university of groningen

faculty of science and engineering

On Certain Elliptic Surfaces With j-Invariant Zero Over Prime Fields of Positive Characteristic

Master Project Mathematics

January 2023

Student: S.E. Bootsma

First supervisor: Prof. dr. J. Top

Second supervisor: Prof. dr. C. Salgado

Abstract

We find prime numbers p so that the elliptic surface defined by the equation

$$y^2 = x^3 + t^{360} + 1$$

has Mordell-Weil rank 68 over $\mathbb{F}_p$. Moreover, we show that, up to finite index, these generating sections are obtained from a reduction modulo p of the characteristic zero case. Furthermore, using both the Tate conjecture for abelian varieties over finite fields and the theory of $\mathbb{F}_{q^2}$-maximal curves, where q is a prime power, we prove that the family of elliptic surfaces over $\mathbb{F}_p$ defined by the equation $y^2 = x^3 + t^{p+1} + 1$ has Mordell-Weil rank $p - 1$.

Keywords— Elliptic Curves, Elliptic Surfaces, Mordell-Weil Rank, Zeta Functions, Finite Fields and Maximal Curves.

Contents

1 Introduction

Elliptic curves remain a fascinating topic in mathematics. In this thesis we have gathered several methods on finding ranks and rank bounds of elliptic curves over function fields of the form $k(t)$, where k is a finite field.

Before we continue suppose that $k = \bar{k} \supset \mathbb{Q}$ is an algebraically closed field. It is the Mordell-Weil-Néron-Lang theorem [15] that asserts that the group of $k(t)$-rational points on a nonconstant elliptic curve $E/k(t)$ is finitely generated. If the j-invariant of E lies in the base field k, then the current rank record is due to Shioda [24] on the curve

$$E_{360}\colon y^2 = x^3 + t^{360} + 1, \tag{1.1}$$

which has rank 68 over $k(t)$. If we restrict to nonconstant j-invariant, the current rank record is 56 found independently by Stiller [28] on the curve

$$E\colon y^2 = 4x^3 - 27t^{-2520}x - 27t^{-2520} \tag{1.2}$$

and by Shioda [23] on the curve

$$E\colon y^2 = x^3 + t^{844}x + t^6. \tag{1.3}$$

A quick investigation shows that the latter two examples are in fact one and the same. Indeed, the elliptic surfaces that these two curves define are k-isogenous (see [9, Def. 1.1.11]) to the elliptic Delsarte surface defined by

$$y^2 = x^3 + t^{840}x + 1. \tag{1.4}$$

The elliptic curve E_{360} is also defined over $\mathbb{Q}(t)$, and we will show that the rank over $\mathbb{Q}(t)$ is at most 34. However, going back to $k = \bar{k} \supset \mathbb{Q}$ and following ideas from [3], we will see that 60 of these independent points are obtained via base changes from rational elliptic surfaces. The remaining 8 are obtained from a base change of an elliptic K3 surface. Furthermore, there exist a finite field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ of smallest degree so that we attain rank 68 over $\mathbb{Q}(\alpha, t)$, but finding this field extension is a nontrivial task.

A lot more about elliptic curves over function fields of the form $\mathbb{F}_{p^n}(t)$ is known. For example the Birch and Swinnerton-Dyer (BSD) conjecture is known for $E_{360}/\mathbb{F}_p(t)$ whenever the prime $p > 3$ (see [33, Theorem 12.2]). Moreover, in certain isotrivial cases it is possible to compute the rank of the Mordell-Weil group over $\mathbb{F}_p(t)$ via zeta functions of curves over finite fields.

Instead of finding a field extension of $\mathbb{Q}$ over which we attain rank 68 we try to find a prime number p so that all the 68 generating sections on the elliptic surface corresponding to E_{360} in characteristic zero exist and remain independent over $\mathbb{F}_p$ after a reduction modulo p. Due to Chebotarev's density theorem there are infinitely many primes that yield rank 68 for the Mordell-Weil group $E_{360}(\mathbb{F}_p(t))$. From the fact that the Néron-Severi group behaves well under reduction modulo primes p of good reduction ([34, Proposition 2.6.2]) we obtain that these sections are, up to finite index, in fact obtained from a reduction modulo p of the characteristic zero case. In particular, once we have found a prime p so that $\operatorname{rank} E_{360}(\mathbb{F}_p(t)) = \operatorname{rank} E_{360}(\bar{\mathbb{F}}_p(t)) = 68$ we know that all the sections in characteristic zero will exist and remain independent over $\mathbb{F}_p$ after a reduction modulo p.

The text is organized as follows. First there is a preliminary section to familiarize the reader with notation and common notions in this area of mathematics. Thereafter, we discuss the main methods used to obtain prime numbers for which the elliptic curve $E_{360}/\mathbb{F}_p(t)$ has high rank. In the last two sections the main results are discussed. We first look at primes $p \equiv 1 \mod 6$ and show that for the primes $p = 44460001$, $p = 96614641$, $p = 133773121$, $p = 177452641$ and $p = 206869681$ we obtain rank 68. Lastly we look at primes $p \equiv 5 \mod 6$ and show, using maximal curves, that the elliptic curve $y^2 = x^3 + t^{p+1} + 1$ has rank $p - 1$ over $\mathbb{F}_p(t)$.

2 Preliminaries

We assume throughout this thesis that the reader is familiar with the basics of both algebraic geometry and algebraic number theory. Topics include schemes, sheaves and their cohomology, and splitting behaviour of primes in number fields. Section I, II and III of [8] and Section I of [14] should suffice.

Moreover, a solid understanding of the theory of elliptic curves such as treated in [25] is assumed. We start by introducing the proper notions and definitions needed.

Let $n \geq 0$ be an integer. Throughout this thesis we write

$$E_n \colon y^2 = x^3 + t^n + 1 \tag{2.1}$$

for an elliptic curve over $k(t)$, where k is a field of characteristic not 2 nor 3.

2.1 Some Algebraic Geometry

Let k be a perfect field, fix an algebraic closure $\bar{k}$ and write $G_{\bar{k}/k}$ for the absolute Galois group of k.

Definition 2.1.1. *An affine algebraic curve C over k is a 1-dimensional affine variety defined over k.*

Definition 2.1.2. *A projective algebraic curve C over k is a 1-dimensional projective variety defined over k.*

Important is that for any affine algebraic curve there always exists a unique smooth projective model. I.e. whenever C/k is an affine algebraic curve, there exists a smooth projective algebraic curve $\tilde{C}/k$ which has the same function field as the affine curve. One way to obtain this is via repeated blow-ups or via a gluing process of affine charts. Fulton's notes [7] are an excellent resource for this material.

Example 2.1.3. *Let $k = \mathbb{F}_q = \mathbb{F}_{p^r}$ be a finite field not of characteristic 2 nor 3, then we have an affine algebraic curve*

$$C \colon s^6 = t^n + 1$$

defined over k for any $n \in \mathbb{Z}_{>0}$. This is a nonsingular affine curve whenever $p \nmid n$. In general, projectivizing this in the naive way (taking the projective closure in $\mathbb{P}^2$) yields a singular projective curve. We illustrate a way to create a smooth projective model for $n = 6l$ with l an integer. In this case we have the curve

$$C \colon s^6 = t^{6l} + 1$$

over the field $k = \mathbb{F}_{p^r}$. Consider a copy of C given by $D \colon y^6 = x^{6l} + 1$. We obtain a smooth projective (cf. [17, Section IIIa.1]) curve $\tilde{C}$ via the gluing maps $t = 1/x$ and $s = y/x^l$. Moreover, the curve obtained has the same function field as C/k so it is the unique smooth model.

From now on when we say C/k is a curve we always mean the smooth projective model of C unless stated otherwise.

Definition 2.1.4. *Let V_1, $V_2 \subset \mathbb{P}^n$ be projective varieties over $\bar{k}$. A rational map from V_1 to V_2 is a map of the form*

$$f \colon V_1 \to V_2, \quad \phi = [f_0, \ldots, f_n]$$

where the functions $f_0, \ldots, f_n \in \bar{k}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined, $\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$.

If V_1 and V_2 are defined over k, then the absolute Galois group $G_{\bar{k}/k}$ acts on ϕ in the obvious way:

$$\phi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)].$$

We say ϕ is defined over k if $\phi = \phi^\sigma$ for all $\sigma \in G_{\bar{k}/k}$.

Definition 2.1.5. *Keep the notation as above. A rational map*

$$\phi = [f_0, \ldots, f_n] \colon V_1 \to V_2$$

is regular (or defined) at $P \in V_1$ if there is a function $g \in \bar{k}(V_1)$ such that

(i) each gf_i is regular at P;

(ii) there is some i for which $(gf_i)(P) \neq 0$.

The most important result we have for curves is the following.

Proposition 2.1.6. *Let C be a curve and $V \subset \mathbb{P}^n$ a variety both defined over $\bar{k}$. Let $P \in C$ be a smooth point, and let $\phi\colon C \to V$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism (of algebraic varieties).*

Proof. See [25, Section II.2, Proposition 2.1]. □

From now on we will just say curve/variety instead of curve/variety over $\bar{k}$. If we work over a not algebraically closed field k it will be stated explicitly.

Definition 2.1.7. *Let $f\colon V_1 \to V_2 \subset \mathbb{P}^n$ be a rational map of projective varieties. We say f is dominant if it has dense image.*

Definition 2.1.8. *We say a projective variety V_1 covers V_2 if there exists a dominant rational map from $V_1 \to V_2$.*

The following is a well-known result about morphisms of curves.

Theorem 2.1.9. *Let $f\colon C_1 \to C_2$ be a morphism between algebraic curves. Then f is constant or surjective.*

Proof. See [8, Section II, Proposition 6.8]. □

Definition 2.1.10. *Let $\phi\colon C_1 \to C_2$ be a morphism of curves defined over k. If ϕ is constant, we define the degree of ϕ to be 0. Otherwise we say that ϕ is a finite map and we define its degree to be*

$$\deg(\phi) = [k(C_1)\colon \phi^*(k(C_2))],$$

where ϕ^* denotes pullback. We say that ϕ is separable, inseparable, or purely inseparable if the field extension $k(C_1)/\phi^*(k(C_2))$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s(\phi)$ and $\deg_i(\phi)$, respectively.

In characteristic 0 all morphisms of curves are separable. In characteristic $p > 0$ this is not necessarily the case.

Example 2.1.11. *Let $k = \mathbb{F}_p$ be a finite field with $p \equiv -1 \mod 6$. Consider the smooth projective curve C/k given by affine equation $C\colon s^6 = t^{p+1} + 1$. We have a morphism of curves $f\colon C \to \mathbb{P}^1$, given by $f(s,t) = (t : 1)$. The degree of this map is just $[k(s,t)\colon k(t)]$ with s and t satisfying the relation $s^6 = t^{p+1} + 1$. As $t^{p+1} + 1$ is neither a square nor a cube in $k(t)$ we find that the degree of f equals 6. Moreover, as the minimal polynomial of s over $k(t)$ is $x^6 - t^{p+1} - 1$, which is separable, we find that the map f is separable.*

The next definition is important for computing the genus of several curves.

Definition 2.1.12. *Let $\phi\colon C_1 \to C_2$ be a nonconstant morphism of smooth curves, and let $P \in C_1$. The ramification index of ϕ at P, denoted by $e_\phi(P)$, is the quantity $e(P) = ord_P(\phi^* t_{\phi(P)})$ where $t_{\phi(P)} \in \bar{k}(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ is unramified at P if $e_\phi(P) = 1$, and that ϕ is unramified if it is unramified at every point of C_1.*

Theorem 2.1.13 (Riemann-Hurwitz)**.** *Let $\phi\colon C_1 \to C_2$ be a nonconstant separable morphism of smooth curves of genera g_1 and g_2, respectively. Then*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1) \tag{2.2}$$

Further, equality holds if and only if one of the following two conditions is true:

(i) $char(k) = 0$.

(ii) $char(k) = p > 0$ and p does not divide $e_\phi(P)$ for any $P \in C_1$.

Proof. See [25, Section II, Theorem 5.9]. □

Definition 2.1.14 (The Frobenius Morphism)**.** *Assume that $char(k) = p > 0$ and let $q = p^r$. For any polynomial $f \in k[X]$, let $f^{(q)}$ be the polynomial obtained from f by raising each coefficient of f to the q^{th} power. Then for any curve C/k, we can define a new curve $C^{(q)}/k$ as the curve whose homogeneous ideal is given by the ideal generated by $\{f^{(q)}\colon f \in I(C)\}$. Further, there is a natural map from C to $C^{(q)}$, called the q^{th}-power Frobenius morphism, given by $\phi\colon C \to C^{(q)}$, $\phi([x_0, \ldots, x_n]) = [x_0^q, \ldots, x_n^q]$.*

Lemma 2.1.15. *Keep the previous notation. Then ϕ is purely inseparable if and only if its degree is q. Moreover, Every map $\psi\colon C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as*

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

where $q = \deg_i(\psi)$ and λ is a separable map.

Proof. See [25, Section II, Corollary 2.12]. □

Definition 2.1.16. *Let C/k be a smooth curve, we get an abelian group of finite formal sums*

$$\mathcal{D}(C) \coloneqq \left\{ \sum_{i=1}^{r} n_i P_i | r \in \mathbb{N}, n_i \in \mathbb{Z}, P_i \in C(\bar{k}) \right\},$$

called the divisor group of C. A divisor $D \in \mathcal{D}(C)$ is called effective if all $n_i \geq 0$ and the degree of D is $\deg(D) = \sum_{i=1}^{r} n_i$.

With notations as above, any nonzero function $h \in \bar{k}(C)$ gives rise to a divisor $\operatorname{div}(h) = \sum_P \operatorname{ord}_P(h)P$ which is of degree 0.

Definition 2.1.17. *We say two divisors D, D' are linearly equivalent if $D - D' = div(h)$ for some $h \in \bar{k}(C)^\times$.*

Note that the absolute Galois group $G_{\bar{k}/k}$ acts on $\mathcal{D}(C)$ in a natural way via $\sigma\left(\sum_{i=1}^{r} n_i P_i\right) \coloneqq \sum_{i=1}^{r} n_i P_i^\sigma$, where P_i^σ indicates the result of the action of the absolute Galois group on the coordinates of the point P_i. A divisor D in the divisor group of C is defined over k if $D = D^\sigma$ for all elements σ of the absolute Galois group. This group is denoted by $\mathcal{D}_k(C)$.

Definition 2.1.18. *The Picard group of the curve C is defined as the abelian group consisting of divisors modulo linear equivalence. It is usually denoted by $Pic(C)$. The abelian group consisting of degree zero divisors modulo linear equivalence is denoted by $Pic^0(C)$.*

Definition 2.1.19. *The Picard group of the curve C/k is the subgroup of $Pic(C)$ which is fixed under the absolute Galois group. It is denoted by $Pic_k(C)$. The subgroup of $Pic^0(C)$, which is fixed by $G_{\bar{k}/k}$ is denoted by $Pic_k^0(C)$.*

Remark 2.1.20. *The Picard group of C/k is not necessarily equal to the group $\mathcal{D}_k(C)$ modulo linear equivalence (over k). See [5] for an overview when this is the case.*

Note that the Picard group is sometimes called the divisor class group, and its degree zero component is sometimes referred to as the Jacobian. We use these notions simultaneously.

There are several equivalent definitions for the notion of abelian variety. The one we adapt is by Milne [16].

Definition 2.1.21 (Group Variety)**.** *A group variety over k is an algebraic variety V over k together with regular maps*

$$\begin{aligned} m\colon V \times_k V \to V \quad &\textit{(multiplication)} \\ inv\colon V \to V \quad &\textit{(inverse)} \end{aligned}$$

and an element $e \in V(k)$ such that the structure on $V(\bar{k})$ defined by m and inv is a group with identity element e. Such a quadruple (V, m, inv, e) is a group in the category of varieties over k.

Definition 2.1.22 (Abelian Variety)**.** *An abelian variety over k is a complete geometrically irreducible group variety over k.*

Definition 2.1.23. *Let A and B be abelian varieties over k and $f\colon A \to B$ a morphism of k-varieties. We say the f is a homomorphism of abelian varieties if $f(P \cdot Q) = f(P) \cdot f(Q)$ for all $P, Q \in A(\bar{k})$.*

Lemma 2.1.24. *Let A/k be an abelian variety. Then A is projective over k and the group law is abelian.*

Proof. See [16, Corollary 1.4 & Theorem 6.4]. □

Definition 2.1.25. *Let A and B be two abelian varieties over k. Suppose that $f\colon A \to B$ is a morphism of algebraic varieties over k. We call f an isogeny if it is surjective, has finite fibers and maps basepoint e_A to basepoint e_B. Whenever such an isogeny exists we call A and B isogenous.*

Lemma 2.1.26. *Let $f\colon A \to B$ be a homomorphism of abelian varieties over k. Then f is an isogeny if and only if it is surjective and $\dim(A) = \dim(B)$.*

Proof. See [16, Proposition 7.1]. □

2.2 Jacobian Varieties

Throughout this section let C/k be a smooth projective curve over a field k and T a k-variety. The definitions and theorems stated here are all found in [16].

Let us first fix some notation. We denote $\mathbf{Var}_k$ for the category of k-varieties, $\mathbf{Ab}$ for the category of abelian groups, and $\mathrm{Pic}^0(T)$ and $\mathrm{Pic}^0(C \times T)$ for the groups of degree zero invertible sheaves on T and $C \times T$ respectively (recall the usual comparison between invertible sheaves and divisors [8, Section II.6]).

Definition 2.2.1. *We define the Picard functor P^0_C by $P^0_C(T) \coloneqq Pic^0(C \times T)/q^* Pic^0(T)$, where q is the natural projection map.*

Important is that this defines a functor from $\mathbf{Var}_k$ to $\mathbf{Ab}$ and it is represented by an abelian variety $\operatorname{Jac} C$ (or J_C), called the Jacobian of C, of dimension the genus of C. The two most important properties of the Jacobian are

$$J_C(k) = \mathrm{Pic}^0_k(C),$$

and whenever $C(k) \neq \emptyset$ and moreover $g(C) > 0$ one has

$$C \hookrightarrow \operatorname{Jac} C$$

via any morphism $P \mapsto [P] - [P_0]$ where $P_0 \in C(k)$.

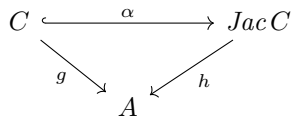
Example 2.2.2. *Let $k = \bar{k}$ be an algebraically closed field and let E/k be an elliptic curve. The Jacobian $Jac\, E$ of E is an abelian variety of dimension 1, i.e. it is a curve. We claim that $Jac\, E \cong E$, i.e. the Jacobian of an elliptic curve is the elliptic curve itself. This follows from the fact that the map*

$$\begin{aligned} f\colon E = E(k) &\to Jac\, E = J_E(k) = Pic^0(E) \\ P &\mapsto [P] - [\mathcal{O}_E] \end{aligned}$$

is an isomorphism. For more details see [25, Section III, Proposition 3.4].

Example 2.2.3 (Jacobian of Hyperelliptic Curve)**.** *Let $k = \bar{k}$ be an algebraically closed field of characteristic $\neq 2, 3$. Consider the smooth curve C/k given by affine equation $C\colon y^2 = x^6 - 1$ (this is the curve arising from the elliptic curve $E_2\colon y^2 = x^3 + t^2 + 1$, see (2.1)). This defines a hyperelliptic curve of genus 2, hence the Jacobian $Jac\, C$ is a 2-dimensional abelian variety. In positive characteristic we have the Frobenius endomorphism on $Jac\, C$. Using this we can compute the rank of $E_2(\mathbb{F}_p(t))$ with $\mathbb{F}_p$ the prime field of k (see Example 5.1.8).*

Theorem 2.2.4 (The Albanese Property)**.** *Suppose $g(C) > 0$, $P_0 \in C(k)$ and denote $\alpha : C \hookrightarrow Jac\, C$ the canonical inclusion. For every abelian variety A/k and every k-morphism $g\colon C \to A$ there exists a unique k-morphism $h\colon Jac\, C \to A$ which is up to translation a homomorphism of groups, so that the diagram*



commutes.

Proof. See [16, Proposition 6.1]. □

Remark 2.2.5. *If $g(C) = 0$, then the canonical map α is not an inclusion. However, any map $g\colon C \to A$ is constant ([16, Proposition 3.9]) implying that the Albanese property still holds.*

We will see that the Jacobian of a curve C is crucial in some of our rank computations.

2.3 Elliptic Curves

In the previous section we discussed some basic algebraic geometry, mostly of curves. This section builds on top of that by discussing projective curves that turn out to have a structure of a group variety. As previously, let k be a field and fix an algebraic closure $\bar{k}$.

Definition 2.3.1. *An elliptic curve E/k is a smooth projective curve of genus 1 together with a k-rational point on E, usually denoted by $\mathcal{O}$.*

What's important and quite remarkable is the following fact.

Theorem 2.3.2. *Any elliptic curve E/k can be written in the so-called Weierstrass form*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients $a_i \in k$ and the point $\mathcal{O} = (0:1:0) \in \mathbb{P}^2$. Moreover, when the characteristic of the field k is neither 2 nor 3 we can take $a_1 = a_3 = a_2 = 0$. In this case we usually write $E\colon y^2 = x^3 + Ax + B$ and say that E/k is in short Weierstrass form.

Proof. See [25, Section III, Proposition 3.1]. □

Definition 2.3.3. *Let E/k be an elliptic curve given by a short Weierstrass equation $E\colon y^2 = x^3 + Ax + B$. The j-invariant of E/k is defined as*

$$-1728\frac{(4A)^3}{\Delta},$$

where $\Delta = -16(4A^3 + 27B^2)$ is a quantity known as the discriminant of the elliptic curve E/k.

Important in our study will be elliptic curves with j-invariant equal to zero. In particular, elliptic curves of the form $E\colon y^2 = x^3 + a$ with $a \in k^\times$.

Definition 2.3.4. *Let E/k be an elliptic curve with k not of characteristic 2 nor 3 given by a short Weierstrass equation. Given $d \in k^\times$ not a square we define the quadratic twist of E by the extension $k(\sqrt{d})$ as*

$$E_d\colon dy^2 = x^3 + Ax + B,$$

which is another elliptic curve over k.

It turns out that an elliptic curve is not only a variety, but it is also a group variety. In particular, the set of k-rational points of E/k inherits a group structure from its Jacobian $J_E(k)$ with the point $\mathcal{O}$ acting as identity. The next lemma tells us why this is the case.

Lemma 2.3.5. *Let E/k be an elliptic curve, then the map $\alpha\colon E(k) \to J_E(k)$ sending P to $[P] - [\mathcal{O}]$ is bijective.*

Proof. See [25, Section III, Proposition 3.4] and compare Example 2.2.2. □

The above tells us that an elliptic curve is in fact an abelian variety of dimension 1. Therefore, the notion of isogeny as in Definition 2.1.25 and the notions isomorphism, endomorphism etc. make perfect sense.

Lemma 2.3.6. *Let E_1 and E_2 be elliptic curves both defined over k and $f\colon E_1 \to E_2$ a nonconstant k-isogeny of degree m. Then there exists a unique k-isogeny $\hat{f}\colon E_2 \to E_1$, called the dual isogeny, so that $\hat{f} \circ f = [m]$.*

Proof. See [25, Theorem 6.1]. □

If E/k is an elliptic curve and $E(k)$ is a finitely generated abelian group we write $r(E(k))$ or rank $E(k)$ for the $\mathbb{Z}$-rank of this group. It is called the Mordell-Weil rank of E/k.

Lemma 2.3.7. *Let E_1 and E_2 be elliptic curves over a field k. Assume that $E_1(k)$ and $E_2(k)$ are both finitely generated. Let $f\colon E_1 \to E_2$ be a k-isogeny, then the groups $E_1(k)$ and $E_2(k)$ have the same rank.*

Proof. The map f has finite fibers, in particular finite kernel. It follows that f is injective on the torsion-free part, hence $r(E_2(k)) \geq r(E_1(k))$. The reverse inequality follows from the dual isogeny. □

Theorem 2.3.8. *Let E and E' be two elliptic curves defined over k. Then they are isomorphic over $\bar{k}$ if and only if they have the same j-invariant.*

Proof. See [25, Section III, Proposition 1.4]. □

The following theorem is the cornerstone of this thesis.

Theorem 2.3.9. *Suppose k is a field which is finitely generated over its prime field. Let A/k be an abelian variety. Then the group of k-rational points $A(k)$ is a finitely generated abelian group and we write $r(A(k))$ for its rank.*

Proof. See [15]. □

Corollary 2.3.10. *Let $k = \mathbb{F}_q$ be a finite field with $q = p^r$ elements. Define $K := k(t)$ the function field of the projective line over k. Let E/K be an elliptic curve, then $E(K)$ is a finitely generated abelian group.*

Proof. This follows immediately from Theorem 2.3.9. □

Remark 2.3.11. *It is important in Theorem 2.3.9 that the field of definition is finitely generated over its prime field. For example, the group of complex points on an elliptic curve is definitely not finitely generated.*

It is unknown how to determine the Mordell-Weil rank of the elliptic curve E/K in general. In this thesis we are concerned with elliptic curves E/K where $K = k(C)$ is the function field of a smooth projective algebraic curve defined over a finite field k. It turns out that there is an equivalence between elliptic curves E/K and certain algebraic surfaces $\mathcal{E}/k$. Next section gives the set-up and preliminaries to discuss this equivalence. However, before we continue we want to state a lemma that will be relevant throughout this thesis.

Lemma 2.3.12. *Let k be a field not of characteristic 2 nor 3 and let E/k be an elliptic curve satisfying $r(E(k)) < \infty$. Suppose that $L := k(\sqrt{-3})$ is a degree 2 field extension of k. Then we have*

$$r(E(L)) = r(E(k)) + r(E'(k)),$$

where E' is the quadratic twist of E/k by L.

Proof. See [3, p. 2-3]. □

Corollary 2.3.13. *Let k be a field not of characteristic 2 nor 3, fix $a \in k^\times$ and let E/k be an elliptic curve given by $E\colon y^2 = x^3 + a$ satisfying $r(E(k)) < \infty$. Suppose that $L := k(\sqrt{-3})$ is a degree 2 extension of k. Then we have*

$$r(E(L)) = 2 \cdot r(E(k)).$$

Proof. The curve E is k-isogenous to the elliptic curve $\hat{E}\colon y^2 = x^3 - 27a$ (see [32, Section 3]). Moreover, the quadratic twist $E'\colon -3y^2 = x^3 + a$ is k-isogenous to $\hat{E}'\colon -3y^2 = x^3 - 27a$. This latter curve is isomorphic to the elliptic curve E. As isogenous curves have the same rank (Lemma 2.3.7) the result follows from Lemma 2.3.12. □

This corollary is quite useful, as for a prime $p \equiv -1 \mod 6$ we get $r(E_n(\mathbb{F}_{p^2}(t))) = 2 \cdot r(E_n(\mathbb{F}_p(t)))$ and the former rank is sometimes easier to calculate. We end this section by defining supersingularity for elliptic curves (not to be confused with supersingular surfaces).

Definition 2.3.14. *Let E/k be an elliptic curve over a field with characteristic $p > 0$. We say E is a supersingular elliptic curve if $End(E)$ is an order in a quaternion algebra, where $End(E)$ are the endomorphisms of E over $\bar{k}$.*

Elliptic curves which are not supersingular are called ordinary. In characteristic zero all elliptic curves are ordinary.

Theorem 2.3.15. *Let E/k be an elliptic curve over a field with characteristic $p > 0$. The endomorphism ring of E is isomorphic to one of*

(i) $\mathbb{Z}$;

(ii) an order in an imaginary quadratic field;

(iii) an order in a quaternion algebra.

In particular, when $End(E)$ is noncommutative we know that E is supersingular.

Proof. See [25, Cor. 9.4]. □

Example 2.3.16. *Suppose q is odd and $q \equiv 2 \mod 3$. Let $B \in \mathbb{F}_q^\times$. Then the elliptic curve E given by $y^2 = x^3 + B$ is supersingular.*

Proof. Denote $\phi = \text{Frob}_q$ for the q^{th} power Frobenius endomorphism on E and $\rho\colon E \to E$ for the endomorphism defined by $\rho(x, y) = (\omega x, y)$ with $\omega \in \mathbb{F}_q$ satisfying $\omega^2 + \omega + 1 = 0$. We have $(\phi \circ \rho)(x, y) = (\omega^q x^q, y^q)$ and $(\rho \circ \phi)(x, y) = (\omega x^q, y^q)$. These are equal if and only if $\omega^q = \omega$, but ω is of order 3 and $q \equiv 2 \mod 3$. Therefore, these cannot be equal and the result follows from Theorem 2.3.15. □

2.4 Algebraic Surfaces and Their Intersection Theory

Throughout this section let $k = \bar{k}$ be an algebraically closed field. Excellent references on this material are [8, Section V & Appendix A], [1] and the Stacks Project [26].

Definition 2.4.1. *An algebraic surface S is an algebraic variety of dimension 2.*

In this thesis we will be interested in irreducible smooth projective surfaces over (algebraically closed) fields. In fact, when we say algebraic surface we will mean irreducible smooth projective surface together with an embedding into $\mathbb{P}^n$, unless stated otherwise.

Just as with curves we can look at divisors on our surface.

Definition 2.4.2. *The divisor group of a surface S is the abelian group*

$$\mathcal{D}(S) = \left\{ \sum_{i=1}^{r} n_i C_i | r \in \mathbb{N}, n_i \in \mathbb{Z}, C_i \subset S \text{ an irreducible curve} \right\}.$$

In a similar fashion as with curves we have that any function $h \in k(S)^\times$ gives rise to a divisor $\text{div}(h)$ and two divisors are once again linearly equivalent if their difference is a divisor of the form $\text{div}(g)$ for some $g \in k(S)^\times$.

Definition 2.4.3. *The group of divisors modulo linear equivalence is called the Picard group of the surface S and it is denoted by $Pic(S)$.*

In order to continue properly we need some more abstract theory. Let R be a ring. Let M be an R-module.

Definition 2.4.4. *The tensor algebra of M over R is the noncommutative R-algebra*

$$T(M) = T_R(M) = \bigoplus_{n \geq 0} T^n(M),$$

with $T^0(M) = R$, $T^1(M) = M$, $T^2(M) = M \otimes_R M$, $T^3(M) = M \otimes_R M \otimes_R M$, etc. Multiplication is defined by the rule that on pure tensors we have

$$(x_1 \otimes x_2 \otimes \ldots \otimes x_n) \cdot (y_1 \otimes y_2 \otimes \ldots \otimes y_n) = x_1 \otimes x_2 \otimes \ldots \otimes x_n \otimes y_1 \otimes y_2 \otimes \ldots \otimes y_n$$

and we extend this by linearity.

Definition 2.4.5. *The exterior algebra $\Lambda(M)$ of M over R is the quotient of $T(M)$ by the two sided ideal generated by the elements $x \otimes x \in T^2(M)$. The image of a pure tensor $x_1 \otimes \ldots \otimes x_n$ in $\Lambda^n(M)$ is denoted $x_1 \wedge \ldots \wedge x_n$. These elements generate $\Lambda^n(M)$, they are R-linear in each x_i and they are zero when two of the x_i are equal (i.e., they are alternating as functions of $x_1, x_2, \ldots, x_n$). The multiplication on $\Lambda(M)$ is graded commutative, i.e., every $x \in M$ and $y \in M$ satisfy $x \wedge y = -y \wedge x$.*

Definition 2.4.6. *Let $(X, \mathcal{O}_X)$ be a scheme and $\mathcal{F}$ an $\mathcal{O}_X$-module. We define the n^{th} exterior power of $\mathcal{F}$ to be the sheafification of the presheaf*

$$U \mapsto \Lambda^n_{\mathcal{O}_X(U)}\left(\mathcal{F}(U)\right),$$

where the right-hand side is the n^{th} exterior power of $\mathcal{O}_X(U)$-modules as in Definition 2.4.5. It is denoted by $\Lambda^n\mathcal{F}$.

Viewing S as a scheme we can now define the canonical bundle of S.

Definition 2.4.7. *The canonical bundle of a surface S is given by*

$$\omega_S \coloneqq \Lambda^2\Omega^1_S,$$

where Ω^1_S denotes the sheaf of 1-forms on S

Note that this is an invertible sheaf on S. Indeed, as $\dim(S) = 2$ we obtain that Ω^1_S is locally free of rank 2. This forces ω_S to be locally free of rank 1, hence invertible. The usual connection between divisors and invertible sheaves then yields the canonical divisor $\mathcal{K}_S$ of the surface S.

Definition 2.4.8. *The Néron-Severi group of a surface S, denoted by $NS(S)$, is the group of divisors $\mathcal{D}(S)$ modulo algebraic equivalence, where we say a divisor D is algebraically equivalent to 0 if there is a connected scheme W and an effective divisor $\bar{D}$ on $S \times W$, such that $\bar{D}$ is flat over W and $D = \bar{D}_{w_1} - \bar{D}_{w_2}$ for two fibers $\bar{D}_{w_1}, \bar{D}_{w_2}$ of $\bar{D}$ at some $w_1, w_2 \in W$.*

Remark 2.4.9. *The statement $\bar{D}$ is flat over W just means that the corresponding morphism is flat.*

Theorem 2.4.10. *The Néron-Severi group of S is a finitely generated abelian group. Its rank is called the Picard number of the surface and is denoted by $\rho(S)$.*

Proof. See [13, Section 6.6]. □

Definition 2.4.11. *The i^{th} Betti number of a surface S is given by*

$$b_i(S) = \dim H^i(S),$$

where we can work with singular cohomology over $\mathbb{C}$ in the case of characteristic zero or generally with l-adic étale cohomology ($l \neq char(k)$).

This latter cohomology theory is defined as follows: fix a prime $l \neq \mathrm{char}(k)$ and denote $\mathbb{Z}_l$ for the ring of l-adic integers, which equals the inverse limit $\varprojlim \mathbb{Z}/l^n\mathbb{Z}$. We define

$$H^i(S, \mathbb{Z}_l) \coloneqq \varprojlim H^i(S, \mathbb{Z}/l^n\mathbb{Z}),$$

where $H^i(S, \mathbb{Z}/l^n\mathbb{Z})$ is not the usual sheaf cohomology, but rather the etalé cohomology[†]. Moreover, we define

$$H^i(S, \mathbb{Q}_l) := H^i(S, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Theorem 2.4.12. *The Betti numbers of S are independent of the chosen cohomology theory.*

Proof. See [8, Appendix C]. □

Theorem 2.4.13 (Poincaré Duality)**.** *The Betti numbers satisfy*

$$b_0 = b_4 \quad \textit{and} \quad b_1 = b_3.$$

Proof. See [8, Appendix C.3]. □

Definition 2.4.14. *We say a surface S is supersingular when its Picard number $\rho(S)$ equals its second Betti number b_2.*

Below we outline some more invariants of algebraic surfaces that will show up in this thesis.

[†]See [8, Appendix C.3].

Definition 2.4.15. *Let S be an algebraic surface, then its Euler number $e(S)$ is given by*

$$e(S) \coloneqq \sum_{i=0}^{4} (-1)^i b_i(S).$$

Together with Poincaré-duality we can write $b_2 = e(S) - 2(b_0 - b_1)$, which will be useful for computations later.

Definition 2.4.16. *Let S be an algebraic surface, its Euler characteristic $\chi(S)$ is defined as the Euler characteristic of its structure sheaf $\mathcal{O}_S$. In other words:*

$$\chi(S) = \sum_{i=0}^{2} (-1)^i \dim H^i(S, \mathcal{O}_S),$$

where $H^i(S, \mathcal{O}_S)$ denotes the usual sheaf cohomology.

Of particular importance in this thesis is the intersection number of two curves on an algebraic surface. We restrict ourselves to the bare minimum.

Definition 2.4.17. *Let S be a smooth algebraic surface and suppose C and D are two distinct irreducible curves on S. Denote f and g local equations for C and D respectively at a point P on S. The intersection multiplicity of C and D at $P \in S$ is defined by*

$$mult_P(C, D) \coloneqq \dim_k \mathcal{O}_{S,P}/(f, g).$$

This gives a well-defined finite number which extends globally to the intersection number of C and D given by $(C.D) \coloneqq \sum_{P \in S} mult_P(C, D)$.

Remark 2.4.18. *The definition applies only to distinct, irreducible curves on S. However, by utilizing the Euler-characteristic of invertible sheaves on S, one can extend the pairing to all of $\mathcal{D}(S)$ such that it is independent under linear equivalence. In particular, it extends to a well-defined pairing on $Pic(S)$. Using this the self-intersection of C is given by*

$$C^2 = (C.C) \coloneqq (C.D),$$

where $D \neq C$ is a divisor linearly equivalent to C. See [8, Section V, Theorem 1.1] for more details.

For further information on intersection theory we refer to [19, Section 4.3] and [8, Section 5]. Additionally, for future reference, the adjunction formula and Noether's formula will now be stated.

Theorem 2.4.19 (Adjunction)**.** *Let $C \subset S$ be an irreducible curve on an algebraic surface S. Then*

$$2p_a(C) - 2 = C^2 + (C.\mathcal{K}_S)\,,$$

where $p_a(C)$ denotes the arithmetic genus of C.

Proof. See [8, Section V, Prop. 1.5]. □

Lemma 2.4.20 (Noether's Formula)**.** *Let S be an algebraic surface, then we have the relation*

$$12\chi(S) = e(S) + \mathcal{K}_S^2,$$

where $\mathcal{K}_S^2$ denotes self-intersection of the canonical divisor $\mathcal{K}_S$.

Proof. This is a corollary of Riemann-Roch for surfaces. See [8, Section V, Remark 1.6.1]. □

2.5 Elliptic Surfaces

Once again let $k = \bar{k}$ be an algebraically closed field and let C/k be a smooth projective curve with function field $K = k(C)$. A good definition for an elliptic surface is the following.

Definition 2.5.1. *An elliptic surface S over C is a smooth projective surface S together with an elliptic fibration over C, i.e. a surjective morphism $f\colon S \to C$ so that*

- *Almost all fibers are smooth curves of genus 1;*
- *No fiber contains an exceptional curve of the first kind, i.e. a smooth rational curve of self-intersection -1;*
- *f admits a section, i.e., a map $s\colon C \to S$ such that $f \circ s = id_C$.*

The second point is a technical requirement, known as "relative minimality", that is necessary in order to eliminate any unnecessary flexibility in the shape of the fibers caused by blow-ups of the surface S. The third point guarantees that the generic fiber (to be defined later) will be an elliptic curve. A complete classification of the singular fibers, using this definition, can be found in [19, Section 5.4].

Example 2.5.2. *Let E be an elliptic curve and C a smooth projective curve, then $E \times C$ is an elliptic surface with the elliptic fibration being the canonical projection onto C. Note that this is quite a peculiar example as none of the fibers are singular.*

One way to visualise sections on an elliptic surface is as follows. Let $S \to \mathbb{P}^1$ be an elliptic surface, and (P) and (O) be sections. Then these sections can be thought of as horizontal curves on S, which intersect all the fibers transversally at 1 point. This is nicely illustrated below:

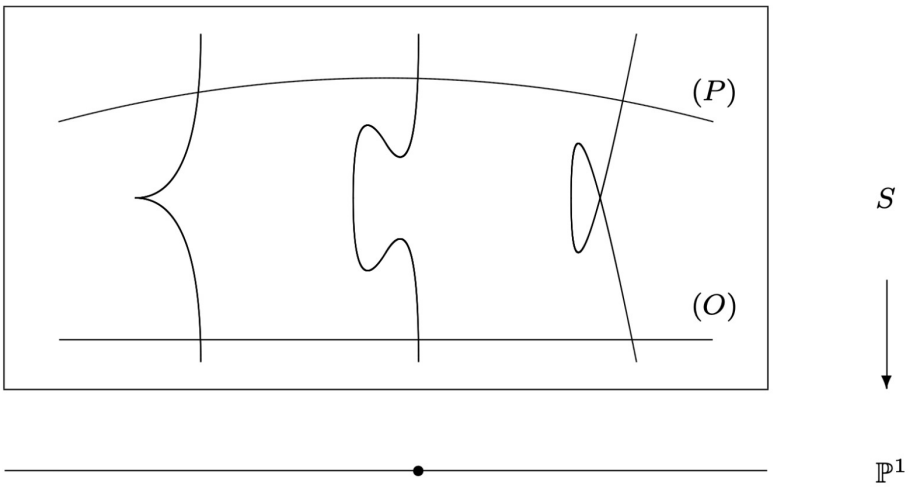


Figure 1: An Elliptic Surface With 2 Visible Sections [19].

Definition 2.5.3. *The generic fiber of an elliptic surface $f\colon S \to C$ is the fiber over the generic point of the curve C. By generic smoothness this defines a smooth curve of genus 1 over the function field $k(C)$. In particular, using that the elliptic surface has a section, the generic fiber becomes an elliptic curve.*

Important is that every section yields a $k(C)$-rational point on the generic fiber and conversely every $k(C)$-rational point on the generic fiber yields a section $C \to S$. As such we use the terminology interchangeably. Moreover, any such section defines a curve on the surface in a natural way. So it makes sense to talk about intersections of two sections.

Definition 2.5.4. *Let P be a $k(C)$-rational point on the generic fiber of an elliptic surface. Also write P for the curve it defines on the surface. We say the section $P \neq \mathcal{O}$ is integral if it does not intersect the zero section, i.e. $(P.\mathcal{O}) = 0$.*

Theorem 2.5.5. *Let C/k be a smooth projective curve. Write $K = k(C)$ and let E/K be an elliptic curve. Then there exists an elliptic surface $f\colon \mathcal{E} \to C$ with generic fiber isomorphic to E/K. Moreover, this elliptic surface is unique up to isomorphism and we call it the Kodaira-Néron model of E/K.*

Proof. See [19, Theorem 5.9]. □

Remark 2.5.6. *Let E/K be written in Weierstrass form. Denote $C' = C \setminus \Sigma$ with Σ the set containing the zeros of the discriminant of E/K, and the poles of the coefficients $a_i \in K$ of the Weierstrass form. The proof of Theorem 2.5.5 constructs the surface by starting with the Weierstrass equation of E/K, viewed as a surface $S' \subset \mathbb{P}^2 \times C'$. One takes the Zariski closure W of S' inside $\mathbb{P}^2 \times C$ and resolves the singularities of W in such a way that the obtained surface is relatively minimal.*

From now on we assume that our elliptic surfaces have at least one singular fiber. The following theorem illustrates why this is important.

Theorem 2.5.7. *Let E be an elliptic curve over the function field K. Assume that the Kodaira–Néron model $\mathcal{E}$ of E has a singular fiber. Then the abelian group $E(K)$ is finitely generated.*

Proof. See [19, Theorem 6.6]. □

Example 2.5.8. *Let $k = \bar{\mathbb{F}}_p$ be an algebraic closure of a finite field of characteristic $p > 3$. Consider for some fixed integer $n > 0$ the elliptic curve $E_n \colon y^2 = x^3 + t^n + 1$ over $k(t) = k(\mathbb{P}^1)$, then the associated elliptic surface $f_n \colon \mathcal{E}_n \to \mathbb{P}^1$ has at least one singular fiber, hence $E(K)$ is finitely generated.*

We will write E/K for the elliptic curve and $\mathcal{E}/k$ for the corresponding elliptic surface. The rank of an elliptic surface is the Mordell-Weil rank of the generic fiber.

Remark 2.5.9. *In this thesis we will look, among other things, at a supersingular elliptic surface with high Mordell-Weil rank. However, we should note that supersingularity and high Mordell-Weil rank are not related. Indeed, one can obtain large Mordell-Weil rank on ordinary elliptic surfaces as well (see [6]).*

Recall that the Picard group of a surface S is the group of divisors modulo linear equivalence. It has a well-defined pairing obtained from the intersection pairing. This pairing also behaves well with respect to algebraic equivalence (see [19, Section 4.3]). In particular, we find that $\mathrm{NS}(S)$ has a well-defined pairing induced from the intersection pairing. For elliptic surfaces this pairing gives a natural lattice structure on their Néron-Severi groups.

Definition 2.5.10. *Let S be an elliptic surface. The trivial lattice $Triv(S)$ is the sublattice of $NS(S)$ generated by the zero section and fiber components.*

Definition 2.5.11. *Let S be an elliptic surface. The essential lattice $L(S)$ is the orthogonal complement of $Triv(S)$ with sign reversed, i.e. $L(S) = (Triv(S)^{\perp})^{-}$.*

Lemma 2.5.12. *Let E/K be an elliptic curve with Kodaira-Néron model $\mathcal{E}/k$ and write $NS(\mathcal{E})_{\mathbb{Q}}$ for the Néron-Severi group tensored with $\mathbb{Q}$. For any $P \in E(K)$, there exists a unique element of $NS(\mathcal{E})_{\mathbb{Q}}$, say $\phi(P)$, satisfying the following conditions:*

(i) $\phi(P) \equiv (P) \mod Triv(\mathcal{E})_{\mathbb{Q}}$, *and* *(ii)* $\phi(P) \perp Triv(\mathcal{E})$,

where $\perp$ means "orthogonal to" in the lattice setting (see [19, Section 2]).

Theorem 2.5.13. *For any $P, Q \in E(K)$, let*

$$\langle P, Q \rangle = -(\phi(P).\phi(Q)). \tag{2.3}$$

This defines a $\mathbb{Q}$-valued symmetric bilinear pairing on $E(K)$ which induces the structure of a positive-definite lattice on $E(K)/E(K)_{tors}$.

Proof. See [19, Section 6.5]. □

The above pairing is called the height-pairing and it is an important tool in showing sections are independent from each other. Moreover, an explicit formula for this pairing is known and provided in the next theorem.

Theorem 2.5.14. *For any $P, Q \in E(K)$ we have*

$$\langle P, Q\rangle = \chi + (P.\mathcal{O}) + (Q.\mathcal{O}) - (P.Q) - \sum_{v\in R} contr_v(P,Q),$$

where χ the Euler characteristic of the surface, R the set of singular fibers and $contr_v(P,Q)$ the local contribution[†] of P and Q at a singular fiber v.

Proof. [19, Theorem 6.24]. □

This is particularly useful for computing height pairings between integral sections on elliptic surfaces with only type II fibers. Indeed, in that case the formula reduces to

$$\langle P, Q\rangle = \chi - (P.Q). \tag{2.4}$$

Lemma 2.5.15. *An element $P \in E(K)$ is a torsion section if and only if $\langle P, P\rangle = 0$.*

Proof. See [19, Proposition 6.31]. □

Lemma 2.5.16. *Let C be a smooth projective curve over an algebraically closed field k. Write $K = k(C)$ and let E/K be an elliptic curve. Take a collection of r points $\{P_1, \dots P_r\}$ in $E(K)$, then they are $\mathbb{Z}$-linearly independent if and only if the height-pairing matrix $(\langle P_i, P_j\rangle)_{i,j=1}^r$ has full rank.*

Proof. By Theorem 2.5.13 the height-pairing gives a well-defined structure of a positive-definite lattice on $E(K)/E(K)_{\text{tors}}$. General lattice theory then gives the result. □

Example 2.5.17. *Consider the elliptic curve $E_{360}\colon y^2 = x^3 + t^{360} + 1$ over $\bar{\mathbb{F}}_p(t)$ with $p \geq 7$. We claim that this is a torsion-free elliptic curve. To see this note that all fibers of the corresponding surface are of type* II*, so there is no local contribution (see [19, Theorem 6.24]). The Euler number is $360(1+1) = 720$ (see [19, Theorem 5.47]) and $\mathcal{K}^2_{\mathcal{E}_{360}} = 0$, as $\mathcal{K}^2_S = 0$ for any elliptic surface S (see Theorem 2.5.28). Plugging this into Noether's formula we get*

$$12\chi(\mathcal{E}_{360}) = 720,$$

hence the Euler characteristic is 60. To conclude, suppose P is a nontrivial torsion section. Via Lemma 2.5.15 and the explicit formula for the height pairing we get

$$\begin{aligned} 0 &= \langle P, P\rangle \\ &= 120 + 2(P.\mathcal{O}), \end{aligned}$$

which forces $(P.\mathcal{O}) = -60$, a contradiction as this should be nonnegative.

This example shows that most of the elliptic curves we are working with will be torsion-free. In particular, finding n independent sections is equivalent to showing the Mordell-Weil rank is at least n.

Theorem 2.5.18. *Let $f\colon S \to C$ be an elliptic surface. Then the Néron-Severi group is a torsion-free finitely generated abelian group (cf. Theorem 2.4.10).*

Proof. See [19, Theorem 6.4]. □

Theorem 2.5.19 (Shioda-Tate Formula)**.** *Let E/K be an elliptic curve. Let $\mathcal{E}$ denote the Kodaira-Néron model of E, $\rho(\mathcal{E})$ its Picard number and r the rank of the Mordell-Weil group of E/K. Then we have*

$$\rho(\mathcal{E}) = 2 + r + \sum_{v\in C}(m_v - 1),$$

where m_v denotes the number of irreducible components of the fiber of $v \in C$.

Proof. See [19, Corollary 6.7]. □

The Shioda-Tate formula is quite useful for determining ranks if we know the Picard number of our surface. There are several classes of surfaces of which we know them, but the rational elliptic surfaces are the most important to us.

[†]See [19, Def. 6.23].

Definition 2.5.20. *Let $f\colon S \to C$ be an elliptic surface. We say S is a rational elliptic surface if the surface S is rational, i.e. S is birationally equivalent to $\mathbb{P}^2$.*

Note that if $S \to C$ is a rational elliptic surface, then $C \cong \mathbb{P}^1$, see, e.g., [19, p. 145].

Lemma 2.5.21. *Let $E/k(t)$ be an elliptic curve given by a Weierstrass equation*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.5}$$

where $a_i \in k[t]$ and $\deg(a_i) \leq i$, such that considered as elliptic surface it contains a singular fiber. Then the Kodaira-Néron model $\mathcal{E}/k$ defines a rational elliptic surface.

Proof. See [19, Section 7.4]. □

By rationality and Noether's formula it follows that the Picard number of a rational elliptic surface S will always be equal to 10 (see [19, Proposition 7.1]). So for rational elliptic surfaces we have the formula

$$r = 8 - \sum_{v \in C}(m_v - 1).$$

The next example computes the type of fibers of an elliptic surface using Tate's algorithm. For an exposition see [19, Section 5.8].

Example 2.5.22. *Consider $k = \bar{\mathbb{F}}_5$ and the elliptic curve $E_1\colon y^2 = x^3 + t + 1$ over $k(t)$. This defines a rational elliptic surface, hence $\rho(\mathcal{E}_1) = 10$. The discriminant of E_1 is $\Delta = 3(t+1)^2$, so that we have a singular fiber above $t = -1$ and possibly one above infinity. We quickly see that the fiber above -1 is of type* II*. To investigate the fiber above infinity we perform a change of variables. Define $r = \frac{1}{t}$ and consider the change of variables $\alpha = r^2x$, $\beta = r^3y$. This yields the elliptic curve given by $\beta^2 = \alpha^3 + r^5 + r^6$. The order of vanishing of the discriminant of this curve at $r = 0$ is 10. Moreover, the order of vanishing of the coefficient $r^5 + r^6$ at $r = 0$ is 5. Hence at $t = \infty$ we find a singular fiber of type* II**, so it has 9 irreducible components. By Shioda-Tate there are no other reducible fibers and the rank of $E_1(k(t))$ is 0.*

The following theorem will be of importance later.

Theorem 2.5.23. *For any elliptic curve E over $K = k(t)$ defined by a minimal[†] Weierstrass equation of the form (2.5) associated with a rational elliptic surface, there are at most 240 K-rational points $P = (x, y)$ of the form*

$$x = gt^2 + at + b, \quad y = ht^3 + ct^2 + dt + e$$

with $a, ..., h \in k$ and they generate the Mordell–Weil group $E(K)$.

Proof. See [19, Theorem 8.33]. □

Definition 2.5.24. *Let $f\colon S \to C$ be an elliptic surface. We say S is an elliptic $K3$ surface if the surface S is $K3$, i.e. has trivial canonical bundle.*

As explained in [19, Section 11.2], if $S \to C$ is an elliptic $K3$ surface, then C is isomorphic to the projective line $\mathbb{P}^1$.

Lemma 2.5.25. *Let $E/k(t)$ be an elliptic curve given by a Weierstrass equation*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in k[t]$ and $\deg(a_i) \leq 2i$ with some i such that $\deg a_i \geq i$. Then the Kodaira-Néron model $\mathcal{E}/k$ defines an elliptic $K3$ surface.

Proof. See [19, Section 11.3]. □

Theorem 2.5.26. *Let $\mathcal{E}/k$ be an elliptic $K3$ surface, then the Picard number $\rho(\mathcal{E}) \leq 22$.*

Proof. The second Betti number of $\mathcal{E}$ equals 22. A result by Igusa [10] implies that $\rho(\mathcal{E})$ is bounded by the second Betti number. □

[†]Meaning that the discriminant is not a twelfth power.

Remark 2.5.27. *Elliptic K3 surfaces which have Picard number 22 are supersingular.*

Theorem 2.5.28 (Canonical Bundle)**.** *The canonical bundle of an elliptic surface $f\colon S \to C$ is given by*

$$\omega_S = f^* \left(\omega_C \otimes \mathcal{L}^{-1}\right),$$

where $\mathcal{L}$ is a certain line bundle of degree $-\chi(S)$ on C. In particular, we have

$$\mathcal{K}_S \approx (2g(C) - 2 + \chi(S))\, F,$$

for a fiber F and moreover $\mathcal{K}_S^2 = 0$.

Proof. See [19, Theorem 5.44]. □

For a rational elliptic surface $f\colon S \to \mathbb{P}^1$ this tells us that $\mathcal{K}_S \approx -F$ for a fiber F. For reference we end this section with a computation of the self intersection number of a section on an elliptic surface.

Lemma 2.5.29. *Let $f\colon S \to C$ be an elliptic surface with a section (P). Then $P^2 = (P.P) = -\chi(S)$.*

Proof. From adjunction we obtain that $2g(P) - 2 = P^2 + (C.\mathcal{K}_S)$. By Theorem 2.5.28 the right hand side equals $P^2 + 2g(C) - 2 + \chi(S)$ as $(C.F) = 1$. By construction we have $g(P) = g(C)$ and hence we find $P^2 = -\chi(S)$. □

2.6 The Zeta Function of a Variety Over a Finite Field

For certain elliptic curves we can calculate their rank via zeta functions. This section gives the required background.

Definition 2.6.1. *Let $V/\mathbb{F}_q$ be a projective variety over the finite field $\mathbb{F}_q$. The zeta function of $V/\mathbb{F}_q$ is the (formal) power series*

$$Z(V/\mathbb{F}_q; T) \coloneqq exp\left(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})| \frac{T^n}{n}\right).$$

Definition 2.6.2. *Let $V/\mathbb{F}_q$ a projective variety and denote $V_{\bar{\mathbb{F}}_q}$ for the base change to an algebraic closure of $\mathbb{F}_q$. The i^{th} Betti number is defined as*

$$b_i(V) \coloneqq \dim H^i(V_{\bar{\mathbb{F}}_q}),$$

where we use l-adic etalé cohomology.

In 1949, André Weil made a series of remarkable conjectures concerning the number of points on varieties defined over finite fields [35]. Today all of them have been proven and we state them as a theorem.

Theorem 2.6.3 (The Weil Conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N and denote $Z(V/\mathbb{F}_q; T)$ its zeta function. The following statements hold:*

- *$Z(V/\mathbb{F}_q; T) \in \mathbb{Q}(T)$;*
- *There is an integer ϵ with $Z(V/\mathbb{F}_q; 1/q^N T) = \pm q^{N\epsilon/2} T^\epsilon Z(V/\mathbb{F}_q; T)$;*
- *The zeta function factors as*

$$Z(V/\mathbb{F}_q; T) = \frac{P_1(T) \cdots P_{2N-1}(T)}{P_0(T) P_2(T) \cdots P_{2N}(T)},$$

with each $P_i(T) \in \mathbb{Z}[T]$, with $P_0(T) = 1 - T$ and $P_{2N}(T) = 1 - q^N T$ and such that for every $0 \leq i \leq 2N$ the polynomial $P_i(T)$ factors over $\mathbb{C}$ as

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T)$$

with $|\alpha_{ij}| = q^{1/2}$ and b_i the i^{th} Betti-number of V.

Proof. This was done mostly by Grothendieck, Deligne, Dwork and Weil using methods beyond what we want to focus on such as l-adic cohomology theory. For the case of elliptic curves see [25, Section V.2]. □

Note that we can obtain $|V(\mathbb{F}_{q^n})|$ from the zeta function by the formula

$$|V(\mathbb{F}_{q^n})| = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q;T)\bigg|_{T=0}. \tag{2.6}$$

In order to compute the zeta function we need to be able to count points over finite field. To do this one can use the Frobenius endomorphism. We now discuss this in the case of elliptic curves.

Definition 2.6.4. *Let $E/\mathbb{F}_q$ be an elliptic curve and let ϕ be the q^{th} power Frobenius endomorphism on E. The quantity $a := q+1-|E(\mathbb{F}_q)|$ is called the trace[†] of ϕ.*

Theorem 2.6.5. *Let $E/\mathbb{F}_q$ be an elliptic curve and let ϕ be the q^{th} power Frobenius endomorphism on E with trace a.*

(a) Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$,

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \alpha^n - \beta^n.$$

(b) The Frobenius endomorphism satisfies

$$\phi^2 - a\phi + q = 0 \quad \text{in } End(E).$$

Proof. See [25, Theorem 2.3.1]. □

Example 2.6.6. *Let $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ be a finite field with characteristic $p \neq 2, 3$. Let E_0/k be the elliptic curve given by short Weierstrass equation $E_0 \colon y^2 = x^3 + 1$. We try to determine its zeta function. Using Theorem 2.6.3 we immediately find that $Z(E_0/k;T) = \frac{P_1(T)}{(1-T)(1-qT)}$. Moreover, by [25, Section V, Theorem 2.4] we find that $P_1(T) = 1 - aT + qT^2$ with $a = q+1-|E(k)|$. It remains to determine $|E(k)|$ and in order to do so we make some case distinctions.*

- *If $p \equiv 2 \mod 3$ then $E_0/\mathbb{F}_p$ is supersingular (see [25, Section V, Example 4.4]) and from [25, Section V, Exercise 5.15] we get*

$$|E_0(\mathbb{F}_{p^n})| = \begin{cases} p^n + 1 & \text{if } n \text{ is odd} \\ \left(p^{n/2} - (-1)^{n/2}\right)^2 & \text{if } n \text{ is even.} \end{cases}$$

- *If $p \equiv 1 \mod 3$ then $E_0/\mathbb{F}_p$ is ordinary and a general formula for the number of points on E_0 is much more complicated. Denote $\mathbb{Z}[\omega]$ for the ring of Eisenstein integers. From [11, Section 18.3] we obtain that $|E_0(\mathbb{F}_p)| = p + 1 + \overline{\left(\frac{4}{\pi}\right)_6}\pi + \left(\frac{4}{\pi}\right)_6\bar{\pi}$, where $p = \pi\bar{\pi}$ is a factorisation into irreducibles in $\mathbb{Z}[\omega]$ with $\pi \equiv 2 \mod (3)$ and $(\frac{4}{\pi})_6$ denotes the sixth power residue symbol (see [11, Section 14.2]). From Theorem 2.6.5 part (a) we deduce that*

$$|E_0(\mathbb{F}_q)| = q + 1 - \left[-\overline{\left(\frac{4}{\pi}\right)_6}\pi\right]^n - \left[-\left(\frac{4}{\pi}\right)_6\bar{\pi}\right]^n,$$

from which one can deduce the zeta function $Z(E_0/k;T)$.

This is particularly useful for us when $p \equiv -1 \mod 6$, as we then find

$$Z(E_0/\mathbb{F}_p;T) = \frac{1+pT^2}{(1-T)(1-pT)}$$

and

$$Z(E_0/\mathbb{F}_{p^2};T) = \frac{(pT+1)^2}{(1-T)(1-p^2T)}.$$

[†]This terminology stems from the fact that ϕ can be seen as a linear transformation on a vector space called the Tate-module (see [25, Section III.7]).

The characteristic $p \equiv 1 \mod 3$ case can be done without appealing to [11, Section 18.3]. Consider the elliptic curve $E\colon y^2 = x^3 + 1$ over $\mathbb{F}_p$. We know that E is ordinary in this case and $\mathrm{End}(E) = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$. We fix the above isomorphism via $\omega \cdot (x, y) \coloneqq (\omega x, y)$ and denote π the Frobenius endomorphism $\mathrm{Frob}_p\colon E \to E$ sending $(x, y) \mapsto (x^p, y^p)$. We would like to find an expression for the Frobenius endomorphism in terms of the Euclidean domain $\mathbb{Z}[\omega]$. To do so write $\pi = a + b\omega$ and note that $\deg(\pi) = p$. In $\mathbb{Z}[\omega]$ this translates to $N(\pi) = p$, where $N(a + b\omega) = a^2 - ab + b^2$.

Note that the subgroup $\langle (0, \pm 1) \rangle \subset E(\mathbb{F}_p)$ is precisely the kernel of $\omega - 1$ and similarly the kernel of 2 is precisely the subgroup of $E(\mathbb{F}_p)$ generated by points of the form $(\star, 0)$. Combining this we find that $\ker(2\omega - 2) = \langle (0, \pm 1), (\star, 0) \rangle$ is a group of $\deg(2) \cdot \deg(\omega - 1) = 12$ elements. A quick inspection of the elements shows this group is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Moreover, we note that π restricted to $\ker(2\omega - 2)$ equals the identity. In other words $\ker(2\omega - 2) \subset E(\mathbb{F}_p) = \ker(\pi - 1)$. This condition means that $(2\omega - 2) | (\pi - 1)$ in $\mathbb{Z}[\omega]$ or equivalently $\pi \equiv 1 \mod (2\omega - 2)$.

The elements 2 and $\omega - 1$ satisfy the relation $2 \cdot 2 + (\omega - 1) \cdot (2 + \omega) = 1$, hence are coprime. By the Chinese remainder theorem we get that $\mathbb{Z}[\omega]/(2\omega - 2) \cong \mathbb{Z}[\omega]/(2) \times \mathbb{Z}[\omega]/(\omega - 1) \cong \mathbb{F}_4 \times \mathbb{F}_3$. The condition $\pi \equiv 1 \mod (2\omega - 2)$ is then equivalent with π getting mapped to $(\bar{1}, \bar{1}) \in \mathbb{F}_4 \times \mathbb{F}_3$. The latter condition precisely tells us that $a \equiv 1 \mod 2$, $b \equiv 0 \mod 2$ and $a + b \equiv 1 \mod 3$. We claim that these properties for π are enough to determine its trace.

Indeed, the trace of π equals

$$\mathrm{Tr}(\pi) = \pi + \bar{\pi} = 2a - b,$$

which is clearly invariant under complex conjugation. Moreover, there are only 12 elements of norm p in $\mathbb{Z}[\omega]$. If η is such an element, then $u\eta$ with u a unit and $\bar{\eta}$ are as well. The units in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm(1 + \omega)$, hence if $\pi = a + b\omega$ satisfies $a \equiv 1 \mod 2$, $b \equiv 0 \mod 2$ and $a + b \equiv 1 \mod 3$, then $u\pi$ does not. In particular, only complex conjugation preserves these relations which is precisely what we wanted.

The above gives us a quick way for computing the number of points in $E(\mathbb{F}_p)$. To see this take the prime $p = 7$. The element $-3 - 2\omega$ is precisely of our desired form and its trace is -4. The formula

$$|E(\mathbb{F}_p)| = p + 1 - \mathrm{Tr}\left(\mathrm{Frob}_p\right)$$

then yields that $|E(\mathbb{F}_7)| = 7 + 1 + 4 = 12$. Part (a) of Theorem 2.6.5 then allows us to compute the zeta function completely.

2.7 Chebotarev's Density Theorem

This section is based on [14]. Throughout denote K a number field, i.e. a finite field extension of $\mathbb{Q}$. Let L be a finite Galois extension of K with Galois group denoted by G. Let $\mathfrak{p}$ be a prime of K (so a prime ideal of $\mathcal{O}_K$) and let $\mathfrak{P}$ be any prime of L lying above $\mathfrak{p}$.

Definition 2.7.1. *The Artin symbol* $\left[\frac{L/K}{\mathfrak{P}}\right]$ *is the unique element* $\sigma \in G$ *so that*

$$\sigma(\alpha) = \alpha^{nm(\mathfrak{p})} \mod \mathfrak{P}$$

for all $\alpha \in L$*, where* $nm(\mathfrak{p})$ *denotes the norm of* $\mathfrak{p}$*.*

Note that for any prime $\mathfrak{p}$, all the primes $\mathfrak{P}$ lying above $\mathfrak{p}$ are isomorphic via elements of G. Hence the values of the Artin symbol $\left[\frac{L/K}{\mathfrak{P}}\right]$ lying over $\mathfrak{p}$ are all conjugate in G. We write $\left[\frac{L/K}{\mathfrak{p}}\right]$ for this conjugacy class.

Remark 2.7.2. *If* L/K *is an abelian extension we abuse the notation and write* $\left[\frac{L/K}{\mathfrak{p}}\right]$ *for the unique element in* G*.*

Definition 2.7.3. *Let* S *be a subset of* $P(K)$*, the set of all primes of* K*. The Dirichlet density of* S *is defined as*

$$\lim_{s \to 1^+} \left(\sum_{\mathfrak{p} \in S} \frac{1}{\#\left(\mathcal{O}_K/\mathfrak{p}\right)^s} \right) \left(\sum_{\mathfrak{p} \in P(K)} \frac{1}{\#\left(\mathcal{O}_K/\mathfrak{p}\right)^s} \right)^{-1}$$

if it exists.

Theorem 2.7.4 (Chebotarev's Density Theorem)**.** *Let L/K be a finite Galois extension of number fields and let $\mathcal{C}$ be a conjugacy class of $Gal(L/K) = G$. Let*

$$P_{\mathcal{C}} \coloneqq \left\{ \mathfrak{p} \in P(K) \colon \mathfrak{p} \text{ is unramified in } L, \left[\frac{L/K}{\mathfrak{p}}\right] = \mathcal{C} \right\}$$

Then, the Dirichlet density of $P_{\mathcal{C}}$ in $\{\mathfrak{p} \in P(K) \colon \mathfrak{p}$ is unramified in $L\}$ exists and is equal to

$$\frac{\#\mathcal{C}}{\#G}.$$

It is hard to underestimate the usefulness of Chebotarev's density theorem in modern (algebraic) number theory. It is particularly useful for showing that certain subsets of the set of prime numbers have a positive density, which implies (but is not equivalent to) the statement that the set has infinite cardinality. The next statement is a corollary of Chebotarev's density theorem.

Corollary 2.7.5. *Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial and denote $\mathcal{P}$ for the set of prime numbers. Then the set*

$$\mathcal{L} = \{p \in \mathcal{P} \colon f \text{ splits completely modulo } p\}$$

has infinite cardinality.

Proof. Let L be the splitting field of f with $[L \colon \mathbb{Q}] = n$. Chebotarev's density theorem implies that the Dirichlet density of the rational primes that split completely in L equals $1/n$ (see [18, Corollary 13.6]). In particular, there are infinitely many rational primes that split completely in L. By the theorem of the primitive element we write $L = \mathbb{Q}(\alpha)$ with $g \in \mathbb{Z}[x]$ the minimal polynomial of α. Up to finitely many exceptions we know that a rational prime p splits completely in L if and only if g splits completely modulo p. It is clear that when g splits completely modulo p, f also splits completely modulo p. □

Corollary 2.7.6. *Let $f_1, \ldots, f_n \in \mathbb{Z}[x]$ be nonconstant polynomials. Then the set*

$$\{p \in \mathcal{P} \colon f_1, \ldots, f_n \text{ have a root modulo } p\}$$

has infinite cardinality.

Proof. Write $f \coloneqq f_1 f_2 \cdots f_n$ and note that according to Corollary 2.7.5 there are infinitely many primes p so that f splits completely modulo p. In particular, for such primes p each of the polynomials f_i has a root modulo p. □

3 The Set-Up

Now that we have the tools available it is time to make precise what we will do. Consider the elliptic curve

$$E_{360} \colon y^2 = x^3 + t^{360} + 1 \tag{3.1}$$

over the field $\mathbb{Q}(t)$. It has discriminant $\Delta = -1728(t^{360} + 1)^2$ and all fibers of the corresponding surface are of type II. Moreover, for any prime $p > 5$ the elliptic surface corresponding to $E_{360}/\mathbb{F}_p(t)$ has only type II fibers as well. In particular, we have good reduction for all rational primes $p > 5$. Throughout this section let p be a prime of good reduction and denote $E_{360}^{\bar{\mathbb{Q}}}$ for the elliptic curve $E_{360}/\bar{\mathbb{Q}}(t)$ and $E_{360}^{\bar{\mathbb{F}}_p}$ for the elliptic curve $E_{360}/\bar{\mathbb{F}}_p(t)$. Recall that the Mordell-Weil rank of $E_{360}^{\bar{\mathbb{Q}}}$ is 68 and that there is a finite field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ of smallest degree so that

$$\operatorname{rank} E_{360}(\mathbb{Q}(\alpha, t)) = 68.$$

We first show that the rank over $\mathbb{Q}(t)$ is bounded by 34.

Lemma 3.0.1. *The rank of $E_{360}/\mathbb{Q}(t)$ is bounded by* 34.

Proof. We have

$$r(E_{360}(\mathbb{Q}(t)))/2 = r(E_{360}(\mathbb{Q}(\sqrt{-3}, t))) \leq r(E_{360}(\bar{\mathbb{Q}}(t))) = 68$$

where the first equality follows from Corollary 2.3.13. □

Definition 3.0.2 (Reduction Modulo a Rational Prime of Good Reduction)**.** *One way to define reduction modulo a rational prime of good reduction is as follows: denote $K = \mathbb{Q}(\alpha)$ with ring of integers $\mathcal{O}_K$. Let $P = (X : Y : Z)$ be a point of E_{360} with $X, Y, Z \in \mathbb{Q}(\alpha, t)$ written in homogeneous coordinates. Multiplying through by a suitable polynomial we can view the coordinates as polynomials in t with coefficients in $\mathbb{Q}(\alpha)$. Reduction modulo p is then defined as reducing the coefficients modulo a prime $\mathfrak{p}$ of K over p, which is done via discrete valuations (see [25, Section VII.1–3] for a complete overview).*

If p is such that the minimal polynomial of α over $\mathbb{Q}$, denoted by $\min_\alpha^{\mathbb{Q}}$, has a root modulo p, then after a reduction modulo p we end up in the field $\mathbb{F}_p(t)$. In general we end up in a field of the form $\mathbb{F}_{p^n}(t)$ for some integer $n > 0$. We remark that, due to Chebotarev's density theorem, there are infinitely many primes so that $\min_\alpha^{\mathbb{Q}}$ has a root modulo p. It is precisely these primes we are looking for.

The next result shows that we do not have to worry about independent sections becoming dependent after a reduction modulo p.

Theorem 3.0.3. *Let $p > 5$ be any prime (so not necessarily with the property that $min_\alpha^{\mathbb{Q}}$ has a root mod p). We have the following injection of finite dimensional $\mathbb{Q}_l$-vector spaces:*

$$NS(\mathcal{E}_{360}^{\bar{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow NS(\mathcal{E}_{360}^{\bar{\mathbb{F}}_p}) \otimes_{\mathbb{Z}} \mathbb{Q}_l, \tag{3.2}$$

where $\mathbb{Q}_l$ denotes the the l-adic rational numbers with $l \neq p$. In particular, since the given Néron-Severi groups are torsion-free, reduction modulo p defines an injection on $NS(\mathcal{E}_{360}^{\bar{\mathbb{Q}}})$.

Proof. See [34, Proposition 2.6.2] for the injection (3.2). □

Note that $E_{360}(\bar{\mathbb{Q}}(t))$ is torsion-free (cf. Example 2.5.17). Let $P, Q \in E_{360}(\bar{\mathbb{Q}}(t))$ be two independent points and denote their reduction modulo p (in $E_{360}(\bar{\mathbb{F}}_p(t))$) by $\tilde{P}$ and $\tilde{Q}$. Following [19, Section 6] we see that

$$\mathrm{NS}(\mathcal{E}_{360}^{\bar{\mathbb{Q}}}) = L_{\bar{\mathbb{Q}}}^- \oplus \mathrm{Triv}(\mathcal{E}_{360}^{\bar{\mathbb{Q}}}),$$

where $L_{\bar{\mathbb{Q}}}^-$ denotes the essential sublattice and $\mathrm{Triv}(\mathcal{E}_{360}^{\bar{\mathbb{Q}}})$ the trivial sublattice. As $E_{360}(\bar{\mathbb{Q}}(t))$ is torsion-free we have

$$E_{360}(\bar{\mathbb{Q}}(t)) \subset L_{\bar{\mathbb{Q}}}^-.$$

Combining this with the injection from (3.2) it follows that $\tilde{P}$ and $\tilde{Q}$ remain independent points. In particular, once p is such that $\mathrm{rank}(E_{360}(\mathbb{F}_p(t)) = \mathrm{rank}(E_{360}(\bar{\mathbb{F}}_p(t)) = 68$ we know that, up to finite index, all sections over $\mathbb{F}_p$ are obtained via a reduction modulo p from the characteristic zero case. By Chebotarev's density theorem there exists infinitely many such primes and in this thesis we have found several such prime numbers p.

Example 3.0.4 (Generation up to finite index)**.** *An example (albeit not for the elliptic curve E_{360}) where a section modulo p generates a smaller index subgroup is as follows.*

Fix the field $k = \mathbb{Q}(t)$ and consider the elliptic curves $E' \colon y^2 = x^3 - 4ax$, and $E \colon y^2 = x^3 + ax$ both over k. These are related via the usual 2-isogenies $\phi \colon E \to E'$ and $\phi' \colon E' \to E$ (see [25, Proposition X.4.9]), which satisfy $\phi \circ \phi' = [2]$ multiplication by 2 on E'. We look for a point that is not divisible by 2 over k, but is divisible by 2 over $\mathbb{F}_p(t)$ for some prime of good reduction. Any element divisible by 2 on E' has to lie in the image of ϕ. Now $(0,0) \neq (\xi, \eta) \in E'(k)$ lies in the image of ϕ if and only if ξ is a square. Suppose $\xi = t^2$, then $\eta^2 = t^6 - 4at^2$ and hence $a \coloneqq 2t^2 - 4$ yields $\eta = 4t - t^3$. Now consider the elliptic curve given by

$$E' \colon y^2 = x^3 - 4(2t^2 - 4)x$$

over $\bar{\mathbb{Q}}(t)$. This defines a rational elliptic surface with two fibers of type III *and one fiber of type* I_0^**. The Shioda-Tate formula implies that $E'(\bar{\mathbb{Q}}(t))$ has rank 2. This Mordell-Weil group has a natural structure of an $\mathbb{Z}[i]$-module induced from the automorphism $\sigma(x, y) = (-x, iy)$. In particular, the rank over $\mathbb{Q}(t)$ can only be 0 or 1. The section $P = (t^2, -t^3 + 4t)$ is completely defined over $\mathbb{Q}$ and is of infinite order, hence $E'(\mathbb{Q}(t))$ has rank 1. Suppose that there would exist a section $Q \in E'(\mathbb{Q}(t))$ so that $[2]Q = P$. Then the x-coordinate $x([2]Q) = t^2$ and using the duplication formula for elliptic curves we see that this is not possible over $\mathbb{Q}(t)$. In particular, P is not divisible by 2 in $E'(\mathbb{Q}(t))$. However, after a reduction modulo 7 we find that $\tilde{P} \coloneqq P \mod 7 = (t^2, 6t^3 + 4t) = [2](t + 4, t + 4)$. I.e. $\tilde{P}$ is divisible by 2 in $E'(\mathbb{F}_7(t))$ and we conclude that the subgroup generated by $\tilde{P}$ generates a smaller index subgroup in $E'(\mathbb{F}_7(t))$ than the subgroup generated by P does in $E'(\mathbb{Q}(t))$.*

Remark 3.0.5. *The map in Theorem 3.0.3 is only an injection. Indeed, we will see that for the prime number $p = 359$ the Mordell-Weil rank of $E_{360}/\mathbb{F}_p(t)$ equals 358. So in positive characteristic more independent sections can arise.*

We end this section by stating some more properties of primes of good reduction. Note that by the Lefschetz principle we can consider $E_{360}^{\mathbb{C}} \coloneqq E_{360}/\mathbb{C}(t)$ instead of $E_{360}/\bar{\mathbb{Q}}(t)$.

Theorem 3.0.6. *The Betti numbers do not change under reduction modulo p, i.e.*

$$b_i\left(\mathcal{E}_{360}^{\mathbb{C}}\right) = b_i\left(\mathcal{E}_{360}^{\bar{\mathbb{F}}_p}\right),$$

where the left-hand side is computed via singular cohomology and the right-hand side using l-adic etalé cohomology.

Proof. The Betti numbers are independent of chosen cohomology theory ([8, Appendix C, Section 3]). The fact that the Betti numbers do not change after a reduction modulo p is a corollary from the Weil conjectures (see [8, Appendix C, Section 1]). □

The above allows us to compute the Betti numbers of $\mathcal{E}_{360}$ using singular cohomology even in characteristic $p > 5$.

We are now finally ready to rigorously state what we will do. Consider the elliptic curve $E_{360}/\bar{\mathbb{Q}}(t)$, which has Mordell-Weil rank 68. We want to find a prime number $p > 5$ so that all these sections are defined over $\mathbb{F}_p$ after a reduction modulo p (they automatically remain independent after reduction modulo a prime $p > 5$). By the above discussion it suffices to find primes $p > 5$ so that

$$\operatorname{rank} E_{360}(\mathbb{F}_p(t)) = \operatorname{rank} E_{360}(\bar{\mathbb{F}}_p(t)) = 68.$$

In the upcoming sections we find such prime numbers.

4 A Toy Example

This section demonstrates the method used to show that $E_{360}/\mathbb{F}_{359}(t)$ has Mordell-Weil rank 358. Consider the elliptic curve $E_1 \colon y^2 = x^3 + t + 1$ over the field $k(t)$ where k is a field not of characteristic 2 nor 3.

Proposition 4.0.1. *The Mordell-Weil group $E_1(k(t))$ is trivial.*

Proof. Without loss of generality we may assume that k contains a primitive sixth root of unity ζ_6. Indeed, if it does not contain a primitive sixth root of unity, we get $E_1(k(t)) \subseteq E_1(L(t))$ with $L = k(\zeta_6)$. If $E_1(L(t)) = 0$, then so is $E_1(k(t))$. Therefore, suppose k contains a primitive sixth root of unity.

Consider the smooth projective algebraic curve C/k defined by an affine equation $C \colon s^6 = t + 1$. The function field of C is given by $k(C) = k(s,t) = k(s)$, as $t = s^6 - 1$. This immediately tells us that C is birationally equivalent to the projective line and hence has genus 0. Over the field extension $k(s) \supset k(t)$ we see that $E_1 \colon y^2 = x^3 + s^6$, which is isomorphic to the elliptic curve $E_0 \colon \eta^2 = \xi^3 + 1$ via the change of variables $\eta = \frac{y}{s^3}$, $\xi = \frac{x}{s^2}$. This curve can also be seen as an elliptic curve over the base field k and we call this curve $\tilde{E}$. We have the relation $E_0 = \tilde{E} \times_k k(s)$, where $\times_k$ denotes the fiber product of k-schemes. In order to continue we first need a lemma.

Lemma 4.0.2. *We have*

$$E_1(k(t)) \subset E_0(k(s)) \cong Mor_k(C, \tilde{E}),$$

where $Mor_k(C, \tilde{E})$ denotes the set of k-morphisms from C to $\tilde{E}$ (which is a group as $\tilde{E}$ is a group variety).

Proof. The first inclusion is clear as $k(t) \subset k(s)$ and $E_1 \cong E_0$ over $k(s)$. In order to prove the isomorphism we first take a point $P = (a(s), b(s)) \in E_0(k(s))$. Associated to this point is the k-morphism $\phi_P \colon C \to \tilde{E}$ given by $(s,t) \mapsto (a(s), b(s))$. Conversely, any k-morphism $\gamma \colon C \to \tilde{E}$ can be written as $\gamma(s,t) = (\gamma_1(s), \gamma_2(s))$, as s determines t completely. This gives rise to the point $P_\gamma = (\gamma_1(s), \gamma_2(s)) \in E_0(k(s))$. This establishes a bijection, which is obviously compatible with the group structures. □

We ask the question: which morphisms correspond to the points in $E_1(k(t))$? The next lemma gives the answer.

Lemma 4.0.3. *The points in $E_1(k(t))$ correspond precisely to the k-morphisms $\gamma\colon C \to \tilde{E}$ so that*

$$\begin{array}{ccc} C & \xrightarrow{\gamma} & \tilde{E} \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\delta} \\ C & \xrightarrow{\gamma} & \tilde{E} \end{array}$$

is a commutative diagram, where $\rho(s,t) = (\zeta_6 s, t)$ and $\delta(\xi,\eta) = (\zeta_6^4\xi, -\eta)$ are both k-automorphisms of order 6 on their respective curves.

Proof. Any point $P = (x(t), y(t)) \in E_1(k(t))$ yields a k-morphism $\gamma_P\colon C \to \tilde{E}$ given by $\gamma(s,t) = (\frac{x(t)}{s^2}, \frac{y(t)}{s^3})$. It is straightforward to check that the diagram commutes.

Conversely, a k-morphism $\gamma(s,t) = (\gamma_1(s,t), \gamma_2(s,t))$ yields a point $P_\gamma = (s^2\gamma_1(s,t), s^3\gamma_2(s,t)) \in E_1(k(s))$. We will use some Galois theory to show this point lies in $E_1(k(t))$. First of all, note that the curve C is irreducible. Moreover, as $\mathrm{char}(k) \neq 2, 3$ we find that $k(s) \supset k(t)$ is a separable algebraic extension and as k contains a primitive 6^{th} root of unity it is also normal. Therefore, $k(s) \supset k(t)$ is a degree 6 Galois extension with Galois group G generated by $\sigma\colon k(s) \to k(s)$ sending $s \mapsto \zeta_6 s$ and $t \mapsto t$.

The fact that γ makes the diagram commute implies that $\gamma_1(\zeta_6 s, t) = \zeta_6^4\gamma_1(s,t)$ and $\gamma_2(\zeta_6 s, t) = -\gamma_2(s,t)$. Using this when applying σ pointwise on P_γ we find that the Galois group G fixes P_γ, so that $P_\gamma \in E_1(k(t))$. □

We are now ready to prove Proposition 4.0.1. Any point $P \in E_1(k(t))$ corresponds to a k-morphism $\gamma\colon C \to \tilde{E}$ so that our diagram commutes. As C is birationally equivalent to the projective line it has genus 0, which implies that γ is a constant morphism. Say that $\gamma(s,t) = Q$, then $\delta(Q) = Q$ and as δ is a degree 1 map this forces Q to be the point at infinity. This means that there is only one such morphism γ and we deduce that the group $E_1(k(t))$ is trivial. □

The above procedure generalizes and will be fruitful later on. However, we would also like to indicate an alternative approach using the theory of elliptic surfaces. In order to do this we consider again the elliptic curve $E_1\colon y^2 = x^3 + t + 1$, but now over the field $\bar{k}(t)$ (cf. Example 2.5.22). This defines a rational elliptic surface $\mathcal{E}/\bar{k}$ (the Kodaira-Néron model) with a singular fiber at $t = -1$ and possibly at $t = \infty$. Using Tate's algorithm (see [19, Section 5.8]) we find for $t = -1$ a fiber of type II, which has 1 irreducible component. For the fiber at infinity we need to do more work. Define $r = \frac{1}{t}$ and consider the change of variables $\alpha = r^2 x$, $\beta = r^3 y$. This yields the elliptic curve given by $\beta^2 = \alpha^3 + r^5 + r^6$. The order of vanishing of the discriminant of this curve at $r = 0$ is 10. Moreover, the order of vanishing of the coefficient $r^5 + r^6$ at $r = 0$ is 5. Hence at $t = \infty$ we find a singular fiber of type II*, so it has 9 irreducible components. The Shioda-Tate formula yields $r(E_1(\bar{k}(t))) = 8 - 8 = 0$, which also implies that $r(E_1(k(t))) = 0$. It remains to show that there is no torsion. However, this is easy as both fibers have no local contribution (cf. Example 2.5.17). We conclude that the group $E_1(\bar{k}(t))$ is trivial, which gives another proof of Proposition 4.0.1.

Both of these methods are useful for determining the rank of elliptic curves of the form

$$E_n\colon y^2 = x^3 + t^n + 1$$

over $\mathbb{F}_p(t)$.

5 Methods for Finding (Bounds on) Ranks

In this section we outline several methods of computing ranks and specific points on the elliptic curve $E_n/\mathbb{F}_p(t)$.

5.1 Morphisms and Rational Points

Let $k = \mathbb{F}_q = \mathbb{F}_{p^m}$ be a finite field and let C be a smooth, projective, geometrically irreducible curve over k. Denote $K \coloneqq k(C)$ the function field of the curve C and suppose $P_0 \in C(k)$. We adopt the following standard terminology; see for example Ulmer [33].

Definition 5.1.1. *Let E be an elliptic curve over K.*

(1) We say E is constant if there is an elliptic curve $\bar{E}$ defined over k such that $E \cong \bar{E} \times_k K$. Equivalently, E is constant if it can be defined by a Weierstrass equation with coefficients in k.

(2) We say E is isotrivial if there exists a finite extension K' of K such that E becomes constant over K'. Note that a constant curve is isotrivial.

(3) We say E is non-isotrivial if it is not isotrivial. We say E is non-constant if it is not constant.

The isotrivial case is the most interesting to us as we have already seen in Section 4. Indeed, the following theorem generalizes the statements seen in Section 4.

Theorem 5.1.2. *Suppose $\bar{E}$ is an elliptic curve over k and let $E = \bar{E} \times_k K$. We have a canonical isomorphism*

$$E(K) \cong Mor_k(C, \bar{E}),$$

where Mor_k denotes morphisms of varieties over k. Under this isomorphism, $E(K)_{tor}$ corresponds to the subset of constant morphisms.

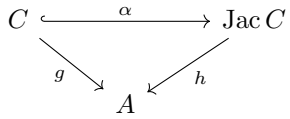
Proof. (From [33, Lecture 1, Section 6].) Note that from the scheme theoretic point of view the set $E(K)$ corresponds precisely to the set of K-morphisms $\mathrm{Spec}(K) \to E$. By the universal property of the fiber product these are in bijection with the set of k-morphisms $\mathrm{Spec}(K) \to \bar{E}$. By assumption the curve C is smooth, hence such a k-morphism extends uniquely to a k-morphism $C \to \bar{E}$. This gives a map from $E(K)$ to $\mathrm{Mor}_k(C, \bar{E})$. If $\eta\colon \mathrm{Spec}(K) \to C$ denotes the canonical inclusion, composition with η ($\phi \mapsto \phi \circ \eta$) induces a map $\mathrm{Mor}_k(C, \bar{E}) \to E(K)$ inverse to the map above. This establishes the desired bijection and this bijection is obviously compatible with the group structures.

Since k is finite, it is clear that a constant morphism goes over to a torsion point. Conversely, if $P \in E(K)$ is torsion, say of order n, then the image of the corresponding $\phi\colon C \to \bar{E}$ must lie in the set of n-torsion points of $\bar{E}$, a discrete set, and this implies that ϕ is constant. □

Corollary 5.1.3. *Suppose C has genus $g(C) \geq 1$, then*

$$rank\, E(K) = rank\, Hom_k(Jac\, C, \bar{E}).$$

Proof. We repeat the Albanese property of the Jacobian of C (see Theorem 2.2.4). Denote $\alpha : C \hookrightarrow \mathrm{Jac}\, C$ the canonical inclusion. For every abelian variety A/k and every k-morphism $g\colon C \to A$ there exists a unique k-morphism $h\colon \mathrm{Jac}\, C \to A$ which is up to translation a homomorphism of groups, so that the diagram



commutes. Taking $\bar{E}/k$ for A/k we obtain that $\mathrm{Mor}_k(C, \bar{E}) \cong \mathrm{Mor}_k(\mathrm{Jac}\, C, \bar{E})$. As the k-morphism h above is, up to translation, a homomorphism of groups we get a surjective map

$$\mathrm{Mor}_k(C, \bar{E}) \twoheadrightarrow \mathrm{Hom}_k(\mathrm{Jac}\, C, \bar{E}),$$

with kernel precisely the constant k-morphisms. In other words

$$E(K)/E(K)_{\mathrm{tor}} \cong \mathrm{Hom}_k(\mathrm{Jac}\, C, \bar{E})$$

and the result follows. □

The rank of this latter expression can be determined via the characteristic polynomial of the Frobenius endomorphism. Indeed, this is precisely the next theorem due to Tate (see [29, Theorem 1]).

Theorem 5.1.4. *Let A and B be abelian varieties over a finite field k, and let f_A and f_B be the characteristic polynomials of their Frobenius endomorphisms relative to k. Then*

$$rank\, Hom_k(A, B) = r\,(f_A, f_B),$$

where $r\,(f_A, f_B)$ is defined as follows. Factor $f_A = \prod P^{a(P)}$ and $f_B = \prod P^{b(P)}$ into a product of irreducibles, then

$$r\,(f_A, f_B) = \sum_P a(P)b(P)\deg(P).$$

Remark 5.1.5. *The above is a corollary of the "Tate conjecture for abelian varieties over finite fields".*

Suppose now that $g(C) \geq 1$ and denote χ_C for the characteristic polynomial of the q^{th} power Frobenius endomorphism on $\operatorname{Jac} C$. The following gives a relation between χ_C and the numerator of the zeta function (see Definition 2.6.1) of the curve C. To ease up notation we write $L_C(T)$ for the numerator of the zeta function of C and we refer to it as the L-polynomial of C.

Lemma 5.1.6. *Suppose we are in the set-up above. Then we have*

$$L_C(T) = T^{2g}\chi_C(1/T).$$

Proof. See [4, Proposition 8.4]. □

The next theorem illustrates some of the properties of the polynomial $L_C(T)$.

Theorem 5.1.7. *Let C by a smooth projective geometrically irreducible curve of genus $g \geq 1$ defined over $\mathbb{F}_q$. Denote $L_C(T)$ for the L-polynomial of C. Then*

(i) *L_C is of the form*

$$L_C(T) = a_0 + a_1T + \cdots + a_{2g}T^{2g},$$

with $a_i \in \mathbb{Z}$ for $0 \leq i \leq 2g$;

(ii) *$a_0 = 1$, $a_{2g} = q^g$ and $a_{2g-i} = q^{g-i}a_i$ for $0 \leq i \leq g$;*

(iii) *L_C factors over $\mathbb{C}$ as*

$$L_C(T) = \prod_{i=1}^{2g}(1 - \alpha_i T),$$

where we can arrange the α_i so that $\alpha_{g+i}\alpha_i = q$ for all $1 \leq i \leq g$.

If we denote for any integer $r \geq 1$, $N_r := |C(\mathbb{F}_{q^r})|$ and $S_r := N_r - (q^r + 1)$, then we also have

(iv) *$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$;*

(v) *Lastly, for $1 \leq i \leq q$ we have*

$$ia_i = S_i a_0 + S_{i-1}a_1 + \cdots + S_1 a_{i-1}.$$

Proof. See [27, Section 5.1]. □

By the last property one sees that from the first g numbers $N_1, \ldots, N_g$ of points on the curve one can obtain the whole L-polynomial and hence the whole characteristic polynomial of Frobenius.

Example 5.1.8. *Let $k = \mathbb{F}_7$ and consider the hyperelliptic curve $C\colon s^6 = t^2 + 1$ of genus 2 and the elliptic curve $E_0\colon y^2 = x^3 + 1$ both over k. We try to determine $\operatorname{rank} \operatorname{Hom}_k(\operatorname{Jac} C, E_0)$ from the L-polynomials of C and E_0. The L-polynomial of E_0, denoted by $L_{E_0}(T)$, is $1 - aT + 7T^2$ with $a = 8 - |E_0(k)|$ (cf. Example 2.6.6). A quick calculation reveals that $|E_0(k)| = 12$, so that $L_{E_0}(T) = 1 + 4T + 7T^2$. It remains to find the L-polynomial of C. Using Magma we find $|C(k)| = 8$ and $|C(\mathbb{F}_{49})| = 46$, hence $S_1 = 0$ and $S_2 = -4$ so that we find*

$$L_C(T) = 49T^4 - 2T^2 + 1.$$

From Lemma 5.1.6 we deduce that $\chi_C = T^4 - 2T^2 + 49 = (T^2 + 4T + 7)(T^2 - 4T + 7)$ and that $\chi_{E_0} = T^2 + 4T + 7$. By Theorem 5.1.4 we conclude that

$$\operatorname{rank} \operatorname{Hom}_k(\operatorname{Jac} C, E_0) = 2.$$

In particular, this shows that we have $r\left(E_2(\mathbb{F}_7(t))\right) \leq r\left(E_2(\mathbb{F}_7(C))\right) = 2$.

Theorem 5.1.4 phrased in terms of zeta functions will be used to compute the rank of $E_{p+1}(\mathbb{F}_p(t))$ for primes congruent to 5 modulo 6.

5.2 Morphisms and Rational Points on Certain Curves

We want to generalize the methods developed in the proof of Proposition 4.0.1 in order to apply them to elliptic curves of the form $E_n\colon y^2 = x^3 + t^n + 1$. So let k be a finite field containing a primitive 6^{th} root of unity ζ_6 and define the elliptic curve $E_f\colon y^2 = x^3 + f(t)$ over $k(t)$, where $f(t)$ is so that the smooth projective algebraic curve C given by affine equation $s^6 = f(t)$ is geometrically irreducible. Then the field extension $k(C) \supset k(t)$ is a degree 6 Galois extension with Galois group generated by $\sigma\colon k(C) \to k(C)$ sending $s \mapsto \zeta_6 s$ and $t \mapsto t$.

We repeat the exact same procedure as in Section 4. Over $k(C)$ the curve $E_f\colon y^2 = x^3 + s^6$ is isomorphic to the elliptic curve $E_0\colon \eta^2 = \xi^3 + 1$. We have the relation $E_0 = \tilde{E} \times_k k(C)$, where $\tilde{E}\colon \eta^2 = \xi^3 + 1$ is defined over k. We remark that the curve E_0 is often called a sextic twist of E_f, as they become isomorphic over a degree 6 extension. From Theorem 5.1.2 we immediately deduce that $E_f(k(t)) \subset E_0(k(C)) \cong \mathrm{Mor}_k(C, \tilde{E})$ and that the constant morphisms corresponds precisely to $E_0(k(C))_{\text{tor}}$.

In this case there is also a description of the $k(t)$-rational points on E_f.

Lemma 5.2.1. *The points in $E_f(k(t))$ correspond precisely to the k-morphisms $\gamma\colon C \to \tilde{E}$ so that*

$$\begin{array}{ccc} C & \xrightarrow{\gamma} & \tilde{E} \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\delta} \\ C & \xrightarrow{\gamma} & \tilde{E} \end{array}$$

is a commutative diagram, where $\rho(s,t) = (\zeta_6 s, t)$ and $\delta(\xi, \eta) = (\zeta_6^4 \xi, -\eta)$ are both k-automorphisms of order 6 on their respective curves.

Proof. The proof of Lemma 4.0.3 essentially carries over, but for completeness we repeat it here in a general context. Take a point $P := (x(t), y(t)) \in E_f(k(t))$, this gives a morphism $\gamma_P\colon C \to \tilde{E}$ via $(s,t) \mapsto \left(\frac{x(t)}{s^2}, \frac{y(t)}{s^3}\right)$. We compute

$$(s,t) \overset{\rho}{\mapsto} (\zeta_6 s, t) \overset{\gamma}{\mapsto} (\zeta_6^4 x(t)/s^2, -y(t)/s^3)$$

and

$$(s,t) \overset{\gamma}{\mapsto} (x(t)/s^2, y(t)/s^3) \overset{\delta}{\mapsto} (\zeta_6^4 x(t)/s^2, -y(t)/s^3),$$

so that the diagram indeed commutes.

Conversely, take any k-morphism $\gamma\colon C \to \tilde{E}$ and write it as $\gamma(s,t) = (\gamma_1(s,t), \gamma_2(s,t))$. This gives the point $P_\gamma = \left(s^2\gamma_1(s,t), s^3\gamma_2(s,t)\right) \in E_f(k(C))$. The exact same argument as in the proof of Lemma 4.0.3 yields the result. □

In the next example we apply this procedure to find a lower bound for the rank of the elliptic curve $E_2\colon y^2 = x^3 + t^2 + 1$ over $\mathbb{F}_p(t)$ with $p \equiv 1 \mod 6$.

Example 5.2.2 (The Elliptic Curve E_2)**.** *Fix a prime p congruent to 1 modulo 6 and set $k = \mathbb{F}_p$, then k contains a primitive sixth root of unity. We try to determine the rank of $E_2(k(t))$. As t^2+1 is not a perfect square nor a cube in $k(t)$ and $C\colon s^6 = t^2+1$ defines an irreducible hyperelliptic curve of genus 2, we are precisely in the required set up. Via quotients of algebraic curves by automorphisms we find two independent k-morphisms so that the diagram commutes, namely $\gamma_1(s,t) = (\zeta_6/s^2, -t/s^3)$ and $\gamma_1'(s,t) = (-1/s^2, -t/s^3)$. To see this note that we have an automorphism on C given by $\sigma(s,t) = (\zeta_6 s, t)$. The subfield of $k(C)$ which is fixed by σ is $k(s^3, t)$ implying we get a surjective morphism $f\colon C \to C/\langle\sigma\rangle : \alpha^2 = t^2 + 1$ sending $(s,t) \mapsto (\alpha = s^3, t = t)$. Take $\eta = st\zeta_6$ and $\nu = \zeta_6^2 s^2$, then $\eta^2 = \nu t^2 = \nu(\nu^3 - 1)$. Define $X := -1/\nu$ and $Y := \eta/\nu^2$, then $Y^2 = X^3 + 1$. So we have a k-morphism sending $(s,t) \mapsto (\zeta_6/s^2, -t/s^3)$. The other k-morphism is obtained from considering a different automorphism of the curve C. It remains to show that they are independent, which Magma quickly does for us.*

This gives a lower bound of 2 for the rank of $E_2(k(t))$. However, we would also like to have an upper bound for the rank. Once again we can do this via the theory of elliptic surfaces. Indeed, the curve

$E_2/\bar{\mathbb{F}}_p(t)$ defines an elliptic surface with singular fibers at $t^2 = -1$, which are easily seen to be irreducible. The fiber at infinity is of Kodaira type IV^*, hence consists of 7 irreducible components. The Shioda-Tate formula yields that $r(E_2(\bar{\mathbb{F}}_p(t))) = 2$, which then yields an upper bound of 2 over $k(t)$. In particular we have found that $r(E_2(\mathbb{F}_p(t))) = 2$ for any prime $p \equiv 1 \mod 6$.

Remark 5.2.3. *For a specific prime p an upper bound can also be obtained via Theorem 5.1.4 (see Example 5.1.8).*

Remark 5.2.4. *Whenever k does not contain a primitive 6^{th} root of unity ζ_6 we can look at $L := k(\zeta_6)$ a degree 2 extension of k. The results in all of Section 5.2 then work with k replaced by L. Using Corollary 2.3.13 we are able to say something about $E_f(k(t))$ again.*

5.3 Vector Space Decomposition

In this section we follow the method outlined in [3]. Although done in characteristic zero, nothing special changes when done in characteristic $p > 0$. The set-up is the usual one: let k be a finite field containing a primitive sixth root of unity $\zeta_6 \in k$. Write $K := k(t)$ and let E/K be an elliptic curve given by affine equation $y^2 = x^3 + f(t)$ for some $f(t) \in K$. This has a natural K-endomorphism ρ of order 6 given by $\rho(x, y) = (\zeta_6^2 x, -y)$. Consider the field extension $L = K(s) \supset K$ where $s^6 = t$. Then L/K is a cyclic Galois extension of degree 6 with Galois group generated by the automorphism $\sigma\colon s \mapsto \zeta_6 s$. If $P \in E(L)$, then we write $P \mapsto P^\sigma$ for the action of σ on the coordinates of P. We can tensor the abelian group $E(L)$ with $\mathbb{Q}$ to obtain a $\mathbb{Q}$-vector space

$$V := E(L) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

This vector space has a natural $\mathbb{Q}(\zeta_6)$-structure via $\zeta_6 \cdot (P \otimes r) = \rho(P) \otimes r$. Moreover, σ extends to a $\mathbb{Q}$-linear map σ_V on V via $\sigma_V(P \otimes r) = P^\sigma \otimes r$. Important is that this map σ_V is also $\mathbb{Q}(\zeta_6)$-linear. Indeed, for a nontrivial point $P = (x, y)$ we compute

$$\begin{aligned} \zeta_6 \cdot (\sigma(x), \sigma(y)) \otimes r &= (\zeta_6^2 \sigma(x), -\sigma(y)) \otimes r \\ &= (\sigma(\zeta_6^2 x), \sigma(-y)) \otimes r \\ &= \sigma_V(\zeta_6 \cdot (x, y) \otimes r), \end{aligned}$$

so that the action of ζ_6 and σ_V commute. In particular, this implies that σ_V is $\mathbb{Q}(\zeta_6)$-linear. The eigenvalues λ of σ_V satisfy $\lambda^6 = 1$, hence they all lie in $\mathbb{Q}(\zeta_6)$ and we find that the $\mathbb{Q}(\zeta_6)$-vector space V decomposes as a direct sum of eigenspaces $V = \sum V_\lambda$. We now investigate these eigenspaces.

Lemma 5.3.1. *Keep the set-up from the above discussion. The $\mathbb{Q}(\zeta_6)$-vector space $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$ splits as a direct sum*

$$\sum_{i=0}^{5} V_{\zeta_6^i},$$

where the $\mathbb{Q}(\zeta_6)$-vector space $V_{\zeta_6^i}$ can be identified with $E^i(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, in which E^i/K is the elliptic curve given by $y^2 = x^3 + t^{6-i} f(t)$.

Proof. It is clear that the eigenspace V_1 corresponds to (nontrivial) points $P \otimes r$ with $P^\sigma - P$ of finite order. Hence some multiple of P is in $E(K)$. This implies $V_1 = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $E^0/K \cong E/K$ via a change of variables, so the result follows. For a nontrivial point $P \otimes r$ to lie in V_{ζ_6} we need $P^\sigma - \rho(P)$ to be of finite order. This means that a multiple of P, say $[m]P := (x, y)$ satisfies $\sigma([m]P) = \rho([m]P) = (\zeta_6^2 x, -y)$. In other words, $x = \alpha(t)s^2$ and $y = \beta(t)s^3$ for some $\alpha, \beta \in k(t)$. These coordinates have to satisfy $\beta(t)^2 s^6 = \alpha(t)^3 s^6 + f(t)$ or equivalently $\beta(t)^2 = \alpha(t)^3 + (1/t)f(t)$. This means that these points are precisely the $k(t)$-rationals points on the elliptic curve with affine equation $y^2 = x^3 + (1/t)f(t)$. Via a change of variables this isomorphic to the elliptic curve given by affine equation $y^2 = x^3 + t^5 f(t)$. It follows that $V_{\zeta_6} = E^5(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, as desired. The other cases follow in a similar fashion. □

This immediately gives the following corollary.

Corollary 5.3.2. *Keeping the set-up from above we find*

$$r(E(L)) = \sum_{i=0}^{5} r(E^i(K)). \tag{5.1}$$

Proof. Note that the left hand side of Equation 5.1 is just $\dim_{\mathbb{Q}}(E(L)\otimes_{\mathbb{Z}}\mathbb{Q})$, which by Lemma 5.3.1 equals $\sum_{i=0}^{5}\dim_{\mathbb{Q}}\left(E^i(K)\otimes_{\mathbb{Z}}\mathbb{Q}\right)$. This latter expression is precisely the right hand side of (5.1). □

Important is that elliptic curves described in the beginning of this section always have even rank. This is because the Mordell-Weil group $E(K)$ inherits a natural $\mathbb{Z}[\zeta_6]$-module structure from the endomorphism ring. This implies that $(x,y)\in E(K)$ and $(\zeta_6^2 x,y)\in E(K)$ are independent points if they exist, something which we will repeatedly use.

Example 5.3.3. *Consider the elliptic curve $E_1\colon y^2=x^3+t+1$ over $K=\mathbb{F}_p(t)$, where $p\equiv 1 \mod 6$. Write $L=\mathbb{F}_p(s)$ where $s^6=t$, then*

$$r(E_1(L))=\sum_{i=0}^{5} r(E^i(K)),$$

where E^i/K is the elliptic curve given by $y^2=x^3+t^i(t+1)$. Note that E_1/L can be written as $E_1\colon y^2=x^3+s^6+1$, which is just the elliptic curve $E_6/\mathbb{F}_p(s)$. In particular we find that

$$r(E_6/\mathbb{F}_p(s))=\sum_{i=0}^{5} r(E^i(K)),$$

where E^i/K is the elliptic curve given by $y^2=x^3+t^i(t+1)$.

This means we can calculate the rank of $E_6/\mathbb{F}_p(t)$ using elliptic curves that contain lower powers of t in their Weierstrass form. Let us work this out explicitly. Fix a prime $p\equiv 1 \mod 6$, then we know by Example 5.3.3 that we need to calculate the rank of 6 different elliptic curves. These elliptic curves over $\mathbb{F}_p(t)$ are given by equations $y^2=x^3+t^i(t+1)$, where $i=0,\dots,5$. For $i=0$ we immediately see that this has rank 0 as deduced in Section 4. For $i=1$ we see that the corresponding elliptic surface has 3 singular fibers, two of type II and one of type IV*. The Shioda-Tate formula yields that the rank (over $\bar{\mathbb{F}}_p(t)$) is equal to 2. However, a quick calculation in Magma [2] shows that for $p=7$ the rank is 0 and for $p=31$ the rank is 2. We deduce that the rank of $E_6/\mathbb{F}_p(t)$ is highly dependent on p, but we are able to find primes for which we attain the geometric[†] Mordell-Weil rank. For now, we have failed in calculating the rank of $E_6/\mathbb{F}_p(t)$ in general.

5.4 Shioda's Algorithm

In 1986 Tetsuji Shioda presented an algorithm for computing the Picard number for certain algebraic surfaces [23]. In this section we explain how this can be used to give an upper bound for the rank of the elliptic curves we are interested in. This section applies Shioda's method as described in [9, Section 7] to a concrete example.

Fix a prime number $p\equiv 1 \mod 720$, denote $k=\bar{\mathbb{F}}_p$ and consider the group $E_{360}(k(t))$. We would like to have an upper bound for its rank. The corresponding elliptic surface $\mathcal{E}_{360}$ has only singular fibers above $t^{360}=-1$ and they are all of type II. This implies that the Euler number $e(\mathcal{E}_{360})=720$ (cf. Example 2.5.17). Moreover, from [21, Theorem 6.12] we have that $b_1(\mathcal{E}_{360})=b_1(\mathbb{P}^1)=0$ so by Poincaré-duality (Theorem 2.4.13) it follows that $b_2(\mathcal{E}_{360})=718$. Noether's formula yields that the Euler characteristic is $\chi(\mathcal{E}_{360})=60$ and we define the Lefschetz number of $\mathcal{E}_{360}$ as

$$\begin{aligned}\lambda(\mathcal{E}_{360}) &\coloneqq b_2(\mathcal{E}_{360})-\rho(\mathcal{E}_{360})\\ &= 718-\rho(\mathcal{E}_{360}).\end{aligned}$$

In particular, once we find the Lefschetz number, the Shioda-Tate formula implies

$$r(E_{360}(k(t)))\le 716-\lambda(\mathcal{E}_{360}).$$

Shioda's algorithm gives the Lefschetz number. We will very roughly sketch the algorithm for our specific elliptic curve. For a complete description of the algorithm see [9, Section 7.1]. The lattice L in the algorithm is generated by the vectors

$$v_1\coloneqq\left(\frac{-1}{3},0,\frac{1}{3},0\right),v_2\coloneqq\left(\frac{-1}{2},0,0,\frac{1}{2}\right),v_3\coloneqq\left(\frac{1}{360},\frac{-1}{360},0,0\right).$$

[†]Meaning over an algebraically closed base field.

The only elements that we have chance to lie in the set Λ as in [9, Section 7] are the vectors of the form $x_i := \left(\frac{60+i}{360}, \frac{-i}{360}, \frac{1}{3}, \frac{1}{2}\right)$ and $z_i := \left(\frac{i-420}{360}, \frac{-i}{360}, \frac{2}{3}, \frac{1}{2}\right)$. As p is a prime congruent to 1 modulo 720 we see that for these vectors the integer c_i always equals 1. It is now relatively straightforward to write Magma code (see Listing 7) that determines for a fixed prime p a lower bound for the amount of elements in Λ. In particular, this provides us with an upper bound for the rank of $E_{360}(k(t))$. Via this method we see that the rank for $p = 44460001$, $p = 96614641$, $p = 133773121$, $p = 177452641$ and $p = 206869681$ is bounded above by 68.

6 Primes Congruent to 1 Modulo 6

Recall from Section 5.3 that we failed in finding the rank of $E_6/\mathbb{F}_p(t)$ for a prime $p \equiv 1 \mod 6$. However, using the Shioda-Tate formula and the fact that $\mathcal{E}_6$ defines a rational elliptic surface we see that the geometric Mordell-Weil rank equals 8. We ask the question: for which primes does $E_6/\mathbb{F}_p(t)$ with $p \equiv 1 \mod 6$ attain its geometric rank? The following conjecture gives the answer.

Conjecture 6.0.1. *Consider the elliptic curve $E_6 \colon y^2 = x^3 + t^6 + 1$ over $\mathbb{F}_p(t)$, where $p \equiv 1 \mod 6$. We know that $r(E_6(\bar{\mathbb{F}}_p(t))) = 8$ and we think that we attain the geometric rank over $\mathbb{F}_p(t)$ if the following conditions are satisfied:*

- *We have a root $\beta_{6,0} \in \mathbb{F}_p$ of the polynomial $G_{6,0} := z^6 + 225z^4 - 405z^2 + 243$.*
- *We have a root of the polynomial $G_{6,0,1} = z^3 - \beta_{6,0}^2 + 1$ in $\mathbb{F}_p$.*
- *We have a root of the polynomial $G_{6,0,2} = z^{12} - \beta_{6,0}^5$ in $\mathbb{F}_p$.*

Equivalently, we need a root of the polynomial

$$\begin{aligned} G_6 := {} & z^{144} + 4380210601797031650z^{120} + 66612598686163181266968375z^{96} \\ & + 335162808845453779072679142322236z^{72} + 27095485078653399252384867877999276575z^{48} \\ & + 76888963563847405657011865732 50z^{24} + 71789798769185258877 0249. \end{aligned}$$

Explanation. We employ Theorem 2.5.23 as the equation for E_6 is minimal. First note that we have the 4 obvious independent sections $(-1, t^3), (-\zeta_6^2, t^3), (-t^2, 1)$ and $(\zeta_6^2 t^2, 1)$, where ζ_6 is a primitive sixth root of unity in $\mathbb{F}_p$. We search for 4 more. In order to do so, let $\beta_{6,0} \in \mathbb{F}_p$ be a root of $G_{6,0}$. We know that the group $E_6(\bar{\mathbb{F}}_p(t))$ is generated by sections of the form $(x, y) \in E_6(\bar{\mathbb{F}}_p(t))$ with $x = gt^2 + at + b$, $y = ht^3 + ct^2 + dt + e$ and $a, b, c, d, e, g, h \in \bar{\mathbb{F}}_p$. Filling these into the equation for E_6 we obtain the following system of equations:

$$\left\{\begin{aligned} -b^3 + e^2 - 1 &= 0 \\ -3ab^2 + 2de &= 0 \\ 2ce - b(a^2 + 2bg) - 2a^2b - b^2g + d^2 &= 0 \\ 2cd - a(a^2 + 2bg) + 2eh - 4abg &= 0 \\ 2dh - g(a^2 + 2bg) - 2a^2g - bg^2 + c^2 &= 0 \\ -3ag^2 + 2ch &= 0 \\ -g^3 + h^2 - 1 &= 0 \end{aligned}\right\}.$$

In order to solve this system we can plug this into software like MATLAB [31]:

```
syms g a b h c d e t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
f = y^2 - x^3 - t^6 - 1;
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 1: Solves System of Equations For E_6.

This yields a number of solutions. Write $r \coloneqq \beta_{6,0}$, then one of them is

$$\left\{\begin{array}{l} g = -\zeta_6(r^2-1)^{1/3} \\ a = (817\zeta_6^3 r^2(r^2-1)^{1/3}(-r^5/12+5r^3/6-3r/4)^{2/3})/288 \\ \quad -(99\zeta_6^3(r^2-1)^{1/3}(-r^5/12+5r^3/6-3r/4)^{2/3})/64 \\ \quad +(65\zeta_6^3 r^4(r^2-1)^{1/3})(-r^5/12+5r^3/6-3r/4)^{2/3})/5184 \\ b = (65\zeta_6^2 r(r^2-1)^{1/3}(-r^5/12+5r^3/6-3r/4)^{1/3})/24 \\ \quad -(451\zeta_6^2 r^3(r^2-1)^{1/3}(-r^5/12+5r^3/6-3r/4)^{1/3})/216 \\ \quad -(\zeta_6^2 r^5(r^2-1)^{1/3}(-r^5/12+5r^3/6-3r/4)^{1/3})/108 \\ h = r \\ c = (65\zeta_6^2 r(-r^5/12+5r^3/6-3r/4)^{2/3})/24 \\ \quad -(451\zeta_6^2 r^3(-r^5/12+5r^3/6-3r/4)^{2/3})/216 \\ \quad -(\zeta_6^2 r^5(-r^5/12+5r^3/6-3r/4)^{2/3})/108 \\ d = -\zeta_6(-r^5/12+5r^3/6-3r/4)^{1/3}) \\ e = r \end{array}\right\}.$$

Using Magma we see that we are in the splitting field of $G_{6,0}$, hence we can take the cube root of both r^2-1 and $-r^5/12+5r^3/6-3r/4$ in $\mathbb{F}_p$. This section is visibly independent of the previous 4 and the $\mathbb{Z}[\zeta_6]$-structure induced from the endomorphism $(x,y) \mapsto (\zeta_6 x, -y)$ yields 2 extra independent sections. Using a root of $G_{6,0,1}$ we can find 2 extra independent sections.

The equivalence of needing roots of $G_{6,0}$, $G_{6,0,1}$ and $G_{6,0,2}$ and of needing a root of G_6 is easily checked with Magma (see below).

```
      R<z> := PolynomialRing(Integers());
      f := z^6 + 225*z^4 - 405*z^2 + 243;
      K<b> := NumberField(f);
      L<x> := PolynomialRing(K);
      h := x^3 - b^2 + 1;
      HasRoot(h); /*If true, then h has a root in K*/
      g := x^12 - b^5;
      HasRoot(g);
      SplField := SplittingField(g);
      SplField;
```

Listing 2: Combining Three Polynomials Into One.

□

Remark 6.0.2. *The above explanation is not a rigorous proof. However, in our search for high rank we might as well hope that a lot of sections are defined over $\mathbb{F}_p$. In the case of $\mathcal{E}_6$, to have a lot of sections defined over $\mathbb{F}_p$, we at least need roots of $G_{6,0}$, $G_{6,0,1}$ and $G_{6,0,2}$. Therefore it makes sense to restrict our search for primes so that these polynomials have roots in $\mathbb{F}_p$.*

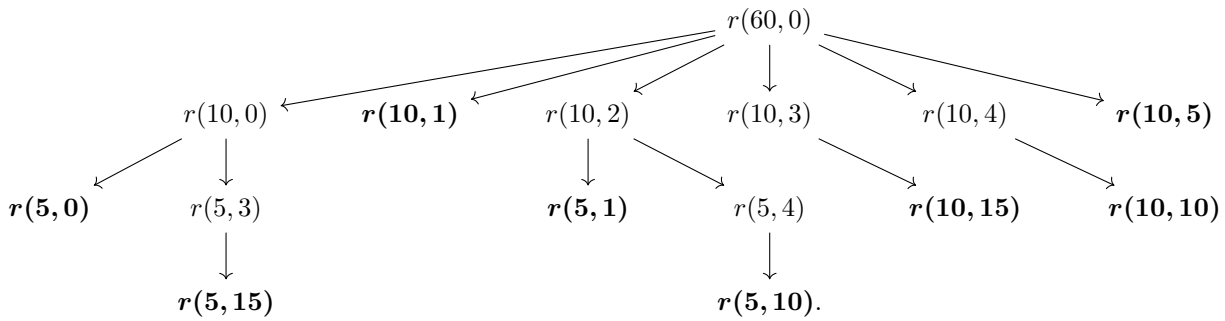
6.1 Finding Prime Numbers That Give High Rank

Using the decomposition found in Section 5.3 we can systematically try to compute the rank of $E_{360}(\mathbb{F}_p(t))$ for $p \equiv 1 \mod 6$. To see this we first fix some notation. Denote $E_{a,b}$ for the elliptic curve over $\mathbb{F}_p(t)$ given by affine equation $y^2 = x^3 + t^b(t^a + 1)$. Denote $r(a, b)$ for its rank over $\mathbb{F}_p(t)$, then our decomposition yields the formula

$$r(360, 0) = \sum_{i=0}^{5} r(60, i). \tag{6.1}$$

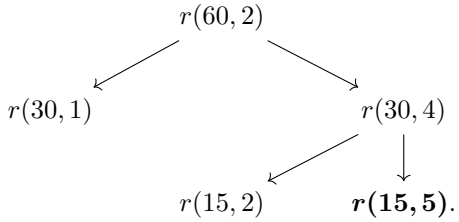
We try to find pieces that correspond to rational elliptic surfaces in order to obtain similar conditions as in Conjecture 6.0.1. Recall that in Lemma 5.3.1 we assumed that the field L is of the form $L = K(s)$ with $s^6 = t$ so that L/K is cyclic Galois of degree 6. We can do the same thing by taking $s^2 = t$ (so that L/K is cyclic of degree 2 with generator σ sending $s \mapsto \zeta_6^3 s$) or $s^3 = t$ (so that L/K is cyclic of degree 3 with generator σ sending $s \mapsto \zeta_6^2 s$). Doing this yields the following formulas for the rank. If $E\colon y^2 = x^3 + f(t^2)$, then the rank of E is the sum of the ranks of $y^2 = x^3 + f(t)$ and $y^2 = x^3 + t^3 f(t)$. If E is given by $E\colon y^2 = x^3 + f(t^3)$, then the rank of E is the sum of the ranks of $y^2 = x^3 + f(t)$, $y^2 = x^3 + t^2 f(t)$ and $y^2 = x^3 + t^4 f(t)$. Using these formulas we now investigate the $r(60, 0)$ case.

Using the order 6 automorphism we find that $r(60, 0) = \sum_{i=0}^{5} r(10, i)$. We look at these ranks one by one as well. Using the order 2 automorphism we find that the $r(10, 0)$ case decomposes into $r(5, 0)$ and $r(5, 3)$, the former surface is rational and the latter $K3$. Using Shioda's formula we know that geometrically $r(5, 0) = 8$ as all fibers of the corresponding rational surface are of type II. Using MATLAB (see Listing 13) we find that a lot of sections are defined over $\mathbb{F}_p$ whenever we have a root $\beta_{5,0}$ of $G_{5,0} = z^{40} + 3732368398z^{30} + 104580047z^{20}/1080 - 209z^{10}/900 + 1/583200000$ in $\mathbb{F}_p$ and a root of $G_{5,0,1} = z^3 - \beta_{5,0}^2$ in $\mathbb{F}_p$. Note that this happens for the prime $p = 1154971$. The following picture nicely illustrates the other decompositions (note that $r(10, 4) = r(10, 10)$, $r(10, 3) = r(10, 15)$, $r(5, 3) = r(5, 15)$ and $r(5, 4) = r(5, 10)$ via a change of variables)

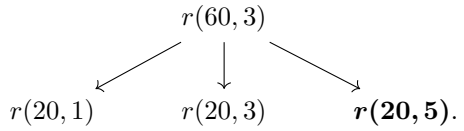


In particular only the $r(5, 0)$ and $r(5, 1)$ cases correspond to rational surfaces. All other cases or either $K3$ or neither $K3$ nor rational. For the $r(5, 1)$ case (geometric rank 8) we obtain a lot of sections defined over $\mathbb{F}_p$ whenever we have a root $\beta_{5,1} \in \mathbb{F}_p$ of the polynomials $G_{5,1} = 5z^8 + 360z^6 - 1350z^4 + 729$ and $G_{5,1,1} = z^3 - \beta_{5,1}^2 + 1$.

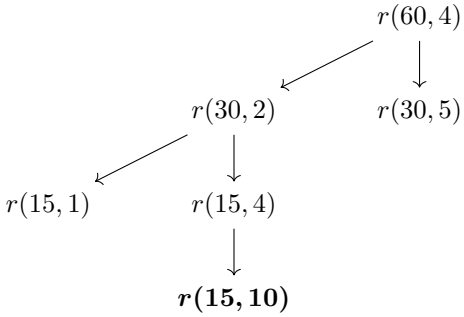
We can play the same game for all other $r(60, i)$ cases, which we will now do. The case $r(60, 1)$ cannot be decomposed any further. For $r(60, 2)$ we get the following diagram



For $r(60,3)$ we get



For $r(60,4)$ we get



and lastly for $r(60,5)$ we have no further decomposition. In this way we barely obtain any rational elliptic surfaces, but there is a way around this. Indeed, we estimate certain ranks using rational elliptic surfaces. To illustrate this, consider the $r(10,10)$ case corresponding to the elliptic curve $E_{10,10}\colon y^2 = x^3+t^{10}(t^{10}+1)$. Performing the substitution $s = t^{10}$ we obtain that $E_{10,10}(\mathbb{F}_p(s)) \subset E_{10,10}(\mathbb{F}_p(t))$ and the former group is isomorphic to $E_{2,2}(\mathbb{F}_p(t))$. This means that $r(10,10) \geq r(2,2)$, so we can bound the rank. The latter curve is quickly analysed as follows. For $p \equiv 1 \mod 6$ the corresponding surface has 2 fibers of type II and 2 fibers of type IV. Using the Shioda-Tate formula we immediately see that the geometric rank is 4. Suppose now that we take p so that the polynomial $G_{2,2} = 4z^3 - 1$ has a root modulo p. Then according to the sections obtained by MATLAB we should get a lot of them defined over $\mathbb{F}_p$. In fact, one can write down 4 explicit independent sections. They are given as $(\alpha, t^2+1/2)$, $(\zeta_6^2\alpha, t^2+1/2)$, $(\alpha t^2, t^3/2+t)$ and $(\zeta_6^2\alpha t^2, t^3/2+t)$ where α is a root of $G_{2,2}$ (cf. Appendix B).

In the same way we get $r(10,5) \geq r(2,1)$, which corresponds to a rational elliptic surface with 3 fibers of type II and 1 fiber of type I_0^*. Therefore it has geometric Mordell-Weil rank equal to 4 and we once again ask ourselves when this has sections defined over $\mathbb{F}_p$. Using MATLAB with sections of the form $(-t+a, ct+d)$ we see that we have a lot of them defined over $\mathbb{F}_p$ whenever $G_{2,1,1} = 3z^4+6z^2-1$ has a root modulo p. Using some more general sections we see that we also need a root of $G_{2,1,2} = -14348907+12597120z^4+4096z^8$.

Similarly we see $r(15,5) \geq r(3,1)$, which corresponds to a rational elliptic surface. It has 4 fibers of type II and 1 of type IV. So the geometric rank is equal to 6. Using MATLAB we find a lot of sections defined over $\mathbb{F}_p$ when the following polynomials have roots mod p:

- $G_{3,1,1} = z^9 - 159z^6/2 + 21z^3 + 1/8$ with root $\beta_{3,1,1}$;
- $G_{3,1,2} = z^9 + 159z^6/2 + 21z^3 - 1/8$ with root $\beta_{3,1,2}$;
- $G_{3,1,1,1} = z^3 - \beta_{3,1,1}^2$;
- $G_{3,1,2,1} = z^3 - \beta_{3,1,2}^2$.

We continue the process.

Again we find $r(20,5) \geq r(4,1)$ a rational elliptic surface with only type II fibers, hence with geometric rank 8. Using MATLAB we get that a lot of sections are defined over $\mathbb{F}_p$ whenever $G_{4,1} = z^{32} + 26480951z^{24} + 772048803z^{16}/8 + 26480951z^8/16 + 1/256$ has a root $\beta_{4,1} \in \mathbb{F}_p$ and the polynomial $G_{4,1,1} = z^3 - \beta_{4,1}^2$ has a root in $\mathbb{F}_p$.

We are not done, via a change of variables we find $r(15,4) = r(15,10) \geq r(3,2)$. Once again we get a rational elliptic surface. This one has 4 fibers of type II and 1 fiber of type IV, hence has geometric rank 6. Via MATLAB we see that a lot of sections will be defined over $\mathbb{F}_p$ when we have a root $\beta_{3,2}$ of $G_{3,2} = z^{18}+1229z^{12}/18+8371z^6/3888+1/1259712$ in $\mathbb{F}_p$ and a root of $G_{3,2,1} = z^3-\beta_{3,2}^2$ in $\mathbb{F}_p$.

Similarly, we investigate $r(5,10) \geq r(1,2)$. The latter corresponds to a rational elliptic surface with three singular fibers of type II, IV and I_0^*, respectively. So it has geometric rank 2 and we always attain it for $p \equiv 1 \mod 6$ as we have the obvious section $(-t,t)$ together with the $\mathbb{Z}[\zeta_6]$-structure.

Second to last, we investigate $r(10,15) \geq r(2,3)$. This gives a rational elliptic surface with 3 fibers of type II and 1 of type I_0^*, meaning it has geometric rank 4. Using MATLAB we see that a lot of sections are defined over $\mathbb{F}_p$ whenever the polynomials $G_{2,3,1} = 3z^4 + 6z^2 - 1$, $G_{2,3,2} = 9z^8 - 18z^6 + 39z^4 + 6z^2 + 1$ and $G_{2,3,3} = z^8 + 18z^4 - 27$ have roots in $\mathbb{F}_p$.

Lastly, we investigate $r(5,15) \geq r(1,3)$, the latter corresponds to a rational elliptic surface with 1 fiber of type II, one of type I_0^* and one of type IV. Therefore it has geometric rank 2 and it is clear that we always attain rank 2 for primes 1 modulo 6. To see this note that we have the obvious section $(-t,t^2)$, so using the $\mathbb{Z}[\zeta_6]$-action we get rank 2.

When we add together all of the geometric ranks, we find that the highest rank we can achieve as a lower bound in this scenario is 52. However, we have not analysed several curves obtained in the decomposition. An important curve to look at is $E_{10,1}\colon y^2 = x^3 + t(t^{10}+1)$.

Lemma 6.1.1. *The rank of $E_{10,1}$ equals the sum of the ranks of $E\colon y^2 = x^3 + t^5 - 5t^3 + 5t$ and $E_{twist}\colon (t^2-4)y^2 = x^3 + t^5 - 5t^3 + 5t$.*

Proof. Via a change of variables we see that $E_{10,1}$ is isomorphic to the curve $E\colon y^2 = x^3 + t^5 + t^{-5}$. Consider now $u = t + 1/t$, which gives a degree 2 extension $\mathbb{F}_p(u) \subset \mathbb{F}_p(t)$. In particular we have that the extension $\mathbb{F}_p(t)$ is obtained by adjoining a root of $u^2 - 4$ to $\mathbb{F}_p(u)$. Using [25, Exercise 10.16] we see that $r(10,1) = r(E_{10,1}(\mathbb{F}_p(u))) + r(E_{\mathrm{twist}}(\mathbb{F}_p(u)))$, where the group $E_{10,1}(\mathbb{F}_p(u))$ can be viewed as the $\mathbb{F}_p(u)$-rational points on the curve $E\colon y^2 = x^3 + u^5 - 5u^3 + 5u$. The result follows. □

The curve E_{twist} determines an elliptic $K3$ surface and the curve $E\colon y^2 = x^3 + u^5 - 5u^3 + 5u$ over $\mathbb{F}_p(u)$ defines a rational elliptic surface with singular fibers all of type II. In particular, the latter surface has geometric Mordell-Weil rank 8. We ask the question: when does $E/\mathbb{F}_p(u)$ attain its geometric rank? Using MATLAB again we see that we at least need the polynomial $G_{10,1,1} = 25z^{16} - 25 \cdot 11340z^{12} - 5 \cdot 240842z^8 - 25 \cdot 2268z^4 + 1$, but also of a bunch of other polynomials with huge coefficients to have roots modulo p. E.g the polynomials $G_{10,1,2} = 13286025z^{16} - 164025 \cdot 28 \cdot z^{12} + 5 \cdot 235718z^8 - 45 \cdot 28z^4 + 1$ and $G_{10,1,3} = 10485760000z^{32} + 796262400000z^{28} + 28673969152000z^{24} + 5919441120000z^{20} + 569262158025z^{16} - 18498253500z^{12} + 280019230z^8 - 24300z^4 + 1$ need roots. Via these polynomials we see that the prime 409 works.

Using this method we can obtain rank 60 just by looking at rational elliptic surfaces. We try to find a prime that attains this.

6.2 List of Polynomials That Need a Root

Here we keep a list of which polynomials need to have roots modulo p in order to obtain (possibly) high rank. Recall that the notation $\beta_{i,j}$ and $\beta_{i,j,k}$ is used to denote a root of the polynomials $G_{i,j}$ and $G_{i,j,k}$ respectively.

- $G_{6,0} = z^6 + 225z^4 - 405z^2 + 243$;
- $G_{6,0,1} = z^3 - \beta_{6,0}^2 + 1$;
- $G_{6,0,2} = z^{12} - \beta_{6,0}^5$;
- $G_{5,0} = z^{40} + 3732368398z^{30} + 104580047z^{20}/1080 - 209z^{10}/900 + 1/583200000$;
- $G_{5,0,1} = z^3 - \beta_{5,0}^2$;
- $G_{5,1} = 5z^8 + 360z^6 - 1350z^4 + 729$;
- $G_{5,1,1} = z^3 - \beta_{5,1}^2 + 1$;
- $G_{2,1,1} = 3z^4 + 6z^2 - 1$;
- $G_{2,1,2} = -14348907 + 12597120z^4 + 4096z^8$;

- $G_{3,1,1} = z^9 - 159z^6/2 + 21z^3 + 1/8$;
- $G_{3,1,2} = z^9 + 159z^6/2 + 21z^3 - 1/8$;
- $G_{3,1,1,1} = z^3 - \beta_{3,1,1}^2$;
- $G_{3,1,2,1} = z^3 - \beta_{3,1,2}^2$;
- $G_{4,1} = z^{32} + 26480951z^{24} + 772048803z^{16}/8 + 26480951z^8/16 + 1/256$;
- $G_{4,1,1} = z^3 - \beta_{4,1}^2$;
- $G_{3,2} = z^{18} + 1229z^{12}/18 + 8371z^6/3888 + 1/1259712$;
- $G_{3,2,1} = z^3 - \beta_{3,2}^2$;
- $G_{2,3,1} = 3z^4 + 6z^2 - 1$;
- $G_{2,3,2} = 9z^8 - 18z^6 + 39z^4 + 6z^2 + 1$;
- $G_{2,3,3} = z^8 + 18z^4 - 27$;
- $G_{2,2} = 4z^3 - 1$;
- $G_{10,1,1} = 25z^{16} - 25 \cdot 11340z^{12} - 5 \cdot 240842z^8 - 25 \cdot 2268z^4 + 1$;
- $G_{10,1,2} = 13286025z^{16} - 164025 \cdot 28 \cdot z^{12} + 5 \cdot 235718z^8 - 45 \cdot 28z^4 + 1$;
- $G_{10,1,3} = 10485760000z^{32} + 796262400000z^{28} + 28673969152000z^{24} + 5919441120000z^{20} + 569262158025z^{16} - 18498253500z^{12} + 280019230z^8 - 24300z^4 + 1$.

Remark 6.2.1. *The polynomials $G_{2,3,1}$ and $G_{2,1,1}$ are equal. Moreover, in order to obtain high rank for $E_{360}(\mathbb{F}_p(t))$ we do not have to check whether $G_{6,0}$, $G_{6,0,1}$ and $G_{6,0,2}$ have roots modulo p, as they do not show up in the decomposition. This leaves 20 polynomials for which we need to determine if they have a root modulo p.*

Remark 6.2.2. *Their exist infinitely many prime numbers p so that all these polynomials have a root in $\mathbb{F}_p$ thanks to Corollary 2.7.6.*

Running a computer program we encounter the primes $p = 44460001$, $p = 96614641$, $p = 133773121$, $p = 177452641$, $p = 206869681$ and $p = 246569041$. Using Magma we see that we attain a lower bound of rank 60 using rational elliptic surfaces (see Listing 5). We however, are interested in the rank 68 case. The remaining 8 independent sections can be found by base changing from the elliptic $K3$ surface found in Lemma 6.1.1.

This elliptic K3 surface is given by the equation $y^2 = x^3 + (t^2 - 4)^3(t^5 - 5t^3 - 5t)$. Going forward, let us refer to this elliptic curve as $E_{K3}/\mathbb{F}_p(t)$. From what we know about the literature, there are no general methods for computing the rank of such curves in a straightforward manner. However, we can do a naive point search and check whether we obtain a lot of independent points. To do this, fix the prime $p = 44460001$ as obtained above. The following piece of Magma code computes points in $E_{K3}(\mathbb{F}_p(t))$ of the form

$$(x, y) = \left(a_0 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4, b_0 + b_1 t + b_2 t^2 + b_3 t^3 + b_4 t^4 + b_5 t^5 + b_6 t^6\right),$$

with $a_i, b_j \in \mathbb{F}_p$.

```
p := 44460001;
K := GF(p);
A<a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6> := AffineSpace(K,12);
S := CoordinateRing(A);
U<t> := PolynomialRing(S);
x := a0+a1*t+a2*t^2+a3*t^3+a4*t^4;
y := b0+b1*t+b2*t^2+b3*t^3+b4*t^4+b5*t^5+b6*t^6;
f := x^3+(t^2-4)^3*(t^5-5*t^3+5*t)-y^2;
I := ideal<S | Coefficients(f)>;
B := Scheme(A,I);
Points(B);
```

Listing 3: Computing Points In $E_{K3}(\mathbb{F}_p(t))$.

Running this code in Magma gives many points. We naively take a few of them and check whether they are independent. The code displayed in Listing 6 shows that we obtain 8 independent points. We conclude that the Mordell-Weil rank of $E_{360}(\mathbb{F}_p(t))$ is at least 68 for $p = 44460001$. Moreover, the primes $p = 96614641$, $p = 133773121$, $p = 177452641$ and $p = 206869681$ also yields a lower bound of 68 in a similar fashion.

Together with the results from Section 5.4 this yields that we have

$$\operatorname{rank} E_{360}(\mathbb{F}_p(t)) = \operatorname{rank} E_{360}(\bar{\mathbb{F}}_p(t)) = 68 \tag{6.2}$$

for the primes $p = 44460001$, $p = 96614641$, $p = 133773121$, $p = 177452641$ and $p = 206869681$.

Combining the above with the results from Section 3 we conclude that we have found five prime numbers p for which the 68 independent sections of Shioda's example exist and remain independent over $\mathbb{F}_p$ after a reduction modulo p. Next section discusses the case where a lot more than 68 independent sections arise when reducing modulo p.

Remark 6.2.3. *Throughout this section we repeatedly invoked Magma to compute the Mordell-Weil rank of certain rational elliptic surfaces over $\mathbb{F}_p$. We can do these computations by hand via several methods:*

(1) performing a complete 2-descent;

(2) using Theorem 7.2.1;

(3) or via brute-forcing.

For our purposes method (3) suffices. Indeed, it is relatively easy to compute sections on these rational elliptic surfaces and check whether they are independent (cf. the K3 case from before). Via this method we can explicitly compute all the 68 generating points on the elliptic curve $E_{360}/\mathbb{F}_p(t)$. Method (2) is not feasible as $p^{g(C)}$ for the curves C appearing becomes too big, too quickly. Method (1) is quite efficient and it is precisely what Magma uses when the usual geometric methods are not available.

7 Primes Congruent to -1 Modulo 6

Recall that a surface S is called supersingular if $\rho(S) = b_2(S)$. This section looks at particular elliptic surfaces that are supersingular and attain high Mordell-Weil rank.

7.1 Integral Sections

It was already known by Tate and Shafarevich [30] that we can construct families of elliptic curves over $\mathbb{F}_p(t)$ that attain arbitrarily large rank over $\bar{\mathbb{F}}_p(t)$. By investigating section 13.4.1 of [19] in a more elementary way we find another such family and we try to explain in depth why unitary matrices yield integral sections on the corresponding surface. To do so we first introduce some notation.

Definition 7.1.1. *Let $\mathbb{F}_{q^2}$ be a finite field. For any element $a \in \mathbb{F}_{q^2}$ we write $\bar{a} \coloneqq a^q$. The unitary group over $\mathbb{F}_{q^2}$ consists of invertible matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat(2, \mathbb{F}_{q^2})$ that satisfy $AA^* = I = A^*A$, where $A^* \coloneqq \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$. This is a group under matrix multiplication denoted by $\boldsymbol{U}(2, \mathbb{F}_{q^2})$.*

Consider now the following theorem based on [19, Theorem 13.42].

Theorem 7.1.2. *Let p be a prime number so that $p \equiv -1 \mod 6$, and let k be the field $\mathbb{F}_{p^2}$. Consider the elliptic curve E over $K = k(t)$ defined by the Weierstrass form:*

$$E_{p+1} \colon y^2 = x^3 + t^{p+1} + 1.$$

Then the rank of $E_{p+1}(K)$ is $2p-2$ and any unitary matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{U}(2, \mathbb{F}_{p^2})$ gives rise to the integral section $P = (-(at+b)^{(p+1)/3}, (ct+d)^{(p+1)/2})$. Moreover, the rank of $E_{p+1}(\mathbb{F}_p(t))$ is $p-1$.

The proof of this theorem in [19] is quite involved and makes use of crystalline cohomology, a concept we prefer not to delve into. However, using Theorem 5.1.4 we can give a much more elementary proof.

The elliptic surface $\mathcal{E}_{p+1}$, corresponding to the equation for E_{p+1}, is covered by a Fermat surface of the form

$$S_{p+1}\colon X^{p+1}+Y^{p+1}+Z^{p+1}+W^{p+1}=0\subset\mathbb{P}^3. \tag{7.1}$$

Indeed, write S_{p+1} affinely as $x^{p+1}+y^{p+1}+z^{p+1}+1=0$, fix an integer l so that $p+1=6l$ and fix an element $i\in\mathbb{F}_{p^2}$ satisfying $i^2=-1$. Then we have a covering map (see Definition 2.1.8)

$$(x,y,z)\mapsto(\xi=x^{2l},\eta=iy^{3l},t=z)$$

from S_{p+1} to $\mathcal{E}_{p+1}$. Take a line m parametrized by t given by $m=(at+b,ct+d,t)\subset\mathbb{A}^3$ where $a,b,c,d\in\mathbb{F}_{p^2}$. In order for this line to lie entirely on the Fermat surface we would need

$$(at+b)^{p+1}+(ct+d)^{p+1}+t^{p+1}+1=0.$$

This gives the following four conditions on $a,b,c,d\in\mathbb{F}_{p^2}$:

$$\begin{Bmatrix}\bar{a}a+\bar{c}c=-1\\ \bar{a}b+\bar{c}d=0\\ \bar{b}a+\bar{d}c=0\\ \bar{b}b+\bar{d}d=-1\end{Bmatrix}.$$

This precisely means that the matrix $B\coloneqq\begin{pmatrix}a&b\\c&d\end{pmatrix}$ satisfies $B^*B=-I$. We conclude that any matrix $B\in\mathrm{Mat}(2,\mathbb{F}_{p^2})$ satisfying $B^*B=-I$ yields a line on the Fermat surface. Of course, any unitary matrix A then yields another line as $(AB)^*(AB)=-I$.

Take a matrix B satisfying $B^*B=-I$, via the covering map this yields the point

$$\Big((at+b)^{(p+1)/3},i(ct+d)^{(p+1)/2}\Big)\in E_{p+1}(\mathbb{F}_{p^2}(t)).$$

We should note that we are not in the same situation as in [19, p. 403]. However, it is not hard to go from our result to theirs. Indeed, in the field $\mathbb{F}_{p^2}$ there always exists an element α satisfying $\alpha^{p+1}=-1$, $\alpha^{(p+1)/3}=-1$ and $\alpha^{(p+1)/2}=-i$. To see this we note that $p^2-1=36l^2-12l$, which is divisible by $(p+1)/3=2l$. Hence there is an element $\alpha\in\mathbb{F}_{p^2}$ so that $\alpha^{2l}=-1$. Then clearly $\alpha^{6l}=-1$ and $\alpha^{3l}=-\alpha^l=-i$. This yields the obvious line $(\alpha,\alpha t,t)$ and any unitary matrix $U\coloneqq\begin{pmatrix}e&f\\g&h\end{pmatrix}$ yields the line $(\alpha et+f\alpha,\alpha gt+h\alpha,t)$ and hence the point

$$\Big(-(et+f)^{(p+1)/3},(gt+h)^{(p+1)/2}\Big)\in E_{p+1}(\mathbb{F}_{p^2}(t)),$$

as desired.

Remark 7.1.3. *The size of the group $\boldsymbol{U}(2,\mathbb{F}_{p^2})$ is $p(p+1)(p^2-1)$. This is a classical, but nontrivial result for which we refer to [12, Proposition 2.3.3] for more details.*

We now investigate in some specific examples how many of these $p(p+1)(p^2-1)$ sections arising from unitary matrices yield independent sections on the elliptic surface. We can do this via the explicit formula for the height pairing from Theorem 2.5.14.

In our set-up, this becomes particularly simple. Indeed, the elliptic surface defined by equation $y^2=x^3+t^{p+1}+1$ has only fibers of type II. Therefore we are left with the following formula for the height pairing on E_{p+1}:

$$\langle P,Q\rangle=(p+1)/6+(P.\mathcal{O})+(Q.\mathcal{O})-(P.Q), \tag{7.2}$$

for points $P,Q\in E_{p+1}(\bar{\mathbb{F}}_p(t))$. Moreover, if the sections P,Q arise from unitary matrices, then they are integral. Indeed, for a point $P=\big(-(et+f)^{(p+1)/3},(gt+h)^{(p+1)/2}\big)\in E_{p+1}(\mathbb{F}_{p^2}(t))$ it is clear that the

corresponding section does not intersect the zero section for $t \in \mathbb{A}^1$. To see what happens at $t = \infty$ we set $s = 1/t$ and write $p + 1 = 6k$. Set $\eta = ys^{3k}$ and $\xi = xs^{2k}$, then a model at infinity is given by

$$\eta^2 = \xi^3 + s^{6k} + 1.$$

The section P is of the form $P = (\alpha t^{2k} + \text{l.o.t}, \beta t^{3k} + \text{l.o.t})^\dagger$ with $\alpha, \beta \in \mathbb{F}_{p^2}$. On the model at infinity this becomes the section $(s^{2k} \cdot (\alpha s^{-2k} + \text{h.o.t}), s^{3k} \cdot (\beta s^{-3k} + \text{h.o.t}))^*$, which has polynomials in s as coordinates and hence does not intersect the zero section at $s = 0$. We conclude that the section P is an integral section. For such sections the height pairing formula (7.2) becomes even simpler:

$$\langle P, Q \rangle = (p + 1)/6 - (P.Q).$$

Remark 7.1.4. *From Lemma 2.5.29 we know that for any $P \in E(K)$ its self-intersection P^2 is given as $P^2 = -\chi(\mathcal{E}_{p+1})$. In a similar fashion as in Example 2.5.17 we find that the Euler number of $\mathcal{E}_{p+1}$ is $2p + 2$. With Noether's formula (2.4.20) we find $-\chi(\mathcal{E}_{p+1}) = -(p + 1)/6$. This implies that $\langle P, P \rangle = (p + 1)/3 + 2(P.\mathcal{O})$ on the elliptic surface $\mathcal{E}_{p+1}$.*

We aim to answer the question: **what is the rank of the subgroup $H \subset E_{p+1}(\mathbb{F}_{p^2}(t))$ generated by sections arising from unitary matrices?** We did not find an answer to this question. However, for the prime $p = 5$ we can do some computations using Magma.

Example 7.1.5. *Fix the prime $p = 5$ so that we consider the elliptic curve $E_6 \colon y^2 = x^3 + t^6 + 1$. By Theorem 7.1.2 we know this has rank 8 over $\mathbb{F}_{25}$ and rank 4 over $\mathbb{F}_5$. Any unitary matrix $U := \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ with coefficients in $\mathbb{F}_{25}$ yields an integral section of the form*

$$\left(-(et + f)^2, (gt + h)^3\right) \in E_6(\mathbb{F}_{25}(t)).$$

Note that taking coefficients in the field $\mathbb{F}_5$ gives well-defined sections over $\mathbb{F}_5$. The only unitary matrices over $\mathbb{F}_5$ are $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ This way we find 2 distinct sections defined over $\mathbb{F}_5$: $(-1, t^3)$ and $(-t^2, 1)$. These sections are independent. Indeed, call $P := (-1, t^3)$ and $Q := (-t^2, 1)$. It is clear that these sections only meet above $t = 1$ and possibly at ∞. Performing the change of variables $s = \frac{1}{t}$ we obtain an affine model $y^2 = x^3 + s^6 + 1$ and the points P and Q correspond to $(-s^2, 1)$ and $(-1, s^3)$ respectively. These clearly do not meet above $s = 0$ and we conclude that the sections P and Q only intersect above $t = 1$.

We now give a computation that shows $(P.Q) = 1$. The above argument shows that we only have to look at the intersection multiplicity of the curves

$$P = Z(y^2 - x^3 - t^6 - 1, x + 1, y - t^3)$$

and

$$Q = Z(y^2 - x^3 - t^6 - 1, x + t^2, y - 1)$$

inside $\mathbb{A}^3$ (with coordinates x, y, t) at the point $(-1, 1, 1)$. We change coordinates $a := x + 1$, $b := y - 1$ and $c := t - 1$. The curve P then corresponds to

$$Z((b + 1)^2 - (a - 1)^3 - (c + 1)^6 - 1, a, b + 1 - (c + 1)^3)$$

and Q corresponds to the curve

$$Z((b + 1)^2 - (a - 1)^3 - (c + 1)^6 - 1, b, a - 1 + (c + 1)^2).$$

The intersection multiplicity is then given by

$$\dim_{\mathbb{F}_5} \left(\frac{\mathbb{F}_5[a, b, c]_{(a,b,c)}}{((b + 1)^2 - (a - 1)^3 - (c + 1)^6 - 1, a, b + 1 - (c + 1)^3, b, a - 1 + (c + 1)^2)} \right),$$

which equals

$$\dim_{\mathbb{F}_5} \left(\frac{\mathbb{F}_5[c]_{(c)}}{(1 - (c + 1)^6, 1 - (c + 1)^3, 1 - (c + 1)^2)} \right) \quad (\star).$$

[†]The abbreviation "l.o.t" means "lower order terms".

[*]The abbreviation "h.o.t" means "higher order terms".

The polynomials $1-(c+1)^6$, $1-(c+1)^3$ *and* $1-(c+1)^2$ *all have a simple root at* $c=0$. *It follows that the ideal* $(1-(c+1)^6, 1-(c+1)^3, 1-(c+1)^2) = (c) \subset \mathbb{F}_5[c]_{(c)}$. *In particular, the expression* $(\star)$ *evaluates to* 1 *and we conclude that* $(P.Q) = 1$.

This implies that the height pairing matrix is $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, *so that we have found two independent sections. Therefore, the subgroup* $H \subset E_6(\mathbb{F}_5(t))$ *generated by sections obtained from unitary matrices over* $\mathbb{F}_5$ *only generates a rank* 2 *subgroup.*

Over $\mathbb{F}_{25} = \mathbb{F}_5(\zeta_3)$, *with* ζ_3 *a cube root of unity, the situation changes drastically. Indeed, using the* $\mathbb{Z}[\zeta_3]$*-action induced from the endomorphism* $(x,y) \mapsto (\zeta_3 x, y)$ *we immediately get the* 4 *independent sections* $(-1, t^3)$, $(-\zeta_3, t^3)$, $(-t^2, 1)$ *and* $(-\zeta_3 t^2, 1)$. *We generate some unitary matrices over* $\mathbb{F}_{25}$ *using Magma (see Listing 8). Two of them are given by* $\begin{pmatrix} 3 & 3\zeta_3+2 \\ 2\zeta_3+3 & 2\zeta_3 \end{pmatrix}$ *and* $\begin{pmatrix} 3\zeta_3+1 & 3\zeta_3+3 \\ 3\zeta_3 & 2\zeta_3+3 \end{pmatrix}$. *Together with the* $\mathbb{Z}[\zeta_3]$*-action this yields* 4 *different sections. A computation in Magma (see Listing 9) shows that they are independent. In particular, the subgroup* $H \subset E_6(\mathbb{F}_{25}(t))$ *generated by sections arising from unitary matrices is of rank* 8 *as well!*

The example above seems to indicate that the subgroup generated by sections arising from unitary matrices does in fact generate, up to finite index, the entire Mordell-Weil group over $\mathbb{F}_{p^2}(t)$. It seems plausible that ideas from [20, Chapter 5.1] may be used to answer this question, but we did not investigate this further.

7.2 Zeta Functions and Maximal Curves

Recall that we are interested in the rank of the group $E_{p+1}(\mathbb{F}_p(t))$. We determine this rank using Theorem 5.1.4. To do so fix a prime number p congruent to -1 modulo 6 and let $k := \mathbb{F}_{p^2} = \mathbb{F}_q$. Then k contains a primitive sixth root of unity and we are precisely in the set-up from Section 5.2. Indeed, define the algebraic curve $C\colon s^6 = t^{p+1} + 1$. Then we know that $E_{p+1}(k(t)) \subset \mathrm{Mor}_k(C, \tilde{E})$ and the morphisms corresponding to rational points are precisely the ones which make a certain diagram commute. Once we know the rank of the group $E_{p+1}(k(t))$ we also know the rank of $E_{p+1}(\mathbb{F}_p(t))$ as $k = \mathbb{F}_p(\sqrt{-3})$ (cf. Lemma 2.3.13). Tate's result (Theorem 5.1.4) gives us a method for determining

$$\operatorname{rank} \mathrm{Mor}_k(C, \tilde{E}) = \operatorname{rank} \mathrm{Hom}_k(\operatorname{Jac} C, \tilde{E}),$$

where the equality follows from Corollary 5.1.3.

The following statement by Tate and Shafarevich [30], which is a corollary of Theorem 5.1.4, proves to be incredibly powerful.

Theorem 7.2.1. *Let* $k = \mathbb{F}_q$ *be a finite field,* C *a geometrically irreducible projective curve and* E *an elliptic curve both defined over* k. *Moreover, denote* $K = k(C)$ *and* E_K *the curve* E *seen over* K. *Let* r *be the rank of* $E_K(K)$ *and denote* $L_{C/k}(T)$, $L_{E/k}(T)$ *for the* L*-polynomials of* C/k *and* E/k *respectively (cf. Section 5.1). Then we have*

$$r = 2h,$$

if $L_{C/k}(T) = L_{E/k}(T)^h \cdot G(T)$ *and* $L_{E/k}(T)$ *irreducible over* $\mathbb{Q}$ *or* $L_{C/k}(T) = L_{E/k}(T)^{h/2} \cdot G(T)$ *and* $L_{E/k}(T) = F(T)^2$ *with* $\gcd(L_{E/k}(T), G(T)) = 1$.

Proof. This is an immediate corollary of Theorem 5.1.4 and Lemma 5.1.6. □

In our case we have that $r = \operatorname{rank} \mathrm{Mor}_k(C, \tilde{E})$, so in order to use this theorem we need to know the zeta functions of C/k and $\tilde{E}/k$.

Lemma 7.2.2. *Consider the elliptic curve* $\tilde{E}\colon y^2 = x^3 + 1$ *over* $k = \mathbb{F}_{p^2} = \mathbb{F}_q$, *where* $p \equiv -1 \mod 6$. *The zeta function is given by*

$$Z(\tilde{E}/k; T) = \frac{(pT+1)^2}{(1-T)(1-p^2T)}.$$

Proof. See Example 2.6.6. □

From this lemma we immediately see that $L_{\tilde{E}/k}(T) = (1+pT)^2$, which is not irreducible over $\mathbb{Q}$. In order to apply Theorem 7.2.1 we need to know how many factors of $1+pT$ appear in $L_{C/k}(T)$ where C is the curve $C\colon s^6 = t^{p+1}+1$ over $k = \mathbb{F}_{p^2}$. We first compute the genus of C.

Lemma 7.2.3. *Let k be a field of characteristic $p \equiv -1 \mod 6$ and let C be the smooth projective curve given by the affine equation $s^6 = t^{p+1}+1$. The genus of C/k is $\frac{5(p-1)}{2}$.*

Proof. Write $p+1 = 6a$ for some integer a and note that the curve C is given by gluing two affines $s^6 = t^{6a}+1$ and $y^6 = x^{6a}+1$ via the gluing maps $t = 1/x$ and $s = y/x^a$ (cf. Example 2.1.3). In particular, the points of infinity of C correspond to the points with $x = 0$ on the affine chart $y^6 = x^{6k}+1$, hence there are 6 of them. Consider the morphism $f\colon C \to \mathbb{P}^1$ sending $(s,t) \mapsto (t:1)$. Then the degree of f is equal to $[k(C)\colon k(t)] = 6$. By Riemann-Hurwitz (Theorem 2.1.13) we find that $2g(C)-2 = 6\cdot(-2)+\sum_{P\in C}(e_f(P)-1)$. The points of C that ramify and that correspond to the affine part of $\mathbb{P}^1$ have to satisfy $t^{p+1} = -1$, hence there are $p+1$ such points with ramification index 6. Moreover, $f^{-1}(1:0)$ consists precisely of the 6 points of infinity of C so no ramification occurs at these points. Filling in the Riemann-Hurwitz formula we obtain $g(C) = 5+\frac{1}{2}(p+1)(5) = \frac{5(p-1)}{2}$, as desired. □

Definition 7.2.4. *Let C/k be a smooth, projective, geometrically irreducible algebraic curve over a finite field $k = \mathbb{F}_q$. We say C is $\mathbb{F}_q$-maximal if it attains the Hasse-Weil bound, i.e. if $|C(\mathbb{F}_q)| = q+1+2g(C)\sqrt{q}$.*

Note that this is only possible if the cardinality of k is a square.

Example 7.2.5 (Hermitian Curves)**.** *Let $k = \mathbb{F}_{q^2}$ be a finite field and let $\mathcal{H}_q/k$ be the algebraic curve given by affine equation $Y^{q+1}+X^{q+1}+1 = 0$. Then this is a k-maximal curve.*

Proof. See [27, Example 6.3.6]. □

Theorem 7.2.6. *Let $C/\mathbb{F}_{q^2}$ be an $\mathbb{F}_{q^2}$-maximal curve. The zeta function of C is*

$$Z(C/\mathbb{F}_{q^2};T) = \frac{(1+qT)^{2g(C)}}{(1-T)(1-q^2T)}.$$

Proof. We know that $b_1 = 2g(C)$ for an algebraic curve, so that $Z(C/\mathbb{F}_{q^2};T) = \frac{P_1(T)}{(1-T)(1-q^2T)}$ where $P_1(T) = \prod_{j=1}^{2g(C)}(1-\omega_j T)$ and $|\omega_j| = q$. Using Theorem 5.1.7 we find that $|C(\mathbb{F}_{q^2})| = q^2+1-\sum_{j=1}^{2g(C)}\omega_j$, which by $\mathbb{F}_{q^2}$-maximality gives the equality

$$-\sum_{j=1}^{2g(C)}\omega_j = 2g(C)q.$$

This together with the fact that $|\omega_j| = q$ forces each $\omega_j = -q$ and the result follows. □

Theorem 7.2.7. *Any algebraic curve over $\mathbb{F}_{q^2}$ that is covered by an $\mathbb{F}_{q^2}$-maximal curve is maximal itself.*

Proof. See [22, Theorem 5.2.1]. □

Lemma 7.2.8. *Let $k = \mathbb{F}_{p^2}$ be a field of characteristic $p \equiv -1 \mod 6$ and let C/k be the smooth projective curve given by the affine equation $s^6 = t^{p+1}+1$. The curve C is an $\mathbb{F}_{p^2}$-maximal curve.*

Proof. We will perform an explicit point counting on the curve C/k. From the genus calculation in the proof of Lemma 7.2.3 we know that C has 6 points at infinity all of which are defined over k. So we just look at the affine equation $s^6 = t^{p+1}+1$ over k. First note that for $t = 0$ we get 6 points and for $t^{p+1} = -1$ we get $p+1$ points. For the remainder assume that $t^{p+1} \notin \{0,-1\}$. As $t^{p+1} = t\bar{t} \in \mathbb{F}_p$ for any $t \in \mathbb{F}_{p^2}$ we find that we need $s \in \mathbb{F}_{p^2}$ and $s^6 \in \mathbb{F}_p$. This is precisely the condition that $s^{6(p-1)} = 1$ and there are $6(p-1)$ such s. Now 6 of these s's satisfy $s^6 = 1$ namely the ones corresponding to $t = 0$. The other $6p-12$ such s satisfy that $s^6-1 = t^{p+1}$ runs through $\mathbb{F}_p^\times$. In particular for any such s we get $p+1$ associated t's. We conclude that $|C(k)| = 6+6+(p+1)+(6p-12)(p+1) = 6p^2-5p+1$, which is precisely the Hasse-Weil upper bound. □

An alternative argument goes as follows. The curve C is covered by the Hermitian curve $\mathcal{H}_p\colon X^{p+1} + Y^{p+1} + 1 = 0$ via $(X, Y) \mapsto (s = iX^{(p+1)/6}, t = Y)$, where $i \in k$ is such that $i^2 = -1$. The curve $\mathcal{H}_p$ is k-maximal, so Theorem 7.2.7 then implies that C/k is k-maximal.

It follows from Theorem 7.2.6 that $Z(C/k;T) = \frac{(1+pT)^{5(p-1)}}{(1-T)(1-p^2T)}$. From Theorem 7.2.1 it now follows that $h = 5(p-1)$ and hence the rank of $E_{p+1}(\mathbb{F}_{p^2}(C))$ equals $10(p-1)$. It remains to find the rank of $E_{p+1}(\mathbb{F}_{p^2}(t))$ and we will deduce this from the rank of $E_{p+1}(\mathbb{F}_{p^2}(C))$. We will follow the same method as described in Section 5.3.

The field $k(C)$ has an order 6 automorphism σ defined by $s \mapsto \zeta_6 s$ and $t \mapsto t$. This induces an order 6 automorphism on $E_{p+1}(k(C))$ via the coordinate-wise action $P \mapsto P^\sigma$ (cf. Section 5.3). We can make the abelian group $E_{p+1}(k(C))$ into a $\mathbb{Q}$-vector space V by tensoring it with $\mathbb{Q}$, i.e.

$$V \coloneqq E_{p+1}(k(C)) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We now claim that V is also a $\mathbb{Q}(\zeta_6)$-vector space. Indeed, the natural action of ζ_6 on $E_{p+1}(k(C))$ given by $\zeta_6 \cdot (x, y) \coloneqq (\zeta_6^2 x, -y)$ gives V the structure of a $\mathbb{Q}(\zeta_6)$-vector space. The automorphism σ extends to a $\mathbb{Q}$-linear map σ_V on V and a quick check reveals that $\sigma(\zeta_6 \cdot (x, y)) = \zeta_6 \cdot \sigma(x, y)$ so that σ_V is in fact a $\mathbb{Q}(\zeta_6)$-linear map of order 6 on V. As all the eigenvalues of σ_V lie in $\mathbb{Q}(\zeta_6)$ we get that V decomposes as a direct sum

$$V = \sum_{i=0}^{5} V_{\zeta_6^i},$$

where $V_{\zeta_6^i}$ denotes the eigenspace of σ_V corresponding to the eigenvalue ζ_6^i. We investigate these eigenspaces one by one. In order to do so write a point $P \in E_{p+1}(k(C)) \setminus \{\mathcal{O}\}$ as

$$P = (\alpha_0 + \alpha_1 s + \alpha_2 s^2 + \alpha_3 s^3 + \alpha_4 s^4 + \alpha_5 s^5, \beta_0 + \beta_1 s + \beta_2 s^2 + \beta_3 s^3 + \beta_4 s^4 + \beta_5 s^5),$$

where each $\alpha_i, \beta_i \in k(t)$ and note that $E_{p+1}(k(C))$ is torsion-free as the corresponding elliptic surface has only type II fibers (cf. Example 2.5.17).

- (The eigenspace V_1) As $E_{p+1}(k(C))$ is torsion-free it follows that $P \otimes r$ lies in V_1 if and only if $P^\sigma = \zeta_6^0 \cdot P = P$ (cf. the proof of Lemma 5.3.1), with

$$\begin{aligned} P^\sigma = (&\alpha_0 + \alpha_1\zeta_6 s + \alpha_2\zeta_6^2 s^2 + \alpha_3\zeta_6^3 s^3 + \alpha_4\zeta_6^4 s^4 + \alpha_5\zeta_6^5 s^5, \\ &\beta_0 + \beta_1\zeta_6 s + \beta_2\zeta_6^2 s^2 + \beta_3\zeta_6^3 s^3 + \beta_4\zeta_6^4 s^4 + \beta_5\zeta_6^5 s^5). \end{aligned}$$

  Comparing coefficients we see that such a point P must be of the form $(\alpha_0, \beta_0) \in E_{p+1}(k(C))$ with $\alpha_0, \beta_0 \in k(t)$. I.e., we look for $k(t)$-rational points on the curve $E_{V_1}\colon y^2 = x^3 + 1$. These corresponds precisely to $E_{V_1}(k)$, which is finite. We conclude that the eigenspace $V_1 = \{0\}$ and does not contribute to the rank.

- (The eigenspace V_{-1}) Here we find that a point P must be of the form $P = (\alpha_0, \beta_3 s^3)$. I.e., we look for $k(t)$-rational points on the curve $E_{V_{-1}}\colon fy^2 = x^3 + 1$ where $f \coloneqq t^{p+1} + 1$. The elliptic curve $E_{V_{-1}}$ is isomorphic to the elliptic curve $y^2 = x^3 + f^3$. We claim that the latter has rank $2p - 2$ over $k(t)$. Indeed, define the algebraic curve $C_{-1}\colon s^2 = t^{p+1} + 1$. This curve has genus $(p-1)/2$ and in a similar fashion as before we find via zeta functions that $\mathrm{Mor}_k(C_{-1}, E_0)$ has rank $2p - 2$. The function field $k(C_{-1})$ has an automorphism determined by $s \mapsto s\zeta_6^3 = -s$. After tensoring with $\mathbb{Q}$ we can once again decompose this into eigenspaces. The $+1$-eigenspace is trivial. The -1-eigenspace corresponds precisely to the $k(t)$-rational points on the curve $y^2 = x^3 + f^3$. We conclude that the eigenspace V_{-1} has dimension $2p - 2$ over $\mathbb{Q}$.

- (The eigenspaces $V_{\zeta_6^2}$ and $V_{\zeta_6^4}$). In this case we look for the $k(t)$-rational points on the curves $E_{V_{\zeta_6^2}}\colon y^2 = x^3 + f^4$ and $E_{V_{\zeta_6^4}}\colon y^2 = x^3 + f^2$ respectively. Define the curve $\mathcal{D}\colon s^3 = t^{p+1} + 1$, which has genus $p - 1$ so that $\mathrm{Mor}_k(\mathcal{D}, E_0)$ has rank $4p - 4$. Tensoring with $\mathbb{Q}$ and decomposing this vector space using the automorphism $s \mapsto \zeta_6^2 s$ we see that we precisely end up looking for the $k(t)$-rational points on $E_{V_{\zeta_6^2}}$ and $E_{V_{\zeta_6^4}}$. This means that the eigenspaces $V_{\zeta_6^2}$ and $V_{\zeta_6^4}$ together have dimension $4p - 4$ over $\mathbb{Q}$.

- (The eigenspaces V_{ζ_6} and $V_{\zeta_6^5}$). In this case we look for the $k(t)$-rational points on the curves $E_{V_{\zeta_6}}\colon y^2 = x^3 + f^5$ and $E_{V_{\zeta_6^5}}\colon y^2 = x^3 + f$ respectively. We claim that these elliptic curves have the same rank over $k(t)$. To see this consider the Frobenius map $\phi\colon E_{V_{\zeta_6^5}} \to E^{(p)}_{V_{\zeta_6^5}}$ given by $(x, y) \mapsto (x^p, y^p)$, where $E^{(p)}_{V_{\zeta_6^5}}\colon y^2 = x^3 + f^p$. We can write $p = 6l - 1$ and by substituting $y = f^{-3l}y$, $x = f^{-2l}x$ we find that $E^{(p)}_{V_{\zeta_6^5}}$ is isomorphic to the elliptic curve given by equation $y^2 = x^3 + 1/f$, which is isomorphic to $E_{V_{\zeta_6}}$. We conclude that $E_{V_{\zeta_6^5}}$ and $E_{V_{\zeta_6}}$ are $k(t)$-isogenous elliptic curves, implying that they have the same rank.

Remark 7.2.9. *A similar argument using the Frobenius map for the eigenspaces $V_{\zeta_6^2}$ and $V_{\zeta_6^4}$ shows that they have the same rank as well.*

We conclude that the vector space V decomposes into 6 pieces. Five of them have dimension $2p - 2$ and one of them is trivial. This implies that the rank of $E_{p+1}(k(t))$ equals $\dim_{\mathbb{Q}}(V_{\zeta_6^5}) = 2p - 2$ and by Corollary 2.3.13 we find that the rank of $E_{p+1}(\mathbb{F}_p(t)) = p - 1$. This finishes the proof of Theorem 7.1.2.

Remark 7.2.10. *The rank over $\bar{\mathbb{F}}_p(t)$ equals $2p - 2$ as well. Indeed, if it were strictly bigger, then the Picard number of the corresponding surface would not be bounded by the second Betti number anymore, a contradiction (cf. Theorem 2.5.26).*

Remark 7.2.11. *Theorem 7.1.2 implies that the rank of the elliptic curve*

$$E_{360}\colon y^2 = x^3 + t^{360} + 1$$

over $\mathbb{F}_{359}(t)$ is 358. This is much higher than 68 and it shows that map (3.2) is not surjective in general.

We would like to end this section with a quick analysis of E_{360} over $\mathbb{F}_{359}(t)$. In this case we can not perform a vector space decomposition as in Section 5.3 over $\mathbb{F}_{359}(t)$. However, we can do this over $\mathbb{F}_q(t)$ with $q = 359^2 = 128881$. Using Magma (see Listings 10, 11 and 12) we see that we obtain 60 independent sections from base changes of rational elliptic surfaces and (at least) 8 independent sections coming from the usual $K3$. Together with Remark 7.2.10 this shows that all the independent sections in characteristic zero exist and remain independent over $\mathbb{F}_{359^2}$, but only half of them exist over $\mathbb{F}_{359}$ due to Corollary 2.3.13.

8 Discussion & Further Developments

In this thesis we have found several prime numbers p so that Shioda's rank 68 example of an elliptic curve over $\bar{\mathbb{Q}}(t)$ has rank 68 over $\mathbb{F}_p(t)$ after reduction modulo p. In particular, we have found 5 prime numbers so that the 68 independent points on the elliptic curve

$$E_{360}\colon y^2 = x^3 + t^{360} + 1$$

over $\bar{\mathbb{Q}}(t)$ reduce to points defined over the field $\mathbb{F}_p(t)$, and moreover remain independent over $\mathbb{F}_p(t)$. These primes are: $p = 44460001$, $p = 96614641$, $p = 133773121$, $p = 177452641$ and $p = 206869681$. The method used for finding these 5 primes is very much akin to that of the characteristic 0 case as found in [3]. In fact, for primes $p \equiv 1 \mod 6$, the method used there completely carries over to the field $\mathbb{F}_p(t)$. A vector space decomposition of the $\mathbb{Q}(\zeta_6)$-vector space $E_{360}(\mathbb{F}_p(t)) \otimes_{\mathbb{Z}} \mathbb{Q}$ yields 60 independent points coming from a base change of rational elliptic surfaces. Via a base change from an elliptic $K3$ surface we got 8 extra independent points and Shioda's algorithm gave an upper bound of 68 for the rank.

This is in stark contrast with primes p congruent to -1 modulo 6, as no such decomposition over $\mathbb{F}_p(t)$ is possible. However, in this case high rank is obtained by analysing a family of elliptic curves depending on the prime p related to certain maximal curves. In fact, via zeta functions of curves over finite fields and a corollary of the Tate conjecture we have shown that

$$E_{p+1}\colon y^2 = x^3 + t^{p+1} + 1$$

has rank $2p - 2$ over $\mathbb{F}_{p^2}(t)$ and rank $p - 1$ over $\mathbb{F}_p(t)$. The former result was already known by Schütt and Shioda ([19, Theorem 13.42]), where they use crystalline cohomology. Our proof is mainly based

on the Tate conjecture for abelian varieties over finite fields, and hence more elementary. Moreover, we extended their result to the rank over $\mathbb{F}_p(t)$.

In particular, the above shows that for $p = 359$ the rank of $E_{360}(\mathbb{F}_p(t))$ is 358. This is significantly higher than the rank we found over $\mathbb{F}_p(t)$ for primes congruent to 1 modulo 6. However, for $p = 359$ only half of the sections in the characteristic zero case reduce to sections over $\mathbb{F}_{359}$. For all the 68 sections in characteristic 0 to exist after reduction modulo 359 we have to consider the base field $\mathbb{F}_{359^2}$.

There are several questions that remain unanswered. To name a few:

(1) What is the rank of the subgroup $H \subset E_{p+1}(\mathbb{F}_{p^2}(t))$, which is generated by sections arising from unitary matrices (see Section 7.1)?;

(2) For which primes $p \equiv 1 \mod 6$ does the elliptic $K3$ surface with equation

$$y^2 = x^3 + (t^2 - 4)^3(t^5 - 5t^3 - 5t)$$

attain Mordell-Weil rank 8 over $\mathbb{F}_p$ (see Section 6.2)?;

(3) What is the rank of the elliptic curve E_{360} over $\mathbb{Q}(t)$?;

(4) What is the degree of the smallest field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ for which the elliptic curve E_{360} has rank 68 over $\mathbb{Q}(\alpha, t)$?;

(5) What is a general formula for the rank of $E_{360}(\mathbb{F}_p(t))$ for any prime $p > 3$?

All of them are interesting in their own right. Question (1), (2) and (3) seem to be solvable in a reasonable time frame. In fact, in Appendix B we made a start answering question (3). Questions (4) and (5) on the other hand seems rather hard to answer, and it would be interesting to see them solved in the future.

A A Basis of Regular 1-Forms on a Certain Curve

This section contains a computation of a basis for the space of regular differentials $H^0\left(C, \Omega^1_{C/k}\right)$ of the curve $C\colon s^6 = t^{p+1} + 1$ over $k = \mathbb{F}_{p^2}$ with $p \equiv -1 \mod 6$ (first appearing in Section 7.2). This was not needed in order to compute any ranks, however such computations seem to be lacking in the literature. Therefore we decided to include such computation in the appendix.

Lemma A.0.1. *Consider the algebraic curve $C\colon s^6 = t^{p+1} + 1$ over $k = \mathbb{F}_{p^2}$ with $p \equiv -1 \mod 6$, write $p + 1 = 6l$ for some integer l and let $\zeta_6 \in k$ be a primitive 6^{th} root of unity. Let $A, B \in \mathbb{Z}$, then the differential $t^A s^B dt$ is in $H^0\left(C, \Omega^1_{C/k}\right)$ if and only if the pair $(A, B) \in \mathbb{Z}^2$ satisfies*

$$\begin{cases} A \geq 0 \\ B \geq -5 \\ -lB - A - 2 \geq 0. \end{cases}$$

In particular, such regular differentials form a basis for $H^0\left(C, \Omega^1_{C/k}\right)$ of cardinality $5(3l-1) = 5(p-1)/2 = g(C)$.

Proof. Take the element $t \in k(C)$ and note that this function vanishes at the points $P_i \coloneqq (\zeta_6^i, 0)$ for $i = 0, \dots 5$. Moreover, we recall from the proof of 7.2.3 that we have 6 points $\mathcal{O}_0, \dots, \mathcal{O}_5$ at infinity for the curve C. This means that the divisor of t is given by $\operatorname{div}(t) = \sum_{i=0}^{5}(P_i) - \sum_{j=0}^{5}(\mathcal{O}_j)$. Consider the differential 1-form dt. The function $1/t$ is a uniformizer at the points $\mathcal{O}_j$ and we find $d(1/t) = -1/t^2 dt$, so dt has poles of order 2 at the points at infinity and no other poles. Recall from Lemma 7.2.3 that the map $f\colon C \to \mathbb{P}^1$ sending $(s, t) \mapsto (t : 1)$, i.e. the function $t \in k(C)$, ramifies above the points with $t^{6l} + 1 = 0$. The ramification index at these points equals 6. There are precisely $6l$ such points and we call them $Q_n = (0, r_n)$, with $n = 1, \dots, 6l$ and r_n such that $r_n^{6l} = -1$. Note that all the points Q_n behaves in exactly the same way, so that

$$\operatorname{div}(dt) = a\sum_{n=1}^{6l}(Q_n) - 2\sum_{j=0}^{5}(\mathcal{O}_j)$$

where the integer a has to satisfy $6al - 12 = 5(p-1) - 2$, an equation coming from the general fact

$$\deg \operatorname{div}(dt) = 2g(C) - 2.$$

Solving this for a yields $a = 5$. In a similar fashion as how we found $\operatorname{div}(t)$, we quickly find that $\operatorname{div}(s) = \sum_{n=1}^{6l}(Q_n) - l\sum_{j=0}^{5}(\mathcal{O}_j)$.

Take integers $A, B \in \mathbb{Z}$ and consider the differential $\omega \coloneqq t^A s^B dt$. The only possibilities where ω has zeros or poles are at the points $\mathcal{O}_j, Q_n$ or P_i. At each $\mathcal{O}_j$ we find multiplicity $-lB - A - 2$, at each Q_n we get multiplicity $B + 5$ and at each P_i we get multiplicity A. In order for ω to be regular we find that we need the following conditions on A and B:

$$\begin{cases} A \geq 0 \\ B \geq -5 \\ -lB - A - 2 \geq 0. \end{cases} \tag{A.1}$$

Solving this system, i.e. counting the points with integer coordinates in this triangle, yields the desired result.

□

B Towards the Rank Of $E_{360}(\mathbb{Q}(t))$

Throughout this thesis we have proven that the rank of the elliptic curve

$$E_{360}\colon y^2 = x^3 + t^{360} + 1$$

over $\mathbb{Q}(t)$ has Mordell-Weil rank at most 34 (see Lemma 3.0.1). One can actually reduce this bound using the following remarks:

(a) The vector space decomposition as done in Section 5.3 can be done over $\mathbb{Q}(\zeta_6, t)$ with $\zeta_6 \in \mathbb{C}$ a primitive sixth root of unity.

(b) Using (a) and some Galois theory we investigate the pieces corresponding to rational surfaces over $\mathbb{Q}(\zeta_6)$ and try to determine their Mordell-Weil rank.

Theorem B.0.1. *The Mordell-Weil rank of the rational elliptic surface over $\mathbb{Q}(\zeta_6)$ defined by equation*

$$E_{2,2}\colon y^2 = x^3 + t^4 + t^2$$

is equal to 0.

Proof. We use the polynomial $G_{2,2} = 4z^3 - 1$ obtained in Section 6.1. Let α be a root of this polynomial and consider the extension $\mathbb{Q}(\zeta_6) \subset \mathbb{Q}(\zeta_6, \alpha)$. This is a degree 3 Galois extension with Galois group G generated by the automorphism $\sigma\colon \alpha \mapsto \zeta_6^2\alpha$. Using Magma we find 4 independent points in $E_{2,2}\left(\mathbb{Q}(\zeta_6, \alpha, t)\right)$, namely $P_1 = (\alpha, t^2 + 1/2)$, $P_2 = (\zeta_6^2\alpha, t^2 + 1/2)$, $Q_1 = (\alpha t^2, t^3/2 + t)$ and $Q_2 = (\zeta_6^2\alpha t^2, t^3/2 + t)$. In particular, we find that $\langle P_1, P_2, Q_1, Q_2\rangle \subset E_{2,2}\left(\mathbb{Q}(\zeta_6, \alpha, t)\right)$ generates subgroup of rank 4, which is precisely the geometric Mordell-Weil rank. Denote $V \coloneqq E_{2,2}\left(\mathbb{Q}(\zeta_6, \alpha, t)\right) \otimes_{\mathbb{Z}} \mathbb{C}$ a complex 4-dimensional vector space. The Galois group G acts on V in the usual way giving a representation $\rho\colon G \to GL(V)$. The image of σ under ρ, using the basis obtained from the points P_1, P_2 , Q_1 and Q_2, corresponds to the matrix

$$M \coloneqq \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Denote $W \coloneqq E_{2,2}\left(\mathbb{Q}(\zeta_6, t)\right) \otimes_{\mathbb{Z}} \mathbb{C}$ which is precisely the subspace of V given by $\{P \in V\colon \rho(\sigma)P = P\} \subset V$. The eigenvalues λ of M satisfy $\lambda^2 + \lambda + 1 = 0$. In particular, 1 is not an eigenvalue implying that $W = \{0\}$. In other words, the rank of $E_{2,2}\left(\mathbb{Q}(\zeta_6, t)\right)$ is zero, as desired. □

Corollary B.0.2. *The rank of $E_{360}(\mathbb{Q}(t))$ is bounded above by* 32.

Proof. This follows immediately from Theorem B.0.1 and Lemma 3.0.1. □

It is possible to repeat the process outlined above for all rational elliptic surfaces and the elliptic $K3$ surface found in Section 6.1. The surfaces with low geometric Mordell-Weil rank (such as 2 or 4) are relatively easy to study. However, when the surface has geometric Mordell-Weil rank 6 or 8, this method becomes computationally challenging as it requires finding independent sections on the surface and understanding the Galois group of the corresponding field extension. This group can become complex when the degree of the extension is high. We decided not to investigate this further due to a lack of time.

C Magma Code

The next piece of code computes prime numbers p so that all the polynomials appearing in Section 6.2 have a root modulo p.

```
P<z> := PolynomialRing(Integers());
/*We first define all the polynomials of which we know we need roots*/
G50 := 583200000*z^40 + 2176717249713600000*z^30 + 56473225380000*z^20 - 135432000*z^10 + 1;
G51 := 5*z^8 + 360*z^6 - 1350*z^4 + 729;
G211 := 3*z^4 + 6*z^2-1;
G212 := 4096*z^8 + 12597120*z^4 - 14348907;
G311 := 8*z^9 - 4*159*z^6 + 21*8*z^3 + 1;
G312 := 8*z^9 + 159*4*z^6 + 21*8*z^3 - 1;
G41 := 256*z^32 + 256*26480951*z^24 + 32*772048803*z^16 + 16*26480951*z^8 + 1;
G32 := 1259712*z^18 + 69984*1229*z^12 + 324*8371*z^6 + 1;
G232 := 9*z^8 - 18*z^6 + 39*z^4 + 6*z^2 + 1;
G233 := z^8 + 18*z^4 - 27;
G22 := 4*z^3 - 1;
G1011 := 25*z^16 - 25*11340*z^12 - 5*240842*z^8 -25*2268*z^4 + 1;
G1012 := 13286025*z^16 - 164025*28*z^12 + 5*235718*z^8 - 45*28*z^4 + 1;
G1023 := 10485760000*z^32 + 796262400000*z^28 + 28673969152000*z^24 + 5919441120000*z^20 +
    569262158025*z^16 - 18498253500*z^12 + 280019230*z^8 - 24300*z^4 + 1;

/*We iterate over all the primes.*/
for i in [1..100000000] do
  n := NthPrime(i);
  /*We check if the prime is 1 modulo 720.*/
  if n mod 720 ne 1 then
    /*We continue to the next iteration in the for loop if the prime is NOT 1 modulo 720.*/
    continue;
  end if;
  /*We define a polynomial ring over the finite field F_p so that we can reduce our polynomials
    modulo p.*/
  Pn<z> := PolynomialRing(GF(n));
  /*We reduce G50 modulo p and check if it has a root.*/
  Ln50 := Pn! G50;
  Bool50,b50 := HasRoot(Ln50);
  if Bool50 eq false then
    /*If is has no root we continue to the next iteration in the for loop.*/
    continue;
  end if;
  /*Once we are here we know G50 has root mod p. We can define a new polynomial using this root
    and
  check if it has a root.*/
  G501 := Pn! z^3 - (b50)^2;
  if HasRoot(G501) eq false then
    continue;
  end if;
  /*We repeat the above process for all the polynomials and iterated roots we need.*/
  Ln51 := Pn! G51;
  Bool51,b51 := HasRoot(Ln51);
  if Bool51 eq false then
    continue;
  end if;

  G511 := Pn! z^3 - b51^2+1;
  if HasRoot(G511) eq false then
    continue;
  end if;

  Ln311 := Pn! G311;
  Bool311,b311 := HasRoot(Ln311);
```

```
  if Bool311 eq false then
    continue;
  end if;

  G3111 := Pn! z^3 - b311^2;
  if HasRoot(G3111) eq false then
    continue;
  end if;

  printf "Test 1: the prime %o has a chance; ~ i = %o \n",n,i;
  Ln312 := Pn! G312;
  Bool312,b312 := HasRoot(Ln312);
  if Bool312 eq false then
    continue;
  end if;

  G3121 := Pn! z^3 - b312^2;
  if HasRoot(G3121) eq false then
    continue;
  end if;

  Ln41 := Pn! G41;
  Bool41,b41 := HasRoot(Ln41);
  if Bool41 eq false then
    continue;
  end if;

  G411 := Pn! z^3 - b41^2;
  if HasRoot(G411) eq false then
    continue;
  end if;

  printf "Test 2: the prime %o has a greater chance; ~ i = %o \n",n,i;
  Ln32 := Pn! G32;
  Bool32,b32 := HasRoot(Ln32);
  if Bool32 eq false then
    continue;
  end if;

  G321 := Pn! z^3 - (b32)^2;
  if HasRoot(G321) eq false then
    continue;
  end if;

  Ln211 := Pn! G211;
  if HasRoot(Ln211) eq false then
    continue;
  end if;

  Ln212 := Pn! G212;
  if HasRoot(Ln212) eq false then
    continue;
  end if;

  Ln232 := Pn! G232;
  if HasRoot(Ln232) eq false then
    continue;
  end if;

  Ln233 := Pn! G233;
  if HasRoot(Ln233) eq false then
```

```
    continue;
  end if;

  printf "Test 3: the prime %o comes really close! ~ i = %o \n",n,i;
  Ln22 := Pn! G22;
  if HasRoot(Ln22) eq false then
    continue;
  end if;

  Ln1011 := Pn! G1011;
  if HasRoot(Ln1011) eq false then
    continue;
  end if;

  Ln1012 := Pn! G1012;
  if HasRoot(Ln1012) eq false then
    continue;
  end if;

  Ln1023 := Pn! G1023;
  if HasRoot(Ln1023) eq false then
    continue;
  end if;
  /*Once we are here we know that we all the roots we need and we print n.*/
  printf "The prime %o works! ~ i = %o \n",n,i;
end for;
```

Listing 4: Computing Primes Which Yield High Rank.

The next piece of code computes the part of the rank of $E_{360}(\mathbb{F}_{44460001}(t))$ that is obtained by base changing from rational elliptic surfaces.

```
p := 44460001;
K := GF(p);
L<t> := FunctionField(K);

/*We define all the elliptic curves that corresponds to rational elliptic surfaces in our
    decomposition*/
E50 := EllipticCurve([0,t^5+1]);
E13 := EllipticCurve([0,t^3*(t+1)]);
E101 := EllipticCurve([0,t^5 - 5*t^3 + 5*t]);
E51 := EllipticCurve([0,t*(t^5+1)]);
E12 := EllipticCurve([0,t^2*(t+1)]);
E23 := EllipticCurve([0,t^3*(t^2+1)]);
E22 := EllipticCurve([0,t^2*(t^2+1)]);
E21 := EllipticCurve([0,t*(t^2+1)]);
E31 := EllipticCurve([0,t*(t^3+1)]);
E41 := EllipticCurve([0,t*(t^4+1)]);
E32 := EllipticCurve([0,t^2*(t^3+1)]);

/*We compute their Mordell-Weil group*/
G50,m50 := MordellWeilGroup(E50);
G13,m13 := MordellWeilGroup(E13);
G101,m101 := MordellWeilGroup(E101);
G51,m51 := MordellWeilGroup(E51);
G12,m12 := MordellWeilGroup(E12);
G23,m23 := MordellWeilGroup(E23);
G22,m22 := MordellWeilGroup(E22);
G21,m21 := MordellWeilGroup(E21);
G31,m31 := MordellWeilGroup(E31);
G41,m41 := MordellWeilGroup(E41);
G32,m32 := MordellWeilGroup(E32);

/*We compute their ranks*/
r50 := TorsionFreeRank(G50);
r13 := TorsionFreeRank(G13);
r101 := TorsionFreeRank(G101);
r51 := TorsionFreeRank(G51);
r12 := TorsionFreeRank(G12);
r23 := TorsionFreeRank(G23);
r22 := TorsionFreeRank(G22);
r21 := TorsionFreeRank(G21);
r31 := TorsionFreeRank(G31);
r41 := TorsionFreeRank(G41);
r32 := TorsionFreeRank(G32);

/*We sum their ranks to get a lower bound for the rank of E360(Fp(t))*/
LBRank := r50 + r13 + r101 + r51 + r12 + r23 + r22 + r21 + r31 + r41 + r32;
LBRank;
```

Listing 5: Lower Bound of 60 Using Rational Surfaces for the Prime 44460001.

The next piece of code computes whether the points found on the elliptic curve

$$y^2 = x^3 + (t^2 - 4)^3(t^5 - 5t^3 + 5t)$$

over $\mathbb{F}_{44460001}(t)$ are independent.

```
K := GF(44460001);
L<t> := FunctionField(K);

/*We define our elliptic K3 surface*/
E := EllipticCurve([0,(t^2-4)^3*(t^5 - 5*t^3 + 5*t)]);

/*We define our points that we found in a matrix.
Each row consists of an array of the form [a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6],
which corresponds to a point x = a0 + ... a4*t^4, y = b0 + ... b6*t^6.*/
X := Matrix(K, 8, 12, [298182, 30824910, 18189043, 8984250, 33116893, 18401627, 40901717,
    27724783, 22118594, 21200495, 29597123, 27118537,
            1639614, 12739358, 26058296, 39263511, 8996056, 17109065, 34957848, 1776259,
    14219251, 21965827, 16744422, 26872802,
            2081116, 16450118, 144746, 13740882, 13419981, 3687933, 27478375, 36065591,
    7749320, 2122377, 31095808, 31254454,
            4982545, 17978612, 39985989, 36174083, 38622024, 38908857, 1657775, 43864532,
    33378226, 23935301, 37178456, 35760240,
            5784117, 4377759, 18649150, 17657829,37501795, 38210606, 22150682, 14671060,
    37972614, 909232, 31369696, 37303844,
            8732268, 9683578, 22032164, 2637656,1802138, 23925728, 29919562, 35245090,
    27344842, 34561779, 6752832, 24221212,
            9443293, 16319437, 25518972, 44233011,1008487, 33455589, 24706356, 43659670,
    36057833, 30978518, 37551194, 25295739,
            10222816, 11502968, 42548665, 24386966,35056860, 38210606, 22150682, 14671060,
    37972614, 909232, 31369696, 37303844]);

/*Define the points on E:*/
x1 := X[1,1] + X[1,2]*t + X[1,3]*t^2 + X[1,4]*t^3 + X[1,5]*t^4;
y1 := X[1,6] + X[1,7]*t + X[1,8]*t^2 + X[1,9]*t^3 + X[1,10]*t^4 + X[1,11]*t^5 + X[1,12]*t^6;
P1 := E![x1,y1];

x2 := X[2,1] + X[2,2]*t + X[2,3]*t^2 + X[2,4]*t^3 + X[2,5]*t^4;
y2 := X[2,6] + X[2,7]*t + X[2,8]*t^2 + X[2,9]*t^3 + X[2,10]*t^4 + X[2,11]*t^5 + X[2,12]*t^6;
P2 := E![x2,y2];

x3 := X[3,1] + X[3,2]*t + X[3,3]*t^2 + X[3,4]*t^3 + X[3,5]*t^4;
y3 := X[3,6] + X[3,7]*t + X[3,8]*t^2 + X[3,9]*t^3 + X[3,10]*t^4 + X[3,11]*t^5 + X[3,12]*t^6;
P3 := E![x3,y3];

x4 := X[4,1] + X[4,2]*t + X[4,3]*t^2 + X[4,4]*t^3 + X[4,5]*t^4;
y4 := X[4,6] + X[4,7]*t + X[4,8]*t^2 + X[4,9]*t^3 + X[4,10]*t^4 + X[4,11]*t^5 + X[4,12]*t^6;
P4 := E![x4,y4];

x5 := X[5,1] + X[5,2]*t + X[5,3]*t^2 + X[5,4]*t^3 + X[5,5]*t^4;
y5 := X[5,6] + X[5,7]*t + X[5,8]*t^2 + X[5,9]*t^3 + X[5,10]*t^4 + X[5,11]*t^5 + X[5,12]*t^6;
P5 := E![x5,y5];

x6 := X[6,1] + X[6,2]*t + X[6,3]*t^2 + X[6,4]*t^3 + X[6,5]*t^4;
y6 := X[6,6] + X[6,7]*t + X[6,8]*t^2 + X[6,9]*t^3 + X[6,10]*t^4 + X[6,11]*t^5 + X[6,12]*t^6;
P6 := E![x6,y6];

x7 := X[7,1] + X[7,2]*t + X[7,3]*t^2 + X[7,4]*t^3 + X[7,5]*t^4;
y7 := X[7,6] + X[7,7]*t + X[7,8]*t^2 + X[7,9]*t^3 + X[7,10]*t^4 + X[7,11]*t^5 + X[7,12]*t^6;
P7 := E![x7,y7];

x8 := X[8,1] + X[8,2]*t + X[8,3]*t^2 + X[8,4]*t^3 + X[8,5]*t^4;
```

```
y8 := X[8,6] + X[8,7]*t + X[8,8]*t^2 + X[8,9]*t^3 + X[8,10]*t^4 + X[8,11]*t^5 + X[8,12]*t^6;
P8 := E![x8,y8];

/*We check whether they are independent*/
IsLinearlyIndependent([P1,P2,P3,P4,P5,P6,P7,P8]);
```

Listing 6: 8 Independent Points In $E_{K3}(\mathbb{F}_{44460001}(t))$.

The next piece of code uses Shioda's algorithm to compute an upper bound for the rank of $E_{360}(\mathbb{F}_{44460001}(t))$.

```
/*Global Variables:*/

/*We fix a prime number p = 1 mod 720.*/
p := 44460001;
/*Smallest element so that p^c*x_i = x_i is always 1 as p = 1 mod 720:*/
c := 1;
/*integers so that ord(x_i) = ord(t*x_i), note gcd(t,360) = 1: (pre-computed array)*/
CoprimeTArray := [1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79,
83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163,
167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229];

/*Functions used:*/

/*Computes rational numbers modulo integers.*/
ModZ := function(a)
  return -Floor(a) + a;
end function;

/*Computes the sum condition appearing in Bas Heine's thesis for c = 1.*/
Sumt := function(t,x)
  term1 := ModZ(t*p*x[1]);
  term2 := ModZ(t*p*x[2]);
  term3 := ModZ(t*p*x[3]);
  term4 := ModZ(t*p*x[4]);
  return term1 + term2 + term3 + term4;
end function;

/*Checks the nonzero condition in Bas's thesis*/
ZeroCheck := function(x)
  if ModZ(x[1]) eq 0 or ModZ(x[2]) eq 0 or ModZ(x[3]) eq 0 or ModZ(x[4]) eq 0 then;
    return false;
  else
    return true;
  end if;
end function;

/*Function that checks if a vector is definitely in the set Lambda. If bool = 1, then it is in
   Lambda. If bool = 0, then it might still be in Lambda
and we might have to search further by increasing CoprimeTArray*/
IsDefInLambda := function(x)
  bool := 0;
  for t in CoprimeTArray do;
    if Sumt(t,x) ne 2*c then;
      bool := 1;
    end if;
  end for;
  return bool;
end function;

/*We can exclude i = 0, as then the coefficients are zero*/
LBSizeLambda := 0;
for i in [1..359] do;
  x_i := [(60+i)/360,-i/360,1/3,1/2];
  z_i := [(i-420)/360,-i/360,2/3,1/2];

  if ZeroCheck(x_i) eq true then;
    /*We check if x_i is in the set Lambda*/
    if IsDefInLambda(x_i) eq 1 then;
      LBSizeLambda := LBSizeLambda + 1;
```

```
    else
      print(x_i);
    end if;
  end if;

  if ZeroCheck(z_i) eq true then;
    /*We check if z_i is in the set Lambda*/
    if IsDefInLambda(z_i) eq 1 then;
      LBSizeLambda := LBSizeLambda + 1;
    else
      print(z_i);
    end if;
  end if;
end for;

/*The vectors in the output might still be in the set Lambda, but using lower bounds for the
    rank this can be excluded.*/
/*Shioda-Tate gives an upperbound for the rank:*/
printf "For p = %o an upperbound for the rank of E_360(F_p(t)) is %o \n",p,716-LBSizeLambda;
```

Listing 7: Computing an Upper Bound for the Rank of $E_{360}(\mathbb{F}_{44460001}(t))$.

The next piece of code computes generators for the unitary group $\boldsymbol{U}(2, \mathbb{F}_{25})$.

```
p := 5;
K := GF(p);
R<x> := PolynomialRing(Integers());
f := x^2+x+1;
H<w> := ext<K|f>;
U := GU(2,H);
M := Matrix(H,2,2,[1,0,0,1]);
TransMat := TransformForm(M, "unitary");
UnitaryGroup := U^(TransMat^(-1));
Generators(UnitaryGroup);
```

Listing 8: Computing Generators for the Unitary Group Over $\mathbb{F}_{25}$.

The next piece of code computes whether the 8 points found in $E_6(\mathbb{F}_{25}(t))$ are independent.

```
p := 5;
K := GF(p);
R<x> := PolynomialRing(Integers());
f := x^2+x+1;
H<w> := ext<K|f>;
U := GU(2,H);
L<t> := FunctionField(H);
E := EllipticCurve([0,t^6+1]);
P := E![-1,t^3];
P1 := E![-w,t^3];
Q := E![-t^2,1];
Q1 := E![-w*t^2,1];
R := E![-(3*t + 3*w+2)^2,((2*w+3)*t + 2*w)^3];
R1 := E![-w*(3*t + 3*w+2)^2,((2*w+3)*t + 2*w)^3];
S := E![-((3*w+1)*t + 3*w+3)^2,((3*w)*t + 2*w+3)^3];
S1 := E![-w*((3*w+1)*t + 3*w+3)^2,((3*w)*t + 2*w+3)^3];
arrray := [P,P1,Q,Q1,R,R1,S1,S];
IsLinearlyIndependent(array);
```

Listing 9: 8 Independent Points In $E_6(\mathbb{F}_{25}(t))$.

The next piece of code computes the part of the rank of $E_{360}(\mathbb{F}_{359^2}(t))$ that is obtained by base changing from rational elliptic surfaces.

```
p := 359;
K := GF(p^2);
L<t> := FunctionField(K);

/*We define all the elliptic curves that corresponds to rational elliptic surfaces in our
    decomposition*/
E50 := EllipticCurve([0,t^5+1]);
E13 := EllipticCurve([0,t^3*(t+1)]);
E101 := EllipticCurve([0,t^5 - 5*t^3 + 5*t]);
E51 := EllipticCurve([0,t*(t^5+1)]);
E12 := EllipticCurve([0,t^2*(t+1)]);
E23 := EllipticCurve([0,t^3*(t^2+1)]);
E22 := EllipticCurve([0,t^2*(t^2+1)]);
E21 := EllipticCurve([0,t*(t^2+1)]);
E31 := EllipticCurve([0,t*(t^3+1)]);
E41 := EllipticCurve([0,t*(t^4+1)]);
E32 := EllipticCurve([0,t^2*(t^3+1)]);

/*We compute their Mordell-Weil group*/
G50,m50 := MordellWeilGroup(E50);
G13,m13 := MordellWeilGroup(E13);
G101,m101 := MordellWeilGroup(E101);
G51,m51 := MordellWeilGroup(E51);
G12,m12 := MordellWeilGroup(E12);
G23,m23 := MordellWeilGroup(E23);
G22,m22 := MordellWeilGroup(E22);
G21,m21 := MordellWeilGroup(E21);
G31,m31 := MordellWeilGroup(E31);
G41,m41 := MordellWeilGroup(E41);
G32,m32 := MordellWeilGroup(E32);

/*We compute their ranks*/
r50 := TorsionFreeRank(G50);
r13 := TorsionFreeRank(G13);
r101 := TorsionFreeRank(G101);
r51 := TorsionFreeRank(G51);
r12 := TorsionFreeRank(G12);
r23 := TorsionFreeRank(G23);
r22 := TorsionFreeRank(G22);
r21 := TorsionFreeRank(G21);
r31 := TorsionFreeRank(G31);
r41 := TorsionFreeRank(G41);
r32 := TorsionFreeRank(G32);

/*We sum their ranks to get a lower bound for the rank of E360(Fp(t))*/
LBRank := r50 + r13 + r101 + r51 + r12 + r23 + r22 + r21 + r31 + r41 + r32;
LBRank;
```

Listing 10: Lower Bound of 60 Using Rational Surfaces Over $\mathbb{F}_{359^2}$.

The next piece of code computes points in $E_{360}(\mathbb{F}_{359^2}(t))$.

```
p := 359;
K<b> := GF(p^2);
A<a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6> := AffineSpace(K,12);
S := CoordinateRing(A);
U<t> := PolynomialRing(S);
x := a0+a1*t+a2*t^2+a3*t^3+a4*t^4;
y := b0+b1*t+b2*t^2+b3*t^3+b4*t^4+b5*t^5+b6*t^6;
f := x^3+(t^2-4)^3*(t^5-5*t^3+5*t)-y^2;
I := ideal<S | Coefficients(f)>;
B := Scheme(A,I);
Points(B);
```

Listing 11: Finding Points on the K3 Surface Over $\mathbb{F}_{359^2}$.

The next piece of code computes whether the points found in $E_{360}(\mathbb{F}_{359^2}(t))$ are independent.

```
p := 359;
K<b> := GF(p^2);
L<t> := FunctionField(K);

/*We define our elliptic K3 surface*/
E := EllipticCurve([0,(t^2-4)^3*(t^5 - 5*t^3 + 5*t)]);

/*We define our points that we found in a matrix.
Each row consists of an array of the form [a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6],
which corresponds to a point x = a0 + ... a4*t^4, y = b0 + ... b6*t^6.*/
X := Matrix(K, 8, 12, [b^8520, b^103920, b^24000, b^70440, b^107880, b^12780, b^56700, b^40500,
    b^14940, b^123660, b^68220, b^32940,
            b^9600, b^9960, b^37320, b^117960, b^85920, 242, 327, 82, 331, 217, 311, 358,
            b^10866, b^107690, b^80704, b^62457, b^88762, b^16299, b^41635, b^11571, 240,b
    ^29318, b^23882, b^4263,
            b^12900, b^71400,b^47460, b^51960, b^29460, b^19350, b^44730, b^69390, b^110970, b
    ^41310,b^45450, b^108630,
            b^15548, b^77558,b^25274, b^68467, b^69188, b^23322, b^95674, b^17186, b^79984, b
    ^62815, b^84552,b^39342,
            b^30000, b^60960, b^45480,b^27480, b^480, 344, 216, 246, 250, 70, 229, 310,
            b^38766, b^10618,b^3643, b^33357, b^116662, b^122589, b^14918, b^48273, b^109967, b
    ^63487,b^33364, b^110553,
            b^61372, b^91162,b^73246, b^49493, b^115012, b^92058, b^97106, b^80194, b^6236, b
    ^93245, b^99588,b^43638
]);

/*Define the points on E:*/
x1 := X[1,1] + X[1,2]*t + X[1,3]*t^2 + X[1,4]*t^3 + X[1,5]*t^4;
y1 := X[1,6] + X[1,7]*t + X[1,8]*t^2 + X[1,9]*t^3 + X[1,10]*t^4 + X[1,11]*t^5 + X[1,12]*t^6;
P1 := E![x1,y1];

x2 := X[2,1] + X[2,2]*t + X[2,3]*t^2 + X[2,4]*t^3 + X[2,5]*t^4;
y2 := X[2,6] + X[2,7]*t + X[2,8]*t^2 + X[2,9]*t^3 + X[2,10]*t^4 + X[2,11]*t^5 + X[2,12]*t^6;
P2 := E![x2,y2];

x3 := X[3,1] + X[3,2]*t + X[3,3]*t^2 + X[3,4]*t^3 + X[3,5]*t^4;
y3 := X[3,6] + X[3,7]*t + X[3,8]*t^2 + X[3,9]*t^3 + X[3,10]*t^4 + X[3,11]*t^5 + X[3,12]*t^6;
P3 := E![x3,y3];

x4 := X[4,1] + X[4,2]*t + X[4,3]*t^2 + X[4,4]*t^3 + X[4,5]*t^4;
y4 := X[4,6] + X[4,7]*t + X[4,8]*t^2 + X[4,9]*t^3 + X[4,10]*t^4 + X[4,11]*t^5 + X[4,12]*t^6;
P4 := E![x4,y4];

x5 := X[5,1] + X[5,2]*t + X[5,3]*t^2 + X[5,4]*t^3 + X[5,5]*t^4;
y5 := X[5,6] + X[5,7]*t + X[5,8]*t^2 + X[5,9]*t^3 + X[5,10]*t^4 + X[5,11]*t^5 + X[5,12]*t^6;
```

```
P5 := E![x5,y5];

x6 := X[6,1] + X[6,2]*t + X[6,3]*t^2 + X[6,4]*t^3 + X[6,5]*t^4;
y6 := X[6,6] + X[6,7]*t + X[6,8]*t^2 + X[6,9]*t^3 + X[6,10]*t^4 + X[6,11]*t^5 + X[6,12]*t^6;
P6 := E![x6,y6];

x7 := X[7,1] + X[7,2]*t + X[7,3]*t^2 + X[7,4]*t^3 + X[7,5]*t^4;
y7 := X[7,6] + X[7,7]*t + X[7,8]*t^2 + X[7,9]*t^3 + X[7,10]*t^4 + X[7,11]*t^5 + X[7,12]*t^6;
P7 := E![x7,y7];

x8 := X[8,1] + X[8,2]*t + X[8,3]*t^2 + X[8,4]*t^3 + X[8,5]*t^4;
y8 := X[8,6] + X[8,7]*t + X[8,8]*t^2 + X[8,9]*t^3 + X[8,10]*t^4 + X[8,11]*t^5 + X[8,12]*t^6;
P8 := E![x8,y8];

/*We check whether they are independent*/
IsLinearlyIndependent([P1,P2,P3,P4,P5,P6,P7,P8]);
```

Listing 12: Finding Independent Sections on the K3 Surface Over $\mathbb{F}_{359^2}$.

D MatLab Code

All the MATLAB code below computes sections of the form $(gt^2 + at + b, ht^3 + ct^2 + dt + e)$ on certain rational elliptic surfaces.

```
syms g a b h c d e t; %These are the variables in Theorem 7.12 in Schutt-Shioda.
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
r1 = 5;
r2 = 0;
%Define the elliptic curve we are working with.
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
%Extract the coefficients with respect to t.
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
%Solve the system of equations arising.
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 13: Solving the Systems of Equations Arising From $E_{5,0}$.

```
syms g a b h c d e t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
r1 = 5;
r2 = 1;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 14: Solving the Systems of Equations Arising From $E_{5,1}$.

```
syms a b c d e f g t;
x = a*t;
y = c*t^2 + d*t;
r1 = 2;
r2 = 2;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
S = solve(v0 == 0, v1 == 0, v2 == 0);
```

Listing 15: Solving the Systems of Equations Arising From $E_{2,2}$.

```
syms g a b h c d e t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
r1 = 2;
r2 = 1;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 16: Solving the Systems of Equations Arising From $E_{2,1}$.

```
syms a b c d e t;
x = a*t + b;
y = c*t^2 + d*t + e;
r1 = 3;
r2 = 1;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0);
```

Listing 17: Solving the Systems of Equations Arising From $E_{3,1}$.

```
syms g a b h c d e t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
r1 = 4;
r2 = 1;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 18: Solving the Systems of Equations Arising From $E_{4,1}$.

```
syms a b c d e h g t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
r1 = 3;
r2 = 2;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0, v6 == 0);
```

Listing 19: Solving the Systems of Equations Arising From $E_{3,2}$.

```
syms a b c d t;
x = a*t^2 + b*t;
y = c*t^3 + d*t^2;
r1 = 2;
r2 = 3;
f = y^2 - x^3 - t^(r2)*(t^(r1) + 1);
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0);
```

Listing 20: Solving the Systems of Equations Arising From $E_{2,3}$.

```
syms g a b h c d e t;
x = g*t^2 + a*t + b;
y = h*t^3 + c*t^2 + d*t + e;
f = y^2 - x^3 - t^5 + 5*t^3 - 5*t;
C = coeffs(f, t);
v0 = C(1);
v1 = C(2);
v2 = C(3);
v3 = C(4);
v4 = C(5);
v5 = C(6);
v6 = C(7);
S = solve(v0 == 0, v1 == 0, v2 == 0, v3 == 0, v4 == 0, v5 == 0 ,v6 == 0);
```

Listing 21: Solving the System of Equations Arising From the Rational Part of $E_{10,1}$.

References

[1] Arnaud Beauville. *Complex Algebraic Surfaces*. London Mathematical Society Student Texts. Cambridge University Press, 2nd edition, 1996.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Jasbir Chahal, Matthijs Meijer, and Jaap Top. Sections on Certain $j = 0$ Elliptic Surfaces, 1999.

[4] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[5] Daniel Coray and Constantin Manoil. On Large Picard Groups and the Hasse Principle for Curves and K3 Surfaces. *Acta Arithmetica*, 76(2):165–189, 1996.

[6] Claus Diem and Jasper Scholten. Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant. II. *J. Number Theory*, 124(1):31–41, 2007.

[7] William Fulton. Algebraic Curves: An Introduction To Algebraic Geometry, 2008.

[8] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[9] Bas Leonard Heijne. *Elliptic Delsarte Surfaces*. PhD thesis, University of Groningen, 2011.

[10] Jun-Ichi Igusa. Betti and Picard Numbers of Abstract Algebraic Surfaces. *Proceedings of the National Academy of Sciences*, 46(5):724–726, 1960.

[11] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer, New York, 2nd edition, 1990.

[12] Peter B. Kleidman and Martin W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1990.

[13] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer Science & Business Media, 1983.

[14] Serge Lang. *Algebraic Number Theory*, volume 110. Springer Science & Business Media, 1994.

[15] Serge Lang and André Néron. Rational Points of Abelian Varieties Over Function Fields. *American Journal of Mathematics*, 81(1):95–118, 1959.

[16] James S. Milne. Abelian Varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[17] David Mumford. *Tata Lectures on Theta II*, volume 43. Birkhäuser, 1984.

[18] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[19] Matthias Schütt and Tetsuji Shioda. *Mordell-Weil Lattices*. Springer, 2019.

[20] Matthias Schütt, Tetsuji Shioda, and Ronald van Luijk. Lines on Fermat surfaces. *J. Number Theory*, 130(9):1939–1963, 2010.

[21] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. https://arxiv.org/pdf/0907.0298.pdf, 2010.

[22] Jean-Pierre Serre, Everett W. Howe, Joseph Oesterle, and Christophe Ritzenthaler. *Rational Points on Curves Over Finite Fields*. Société Mathématique de France, 2020.

[23] Tetsuji Shioda. An Explicit Algorithm for Computing the Picard Number of Certain Algebraic Surfaces. *American Journal of Mathematics*, 108(2):415–432, 1986.

[24] Tetsuji Shioda. Some Remarks on Elliptic Curves Over Function Fields. *Astérisque*, 209, 1992.

[25] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2009.

[26] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2022.

[27] Henning Stichtenoth. *Algebraic Function Fields and Codes*, volume 254. Springer Science & Business Media, 2009.

[28] Peter Stiller. The Picard Numbers of Elliptic Surfaces With Many Symmetries. *Pacific Journal of Mathematics*, 128(1):157–189, 1987.

[29] J. Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones Mathematicae*, 2:134–144, 1966.

[30] John Tate and Igor Rostislavovich Shafarevich. The Rank of Elliptic Curves. In *Doklady Akademii Nauk*, volume 175, pages 770–773. Russian Academy of Sciences, 1967.

[31] MATLAB. *Version R2020a*. The MathWorks Inc., Natick, Massachusetts, 2020.

[32] Jaap Top. *Descent by 3-isogeny and 3-rank of quadratic fields*. Erasmus Universiteit Rotterdam. Econometrisch Instituut, 1991.

[33] Douglas Ulmer. Park City Lectures on Elliptic Curves over Function Fields. In *Arithmetic of L-functions*, volume 18, pages 211–277. American Mathematical Soc., 2011.

[34] Ronald Martinus Van Luijk. *Rational Points on K3 Surfaces*. PhD thesis, University of California, Berkeley, 2005.

[35] André Weil. Numbers of Solutions of Equations in Finite Fields. *Bulletin of the American Mathematical Society*, 55(5):497–508, 1949.