.

Example 1.3 can be generalized to number fields. The places of a number field consist of a trivial place, prime places, and places given by embeddings into either $\mathbb{R}$ or $\mathbb{C}$. If r_1 is

the number of distinct field embeddings from $K \to \mathbb{R}$ and $2r_2$ is the number of distinct field embeddings from $K \to \mathbb{C}$, then $[K : \mathbb{Q}] = r_1 + 2r_2$. If $K = \mathbb{Q}(\theta)$, then the distinct embeddings from K into $\mathbb{R}$ and $\mathbb{C}$ are given by the distinct real and complex roots of the minimal polynomial of θ, respectively. These embeddings give rise to $r_1 + r_2$ places on K coming from the restriction of the standard absolute value on $\mathbb{R}$ or $\mathbb{C}$ to the image of the embedding. There are half as many complex places as complex embeddings since every embedding has a complex conjugate embedding and $|a + bi| = |a - bi|$ in $\mathbb{C}$.

Theorem 1.4. *An archimedean place of K is given by an embedding of K into either $\mathbb{R}$ or $\mathbb{C}$. A non-archimedean place is given by a prime ideal of O_K under the bijection*

$$\begin{aligned} \mathfrak{p} &\mapsto |\cdot|_{\mathfrak{p}} \\ \{x \in O_K : |x|_v < 1\} &\leftarrow\!\shortmid |\cdot|_v \end{aligned}$$

where for any fixed $c \in (1, \infty)$, $|a|_{\mathfrak{p}} = c^{-n}$ where n satisfies $aO_K = \mathfrak{p}^n\mathfrak{t}$, but $\mathfrak{p} \nmid \mathfrak{t}$.

Proof. See [2, Chapter 4, Theorem 1]. □

The reason for generalizing our problem from $\mathbb{Q}$ to K is because our story only minorly changes. We can write $K = \mathbb{Q}(\theta) = \mathbb{Q}[x]/\langle f(x)\rangle$ for $f(x) \in \mathbb{Z}[x]$ by the primitive root theorem. While we have $\mathbb{Z}[\theta] \subseteq O_K$, equality does not generally hold, as O_K can be larger than $\mathbb{Z}[\theta]$. Instead, O_K is a computable free $\mathbb{Z}$-module of rank $\deg f(x) = [K : \mathbb{Q}]$. For a detailed explanation of an algorithm that computes O_K, see [4, Algorithm 6.1.8]. The ring O_K is a Dedekind domain, meaning for a fixed prime $p \in \mathbb{Z}$, $pO_K = \prod_{i=1}^m \mathfrak{p}_i^{e_{\mathfrak{p}_i}}$ for a unique and finite set of prime ideals *over* p, where $\mathfrak{p}_i \subset O_K$ and $e_{\mathfrak{p}_i} \in \mathbb{Z}_{>0}$ is called the ramification index of $\mathfrak{p}_i$ over p. The finite field $O_K/\mathfrak{p}$ is a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with dimension $f_{\mathfrak{p}} = [O_K/\mathfrak{p} : \mathbb{F}_p]$ called the *inertial degree* of $\mathfrak{p}$. As seen in [17, Chapter 3, Theorem 21], if $aO_K = \prod_{i=1}^m \mathfrak{p}_i^{e_{\mathfrak{p}_i}}$, then $\sum_{i=1}^m e_{\mathfrak{p}_i} f_{\mathfrak{p}_i} = [K : \mathbb{Q}]$.

If a prime $\mathfrak{p}$ satisfies $e_{\mathfrak{p}} = 1$ then it is *unramified*, if $f_{\mathfrak{p}} = 1$ then $\mathfrak{p}$ is *totally ramified*, if $p \nmid e_{\mathfrak{p}}$ then $\mathfrak{p}$ is *tamely ramified*, and if $e_{\mathfrak{p}}$ is a prime power of p then $\mathfrak{p}$ is *wildly ramified*.

For all primes p except for the finitely many that satisfy $p \,\big|\, [O_K : \mathbb{Z}[\theta]]$, it suffices to consider $f(x) \pmod p \in \mathbb{F}_p[x]$ to compute the primes over p. In this case, if $f(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod p$ where each g_i is irreducible in $\mathbb{F}_p[x]$, there are r unique prime ideals above p satisfying $\mathfrak{p}_i = \langle p, g_i(\theta)\rangle$, $e_{\mathfrak{p}_i} = e_i$, and $f_{\mathfrak{p}_i} = \deg g_i$. There is a more sophisticated algorithm to compute the decomposition $aO_K = \prod_i^m \mathfrak{p}_i^{e_i}$, for $p \,\big|\, [O_K : \mathbb{Z}[\theta]]$ as described in [4, Algorithm 6.2.9].

Example 1.5. Let $K = \mathbb{Q}\left(\sqrt{-23}\right) \cong \mathbb{Q}[x]/\langle x^2+23\rangle$. We have

$$O_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right] = \frac{\mathbb{Z}[x]}{\langle x^2-x+6\rangle}$$

and $[O_K \colon \mathbb{Z}[\sqrt{-23}]] = 2$. Thus, for every prime $p \neq 2$, primes above p are given by the irreducible factors of $x^2+23 \pmod p$. The polynomial $x^2+23 \pmod p$ is irreducible exactly when -23 is not a square mod p. In this the case there is a single prime above p given by $\mathfrak{p} = \langle p\rangle$ with $e_\mathfrak{p} = 1$ and $f_\mathfrak{p} = 2$. However, if $a^2 \equiv -23 \pmod p$ for some $a \in \mathbb{Z}$, there are two ideals $\mathfrak{p}_1, \mathfrak{p}_2$ above p given by $\mathfrak{p}_1 = \langle p, \sqrt{-23}+a\rangle$ and $\mathfrak{p}_2 = \langle p, \sqrt{-23}-a\rangle$ where $e_{\mathfrak{p}_1} = e_{\mathfrak{p}_2} = f_{\mathfrak{p}_1} = f_{\mathfrak{p}_2} = 1$. The ideals over $p = 2$ are $\mathfrak{p}_1 = \langle 2, \sqrt{23}+1\rangle$ and $\mathfrak{p}_2 = \langle 2, \sqrt{23}\rangle$.

The absolute value $|\cdot|_v$ extends naturally to K_v, and K is dense in K_v with respect to $|\cdot|_v$. The following objects are associated with K_v.

- The *ring of integers* of K_v is $R_v = \{x \in K_v \colon |x|_v \leq 1\}$.
- The *maximal ideal* of R_v is $M_v = \{x \in K_v \colon |x|_v < 1\}$.
- A *uniformizer* of M_v is any $\pi \in R_v$ such that $M_v = \pi R_v$.
- The *residue field* of K_v is $k_v = R_v/M_v$.

The ring R_v is a *discrete valuation ring* with a *valuation* $v : K_v \to \mathbb{Z} \cup \{\infty\}$ given by $v(\alpha) = -\log(|\alpha|_v)$. If v corresponds to the prime $\mathfrak{p}$, then $v\left(\frac{a}{b}\right) = m - n$ where m and n are maximal such that $\mathfrak{p}^m \,\big|\, aO_K$ and $\mathfrak{p}^n \,\big|\, bO_K$. The ring R_v is an inverse limit given by

$$\varprojlim_i \frac{R_v}{\pi^i R_v}$$

where every element $\alpha \in R_v$ can be represented with a sequence $(a_i)_{i\in\mathbb{Z}_{>0}}$ where $a_{i+1} \equiv a_i \pmod{M_v^i}$.

Example 1.6. For every prime place $|\cdot|_p$ of $\mathbb{Q}$, the completion of $\mathbb{Q}$ is the field of p-adic numbers $\mathbb{Q}_p$, and the ring of integers is $\mathbb{Z}_p$, consisting of p-adic integers. Much like $\mathbb{Q}_p$, any p-adic integer α can be expressed as a sum $\alpha = \sum_{n=0}^{\infty} a_n p^n$, such that $a_n \in \{0, \ldots, p-1\}$. The unique maximal ideal in $\mathbb{Z}_p$ is $p\mathbb{Z}_p$ with uniformizer p, and the residue field is $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$.

Generally, if v corresponds to the prime $\mathfrak{p}$ above p, then the extension $K_v/\mathbb{Q}_p$ is finite with degree $[K_v\colon \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p} \leq [K\colon \mathbb{Q}]$. The ring $R_v = (O_K)_v$ is the integral closure of $\mathbb{Z}_p$ inside K_v. The maximal ideal is $\mathfrak{p}$, with uniformizer $p^{e_\mathfrak{p}}$, and the residue field is $\mathbb{F}_q$ where $q = p^{f_\mathfrak{p}}$.

We call K_v unramified, totally ramified, tamely ramified, or wildly ramified, depending on the behavior of $\mathfrak{p}$ over p. When K_v is totally ramified, $K_v = \mathbb{Q}_p[p^{1/e_\mathfrak{p}}]$ and when K_v is unramified, $K_v = \mathbb{Q}_p[\zeta]$ where ζ is a primitive $(p^{f_\mathfrak{p}} - 1)$th root of unity.

Example 1.7. For $K = \mathbb{Q}\left(\sqrt{-23}\right)$, the primes above 2 are $\mathfrak{p}_1 = \langle 2, \sqrt{23} + 1\rangle$ and $\mathfrak{p}_2 = \langle 2, \sqrt{23}\rangle$. The completion corresponding to both prime ideals is $\mathbb{Q}_2$ and the residue field is $\mathbb{F}_2$. There is a single prime ideal over 5, given by $\mathfrak{p} = \langle 5\rangle$ and the corresponding local field is unramified meaning $K_\mathfrak{p} = \mathbb{Q}_5(\zeta)$ where $\zeta = -1$ is the primitive 2nd root of unity. The local ring is $R_v = \mathbb{Z}_5[\zeta] = \mathbb{Z}_5$ and the residue field is $k_\mathfrak{p} = \mathbb{F}_{5^2}$.

Finally, there is a unique *maximal unramified extension* of $\mathbb{Q}_v$ in K_v defined as

$$K_v^{\text{unr}} = \bigcup_{\substack{E \subseteq K_v \\ E/\mathbb{Q}_v \text{is finite} \\ \text{and unramified}}} E.$$

1.1.2 Geometry

For a comprehensive overview of the required algebraic geometry, see Silverman [21, Sections I-III] and Hartshorne [12, Chapters 1 and 4]. An *affine plane curve* C, defined over a ring R, is defined by a bivariate polynomial $f(x, y)$ with coefficients in R. The points on C over R, denoted $C(R)$, are points $(x_0, y_0) \in R^2$ satisfying $f(x_0, y_0) = 0$. A *projective plane curve* defined over a field K, is defined by a homogeneous polynomial $f(x, y, z)$ with coefficients in K. The points on the curve over K, denoted $C(K)$, are projective points $[x_0\colon y_0\colon z_0] \in \mathbb{P}^2(K)$ satisfying $f(x_0, y_0, z_0) = 0$.

A *projective curve* C, defined over a field K, is more generally a prime ideal $I(V) \subseteq K[X_1, \ldots, X_{n+1}]$ generated by homogeneous polynomials in V such that the *function field of* C *over* $\bar{K}$,

$$\bar{K}(C) = \text{Fr}\left(\frac{\bar{K}[X_1, \ldots, X_{n+1}]}{I(V \cap \mathbb{A}^n)}\right),$$

has transcendence degree 1 over $\bar{K}$. The points of C over K are projective points $[x_1\colon \ldots\colon x_{n+1}] \in \mathbb{P}^n(K)$ such that $f(x_1, \ldots, x_{n+1}) = 0$ for all $f \in I(V)$.

A *singularity* of an affine plane curve $C\colon f(x,y) = 0$ defined over K is a pair $(a,b) \in \bar{K}^2$ such that $f(a,b) = \frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0$. A *singularity* of a projective curve $C\colon I(V) \subseteq K[X_1,\ldots,X_{n+1}]$ is some $P \in \mathbb{P}^n(\bar{K})$ such that the Jacobian matrix of the generating polynomials of $I(V)$ evaluated at P does not have full rank. A curve is *smooth* if there are no singularities over $\bar{K}$ and *singular* otherwise.

Proposition 1.8. *For any smooth projective curve C defined over K,*

$$K(C) \cong Fr\left(\frac{K(x)[y]}{\langle f(x,y)\rangle}\right)$$

for some irreducible, possibly singular $f(x,y) \in K[x,y]$.

Proof. See [12, Chapter 1, Theorem 6.9]. □

Remark 1.9. The algorithm we present will generally be for curves in embedded in higher dimensions, but it turns out that deciding if any curve C has a point over K can be reduced to deciding if $f(x,y)$ has points over K for two choices of $f(x,y)$.

For a proper definition of the genus of a curve, see [12, Chapter 4, Section 1]. The *arithmetic genus* of an irreducible projective plane curve $D : f(x,y,x) = 0$ is

$$g_{ar} = \frac{(d-1)(d-2)}{2}$$

where d is the degree of $f(x,y,z)$. Note that arithmetic genus can be defined for curves that are not necessarily plane or projective, but the formula differs. The *geometric genus* of a projective curve C is the topological genus of the Riemann surface formed by the points on C over $\mathbb{C}$. When C is smooth, the arithmetic genus and geometric genus agree, but in general the arithmetic genus is an upper bound for the geometric genus. Unless otherwise stated, when we refer to genus we mean geometric genus.

Definition 1.10. An *elliptic curve* over a field K is a smooth projective curve of genus 1 defined over K with a distinguished point $\mathcal{O} \in E(K)$.

Equivalently, due to the Riemann Roch theorem [21, Proposition III.3.1], an elliptic curve over K is a projective plane curve that has a model

$$y^2z + a_1xyz + a_3y^2z = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $\mathcal{O} = [0\colon 1\colon 0]$ and $a_1, a_3, a_2, a_4, a_6 \in K$.

The points of an elliptic curve over a field form an abelian group. We denote the group operation on $E(K)$ with the usual "$+, -$" notation. If the characteristic of K is not 2 or 3, then there exists a short Weierstrass model for E given by $y^2 = x^3 + Ax + B$ where $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. An elliptic curve E has a discriminant

$$\Delta(E) = -16(4A^3 + 27B^2)$$

and a j-invariant

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)}.$$

Maps between projective curves $\phi\colon C_1 \to C_2$ are important for our study, but only when C_1 and C_2 are smooth. When this is the case, the maps between them behave nicely.

Definition 1.11. Given two smooth, projective curves C_1 and C_2 defined over K, a *morphism* $\phi\colon C_1 \to C_2$ is a tuple

$$\phi = [\phi_1\colon \ \ldots : \phi_n] \in \mathbb{P}^n(K(C_1))$$

such that for every point $P \in C_1(\bar{K})$, there is some nonzero $\gamma \in K(C_1)$ satisfying

$$[\gamma\phi_1(P)\colon \ \ldots : \gamma\phi_n(P)] \in C_2(\bar{K}).$$

Remark 1.12. The coefficients of morphisms are not well-defined. Even so, there are good ways to represent such maps, for example on some $\mathbb{A}^n \subseteq \mathbb{P}^n$ via a birational map.

Definition 1.13. There is an action of $\mathrm{Gal}(\bar{K}/K)$ on $C(\bar{K})$ given by

$$P = [P_1\colon \ \ldots : P_n] \mapsto [\sigma(P_1)\colon \ \ldots : \sigma(P_n)] = P^\sigma$$

where $\sigma \in \mathrm{Gal}(\bar{K}/K)$ acts on coordinates. Moreover, we can define $\phi^\sigma\colon C_1 \to C_2$ by

$$\phi^\sigma(P) = \phi(P^{(\sigma^{-1})})^\sigma$$

where σ essentially acts on coefficients of ϕ. When $\phi^\sigma = \phi$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we say ϕ *is defined over* K.

Definition 1.14. Given two elliptic curves E_1 and E_2 with distinguished points $\mathcal{O}_1$ and $\mathcal{O}_2$, an *isogeny* $\phi\colon E_1 \to E_2$ is a nonconstant morphism of elliptic curves such that $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

The distinction between a morphism and an isogeny is subtle and can lead to confusion in terminology. An invertible morphism between elliptic curves is not the same thing as an invertible isogeny between elliptic curves. Two curves are *isomorphic as curves* if there is an invertible morphism between them. Meanwhile, two elliptic curves are *isomorphic as elliptic curves* if there is an invertible isogeny between them. To emphasise this difference, we will often avoid the use of the word "isomorphism" when dealing with elliptic curves and pointless curves simultaneously.

Proposition 1.15.

1. *Every morphism between projective curves is either surjective or constant.*
2. *Every morphism of elliptic curves $\phi\colon E_1 \to E_2$ satisfies $\phi = \tau_{\phi(\mathcal{O})} \circ \epsilon$, where $\epsilon\colon E_1 \to E_2$ is an isogeny and $\tau_{\phi(\mathcal{O})}\colon E_2 \to E_2$ is a translation map satisfying $\tau(P) = P + \phi(\mathcal{O})$.*

Proof. For a proof of the first statement, see [12, Chapter 2, Proposition 6.8] and see [21, Theorem III.4.10] for a proof of the second. □

1.1.3 Polynomial Computations

We recall an easily computable determinant that is useful when determining if two polynomials share a common factor.

Definition 1.16. Let F be a field with $f(x) = a_n x^n + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m +$

$\cdots + b_1 x + b_0$ polynomials in $F[x]$ satisfying $m, n > 0$. The *resultant* of f and g is given by

$$\operatorname{Res}(f,g) := \det \left(\begin{array}{c} \left.\begin{bmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \end{bmatrix}\right\} m \text{ rows} \\ \left.\begin{bmatrix} b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & & \vdots \\ 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{bmatrix}\right\} n \text{ rows} \end{array} \right).$$

If $f, g \in F[X_1, \ldots, X_N]$, define $\operatorname{Res}_{X_i}(f,g) \in F[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$ to be the univariate resultant over the field $F(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$.

Note the horizontal line in the middle of the matrix is meant to emphasize that the columns above the line do not necessarily align with the columns below the line. That is, m is not necessarily equal to n. Instead, the matrix is formed by creating the top and bottom matrices separately and "stacking" them.

Proposition 1.17. *Following the notation above,*

1. *If $f(x), g(x) \in F[x]$, the resultant $Res(f,g) = 0$ if and only if $a_n = b_m = 0$ or there exists some $c \in \bar{F}$ such that $f(c) = g(c)$.*

2. *If $f, g \in F[X_1, \ldots, X_n]$, let*

   - *$\alpha(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ be the leading coefficient of f regarded as a polynomial in X_i,*
   - *$\beta(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ be the leading coefficient of g regarded as a polynomial in X_i,*
   - *$h(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots X_n) = Res_{X_i}(f,g)$.*

   Then $h = 0$ identically if and only if $\alpha = \beta = 0$ identically or there exists some $q(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ of positive X_i-degree such that $q \mid f$ and $q \mid g$.

3. *Moreover,* $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \in \bar{K}$ *satisfies* $h(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = 0$ *if and only if* $\alpha(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \beta(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = 0$ *or there exists an* $x_i \in \bar{K}$ *such that* $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$.

Proof. See [14, Theorem 5.7] for a proof of the first statement. The second and third statements follow from the first using Gauss's lemma. □

Proposition 1.18. *Let* $f(x) \in K[x]$. *There exists an algorithm to find all the roots of* f *in some finite computable extension* L/K.

Proof. See [4, Algorithm 2.6.3] for such an algorithm. □

1.2 Input to the Algorithm

Unless otherwise stated, assume all curves are smooth and projective of genus 1 defined over the fixed number field K. If two curves C and C' are isomorphic as curves over K, then $C(K) \neq \emptyset$ if and only if $C'(K) \neq \emptyset$. It therefore suffices for the input of the algorithm to be a K-isomorphism class of a curve. A concrete way to specify a curve C is with homogeneous polynomials $F_1, \ldots, F_r \in K[X_1, \ldots, X_{n+1}]$ generating a prime ideal. We call the set $C\colon \{F_1, \ldots, F_r\}$ a *model* of the K-isomorphism class represented by C.

The computer algebra software MAGMA [3] has an entire page dedicated to models of genus 1 curves. One property of a model C is its *degree* n, which we will give a natural definition to in Remark 4.12. We will see in Lemma 4.9 that C has a point over K if and only if $n = 1$. There are "nice" models for C if the degree is $n = 1, 2, 3, 4, 5$ and MAGMA has implemented many of the algorithms in this paper for these models. In our case, they are not immediately useful as computing the degree of C is equivalent to determining if C has a point over K.

Recall from Proposition 1.8 that the function field of C is given by

$$K(C) \cong \mathrm{Fr}\left(\frac{K(x)[y]}{\langle f(x,y)\rangle}\right)$$

for some affine plane curve $f(x, y) = 0$ with $f(x, y) \in K[x, y]$ irreducible, but possibly singular. The input to our algorithm will be a bivariate polynomial $f(x, y)$ that uniquely defines the function field $K(C)$ up to K-isomorphism. This natural representation arises from

a contravariant categorical equivalence between curves and function fields with transcendence degree one.

In our context, the best way to think of $f(x, y)$ is as some affine patch of a projective plane curve $\hat{C}\colon F(X, Y, Z) = 0$. For example, if C is a plane curve, then $\hat{C} = C$. Otherwise, $\hat{C}$ is obtained by projecting C onto $\mathbb{P}^2$. Projection does not preserve smoothness, but the act of projection from $\mathbb{P}^m \to \mathbb{P}^{m-1}$ only creates finitely many singularities on the resulting curve. Thus the projection of C to $\mathbb{P}^2$, denoted $\hat{C}$, has finitely many singularities.

Definition 1.19. We call any $\hat{C}\colon F(X, Y, Z) = 0$ with

$$K(C) \cong \mathrm{Fr}\left(\frac{K(x)[y]}{\langle F(x, y, 1)\rangle}\right)$$

a *(possibly) singular model* for C.

The projection map $C \to \hat{C}$ is defined over K, surjective, and even injective away from the singular points of $\hat{C}$. Moreover, the singularities of $\hat{C}$ correspond to a finite number of points on C [12, Chapter 1, Lemma 6.4]. One can recover a smooth model for C from $\hat{C}$ by "blowing up" the singularities on $\hat{C}$. Blowing up a singularity is a process of resolving a singularity by embedding $\hat{C}$ in a larger projective space. Repeatedly blowing up the singularities of a curve until it is smooth is a process called desingularization. Blowing up a singularity does not change the geometric genus of a curve and can only decrease its arithmetic genus. Thus, $\hat{C}$ always has arithmetic genus at least 1 and geometric genus exactly 1.

Example 1.20. Consider C given by

$$\mathbb{Q}(C) \cong \mathrm{Fr}\left(\frac{\mathbb{Q}(x)[y]}{\langle f(x, y)\rangle}\right)$$

where $f(x, y) = y^2 - x^4 - 1 = 0$. The singular model for C is

$$\hat{C}\colon F(X, Y, Z) = Y^2Z^2 - X^4 - Z^4 = 0$$

and has arithmetic genus 3. There is one singularity on $\hat{C}$ at $[0\colon 1\colon 0]$. The curve $\hat{C}$ naturally lives in the weighted projective space $\mathbb{P}(1, 2, 1)$ with Y the variable of degree 2:

$$\hat{C}\colon Y^2 - X^4 - Z^4 = 0.$$

We blowup $\hat{C}$ at $[0\colon 1\colon 0]$ using the map $[X\colon Y\colon Z] \mapsto [X^2\colon XZ\colon Z^2\colon Y]$ to get a projective curve C in $\mathbb{P}^3$. If $[S\colon T\colon U\colon V]$ are the coordinates of $\mathbb{P}^3$, C is given by

$$C\colon \begin{cases} 0 = T^2 - SU \\ 0 = V^2 - S^2 - U^2 \end{cases}$$

which is easily checked to be smooth. The projection map $C \to \hat{C}$ given by $[S\colon T\colon U\colon V] \mapsto [S^2\colon V\colon U^2]$ is surjective and automatically injective away from inverse image of $[0\colon 1\colon 0]$. In this case, the point $[0\colon 0\colon 0\colon 1] \in C(\mathbb{Q})$ is the only preimage of $[0\colon 1\colon 0]$ and so the projection map is a $\mathbb{Q}$-isomorphism.

The projection map $C \to \hat{C}$ reduces the problem of deciding if C has a rational point to deciding if the plane curve $\hat{C}\colon F(X,Y,Z) = 0$ has a rational point. If we find a rational point on $\hat{C}$, then we know it will pullback to at least one rational point on C. Furthermore, we can determine if $\hat{C}\colon F(X,Y,Z) = 0$ has a solution in $\mathbb{P}^2$ by looking at two affine patches of $\hat{C}$. That is, we can look at the affine models $f_1(x,y) := F(X,Y,1)$ and $f_2(x,z) := F(X,1,Z)$ and note that any $[X\colon Y\colon Z]$ satisfying $F(X,Y,Z) = 0$ will map to a point on $f_1(x,y)$ or $f_2(x,z)$ unless $Y = Z = 0$. This means that the only point on $\hat{C}$ that is not on one of the affine curves $f_1(x,y) = 0$ or $f_2(x,z) = 0$ is $[1\colon 0\colon 0]$. The first step of the algorithm is to check if $F(1,0,0) = 0$.

1.3 Computing Singularities

The first nontrivial step of the algorithm is to determine if there are any K-rational singularities on the singular model $\hat{C}$. We return $C(K) \neq \emptyset$ if there exists a K-rational singularity since the projection map $C \to \hat{C}$ is surjective and defined over K. We will check if $\hat{C}$ has a K-rational singularity by looking at two affine patches of $\hat{C}$. The algorithm presented in this section will also be able to compute the distinct singularities of $\hat{C}$, as well as the finite extension L/K all the singularities are contained in.

Proposition 1.21. *Given $f(x,y) \in K[x,y]$ irreducible, let*

$$h(x) = Res_y\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) \quad \text{and} \quad k(y) = Res_x\left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right).$$

1. *Then* $h(x)$ *and* $k(y)$ *are not identically* 0.

2. *If* $(\alpha, \beta) \in \bar{K}$ *is a singularity of* $D\colon f(x, y) = 0$*, then* $h(\alpha) = k(\beta) = 0$.

Proof. Firstly, since $f(x, y)$ is irreducible, its partial derivatives do not have any nonconstant common factor and the leading coefficients of both partial derivatives in either variable is nonzero. Hence, neither $h(x)$ nor $k(y)$ is identically 0. For the second claim, note that $(\alpha, \beta) \in \bar{K}$ is a singularity when

$$\frac{\partial f}{\partial x}(\alpha, \beta) = \frac{\partial f}{\partial y}(\alpha, \beta) = 0.$$

So by Proposition 1.17, we have $h(\alpha) = k(\beta) = 0$ as desired. □

Proposition 1.21 immediately gives us the following algorithm.

Algorithm 1: Has Rational Singularity

Input: An irreducible $f(x, y) \in K[x, y]$ and a field K.

Output: TRUE if $f(x, y) = \nabla f(x, y) = 0$ has a solution over K and FALSE otherwise.

```
1  h(x) ← Res_y(∂f/∂x, ∂f/∂y);
2  k(y) ← Res_x(∂f/∂x, ∂f/∂y);
3  A ← Roots(h(x)) ;                    # We only need the distinct roots.
4  B ← Roots(k(y));
5  A ← A ∩ K;
6  B ← B ∩ K;
7  for (α, β) ∈ A × B do
8      if f(α, β) = 0 then
9          return True;
10     end
11 end
12 return False;
```

Remark 1.22. By removing lines 5 and 6 from Algorithm 1 and modifying it to return all $(\alpha, \beta) \in A \times B$ such that $f(\alpha, \beta) = 0$, we also have an algorithm to compute all the singularities of $D\colon f(x, y) = 0$. There are more sophisticated and efficient methods, such as the ones studied in [16], to find the singular points of an algebraic curve.

Chapter 2

Determining Local Solubility

The goal of this chapter is to explicitly construct an algorithm to decide if C satisfies the following definition.

Definition 2.1. A curve C defined over K is *everywhere locally soluble* (or just locally soluble) if $C(K_v) \neq \emptyset$ for all nontrivial places v of K.

If we find that $C(K_v) = \emptyset$ for a single place, then $C(K) = \emptyset$ and the algorithm to determine if C has a rational point will terminate. However, even if $C(K_v) \neq \emptyset$ for all places v, we are unable to determine if $C(K) \neq \emptyset$ without a conjecture. This is because smooth projective curves of genus 1 do not satisfy the *local-global principle* and are one of the simplest examples of algebraic varieties that do not.

Let $D\colon f(x, y) = 0$ denote any one of the three affine patches of the singular model $\hat{C}$. Recall that it suffices to determine if one of two of these affine patches has a point over K_v to decide if $C(K_v) \neq \emptyset$. For the archimedean places v, we will be able to directly determine if $D(K_v) \neq \emptyset$. However, for a non-archimedean places we will only check if $D(R_v) \neq \emptyset$. This will not be a problem as long as we check all three affine patches of $\hat{C}$ for points over R_v.

Proposition 2.2. *Given a curve C and a non-archimedean place v, there exists some $P \in C(K_v)$ if and only if $D(R_v) \neq \emptyset$ for one of the three affine patches of the singular model for C.*

Proof. ($\Leftarrow$): This direction is clear since $D(R_v) \subseteq \hat{C}(K_v)$ for any affine patch D.

($\Rightarrow$): Assume $C(K_v) \neq \emptyset$, meaning there is some $[\alpha\colon \beta\colon \gamma] \in \hat{C}(K_v)$. Let $M = \max\{|\alpha|_v, |\beta|_v, |\gamma|_v\}$ and note $M > 0$ since $[0\colon 0\colon 0] \notin \mathbb{P}^2$. Then

$$P := \left[\frac{\alpha}{M}\colon \frac{\beta}{M}\colon \frac{\gamma}{M}\right] = [\alpha\colon \beta\colon \gamma] \in \hat{C}(R_v)$$

since each coordinate has magnitude less than or equal to 1 with respect to $|\cdot|_v$. Since one of the coordinates has magnitude 1, it is a unit in R_v and we can scale P by the unit's inverse to get a 1 in one of the coordinates. Thus, $P \in \hat{C}(R_v)$ has a 1 in one of its coordinates as desired. □

In the following algorithm, we recap some of preprocessing that should be done on $\hat{C} : F(X, Y, Z)$ as well as outline the rest of this chapter.

Algorithm 2: Is Locally Soluble.

Input: An irreducible, homogeneous $F(X, Y, Z) \in K[X, Y, Z]$.

Output: TRUE if $F(X, Y, Z) = 0$ has a solution in $\mathbb{P}^2(K_v)$ for all nontrivial places v and FALSE otherwise.

```
f_1(x, y) ← F(X, Y, 1);
f_2(x, y) ← F(X, 1, Z);
f_3(x, y) ← F(1, Y, Z);
if f_3(0, 0) = 0 then
    return True;
end
if Has_Rational_Singularity(f_1, K) or Has_Rational_Singularity(f_2, K) then
    return True;
end
for embedding K ↪ ℝ do
    g_1 ← Embed_Coefficients(f_1);
    g_2 ← Embed_Coefficients(f_2);
    if Has_Real_Point(g_1) is False or Has_Real_Point(g_2) is False then
        return False;
    end
end
for i ∈ {1, 2, 3} do
    S ← Potentially_Bad_Primes(f_i);
    for 𝔭 ∈ S do
        if Has_Point_Over_Prime(f_i, 𝔭) is False then
            return False;
        end
    end
end
return True;
```

Line 1 through 9 are preprocessing steps discussed in Chapter 1. Lines 10 through 16 determine if $C(K_v) \neq \emptyset$ for archimedean places and the rest determines if $C(K_v) \neq \emptyset$ for non-archimedean places. We will see in Corollary 2.20 that for most places v, C always has a point over K_v. Moreover, the set of places where C may not have a point over K_v is finite and computable. We will then go through all the places in this set and test if $C(K_v) = \emptyset$. If we are lucky, then C will not be locally soluble and we will be able to conclude that C does not have a rational point.

2.1 Archimedean Localizations

Recall from Theorem 1.4 that archimedean places correspond to embeddings of K into $\mathbb{R}$ or $\mathbb{C}$. If v comes from an embedding into $\mathbb{R}$, then the completion with respect to $|\cdot|_v$ is $K_v = \mathbb{R}$. Likewise, if v comes from a complex embedding, $K_v = \mathbb{C}$. This section focuses on determining whether C has points over $\mathbb{R}$ or $\mathbb{C}$.

Lemma 2.3. *For any curve C defined over K, there is a point $P \in C(\mathbb{C})$.*

Proof. Any nonconstant polynomial has a root over $\mathbb{C}$ by the fundamental theorem of algebra. □

It is possible that $C(\mathbb{R}) = \emptyset$. An example of such a curve is given by the desingularization of $y^2 = -x^4 - 1$. The algorithm to determine if any algebraic curve has a real point consists of two parts: first, we reduce the problem to deciding if a univariate polynomial has a real root. Second, we decide if the univariate polynomial has a root. This method is adapted from Jacobson [14, Section 5.5].

Proposition 2.4. *For any $f(x,y) \in \mathbb{R}[x,y]$, if $f(x,y) = 0$ has a solution in $\mathbb{R}^2$ then $g(x,y) = (y-d)\frac{\partial f}{\partial x} - (x-c)\frac{\partial f}{\partial y} = 0$ has a solution in $\mathbb{R}^2$ for any $c, d \in \mathbb{R}$.*

Proof. Fix $x_0, y_0, c, d \in \mathbb{R}$ such that $f(x_0, y_0) = 0$. If $f(x,y) = \nabla f(x,y) = 0$ has a solution or $f(c,d) = 0$, the claim is shown. Consider the closed disk D centered at (c,d) with radius $\sqrt{(x_0-c)^2 + (y_0-d)^2}$ and let $S = D \cap \{(x,y) \in \mathbb{R}^2 \colon f(x,y) = 0\}$. The set S disk is closed, bounded, and thus compact in $\mathbb{R}^2$, meaning is also compact. Hence, $d(x,y) := \sqrt{(x-c)^2 + (y-d)^2}$ achieves a minimum on S. Let $(a,b) \in S$ be any point achieving the minimum.

Consider the open ball B centered at (c, d) with radius $d(a, b)$. By definition of (a, b), we know $B \cap S = \emptyset$. Since $\nabla f(a, b) \neq 0$ and $f(c, d) \neq 0$, then the tangent vector

$$T(a, b) = \begin{bmatrix} -\frac{\partial f}{\partial y}(a, b) \\ \frac{\partial f}{\partial x}(a, b) \end{bmatrix}$$

must be orthogonal to the vector from (c, d) to (a, b). Otherwise, the tangent line $(a, b) + tT(a, b)$ intersects B and there is a point $(a_1, b_1) \in B \cap S$. The dot product of orthogonal vectors is 0, giving us

$$T(a, b) \cdot (a - c, b - d) = 0$$

and thus $g(a, b) = 0$ as desired. □

Lemma 2.5. *Assume $f(x, y)$ is irreducible with nonzero degree in y. Then for all but finitely many $c \in \mathbb{R}$, the polynomials*

$$g(x, y) = y\frac{\partial f}{\partial x} - (x - c)\frac{\partial f}{\partial y}$$
$$h(x) = Res_y(f, g)$$
$$k(y) = Res_x(f, g)$$

satisfy $h(x) \neq 0$ and $k(y) \neq 0$.

Proof. Let $g(t, x, y) = y\frac{\partial f}{\partial x} - (x - t)\frac{\partial f}{\partial y}$ and let $h(t, x) = \text{Res}_y(f, g)$. Assume $h(t, x) = 0$ identically, meaning $f(x, y)$ and $g(t, x, y)$ share a common factor in $\mathbb{R}[t, x, y]$ of positive y-degree. Since $f(x, y)$ is irreducible in $\mathbb{R}[t, x, y]$, we have $f(x, y)q(t, x, y) = g(t, x, y)$ for some $q(t, x, y) \in \mathbb{R}[t, x, y]$. But for any distinct $c_1, c_2 \in \mathbb{R}$,

$$f(x, y)(q(c_1, x, y) - q(c_2, x, y)) = g(c_1, x, y) - g(c_2, x, y) = (c_1 - c_2)\frac{\partial f}{\partial y}(x, y).$$

However, since $f(x, y)$ is irreducible, it divides $\frac{\partial f}{\partial y}$ only when $\frac{\partial f}{\partial y} = 0$, which contradicts $f(x, y)$ having positive y-degree. So $h(t, x)$ has at most finitely many roots as a polynomial in t. Let $h(x) := h(c, x) \neq 0$ for some $c \in \mathbb{R}$ and similarly define $g(x, y) := g(c, x, y)$. Since $\gcd(f, g) = 1$ for our choice of c, we know $h(x) \neq 0$ and $k(y) = \text{Res}_x(f, g) \neq 0$. □

If $f(x, y) = 0$ is an affine patch of a singular model of a genus 1 curve C, then the hypotheses of Lemma 2.5 are satisfied. To compute the desired $g(x, y)$, we try $c = 0$ and check if

$\gcd(f, g) = 1$. If not, we try $c = 1$ and so on until $\gcd(f, g) = 1$ and thus $h(c, x) \neq 0$.

Lemma 2.6. *Let $f(x, y) \in \mathbb{R}[x, y]$ be irreducible with nonzero y-degree and let $g(x, y)$ be given from Lemma 2.5. There is a computable $m \in \mathbb{R}$ such that $F(x, y) := f(m(x + y), y)$ simultaneously satisfies the following properties.*

1. *If n is the total degree of $f(x, y)$, then $F(x, y)$ can be written*

$$F(x, y) = cy^n + P(x, y)$$

   for a nonzero constant $c \in \mathbb{R}$ and $P(x, y) \in \mathbb{R}[x, y]$ with y-degree less than n.

2. *If $G(x, y) := g(m(x + y), y)$, then any distinct $(a_1, b_1), (a_2, b_2) \in \mathbb{C}^2$ that are solutions to $F(x, y) = G(x, y) = 0$ satisfy $a_1 \neq a_2$.*

Proof. We can separate the degree n homogeneous part of $f(x, y)$ by writing $f(x, y) = p(x, y) + f_n(x, y)$ where $p(x, y)$ has total degree less than n and $f_n(x, y) = \sum_{i+j=n} a_{i,j} x^i y^i$. We have

$$\begin{aligned} F(x, y) &= p(m(x + y), y) + \sum_{i+j=n} a_{i,j}(m(x + y))^i y^j \\ &= p(m(x + y), y) + \sum_{i+j=n} a_{i,j} m^i (x + y)^i (y)^j \\ &= P(x, y) + \sum_{i+j=n} a_{i,j} m^i y^n \end{aligned}$$

where $P(x, y)$ has y-degree less than n. However,

$$f_n(m, 1) = \sum_{i+j=n} a_{i,j} m^i.$$

Since $f_n(x, y)$ is homogeneous, we know $f_n(x, 1) \neq 0$ identically and univariate $f_n(x, 1)$ has a finite number of computable roots. Choosing a nonzero $m \in \mathbb{R}$ that avoids the roots of $f_n(x, 1)$ satisfies our first required condition.

Picking an $m \in \mathbb{R}$ such that the second condition is fulfilled takes more work. Let $h(x)$ and $k(y)$ be defined from Lemma 2.5. Let $\{r_1, \ldots, r_u\}$ be the roots of $h(x)$ and $\{s_1, \ldots, s_v\}$ the roots of $k(y)$ such that all the roots are contained in some finite extension L/K. Then the

set

$$\{(r,s) \in L^2 \colon r \in \{r_1, \ldots, r_u\}, s \in \{s_1, \ldots, s_v\}\}$$

contains all solutions in $\mathbb{C}^2$ to $f(x,y) = g(x,y) = 0$. We can then compute

$$(r_i - r_{i'})(s_j - s_{j'})^{-1} \in L$$

for all of the finitely many tuples (i,j,i',j') with $i \neq i'$ and $j \neq j'$. We claim any $m \in \mathbb{R}$ avoiding all of these elements satisfies our second condition. Any $(a,b) \in \mathbb{C}^2$ satisfying

$$F(a,b) = G(a,b) = 0 = f(m(a+b),b) = g(m(a+b),b)$$

also satisfies

$$m(a+b) = r_i \quad b = s_j$$

for some i,j and thus $(a,b) = (m^{-1}r_i - s_j, s_j)$. Then any distinct $(a_1,b_1),(a_2,b_2) \in \mathbb{C}^2$ satisfying

$$F(a_1,b_1) = G(a_1,b_1) = 0 = F(a_2,b_2) = G(a_2,b_2)$$

also satisfying $a_1 = a_2$ imply

$$m^{-1}r_i - s_j = m^{-1}r_{i'} - s_{j'}$$

for some $i \neq i'$ and $j \neq j'$. Thus, choosing some $m \in \mathbb{R}$ such that $m \neq (r_i - r_{i'})(s_j - s_{j'})^{-1}$ and m not a root of $f_n(x,1)$ satisfies the desired conditions simultaneously. □

Note that

$$\begin{cases} x' &= m(x+y) \\ y' &= y \end{cases}$$

is an invertible change of coordinates defined over $\mathbb{R}$ where

$$F(x,y) = f(x',y')$$

and

$$f(x',y') = F\left(m^{-1}x' - y', y'\right).$$

Thus, $f(x,y)$ has a real root if and only if $F(x,y)$ has a real root and the same is true for

$g(x, y)$ and $G(x, y)$. The conditions guaranteed in Lemma 2.6 let us make an even stronger statement.

Theorem 2.7. *Let $H(x) = Res_y(F, G)$ where $F(x, y), G(x, y) \in \mathbb{R}[x, y]$ are given in Lemma 2.6. Then $H(x) = 0$ has a solution in $\mathbb{R}$ if and only if $f(x, y) = 0$ has a solution in $\mathbb{R}^2$.*

Proof. ($\Leftarrow$): If $(a, b) \in \mathbb{R}^2$ satisfies $f(a, b) = 0$, then $g(a, b) = 0$ and

$$F(m^{-1}a + b, b) = 0 = G(m^{-1}a + b, b).$$

Thus, the resultant satisfies $H(m^{-1}a + b) = 0$ where $m^{-1}a + b \in \mathbb{R}$.

($\Rightarrow$): Assume $a \in \mathbb{R}$ satisfies $H(a) = 0$. Since the leading coefficient of $F(x, y)$ is constant, we know $F(a, y)$ and $G(a, y)$ must share a common factor $q(y) \in \mathbb{R}[y]$ of positive degree. Any root of $q(y)$, denoted $z \in \mathbb{C}$ has a conjugate root $\bar{z}$ meaning (a, z) and $(a, \bar{z})$ satisfy

$$F(a, z) = F(a, \bar{z}) = 0 = G(a, z) = G(a, \bar{z})$$

By the second assumption on F from Lemma 2.6, this implies $z = \bar{z} \in \mathbb{R}$. Thus, $F(a, z) = 0$ is a real solution and $f(m(a + z), z) = 0$ is a real solution. □

We have successfully reduced the problem of determining if $f(x, y) = 0$ has a real solution to determining if the univariate polynomial $H(x)$ has a real root.

Algorithm 3: Has Real Point.

Input: An irreducible $f(x, y) \in \mathbb{R}[x, y]$ of positive y-degree.

Output: TRUE if $f(x, y) = 0$ has a real solution and FALSE otherwise.

$g(x, y) \leftarrow y\frac{\partial f}{\partial x} - x\frac{\partial f}{\partial y}$;
$c \leftarrow 1$;
while $\gcd(f, g) \neq 1$ **do**
    $g(x, y) \leftarrow y\frac{\partial f}{\partial x} - (x - c)\frac{\partial f}{\partial y}$;
    $c \leftarrow c + 1$;
end
$h(x) \leftarrow \mathrm{Res}_y(f, g)$;
$k(y) \leftarrow \mathrm{Res}_x(f, g)$;
$n \leftarrow$ `Total_Degree`(f);
$f_n(x, y) \leftarrow$ `Homogeneous_Part`$(f(x, y), n)$;
$\{r_1, \ldots, r_u\} \leftarrow$ `Roots`$(h(x))$; `# We compute distinct roots only.`
$\{s_1, \ldots, s_v\} \leftarrow$ `Roots`$(k(y))$;
$A \leftarrow$ `Roots`$(f_n(x, 1))$;
for $i \neq i' \in \{1, \ldots, u\}$ *and* $j \neq j' \in \{1, \ldots, v\}$ **do**
    $A \leftarrow A \cup \{(r_i - r_{i'})(s_j - s_{j'})^{-1}\}$;
end
$m \leftarrow 0$;
while $m \in A$ **do**
    $m \leftarrow m + 1$;
end
$H(x) \leftarrow \mathrm{Res}_y(f(m(x + y), y), g(m(x + y), y))$;
return `Count_Real_Roots`$(H(x)) > 0$;

Example 2.8. Consider the curve represented by $f(x, y) = -y^2 + x^4 - x^2 + 1$ and note

$$g(x, y) = y\left(4x^3 - 2x\right) - x\left(-2y\right) = 4x^3y$$

satisfies $\gcd(f, g) = 1$. We compute

$$\begin{aligned} h(x) &= 16x^{10} - 16x^8 + 16x^6 \\ k(y) &= -256y^{10} + 768y^8 - 768y^6 + 256y^4 \end{aligned}$$

where $h(x)$ has distinct roots

$$\left\{0, \frac{\sqrt{3} \pm i}{2}, \frac{-\sqrt{3} \pm i}{2}\right\}$$

and $k(y)$ has distinct roots

$$\{0, \pm 1\}.$$

Furthermore, $f_n(x,1) = x^4$ has 0 as its only root. The choices of m that we must avoid are thus

$$\left\{ \begin{matrix} 0, & \pm 1\left(\frac{\sqrt{3}+i}{2}\right), & \pm 1\left(\frac{\sqrt{3}-i}{2}\right), & \pm 1\left(\sqrt{3}\right), & \pm 1\left(i\right), \\ & \pm 2\left(\frac{\sqrt{3}+i}{2}\right), & \pm 2\left(\frac{\sqrt{3}-i}{2}\right), & \pm 2\left(\sqrt{3}\right), & \pm 2\left(i\right) \end{matrix} \right\}$$

meaning $m = 1$ is a suitable choice of m. We then compute

$$\begin{aligned} f(x+y,y) &= x^4 + 4x^3y + 6x^2y^2 - x^2 + 4xy^3 - 2xy + y^4 - 2y^2 + 1 \\ g(x+y,y) &= 4x^3y + 12x^2y^2 + 12xy^3 + 4y^4 \\ H(x) &= -256x^{10} + 1024x^8 - 1792x^6 + 1792x^4 - 1024x^2 + 256 \end{aligned}$$

We compute the roots of $H(x)$ to be

$$\left\{ \pm 1, \frac{\sqrt{3} \pm i}{2}, \frac{-\sqrt{3} \pm i}{2}, \pm i \right\}$$

two of which are real, meaning $f(x,y) = 0$ has a real solution as desired.

Our proof of Theorem 2.7 even tells us exactly how to find this real solution. Namely, we can compute

$$q(y) = \gcd(F(1,y), G(1,y)) = y + 1$$

and conclude $(1,-1)$ is a solution to $F(x,y)$, meaning $(0,-1)$ is a solution to $f(x,y)$.

There is a well-known method of Sturm that determines the number of real roots of any univariate polynomial without having to factor it. We state it here for completeness.

Theorem 2.9 (Sturm's Theorem)**.** *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ have positive degree. Define*

the sequence

$$\begin{aligned} f_0(x) &= f(x) \\ f_1(x) &= f'(x) \\ f_2(x) &= -Rem(f(x), f'(x)) \\ &\vdots \\ f_{i+1}(x) &= -Rem(f_{i-1}(x), f_i(x)) \\ &\vdots \\ f_s(x) &= 0 \end{aligned}$$

where $Rem(f_{i-1}(x), f_i(x)) \in \mathbb{R}[x]$ *is the remainder of* $f_{i-1}(x)$ *when divided by* $f_i(x)$ *in the euclidean domain* $\mathbb{R}[x]$*. Let* $M = 1 + \sum_{i=0}^{n} |a_i|$*. Then the number of distinct roots of* $f(x)$ *is given by* $V_{-M} - V_M$ *where* V_c *is the number of sign changes in the sequence* $(f_0(c), \ldots, f_s(c))$*.*

Determining if the univariate polynomial $H(x)$ has a real root is as easy as running the euclidean algorithm, evaluating the sequence of remainders at $-M$ and M, and counting the sign variations in the resulting sequences.

2.2 Prime Localizations

In this section, we fix a non-archimedean place v corresponding to the prime ideal $\mathfrak{p} \subset O_K$ above the prime $p \in \mathbb{Z}$ given by Theorem 1.4. A curve C defined over K always has a model defined over O_K since we can scale the defining polynomials of C by the product of the denominators of the coefficients. Let C/Q for some quotient $Q = O_K/I$ denote the curve defined over Q with points $P \in C(Q)$ coming from the natural projection map $O_K \to Q$. Recall from Proposition 2.2 that we only need to determine if $D(R_v) \neq \emptyset$ for an affine plane curve $D\colon f(x, y) = 0$ defined over R_v that is possibly singular. The algorithm presented in this section will determine if any irreducible bivariate polynomial $f(x, y)$ has a root in K_v for every non-archimedean place v. To our knowledge, determining the local solubility of arbitrary curves has not been documented, despite its well-known concept. We begin this section by recalling two necessary and fundamental theorems from number theory.

Lemma 2.10 (Hensel's Lemma)**.** *Let* $f(x, y) \in R_v[x, y]$ *and* $i \in \mathbb{Z}_{>0}$*. If there exists some*

$(a, b) \in R_v/\mathfrak{p}^i \times R_v/\mathfrak{p}^i$ such that

$$f(a, b) \equiv 0 \pmod{\mathfrak{p}^i} \text{ and } \nabla f(a, b) \not\equiv 0 \pmod{\mathfrak{p}^i},$$

then for all $j > i$, there exists a pair $(a_j, b_j) \in R_v/\mathfrak{p}^j \times R_v/\mathfrak{p}^j$ such that

$$f(a_j, b_j) \equiv 0 \pmod{\mathfrak{p}^j} \text{ and } (a_j, b_j) \equiv (a_i, b_i) \pmod{\mathfrak{p}^i}.$$

Moreover, such a sequence defines a pair $(A, B) \in R_v \times R_v$ such that $f(A, B) = 0$.

Proof. See [9, Theorem 1]. □

Theorem 2.11 (Hasse-Weil bound for singular curves)**.** *Given a projective curve C defined over k_v with arbitrary geometric genus, arithmetic genus g_{ar}, and $\#k_v = q$,*

$$|\#C(k_v) - (q + 1)| \leq 2g_{ar}\sqrt{q}.$$

Proof. See Aubry and Perret [1, Corollary 2.4]. □

Corollary 2.12. *Let C be a projective curve defined over K of arbitrary genus with a singular model $\hat{C}\colon F(X, Y, Z) = 0$ defined over O_K. Let d be the degree of $F(X, Y, Z)$ and let s be number of distinct k_v-rational singularities of $\hat{C}/k_v$. If $\#k_v = q$ and*

$$q > \frac{-2 + 2s + (d-1)^2(d-2)^2 + (d-1)(d-2)\sqrt{-4 + 4s + (d-1)^2(d-2)^2}}{2},$$

then $C(K_v) \neq \emptyset$.

Proof. By Theorem 2.11,

$$\#\hat{C}(k_v) \geq -2g_{ar}\sqrt{q} + (q + 1)$$

where g_{ar} is the arithmetic genus of $\hat{C}/k_v$. Since $\hat{C}$ is an irreducible projective plane curve, $g_{ar} = \frac{(d-1)(d-2)}{2}$. This gives us the bound

$$\#\hat{C}(k_v) \geq -\sqrt{q}(d-1)(d-2) + (q + 1)$$

One can check that $-\sqrt{q}(d-1)(d-2) + (q + 1) > s$ is equivalent to

$$q > \frac{-2 + 2s + (d-1)^2(d-2)^2 + (d-1)(d-2)\sqrt{-4 + 4s + (d-1)^2(d-2)^2}}{2}.$$

When this holds, we have a point $\widetilde{P} \in \hat{C}(k_v)$ that is a not a singularity since $\#\hat{C}(k_v) > s$. Recall $\widetilde{P}$ can be scalled to represent a solution to $f(x,y) \equiv 0 \pmod{\mathfrak{p}}$ for some affine patch $D\colon f(x,y) = 0$ of $\hat{C}$. By Lemma 2.10, we can lift $\widetilde{P}$ to a point $P \in D(R_v) \subseteq \hat{C}(K_v)$. Since every K_v point on $\hat{C}$ corresponds to a finite number of K_v points on C, the result is shown. □

For a non-archimedean place v such that $\#k_v$ is larger than

$$\frac{-2 + 2s + (d-1)^2(d-2)^2 + (d-1)(d-2)\sqrt{-4 + 4s + (d-1)^2(d-2)^2}}{2},$$

we can assume C has a point over K_v. All that is left to do is to show that this quantity is independent of v for all but a finite number of computable v. Since d is fixed, this is equivalent to showing s is constant for all but a finite number of computable v. We do so by computing the places for which the difference between the number of singularities of D/k_v and D is nonzero for any affine patch $D\colon f(x,y) = 0$. In other words, we will demonstrate that reducing $f(x,y)$ mod $\mathfrak{p}$ does not make it acquire singularities for large primes. Even in the case of elliptic curves, acquiring singularities when reducing modulo $\mathfrak{p}$ is possible.

Example 2.13. For any prime $p \in \mathbb{Z}$, consider the elliptic curves E_1 and E_2 given by

$$E_1\colon y^2 = x^3 + p^6$$
$$E_2\colon y^2 = x^3 + 1.$$

There is an elliptic curve isomorphism $E_1 \to E_2$ given by $(x,y) \mapsto (\frac{x}{p^2}, \frac{y}{p^3})$ and their reductions $\widetilde{E_i} := E_i/\mathbb{F}_p$ are given by

$$\widetilde{E_1}\colon y^2 = x^3$$
$$\widetilde{E_2}\colon y^2 = x^3 + 1.$$

We can see $\widetilde{E_1}$ contains the singularity $(0,0)$. However, $(x,y) \in \widetilde{E_2}(\mathbb{F}_p)$ is singular only if $2y \equiv 3x^2 \equiv 0$ which implies

$$4y^2 \equiv 9x^4 \equiv 0 \pmod{p}.$$

This means when $p \neq 2, 3$, we have $y^2 \equiv 0$ and $-x \equiv x^4 \equiv 0$. However, this contradicts $y^2 \equiv x^3 + 1$. Thus if $p > 3$, the curve $\widetilde{E_2}$ is non-singular while $\widetilde{E_1}$ is singular.

Remark 2.14. For an elliptic curve E defined over K, a place v is called a *place of bad*

reduction for E if E/k_v is no longer smooth. The places of bad reduction for E correspond exactly to the primes for which the discriminant $\Delta(E)$ has positive valuation with respect to v as seen in [21, Proposition VII.5.1].

We define a similar notion of a place of bad reduction, but for any curve of arbitrary genus. Furthermore, we show how to compute the places of bad reduction.

Definition 2.15. A non-archimedean place v is called a *place of bad reduction* for a curve C defined over K if the number of singularities of C/k_v is greater than the number of singularities of C.

Remark 2.16. In Chapter 3 we compute an elliptic curve J isomorphic to C over some extension L/K. Even though the places of bad reduction are computable for J, places of bad reduction are not invertible morphism invariant even over K.

The goal of the next proposition is to compute an algebraic integer analogous to the discriminant that detects where the affine plane curve $D\colon f(x,y)=0$ has bad reduction.

Lemma 2.17. *Let $D\colon f(x,y)=0$ be defined over O_K with $f(x,y)$ irreducible of positive x-degree and positive y-degree. Let*

$$\begin{aligned} h(x) &= Res_y\left(f, \frac{\partial f}{\partial x}\right) \\ k(x) &= Res_y\left(f, \frac{\partial f}{\partial y}\right) \\ G(x) &= \gcd(h(x), k(x)) \\ A(x) &= \frac{h(x)}{G(x)} \\ B(x) &= \frac{k(x)}{G(x)} \end{aligned}$$

where $G(x) \in K[x]$ is monic. For some computable $c, C_0, C_1 \in O_K$, we have $C_0A(x), C_1B(x) \in O_K[x]$ and

$$R := c \cdot Res(C_0A(x), C_1B(x)) \in O_K$$

is nonzero. Furthermore, for any prime $\mathfrak{p} \subset O_K$ such that $R \notin \mathfrak{p}$, there is an injective mapping Φ from the distinct x-coordinates of singularities of D/k_v to the distinct x-coordinates of singularities of D.

Proof. Let the x-coordinates of the singularities of D comprise the set $\{\alpha_1, \ldots, \alpha_t\} \subset \bar{K}$. The set $\{\alpha_1, \ldots, \alpha_t\}$ is exactly the distinct x-coordinates of the common roots of $f, \frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ in $\bar{K}$. If $h(x)$ or $k(x)$ were identically zero, then one of $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}$ is also identically zero since $f(x, y)$ is irreducible. However, since $f(x, y)$ has positive x-degree and positive y-degree, the polynomials $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are non-zero.

Hence, $h(x)$ and $k(x)$ are nonzero and

$$h(x) = k(x) = 0$$

only has solutions in the set $\{\alpha_1, \ldots, \alpha_t\}$. Thus, each common factor of $h(x)$ and $k(x)$ in $\bar{K}[x]$ has the form $(x - \alpha_i)^{s_i}$ for some $s_i \in \mathbb{Z}_{>0}$ and

$$\gcd(h(x), k(k)) := G(x) = (x - \alpha_1)^{s_1} \cdots (x - \alpha_t)^{s_t} \in K[x].$$

Let

$$c := \prod_{i=1}^{t} g_{i,\text{denom}}, \qquad \text{where} \qquad G(x) = \sum_{i=0}^{\deg G(x)} \frac{g_{i,\text{num}}}{g_{i,\text{denom}}} x_i$$

and all $g_{i,\text{num}} \in O_K$ are nonzero. Similarly for $A(x)$ and $B(x)$, let C_0 and C_1 denote the product of the denominators of their coefficients. Then $c, C_0, C_1 \in O_K$ satisfy $C_0A(x), C_1B(x) \in O_K[x]$. Since $c, C_0, C_1 \in O_K$ are nonzero and $A(x)$ does not share a common root with $B(x)$ in $\bar{K}$, the integer $R = c \cdot \text{Res}(C_0A(x), C_1B(x)) \in O_L$ is nonzero and the first claim is shown.

Now, fix a non-archimedean place v corresponding to a prime $\mathfrak{p} \subset O_K$ such that $R \notin \mathfrak{p}$. Note

$$0 \not\equiv R \equiv c \cdot \text{Res}(C_0A(x), C_1B(x)) \equiv c \cdot \text{Res}(C_0A(x) \bmod \mathfrak{p}, C_1B(x) \bmod \mathfrak{p}) \pmod{\mathfrak{p}}$$

since the resultant is a determinant calculation of a matrix in O_K. Thus, $c \not\equiv 0 \pmod{\mathfrak{p}}$ and $C_0A(x) \pmod{\mathfrak{p}}$ shares no common factors with $C_1B(x) \pmod{\mathfrak{p}}$. We have that

$$cC_0h(x) = C_0A(x)cG(x) \qquad cC_1k(x) = C_1B(x)cG(x).$$

So, if both $h(x), k(x) \pmod{\mathfrak{p}}$ are identically 0, then $cG(x) \pmod{\mathfrak{p}}$ is identically 0 since $C_0A(x), C_1B(x) \pmod{\mathfrak{p}}$ are not both identically 0. However, this implies that each coefficient of $cG(x)$ is in $\mathfrak{p}$. In particular, the leading coefficient $c \in \mathfrak{p}$ which is a contradiction. Thus, we can assume one of $h, k \pmod{\mathfrak{p}}$ are non-zero and there are consequently finitely

many singularities of D/k_v: $f(x,y) \equiv 0 \pmod{\mathfrak{p}}$.

Let L/K contain each α_i as well as the singularities of D/k_v. That is, the extension L/K is large enough such that ℓ_w/k_v contains the coordinates of D/k_v where ℓ_w is the residue field of L for any place w corresponding to a prime $\mathfrak{q} \subset O_L$ lying over $\mathfrak{p}$. Let $(\gamma, \delta) \in \ell_w \times \ell_w$ be a singularity of D/k_v; i.e., a pair $(\gamma, \delta) \in O_L \times O_L$ such that

$$f(\gamma,\delta) \equiv \nabla f(\gamma,\delta) \equiv 0 \pmod{\mathfrak{q}}.$$

Since the resultant computation commutes with reduction modulo $\mathfrak{q}$, we have

$$h(\gamma) \equiv k(\gamma) \equiv 0 \pmod{\mathfrak{q}}.$$

Since at least one of $cC_0 \pmod{\mathfrak{p}}$ and $cC_1 \pmod{\mathfrak{p}}$ are nonzero, either $C_0A(\gamma) \equiv C_1B(\gamma) \equiv 0 \pmod{\mathfrak{q}}$ or $cG(\gamma) \equiv 0 \pmod{\mathfrak{q}}$. However, since $C_0A(x) \pmod{\mathfrak{p}}$ and $C_1B(x) \pmod{\mathfrak{p}}$ share no roots, we can assume $cG(\gamma) \equiv 0 \pmod{\mathfrak{q}}$. Thus, every singularity (γ, δ) of D/k_v satisfies

$$\mu_i\gamma \equiv \lambda_i \pmod{\mathfrak{q}}$$

for some i where $\alpha_i = \frac{\lambda_i}{\mu_i}$ and $\lambda_i, \mu_i \in O_L$. Let Φ be the map such that $\Phi(\gamma) = \alpha_i$. Since $\gamma \equiv \lambda_i(\mu_i)^{-1} \pmod{\mathfrak{q}}$ is the unique element in ℓ_w solving $\mu_i x \equiv \lambda_i \pmod{\mathfrak{q}}$, we know Φ is injective. □

Remark 2.18. If O_K has class number 1, such as the case when $K = \mathbb{Q}$, then Lemma 2.17 can be made simpler. Instead, we can let $G(x) = \gcd(h(x), k(x))$ as a gcd in O_K and let c be the gcd of the coefficients of $G(x)$. This ensures $G(x), A(x), B(x) \in O_K[x]$, the reduction $G(x) \not\equiv 0 \pmod{\mathfrak{p}}$, and $A(x) \equiv B(x) \equiv 0 \pmod{\mathfrak{p}}$ has no solutions for any $\mathfrak{p}$ such that $R \in \mathfrak{p}$. One can check that this is a necessary condition for the existence of Φ. In particular, we do not need to compute C_0 or C_1.

Theorem 2.19. *Let D: $f(x,y) = 0$ be defined over O_K with $f(x,y)$ irreducible of positive x-degree and positive y-degree. There is a computable $R \in O_K$ with the following equivalent properties.*

- *If $R \notin \mathfrak{p}$, then the number of singularities of D/k_v is at most the number of singularities of D.*
- *If v is a place of bad reduction for D, then $R \in \mathfrak{p}$.*

Proof. The equivalence of the two statements follows from the definition of a place of bad reduction. Let R_x be the integer computed from Lemma 2.17 and let R_y be the integer computed from Lemma 2.17 replacing $f(x,y)$ with $f(y,x)$. Let $R := R_x \cdot R_y$ or even $R = \operatorname{lcm}(R_x, R_y)$ if O_K has class number 1. Then any prime $\mathfrak{p} \subset O_K$ such that $R \notin \mathfrak{p}$ also satisfies $R_x \notin \mathfrak{p}$ and $R_y \notin \mathfrak{p}$. For such $\mathfrak{p}$, let Φ_x, Φ_y be the maps coming from Lemma 2.17 and define $\Phi := \Phi_x \times \Phi_y$ on the singularities of D/k_v. Since Φ_x and Φ_y are injective, the map Φ is injective as well and so the domain is smaller than the codomain as desired. □

Corollary 2.20. *Let C be a projective curve defined over K with a projective singular model $\hat{C}\colon F(X,Y,Z) = 0$. Let d be the total degree of $F(X,Y,Z)$ and let s be the number of distinct singularities of $\hat{C}$. Let D_1, D_2, and D_3 be the affine patches of $\hat{C}$. Given R_1, R_2, and $R_3 \in O_K$ from Theorem 2.19, let $R = R_1 \cdot R_2 \cdot R_3$ and write $RO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. For all $\mathfrak{p} \subset O_K$, if $\mathfrak{p} \neq \mathfrak{p}_i$ for any i and*

$$\#k_v > \frac{2s - 2 + (d-1)^2(d-2)^2 + (d-1)(d-2)\sqrt{4s + (d-1)^2(d-2)^2 - 4}}{2},$$

then $\hat{C}(R_v) \neq \emptyset$. In particular, $C(K_v) \neq \emptyset$ for all but a finite number of computable places.

Proof. By Theorem 2.19, for every $j = 1, 2, 3$ we know the number of singularities in every D_j/k_v is at most the number of singularities of D_j. Thus, the number of singularities of $\hat{C}/k_v$ is at most the number of singularities of $\hat{C}$. In particular, the number of distinct k_v-rational singularities of $\hat{C}$ is less s. The result then directly follows from Corollary 2.12. □

Corollary 2.20 gives us one of the two algorithms needed in determining if $C(K_v) \neq \emptyset$ for the prime places. In particular, it allows us to compute the finite set of primes of O_K such that $C(K_v)$ may be empty. We call these primes the *potentially bad primes* of C.

Algorithm 4: Potentially Bad Primes.

Input: An irreducible polynomial $f(x,y) \in O_K$.

Output: A set of primes S such that $f(x,y) \equiv 0 \pmod{\mathfrak{p}}$ has a solution for every $\mathfrak{p} \notin S$.

Function `ComputeR`$(f(x,y))$**:**
- $h(x) \leftarrow \mathrm{Res}_y\left(f, \frac{\partial f}{\partial x}\right)$;
- $k(x) \leftarrow \mathrm{Res}_y\left(f, \frac{\partial f}{\partial y}\right)$;
- $G(x) \leftarrow \gcd(h,k)$;
- $c \leftarrow$ `Product_of_Denominators_of_Coefficients`$(G(x))$;
- $A(x) \leftarrow \frac{h(x)}{G(x)}$;
- $A(x) \leftarrow$ `Product_of_Denominators_of_Coefficients`$(A(x)) \cdot A(x)$;
- $B(x) \leftarrow \frac{k(x)}{G(x)}$;
- $B(x) \leftarrow$ `Product_of_Denominators_of_Coefficients`$(B(x)) \cdot B(x)$;
- **return** $c \cdot \mathrm{Res}(A,B)$;

$R_x \leftarrow$ `ComputeR`$(f(x,y))$;

$R_y \leftarrow$ `ComputeR`$(f(y,x))$;

$R \leftarrow R_x \cdot R_y$;

$S \leftarrow$ `Prime_Factors`(R);

$d \leftarrow$ `Degree`(f);

$U \leftarrow \frac{2s-2+(d-1)^2(d-2)^2+(d-1)(d-2)\sqrt{4s+(d-1)^2(d-2)^2-4}}{2}$;

$S \leftarrow S \cup$ `Primes_Less_Than`(U);

return S;

Example 2.21. Consider the smooth curve $C : 3x^3 + 4y^3 + 5z^3 = 0$ of genus 1. Firstly, we compute

$$\frac{2s-2+(d-1)^2(d-2)^2+(d-1)(d-2)\sqrt{4s+(d-1)^2(d-2)^2-4}}{2} = 1,$$

meaning $C(\mathbb{F}_p)$ has a solution over every prime p by Theorem 2.11. Considering the affine patch

$$D : f(x,y) = 3x^3 + 4y^3 + 5 = 0,$$

we compute

$$\begin{aligned} h(x) &= 729x^6 \\ k(x) &= 15552x^6 + 51840x^3 + 43200 \\ G(x) &= 1 \\ A(x) &= h(x) \\ B(x) &= k(x) \\ R_x &= 2^{36}3^{54}5^{12} \end{aligned}$$

and similarly $R_y = 2^{36}3^{54}5^{12}$, meaning the only primes for which $D/\mathbb{F}_p$ has a singularity are the primes $2, 3, 5$. We repeat this process for all affine patches of C, but no new potential bad primes are discovered. Thus, using Lemma 2.10, we can conclude that $C(K_v) \neq \emptyset$ for every prime greater than 5.

Example 2.22. Consider the genus 0 curve $C : x^2z^2 + xy^2z - 5xyz^2 + y^4 + y^3z + 3y^2z^2 = 0$ which has singularities $(0:0:1), (1:0:0)$. Firstly, we compute

$$\frac{2s - 2 + (d-1)^2(d-2)^2 + (d-1)(d-2)\sqrt{4s + (d-1)^2(d-2)^2 - 4}}{2} \approx 37.9,$$

meaning $C(\mathbb{F}_p)$ has at least three points over every prime p greater than 38 by Theorem 2.11. Consider the affine patch $D : f(x,y) = x^2 + xy^2 - 5xy + y^4 + y^3 + 3y^2 = 0$ containing the singularity $(0,0)$. Following Theorem 2.19, we compute

$$\begin{aligned} h(x) &= 9x^4 + 242x^3 - 429x^2 \\ k(x) &= 144x^6 + 4424x^5 - 6959x^4 - 3850x^3 - 1287x^2 \\ G(x) &= x^2 \\ A(x) &= 9x^2 + 242x - 429 \\ B(x) &= 144x^4 + 4424x^3 - 6959x^2 - 3850x - 1287 \\ R_x &= 2^2 3^4 11^2 13^2 68721449 \end{aligned}$$

similarly we compute $R_y = 2^2 3^2 11^2 13^2$ meaning the only primes for which

$$f(x,y) \equiv \nabla f(x,y) \equiv 0 \pmod{p}$$

can have more than one solution are the primes $2, 3, 11, 13$ or 68721449. Doing the same for the other affine patches yields all the potentially bad primes of C, which are computed to be $\{2, 3, 11, 13, 233, 8936387, 68721449\}$. Using Lemma 2.10, we can therefor conclude that $C(\mathbb{Q}_p) \neq \emptyset$ for every prime greater than 38, not including $233, 8936387$, or 68721449.

We now move on to working with a fixed prime $\mathfrak{p}$ that might satisfy $C(K_v) = \emptyset$. The first thing we can do is look at $D/k_v : f(x, y) \equiv 0 \pmod{p}$ since we are able to enumerate all tuples $(a, b) \in k_v^2$ and directly check if (a, b) is a singularity. If there is some non-singular k_v-rational point, we can utilize Hensel's Lemma to lift it to a point in K_v. However, even if all the points on D/k_v are singularities, we could have $D(K_v) \neq \emptyset$ or $D(K_v) = \emptyset$. For example, the curve $D : pf(x, y) = 0$ satisfies $D(\mathbb{F}_p) = \mathbb{F}_p^2$ and all the points are singularities. In some sense, looking mod $\mathfrak{p}$ might be too discrete of a view. To increase the resolution of D/k_v, we work over $R_v/\mathfrak{p}^i$ for increasing values of i. The ring $R_v/\mathfrak{p}^i$ has all the same properties as k_v that we care about in this context. That is, we can enumerate all tuples $(a, b) \in R_v/\mathfrak{p}^i \times R_v/\mathfrak{p}^i$ and directly check if (a, b) is a singularity. Furthermore, if (a, b) is not a singularity we can still lift it up to a point in R_v with Hensel's Lemma. The following propositions ensure that the process of checking for points modulo $\mathfrak{p}^i$ for increasing i terminates.

Lemma 2.23. *If there exists an $i \in \mathbb{Z}_{>0}$ such that $D(R_v/\mathfrak{p}^i) = \emptyset$, then $D(R_v) = \emptyset$.*

Proof. If $f(a, b) = 0$ for $a, b \in R_v$, then

$$f(a, b) \equiv f(a \bmod \mathfrak{p}^i, b \bmod \mathfrak{p}^i) \equiv 0 \pmod{\mathfrak{p}^i}$$

for all i since $R_v = \varprojlim R_v/\mathfrak{p}^i$. □

Proposition 2.24. *If D does not contain any R_v-rational singularities, there exists some $i \in \mathbb{Z}_{>0}$ such that $D(R_v/\mathfrak{p}^i)$ does not have any $(R_v/\mathfrak{p}^i)$-rational singularities.*

Proof. First, if $D(R_v/\mathfrak{p}^i) = \emptyset$ for a single i, then the claim is trivially shown. So proceed assuming both that ever $P \in D(R_v)$ is non-singular and that $D(R_v/\mathfrak{p}^i) \neq \emptyset$ for all $i \in \mathbb{Z}_{>0}$. For the purpose of contradiction, assume that $D(R_v/\mathfrak{p}^i)$ consists only of singularities for every $i \in \mathbb{Z}_{>0}$. That is,

$$f(a, b) \equiv 0 \pmod{\mathfrak{p}^i} \quad \text{implies} \quad \nabla f(a, b) \equiv 0 \pmod{\mathfrak{p}^i}$$

for all $a, b \in R_v$. Furthermore, since

$$f(a,b) \equiv 0 \pmod{\mathfrak{p}^{i+1}} \quad \text{implies} \quad f(a,b) \equiv 0 \pmod{\mathfrak{p}^i},$$

we know

$$f(a,b) \equiv 0 \pmod{\mathfrak{p}^i} \quad \text{implies} \quad f(a,b) \equiv 0 \pmod{\mathfrak{p}^j}$$

for all $1 \leq j \leq i$. We now consider two cases.

1. Assume there exists a sequence $(a_i, b_i)_{i \in \mathbb{Z}_{>0}}$ such that $(a_i, b_i) \in D(R_v/\mathfrak{p}^i)$ and

   $$(a_{i+1}, b_{i+1}) \equiv (a_i, b_i) \pmod{\mathfrak{p}^i}$$

   for all $i \in \mathbb{Z}_{>0}$. Since

   $$f(a_i, b_i) \equiv \nabla f(a_i, b_i) \equiv 0 \pmod{\mathfrak{p}^i}$$

   for all $i \in \mathbb{Z}$, the sequence $(a_i, b_i)_{i \in \mathbb{Z}_{>0}}$ defines a pair $(A, B) \in R_v^2$ such that

   $$f(A, B) = \nabla f(A, B) = 0.$$

   This contradicts the assumption that $D(R_v)$ contains no singularities.

2. Assume no such sequence exists. That is, for any fixed $(a_1, b_1) \in D(k_v)$, there exists some $e \in \mathbb{Z}_{\geq 1}$ such that $(a_e, b_e) \in D(R_v/\mathfrak{p}^e)$ satisfies

   $$(a_e, b_e) \equiv (a, b) \pmod{\mathfrak{p}},$$

   but no $(a_{e+1}, b_{e+1}) \in D(R_v/\mathfrak{p}^{e+1})$ satisfies

   $$(a_{e+1}, b_{e+1}) \equiv (a_e, b_e) \pmod{\mathfrak{p}^e}.$$

   Since $(a_1, b_1) \in D(k_v)$ was arbitrary, we can write $\{P_1, \ldots, P_\ell\} = D(k_v)$ and assign P_i a corresponding integer e_i such that no $Q \in D(R_v/\mathfrak{p}^{e_i})$ satisfies $P \equiv P_i \pmod{\mathfrak{p}}$. Let $E = \max_i\{e_i\} + 1$ and note $(a_E, b_E) \in D(R_v/\mathfrak{p}^E)$ projects to some $P_i \in D(k_v)$. This contradicts the defining property of E.

In any case, we arrive at a contradiction as desired. □

Corollary 2.25. *Assume D has no R_v-rational singularities, then there exists some $i \in \mathbb{Z}_{>0}$ such that $D(R_v/\mathfrak{p}^i) = \emptyset$ if and only if $D(R_v) = \emptyset$.*

Proof. The forward direction is Lemma 2.23. For the converse, consider the i such that $D/(R_v/\mathfrak{p}^i)$ has no $(R_v/\mathfrak{p}^i)$-rational singularities from Proposition 2.24. If $D(R_v/\mathfrak{p}^i) \neq \emptyset$, any point $P \in D(R_v/\mathfrak{p}^i)$ can be lifted to some $P \in D(R_v)$ by Hensel's Lemma as desired. □

Corollary 2.25 proves that searching for points on $D(R_v/\mathfrak{p}^i)$ for increasing i terminates when we either find a non-singular point or find no points. Moreover, we are guaranteed that one of these conditions hold for some $i \in \mathbb{Z}_{>0}$ as long as D has no R_v-rational singularities. We can guarantee this is the case by using Algorithm 1.

Algorithm 5: Has Point Over Prime.

Input: An irreducible polynomial $f(x, y) \in O_K$ and a prime $\mathfrak{p} \subset O_K$.
Output: True if $f(x, y) \equiv 0$ has a solution in R_v^2 and False otherwise.

```
if Has_Rational_Singularity(f, K_v) then
    return True;
end
i ← 1;
while True do
    Is_Empty ← True;
    for (a, b) ∈ R_v/p^i × R_v/p^i do
        if f(a, b) ≡ 0 (mod p^i) then
            if ∇f(a, b) ≢ 0 (mod p^i) then
                return True;
            end
            Is_Empty ← False;
        end
    end
    if Is_Empty then
        return False;
    end
    i ← i + 1;
end
```

Example 2.26. Following Example 2.21 with $C : 3x^3 + 4y^3 + 5z^3 = 0$, we know that $C(\mathbb{Q}_p) \neq \emptyset$ for every prime except possibly for $p = 2, 3$, and 5. We let $f(x, y) := 3x^3 + 4y^3 + 5$

and compute $\nabla f(x,y) = (9x^2, 12y^2)$. Note that $(1,1)$ satisfies

$$f(1,1) \equiv 0 \pmod 2 \quad \text{while} \quad \nabla f(1,1) \equiv (1,0) \not\equiv 0 \pmod 2.$$

Similarly for $p = 5$,

$$f(0,2) \equiv 0 \pmod 5 \quad \text{while} \quad \nabla f(0,2) \equiv (0,3) \not\equiv 0 \pmod 5.$$

However for $p = 3$, the only solutions to $3x^3 + 4y^3 + 5 \equiv 0 \pmod 3$ are $(0,1), (1,1)$, and $(2,1)$. all of which simultaneously satisfy $\nabla f(x,y) \equiv 0 \pmod 3$. However, the point $(3,4) \in \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ satisfies

$$f(3,4) \equiv 0 \pmod 9 \quad \text{while} \quad \nabla f(3,4) \equiv (0,3) \not\equiv 0 \pmod 9.$$

Thus, for every $p = 2, 3$, and 5 there is some integer e and a point $P \in D(\mathbb{Z}_p/p^e\mathbb{Z}_p)$ that is not a singularity. Using Hensel's Lemma, we can lift P to $D(\mathbb{Z}_p)$, meaning $D(Z_p) \neq \emptyset$ for $p = 2, 3$ and 5. Example 2.21 tells is that $D(\mathbb{Z}_p) \neq \emptyset$ for all other primes, meaning have shown $C : 3x^3 + 4y^3 + 5z^3 = 0$ has a solution over $\mathbb{Q}_p$ for all primes p. We also see that $D(\mathbb{R}) \neq \emptyset$ since $f(x,0) = 0$ is a cubic equation which always has real roots. Thus, $C : 3x^3 + 4y^3 + 5z^3 = 0$ is locally soluble.

Chapter 3

Computing the Jacobian

Now that we can determine if a curve C defined over K is locally soluble, we need to turn to the theory of elliptic curves to measure the extent to which C fails the local-global principle. The first step is to produce an elliptic curve that is isomorphic to C over some extension of K. This task is straightforward as $C(\bar{K})$ has infinitely many points. For example, we can take the singular model $\hat{C}\colon F(X,Y,Z) = 0$ and solve $F(X,0,1) = 0$ for some solution $(a : 0 : 1) \in \hat{C}(L)$ where L/K is a finite extension. We can then find the preimage of $(a : 0 : 1)$ under the projection map $C \to \hat{C}$ to get a point in $C(L)$.

By Definition 1.10, this means that C defined over L is an elliptic curve and has a Weierstrass model due to the Riemann Roch theorem. Finding such a model is feasible via *Riemann Roch calculations,* which are computationally quite expensive. Hess [13] provides an algorithm for computing these models and a function to find a such a model is implemented in MAGMA [3, `EllipticCurve(C, P)`]. The elliptic curve model obtained by finding a point in $C(\bar{K})$ is not unique as there are infinitely many points to choose from. The Jacobian of C is a particular elliptic curve that satisfies a universal property depending on K.

Recall from Definition 1.13 that any elliptic curve E defined over K and any invertible morphism $\phi\colon C \to E$ defines another invertible morphism ϕ^σ for each $\sigma \in \mathrm{Gal}(\bar{K}/K)$. The map

$$\varphi_\sigma = \phi^\sigma \circ \phi^{-1}\colon E \to E$$

is then an invertible morphism. Since φ_σ is an invertible morphism from E to itself, we can apply Proposition 1.15 and decompose

$$\varphi_\sigma = \tau_{P_\sigma} \circ \epsilon_\sigma$$

for a translation map τ_{P_σ} and an invertible isogeny ϵ_σ.

Definition 3.1. A *Jacobian* for a curve C of genus 1 defined over K consists of an elliptic

curve J defined over K and an invertible $\bar{K}$-morphism $\phi\colon C \to J$ such that for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$, the morphism $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}\colon E \to E$ is a translation-by-P_σ map for some $P_\sigma \in E(\bar{K})$.

One can intuitively interpret the Jacobian as an elliptic curve model for C that is "isogeny free" with respect to ϕ. The usefulness of such a definition is apparent after noting that it gives way to a group action of $J(\bar{K})$ on $C(\bar{K})$. This group action will be particularly important in Chapter 4.

Proposition 3.2. *There is a free and transitive group action $\mu\colon C \times J \to C$ given by $\mu(Q, P) = \phi^{-1}(\phi(Q) + P)$. Moreover, the map μ is defined over K.*

Proof. For all $P_1, P_2 \in J(\bar{K})$ and $Q \in C(\bar{K})$,

$$\mu(\mu(Q, P_1), P_2) = \phi^{-1}(\phi(\phi^{-1}(\phi(Q) + P_1)) + P_2) = \phi^{-1}(\phi(Q) + P_1 + P_2) = \mu(Q, P_1 + P_2)$$

and

$$\mu(Q, \mathcal{O}) = \phi^{-1}(\phi(Q) + \mathcal{O}) = Q$$

making μ define a group action. The group action is transitive since for any two $Q_1, Q_2 \in C(\bar{K})$, the point $P := \phi(Q_2) - \phi(Q_1)$ satisfies $\mu(Q_1, P) = Q_2$. The group action is also free since $\mu(P, Q) = Q$ implies $P = \phi(Q) - \phi(Q) = \mathcal{O}$. Moreover, since $\varphi_\sigma(P) = P + P_\sigma$, we have

$$\begin{aligned}
\mu^\sigma(Q, P) =& (\phi^{-1})^\sigma(\phi^\sigma(Q) + P) \\
&= (\phi^{-1})^\sigma((\varphi_\sigma \circ \phi)(Q) + P) \\
&= (\phi^{-1})^\sigma(\phi(Q) + P_\sigma + P) \\
&= (\phi^\sigma)^{-1}(\phi(Q) + P_\sigma + P) \\
&= \phi^{-1}\varphi_\sigma^{-1}(\phi(Q) + P_\sigma + P) \\
&= \phi^{-1}(\phi(Q) + P_\sigma + P - P_\sigma) \\
&= \phi^{-1}(\phi(Q) + P) \\
&= \mu(Q, P).
\end{aligned}$$

So μ is defined over K. □

The map μ induces a *subtraction map*, $\nu\colon C \times C \to J$ given by $\nu(Q, Q') = \phi(Q) - \phi(Q')$.

Proposition 3.3. *The subtraction map $\nu\colon C \times C \to J$ is defined over K.*

Proof. For $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have

$$\nu(Q_2, Q_1)^\sigma = \phi(Q_2)^\sigma - \phi(Q_1)^\sigma = \nu(\mu(Q_2, \mathcal{O}))^\sigma, \mu(Q_1, \mathcal{O})^\sigma) = \nu(\mu(Q_2^\sigma, \mathcal{O}), \mu(Q_1^\sigma, \mathcal{O})) = \nu(Q_2^\sigma, Q_1^\sigma)$$

where the first equality follows from the group operation on E being defined over K and the third equality following from μ being defined over K. □

Remark 3.4. As remarked in Silverman [21, Lemma X.3.1], the maps μ and ν define interactions between $E(\bar{K})$ and $C(\bar{K})$ that agree with the usual intuitions of abelian groups. Notably, for any $P, P_1, P_2 \in E(\bar{K})$ and $Q, Q_1, Q_2 \in C(\bar{K})$, if we write $\mu(Q, P) = Q + P$ and $\nu(Q_1, Q_2) = Q_1 - Q_2$ then

$$\begin{aligned} Q + \mathcal{O} &= Q \qquad & Q - Q &= \mathcal{O} \\ P + (Q + (-P)) &= Q \qquad & (Q + P) - P &= Q \\ (Q_1 + P_1) - (Q_2 + P_2) &= (Q_1 - Q_2) + (P_1 - P_2). \end{aligned}$$

The "plus and minus" notation is the same as the notation used for the group law on $E(\bar{K})$, but the equalities above tell us that both these notations interact in the way expected. For $Q_1, Q_2 \in C(\bar{K})$, the expression $Q_1 + Q_2$ is left undefined, which is where this notation breaks down.

Lemma 3.5. *If J is a Jacobian for an elliptic curve E defined over K, then E and J are K-isomorphic as elliptic curves.*

Proof. Let μ and ν be as defined above and consider $\mathcal{O} \in E(K)$. Define $\psi\colon J \to E$ by $\psi(P) = \mu(\mathcal{O}, P) = \phi^{-1}(\phi(\mathcal{O}) + P)$ which is defined over K. Note that $\psi^{-1}(Q) = \nu(Q, \mathcal{O})$ and is defined over K and moreover $\psi(\mathcal{O}) = \mathcal{O}$, meaning $J \cong E$ as elliptic curves. □

Proposition 3.6. *A Jacobian J of a curve C defined over K is unique up to K-isomorphism of elliptic curves.*

Proof. Let $\phi\colon C \to J$ and $\phi'\colon C \to J'$ be the invertible $\bar{K}$-morphisms that define the Jacobians J and J' of C. We can post compose ϕ with a translation map and the resulting map is still invertible. So, assume without loss of generality that $\phi^{-1}(\mathcal{O}) = \phi'^{-1}(\mathcal{O}') = Q_0$ for

some $Q_0 \in C(\bar{K})$. It follows that $\phi' \circ \phi^{-1} \colon J \to J'$ is an isomorphism of elliptic curves since $\phi' \circ \phi^{-1}(\mathcal{O}) = \mathcal{O}$. Moreover,

$$(\phi' \circ \phi^{-1})^\sigma = \phi'^\sigma \circ (\phi^\sigma)^{-1} = \varphi'_\sigma \circ \phi' \circ \phi^{-1} \circ \varphi_\sigma^{-1} = \tau_{P'_\sigma + \phi' \circ \phi^{-1}(-P_\sigma)} \circ \phi' \circ \phi^{-1}$$

for any $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Hence, $(\phi' \circ \phi^{-1})^\sigma \circ (\phi' \circ \phi^{-1})^{-1}$ is translation by $P'_\sigma - \phi' \circ \phi^{-1}(P_\sigma) \in J(\bar{K})$ meaning $\phi' \circ \phi^{-1} \colon J \to J'$ makes J' a Jacobian for J. Since J is an elliptic curve defined over K, the result follows from Lemma 3.5. □

Remark 3.7. Following Proposition 3.6, we call the elliptic curve K-isomorphism class corresponding to J, *the Jacobian* of C. There are several useful models for the Jacobian.

In general, it is difficult to construct an explicit model for the Jacobian. The goal of this chapter is to develop the background and tools needed to give an explicit algorithm for giving a short Weierstrass curve equation for the Jacobian. We largely follow an outline presented by Sutherland [23], but we deal with more cases and explicitly write out an algorithm. In [24], we give a robust, albeit naive, implementation in MAGMA for curves defined over $\mathbb{Q}$ with j-invariant not 0 nor 1728.

3.1 Twists and Torsors

Recall there are many choices of elliptic curves defined over K that are related to C via an invertible $\bar{K}$-morphism. In this section, we consider the collection of all such choices up to a natural equivalence in a set we call the twists of C.

Definition 3.8. A curve C' is a *twist* of C if C and C' are related by an invertible $\bar{K}$-morphism $\phi \colon C \to C'$. The set $\mathrm{Twist}(C/K)$ denotes classes of twists of C up to invertible K-morphism.

Example 3.9. A *quadratic twist* by a non-square $d \in K$ of an elliptic curve $E \colon y^2 = x^3 + Ax + B$ is $E_d \colon y^2 = x^3 + d^2A + d^3B$ and is the codomain the elliptic curve isomorphism $\chi_d(x, y) = (dx, d^{3/2}y)$ over $K(\sqrt{d}) \subset \bar{K}$. For the nontrivial $\sigma \in \mathrm{Gal}(K(\sqrt{d})/K)$, we have $\chi_d^\sigma(x, y) = (\sigma(d)x, \sigma(d^{1/2})^3 y) = (dx, -d^{3/2}y)$ and $\chi_d^\sigma \circ \chi_d^{-1} = [-1]$. Since $[-1]$ is not a translation map, E_d is not the Jacobian of E over K as expected.

Analogous to the needed distinction of invertible K-morphisms and elliptic curve isomorphisms, Example 3.9 motivates why we may only want to consider elliptic curve isomorphisms. That is, twists given by invertible isogenies.

Definition 3.10. An elliptic curve E' is a *elliptic curve twist* of another elliptic curve E if they are related by an invertible isogeny $\phi\colon E \to E'$ over $\bar{K}$. The set $\mathrm{ETwist}(E/K)$ denotes the elliptic curve K-isomorphism classes of elliptic curve twists of E.

There is a natural map $\mathrm{ETwist}(E/K) \to \mathrm{Twist}(E/K)$ that has possibly non trivial kernel as the equivalence relation in each set is different.

Definition 3.11. For a curve C, the group $\mathrm{Isom}(C)$ is the group of invertible $\bar{K}$-morphisms from C to itself. For an elliptic curve E , the group $\mathrm{Aut}(E)$ is the set of all invertible isogenies over $\bar{K}$ from E to itself.

Remark 3.12. Note that $\mathrm{Aut}(E) \subset \mathrm{Isom}(E)$ is the subset of invertible morphisms that fix $\mathcal{O}$. With the exception of $\tau_{\mathcal{O}}$, all translation maps are instances of isomorphisms in $\mathrm{Isom}(E) \setminus \mathrm{Aut}(E)$. Later in Theorem 4.7, we will see

$$\mathrm{ETwist}(E/K) \cong H^1\big(K, \mathrm{Aut}(E)\big) \text{ and } \mathrm{Twist}(C/K) \cong H^1\big(K, \mathrm{Isom}(C)\big).$$

The Jacobian of C is clearly an element in $\mathrm{Twist}(C/K)$. The twists of J are also elements in this group, but have a different relation to C. In particular, J represents the only class of twists that define a free and transitive action on C.

Definition 3.13. A *principal homogeneous space* (or *E-torsor*) for an elliptic curve E defined over K is a curve C and a map $\mu\colon C \times E \to C$ defined over K such that $\mu\colon C(\bar{K}) \times E(\bar{K}) \to C(\bar{K})$ is a free and transitive group action.

Remark 3.14. Much like the one developed in Proposition 3.3, any free and transitive action $\mu\colon C \times E \to C$ defines a subtraction map $\nu\colon C \times C \to E$ defined over K given by $\nu(P, Q) = P - Q$ where $P - Q$ is the unique point on E such that $P = \mu(Q, P - Q)$. This is proved by Silverman [21, Proposition X.3.2]. We continue to use the notation described in Remark 3.4.

Note that C is a J-torsor due to Proposition 3.2. We now prove that the Jacobian is the class of twists giving C the data of a torsor.

Proposition 3.15. *A curve C is an E-torsor of an elliptic curve E defined over K if and only if E is a Jacobian of C.*

Proof. ($\Rightarrow$): By fixing any $Q_0 \in C(\bar{K})$, we can define a morphism $\phi\colon C \to E$ by $\phi(Q) = Q - Q_0$. Then for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have $\phi^\sigma(Q) = Q - Q_0^\sigma$ and $\phi^{-1}(P) = Q_0 + P$. Thus,

$$\varphi_\sigma(P) = (Q_0 + P) - Q_0^\sigma = P + (Q_0 - Q_0^\sigma) = \tau_{Q_0 - Q_0^\sigma}(P)$$

making E a Jacobian of C.

($\Leftarrow$): See Proposition 3.2. □

Our goal is to compute a model for the Jacobian. We recall a few fundamental facts from Silverman [21] to help us first compute an elliptic curve defined over K isomorphic to C over $\bar{K}$.

Theorem 3.16. *Let E_1 and E_2 be elliptic curves defined over K and let $y^2 = x^3 + Ax + B$ be the short Weierstrass model of E_1 with $A, B \in K$.*

1. *The j-invariant is elliptic curve $\bar{K}$-isomorphism invariant and has the formula*

$$j(E_1) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

2. *The classes $[E_1], [E_2] \in \mathrm{ETwist}(E_1/K)$ satisfy $[E_1] = [E_2]$ if and only if $j(E_1) = j(E_2)$.*

3. *For every $j \in K$, there is some elliptic curve E defined over K such that $j(E) = j$.*

Proof. The two statements are [21, Proposition III.1.4]. For the third statement, one can check the following choices of A and B make $E : y^2 = x^3 + Ax + B$ the curve with the desired j-invariant:

- If $j = 0$, let $A = 0$, $B = 1$.
- If $j = 1728$, let $A = 1$, $B = 0$.
- If $j \neq 0, 1728$, let $A = 3j(1728-j)$ and $B = 2j(1728-j)^2$.

In particular, it is easy to check that $\Delta(E) \neq 0$, meaning E is smooth and an elliptic curve as desired. □

Definition 3.17. The *j-invariant of a curve C*, denoted $j(C)$, is the j-invariant of the elliptic curve C defined over $\bar{K}$ with any distinguished point $\mathcal{O} \in C(\bar{K})$.

Note that $j(C)$ is well-defined since any two elliptic curves C and C' defined over L/K with distinguished points at infinity $\mathcal{O} \in C(L)$ and $\mathcal{O}' \in C'(L)$ are related by the invertible L-isogeny $\tau_{\mathcal{O}'-\mathcal{O}} \colon C \to C'$ meaning $[C] = [C']$ in $\mathrm{ETwist}(C/L)$. By Theorem 3.16, this means their j-invariant are the same.

Theorem 3.18. *The j-invariant of a curve C defined over K satisfies $j(C) \in K$.*

Proof. Let $Q \in C(L)$ be a point for some finite, normal, and therefore Galois extension L/K. Let E be the short Weirstrass model for C defined over L and let $\phi \colon C \to E$ be the invertible L-isomorphism such that $\phi(Q) = \mathcal{O}$. For any $\sigma \in \mathrm{Gal}(L/K)$, we have a map $\phi^\sigma : C^\sigma \to E^\sigma$ where σ acts on C and E by acting on the coefficients of their defining polynomials. Since the coefficients of the polynomials in C are in K, $C^\sigma = C$. Thus, $\phi \circ (\phi^\sigma)^{-1} \colon E^\sigma \to E$ defines an invertible isogeny and so $j(E^\sigma) = j(E)$ by Theorem 3.16. Since

$$j(E)^\sigma = j(E^\sigma) = j(E)$$

for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we must have $j(E) \in K$ as desired. □

Since $j(C) \in K$, we can compute an elliptic curve E defined over K with $j(E) = j(C)$ from Theorem 3.16, giving us a twist of C. However, we want more than just a model for a twist of C defined over K. We want a computable invertible morphism between the two. Before we are able to do so, we need one more proposition.

Proposition 3.19. *Let $E' : y^2 = x^3 + A'x + B'$ and $E : y^2 = x^3 + Ax + B$ be two elliptic curves defined over K with $j(E') = j(E)$. Then there exists a nonzero $\lambda \in \bar{K}$ such that $A = \lambda^4 A'$ and $B = \lambda^6 B'$. Furthermore, $[K(\lambda) : K] \,\big|\, a$ where $a = 4, 6$, or 2 when $B' = 0$, $A' = 0$, or $A'B' \neq 0$, respectively.*

Proof. Consider the following cases:

- If $A'B' \neq 0$, then from the definition of the j-invariant, we deduce that $B^2A'^3 = B'^2A^3$. By letting $\lambda = \sqrt{BA'/(B'A)}$, we see that $A = \lambda^4 A'$ and $B = \lambda^6 B'$.
- If $B' = 0$, then $B = 0$ and $\lambda = \sqrt[4]{A/A'}$ gives the desired result.
- If $A' = 0$, then $A = 0$ and $\lambda = \sqrt[6]{B/B'}$ gives the desired result.

The result on $[K(\lambda) : K]$ follows from the formula of λ. □

An immediate corollary of Proposition 3.19 gives us a computable elliptic curve isomorphism between any two curves of the same j-invariant. The isomorphism is $\chi_\lambda : E' \to E$ where $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$.

Corollary 3.20. *Every curve C is the twist of an elliptic curve E defined over K. Moreover, the model for E is computable and the invertible morphism $\phi\colon C \to E$ defined over a finite extension L/K is computable.*

Proof. We can compute some point $Q \in C(L')$ over a finite Galois extension L'/K. We can then perform Riemann Roch calculations to compute a model E over L' and an invertible morphism $\phi\colon C \to E$ such that $\phi(Q) = \mathcal{O}$. We can then compute $j(C) = j(E) \in K$ and use Theorem 3.16 to compute another model E' over K such that E' is a twist of C. Using Proposition 3.19, we compute the elliptic curve $K(\lambda)$-isomorphism $\chi_\lambda\colon E \to E'$. The composition

$$\phi' = \chi_\lambda \circ \phi\colon C \to E$$

is thus an invertible L-morphism where $L = L'(\lambda)$. □

Let us write down this corollary in an algorithm.

Algorithm 6: Compute Twist

Input: A model for a curve C, a singular model $\hat{C} : F(X, Y, Z) = 0$, and a projection map $\pi : C \to \hat{C}$.

Output: An elliptic curve E defined over K, a field L/K, and a map $\phi : C \to E$ defined over L such that E is a twist of C through ϕ.

$Q \leftarrow \emptyset$;
$L' \leftarrow K$;
$i \leftarrow 0$;
while $Q = \emptyset$ **do**
    $L' \leftarrow$ splitting field of $F(X, 0, 1)$; `# Note` L'/K `is Galois.`
    for $a \in$ `Roots`$(F(X, 0, 1))$ **do**
        if $\nabla F(a, 0, 1) \neq 0$ **then**
            $Q \leftarrow \pi^{-1}((a, 0, 1))$;
        end
    end
    $i \leftarrow i + 1$;
end
$E', \phi' \leftarrow$ `Riemann_Roch_Calculation`(C, Q);
$j \leftarrow j(E') \in K$;
Write $E' : y^2 = x^3 + A'x + B'$;
if $j = 1728$ **then**
    $A \leftarrow 1$;
    $B \leftarrow 0$;
    $\lambda \leftarrow \sqrt[4]{A/A'}$;
else if $j = 0$ **then**
    $A \leftarrow 0$;
    $B \leftarrow 1$;
    $\lambda \leftarrow \sqrt[6]{B/B'}$;
else
    $A \leftarrow 3j(1728 - j)$;
    $B \leftarrow 2j(1728 - j)^2$;
    $\lambda \leftarrow \sqrt{\frac{AB'}{A'B}}$;
end
$E \leftarrow E : y^2 = x^3 + Ax + B$;
$L \leftarrow L'(\lambda)$;
$\chi_\lambda \leftarrow (x, y) \mapsto (\lambda^2 x, \lambda^3 y)$;
$\phi \leftarrow \chi_\lambda \circ \phi'$;
return E, L, ϕ;

Remark 3.21. The first 12 lines of Algorithm 6 search for a non-singular point on $\hat{C}(\bar{K})$ to get a point on $C(\bar{K})$ through π^{-1}. There are certainly better ways to do this, but the method outlined works and always terminates since $\hat{C}$ has finitely many singularities.

Example 3.22. Following Example 2.26, we consider the smooth curve of genus 1 $C : F(X, Y, Z) = 3y^3 + 4x^4 + 5z^3 = 0$. We compute the splitting field $L'/\mathbb{Q}$ of $F(X, 0, 1)$ to be

$$L' = \mathbb{Q}(\theta) = \frac{\mathbb{Q}[x]}{\langle x^6 + 75 \rangle}$$

where $Q = [(\theta^4 + 15\theta) : 0 : 30]$ is a point on $C(L')$. Using Riemann Roch calculations, we compute $E' : y^2 = x^3 - \frac{12301875}{16}$ and $\phi : C \to E$ where $\phi(X : Y : Z) = (\phi_1(X : Y : Z), \phi_2(X : Y : Z), \phi_3(X : Y : Z))$ is given by

$$\begin{aligned}
\phi_1(X : Y : Z) &= \frac{-15Y}{4} \\
\phi_2(X : Y : Z) &= \frac{(9\theta^5 + 45\theta^2)X}{32} \\
\phi_3(X : Y : Z) &= \frac{(\theta^5 + 5\theta^2)X}{50} + Z.
\end{aligned}$$

It is easy to verify $\phi(Q) = [0 : 1 : 0]$. In this case, since E' is already defined over the base field $\mathbb{Q}$, we can take $E = E'$, $L = L'$, and $\phi = \phi'$.

While E is a twist of C, it is not the only one. That is, the result from Algorithm 6 is likely not the Jacobian, but it is close. We still need to compute an elliptic curve isomorphism that transforms E into a Jacobian for C.

3.2 Constructing the Jacobian

There are many models for the Jacobian of C as we have defined it. The algorithm presented here will find an arbitrary model for the Jacobian in short Weierstrass form when $j(C) \neq 0, 1728$. We start by recalling an elementary fact about the set of automorphisms on an elliptic curve. Let $\mu_n \subseteq \bar{K}$ denote the nth roots of unity and $\zeta_n \in \mu_n$ the primitive nth root of unity.

Theorem 3.23. *Let K be a field of characteristic not equal to 2 or 3 and E an elliptic curve defined over K. Then $Aut(E)$ is a cyclic group of order 4, 6, or 2. Specifically,*

- *if* $j(E) = 1728$, *then* $Aut(E) \cong \langle \chi_{\zeta_4} \rangle$;
- *if* $j(E) = 0$, *then* $Aut(E) \cong \langle \chi_{\zeta_6} \rangle$;
- *and if* $j(E) \neq 0, 1728$, *then* $Aut(E) \cong \langle \chi_{-1} \rangle$.

Proof. See [21, Corollary III.10.2]. □

If $j(E) \neq 0, 1728$, then $\mathrm{Aut}(E)$ is always generated by morphisms defined over K. This is not true if $j(E) = 0$ or 1728 since K in need not contain a primitive nth root of unity. For example, $E : y^2 = x^3 - x$ is defined over $\mathbb{Q}$ but has automorphisms defined over $\mathbb{Q}(\sqrt{-1})$. This fact will cause annoyance for our situation as it means we might have to extend the base field to represent elements in $\mathrm{Aut}(E)$.

We now explain the connection of $\mathrm{Aut}(E)$ to the problem of computing J from a twist. Let C be a twist of E defined over K given by an invertible $\bar{K}$-morphism $\phi\colon C \to E$. Recall $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}\colon E \to E$ is an invertible isogeny that can be decomposed as $\varphi_\sigma = \tau_{P_\sigma} \circ \varepsilon_\sigma$ where τ_{P_σ} is translation by $P_\sigma = \varphi_\sigma(\mathcal{O})$ and $\varepsilon_\sigma \in \mathrm{Aut}(E)$.

Lemma 3.24. *Let* E *be a twist of* C *defined over* K *via* $\phi\colon C \to E$ *with* $\phi^\sigma \circ \phi^{-1} = \varphi_\sigma = \tau_{P_\sigma} \circ \varepsilon_\sigma$. *Then* E *is the Jacobian of* C *if and only if* $\varepsilon\colon Gal(\bar{K}/K) \to Aut(E)$ *given by* $\varepsilon(\sigma) = \varepsilon_\sigma$ *is the trivial homomorphism.*

Proof. Immediate from the definition of the Jacobian. □

Note that

$$\ker \varepsilon = \{\sigma \in \mathrm{Gal}(\bar{K}/K) : \epsilon_\sigma = [1]\}$$

is always a subgroup of $\mathrm{Gal}(\bar{K}/K)$. However, when $j(E) = 0, 1728$ this subgroup is not necessarily normal since ε is not a homomorphism. In these edge cases, in order for ε_σ to be defined over K, we need the necessary roots of unity to be in K.

Lemma 3.25. *Let* $\varepsilon\colon Gal(\bar{K}/K) \to Aut(E)$ *as defined in Lemma 3.24. If*

- $j(E) = 1728$ *and* K *contains a forth root of unity,*
- *or* $j(E) = 0$ *and* K *contains a third root of unity,*
- *or* $j \neq 0, 1728$,

then ε is a group homomorphism.

Proof. The assumptions imply that every element in $\mathrm{Aut}(E)$ is defined over K. For each $\sigma, \rho \in \mathrm{Gal}(\bar{K}/K)$, we have

$$\varphi_{\rho\sigma} = \phi^{\rho\sigma} \circ \phi^{-1} = (\phi^{\sigma})^{\rho} \circ (\phi^{-1})^{\rho} \circ \phi^{\rho} \circ \phi^{-1} = \varphi_{\sigma}^{\rho} \circ \varphi_{\rho}$$

and

$$\varphi_{\sigma}^{\rho} \circ \varphi_{\rho} = \tau_{P_\sigma}^{\rho} \circ \varepsilon_{\sigma}^{\rho} \circ \tau_{P_\rho} \circ \varepsilon_{\rho} = \tau_{P_\sigma^{\rho} + \varepsilon_\sigma(P_\rho)} \circ \varepsilon_\sigma \circ \varepsilon_\rho$$

since ε_σ is defined over K. But, $\varphi_{\rho\sigma} = \tau_{P_{\rho\sigma}} \circ \varepsilon_{\rho\sigma}$ meaning $\varepsilon_{\rho\sigma} = \varepsilon_\sigma \circ \varepsilon_\rho = \varepsilon_\rho \circ \varepsilon_\sigma$ as desired. □

Our strategy to compute the Jacobian will be to twist J such that ε becomes the trivial homomorphism. We can do so by computing the fixed field $F := \bar{K}^{\ker \varepsilon}$. Then the fundamental theorem of Galois theory tells us

$$\mathrm{Gal}(F, K) \cong \frac{\mathrm{Gal}(\bar{K}/K)}{\ker \varepsilon} \leq \mathrm{Aut}(E)$$

is a cyclic subgroup of order $n = 1, 2, 3, 4$, or 6. If $n = 1$, we are done as then E is already the Jacobian by Lemma 3.24. A standard result from Kummer theory allows us to get a nice representation for F.

Lemma 3.26. *Let $\langle \zeta_n \rangle = \mu_n \subset K$ and let $Gal(F, K)$ be cyclic of order n. Then $F \cong K(\sqrt[n]{d})$ for some computable unit $d \in K$. Moreover, $Gal(K(\sqrt[n]{d})/K) \cong \langle \omega \rangle$ where $\omega(z) = \zeta_n z$.*

Proof. See [19, Theorem 12.1.1]. □

After identifying $F \cong K(\sqrt[n]{d})$ for some $d \in K$, we are able to compute the twist $E_d : y^2 = x^3 + d^{-4/n}Ax + d^{-6/n}B$. Miraculously, this twist with the new morphism $\tilde{\phi} := \chi_{\sqrt[n]{d}} \circ \phi \colon C \to E_{\sqrt[n]{d}}$ is the Jacobian of C.

Theorem 3.27. *Let E be a twist of C defined over K via the invertible morphism $\phi : C \to E$. Let $j(E)$ and K satisfy the hypotheses of Lemma 3.25 with $\bar{K}^{\ker \varepsilon} = K(\sqrt[n]{d})$ given from Lemma 3.26. Then E_d with the map $\tilde{\phi} = \chi_{\sqrt[n]{d}} \circ \phi \colon C \to E_d$ makes E_d a model for the Jacobian of C.*

Proof. As a slight abuse of notation, let $\chi_d = \chi_{\sqrt[n]{d}}$.Write $\tilde{\varphi}_\sigma = \tau_{\tilde{P}_\sigma} \circ \tilde{\varepsilon}_\sigma$ and define $\tilde{\varepsilon}\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E_d)$ to be the homomorphism $\sigma \mapsto \tilde{\varepsilon_\sigma}$. Let $\langle\omega\rangle = \mathrm{Gal}(K(\sqrt[n]{d})/K) \cong \varepsilon\left(\mathrm{Gal}(\bar{K}/K)\right)$ with $\omega(z) = \zeta z$ for $\langle\zeta\rangle = \mu_n$. For any $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we have

$$\tilde{\varphi}_\sigma = \tilde{\phi}^\sigma \circ \tilde{\phi}^{-1} = \chi_d^\sigma \circ \phi^\sigma \circ \phi^{-1} \circ \chi_d^{-1} = \chi_d^\sigma \circ \varphi_\sigma \circ \chi_d^{-1} = \chi_d^\sigma \circ \tau_\sigma \circ \chi_d^{-1}.$$

Furthermore,

$$\chi_d^\omega(x, y) = (\omega(d^{1/n})^2 x, \omega(d^{1/n})^3 y) = (\zeta^2 d^{2/n} x, \zeta^3 d^{3/n} y) = \chi_d \circ \chi_\zeta.$$

Since $\omega \mapsto \varepsilon_{-\omega}$ is an isomorphism, we can assume $\varepsilon_\omega = \chi_{-\zeta}$ meaning $\chi_\zeta \circ \varepsilon_\omega = [1]$. Now,

$$\tilde{\varphi}_\omega = \chi_d^\omega \circ \tau_\omega \circ \chi_d^{-1} = \chi_d \circ \chi_\zeta \circ \tau_{P_\omega} \circ \varepsilon_\omega \circ \chi_d^{-1} = \tau_{\chi_d(\chi_\zeta(P_\omega))} \circ \chi_d \circ \chi_\zeta \circ \varepsilon_\omega \circ \chi_d^{-1} = \tau_{\chi_d(\chi_\zeta(P_\omega))}$$

and so $\tilde{\varepsilon}(\omega) = [1]$. Note that

$$\frac{\mathrm{Gal}(\bar{K}/K)}{\ker \varepsilon} \cong \mathrm{Gal}(K(\sqrt[n]{d})/K)$$

implies any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ satisfies $\sigma = \omega^k \circ \rho$ for some $\rho \in \ker \varepsilon$ and $k \in \mathbb{Z}$. Since $\tilde{\varepsilon}$ is a homomorphism,

$$\tilde{\varepsilon}(\sigma) = \tilde{\varepsilon}(\omega^k) \circ \tilde{\varepsilon}(\rho) = \tilde{\varepsilon}(\omega)^k = [1]$$

as desired. □

Remark 3.28. In practice, we need only consider $\varepsilon\colon \mathrm{Gal}(L/K) \to \mathrm{Aut}(E)$ where L/K is the finite Galois extension over which $\phi\colon C \to E$ is defined. This is because $\varphi_\sigma = \varphi_\rho$ when $\rho|_L = \sigma|_L$. Since we can compute the finite set $\mathrm{Gal}(L/K)$, we can explicitly compute $\ker \varepsilon$ in the naive way. The computation of the fixed field $L^{\ker \varepsilon}$ is then as simple as checking if the generators of L are fixed by all $\sigma \in \ker \varepsilon$.

Combining Theorem 3.27 with Algorithm 6 gives us our algorithm to compute a model for the Jacobian of C.

Algorithm 7: Compute Jacobian.

Input: A model for a curve C defined over K, a singular model $\hat{C} : F(X, Y, Z) = 0$, and a projection map $\pi \colon C \to \hat{C}$. We require K and $j(C)$ satisfy the requirements in Lemma 3.25.

Output: An elliptic curve J defined over K and an invertible morphism $\tilde{\phi} \colon C \to J$ making J a Jacobian of C.

$E, L, \phi \leftarrow$ `Compute_Twist`$(C, \hat{C}, \pi)$;
$G \leftarrow \mathrm{Gal}(L/K)$;
Function `epsilon`(σ)**:**
  $\varphi_\sigma \leftarrow \phi^\sigma \phi^{-1}$;
  $P_\sigma \leftarrow \varphi_\sigma(\mathcal{O})$;
  return $\tau_{-P_\sigma}\varphi_\sigma$; `# This is` $\varepsilon_\sigma \in \mathrm{Aut}(E)$
$\ker \leftarrow \{\}$;
for $\sigma \in G$ **do**
  if `epsilon`$(\sigma) = [1]$ **then**
    $\ker \leftarrow \ker \cup \{\sigma\}$;
  end
end
$K(\sqrt[n]{d}) \leftarrow L^{\ker}$; `#` $n = [L^{\ker} \colon K] = 1, 2, 3, 4,$ `or` 6.
$\chi_d \leftarrow (x, y) \mapsto (d^{2/n}x, d^{3/n}y)$;
Write $E : y^2 = x^3 + Ax + B$;
$J \leftarrow E_d : y^2 = x^3 + d^{-4/n}Ax + d^{-6/n}B$;
return $J, \chi_d \circ \phi$;

Remark 3.29. We do not provide an algorithm in the case $j(E) = 0$ or 1728 and K does not have the required root of unity. When this is the case, we suspect it suffices to extend the base field and twist back to K. We leave this for future work.

Example 3.30. Following Example 3.22, the curve $C : F(X, Y, Z) = 3y^3 + 4x^4 + 5z^3 = 0$ is related to $E : y^2 = x^3 - \frac{12301875}{16}$ via a computable isomorphism $\phi : C \to E$ defined over $L = \mathbb{Q}(\theta)$ where $[L : \mathbb{Q}] = 6$. We have that $j(C) = 0$ and $\mathbb{Q}$ does not contain a third root of unity. Even though our algorithm is not guaranteed to terminate in such cases, in this example it does. Using MAGMA [3, `Automorphisms(L)`], we compute $\mathrm{Gal}(L/K) = \langle [-1], \rho \rangle$ where $\rho(\theta) = \frac{(\theta^4+5\theta)}{10}$. For each $\sigma \in \mathrm{Gal}(L/K)$, we compute

$$\varepsilon_\sigma = \tau_{-\phi^\sigma \circ \phi^{-1}(\mathcal{O})} \circ \phi^\sigma \circ \phi^{-1}.$$

Using some non-trivial point $Q \in E(\mathbb{Q})$, found say by enlarging L and computing another

point on $C(L)$, we check if $\varepsilon_\sigma(Q) = Q$. Since ε_σ has trivial kernel, this is sufficient to check $\varepsilon_\sigma = [1]$. In this case, we find all $\varepsilon_\sigma = [1]$. Thus, the fixed field $L^{\ker \varepsilon} = \mathbb{Q}$ and $n = 1$, meaning E is in fact already a Jacobian of C.

Chapter 4

Descent

Up to this point in the thesis, we have not assumed any conjecture. Even so, we have decided if $C(K_v) = \emptyset$ for every place v of K and we have computed an elliptic curve J defined over K for which C is a J-torsor. The fact that genus 1 curves fail the local-global principle makes it difficult to use the local solubility of C in a useful way. The idea is to classify the group action of $J(\bar{K})$ on C and then compute $J(K)$ to determine if the action is trivial. The process of "descent" on elliptic curves typically refers to computing a set of generators for $J(K)$. There is no known algorithm to do this that terminates in finite time without assuming the Tate-Shafarevich conjecture. The outline we present is adapted from Silverman [21, Section X].

The outline of this chapter is as follows. We start by defining the *Weil-Châtelet group*, which classifies types of E-torsors up to a natural equivalence. Then, we describe a subset of E-torsors called n-coverings and explain exactly how cosets in $E(K)/nE(K)$ give rise to n-coverings. Next, we see how a collection of locally soluble n-coverings form a computable group called the *n-Selmer group*, whose group operation differs from the operation on the group E-torsors. Intuitively, the *Tate-Shafarevich group* measures this difference. Finally, we write down the algorithm that decides if $C(K)$ is nonempty assuming $Ш(E/K)$ is finite.

4.1 The Weil-Châtelet Group

Remark 4.1. Even though modules are typically defined over rings, a G-module is a module over the group ring of G. The group ring of G is the free abelian group of elements in G with multiplication coming from the operation in G and extending by linearity. Equivalently, the definition works by requiring M to be an abelian group with a G-action.

Definition 4.2. Given a group G and a G-module M, a *crossed homomorphism* is a map $\alpha\colon G \to M$ such that $\alpha(g_1 g_2) = \alpha(g_1) + g_1\alpha(g_2)$. A principle crossed homomorphism, given

by some $m \in M$, is the map $\alpha_m(g) = gm - m$.

It is easy to check that a principle crossed homomorphism is a crossed homomorphism and moreover that the sum of any two crossed homomorphisms is a crossed homomorphism. Hence, crossed homomorphisms form a group under point wise addition.

Proposition 4.3. *Suppose $G = Gal(\bar{K}/K)$ and M is a discrete[1] G-module. A crossed homomorphism $\alpha\colon G \to M$ is continuous[2] if and only if there is finite index normal subgroup $N \subseteq G$ such that $\alpha^{-1}(0) \subseteq N$.*

Proof. See [11, Chapter 4.1 and Remark 6.7]. □

Remark 4.4. Proposition 4.3 can be restated as the existence of a finite Galois extension L/K such that $\alpha^{-1}(0) = \mathrm{Gal}(\bar{K}/L)$. If α_m is a principle crossed homomorphism, then $\alpha_m^{-1}(0) = \mathrm{Stab}_G(m) \leq G$. Using the Galois correspondence, $\mathrm{Stab}_G(m)$ corresponds to a finite extension L/K and we can take the normal closure of L/K to get a finite Galois extension. Thus, all principle crossed homomorphisms are continuous.

Definition 4.5. Given a field K and a $\mathrm{Gal}(\bar{K}/K)$-module M, the *first Galois cohomology group*, denoted $H^1(K, M)$, is the quotient group of continuous crossed homomorphisms from $\mathrm{Gal}(\bar{K}/K)$ to M modulo the group of continuous principle crossed homomorphisms.

Often, our $\mathrm{Gal}(\bar{K}/K)$-module is $E(\bar{K})$ or $E(\bar{K})[n]$. When this is the case we use the notation $H^1(K, E)$ to mean $H^1(K, E(\bar{K}))$ and $H^1(K, E[n])$ to mean $H^1(K, E(\bar{K})[n])$. For any point $P \in E(\bar{K})$, a principle crossed homomorphism is given by $\alpha_P(\sigma) = P^\sigma - P$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$.

Definition 4.6. Given a field K and a non-abelian group N with a $\mathrm{Gal}(\bar{K}/K)$ action, the first Galois cohomology set, denoted $H^1(K, N)$, is the set of equivalence classes of continuous crossed homomorphisms $\mathrm{Gal}(\bar{K}/K) \to N$ under the relation $\alpha \sim \beta$ if and only if there is some $n \in N$ such that $n^\sigma \alpha(\sigma) = \beta(\sigma) n$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$.

If N is abelian then both definitions of Galois cohomology agree and there is an operation on $H^1(K, N)$. However, if N is non-abelian as is the case when $N = \mathrm{Isom}(C)$, then $H^1(K, N)$

[1] Meaning the action $G \times M \to M$ is continuous with respect to the Krull topology on G and the discrete topology on M.

[2] Meaning α is continuous with respect the Krull topology on G and the discrete topology on M.

is no longer a group even though one can check the equivalence relation is still well-defined. The principle continuous crossed homomorphisms still represent a class inside $H^1(K, N)$.

Recall that Proposition 3.15 states a curve C is an E-torsor exactly when E is a Jacobian for C. Equivalently E satisfies the property that $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ is translation by P_σ for some $P_\sigma \in E(\bar{K})$. As seen in Lemma 3.25, we have $\varphi_{\rho\sigma} = \varphi_\sigma^\rho \circ \varphi_\rho$ which is exactly the condition for $\varphi\colon \sigma \mapsto \varphi_\sigma$ to be a crossed homomorphism $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Isom}(E)$. Strikingly, classes of these φ completely comprise $H^1(K, \mathrm{Isom}(E))$.

Theorem 4.7. *There is a bijection* $\mathrm{Twist}(C/K) \to H^1(K, \mathrm{Isom}(C))$.

Proof. Let C' be a twist of C via an invertible $\bar{K}$-morphism $\phi\colon C' \to C$. We first show the map $[C] \mapsto \varphi$ where $\varphi\colon \sigma \mapsto \phi^\sigma\phi^{-1}$ is well-defined. Fix another twist C'' of C with an invertible $\bar{K}$-morphism $\zeta\colon C'' \to C$ representing the same class as C' in $\mathrm{Twist}(C/K)$ via the invertible K-morphism $\theta\colon C' \to C''$. Let $\rho = \zeta\theta\phi^{-1}$ and note

$$(\rho^\sigma)(\phi^\sigma\phi^{-1}) = \zeta^\sigma\theta^\sigma\phi^{-1} = \zeta^\sigma\theta\phi^{-1} = \zeta^\sigma\zeta^{-1}(\zeta\theta\phi^{-1}) = \zeta^\sigma\zeta^{-1}\rho$$

meaning $\phi^\sigma\phi^{-1} \sim \zeta^\sigma\zeta^{-1}$ and the map $[C] \mapsto \varphi$ is well defined.

To show injectivity, assume C' and C'' are both twists of C such that there is a $\rho \in \mathrm{Isom}(C)$ satisfying $(\rho^\sigma)(\phi^\sigma\phi^{-1}) = (\zeta^\sigma\zeta^{-1})\rho$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. We can define $\theta\colon C' \to C''$ given by $\zeta^{-1}\rho\phi$ and note

$$\theta^\sigma = \zeta^{-\sigma}\rho^\sigma\phi^\sigma(\phi^{-1})\phi = \zeta^{-\sigma}(\zeta^\sigma\zeta^{-1})\rho\phi = \zeta^{-1}\rho\phi = \theta$$

meaning $[C'] = [C'']$ as desired.

Showing surjectivity of this map takes more work. Recall there is a familiar action of $\mathrm{Gal}(\bar{K}/K)$ on the function field $F = \bar{K}(C)$. That is, any $g \in F$ can be viewed as a rational map and g^σ is obtained by applying σ to each coefficient of g. Now fix some $\alpha \in H^1(K, \mathrm{Isom}(C))$ and note we can "twist" the natural group action by letting $g^{\alpha(\sigma)} = g^\sigma \circ \alpha(\sigma)$. Let $\mathcal{F} \subset F$ denote the fixed field of this twisted action of $\mathrm{Gal}(\bar{K}/K)$. We will show that $\mathcal{F}$ is the function field of a curve C'.

Since this twisted action of $\mathrm{Gal}(\bar{K}/K)$ is still continuous on $K(C)$, we know $\mathcal{F} \otimes \bar{K} \cong F$ [21,

II.5.3.1]. Now assume $g \in F \cap \bar{K}$ is a constant function fixed by the twisted action. We have

$$g = g^\sigma \circ \alpha(\sigma) = [\sigma(g)] \circ \alpha(\sigma)$$

and so $\alpha = \alpha_g$ is a principle crossed homomorphism. Thus, $\mathcal{F} \otimes \bar{K} = \bar{K}(C') \cong F$ for some smooth projective curve C' [12, I.6.12] where the isomorphism is equivariant with respect to the twisted action on $K(C')$ and the standard action on F. This means that there is a $\bar{K}$-isomorphism $\phi\colon C \to C'$ such that $\phi^*\colon \mathcal{F} \otimes \bar{K} \to F$ is an isomorphism satisfying $\phi^*\left(g^{\alpha(\sigma)}\right) = \phi^*(g)^\sigma$. Define $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ and note for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $g \in F$,

$$g\phi^\sigma = \phi^*(g)^\sigma = \phi^*\left(g^{\alpha(\sigma)}\right) = g^\sigma \alpha(\sigma)\phi$$

implying $\varphi_\sigma = \phi^\sigma\phi^{-1} \sim \alpha(\sigma)$ as desired. □

The surjectivity of the map is interesting as it implies we can go from an action on a function field given by $\alpha \in H^1(K, \mathrm{Isom}(C))$ to a familiar map φ. In particular, if $\alpha \in H^1(K, \mathrm{Isom}(E))$ is always a translation map, then the corresponding class of twists of E is the Jacobian.

Remark 4.8. One might recall there was an issue in computing J in the case $j(C) = 0, 1728$ and K did not contain either a fourth or sixth root of unity. The trouble in these cases was that a certain map $\varepsilon\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E)$ was not a homomorphism. That is, for all $\sigma, \rho \in \mathrm{Gal}(\bar{K}/K)$,

$$\varepsilon(\sigma\rho) = \varepsilon(\sigma)^\rho \varepsilon(\rho) \neq \varepsilon(\sigma)\varepsilon(\rho)$$

since ε_σ was not defined over K. However, this is exactly the condition for $\varepsilon \in H^1(K, \mathrm{Aut}(E))$ and consequently $\varepsilon \in H^1(K, \mathrm{Isom}(E))$. From Theorem 4.7, we know ε is in bijection with a twist of C, say C', such that $\varphi_\sigma = \varepsilon_\sigma$ for all σ. This curve C' is interesting analogous to the opposite of the Jacobian for C as it is "translation free."

Even in the case C is an elliptic curve, the bijection in Theorem 4.7 has the weakness of only being a bijection of sets since $H^1(K, \mathrm{Isom}(E))$ is not a group. We have a much more useful bijection when we restrict our study to E-torsors instead of E twists.

Lemma 4.9. *Let C be an E-torsor with $Q_0 \in C(\bar{K})$, then $\alpha\colon Gal(\bar{K}/K) \to E(\bar{K})$ defined by $\alpha\colon \sigma \mapsto Q_0^\sigma - Q_0$ is a continuous crossed homomorphism. If $Q_1 \in C(\bar{K})$ is another point with $\beta\colon \sigma \mapsto Q_1^\sigma - Q_1$, then $\alpha = \beta$ in $H^1(K, E)$. Let α_C denote this unique class of*

continuous crossed homomorphisms in $H^1(K, E)$. *The element* $\alpha_C \in H^1(K, E)$ *is trivial if and only if* C *has a* K*-rational point.*

Proof. We check

$$\alpha(\sigma)^\tau + \alpha(\tau) = (Q_0^\sigma - Q_0)^\tau + Q_0^\tau - Q_0 = Q_0^{\tau\sigma} - Q_0^\tau + Q_0^\tau - Q_0 = Q_0^{\tau\sigma} - Q_0 = \alpha(\tau\sigma)$$

meaning α is a crossed homomorphism. To check continuity, note that $\alpha^{-1}(0) \subseteq \mathrm{Gal}(\bar{K}/K)$ is the subset consisting of elements fixing the coordinates of Q_0, which is $\mathrm{Gal}(\bar{K}/L)$ where L is the normal closure of $K(Q_0)$.

We now see

$$(\beta - \alpha)(\sigma) = Q_1^\sigma - Q_1 - (Q_0^\sigma - Q_0) = (Q_1 - Q_0)^\sigma - (Q_1 - Q_0)$$

which is a principle crossed homomorphism since $Q_1 - Q_0 \in E(\bar{K})$. Thus, $\alpha = \beta$ modulo principle crossed homomorphisms. If C has a K-rational point $Q \in C(K)$, then

$$\alpha_C \colon \sigma \mapsto Q^\sigma - Q = Q - Q = \mathcal{O}$$

is the trivial element.

Conversely, assume that $\alpha_C : \sigma \mapsto Q^\sigma - Q$ is principle where $Q \in C(\bar{K})$ is arbitrary. Thus means there is some $P \in E(\bar{K})$ such that

$$Q^\sigma - Q = P^\sigma - P$$

for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$. This implies $(Q + (-P))^\sigma = (Q + (-P))$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and so $Q + (-P) \in C(K)$. □

Lemma 4.9 hints at why we are considering Galois cohomology: the curve C has a K-rational point if and only if α_C is the identity in $H^1(K, E)$. Due to a bijection with the Weil-Châtelet group, we call α_C *the trivial torsor* if and only if C has a K-rational point.

Definition 4.10 (Weil-Châtelet group)**.** The Weil-Châtelet group $\mathrm{WC}(E/K)$ of an elliptic curve E defined over K is the set of equivalence classes of E-torsors under the relation $C \sim C'$ if and only if there is an invertible K-morphism $\theta \colon C \to C'$ satisfying $\theta(P) - \theta(Q) = P - Q$ for all $P, Q \in C(\bar{K})$.

Two E-torsors are equivalent exactly when there is an invertible K-morphism $\theta\colon C \to C'$ between them respecting the action of $E(\bar{K})$. That is, for the typical group action maps $\mu\colon C \times E \to C$ and $\nu\colon C \times C \to E$,

$$\theta \circ (\mu \circ (\theta \times [1])) = \mu' \text{ and } \nu \circ (\theta \times \theta) = \nu'$$

where μ' and ν' are the group action maps on C'. In other words, two E-torsors are equivalent when they are isomorphic as curves over K via an isomorphism that does not change the action of $E(\bar{K})$. The group operation on $\mathrm{WC}(E/K)$ is given by a bijection to Galois cohomology.

Theorem 4.11. *There is a bijection from* $\mathrm{WC}(E/K)$ *to* $H^1(K, E)$ *given by* $[C] \mapsto \alpha_C$.

Proof. We first show that the map is well-defined. Let $[C] = [C']$, meaning there is some $\theta\colon C \to C'$ satisfying $\theta(Q^\sigma) = \theta(Q)^\sigma$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ while respecting the group action of $E(\bar{K})$ on $C(\bar{K})$ and $C'(\bar{K})$. We can choose any point in C or C' to define α_C and $\alpha_{C'}$, so let $Q_0 \in C(\bar{K})$ and $\theta(Q_0) \in C'(\bar{K})$. Note

$$\begin{aligned}(\alpha_{C'} - \alpha_C)(\sigma) &= (\theta(Q_0)^\sigma - \theta(Q_0)) - (Q_0^\sigma - Q_0)\\ &= (\theta(Q_0^\sigma) - \theta(Q_0)) - (Q_0^\sigma - Q_0)\\ &= (Q_0^\sigma - Q_0) - (Q_0^\sigma - Q_0)\\ &= \mathcal{O}\end{aligned}$$

Meaning $\alpha_C = \alpha_{C'}$ as desired.

We now show that $[C] \mapsto \alpha_C$ is injective. Assume C_1 and C_2 are two E-torsors defined over K such that $\alpha_{C_1} = \alpha_{C_2}$, meaning $\alpha_{C_2} - \alpha_{C_1}\colon \sigma \mapsto P^\sigma - P$ for some $P \in E(\bar{K})$. Let $Q_1 \in C_1(\bar{K})$ and $Q_2 \in C_1(\bar{K})$ be arbitrary and let $\theta\colon C_1 \to C_2$ be defined as

$$\theta(Q) = (Q - Q_1) + Q_2 + (-P)$$

We can see that θ respects the action of E since

$$\theta(Q) - \theta(R) = ((Q - Q_1) + Q_2 + (-P)) - ((R - Q_1) + Q_2 + (-P)) = Q - R$$

Moreover, we can see θ is defined over K since

$$\begin{aligned}\theta(Q)^\sigma &= (Q^\sigma - Q_1^\sigma) - P^\sigma + Q_2^\sigma \\ &= (Q^\sigma - Q_1^\sigma) - P^\sigma + Q_2^\sigma - ((Q_2^\sigma - Q_2) - (Q_1^\sigma - Q_1) - (P^\sigma - P)) \\ &= (Q^\sigma - Q_1^\sigma) + (Q_1^\sigma - Q_1) - P^\sigma + (P^\sigma - P) + Q_2^\sigma - (Q_2^\sigma - Q_2) \\ &= (Q^\sigma - Q_1) - P + Q_2 \\ &= \theta(Q^\sigma)\end{aligned}$$

meaning θ is an equivalence of E-torsors and $[C_1] = [C_2]$.

Finally, to see that $[C] \mapsto \alpha_C$ is surjective we fix an arbitrary $\alpha \in H^1(K, E)$. There is a natural map $\tau\colon E(\bar{K}) \to \mathrm{Isom}(E)$ given by $P \mapsto \tau_P$ meaning $\tau \circ (-\alpha) \in H^1(K, \mathrm{Isom}(E))$ and using Theorem 4.7 there is some twist of E, denoted C, with $\phi\colon C \to E$ an invertible $\bar{K}$-morphism. This twist satisfies $\varphi_\sigma = \phi^\sigma\phi^{-1} = \tau_{-\alpha(\sigma)}$ meaning E is a Jacobian of C and C is an E-torsor. Letting $P = \phi^{-1}(\mathcal{O})$ we have

$$\begin{aligned}\alpha_C(\sigma) = P^\sigma - P &= (\phi^\sigma)^{-1}(\mathcal{O}) - \phi^{-1}(\mathcal{O}) \\ &= (\tau_{-\alpha(\sigma)}\phi)^{-1}(\mathcal{O}) - \phi^{-1}(\mathcal{O}) \\ &= \phi^{-1}\tau_{\alpha(\sigma)}(\mathcal{O}) - \phi^{-1}(\mathcal{O}) \\ &= \phi^{-1}(\alpha(\sigma)) - \phi^{-1}(\mathcal{O})\end{aligned}$$

Recall the action of an E-torsor C satisfies $Q - R = \phi(Q) - \phi(R)$ and so

$$\alpha_C(\sigma) = \phi^{-1}(\alpha(\sigma)) - \phi^{-1}(\mathcal{O}) = \alpha(\sigma)$$

Thus, $[C] \mapsto \alpha_C = \alpha$ as desired. □

Remark 4.12. The *degree* of a curve C as mentioned in Chapter 1, is the order of $[C] \in \mathrm{WC}(E/K)$. It is not in the scope of this thesis, but if C is locally soluble of degree n, then C admits a model in $\mathbb{P}^{n-1}$. See Stoll [22, pg. 9].

The class $[C]$ represents the trivial element in $\mathrm{WC}(E/K)$ if and only if $[C]$ has a K-rational point. We can therefore interpret Chapter 2, as an algorithm for determining if $[C]$ is trivial inside $\mathrm{WC}(E/K_v)$ for all places v. To utilize the locally solubility algorithm, we first need to relate $\mathrm{WC}(E/K)$ to $\mathrm{WC}(E/K_v)$.

Definition 4.13 (Decomposition Group)**.** The decomposition group of K with respect to a place v is

$$G_v = \{\sigma \in \mathrm{Gal}(\bar{K}/K) : \sigma(M_v) = M_v\} \leq \mathrm{Gal}(\bar{K}/K).$$

For a non-archimedean place, $M_v = \mathfrak{p} \subset K$ for some prime ideal in K and G_v is exactly the subgroup of $\mathrm{Gal}(\bar{K}/K)$ that is $\mathfrak{p}$ stable.

Proposition 4.14. *There is an isomorphism $G_v \cong Gal(\bar{K}_v/K_v)$.*

Proof. See [20, Chapter 2, Corollary 4]. □

Using this isomorphism, we have that $H^1(\mathrm{Gal}(\bar{K}_v/K_v), M) \cong H^1(G_v, M)$, which is useful since $G_v \leq \mathrm{Gal}(\bar{K}/K)$.

Proposition 4.15. *For any $S \leq G$ and $N \subseteq M$, There is a well-defined group homomorphism $H^1(G, N) \to H^1(S, M)$ given by the restriction of $\alpha \in H^1(G, N)$ to S.*

Proof. If $\alpha = \beta$ inside $H^1(G, N)$, then $\alpha - \beta$ is a principle crossed homomorphism. Restricting $\alpha - \beta$ to S does not change this, making the inclusion well-defined. Moreover, $(\alpha + \beta)|_S = \alpha|_S + \beta|_S$ meaning the map is a homomorphism. □

This gives us a well-defined homomorphism $H^1(K, E) \to H^1(G_v, E(\bar{K}_v)) \cong H^1(K_v, E)$ which is equivalently a homomorphism $\mathrm{WC}(E/K) \to \mathrm{WC}(E/K_v)$.

Corollary 4.16. *Let $\iota\colon \mathrm{WC}(E/K) \to \mathrm{WC}(E/K_v)$ send $[C]$ where C is an E-torsor to $[C]$ where C is considered an E-torsor over K_v. The following diagram commutes*

$$\begin{array}{ccc} \mathrm{WC}(E/K) & \xrightarrow{\iota} & \mathrm{WC}(E/K_v) \\ \downarrow\cong & & \downarrow\cong \\ H^1(K, E) & \xrightarrow{\psi} & H^1(K_v, E) \end{array}$$

where ψ is given by Proposition 4.15.

Proof. First we must show that if C is considered to be defined over K_v, it is an E-torsor where E is defined over K_v. By Proposition 3.15, E is the Jacobian of C meaning there is some $\phi\colon C \to E$ defined over $\bar{K}$ satisfying $\varphi_\sigma = \phi^\sigma \phi^{-1}$ is translation by $P_\sigma \in E(\bar{K})$.

Note that ϕ is also defined over $\bar{K}_v$ and also satisfies $\varphi_\sigma = \phi^\sigma \phi^{-1}$ is translation by $P_\sigma \in E(\bar{K}) \subseteq E(\bar{K}_v)$ for all $\sigma \in G_v \cong \mathrm{Gal}(\bar{K}_v/K_v)$. Also note that if $[C] = [C']$ as K_v-torsors, they are related by an invertible K_v-morphism respecting the action of $E(\bar{K}_v)$, but this is automatically then a K-morphism respecting the action of $E(\bar{K})$. Thus, the map ι is well-defined on sets.

To show that the diagram commutes, note that $\psi(\alpha_C) = \alpha_C|_{G_v}$ and $\alpha_C|_{G_v}(\sigma) = \alpha_C(\sigma) = Q_0^\sigma - Q_0$ for any $Q_0 \in E(\bar{K}) \subseteq E(\bar{K}_v)$ and any $\sigma \in \mathrm{Gal}(\bar{K}_v/K)$. This by definition is the same map obtained from the bijection in Theorem 4.11 when considering C over K_v. □

Corollary 4.16 lets us interpret the kernel of the map $H^1(K, E) \to H^1(K_v, E)$ as curves C defined over K that have a rational point over K_v. This brings us to one of the most important groups of this thesis.

Definition 4.17 (Tate-Shafarevich Group)**.** Let $Ш(E/K)$ denote the kernel of the group homomorphism

$$\mathrm{WC}(E/K) \to \prod_v \mathrm{WC}(E/K_v)$$

Remark 4.18. Notice that $[C] \in Ш(E/K)$ exactly when C is locally soluble, which we can determine due to Chapter 2. Moreover, $[C]$ is trivial in $Ш(E/K)$ exactly when C has a K rational point. The remainder of this thesis will be attempting to determine the order of $[C] \in Ш(E/K)$ since nonzero order means C does not have a K-rational point. We will see that there exists an algorithm to determine if C has order n for a fixed $n > 1$, but this is not be enough to determine the order of C since it is not known if $\#Ш(E/K) < \infty$.

We need the following conjecture.

Conjecture 4.19. *There is no element of infinite order in* $Ш(E/K)$.

Note this is a weaker statement than $\#Ш(E/K) < \infty$, but is still not the weakest conjecture we can assume. We will see later in Conjecture 4.40 that we only need there to be there to be no infinitely n-divisible elements in $Ш(E/K)$.

4.2 Torsors as n-coverings

Computing the order of $\alpha_C \in H^1(K, E)$, or equivalently the degree of C, is equivalent to deciding if C has a rational point. While we are unable to directly do so, we are able to find

an n such that α_C has order n^m for some $m \in \mathbb{Z}$. In this section, we fix an integer $n \in \mathbb{Z}_{>0}$ and look at a specific set of E-torsors that interact with the multiplication by n isogeny, $[n]$, defined over K.

Definition 4.20. A curve C is an *n-covering* of an elliptic curve E defined over K when C is a twist of E given by the invertible $\bar{K}$-morphism $\phi\colon C \to E$ and there exists a K-morphism $\pi\colon C \to E$ such that the following diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\phi} & E \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle[n]} & \\ & E & \end{array}$$

Lemma 4.21. *If C is an n-covering of an elliptic curve E defined over K, then C is an E-torsor.*

Proof. Note

$$[n] \circ \phi^\sigma \circ \phi^{-1} = [n]^\sigma \circ \phi^\sigma \circ \phi^{-1} = ([n] \circ \phi)^\sigma \circ \phi^{-1} = \pi^\sigma \circ \phi^{-1} = \pi \circ \phi^{-1} = [n].$$

Thus, $(\phi^\sigma \circ \phi^{-1} - [1])(P) \in E(\bar{K})[n]$ for all $P \in E(\bar{K})$. However, $E(\bar{K})[n] \neq E(\bar{K})$ for $n > 1$. Since all morphisms are either surjective or constant (Proposition 1.15), we know $\phi^\sigma \circ \phi^{-1} - [1]$ must be constant. Hence, $\phi^\sigma \circ \phi^{-1} = \tau_{P_0}$ for some $P_0 \in E(\bar{K})[n]$. In particular, E is a Jacobian for C and so C is an E-torsor. □

Definition 4.22. Two n-coverings of E given by $\pi : C \to E$ and $\pi' : C' \to E$ are *equivalent* if there is an invertible K-morphism $\theta\colon C \to C'$ such that the following diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\theta} & C' \\ & {\scriptstyle\pi}\searrow \quad \swarrow{\scriptstyle\pi'} & \\ & E & \end{array}$$

Definition 4.22 should look familiar to that of Definition 4.10 and in fact is a stronger notion of equivalence. It should not be too surprising that the set of all n-coverings are in bijection to a similar group to $H^1(K, E)$, now depending on $[n]$.

Remark 4.23. It is not true that $H^1(K, E[n])$ is a subgroup of $H^1(K, E)$ even though there is a natural inclusion-like homomorphism $H^1(K, E[n]) \to H^1(K, E)$. Since the equivalence

relation in these groups are different, the map has nontrivial kernel which we examine next in Section 4.3.

Proposition 4.24. *The Galois cohomology group $H^1(K, E[n])$ is in bijective correspondence with equivalence classes of n-coverings.*

Proof. Let T be the classes of all n-coverings of E up to n-covering equivalence. Since n-covering equivalence implies E-torsor equivalence, we know that $T \subseteq \mathrm{WC}(E/K)$. Thus, the map $T \to H^1(K, E)$ from Theorem 4.11 is well-defined up to equivalence of n-coverings as well as injective. Let S be the image of the map $T \to H^1(K, E)$.

($S \subseteq H^1(K, E[n])$): Let $\alpha_C \in S$ be an E-torsor via $\phi : C \to E$ as well as an n-covering via $\pi : C \to E$. From Lemma 4.21, we know

$$[n] = [n]\phi^\sigma\phi^{-1} = [n]\tau_{\alpha(\sigma)}$$

and so $\alpha_C(\sigma) \in E(\bar{K})[n]$.

($S \supseteq H^1(K, E[n])$): Let $\psi : H^1(K, E[n]) \to H^1(K, E)$ be the natural map from Proposition 4.15. If $\alpha \in H^1(K, E[n])$, then there is an E-torsor C such that $\alpha \mapsto \alpha_C$ under ψ. The bijection in Theorem 4.11 tells us the invertible $\bar{K}$-morphism $\phi\colon C \to E$ satisfies $\phi^\sigma\phi^{-1} = \tau_{\alpha(\sigma)}$ where now $\alpha(\sigma) \in E(\bar{K})[n]$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. We define $\pi : C \to E$ by $\pi(P) := [n]\phi(P)$. To see π is defined over K note

$$\begin{aligned}\pi(P)^\sigma &= ([n]\phi(P))^\sigma \\ &= [n]\phi^\sigma(P^\sigma) \\ &= [n](\alpha(\sigma) + \phi(P^\sigma)) \\ &= [n]\phi(P^\sigma) = \pi(P^\sigma)\end{aligned}$$

and so π is defined over K making C an n-covering. □

The next proposition tells us that we can always compute some n such that C is an n-covering.

Proposition 4.25. *Let E be a Jacobian of the curve C defined over K via the invertible morphism $\phi\colon C \to E$ defined over the Galois extension L/K. Then C admits an n-covering of E with $n = [L : K]$.*

Proof. We only need to show that $\pi := [n]\phi$ is defined over K. For any $\sigma \in \mathrm{Gal}(L/K)$, let $\phi^\sigma \phi^{-1} = \tau_{P_\sigma}$ for $P_\sigma \in E(\bar{K})$. Since L/K is Galois, we know $\#\,\mathrm{Gal}(L/K) = n$. For any $\rho \in \mathrm{Gal}(\bar{K}/K)$, we still have $\phi^{\rho\sigma}(\phi^\rho)^{-1} = \tau_{P_{\rho\sigma}}$ and so $\phi^\rho : C \to E$ still gives C the structure of an E-torsor. Thus,

$$\begin{aligned}\pi^\rho = [n]\phi^\rho &= \sum_{\sigma \in \mathrm{Gal}(L/K)} \phi^\rho \\ &= \sum_{\sigma \in \mathrm{Gal}(L/K)} \tau_{-P_{\rho\sigma}} \phi^{\rho\sigma}\end{aligned}$$

Since $\mathrm{Gal}(L/K)$ is normal inside of $\mathrm{Gal}(\bar{K}/K)$, we know ρ acts as a permutation on $\mathrm{Gal}(L/K)$. In particular, we have $\rho\,\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K)$ and thus

$$\sum_{\sigma \in \mathrm{Gal}(L/K)} \tau_{-P_{\rho\sigma}} \phi^{\rho\sigma} = \sum_{\sigma \in \mathrm{Gal}(L/K)} \tau_{-P_\sigma} \phi^\sigma = [n]\phi = \pi$$

as desired. □

Since $\mathrm{Gal}(L/K)$ is finite and computable, so is $[L : K] = n$ where C is an n-covering of E. That is, Algorithm 7 allows us to compute the $\phi : C \to E$ and $\pi : C \to E$ making C and n-covering and $\alpha_C \in H^1(K, E[n])$.

4.3 The Selmer Group

Up to this point, we have not used the fact that C is locally soluble when considering it as an n-covering of the Jacobian. Recall that C is locally soluble exactly when it represents an element in $Ш(E/K)$. Analogously, when C is an n-covering that is also locally soluble, we are able to identify it in a more specific group called the *n-Selmer group*. To motivate this group, we need to explore more deeply the interaction between E-torsors and $E[n]$.

Recall that $E(\bar{K}) \xrightarrow{n} E(\bar{K})$ is surjective when $n > 1$, but when restricting to K-rational points we instead get an exact sequence:

$$0 \to E(K)[n] \to E(K) \xrightarrow{n} E(K) \tag{4.1}$$

and it turns out that this sequence extends via a map $\delta : E(K) \to H^1(K, E[n])$.

Proposition 4.26. *There is a well-defined homomorphism $\delta : E(K) \to H^1(K, E[n])$ such that $\ker\delta = nE(K)$ and $\operatorname{img}\delta = \ker\psi$ where $\psi\colon H^1(K, E[n]) \to H^1(K, E)$ is inclusion.*

Moreover, for every place v of K, there is a well-defined homomorphism $\delta_v : E(K_v) \to H^1(K_v, E[n])$ satisfying $\ker\delta = nE(K_v)$ and $\operatorname{img}\delta_v = \ker\psi$ where $\psi\colon H^1(K_v, E[n]) \to H^1(K_v, E)$.

Proof. First, if $E(K) = E(K)[n]$ we note $\delta = 0$ satisfies all the conditions needed. For any $P \in E(K)$ there is some $Q \in E(\bar{K})$ such that $P = nQ$. Let

$$\delta(P) = \alpha_Q \quad \text{where} \quad \alpha_Q(\sigma) = Q^\sigma - Q$$

and note $[n]\alpha(\sigma) = nQ^\sigma - nQ = P^\sigma - P = \mathcal{O}$. Even though α_Q is principle and thus trivial in $H^1(K, E)$, it is not necessarily principle in $H^1(K, E[n])$ as Q may not be n-torsion. For two such choices of $Q_0, Q_1 \in E(\bar{K})$ their corresponding crossed homomorphisms satisfy

$$\alpha_{Q_1}(\sigma) - \alpha_{Q_0}(\sigma) = (Q_1^\sigma - Q_1) - (Q_0^\sigma - Q_0) = (Q_1 - Q_0)^\sigma - (Q_1 - Q_0) = \alpha_{Q_1 - Q_0}(\sigma)$$

where $n(Q_1 - Q_0) = nQ_1 - nQ_0 = P - P = \mathcal{O} \in E(\bar{K})$ and thus δ is well-defined. By the same argument, $\delta(P_1 + P_0) = \alpha_{Q_1+Q_0} = \alpha_{Q_1} \circ \alpha_{Q_0}$ and δ is a homomorphism.

To show $\ker\delta = nE(K)$, we know already $nE(K) \subseteq \ker\delta$ since then $Q \in E(\bar{K})[n]$ implies α_Q is trivial. For the opposite containment, let $\delta(P) = \alpha_Q$ and assume α_Q is trivial meaning $\alpha_Q(\sigma) = Q_0^\sigma - Q_0$ for some $Q_0 \in E(\bar{K})[n]$. This means for all $\sigma \in \operatorname{Gal}(\bar{K}/K)$,

$$(Q^\sigma - Q) = (Q_0^\sigma - Q_0)$$

and so $(Q - Q_0)^\sigma = Q - Q_0$ giving $Q - Q_0 \in E(K)$. Note that $n(Q - Q_0) = nQ - nQ_0 = P - \mathcal{O}$ and thus $P \in nE(K)$.

To show $\operatorname{img}\delta = \ker\psi$, we immediately have $\operatorname{img}\delta \subseteq \ker\psi$ since α_Q is principle and thus trivial in $H^1(K, E)$. Now suppose that $\psi(\alpha)$ is trivial for some $\alpha \in 1(K, E[n])$. Then $\psi(\alpha)(\sigma) = Q_0^\sigma - Q_0$ for some $Q_0 \in E(\bar{K})$. By the definition of ψ, then $\alpha = \alpha_{Q_0}$ where

$$\mathcal{O} = n\alpha_{Q_0}(\sigma) = (nQ_0)^\sigma - (nQ_0)$$

for all σ. Thus, $nQ_0 \in E(K)$ and $\delta(nQ_0) = \alpha$.

This exact proof still works when we replace K with K_v. □

Many of the arguments made in this section can be simplified if one is comfortable with standard arguments from group cohomology.

Definition 4.27. The maps δ and δ_v defined in Proposition 4.26 are called *connecting homomorphisms*.

The connecting homomorphism gives us the following exact sequence:

$$0 \to E(K)[n] \to E(K) \xrightarrow{n} E(K) \xrightarrow{\delta} H^1(K, E[n]) \tag{4.2}$$

Note that n is surjective if and only if $\operatorname{img}(\delta) = 0$. This is almost never the case and so the following corollary is useful to us.

Corollary 4.28. *For $\alpha_C \in H^1(K, E[n])$ where C is an n-covering of E, we have $\alpha_C \in \operatorname{img}\delta$ if and only if $C(K) \neq \emptyset$.*

Proof. By Proposition 4.26, we know α_C is trivial when considered as an element in $H^1(K, E)$ and thus $[C] \in \mathrm{WC}(E/K)$ is trivial, making $C(K) \neq \emptyset$. Conversely, if $C(K) \neq \emptyset$ then $\alpha_C \in H^1(K, E)$ is trivial and $\alpha_C \in \operatorname{img}\delta$ (Lemma 4.9). □

We can then extend the exact sequence (4.2) to

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[n] & \longrightarrow & E(K) & \xrightarrow{n} & E(K) \\ & & & & & \xrightarrow{\delta} & \\ & & H^1(K, E[n]) & \longrightarrow & H^1(K, E) & \xrightarrow{n} & H^1(K, E). \end{array} \tag{4.3}$$

Note that the kernel and image of δ given in Proposition 4.26 are exactly what is needed for exactness. When we take the appropriate kernels and trace through definitions, we get the truncated short exact sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0. \tag{4.4}$$

This short exact sequence has nice geometric interpretation in the context of determining if C has a K-rational point. Namely, the cosets of the *Mordeil-Weil group* $E(K)/nE(K)$

generate the classes of n-coverings that have a K-rational point. Since C is one of these n-coverings, we have a way to check if C is K-rational given we can compute $E(K)/nE(K)$, δ, and a representation of $\alpha_C \in H^1(K, E[n])$. In order to achieve the second two goals, we must assume that C is locally soluble. See Remark 4.32.

For any place v of K, the sequence (4.4) is still exact when replacing each K with K_v and δ with δ_v. From Proposition 4.15, we then have the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{\Omega}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\delta_v} & \prod_v H^1(K_v, E[n]) & \longrightarrow & \prod_v H^1(K_v, E)[n] & \longrightarrow & 0 \end{array} \tag{4.5}$$

where Ω is either composition. The following proposition tells us Ω is well-defined.

Proposition 4.29. *Diagram 4.5 commutes.*

Proof. We will show that the diagram commutes for a single place v and note the result follows. Consider $P + nE(K) \in E(K)/nE(k)$ and note $\delta(P + nE(K)) = \delta(P) = \alpha$ where $\alpha(\sigma) = Q^\sigma - Q$ with $Q \in E(\bar{K})$ satisfying $nQ = P$. Similarly, note $\delta_v(P + nE(K_v)) = \delta_v(P) = \alpha'$ where $\alpha'(\sigma) = Q'^\sigma - Q'$ for $\sigma \in G_v$ and $Q' \in E(\bar{K_v})$ satisfying $nQ' = P$. Note that $\alpha'(\sigma) - \alpha|_{G_v}(\sigma) = (Q' - Q)^\sigma - (Q' - Q)$ is trivial since $Q' - Q \in E(\bar{K_v})$. For the second square, the result follows immediately from the definition of the maps. □

The kernel of the right most vertical map in 4.5 is by definition $Ш(E/K)[n]$ and $E(K)/nE(K)$ injects into the kernel of the middle vertical map. We define that kernel to be the following group.

Definition 4.30. The *nth*-Selmer group, denoted $S^{(n)}(E/K)$, is given by

$$\ker\left(\Omega : H^1(K, E[n]) \to \prod_v H^1(K_v, E)[n]\right)$$

The definition of which gives us the important exact sequence

$$0 \to E(K)/nE(K) \xrightarrow{\delta} S^{(n)}(E/K) \to Ш(E/K)[n] \to 0 \tag{4.6}$$

This exact sequence is how we will get a handle on the torsion of $Ш(E/K)$, i.e. by computing $\alpha_C \in S^{(n)}(E/K)$ and $\operatorname{img}\delta$ for various values of n and hoping $\alpha_C \in \operatorname{img}\delta$.

From it's current definition it is clear that $S^{(n)}(E/K)$ is a subgroup of $H^1(K, E[n])$, but we can go further with this description.

Definition 4.31. The *inertia group* of K with respect to a place v is

$$I_v := \operatorname{Gal}(\bar{K}_v/K_v^{\text{unr}}) \leq G_v \leq \operatorname{Gal}(\bar{K}/K)$$

where K_v^{unr} is the maximal unramified extension of K_v.

Remark 4.32. A crossed homomorphism $\alpha \in H^1(K_v, E[n])$ is difficult to represent in an algorithm since it is a map whose domain is the infinite group $\operatorname{Gal}(\bar{K}_v/K_v)$. However, if we assume α restricted to I_v is trivial, then α is determined by its mapping on $\operatorname{Gal}(K_v^{\text{unr}}/K_v)$, which is well studied by Serre [20, Chapters 7 and 8]. For example, as seen in [20, Example 7.15(b)], this group is dense with respect to lifts of the Frobenius isomorphism and so α is determined by its action on just this one isomorphism. This motivates the distinction between crossed homomorphisms trivial on I_v and ones that are not.

Definition 4.33. Given a place v of K, a crossed homomorphism $\alpha \in H^1(K, E[n])$ is *unramified at* v if α restricted to I_v is trivial. For any finite set of places S, we define

$$H^1(K, E[n]; S) = \{\alpha \in H^1(K, E[n]) : \alpha \text{ is unramified for all } v \notin S\}$$

Lemma 4.34. *If S contains all archimedean places of K and is finite, then the group $H^1(K, M; S)$ is finite and computable.*

Proof. Note that the action of $\operatorname{Gal}(\bar{K}/K)$ is trivial on $E(K)[n]$ and so

$$H^1(K, E[n]; S) = \operatorname{Hom}(\operatorname{Gal}(\bar{K}/K), E[n]; S)$$

where $\operatorname{Hom}(\operatorname{Gal}(\bar{K}/K), E[n]; S)$ is the set of group homomorphisms that are trivial on I_v for all $v \notin S$. A result from Kummer Theory found in Silverman [21, Proposition VIII.1.6] tells us that we can construct a finite Galois extension L/K such that $H^1(\operatorname{Gal}(L/K), E[n])$ is unramified outside S and $\operatorname{Gal}(L/K)$ has elements of order at most n. The natural map

$$\operatorname{Hom}(\operatorname{Gal}(\bar{K}/K), E[n]; S) \to \operatorname{Hom}(\operatorname{Gal}(L/K), E[n]; S)$$

is then an isomorphism [21, Lemma X.4.3]. One can explicitly compute the extension L/K given S using class group computations. See Silverman [21, VIII Excercise 1]. □

Lemma 4.34 allows us to concretely represent the homomorphisms in $H^1(K, E[n]; S)$ as maps in $\mathrm{Hom}(\mathrm{Gal}(L/K), E[n])$, which have a finite domain. The usefulness of this is seen in the following lemma.

Theorem 4.35. *Let S be the subset of the places v of K containing all archimedean places, all primes containing n, and all primes such that E/k_v is singular.*

Then $S^{(n)}(E/K)$ is a subgroup of $H^1(K, E[n]; S)$. In particular, $S^{(n)}(E/K)$ is finite and computable.

Proof. See [21, X.4.2]. □

Remark 4.36. The places for which E/k_v is singular are exactly the primes dividing the discriminant of E. In particular, the set S in Theorem 4.35 is finite and computable.

While $S^{(n)}(E/K)$ is highly abstract, Theorem 4.35 tells us it is a finite abelian group. Moreover, its elements form a subgroup of maps in $\mathrm{Hom}(\mathrm{Gal}(L/K), E[n])$. Recall any abelian group is isomorphic to $(\prod_{i=1}^{N} \mathbb{Z}/q\mathbb{Z})/R$ for some $q \in \mathbb{Z}$ representing the maximum order of an element, some $N \in \mathbb{Z}$, and some subgroup R of $(\prod_{i=1}^{N} \mathbb{Z}/q\mathbb{Z})$ called the *relation lattice*. The issue of computing the isomorphism $S^{(n)}(E/K) \cong (\prod_{i=1}^{N} \mathbb{Z}/q\mathbb{Z})/R$ is nontrivial and outside the scope of this thesis. We refer the reader to a series of papers all about this computation [5] [6] [7] [22].

Theorem 4.37. *Stoll [22, Theorem 2.4]. There is an effective procedure for computing the n-Selmer group of an elliptic curve over a number field K. It requires class group and unit group computations in extensions of K of the form $K(T_1, T_2)$, where T_1, T_2 is an unordered pair of n-torsion points of E.*

While computing $S^{(n)}(E/K)$ can technically be done, it is simply too expensive to do for even moderately sized n due to expensive class group computations.

Remark 4.38. Work by Hallgren [10] and Jean-François and Fang [15] show that there is an efficient quantum algorithm to perform class group computations. This means that computing $S^{(n)}(E/K)$ can be done efficiently on a quantum computer.

Even modulo the class group computations, there needs to be a way to represent the curve C as an element in $S^{(n)}(E/K)$ and identify the subgroup $\operatorname{img}\delta \subseteq S^n(E/K)$ that agrees with the computable representation of $S^n(E/K)$. That is, there must be some computable translation between geometric representations of elements in $S^{(n)}(E/K)$, elements in $H^1(K, E[n]; S)$, and elements in $(\prod_{i=1}^{N} \mathbb{Z}/q\mathbb{Z})/R$. In practice, MAGMA currently has implementations for computing $S^{(n)}(E/\mathbb{Q})$ for $n = 2, 4, 8, 3, 9, 5$ as there are nice geometric representations for elements in $S^{(n)}(E/\mathbb{Q})$ for such n. Such models are described in [8] and [3, "Models of Genus 1 Curves"]. We summarize this section with the following diagram.

$$\begin{array}{ccccccc}
\alpha_C & & \operatorname{Hom}(\operatorname{Gal}(L/K), E[n]; S) & & n-\text{covering classes} & & \operatorname{WC}(E/K) \\
\cap & & \cong\uparrow & & \downarrow\cong & & \downarrow\cong \\
S^{(n)}(E/K) & \hookrightarrow & H^1(K, E[n]; S) & \longrightarrow & H^1(K, E[n]) & \longrightarrow & H^1(K, E) \\
\delta\uparrow & & & & & & \\
E(K)/nE(K) & & & & & &
\end{array}$$

where α_C is the crossed homomorphism corresponding to the locally soluble curve C defined over K. It is clear that if $E(K)/nE(K)$ and $S^{(n)}(E/K)$ are computable, then we can compute $\operatorname{img}\delta$ and consequently decide if $C(K) \neq 0$. In the algorithm we present, we essentially compute $E(K)/nE(K)$ along the way to deciding if $C(K) \neq \emptyset$.

4.4 The Decisional Procedure

We are finally ready to present the decisional procedure that terminates based on the Tate-Shafarevich conjecture. It is important to note that we are treating a subroutine to compute $S^{(k)}(E/K)$, for any $k \in \mathbb{Z}_{>0}$, as a black box. That is, there must be an algorithm to check equality in $S^{(k)}(E/K)$, we must be able perform the group operation on any two elements, and we must be able to call the following functions:

- `Selmer_Group`(E, k): Returns a generating set for $S^{(k)}(E/K)$.
- `Selmer_Representation`(C, ϕ, E, k): Given a locally soluble curve C such that $\phi\colon C \to E$ makes C an E-torsor, returns an element equivalent to $\alpha_C \in S^{(k)}(E/K)$.
- δ`_Selmer_Representation`$(\{P_1, \ldots, P_u\}, E, k)$: Given a set of points $\{P_1, \ldots, P_u\} \subseteq$

$E(K)$, computes the generators of the subgroup of $S^{(k)}(E/K)$ under the connecting homomorphism δ.

- `Multiplication_Selmer_Representation`(E, k, ℓ): Given some $\ell \in \mathbb{Z}_{>0}$, computes the matrix for the map $[\ell]_* : S^{(k)}(E/K) \to S^{(k)}(E/K)$ where $\alpha \mapsto [\ell] \circ \alpha$.

While all these algorithms can be written down, not all of them are practical as mentioned in the remarks proceeding Theorem 4.37. Our strategy for determining if $C(K) \neq \emptyset$ is to determine the order of $\alpha_C \in Ш(E/K)$. There is a diagram for all $m \in \mathbb{Z}$ given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/n^m E(K) & \longrightarrow & S^{(n^m)}(E/K) & \longrightarrow & Ш(E/K)[n^m] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [n^{m-1}]} & & \downarrow{\scriptstyle [n^{m-1}]_*} & & \downarrow{\scriptstyle [n^{m-1}]} & & \\ 0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & S^{(n)}(E/K) & \longrightarrow & Ш(E/K)[n] & \longrightarrow & 0. \end{array}$$

Definition 4.39. The *m-relative Selmer group* is defined by

$$S^{(n,m)}(E/K) := [n^{m-1}]_*\left(S^{(n^m)}(E/K)\right).$$

Tracing through definitions yields another exact sequence

$$0 \to E(K)/nE(K) \to S^{(n,m)}(E/K) \to n^{m-1}Ш(E/K)[n^m] \to 0. \tag{4.7}$$

The relative Selmer group is computable sine $S^{(n)}(E/K)$ is computable and the hope is that for some $m \in \mathbb{Z}$, it is isomorphic to $E(K)/nE(K)$ through δ. Equivalently, we hope the following conjecture is true.

Conjecture 4.40. *For all $n \in \mathbb{Z}_{>1}$ there exists an $m \in \mathbb{Z}_{>0}$ such that*

$$n^{m-1}Ш(E/K)[n^m] = 0.$$

Equivalently, the sequence of groups $\left(Ш(E/K)[n^m]\right)_{m\in\mathbb{Z}_{>0}}$ stabilizes.

When this is the case, we know $\operatorname{img}\delta = S^{(n,m)}(E/K)$ and so a generating set of $E(K)/nE(K)$ is given by any set of points $\{P_1, \ldots, P_u\}$ such that $\delta(\{P_1, \ldots, P_u\})$ generate $S^{(n,m)}(E/K)$. We can find these points by brute force by naively enumerating the possible x-coordinates of points on $E(K)$.

Definition 4.41. The *(naive, logarithmic) height function* on E is $h_x : E(\mathbb{Q}) \to \mathbb{R}$ such that

$$h_x((x,y)) = \log H(x)$$
$$h_x(\mathcal{O}) = 0$$

where $H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}$.

Proposition 4.42. *For every constant $C \in \mathbb{R}$, the set*

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C\}$$

is finite and computable.

Proof. We clearly see for a fixed $C \in \mathbb{R}$, there are $(C+1)^2$ choices for $(p,q) \in \mathbb{Z}^2_{>0}$ such that $H\left(\frac{p}{q}\right) \leq C$ and so there are finitely many choices for x-coordinates of a point P satisfying $h(P) \leq \log C$. The result follows noting that there are at most two points $P \in E(\mathbb{Q})$ with a given x-coordinate. One can compute such a set by writing $E : y^2 = x^3 + Ax + B$ and checking if

$$\left(\frac{p}{q}\right)^3 + A\left(\frac{p}{q}\right) + B$$

is a square for every candidate choice of $\frac{p}{q}$. □

Proposition 4.42 holds when we replace $\mathbb{Q}$ with K and define height similarly. Silverman [21, VIII.5.4] has a detailed analysis of different height functions.

Definition 4.43. For any $m \in \mathbb{Z}_{>0}$, the *rational-point group* $T_{(n,m)}(E/K)$ is the subgroup of $S^{(n)}(E/K)$ generated by $\delta(\{P_1, \ldots, P_u\})$ where $\{P_1, \ldots, P_u\} = \{P \in E(\mathbb{Q}) : h_x(P) \leq m\}$.

Assuming Conjecture 4.40, there must be some $m \in \mathbb{Z}_{>0}$ for which a finite set of points in $E(K)/nE(K)$ generate $S^{(n,m)}(E/K)$ under the δ map, so checking if $\alpha_C \in \operatorname{img}\delta$ is equivalent to checking if $\alpha_C \in S^{(n,m)}(E/K)$. The only thing that is left to do is to find such an $m \in \mathbb{Z}_{>0}$. From the definition of the relative Selmer group and rational point group,

$$S^{(n,m)}(E/K) \subseteq S^{(n,m-1)}(E/K) \subseteq \cdots \subseteq S^{(n,1)}(E/K) = S^{(n)}(E/K)$$
$$T_{(n,r)}(E/K) \supseteq T_{(n,r-1)}(E/K) \supseteq \cdots \supseteq T_{(n,2)}(E/K) \supseteq T_{(n,1)}(E/K).$$

Conjecture 4.40 can thus be restated as the existence of some $R \in \mathbb{Z}$ such that

$$S^{(n,R)}(E/K) = T_{(n,R)}(E/K).$$

In this case, if $m \in \mathbb{Z}_{>0}$ is minimal satisfying $n^{m-1}Ш(E/K)[n^m] = 0$ and M is the maximum of $h_x(P)$ for a choice of generators $P \in E(K)/nE(K)$, then $R = \max\{m, M\}$ suffices.

Remark 4.44. Any process of enumerating the points of $E(K)$ can be used when attempting to find a set that generates $S^{(n,m)}(E/K)$ under δ. The only requirement is that such a process lists any specific point in finite.

Algorithm 8: Has K point.

Input: A smooth curve C of genus 1.

Output: True if $C(K) \neq \emptyset$ or False otherwise.

```
if Locally_Soluble(C) is False then
    return True;
end
E, L, φ ← Compute_Jacobian(C);
L ← Normal_Closure(L);
n ← [L : K];
α_1, ..., α_r ← Selmer_Group(n);
α_C ← Selmer_Representation(C, E, φ, n);
m ← 1;
while True do
    β_1, ..., β_s ← Selmer_Group(E, n^m);
    A ← Multiplication_Map_Representative(E, n^m, n^{m-1});
    γ_1, ..., γ_t ← A({β_1, ..., β_s});          # This generates S^{(n,m)} ⊂ S^{(n)}.
    {P_1, ..., P_u} ← Points_With_Bounded_Height(E, m);
    ε_1, ..., ε_v ← δ_Selmer_Representation({P_1, ..., P_u}, E, n));
    ;                                             # This generates T_{(n,m)} ⊂ S^{(n)}
    if ⟨γ_1, ..., γ_t⟩ = ⟨ε_1, ..., ε_v⟩ then
        if α_C ∈ ⟨γ_1, ..., γ_t⟩ then
            return True;
        end
        else
            return False;
        end
    end
    m ← m + 1;
end
```

Algorithm 8 only terminates if there is an $m \in \mathbb{Z}$ such that $S^{(n,m)} = T_{(n,m)}$ as expected. When this is the case, we know that $\delta(\{P_1, \ldots, P_u\})$ generates $S^{(n,m)}(E/K)$ and so $\{P_1, \ldots, P_u\}$ generates $E(K)/mE(K)$. If $\alpha_C \notin \langle \operatorname{img} \delta(\{P_1, \ldots, P_u\}) \rangle \cong \langle \operatorname{img}(E(K)/nE(K)) \rangle$, then it is nonzero in $Ш(E/K)[n]$ and thus does not have a K-rational point. Otherwise, $\alpha_C \in \operatorname{img} \delta$ and $C(K) \neq \emptyset$ as seen in Corollary 4.28.

In the strategy outlined, we decide if C has a K-rational point essentially by computing $E(K)/mE(K)$ where E is the Jacobian of C. We conclude the content of this thesis with a

theorem stating why this is necessary.

Theorem 4.45. *There is an algorithm to decide if a smooth curve of genus 1 defined over K has a K-rational point if and only if there is an algorithm to compute $E(K)/nE(K)$ for any elliptic curve E defined over K and any $n \in \mathbb{Z}_{>0}$.*

Proof. ($\Rightarrow$): An algorithm to compute $E(K)/nE(K)$ can be constructed as followed.

1. Compute the finite group $S^{(n)}(E/K)$ (Theorem 4.37).
2. For each $\alpha \in S^{(n)}(E/K)$, construct an n-covering C such that $\alpha_C = \alpha$ (Proposition 4.24).
3. For each n-covering above, decide if $\alpha_C \in \operatorname{img}\delta$ by using an algorithm to decide if C has a point over K (Corollary 4.28).
4. For successive $r \in \mathbb{Z}_{>0}$, compute $T_{(n,r)} = \langle\delta(\{P_1, \ldots, P_{u_r}\})\rangle$ until $T_{(n,r)} = \operatorname{img}\delta$. When equality holds, the points $\{P_1, \ldots, P_{u_r}\}$ generate $E(K)/nE(K)$ (Equation 4.6).

($\Leftarrow$): An algorithm to decide if C has a point over K can be constructed as followed.

1. Decide if C is locally soluble and compute J, the Jacobian of C (Chapters 2 and 3).
2. Compute the finite group $S^{(n)}(J/K)$ (Theorem 4.37).
3. Compute a generating set for $J(K)/nJ(K)$ with representatives $\{P_1, \ldots, P_u\}$, then compute $\operatorname{img}\delta = \langle\delta(\{P_1, \ldots, P_u\})\rangle$ (Definition 4.27).
4. Compute $\alpha_C \in S^{(n)}(J/K)$ using Proposition 4.24 and check if $\alpha_C \in \operatorname{img}\delta$. Then C has a point over K if and only if $\alpha_C \in \operatorname{img}\delta$ (Corollary 4.28).

No conjecture is needed for this equivalence. □

Chapter 5

Conclusion

When considering the difficulty of implementing an algorithm to determine if a smooth curve C of genus 1 defined over a number field K has a K-rational point, the following should be noted.

- It is relatively easy to determine if C has a point over K_v for every place v of K, but this does not directly tell us if C has a point over K.
- An algorithm to determine if C has a point over K exists if and only if there is an algorithm to compute the Mordeil-Weil group, $E(K)/nE(K)$.
- Assuming the Tate-Shafarevich conjecture, one can compute $E(K)/nE(K)$ and decide if C has a point over K.
- The best known strategy for computing $E(K)/nE(K)$ under the assumption of the Tate-Shafarevich conjecture is not practical as it performs class group computations over an extension of K.

In this work, we gave fairly explicit pseudocode for the procedure that determines if C has a rational point. In the case $K = \mathbb{Q}$ and $j(C) \neq 0, 1728$, MAGMA code for computing the Jacobian and determining the local solubility of C can be found in the GitHub repository [24]. The benefit of these algorithms over the existing ones in MAGMA is that they work for arbitrary degree curves.

Bibliography

[1] Yves Aubry and Marc Perret. A Weil theorem for singular curves. *De Gruyter*, 1996.

[2] Zenon I. Borevich and Igor R. Shafarevich. *Number Theory*. Pure & Applied Mathematics. Academic Press, New York, NY, 1966. ISBN 0121178501 9780121178505.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 2010. ISBN 978-3-662-02945-9.

[5] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves, I. Algebra. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2008, 07 2006. doi: 10.1515/CRELLE.2008.012.

[6] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves, II. Geometry. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 632, 12 2006. doi: 10.1515/CRELLE.2009.050.

[7] John Cremona, Tom Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll. Explicit n-descent on elliptic curves. III. Algorithms. *Mathematics of Computation*, 84, 07 2011. doi: 10.1090/S0025-5718-2014-02858-5.

[8] Tom Fisher. The invariants of a genus one curve. *Proceedings of the London Mathematical Society*, 2006.

[9] Marvin J. Greenberg. Rational points in henselian discrete valuation rings. *Publications mathématiques de l'IHÉS*, 1966.

[10] Sean Hallgren. *Quantum Algorithms for Class Group of a Number Field*, pages 694–696. Springer US, Boston, MA, 2008. ISBN 978-0-387-30162-4. doi: 10.1007/978-0-387-30162-4_310. URL https://doi.org/10.1007/978-0-387-30162-4_310.

[11] David Harari. *Galois Cohomology and Class Field Theory*. Universitext. Springer, 2020. ISBN 978-3-030-43901-9.

[12] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 2013. ISBN 9781475738490.

[13] Florian Hess. *Computing Riemann-Roch spaces in algebraic function fields and related topics*. Academic Press Limited, 2001.

[14] Nathan Jacobson. *Basic Algebra 1*. Dover Publications, 2009. ISBN 9780486471891.

[15] Biasse Jean-François and Song Fang. *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, pages 893–902. 2016. doi: 10.1137/1.9781611974331.ch64. URL https://epubs.siam.org/doi/abs/10.1137/1.9781611974331.ch64.

[16] Zhongxuan Luo, Erbao Feng, and Jielin Zhang. Computing Singular Points of Projective Plane Algebraic curves by Homotopy Continuation Methods. *Discrete Dynamics in Nature and Society*, 2014.

[17] Daniel A. Marcus. *Number Fields*. Springer, 2018. ISBN 978-3-319-90233-3.

[18] Paulo Ribenboim. *The Theory of Classical Valuations*. Springer Monographs in Mathematics. Springer, 1999. ISBN 978-1-4612-0551-7.

[19] Steven Roman. *Field Theory*. Graduate Texts in Mathematics. Springer, 2005. ISBN 978-0-387-27678-6.

[20] Jean-Pierre Serre. *Local Fields*. Springer, 2013. ISBN 978-1-4757-5673-9.

[21] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009. ISBN 9780387094939.

[22] Michael Stoll. Descent on elliptic curves, 2006.

[23] Andrew Sutherland. *Introduction To Arithmetic Geometry*. Massachusetts Institute of Technology: MIT OpenCouseWare, Spring 2023. URL https://ocw.mit.edu/.

[24] Nicolas Swanson. Deciding if a Genus 1 Curve has a Point, 2024. URL https://github.com/Nicswansonvt/DecidingIfGenus1CurvehasQPoint.