Università degli Studi di Padova

Dipartimento di Matematica “Tullio Levi-Civita”

Corso di Laurea Magistrale in Mathematics

Rational Elliptic Surfaces and absence of rank jump in fibres

Relatore:

Ch.mo Prof. Ramke Kloosterman

Laureando:

Marcello Bonaccorsi

Matricola N. 2089411

Anno Accademico 2023/2024

13 Dicembre 2024

Ringraziamenti

Vorrei innanzitutto ringraziare il mio relatore, il Prof. Kloosterman, per l'attenzione e la disponibilità dimostrate nel corso di questo progetto di tesi. Uno degli aspetti più affascinanti di questo lavoro è stato lo studio di oggetti che rappresentano un punto di incontro tra diversi ambiti della matematica. Grazie alla sua supervisione e ai suoi preziosi consigli, ho avuto l'opportunità di spaziare tra discipline e tecniche diverse, dando vita a un lavoro eclettico di cui sono particolarmente entusiasta.

Un ringraziamento speciale va ai miei genitori e a mia sorella, che mi hanno sostenuto con affetto e dedizione durante questo lungo e impegnativo percorso. Hanno condiviso con me gioie e delusioni, e considero questo risultato tanto mio quanto loro.

Infine, desidero esprimere la mia gratitudine ai miei amici, che con il loro affetto e il loro sostegno hanno reso questi anni universitari indimenticabili. Le infinite serate di giochi, scherzi e follie che abbiamo condiviso hanno portato colore e leggerezza in questo viaggio.

Contents

Introduction

Let $\pi : X \to \mathbb{P}^1$ be a non-costant elliptic surface defined over $\mathbb{Q}$ with a section. A generic fibre E is an elliptic curve over the function field $\mathbb{Q}(t)$ hence we can consider the group of $\mathbb{Q}(t)$-rational points of E. Each section $\sigma : C \to S$ is in bijective correspondence with a $\mathbb{Q}(t)$-rational point of a generic fibre of π. Since $\mathbb{Q}(t)$ is finitely generated over $\mathbb{Q}$, the Mordell–Weil Theorem is still valid in this context (Lang-Néron), hence the set of $\mathbb{Q}(t)$-rational points of E is a finitely generated abelian group and is called the Mordell-Weil group $\mathrm{MW}(X, \pi)$.
Since all but finitely many fibers of π are elliptic curves, it is interesting to study the relationship between the Mordell-Weil rank of the surface and the rank of the fibres. Silverman's specialization theorem [10] states that for almost all specializations at $b \in \mathbb{P}^1(\mathbb{Q})$, the rank of the associated elliptic curve defined over $\mathbb{Q}$ is at least rkMW(X,π). In other words, for all but finitely many $b \in \mathbb{P}^1(\mathbb{Q})$ the fibre X_b is an elliptic curve with rk$X_b(\mathbb{Q}) \geq$ rk MW(X,π). Consider now the follwing two sets

$$\mathcal{I}(X, \pi) = \{b \in \mathbb{P}^1(\mathbb{Q}) : X_b \text{ elliptic curve } \operatorname{rk} X_b(\mathbb{Q}) > \operatorname{rk}\mathrm{MW}(X, \pi)\},$$

$$\mathcal{N}(X, \pi) = \{b \in \mathbb{P}^1(\mathbb{Q}) : X_b \text{ elliptic curve } \operatorname{rk} X_b(\mathbb{Q}) = \operatorname{rk} MW(X, \pi)\},$$

of points $b \in \mathbb{P}^1(\mathbb{Q})$ where the rank jumps and where it does not jump respectively. The question is whether these sets are infinite.

The infinitude of $\mathcal{I}(X, \pi)$ has been the focus of extensive research. Salgado, in [12], provides an example involving k-unirational elliptic surfaces over number fields. In [14] Cassels and Schinzel construct an elliptic surface over a global field K using quadratic twists, where $\operatorname{rk}\mathrm{MW}(X, \pi) < \operatorname{rk}(E_t)$ for all but finitely many $t \in \mathbb{P}^1(K)$. However, this is an example of an isotrivial surface, while our interest lies in non-isotrivial surfaces. For non-isotrivial surfaces, Silverman formulated the so-called *density conjecture* in [15], which states: Let $\pi : X \to \mathbb{P}^1(\mathbb{Q})$ a non-isotrivial elliptic surface then

$$\operatorname{rk} X_b \in \{\operatorname{rk}\mathrm{MW}(X, \pi), \operatorname{rk}\mathrm{MW}(X, \pi){+}1\}$$

for all $b \in \mathbb{P}^1(\mathbb{Q})$ outside a set of density 0 in $\mathbb{P}^1(\mathbb{Q})$. Let us consider the case where $\operatorname{rk}\mathrm{MW}(X) = 0$. Assuming the density conjecture, one can reasonably expect the following:

Conjecture 1. *Let $\pi : X \to \mathbb{P}^1(\mathbb{Q})$ a non-isotrivial elliptic surface with $\operatorname{rk}\mathrm{MW}(X) = 0$. Then there are infinitely many $b \in \mathbb{P}^1(\mathbb{Q})$ with $\operatorname{rk} X_b(\mathbb{Q}) = 0$.*

At present, there is no known example of a non-isotrivial elliptic surface with an infinite $\mathcal{N}(X, \pi)$. In [5], Caro and Pasten construct an example under the assumption of the Lenstra–Pomerance–Wagstaff conjecture on the infinitude of Mersenne primes. In particular, they analyze the non-isotrivial Legendre elliptic surface defined by the Weierstrass equation

$$y^2 = x(x+1)(x+t),$$

which is known to have $\operatorname{rk}\mathrm{MW}(X,\pi) = 0$. Using $t = 2^q$ where $q \in \mathbb{N},\ q \geq 5$ and $2^q - 1$ is a Mersenne prime, they show that the rank of the associated fiber is always 0. This provides an example, albeit strongly dependent on specific conditions. It is thus natural to explore alternative methods for identifying surfaces with this property. In this thesis we show that the non-isotrivial elliptic surface $\pi : Y \to \mathbb{P}^1$ defined over $\mathbb{Q}$ by the affine Weierstrass equation

$$y^2 = x(x-(t-2))(x-t)$$

has the desired property, conditional on the existence of infinitely many twin primes. Remarkably, both cases reveal a deep connection between the properties of specific prime families and the behavior of ranks in the associated elliptic surfaces. Thus, proving the infinitude of Mersenne primes or twin primes would have profound implications across various fields of mathematics.

The thesis is organized as follows: the first chapter reviews the theory of elliptic curves, following [1]. The focus is on studying the rank of elliptic curves using the descent method and the parity conjecture. The second chapter covers elliptic surfaces, the Mordell-Weil rank, and Tate's algorithm. The main results are presented in the third chapter while the appendix provides additional details on key tools used in the proofs. In chapter 3, we show that under the assumption of Conjecture 2, both $\mathcal{I}(Y,\pi)$ $\mathcal{N}(Y,\pi)$ are infinite. The final section collects observations and conjectures on the distribution of twin prime pairs in $\mathbb{N}$, illustrating how elliptic surface theory enhances our understanding of natural number structures. This interplay between different mathematical fields often leads to unexpected and profound insights, offering a glimpse into a deeper dimension of knowledge.

Chapter 1

Elliptic curves

In this chapter we we discuss the basic theory of elliptic curves.

1.1 Weierstrass equation

Let K be a field and $\bar{K}$ be an algebraic closure of K.

Definition 1.1.1. An elliptic curve over K written E/K is a smooth, projective, algebraic curve of genus 1 together with a point $O \in E(K)$.

The Riemann-Roch theorem gives us the possibility to define an elliptic curve over a field in another way:

Definition 1.1.2. An elliptic curve over a field K is a nonsingular projective plane curve of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

It is called *Weierstrass equation* where $a_1, a_2, a_3, a_4, a_6 \in K$. Moreover $O = [0, 1, 0]$ is the base point.

In general we deal with the Weierstrass equation with inhomogeneous coordinates $x = X/Z$ and $y = Y/Z$,

$$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

Theorem 1.1.3. *When* char $\bar{K} \neq 2, 3$, *every elliptic curve E/K is isomorphic to a curve of non-homogeneous form*

$$E : y^2 = x^3 + ax + b, \quad a, b \in K. \tag{1.2}$$

Proof. Completing the square we can simplify the equation 1.1. Thus by substitution

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3),$$

we obtain an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1 + 4a_2, \qquad b_4 = 2a_4 + a_1a_4, \qquad b_6 = a_3^2 + 4a_6.$$

Now we apply the following change of variables

$$(x, y) \longmapsto (\frac{x - 3b^2}{36}, \frac{y}{108})$$

to eliminate the x^2 term, yelding the simpler equation

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{1.3}$$

□

We also define the following quantities:

- $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$
- $c_4 = b_2^2 - 24b_4,$
- $c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$
- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$
- $j = c_4^3/\Delta.$

Definition 1.1.4. The quantity $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ is the *discriminant* of the Weierstrass equation, the quantity j is the $j-$ *invariant* of the elliptic curve.

The discriminant of an elliptic curve is really important in order to determine singular elliptic curves.

Remark 1.1.5. *Let E/K an elliptic curve over a field K and $P = (x, y)$ which satisfies a Weierstrass equation*

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 + a_2x^2 + a_4x + a_6 = 0.$$

P is a singular point if and only if

$$\frac{\partial f}{\partial x}(P) = 0 \qquad \text{and} \qquad \frac{\partial f}{\partial y}(P) = 0.$$

If a curve has a singular point then it is called a singular curve.

It follows that there are $\alpha, \beta \in \bar{K}$ such that the Taylor series expansion of $f(x, y)$ at P has the form

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

Definition 1.1.6. With notation as above, the singular point P is a *node* if $\alpha \neq \beta$. In this case, the lines

$$(y - y_0) - \alpha(x - x_0) \;\; \textit{and} \;\; (y - y_0) - \beta(x - x_0)$$

are the *tangent lines* at P. Conversely if $\alpha = \beta$, we say that P is a *cusp*, in which case the *tangent line* at P is given by

$$y - y_0 = \alpha(x - x_0).$$

Proposition 1.1.7. *The curve given by a Weierstrass equation satisfies:*

(a) It is nonsingualar if and only if $\Delta \neq 0$.

(b) It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.

(c) It has a cusp if and only if $\Delta = c_4 = 0$.

In cases (b) and (c) there is only one singular point.

Proof. See [1, Proposition III.1.4]. □

1.2 The Group Law

Let E be an elliptic curve given by a Weierstrass equation together with $O = [0, 1, 0]$ at infinity. We define an operation to endow the curve with the group structure.

Definition 1.2.1. Let $P, Q \in E$, L the line through P and Q and let R be the third point of intersection of L with E. Let l the line through R and O. Then l intersects E at R, O and a third point. We denote that third point by $P \oplus Q$.

Remark 1.2.2. *Note that this definition rely on Bezout's theorem which guarantee that R exists and is unique.*

Proposition 1.2.3. *The composition law has the following properties:*

(a) If a line L intersect E at the (non necessarily distinct) points P,Q,R then

$$(P \oplus Q) \oplus R = O.$$

(b) $P \oplus O = P$ for all $P \in E$.

(c) $P \oplus Q = Q \oplus P$ for all $P, Q \in E$.

(d) Let $P \in E$. There is a point of E, denoted by $(-P)$, satisfying

$$P \oplus (-P) = O.$$

(e) Let P,Q,$R \in E$. Then

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

E endowed with the composition law has the structure of abelian group and O is the identity element.

Proof. All the points are easy except for the associativity (e). For a detailed proof see [1, Proposition III.2.2]. □

Definition 1.2.4. Let E be a (possibly singular) curve given by a Weierstrass equation. The nonsingular part of E, denoted by E_{ns}, is the set of nonsingular points of E. Similarly, if E is defined over K, then $E_{ns}(K)$ is the set of nonsingular points of $E(K)$.

Proposition 1.2.5. *Let E be a curve given by a Weierstrass equation with $\Delta = 0$, so E has a singular point S. Then the composition law makes E_{ns} into an abelian group.*

(a) Suppose that E has node, so $c_4 \neq 0$, and let

$$y = \alpha_1 x + \beta_1 \quad \textit{and} \quad y = \alpha_2 x + \beta_2$$

be the distinct tangent lines to E at S. Then the map

$$E_{ns} \longrightarrow \bar{K}^*, \quad (x, y) \longmapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

is an isomorphism of abelian groups.

(b) Suppose that E has node, so $c_4 = 0$, and let

$$y = \alpha x + \beta$$

be the tangent line to E at S. Then the map

$$E_{ns} \longrightarrow \bar{K}^+, \quad (x, y) \longmapsto \frac{x - x(S)}{y - \alpha x - \beta}$$

is an isomorphism of abelian groups.

Proof. [1, Proposition III.2.5]. □

Notation 1. From now on indicate the group operation with the usual $+$. For $m \in \mathbb{Z}$ and $P \in E$, we let

$$[m]P = P + ... + P, \quad |m| \textit{ times and } m > 0,$$

$$[m]P = -P - P - P \quad |m| \textit{ times and } m < 0,$$

$$[0]P = O.$$

Definition 1.2.6. Let E an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The $m-torsion\ subgroup\ of\ E$, denoted by $E[m]$, is the set of points of E of order m,

$$E[m] = \big\{P \in E : [m]P = O\big\}.$$

The *torsion subgroup of E*, denoted by E_{tors}, is the set of points of finite order,

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over K, then $E_{tors}(K)$ denotes the points of finite order in $E(K)$.

1.3 Isogenies

Definition 1.3.1. Let E_1 and E_2 be elliptic curves. An *isogeny* form E_1 to E_2 is a morphism

$$\varphi : E_1 \to E_2 \qquad \text{satysfing} \qquad \varphi(O) = O.$$

Two elliptic curves are *isogenous* if there is an isogeny from E_1 to E_2 with $\varphi(E_1) \neq \{O\}$.

Example 1.3.2. For each $m \in \mathbb{Z}$ we define the $multiplication - by - m$ isogeny

$$[m] : E \to E$$

in the natural way (See Notation 1).

Theorem 1.3.3. *Let*

$$\varphi : E_1 \longrightarrow E_2$$

be an isogeny. Then

$$\varphi(P + Q) = \varphi(P) + \varphi(Q) \qquad for\ all\ P, Q \in E_1.$$

Proof. See [1, Theorem III.4.8]. □

Corollary 1.3.4. *Let $\varphi : E_1 \to E_2$ be a nonzero isogeny. Then*

$$\ker \varphi = \varphi^{-1}(O)$$

is a finite group.

Proof. From 1.3.3 we deduce that it is a subgroup of E_1 and it is of finite order [1, Proposition III.2.6a]. □

Now we define the *degree* of an isogeny and then isogenies called the *dual isogenies*. If $\varphi : E_1 \longrightarrow E_2$ is non constant then we can define an injective map as follows:

$$\varphi^* : K(E_2) \longrightarrow K(E_1), \qquad \varphi^* f := f \circ \phi.$$

Because of [1, Theorem II.2.4], $K(E_1)$ is a finite extension of $\varphi^*(K(E_2))$ therefore we can give the following definition:

Definition 1.3.5. Let $\varphi : E_1 \longrightarrow E_2$ be an isogeny. If φ is constant, we define the degree of φ to be 0, otherwise

$$\deg(\varphi) = [K(E_1) : \varphi^*(K(E_2))].$$

Theorem 1.3.6. *Let $\varphi : E_1 \longrightarrow E_2$ be a noncostant isogeny of degree m. Then there exist a unique isogeny*

$$\hat{\varphi} : E_2 \longrightarrow E_1 \qquad satisfying \qquad \hat{\varphi} \circ \varphi = [m].$$

Proof. See [1, Theorem III.6.1]. □

Definition 1.3.7. Let $\varphi : E_1 \to E_2$ be an isogeny. The *dual isogeny* to φ is the isogeny

$$\hat{\varphi} : E_2 \to E_1.$$

given in Theorem 1.3.6.

Theorem 1.3.8. *Let*

$$\varphi : E_1 \to E_2$$

be an isogeny.

(a) Let $m = \deg \varphi$. Then

$$\hat{\varphi} \circ \varphi = [m] \quad \text{on } E_1 \quad \text{and} \quad \varphi \circ \hat{\varphi} = [m] \quad \text{on } E_2.$$

(b) $\lambda : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \varphi} = \hat{\varphi} \circ \hat{\lambda}.$$

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}.$$

(d) For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \qquad \deg[m] = m^2.$$

(e) $\deg \hat{\varphi} = \deg \varphi$.

(f) $\hat{\hat{\varphi}} = \varphi$.

Proof. If φ is constant then the entire theorem is trivial, and similarly (b) and (c) are trivial if λ or ψ is constant. We may assume that all isogenies are nonconstant.

(a) The first statement is the defining property of $\hat{\varphi}$. For the second consider

$$(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ [m] = [m] \circ \varphi.$$

hence $\varphi \circ \hat{\varphi} = [m]$ since φ is not constant.

(b) Let $n = \deg \lambda$, we have

$$(\hat{\varphi} \circ \hat{\lambda}) \circ (\lambda \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = [n] \circ \hat{\varphi} \circ \varphi = [nm].$$

The uniqness statement in Theorem 1.3.6 implies that

$$\hat{\varphi} \circ \hat{\lambda} = \widehat{\lambda \circ \varphi}.$$

(c) See [1, Theorem III.6.2c].

(d) This is true for $m = 0$ by definition, and easily true for $m = 1$. Using (c) with $\varphi = [m]$ and $\psi = 1$ yields

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]},$$

and ascending and descending induction shows that $\widehat{[m]} = [m]$ holds for all m. Now let $d = \deg[m]$ and consider the multiplication-by-d map. Thus using the definition of dual isogeny and $[m] = \widehat{[m]}$, we obtain

$$[d] = \widehat{[m]} \circ [m] = [m^2].$$

The endomorphism ring of an elliptic curve is a torsion free $\mathbb{Z}$-module ([1], Proposition 4.2) hence it follows that $d = m^2$.

(e) Let $m = \deg \varphi$. Using (d) and (a), we find that

$$m^2 = \deg[m] = \deg(\varphi \circ \hat{\varphi}) = (\deg \varphi)(\deg \hat{\varphi}) = m(\deg \hat{\varphi}).$$

Hence $m = \deg \hat{\varphi}$.

(f) Again $m = \deg \varphi$. We easily obtain the statement by (a), (b), and (d).

□

Corollary 1.3.9. *Let E an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$.*

(a) $\deg[m] = m^2$.

(b) If $m \neq 0$ in K, i.e. if either char(K) = 0 or p = char(K) > 0 and $p \nmid m$ then

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) If char$(K) = p > 0$ then one of the following is true:

- $E[p^e] = \{O\}$ *for all* $e \in \mathbb{N}$.
- $E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$ *for all* $e \in \mathbb{N}$.

Proof. See [1, Corollary III.6.4]. □

1.4 The Weil Pairing

Definition 1.4.1. The *divisor group* of a curve C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P).$$

Where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The *degree of* D is defined by

$$\deg D = \sum_{P \in C} n_P.$$

The *Divisors of degree* 0 form a subgroup of $\operatorname{Div}(C)$, which we denote by

$$\operatorname{Div}^0(C) = \big\{ D \in \operatorname{Div}(C) : \deg D = 0 \big\}.$$

If C is defined over K, we let $G_{\bar{K}/K}$ act on $\operatorname{Div}(C)$ by

$$D^\sigma = \sum_{P \in C} n_P (P^\sigma).$$

Then D *is defined over* K *if* $D^\sigma = D$ for all $\sigma \in G_{\bar{K}/K}$. We denote the group of divisors defined over K by $\operatorname{Div}_K(C)$, and similarly $\operatorname{Div}^0_K(C)$. Assume now that the curve C is smooth, and let $f \in K(C)^*$. Then we can associate to f the divisor $\operatorname{div}(f)$ given by

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P).$$

This is a divisor. If $\sigma \in G_{\bar{K}/K}$, then it is easy to see that

$$\operatorname{div}(f^\sigma) = (\operatorname{div}(f))^\sigma.$$

Definition 1.4.2. A divisor $D \in \operatorname{Div}(C)$ is *principal* if it has the form $D = \operatorname{div}(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are *linearly equivalent* written $D_1 \sim D_2$ if $D_1 - D_2$ is *principal*. Moreover we define the *Picard Group* $\operatorname{Pic}(C)$ as the quotient of $\operatorname{Div}(C)$ with the subgroup of principal divisors. Finally, we write the quotient of $\operatorname{Div}^0(C)$ by the subgroup of principal divisors as $\operatorname{Pic}^0(C)$.

Proposition 1.4.3. *Let C be a smooth curve and let $f \in \bar{K}(C)^*$.*

1. $\operatorname{div}(f) = 0$ *if and only if* $f \in \bar{K}^*$.
2. $\deg(\operatorname{div}(f)) = 0$.

Proof. See [1, Proposition II.3.1]. □

Now we give a corollary useful in the definition of Weil-Pairing.

Corollary 1.4.4. *Let C/K a curve over the field K and let $D = \sum_{P \in E} n_P(P)$ be a divisor of degree 0. Then D is a principal divisor if and only if*

$$\sum_{P \in E} [n_P] P = O.$$

Proof. See [1, Proposition II.3.4], and [1, Corollary II.3.5]. □

We are finally ready to describe the Weil-Pairing. Let E/K be an elliptic curve and $m \geq 2$ an integer which we assume to be prime to $p = char(K)$ if $p > 0$. From the previous section we know that the group of m-torsion points $E[m]$ has the form

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

The aim of this section is to define a bilinear pairing which is Galois invariant.
Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ satisfying

$$\operatorname{div}(f) = m(T) - m(O).$$

Now take $T^{'} \in E$ to be a point with $[m]T^{'} = T$. Then there is a similar function $g \in \bar{K}(E)$ satisfying

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T^{'} + R) - (R).$$

It is easy to verify that the functions $f \circ [m]$ and g^m have the same divisor, so multiplying f by an appropriate constant from $\bar{K}^*$, we may assume that

$$f \circ [m] = g^m.$$

Now let $S \in E[m]$ be another m-torsion point, where we allow $S = T$. Then for any point $X \in E$ we have

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Thus considered as a function of X, the function $g(X+S)/g(X)$ takes on only finitely many values, i.e., for every X, it is an m-th root of unity. In particular, the morphism

$$S \rightarrow g(X+S)/g(X)$$

is constant (for further details see [1].III.8). We can define the $Weil - Pairing$ as

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

by setting

$$e_m(S,T) = \frac{g(X+S)}{g(X)},$$

where $X \in E$ is any point such that $g(X+S)$ and $g(X)$ are both defined and nonzero. We use μ_m to indicate the group of m^{th} roots of unity.

Proposition 1.4.5. *The Weil $e_m - pairing$ has the following properties:*

1. *It is bilinear:*
$$e_m(S_1 + S_2, T) = e_m(S_1, T) + e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1) + e_m(S, T_2).$$

2. *It is nondegenerate:*
$$If\ e_m(S,T) = 1\ for\ all\ S \in E[m],\ then\ T = O.$$

3. *It is Galois invariant:*
$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) \quad for\ all\ \sigma\ in\ G_{\bar{K}/K}.$$

Proof. See [1, Proposition III.8.1].

□

Corollary 1.4.6. *There exist points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive m^{th} root of unity. In particular, if $E[m] \subset E(K)$, then $\mu_m \subset K^*$.*

Proof. If $S, T \in E[m]$ then $e_m(S,T) \subset \mu_m$, for example equal to μ_l. It follows that

$$1 = e_m(S,T)^l = e_m([l]S, T) \quad \forall\ S, T \in E[m].$$

The nondegeneracy of Weil Pairing implies that $[l]S = O$ for every $S \in E[m]$. Thus $E[m] \subset E[n]$, from Corollary 1.3.9 we get that $l = n$. Suppose now that $E[m] \subset E(K)$, the Galois invariance of the e_m-pairing implies that $e_m(S,T) \in K^*$ for all $S, T \in E[m]$ hence we get the desired result. □

1.5 Reduction of an elliptic curve

In this section we indicate K a local field complete respect to a discrete valuation ν. R will be the ring of integer of K, $\mathcal{M}$ the maximal ideal of R, π a uniformizer for R and $k = R/M$ the residue field of R. Furthermore we assume that $\nu(\pi) = 1$ and both K and k are perfect fields. Let E/K be an elliptic curve with a Weierstrass equation.

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

After the substitution $(x, y) \to (u^{-2}x, u^{-3}y)$ we get

$$E/K : y^2 + ua_1xy + u^3a_3y = x^3 + u^2a_2x^2 + u^4a_4x + u^6a_6.$$

By choosing u properly we obtain a Weierstrass equation with all coefficients in R. Consequently, the discriminant Δ of the Weierstrass equation satisfies $\nu(\Delta) \geq 0$. Now we are ready to define the minimal Weierstrass equation.

Definition 1.5.1. Let E/K be an elliptic curve. A Weierstrass equation for E is called $minimal\ Weiestrass\ equation\ for\ E\ at\ \nu$ if $\nu(\Delta)$ is minimized subject to the condition that $a_1, a_2, a_3, a_4, a_6 \in R$. This minimal value of $\nu(\Delta)$ is called the $valuation\ of\ minimal\ disciminant\ of\ E\ at\ \nu$.

Proposition 1.5.2. *Every elliptic curve E/K has minimal Weierstrass equation.*

Proof. It is enough to find some Weierstrass equations with all $a_i \in R$ and search for one that minimize $\nu(\Delta)$. The existence is due to the fact that ν has only discrete values. □

We now introduce the operation of "reduction modulo π" which we denote by a tilde.

Definition 1.5.3. Let E/K an elliptic curve with his minimal Weiestrass equation. Reducing his coefficients modulo π we obtain a equation over k:

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}.$$

The curve $\tilde{E}/k$ is called the $reduction\ of\ E\ modulo\ \pi$.

Definition 1.5.4. Let E/K be an elliptic curve, and let $\tilde{E}/k$ be the reduction modulo π of a minimal Weiestrass equation for E/K.

(a) E/K has good reduction if $\tilde{E}/k$ is smooth.

(b) E/K has multiplicative reduction if $\tilde{E}/k$ has a node.

(c) E/K has additive reduction if $\tilde{E}/k$ has a cusp.

In both cases (b) and (c) we say E/K has bad reduction. If E has multiplicative reduction, then the reduction is said to be split if the slopes of the tangent lines at the node are in k, and otherwise it is said to be nonsplit.

The following proposition plays a crucial role in order to understand the structure of the Mordell-Weil group of an elliptic curve.

Proposition 1.5.5. *Let E/K be an elliptic curve be an elliptic curve and let $m \geq 1$ be an integer that is relatively prime to $char(k)$ and assume further that the reduced curve is non-singular. Then the reduction map*

$$E(K)[m] \to \tilde{E}(k)$$

is injective, where $E(K)[m]$ denotes the set of points of order m in $E(K)$.

Proof. From [1, Proposition VII.3.1a], we deduce that

$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}$$

has no nontrivial points of order m. If we assume that $\tilde{E}$ is nonsingular, then

$$E_0 = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}$$

results to be equal to $E(K)$ and $\tilde{E}_{ns}(k) = \tilde{E}(k)$, so m-torsion of $E(K)$ injects into $\tilde{E}(k)$. □

Proposition 1.5.6. *Let E/K be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation, and let c_4 be the usual expression involving $a_1, \ldots.., a_6$.

(a) E has good reduction if and only if $\nu(\Delta) = 0$. In this case $\tilde{E}/k$ is an elliptic curve.

(b) E has multiplicative reduction if and only if $\nu(\Delta) > 0$ and $\nu(c_4) = 0$, i.e. $\Delta \in \mathcal{M}$ and $c_4 \in R^*$. In this case

$$\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^*.$$

(c) E has additive reduction if and only if $\nu(\Delta) > 0$ and $\nu(c_4) > 0$, i.e. $\Delta, c_4 \in \mathcal{M}$. In this case

$$\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^+.$$

Proof. Applying Proposition 1.1.7 and Proposition 1.2.5 to the reduced curve $\tilde{E}/k$ we prove all the three statements.

□

1.6 Elliptic curves over Global Field

In this section we briefly treat some of the main results concerning the theory of Mordell-Weil group of an elliptic curve.
Let K be a number field and let E/K be an elliptic curve.

Theorem 1.6.1. *(Mordell-Weil). The group $E(K)$ is finitely generated.*

The proof of this theorem consists of two quite distinct parts, the so-called "weak Mordell–Weil theorem," and the "infinite descent" using height functions. The Mordell–Weil theorem tells us that the Mordell–Weil group $E(K)$ has the form

$$E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$$

where the torsion subgroup $E(K)_{tors}$ is finite and the *rank* r of $E(K)$ is a nonnegative integer. Chapter VIII of [1] gives a detailed description of the theory behind this fundamental theorem.

Theorem 1.6.2. *(Weak Mordell-Weil Theorem). Let K be a number field, let E/K be an elliptic curve, and let $m \geq 2$ be an integer. Then*

$$E(K)/mE(K)$$

is a finite group.

Proof. See [1, VIII.I]. □

Definition 1.6.3. The *Kummer Pairing*

$$k : E(K) \times G_{\bar{K}/K} \longrightarrow E[m]$$

is defined as follows. Let $P \in E(K)$ and choose any point $Q \in E(\bar{K})$ satysfing $[m]Q = P$. Then

$$k(P, \sigma) = Q^{\sigma} - Q,$$

The next result describes basic properties of the Kummer pairing.

Proposition 1.6.4. *(a) The Kummer pairing is well-defined.*

(b) The Kummer pairing is bilinear.

(c) The kernel of the Kummer pairing on the left is $mE(K)$.

(d) The kernel of the Kummer pairing on the right is $G_{\bar{K}/L}$ where,

$$L = K([m]^{-1}E(K))$$

is the compositum of all fields $K(Q)$ as Q ranges over the points in $E(\bar{K})$ satisfying $[m]Q \in E(K)$.

Hence the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times G_{L/K} \longrightarrow E[m].$$

Proof. See [1, Proposition VIII.1.2]. □

At the end of this section, we present some results from VIII.8 of [1] that will be useful in the section concerning the Tate's algorithm.

Definition 1.6.5. A *global minimal Weierstrass equation for E/K* is a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E/K such that $a_1, a_2, a_3, a_4, a_6 \in R$ and the discriminant Δ of the equation satisfies $\mathcal{D}_{E/K} = (\Delta)$ where $\mathcal{D}_{E/K}$ is the *minimal discriminant* of E/K.

Corollary 1.6.6. *If K has class number one, then every elliptic curve E/K has a global minimal Weierstrass equation. In particular, this is true for $K = \mathbb{Q}$.*

Proof. It is a direct conseguence of [1, Proposition VIII.8.2]. □

1.7 Descent Procedure

For this section we let E/K be an elliptic curve and $m \geq 2$ an integer, and we assume

$$E[m] \subset E(K).$$

Under this assumption there is a pairing

$$k : E(K) \times G_{\bar{K}/K} \longrightarrow E[m]$$

defined by

$$k(P, \sigma) = Q^{\sigma} - Q,$$

where $Q \in E(\bar{K})$ is chosen to satisfy $[m]Q = P$. Proposition 1.6.4 states that the kernel on the left is $mE(K)$ so we may view k as an homomorphism

$$\delta_E : E(K)/mE(K) \longrightarrow Hom(G_{\bar{K}/K, E[m]}),$$

$$\delta_E(P)(\sigma) = k(P, \sigma).$$

We also observe that our assumption $E[m] \subset E(K)$ implies that $\mu_m \subset K^*$. This follows from the basic properties of the Weil pairing,

$$e_m : E[m] \times E[m] \longrightarrow \mu_m.$$

Finally since $\mu_m \subset K^*$, Hilbert's Theorem 90 [1, Theorem B.2.5c] says that every homomorphism $G_{\bar{K}/K} \to \mu_m$ has the form

$$\sigma \longrightarrow \frac{\beta^{\sigma}}{\beta} \quad \textit{for some } \beta \in \bar{K}^* \textit{ satisfying } \beta^m \in K^*.$$

Theorem 1.7.1. *With notations as above, there is a bilinear pairing*

$$b : E(K)/mE(K) \times E[m] \to K^*/(K^*)^m$$

satisfying

$$e_m\big(\delta_E(P), T\big) = \delta_K\big(b(P, T)\big).$$

1. *The pairing b is non degenerate on the left.*
2. *Let $S \subset M_K$ be the union of the set of infinite places, the set of finite primes at which E has bad reduction, and the set of finite primes dividing m. Then the image of the pairing lies in the following subgroup of $K^*/(K^*)^m$:*

$$K(S, m) = \big\{b \in K^*/(K^*)^m : ord_{\nu}(b) \equiv 0 \pmod{m} \textit{ for all } \nu \notin S\big\}.$$

3. *The pairing b may be computed as folllows. For each $T \in E[m]$, choose functions $f_T, g_T \in K(E)$ satisfying the conditions*

$$div(f_T) = m(T) - m(O) \qquad \textit{and } f_T \circ [m] = g_T^m$$

. Then for any point $P \neq T$,

$$b(P, T) \equiv f_T(P) \qquad (mod\ (K^*)^m).$$

Proof. Hilbert's Theorem 90 [1, Theorem B.2.5c] shows that the pairing is well-defined. Bilinearity follows from bilinearity of the Kummer pairing and bilinearity of the Weil-pairing.

1. In order to prove nondegeneracy on the left, we suppose that $b(P,T) = 1$ for all $T \in E[m]$. This means that for all $T \in E[m]$ and all $\sigma \in G_{\bar{K}/K}$,

   $$e_m(k(P,\sigma),T) = 1.$$

   The nondegeneracy of the Weil pairing implies that $k(P,\sigma) = 0$ for all σ, and then the properties of Krummer Pairing tell us that $P \in mE(K)$.

2. In this part of the proof some theory about ramification and algebraic fields is needed. We give as reference [1, Theorem X.1.1] and [1, VIII.I].

3. Choose $Q \in E(\bar{K})$ and $\beta \in \bar{K}^*$ satisfying

   $$P = [m]Q \quad \textit{and} \quad b(P,T) = \beta^m.$$

Then for all $\sigma \in G_{\bar{K}/K}$ we have by definition

$$e_m(\delta(P)(\sigma),T) = \delta_K(b(P,T))(\sigma),$$

$$e_m(Q^\sigma - Q,T) = \frac{\beta^\sigma}{\beta},$$

$$g_T(X + Q^\sigma - Q)/g_T(X) = \beta^\sigma/\beta,$$

$$g_T(Q)^\sigma/g_T(Q) = \beta^\sigma/\beta \quad \textit{putting } X = Q.$$

Since δ_K is an isomorphism, it follows that $g_T(Q)^m \equiv \beta^m \pmod{(K^*)^m}$. Therefore

$$f_T(P) = f_T \circ [m](Q) = g_T(Q)^m \equiv \beta^m = b(P,T) \pmod{(K^*)^m}.$$

□

Now we focus on the special case $m = 2$. Under the assumption that $E[m] \subset E(K)$, we may take a Weiestrass equation for E of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \textit{with } e_1, e_2, e_3 \in K.$$

The three nontrivial 2-torsion points are

$$T_1 = (e_1, 0), \quad T_2 = (e_2, 0), \quad T_3 = (e_3, 0).$$

Letting T one of these points, we claim that the associated function is $f_T = x - e$. It is clear that this function has the correct divisor,

$$div(x - e) = 2(T) - 2(O)$$

It is then a calculation to check that

$$x \circ [2] = (\frac{x^2 - 2ex - 2e^2 + 2(e_1 + e_2 + e_3)e - (e_1e_2 + e_1e_3 + e_2e_3)}{2y})^2,$$

so $x - e_1$ has both of the properties needed to be f_T.
Now suppose that we have chosen a pair $(b_1, b_2) \in K(S, 2) \times K(S, 2)$ and that we want to determine whether there is a point $P \in E(K)/2E(K)$ satysfing

$$b(P, T_1) = b_1, \qquad b(P, T_2) = b_2.$$

Such a point exist if and only if there is a solution

$$(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$$

to the system of equations

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad b_1 z_1^2 = x - e_1, \quad b_2 z_2^2 = x - e_2.$$

We substitute the latter two equations into the former and define a new variable z_3 by $y = b_1 b_2 z_1 z_2 z_3$, which is permissible since b_1, b_2, z_1 and z_2 take only nonzero values. This yields the three equations

$$b_1 b_2 z_3^2 = x - e_3, \quad b_1 z_1^2 = x - e_1, \quad b_2 z_2^2 = x - e_2.$$

Finally eliminating x gives the pair of equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1, \quad b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1.$$

Notice that if we do find a solution (z_1, z_2, z_3), then we immediately recover the corresponding point in $E(K)/2E(K)$ using the formulas

$$x = b_1 z_1^2 + e_1, \quad y = b_1 b_2 z_1 z_2 z_3.$$

Finally we must deal with the fact that the definition $b(P, T) = f_T(P)$ cannot be used if it happens that $P = T$. In other words, there are two pairs (b_1, b_2) that do not arise from the above procedure, namely the pairs $(b(T_1, T_1), b(T_1, T_2))$ and $(b(T_2, T_1), b(T_2, T_2))$. These values may be computed using linearity as

$$\begin{aligned} b(T_1, T_1) &= b(T_1, T_1 + T_2) b(T_1, T_2)^{-1} \\ &= b(T_1, T_3) b(T_1, T_2)^{-1} = \frac{e_1 - e_3}{e_1 - e_2}, \end{aligned}$$

and simililarly

$$b(T_2, T_2) = \frac{e_2 - e_3}{e_2 - e_1}.$$

We summarize everything in the following fundamental proposition.

Proposition 1.7.2. *(Complete 2-Descent). Let E/K be an elliptic curve given by a Weierstrass equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \quad \textit{with } e_1, e_2, e_3 \in K.$$

Let $S \subset M_K$ be a finite set of places of K including all archimedean places, all places dividing 2, and all places at which E has bad reduction. Further let

$$K(S, 2) = \big\{ b \in K^*/(K^*)^2 : ord_\nu(b) \equiv 0 \pmod 2 \ \textit{for all } \nu \notin S \big\}.$$

Then there is an injective morphism

$$E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

defined by

$$P=(x,y) \longmapsto \begin{cases} (x-e_1, x-e_2) & if\ x \neq e_1, e_2, \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1-e_2\right) & if\ x = e_1, \\ \left(e_2-e_1, \frac{e_2-e_3}{e_2-e_1}\right) & if\ x = e_2, \\ (1,1) & if\ x=\infty,\ i.e., if\ P=O. \end{cases} \tag{1.4}$$

Let $(b_1, b_2) \in K(S,2) \times K(S,2)$ be a pair that is not in the image of one of the three points $O, (e_1, 0), (e_2, 0)$. Then (b_1, b_2) is the image of a point

$$P=(x,y) \in E(K)/2E(K)$$

if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1,$$
$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1,$$

have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then we can take

$$P=(x,y)=(b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

Chapter 2

Elliptic Surfaces

In this chapter we will mainly follow the exposition of [3] and [4]. The section about Algebraic surfaces and intersection theory comes from [2].

2.1 Elliptic surfaces

We shall define elliptic surfaces in a geometric way. Therefore we let $k = \bar{k}$ denote an algebraically closed field, and C a smooth projective curve over k.

Definition 2.1.1. An $elliptic\ surface$ S over C is a smooth projective surface S with an elliptic fibration over C, i.e. a surjective morphism

$$\pi : S \to C,$$

such that:

1. almost all fibres are smooth curves of genus 1,

2. is *relatively minimal* i.e.no fibrer contains an exceptional curve of the first kind.

Remark 2.1.2. *The second condition stems from the classification of algebraic surfaces. An exceptional curve of the first kind is a smooth rational curve of self-intersection (-1).*

Example 2.1.3. We investigate one of the standard examples of elliptic surfaces: the cubic pencil. Let F and $G \in k[X, Y, Z]$ be homogeneous cubic polynomials without common factor. Consider the cubic pencil

$$S : \quad sF + tG = 0, \quad [s, t] \in \mathbb{P}^1.$$

Indeed, S is a rational surface, since the ratio s/t is expressed by F and G, so the function field of S in the (often to be taken affine) coordinates $x = X/Z$, $y = Y/Z$ is simply $k(S) = k(x, y)$. If the pencil contains at least one smooth cubic curve, then the cubic pencil defines a genus one fibration over the $\mathbb{P}^1$-line with homogeneous coordinates $[s, t]$ (possibly after resolving singularities of S as a projective surface in $\mathbb{P}^2 \times \mathbb{P}^1$). Since k is algebraically closed, S gives in fact an elliptic surface with sections given by the base points of the cubic pencil. Here we have to pay special attention when there are infinitely near (i.e. multiple) base points: then there are singularities involved, and each multiple base points represents the components of the exceptional divisor of the resolution ((-2)-curves contained in some fibre) plus a section meeting one of these components (a (-1)-curve not contained in any fibre).

Definition 2.1.4. A section of an elliptic surface $\pi : S \to C$ is a morphism

$$\sigma : C \to S \quad \textit{such that} \;\; \pi \circ \sigma = id_C.$$

The existence of a section is very convenient since then we can work with a Weierstrass equation where we regard the genric fibre E as an elliptic curve over the function field $k(C)$. In particular, we will see that the sections form an abelian group: $E(k(C))$. Here we choose one section as the origin of the group law. We call it zero section and denote it by O. In order to preserve some properties, we assume that

1. Every elliptic surface has a section.

2. Every elliptic surface S has a singular fiber. In particular, S is not isomorphic to a product $E \times C$.

Definition 2.1.5. Let $\pi : S \to C$ be an elliptic fibration and $v \in C$ a generic point of C. We call $E = f^{-1}(v)$ the *generic fiber* of S. The second convention guarantees that the generic fibre E is an elliptic curve over the function field $k(C)$.

Remark 2.1.6. *As the generic fiber is an elliptic curve over $k(C)$, the elliptic surface S may be locally represented in the Weierstrass form, namely*

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \quad a_i(t) \in k(C), \; \textit{for every } i.$$

The assumption of a section is fairly strong. In fact, it rules out a number of surfaces as for example Enriques surfaces. Now we investigate the relationship between an elliptic surface and its generic fibre.

Proposition 2.1.7. *The sections of $\pi : S \to C$ are in natural bijective correspondence with the $k(C)$-rational points of the generic fibre E.*

Proof. Any section $\sigma : C \to S$ defines a curve $D = \sigma(C) \cong C$ inside S which meets every fibre transversally in a single point. The curve D can be extended naturally by the Zariski closure thus it meets the generic fibre in a single $k(C)$-rational point.
Conversely, let P be a $k(C)$-rational point on the generic fibre E. A priori, P is only defined on the smooth fibres, but we can consider the closure Γ of P in S (so that $\Gamma \cap E = P$). Restricting the fibration to Γ, we obtain a birational morphism of Γ onto the non-singular curve C.

$$f_{|\Gamma} : \Gamma \to C.$$

By Zariski's main theorem, $f_{|\Gamma}$ is an isomorphism hence Γ is the unique section associated to the k(C)-rational point P. □

Remark 2.1.8. *Summarizing an elliptic surface S over C (with section) gives rise to an elliptic curve E over the function field $k(C)$ by way of the generic fibre.*

2.2 Kodaira-Néron Model

Given an elliptic curve E over the function field $k(C)$ of a curve C, the Koidara-Néron model describes how to associate an elliptic surface $\pi : S \to C$ over k to E, whose generic fibre returns exactly E.

Definition 2.2.1. Let E be an elliptic curve over the function field $k(C)$ of a curve C. Suppose that there exists an elliptic surface S over C whose generic fibre is isomorphic to $E/k(C)$. In this case, we say that $\pi : S \to C$ (or simply S) is the Kodaira Néron model of $E/k(C)$. We also call S the elliptic surface associated with $E/k(C)$.

Proposition 2.2.2. *Given an elliptic curve over a function field $E/k(C)$, the Kodaira-Néron model exists and is unique up to isomorphisms.*

Proof. We will sketch the main lines about existence, for uniqeness see [4, Theorem 5.19]. At first, we can omit the singular fibres. Here we remove all those points from C where the discriminant vanishes. We indicate the resulting punctured curve by C°. Above every point of C° we read off the fibre, a smooth elliptic curve, from E. This gives a quasi-projective surface S° with a smooth elliptic fibration

$$\pi^\circ : S^\circ \to C^\circ.$$

. Here one can simply think of the Weierstrass equation restricted to C° (after adding the point at ∞ to every smooth fibre). It remains to fill in suitable singular fibres at the points omitted from C. For instance, if the Weierstrass form of E defines a smooth surface everywhere, then all fibres turn out to be irreducible. The singular fibres are either nodal or cuspidal rational curves. If the surface is not smooth somewhere, then we resolve singularities minimally. We will give an explicit description of the desingularisation process in the next sections. □

Remark 2.2.3. *The previous results can be summarize by the following correspondence:*

$$\{relatively\ minimal\ elliptic\ surfaces\ S\ over\ C\} \longleftrightarrow \{elliptic\ curves\ E\ over\ k(C)\}.$$

2.3 Algebraic Surfaces

In order to gain detailed knowledge about algebraic surfaces, it is essential to understand the curves on a given surface S. Here S will always be assumed to be an irreducible smooth projective surface over an algebraically closed field $\bar{k}$. Many notions and constructions considered in this section carry over more or less directly from the case of curves.

Definition 2.3.1. The *divisor group* of an algebraic surface S, denoted by $\mathrm{Div}(S)$, is the group generated by the irreducible subvarieties of codimension 1 of S. Thus a divisor $D \in \mathrm{Div}(S)$ is a formal sum

$$D = \sum_{i=1}^{n} a_i(C_i),$$

where $a_i \in \mathbb{Z}$ and $C_i \subset S$ are irreducible curves lying on the surface S. The $C_i's$ are called *components of the divisor D*.

Recall that for any irreducible curve $C \subset S$, the *local ring of S at C* is

$$\mathcal{O}_{S,C} = \bigcup_{P \in C} \mathcal{O}_{S,P}.$$

The non-singularity of the curves implies that $\mathcal{O}_{S,C}$ is a discrete valuation ring. We denote its valuation by ord_C and $ord_C(f)$ is the degree of vanishing of f along C. We extend this to

$$\mathrm{ord}_C : k(S)^* \longrightarrow \mathbb{Z}$$

and use this to define a homomorphism

$$\mathrm{div} : k(S)^* \longrightarrow \mathrm{Div}(S),$$

$$f \longmapsto \sum \mathrm{ord}_C(f)C.$$

A divisor is *principal* if it is the divisor of a function div(f). Two divisors $D_1, D_2 \in \mathrm{Div}(S)$ are *linearly equivalent* if their difference is principal and we write $D_1 \sim D_2$. Moreover we define the *Picard group* as

$$\mathrm{Pic}(S) := \mathrm{Div}(S)/\sim.$$

Let C_1 and C_2 be irreducible curves on S, and let $P \in C_1 \cap C_2$. Fix local equations $f_1, f_2 \in k(S)^*$ for C_1, C_2 around P, that is $f_i \in \mathcal{O}_{S,P}$ so that $\mathrm{ord}_{C_i}(f_i) = 1$ and $\mathrm{ord}_C(f_i) = 0$ for every other irreducible curve C containing P.

Definition 2.3.2. We say that C_1 and C_2 *intersect trasversally* at P if f_1 and f_2 generate the maximal ideal of the local ring $\mathcal{O}_{S,P}$.

If C_1 and C_2 are irreducible curves that meet everywhere trasversally, then $(C_1.C_2)$ is the number of intersection points. We can extend this definition to all the divisors.

Theorem 2.3.3. *There is a unique symmetric bilinear pairing*

$$\mathrm{Div}(X) \times \mathrm{Div}(X) \longrightarrow \mathbb{Z}, \qquad (D_1, D_2) \longmapsto D_1.D_2,$$

with the following two properties:

1. *If C_1 and C_2 are irreducible curves that meet everywhere trasversally, then $(C_1.C_2) = |(C_1 \cap C_2)|$.*
2. *If $D, D_1, D_2 \in \mathrm{Div}(S)$ are divisors with $D_1 \sim D_2$ then $D.D_1 = D.D_2$.*

Proof. See [2, Theorem III.7.2]. □

Example 2.3.4. Let C_1,$C_2 \subset \mathbb{P}^2$ be curves of degree n_1, n_2 respectively, and let H_1, H_2 be distinct lines. Then

$$\deg(C_i) = n_i = \deg(n_i H_i) \Rightarrow \quad C_i \sim n_i H_i.$$

Further, $(H_1.H_2) = 1$ so we can compute

$$(C_1.C_2) = (n_1 H_1).(n_2 H_2) = n_1 n_2 (H_1 H_2) = n_1 n_2 = \deg(C_1)\deg(C_2).$$

The equality $(C_1.C_2) = \deg(C_1)\deg(C_2)$ over $\mathbb{P}^2$ is called *Bezout's Theorem.*

Theorem 2.3.3 does not give a practical method for computing the intersection of two divisors hence a smarter way is to assign multiplicities to the intersection points as follows:

Definition 2.3.5. Let $D \in \mathrm{Div}(S)$ be a divisor and let $P \in S$. A *local equation* for D at P is a function $f \in k(S)^*$ with the property that

$$P \notin D - \mathrm{div}(f).$$

Now let $D_1, D_2 \in \mathrm{Div}(S)$ be divisors, and let $P \in S$ be a point which does not lie on a common component of D_1 and D_2. Choose local equations $f_1, f_2 \in k(S)^*$ for D_1, D_2 respectively.

Definition 2.3.6. The (*local*) *intersection index of* D_1 *and* D_2 *at* P is defined to be the quantity

$$(D_1.D_2)_P = dim_k \mathcal{O}_{S,P}/(f_1, f_2).$$

Remark 2.3.7. *Notice that* $(D_1.D_2)_P = 0$ *if* $P \in D_1 \cap D_2$, *since if* $P \notin D_i$ *then* $f_i = 1$ *will be a local equation for* D_i *at* P.

The next result explains how the local intersection indices can be used to calculate the global intersection number $D_1.D_2$.

Proposition 2.3.8. *Let* D_1,$D_2 \in \mathrm{Div}(S)$ *be a divisors with no common components. Then the local intersection index* $(D_1.D_2)$ *is finite for all* $P \in S$ *and*

$$(D_1.D_2) = \sum_{P \in D_1 \cap D_2} (D_1.D_2)_P.$$

Proof. See [2, Proposition III.7.4]. □

Example 2.3.9. An important example relating the intersection theory is the *self intersection* $D^2 = (D.D)$ of a divisor D. One approach is to find a $D^{'} \sim D$ with no common components and then compute $(D.D^{'})$.
For example, let C a curve over $\mathbb{P}^2$ of degree n, then by the previous example $C^2 = n^2$. This approach works in this particular case since for any line H , $C \sim nH$. In general, it could be much more difficult to find an appropriate $D^{'}$.

Now we give the definition of *fibered surface*. This is really useful to understand the geometry of the curves over an elliptic surface.

Definition 2.3.10. A *fibered surface* is a non-singular projective surface S, a non-singular curve Γ, and a surjective morphism $\pi : S \to \Gamma$. For any $t \in C$, the *fiber of* S *lying over* t is the curve $S_t = \pi^{-1}(t)$. Note that S_t will be a non-singular curve for all but finitely many $t \in S$. Let $C \subset S$ be an irreducible curve lying on a fibered surface, then $\pi : C \to \Gamma$ is either costant or surjective ([1],II,2.3). If it is constant then C lies in the fiber S_t and we call C *fibral* otherwise *horizontal*.

Remark 2.3.11. *Every elliptic surface is in particular a fibered surface.*

Definition 2.3.12. A divisor $D \in \mathrm{Div}(S)$ on a fibered surface S is called *fibral* if all its components are fibral and is called *horizontal* if all its components are horizontal. Every divisor can be uniquely written as the sum of horizontal divisor and fibral divisor.

2.4 Singular Fibres

In this section we will discuss the possible singular fibres of elliptic surfaces as classified by Kodaira Suppose that $F_v = f^{-1}(v)$ is a singular fibre ($v \in C(k)$). We write it as a divisor on S with multiplicities:

$$F_v = \sum_{i=0}^{m_v-1} \mu_{v,i}\Theta_{v,i}$$

where

- m_v is the number of the (distinct) irreducible components in F_v ,
- $\Theta_{v,i}$ ($0 \leq i \leq m_{v-1}$) are the irreducible components,
- $\mu_{v,i}$ the multiplicity of $\Theta_{v,i}$ in F_v (a positive integer).

Theorem 2.4.1. *1. There exists a unique component of F_v which intersects the zero section (O); it is called the identity component and denoted by $\Theta_{v,0}$. The coefficient $\mu_{v,0} = 1$.*

2. If F_v is an irreducible singular fibre (i.e. $m_v = 1$ and $F_v = \Theta_{v,0}$) , then $\Theta_{v,0}$ is either a rational curve with a node (type I_1) or a rational curve with a cusp (type II).

3. If F_v is a reducible singular fibre ($m_v > 1$) then every component $\Theta_{v,i}$ is a smooth rational curve which has self-intersection number (-2).

Proof. The first two statements of the theorem are clear; the third often files under the title of Zariski's lemma [4, Theorem 5.11]. □

Now we are ready for the complete classification of the singular fibres.

Theorem 2.4.2. *All possible types of reducible singular fibres are classified into the following types with $m > 1$ and $b \geq 0$:*

$$I_m, I_b^*, III, IV, II^*, III^*, IV^*.$$

(for semplicity, we write m and Θ_i dropping the subscript v).

- *I_m : $F_v = \Theta_0 + ... + \Theta_{m-1}$, where for $m \geq 3$, $(\Theta_i.\Theta_{i+1}) = 1$ for all $i = 0, 1, ..., m-1$ ciclically, i.e. $(\Theta_{m-1}.\Theta_0) = 1$. For $m = 2$, $(\Theta_{m-1}.\Theta_0) = 2$.*
- *I_b^* : $F_v = \Theta_0 + ... + \Theta_3 + 2\Theta_4 + ... + 2\Theta_{b+4}$, $m = b + 5$, $b \geq 0$. Here $(\Theta_0.\Theta_4) = (\Theta_1.\Theta_4) = 1$, $(\Theta_2.\Theta_{b+4}) = (\Theta_3.\Theta_{b+4}) = 1$ and $(\Theta_4.\Theta_5) = ... = (\Theta_{b+3}.\Theta_{b+4}) = 1$.*
- *III : $F_v = \Theta_0 + \Theta_1$, $m = 2$, where the two components intersect at a single point with $(\Theta_0.\Theta_1) = 2$.*
- *IV : $F_v = \Theta_0 + \Theta_1 + \Theta_2$, $m = 3$, where all three components meet at a single point and $(\Theta_0.\Theta_1) = (\Theta_0.\Theta_2) = (\Theta_1.\Theta_2) = 1$.*

- $II^* \, : \, F_v = \Theta_0 + 2\Theta_7 + 3\Theta_6 + 4\Theta_5 + 5\Theta_4 + 6\Theta_3 + 4\Theta_2 + 2\Theta_1 + 3\Theta 8, \quad m = 9,$ *where* $(\Theta_0.\Theta_7) = (\Theta_7.\Theta_6) = (\Theta_6.\Theta_5) = (\Theta_5.\Theta_4) = (\Theta_4.\Theta_3) = (\Theta_3.\Theta_2) = (\Theta_2.\Theta_1) = (\Theta_3.\Theta_8) = 1.$

- $III^* \, : \, F_v = \Theta_0 + 2\Theta_1 + 3\Theta_2 + 4\Theta_3 + 3\Theta_4 + 2\Theta_5 + \Theta_6 + 2\Theta_7, \; m = 8,$ *where* $(\Theta_0.\Theta_1) = (\Theta_1.\Theta_2) = (\Theta_2.\Theta_3) = (\Theta_3.\Theta_4) = (\Theta_4.\Theta_5) = (\Theta_5.\Theta_6) = (\Theta_3.\Theta_7) = 1.$

- $IV^* \; F_v = \Theta_0 + \Theta_1 + 2\Theta_2 + 3\Theta_3 + 2\Theta_4 + \Theta_5 + 2\Theta_6, \; m = 7,$ *where* $(\Theta_1.\Theta_2) = (\Theta_2.\Theta_3) = (\Theta_3.\Theta_4) = (\Theta_4.\Theta_5) = (\Theta_3.\Theta_6) = (\Theta_6.\Theta_0) = 1.$

Proof. The proof that our list is complete generally amounts to Tate's algorithm over perfect fields. □

2.5 Tate's algorithm

In this section we shall discuss Tate's algorithm to some extent. The missing details could be found in the original exposition of Tate or in chapter IV of [2].
Essentially Tate's algorithm takes as input a Weierstrass equation of an elliptic curve and computes, among other things, the reduction type and the (local) minimal Weierstrass form.

For the sake of simplicity, we shall limit ourselves to perfect fields of characteristic different from two. This restriction enables us to work with an *extended Weierstrass equation* :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

The discriminant is given by

$$\Delta = -27a_6^2 + 18a_2a_4a_6 + a_2^2a_4^2 - 4a_2^3a_6 - 4a_4^3.$$

In order for a fibre to be singular, the discriminant Δ has to vanish. Very much to our advantage, we can work locally, so we fix a local parameter t on C with normalized valuation ν. Assume that there is (or rather there could be) a singular fibre at $t = 0$, that is, the vanishing order of Δ at $t = 0$ satisfies $\nu(\Delta) > 0$. By a translation in x, we can move the singularity to $(0, 0)$. Then the extended Weierstrass form transforms to

$$y^2 = x^3 + a_2'x^2 + ta_4'x + ta_6'.$$

If $t \nmid a_2'$ then the above equation at $t = 0$ describes a nodal rational curve. We call the reduction *multiplicative*. If $t|a_2'$, then the equation defines a *cuspidal* rational curve at $t = 0$. We call it *additive* reduction. In either case, the special point $(0, 0)$ is a surface singularity if and only if $t|a_6^{'}$.
Let $t \nmid a_2$. From the summand ${a_2'}^3ta_6'$ of Δ, it is immediate that $(0, 0)$ is a surface singularity if and only if

$$\nu(\Delta) > 1.$$

Otherwise $(0, 0)$ is only a singularity of the fibre, but not of the surface. Hence the singular fibre at t = 0 is the irreducible nodal rational curve with associated Kodaira symbol I_1. Assume now that $\nu(\Delta) > 1$. We have to resolve the singularity at $(0,0)$. Let m the greatest integer not exceding $n/2$. Then translate x such that $t^{m+1}|a_4$:

$$y^2 = x^3 + a_2''x^2 + t^{m+1}a_4''x + a_6''.$$

Then $\nu(\Delta) = n$ is equivalent to $\nu(a_6^{''})$. Now we blow up the surface m times successively at the point $(0,0)$. The first $(m-1)$ blow-ups introduce two $\mathbb{P}^1$'s each. In the chart $x' = t^j x$, $y' = t^j y$ for the jth blow-up, the exceptional divisors are locally given by

$$y^{'2} = a_2(0)x^{'2}.$$

In particular, the exceptional divisors come in pairs of rational curves which are conjugate over $k(\sqrt{a_2(0)})/k$. Depending on whether $\sqrt{a_2(0)} \in k$ or not, one distinguishes split and non-split multiplicative reduction.
After each blow-up $(j = 1, ..., m-2)$, we continue with another blow-up at $(0,0)$, the intersection point of the two latest exceptional divisors. After the final blow-up, the local equation of the special fibre is

$$y^2 = a_2(0)x^2 + (a_6''/t^{2m})(0).$$

One easily checks that this encodes a single rational component, if $n = 2m$ is even, or again two components if $n = 2m+1$ is odd. In either case, the surface blown up $(m-1)$-times is smooth locally around $t = 0$,so we have reached the resolution of the surface singularity in the special fibre. In summary, the process of desingularization has added $(n-1)$ rational curves of self-intersection -2. Hence the singular fibre consists of a cycle of n rational curves, meeting transversally. In this case Koidara symbol associated is I_n.
Consider the case $t|a_2'$. We have to determine whether $(0,0)$ is a surface singularity, i.e. whether $t|a_6'$. If the characteristic is different from 2 and 3, then this is equivalent to

$$\nu(\Delta) > 2.$$

If $(0,0)$ is a smooth surface point, then the singular fibre is a cuspidal rational curve. We denote it by the Kodaira type II.
If $(0,0)$ is a surface singularity, there are three possibilities for the exceptional divisor of the first blow-up:

1. a rational curve of degree two, meeting the strict transform of the cuspidal curve tangentially in one point;

2. Two lines, possibly conjugate in a quadratic extension of k, meeting the strict transform of the cuspidal curve in one point;

3. a double line.

In the first two cases, we have reached the desingularization and refer to type III resp. IV. The third case requires further blow-ups, each introducing lines of multiplicity up to six and self-intersection (-2). The resolution process branches into three cases here depending on the singularities on the double line:

1. three rational double points, type I_0^*;

2. two singularities, type $I_n^*, n > 0$.

3. one singularity, types II^*, III^*, IV^* or non-minimal.

If the characteristic differs form 2 and 3, then we can determine the type of singular fibre directly from the discriminant and the vanishing orders of a_4 and a_6. This is due to the simplified Weierstrass form (1.3) of the equation of the fibre. In ([3], pg. 66) it is possible to find a table which encodes information about these cases.

In the non-minimal case $\nu(a_i) \geq i$ for each i. This means that the singularity of the Weierstrass model is not a rational double point and we can simplify the Weierstrass form locally as follows: Pick a local coordinate t of the base curve such that the special fibre sits at $t = 0$. Then rescale by the admissible transformation

$$(x, y) \to (t^2 x, t^3 y),$$

we obtain an isomorphic equation that is integral at t. Such a transformation lets $\nu(\Delta)$ drop by 12, hence it can only happen a finite number of times. We call this process minimalising and the resulting equation the $minimal\ Weierstrass\ form$ (locally at t = 0).

Remark 2.5.1. *The notion of minimality involves a little subtlety. Namely, we work in the coordinate ring $k(C)$ of a chosen affine open of the base curve C. For instance, if the base curve C is isomorphic to $\mathbb{P}^1$, then $k(C) = k(t)$ and every ideal in $k(C)$ is principal. In consequence of Corollary 1.6.6, an elliptic surface over $\mathbb{P}^1$ admits a global minimal Weierstrass equation(1.6.5). In general there might not be a global minimal Weierstrass form.*

2.6 Mordell-Weil Group and Neron-Severi lattice

We have seen how a rational point on the generic fibre gives rise to a section on the corresponding elliptic surface and viceversa (Remark 2.2.3). In this section we go deeper in the theory. From now on we use $K = k(C)$.

Definition 2.6.1. The K-rational points $E(K)$ form a group which is traditionally called Mordell-Weil group. We will usually denote the points on E by P, Q.

Each point P determines a section $\bar{P} : C \to S$ which we interprete as a divisor on S. To avoid confusion, we shall denote this curve by $\bar{P}$. Moreover we define another object

Definition 2.6.2. The Neron-severi group of an elliptic surface is defined as

$$\mathrm{NS}(S) = \mathrm{Div}(S)/\approx,$$

where $\approx$ denotes the algebraic equivalence. The rank of $\mathrm{NS}(S)$ is called the Picard number:

$$\rho(S) = rank(\mathrm{NS}(S)).$$

Roughly speaking, two divisors are called algebraically equivalent ($D \approx D'$) if they belong to the same family of divisors on X.

Remark 2.6.3. *In the case of an elliptic fibration $\pi : S \to C$ any two fibres are algebraically equivalent.*

We now state the three fundamental results that relate the Mordell-Weil group and the Neron-Severi group of an elliptic surface with section. All theorems require our assumption that the elliptic surface has a singular fibre.

Theorem 2.6.4. *$E(K)$ is finitely generated group.*

This result is a special case of the Mordell-Weil theorem, in generality for abelian varieties over suitable global fields. Here we will sketch the geometric argument. The first step is to prove the corresponding result for the Neron-Severi group.

Theorem 2.6.5. NS(S) *is finitely generated and torsion-free.*

Proof. The finiteness part is again valid in more generality for projective varieties as a special case of the theorem over abelian varieties. On an elliptic surface, one can use intersection theory to prove both claims. The connection between these two theorems is provided by a third theorem. □

Theorem 2.6.6. *Let T denote the subgroup of* NS(S) *generated by the zero section and fibre components. Then the map $P \to \bar{P}$ mod T gives an isomorphism*

$$E(K) \equiv \mathrm{NS}(S)/T.$$

In other words, the above theorem states that NS(S) is generated by fibre components and sections. In the sequel, we sketch the main lines of proof of the previous theorem.

Definition 2.6.7. Let D,$D' \in \mathrm{Div}(S)$. We say they are *numerically equivalent*:

$$D \equiv D' \ \ if \ \ (D.C) = (D'.C) \ \ \forall C \subset S.$$

We have the following implication

Lemma 2.6.8. *On any projective surface, algebraic equivalence implies numerical equivalence.*

Proof. See [4, Lemma 4.15]. □

The intersection of divisors defines a symmetric bilinear pairing on NS(S). It endows NS(S) up to torsion with the structure of an integral lattice, the Neron-Severi lattice.

Lemma 2.6.9. *Modulo numerical equivalence, the Neron-Severi group is finitely generated.*

Proof. See [3, Lemma 6.4]. □

This result is very convenient for practical reasons, since we can now solve problems concerning divisor classes in NS(S) simply by calculating intersection numbers.

Definition 2.6.10. The trivial lattice $\mathrm{Triv}(S)$ is the sublattice of $\mathrm{NS}(S)$ generated by the zero section and fibre components.

Since any two fibres are algebraically equivalent, the only fibre components we have to consider for the trivial lattice are a general fibre F and fibre components not met by the zero section. Using the same notation of the section about singular fibres, we can decompose the trivial lattice $\mathrm{Triv}(S) \subset \mathrm{NS}(S)$ as orthogonal sum

$$\mathrm{Triv}(S) = \big\langle (O), F \big\rangle \oplus \bigoplus_{v \in R} T_v,$$

where R denotes the finite subset of points on the base curve where the singular fibres are located. The following proposition clarify why $\mathrm{Triv}(S)$ is so important.

Proposition 2.6.11. *The divisor classes of* $\{\bar{O}, F, \Theta_{v,i}; v \in R, 1 \le i \le m_v - 1\}$ *form a* $\mathbb{Z}$*-basis of* T*. In particular*

$$rank(T) = 2 + \sum_{v \in R} m_v - 1.$$

Proof. See [3, Proposition 6.6]. □

Now we prove Theorem 2.6.6 and Theorem 2.6.4 descends as corollary.

Proof. The idea is to exhibit a map inverse to the function given in the statement. For this purpose, it will be convenient to view the generic curve E as a curve on S. We start by defining a homomorphism

$$\mathrm{Div}(S) \to \mathrm{Div}(E),$$

as follows: As stated in 2.3.12, any divisor D on S decomposes into a horizontal part, consisting of sections and a vertical divisor consisting of fibre components:

$$D = D' + D'', \quad D' \text{ horizontal}, D'' \text{ vertical}.$$

Then the horizontal part D' and E intersect properly, giving a divisor on E of degree $(D'.E)$. This (K-rational) divisor is called the restriction of D to E:

$$D_{|E} := D' \cap E \in \mathrm{Div}(E).$$

In terms of *linear equivalence* $\sim$ (on E and S), it easy to see that

$$D_{|_E} \sim_E 0 \iff D \sim_S D'', \quad D'' \ \text{ vertical}.$$

By Abel's Theorem [4, Lemma 3.5], for E over K, the divisor D determines a unique point $P \in E(K)$ by the following linear equivalence of degree zero divisors:

$$D_{|_E} - (D'.E)O \sim_E P - O.$$

Therefore we can define a homomorphism

$$\psi : \mathrm{Div}(S) \to E(K).$$

$$\psi(D) = P.$$

The kernel of ψ can be seen to be

$$\ker(\psi) = \big\langle D \in \mathrm{Div}(S); D \approx 0 \big\rangle + \mathbb{Z}\bar{O} + \big\langle D \in \mathrm{Div}(S); D \text{ vertical} \big\rangle.$$

Hence ψ induces the claimed isomorphism. □

Corollary 2.6.12. *Let S be an elliptic surface with section. Denote the generic fibre by E. Then*

$$\rho(S) = rankT + rankE(K) = 2 + \sum_{v \in R}(m_v - 1) + rankE(K).$$

2.7 Rational Surfaces

In this thesis we will study a particular type of elliptic surface called *rational*. It is known that these surfaces have some important properties but first we recall some results by Tate's algorithm section.

Lemma 2.7.1. *Any elliptic surface over $\mathbb{P}^1$ admits a globally minimal Weierstrass equation with polynomial coefficients $a_i(t) \in k(t)$:*

$$y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t).$$

Proof. It is Remark 2.5.1. □

In terms of the Weierstrass form with polynomial coefficients, minimality requires

$$\nu(a_4) < 4 \quad \text{or} \quad \nu(a_6) < 6 \quad \text{each place of } \mathbb{P}^1.$$

After minimalising at all finite places, we fix the smallest integer n such that $\deg(a_i) \leq ni$. Throughout a change of variables, we derive a local equation at ∞ with coefficients

$$a_i' = s^{ni}a_i(1/s).$$

Alternatively, we can homogenize the coefficients $a_i(t)$ as polynomials in two variables s,t of degree ni. Then the discriminant is a homogeneous polynomial of degree $12n$. The integer n has an important property: It determines how an elliptic surface over $\mathbb{P}^1$ with section fits into the classification of projective surfaces. We let k denote the Kodaira dimension. For a rational elliptic surface we have $n = 1$ and $k = -\infty$.

Definition 2.7.2. A *rational elliptic surface* S is a (smooth projective) rational surface over $k(= \bar{k})$, which is given with a relatively minimal elliptic fibration $\pi : S \to C$.

Remark 2.7.3. *Recall that S is called a rational surface over k if its function field $k(S)$ is a purely transcendental extension of dimension 2 over k, or equivalently, if S is birationally equivalent to the projective plane $\mathbb{P}^2$.*

In the case of a rational elliptic surface, the base curve C is the projective line: $\mathbb{P}^1$ and $K = k(t)$ is a rational function field. This follows, for instance , directly from Lüroth's theorem stating that the only function field $k(C)$ contained in a purely transcendental extension of k is a rational function field.

Proposition 2.7.4. *Let E an elliptic curve over the function field $k(t)$ with global minimal Weierstrass form*

$$E : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

where $a_i \in k(t)$ for each i. Then the associated elliptic surface $\pi : S \to \mathbb{P}^1$ is a rational elliptic surface if and only if

$$\deg a_i(t) \leq i \quad \forall i.$$

Proof. The necessity is clear by above argument. Conversely, such a generalised Weierstrass form defines a rational elliptic surface if and only if it has a singular fibre. That is, no admissible transformation makes each a_i into an ith power. In particular, this holds if the discriminant Δ is not a twelfth power. The last characterization is an equivalence if $\mathrm{char}(k) \neq 2, 3$. The exceptions in those characteristics are due to the existence of wild ramification. Further details can be found in [4], Sect.5.9. □

Proposition 2.7.5. *The Néron-Severi lattice* $\mathrm{NS}(S)$ *is unimodular and of rank* $\rho = 10$.

Proof. See [4, Proposition 7.1]. □

Chapter 3

Main Results

In this chapter we want to analyze the family of elliptic curves $y^2 = x(x-p)(x-q)$ where $\{p, q\}$ is a pair of twin primes and we show that the rank of these curves oscillates between 0 and 1 while as elliptic surface the $rkMW(Y, \pi) = 0$. Moreover assuming that there are infinite pairs of twin primes, we will find that both $\mathcal{N}(Y, \pi)$ and $\mathcal{I}(Y, \pi)$ are infinite.

3.1 The rational elliptic surface

Let t be the affine coordinate on $\mathbb{P}^1$. Consider the elliptic surface $\pi : Y \to \mathbb{P}^1$ defined over $\mathbb{Q}$ by the affine Weierstrass equation

$$y^2 = x(x-(t-2))(x-t).$$

Lemma 3.1.1. *The elliptic surface is non-isotrivial and rational. It has 3 singular fibres: at $t = 0$ of Kodaira type I_2, at $t = 2$ of Kodaira type I_2 and at $t = \infty$ of Kodaira type I_2^*.*

Proof. The discriminant of the elliptic surface is $4t^2(t-2)^2$. Using Tate algorithm we obtain the classification of the singular fibres. □

Lemma 3.1.2. *We have $rk\ MW(Y, \pi) = 0$. In fact, the group of sections over $\mathbb{C}$ is formed by the 2-torsion sections.*

Proof. Let us base change to $\mathbb{C}$. Since $\pi : Y \to \mathbb{P}^1$ is a rational elliptic surface with singular fibres I_2, I_2, I_2^*, its group of sections is given in the entry 71 of the Main Theorem of [6].

□

3.2 Parity of the rank of elliptic curves

In order to show that both $\mathcal{I}(Y, \pi)$ and $\mathcal{N}(Y, \pi)$ have infinite cardinality, we now study the rank of elliptic curves $y_{p,q} = x(x-p)(x-q)$ where (p, q) is a pair of twin primes.
In appendix A, we briefly discuss the main properties of twin primes. In particular, every pair of twin primes greater than $(3, 5)$ is of the form $(6n-1, 6n+1)$ for some natural number n. Our goal requires us to focus solely on the latter case.

Notation 2. From now on every twin prime pair is meant to be of the form $(p, q) = (6n - 1, 6n + 1)$ for some $n \in \mathbb{N}$ so that $p > 3$ and $q > 5$.

Lemma 3.2.1. *Let (p, q) be a twin prime pair and $E_{p,q}$ associated elliptic curve $y_{p,q} = x(x - p)(x - q)$. Then $E_{p,q}$ has multiplicative reduction at p and q (split reduction at one of the primes and non-split reduction at the other prime), an additive reduction at 2 and good reduction at all other primes.*

Proof. The discriminant of $E_{p,q}$ is $\Delta = 2^6 p^2 q^2$ hence the bad primes are $2, p, q$. Reducing the equation modulo p and q we obtain

$$y^2 = x^3 - 2x^2 \ (mod\ p), \qquad\qquad y^2 = x^3 + 2x^2 \ (mod\ q).$$

Both these curves are cubic curves with a node. Now the tangent lines at (0,0) are given by the equations

$$y^2 = -2x^2 \ (mod\ p), \qquad\qquad y^2 = 2x^2 \ (mod\ q).$$

Therefore $E_{p,q}$ has split multiplicative reduction at p if (-2) is a square over $\mathbb{F}_p$ and has split multiplicative reduction at q if 2 is a square over $\mathbb{F}_q$. Using Legendre symbol properties (see appendix B) we deduce that if p is congruent to 1 or 3 modulo 8 then (-2) is a square over F_p otherwise 2 is a square over F_q. It remains to analyze the reduction at 2. The associated equation is

$$y^2 = x(x + 1)^2$$

and changing the variables $x \to x$ and $y \to x + y$ we obtain the standard cusp form

$$y^2 - x^3 = 0.$$

□

Now we analyze the parity of the rank of the elliptic curves $E_{p,q}$. In particular, we need to study $w(E/\mathbb{Q}_2)$. We refer to [7] for a complete review of the theory of Root numbers and parity phenomena. We are mainly interested in the table of Appendix A in [7]. Since $(C_\Delta, C_6, C_4) = (6\ , \geq 7,\ 4)$ and $c_4^{'} \equiv 3\ \ (mod\ 4)$ for every $E_{p,q}$, there are only 2 cases to study:
if $c_4^{'} - 4c_{6,7} \equiv 7\ or\ 11\ \ (mod\ 16)$ than $w(E/\mathbb{Q}_2) = +1$ otherwise $w(E/\mathbb{Q}_2) = -1$.

Lemma 3.2.2. *Let $n \in \mathbb{N}$ such that (6n-1 , 6n+1) is pair of twin primes. If $4n^2 - 12n + 3 \equiv 11$ or 7 $(mod\ 16)$ than $w(E/\mathbb{Q}) = 1$ otherwise $w(E/\mathbb{Q}) = -1$.*

Proof. $w(E/\mathbb{Q}) = -\prod_{l=2,p,q} w(E/\mathbb{Q}_l)$ and $w(E/\mathbb{Q}_p)w(E/\mathbb{Q}_q) = -1$ hence
$w(E/\mathbb{Q}) = w(E/\mathbb{Q}_2)$. Further $c_4^{'} - 4c_{6,7} = 4n^2 - 12n + 3$ therefore
if $4n^2 - 12n + 3 \equiv 11\ or\ 7\ (mod\ 16)$ than $w(E/\mathbb{Q}) = 1$ otherwise $w(E/\mathbb{Q}) = -1$. □

Remark 3.2.3. *Every $n \in \mathbb{N}$ congruent to $\{1, 2\}$ mod 4 satisfies the upper congruence while every n congruent to $\{0, 3\}$ mod 4 does not.*

3.3 The Descent Method

In this section, through the 2-Descent-Method, we bound the rank of the family of elliptic curves $E_{p,q}$.

Lemma 3.3.1. *For every twin prime pair the associated elliptic curve $E_{p,q}$ has rank at most 3.*

Proof. It is a direct conseguence of 3.2.1 and of Proposition 5.6 of [8]: the rank r of an elliptic curve E over $\mathbb{Q}$ satisfies

$$r \leq t_1 + 2t_2 - 1.$$

Here t_1 indicates the number of primes where $E/\mathbb{Q}$ has a multiplicative reduction and t_2 the number of primes of addittive reduction. □

Even if this is a powerful lemma, it is not enough to exclude the possibilities of rank $= 2$ or 3 so we need to apply the 2-Descent method.
Let (p, q) pair of twin primes and $E_{p,q}$ the associated elliptic curve

$$y^2 = x(x - p)(x - q). \tag{3.1}$$

Reducing the equation modulo 3, we check that the cardinality of $E_{p,q}(\mathbb{F}_3) = 4$. Since $E[2] \subset E_{tors}(\mathbb{Q})$ and $E_{tors}(\mathbb{Q})$ injects into $E_{p,q}(\mathbb{F}_3)$ we see that

$$E_{tors}(\mathbb{Q}) = E[2]$$

A complete set of representative is given by

$$\mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm pq, \pm 2p, \pm 2q, \pm 2pq\}.$$

Now we consider the map given in Proposition 1.7.2:

$$E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2),$$

say with

$$e_1 = 0, \qquad e_2 = p, \qquad e_3 = q.$$

There are 256 pairs $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ and for each pair, we must check to see whether it comes from an element of $E(\mathbb{Q})/2E(\mathbb{Q})$. Firstly we compute the image of $E[2]$ in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$

$$O \to (1, 1), \quad (0, 0) \to (pq, -p), \quad (p, 0) \to (p, -2p), \quad (q, 0) \to (q, 2).$$

It remains to determine for every other pair (b_1, b_2) whether the system

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = p \\ b_1 z_1^2 - b_1 b_2 z_3^2 = q \end{cases} \tag{3.2}$$

Has a solution $z_1, z_2, z_3 \in \mathbb{Q}$. Proceding systematically we now reduce the number of cases that must be considered.

1. if $b_1 < 0$ and $b_2 > 0$ then $b_1z_1^2 - b_2z_2^2 = p$ has no solution over $\mathbb{R}$.

2. if $b_1 < 0$ and $b_2 < 0$ then $b_1z_1^2 - b_1b_2z_3^2 = q$ has no solution over $\mathbb{R}$.

3. the four 2-torsion points $\{O, (0,0), (p,0), (q,0)\}$ map respectively to the four point $(1,1)$, $(pq, -p)$, $(p, -2p)$, $(q, 2)$.

4. if (b_1, b_2) is in the image of Mordell-Weil group, the same is true for $(b_1, b_2)(pq, -p) = (pqb_1, -pb_2)$ and similarly $(pb_1, -2pb_2)$, $(qb_1, 2b_2)$ hence we can assume that $b_1 \in \{1, -1, 2, -2\}$. Moreover by the first point we can conclude that $b_1 \in \{1, 2\}$.

5. If p divides b_2 but not b_1 then there are no solutions. Indeed consider the p-adic valuation $\nu_p : \mathbb{Q} \to \mathbb{Z}$ and the p-adic field $\mathbb{Q}_p$. If the system (3.2) has a solution in $\mathbb{Q}$ then it has solution in the p-adic field. Observe that $\nu_p(b_1z_1^2 - b_2z_2^2) = 1$ and $\nu_p(b_1z_1^2 - b_2z_2^2) \geq \min\{2\nu_p(z_1), 1 + 2\nu_p(z_2)\}$. The equality holds if $2\nu_p(z_1) \neq 1 + 2\nu_p(z_2)$ which is true because the former is even and the latter is odd. We conclude that $1 + 2\nu_p(z_2) = 1 \iff \nu_p(z_2) = 0$ and $\nu_p(z_1) \geq 1$. Consider now $\nu_p(b_1z_1^2 - b_1b_2z_3^2) = \min\{2\nu_p(z_1), 1 + 2\nu(z_3)\} = 0$. We know that $\nu_p(z_1) > 0$ hence $1 + 2\nu_p(z_3) = 0$ which is impossible.

6. if q divides b_2 but not b_1 there are no solutions. Similar proof of point (5).

7. If $2|b_1$ and $2 \nmid b_2$ there are no solutions. Indeed suppose by contradiction that the system (3.2) has solution in $\mathbb{Q}$ then it has solution in $\mathbb{Q}_2$. Consider the 2-adic valuation $\nu_2 : \mathbb{Q} \to \mathbb{Z}$ and observe that $\nu_2(b_1z_1^2 - b_2z_2^2) = 0$.
   Moreover $\nu_2(b_1z_1^2 - b_2z_2^2) = \min\{1 + 2\nu_2(z_1), 2\nu(z_2)\}$ then $\nu_2(z_1) \geq 0$ and $\nu_2(z_2) = 0$. On the other hand, $\nu_2(b_1z_1^2 - b_1b_2z_3^2) = 0$ implies $\nu_2(z_1) < 0$ and $\nu_2(z_3) < 0$.

8. If $2|b_1$ and $2|b_2$ there are no solutions. Indeed suppose by contradiction that the system (3.2) has solution in $\mathbb{Q}$ then it has solution in $\mathbb{Q}_2$. Consider the 2-adic valuation $\nu_2 : \mathbb{Q} \to \mathbb{Z}$ and observe that $\nu_2(b_1z_1^2 - b_2z_2^2) = 0$.
   Moreover $\nu_2(b_1z_1^2 - b_2z_2^2) = \min\{1 + 2\nu_2(z_1), 1 + 2\nu(z_2)\}$ then $\nu_2(z_1) < 0$ and $\nu_2(z_2) < 0$. On the other hand $b_1b_2 = b_1^{'}b_2^{'}$ where $(2, b_1^{'}, b_2^{'}) = 1$ hence $\nu_2(b_1z_1^2 - b_1^{'}b_2^{'}z_3^2) = \min\{1 + 2\nu_2(z_1), 2\nu_2(z_3)\} = 0 \Rightarrow \nu_2(z_3) = 0$ and $\nu_2(z_1) = 0$.

Remark 3.3.2. *These observations substantially reduces the number of cases that must be considered to the pairs* $(b_1, b_2) = (1, 2), (1, -1), (1, -2)$.

Lemma 3.3.3. *Suppose that* $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ *where* $b_1 = 1$ *and* $b_2 \in \{-1, \pm 2\}$ mod $(\mathbb{Q}^*)^2$ *is the image of a point* $P \in E_{p,q}(\mathbb{Q})/2E_{p,q}(\mathbb{Q})$. *Then* $(b_1, b_2) = (1, 2) \iff p \equiv 7 \bmod 8$ *or* $(b_1, b_2) = (1, -2) \iff p \equiv 1 \bmod 8$.

Proof. As we have seen before, it is enough to considerate just three cases.
Let $(b_1, b_2) = (1, 2)$. Observe that $\nu_p(z_1^2 - 2z_2^2) = 1$ and $\nu_p(z_1^2 - 2z_2^2) \geq \min\{2\nu_p(z_1), 2\nu_p(z_2)\}$. If $\nu_p(z_1) \neq \nu_p(z_2)$ then $\min\{2\nu_p(z_1), 2\nu_p(z_2)\} = 1$ which is impossible therefore $\nu_p(z_2) = \nu_p(z_1)$. Since $\mathbb{Q} \subset \mathbb{Q}_p$, we can write $z_1 = p^t(a_1 + pu_1)$ and $z_2 = p^t(a_2 + pu_2)$ where $a_1, a_2 \in \{0, 1, ..., p-1\}$, u_1 and u_2 are units of p-adic field and $t \in \mathbb{Z}$. Substituting

z_1 and z_2 in the first equation of (3.2), multiplying on the right and on the left side by p^{-2t} and reducing modulo p we obtain

$$a_1^2 - 2a_2^2 \equiv 0 \mod p. \tag{3.3}$$

Equation (3.3) admits solution $\iff \left(\frac{2}{p}\right) = 1$. As shown in appendix B.1, this means that $p \equiv 1, 7 \mod 8$.

The same reasoning for the q-adic field and q-adic valuation gives us

$$a_1^2 - 2a_2^2 \equiv 0 \mod q. \tag{3.4}$$

Equation (3.4) admits solution $\iff \left(\frac{2}{q}\right) = 1$ i.e. $q \equiv 1, 7 \mod 8$. Summarizing the system (3.2) admits solution $\iff p \equiv 7 \bmod 8$ and $q \equiv 1 \bmod 8$.

Let $(b_1, b_2) = (1, -2)$. Similar proof as before. In this case the conditions are

$$\left(\frac{-2}{p}\right) = 1, \qquad \left(\frac{-2}{q}\right) = 1.$$

If $p \equiv 1$ modulo 8 then $q \equiv 3$ modulo 8 and this is admissible condition.
If $p \equiv 3$ modulo 8 $\Rightarrow q \equiv 5$ modulo 8 and this not satisfy the system.

Let $(b_1, b_2) = (1, -1)$. This is not an admissible case.
Observe that $\nu_p(z_1^2 + z_2^2) = 1$ and $\nu_p(z_1^2 + z_2^2) \geq \min\{2\nu_p(z_1), 2\nu_p(z_2)\}$. If $\nu_p(z_1) \neq \nu_p(z_2)$ then $\min\{2\nu_p(z_1), 2\nu_p(z_2)\} = 1$ which is impossible therefore $\nu_p(z_2) = \nu_p(z_1)$. Repeating the same procedure of the upper point we obtain the conditions

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{-1}{q}\right) = 1.$$

This is impossible because $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1$ modulo 4, see appendix B.1, but then $q \equiv 3$ modulo 4 and $\left(\frac{-1}{q}\right) = -1$.

□

3.4 Final Results

The final step is to show that for every n congruent to $\{0, 3\}$ modulo 4 such that $(6n - 1, 6n + 1)$ is a pair of twin prime, the associated elliptic curve $E_{p.q}$ has rank ≤ 1 while the elliptic curves associated to n congruent to $\{1, 2\}$ modulo 4 have rank 0.

Proposition 3.4.1. *Let $n \in \mathbb{N}$ such that $(p, q) = (6n-1, 6n+1)$ is a pair of twin primes and let $E_{p.q}$ the associated elliptic curve of equation $y^2 = x(x-p)(x-q)$.*
If $n \in \{1, 2\} \bmod 4$ then $rkE_{p.q} = 0$ otherwise $n \in \{0, 3\} \bmod 4$ then $rkE_{p.q} \leq 1$ and if the Parity Conjecture is true, then the equality holds.

Proof. As seen in the previous section, there are 2 possible cases that correspond to the image of a point of infinite rank on the elliptic curve.

1. If $n \equiv 0 \mod 4 \Rightarrow p \equiv -1 \mod 8 \Rightarrow (b_1, b_2) = (1, 2)$.
2. If $n \equiv 3 \mod 4 \Rightarrow p \equiv 1 \mod 8 \Rightarrow (b_1, b_2) = (1, -2)$.
3. If $n \equiv 1, 2 \Rightarrow p$ is congruent respectively to $5, 4 \mod 8$ hence there are no points of infinite order.

It remains to prove that if $n \equiv 0$ *or* 3 modulo 4, the system (3.2) admits a solution $(z_1, z_2, z_3) \in \mathbb{Q}$. We can achieve this result by assuming the Parity Conjecture and easily conclude that $rkE_{p.q} = 1$. □

3.5 Computational aspects

The computation of the Mordell-Weil group of an elliptic curve remains one of the most challenging problems in modern mathematics. To date, no universal algorithm exists that works for all elliptic curves. In this section, we utilize the free computer package Pari [11] to calculate rational points in specific cases.

Additionally, it is intriguing to examine the cardinalities of $\mathcal{N}(Y, \pi)$ and $\mathcal{I}(Y, \pi)$ assuming the validity of the parity conjecture. To investigate how many elliptic curves of rank 0 and 1 exist within a given range of natural numbers, the following code proves to be particularly useful.

```
from matplotlib import pyplot as plt
import numpy as np
from math import sqrt
def prime(number):
    if number <= 1:
        print(False)
    for i in range(2, int(number**0.5) + 1):
        if number % i == 0:
            return False
    return(True)

#check if n natural number is prime

def twins(n):

    if prime(6*n-1)==True and prime(6*n+1)==True:
        return True
    else:
        return False

#check if n produces a pair of twin primes

def atwins(n):
    for m in range(1,n+1):
        if twins(m)== True:
            print(m,[6*m-1,6*m+1])

# print all m natural numbers less then n that produce a pair of twin primes

def rank(n):
    a = 4
    b = -12
    c = 3
    d = 11
    e = 7
    modulo = 16
    if (a*n**2 + b*n + c - d)%modulo == 0:
        return([n,0])
    elif (a*n**2 + b*n + c - e)%modulo == 0:
        return([n,0])
    else:
        return([n,1])

# This function checks if the elliptic curve E_{p,q} associated to n has rk = 0.

def allclass(n):
    RK0 = []  # Stores data for rank 0 cases
    RK1 = []  # Stores data for rank 1 cases

    # Populate RK0 and RK1
    for m in range(1, n+1):  # Loop through all numbers from 1 to n
        if twins(m) == True:  # Check if m satisfies the `twins` condition
            if rank(m) == [m, 0]:  # If `rank(m)` returns `[m, 0]`
                RK0.append([m, 0, 6*m-1, 6*m+1])  # Add to RK0 list
            else:
                RK1.append([m, 1, 6*m-1, 6*m+1])  # Otherwise, add to RK1 list

    # Determine the maximum number of rows
    max_rows = max(len(RK0), len(RK1))

    # Print entries in two columns
    print(f"{'RK0':<30} | {'RK1':<30}")  # Header
    print("-" * 63)  # Divider

    for i in range(max_rows):
        # Get entries from RK0 and RK1 if they exist
        col1 = (
            f"N: {RK0[i][0]} rk: {RK0[i][1]} p: {RK0[i][2]} q: {RK0[i][3]}"
            if i < len(RK0)
            else ""  )
        col2 = (
            f"N: {RK1[i][0]} rk: {RK1[i][1]} p: {RK1[i][2]} q: {RK1[i][3]}"
            if i < len(RK1)
            else "")
        print(f"{col1:<30} | {col2:<30}")
# This function prints two lists: the first one with elliptic curves
# of rank 0, the second one with supposed rank 1.

def tallclass(n):
    RK0 = []
    RK1 = []
    for m in range(1, n + 1):
        if twins(m):
            if rank(m) == [m, 0]:
                RK0.append([m, 0])
            else:
                RK1.append([m, 1])
    if len(RK0) == 0:  # Avoid division by zero
        return 0
    return len(RK1) / len(RK0)
   # ratio between the number of elliptic curves of rank 1 and rank 0 in
   # a given range of numbers.

def plot(n):
    x = np.arange(1, n, 100)
    y = [tallclass(l) for l in x]
    plt.plot(x,y)

# Plot the graph of tallclass.
```

The figures on pages 45–46 show the results of the plot function with inputs $n = 8000, 80000, 800000$. It is really interesting to observe that, at least in the considered range of numbers, the graph of the function seems to tend toward 1. In other words, there seems to be approximately the same number of elliptic curves with rank 1 and rank 0. Moreover we can also say something about the distribution of twin primes. In Proposition 3.4.1, we have seen how the rank of an elliptic curve $E_{p,q}$ with $(p, q) = (6n - 1, 6n + 1)$, $n \in \mathbb{N}$ pair of twin prime depends on $n \bmod 4$. Specifically, there appears to be approximately the same number of twin prime pairs $(6n - 1, 6n + 1)$ with $n \equiv 1, 2 \mod 4$ and $n \equiv 0, 3 \mod 4$.
We want to emphasize that the preceding observations are primarily based on the parity conjecture and, secondly, on calculations; therefore, they do not claim to have universal validity.

At the end of this section we compute the generator of the free part of Mordell-Weil group for the cases $n = 3, 7, 12$. It easy to check using the previous algorithm that they generate pair of twin primes and by proposition 3.4.1 that the conjectured rank of the associated elliptic curve is 1.

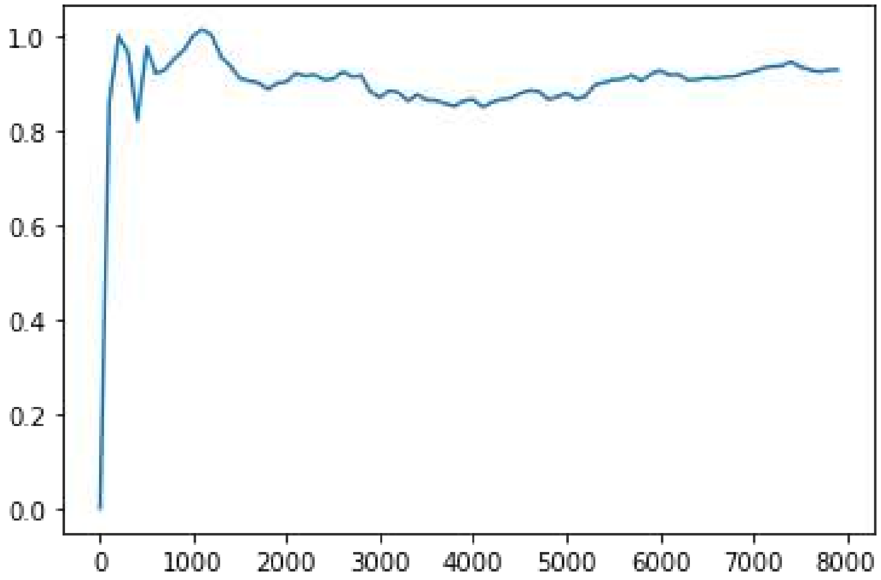

Figure 3.1: Plot(8000)

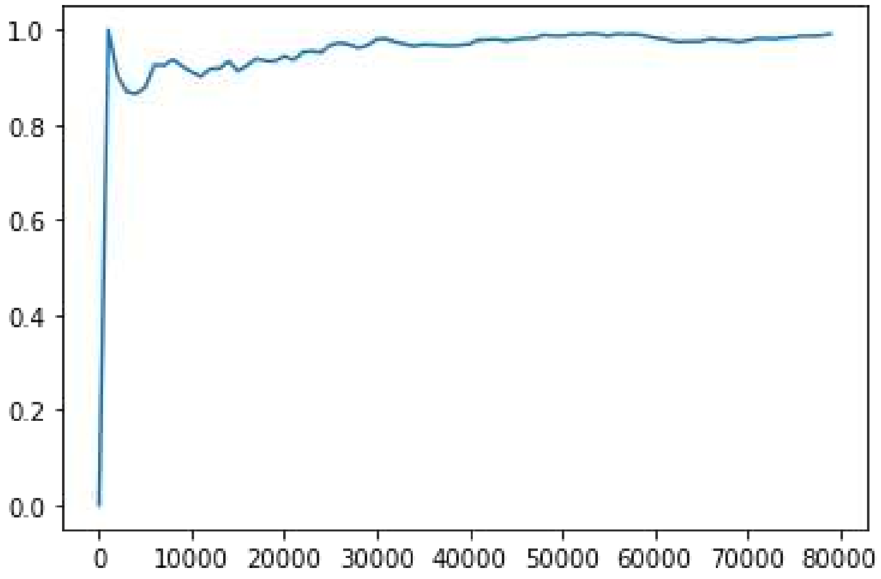

Figure 3.2: Plot(80000)

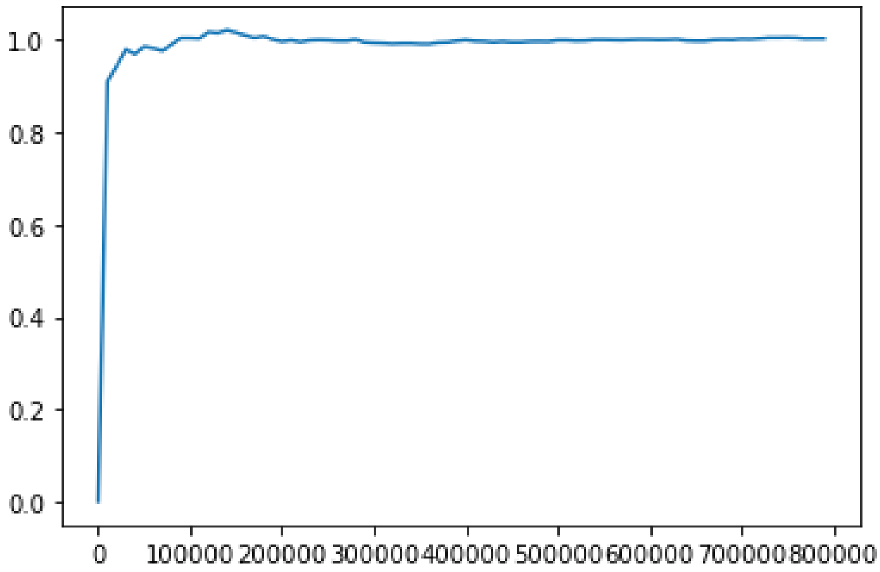

Figure 3.3: Plot(800000)

Let $n = 3$ by the 2-descent method we have to find a solution to

$$\begin{cases} {z_1}^2 + 2z_2^2 = 17 \\ {z_1}^2 + 2z_3^2 = 19 \end{cases} \tag{3.5}$$

Manipulating a little bit the system and with the help of PARI we find the following solution $(z_1, z_2, z_3) = (\frac{11}{3}, \frac{4}{3}, \frac{5}{3})$ hence

$$P = \left(\frac{121}{9}, \frac{440}{27}\right).$$

Let $n = 7$ then $(z_1, z_2, z_3) = (\frac{11}{9}, \frac{40}{9}, \frac{41}{9})$ and

$$P = \left(\frac{121}{81}, \frac{36080}{729}\right).$$

Lastly for $n = 12$, PARI gives as result

$$P = \left(\frac{3853369}{47089}, \frac{904079280}{10218313}\right).$$

Observe that the computational complexity rapidly increases hence it is really difficult to calculate P even for $n = 23$. However, we have demonstrated for these three cases that the prediction of rank equal to 1 has indeed been confirmed.

Appendix A

Twin prime

Twin primes are primes of the form $(p, p + 2)$ where p is prime number. There are many proofs for the infinitude of prime numbers, but it is very difficult to prove whether there are an infinite number of pairs of twin primes. Most mathematicians agree that the evidence points toward this conclusion, but numerous attempts at a proof have been falsified by subsequent review.

Theorem A.0.1. *Every prime number except for 2 and 3 is of the form* $6n - 1$ *or* $6n + 1$ *for some* $n \in \mathbb{N}$ *.*

Proof. Let $m \in \mathbb{N}$, $m > 3$. By euclidean division

$$m = 6q + r$$

with $r \in \{0, 1, 2, 3, 4, 5\}$.

(a) if $r = 0, 2, 4$ then m is not prime because is divisible by 2.

(b) if $r = 3$ then m is divisible by 3 and is not prime.

Therefore $m = 6q + 1$ or $m = 6q + 5 = 6(q + 1) - 1$. □

Corollary A.0.2. *Every pair of twin primes except* $(3, 5)$ *is of the form* $(6n - 1, 6n + 1)$ *for some* $n \in \mathbb{N}$.

Conjecture 2. *There are infinitely many pairs of twin primes.*

Appendix B

Legendre symbol

Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise.

Definition B.0.1. The *Legendre Symbol* is a function of a and p defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \; if \;\; a \; is \; quadratic \; residue \mod p \; and \not\equiv 0 \pmod{p} \\ -1 \; if \;\; a \; is \; quadratic \; nonresidue \pmod{p} \\ 0 \; if \;\; a \equiv 0 \; (mod \; p) \end{cases} \tag{B.1}$$

B.1 Properties of the Legendre symbol

In this section we list some useful properties of Legendre symbol

1. The Legendre symbol is a completely multiplicative function of its top argument:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \qquad (a, b) \in \mathbb{Z}.$$

2. Quadratic Reciprocity Law: For two distinct odd prime numbers l and p, the following identity holds:

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{(\frac{l-1}{2})(\frac{p-1}{2})}.$$

3. As supplement to the Quadratic Reciprocity Law :

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \; if \;\; p \equiv 1 \pmod{4} \\ -1 \; if \;\; p \equiv 3 \pmod{4} \end{cases} \tag{B.2}$$

4.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \; if \;\; p \equiv 1 \; or \; 7 \pmod{8} \\ -1 \; if \;\; p \equiv 3 \; or \; 5 \pmod{8} \end{cases} \tag{B.3}$$

Remark B.1.1. *From point 3 and 4 we deduce that*

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1 \; or \; 3 \pmod{8}.$$

Bibliography

[1] J.H. Silverman. *“The Arithmetic of Elliptic Curves”*, Springer, New York, 2 edition, 2016.

[2] J.H. Silverman. *“Advanced Topics in the Arithmetic of Elliptic Curves ”*, Springer; I edition 1994.

[3] M. Schütt, T. Shioda . *“Elliptic surfaces ”*. Algebraic Geometry in East Asia - Seoul 2008 pp. 51-160.

[4] M. Schütt, T. Shioda . *“Mordell-Weil Lattices ”*. Springer, 2019.

[5] J. Caro, H. Pasten. *”On the fibres of an elliptic surface where the rank does not jump”*. Bulletin of the Australian Mathematical Society, 25 October 2022.

[6] K. Oguiso, T. Shioda. *”The Mordell-Weil lattice of a rational elliptic surface”*. Comment. Math. Univ. St. Paul. 40 (1991), no. 1, 83-99.

[7] L.C. Kellock,V. Dokchitser. *”Root numbers and parity phenomena”*. Bulletin of the London Mathematical Society,2023.

[8] J.S. Milne. *”Elliptic curves”*. BookSurge Publishers, 2006.

[9] S. Lang, A. Neron . *”Rational points of abelian varieties over function fields”*. Amer. J. Math. 81 (1959), 95-118.

[10] J. Silverman . *”Heights and the specialization map for families of abelian varieties.”* J. Reine Angew. Math. 342 (1983), 197-211.

[11] PARI/GP, 2005. http://pari.math.u-bordeaux.fr/.

[12] C. Salgado. *”On the rank of the fibers of rational elliptic surfaces”*. Algebra Number Theory 6 (2012), no. 7, 1289-1314.

[13] B. Conrad, K. Conrad, H. Helfgott. *”Root numbers and ranks in positive characteristic”*. Adv. Math. 198 (2005), no. 2, 684-731.

[14] J. Cassels, A. Schinzel. *”Selmers conjecture and families of elliptic curves”*. Bull. London Math. Soc. 14 (1982), no.4, 345-348.

[15] J.H. Silverman . *”Divisibility of the Specialization Map for Families of Elliptic Curves”*. American Journal of Mathematics Vol. 107, No. 3 (Jun., 1985), pp. 555-565. Published By: The Johns Hopkins University Press.