The Rank of Elliptic Curves over Function Fields of Finite Fields

Hannah Bull

May 2014

A thesis submitted in partial fulfilment of the requirements of the degree of Bachelor of Philosophy/Bachelor of Science (Honours) in Mathematics of the Australian National University and the National University of Singapore

Australian National University

NUS National University of Singapore

Declaration

The mathematics in this paper is well known and is certainly not of my own creation. I also owe much credit to my supervisor, Dr. James Borger, who patiently explained to me many of the ideas and proofs. What little remains, I claim as my own synthesis.

Hannah Bull

Acknowledgements

I have been fortunate to have had many fantastic mathematics teachers. First and foremost, I would like to thank my supervisor, Jim, for suggesting a fascinating topic and for providing me with invaluable help and advice. I would also like to thank David, for teaching me much about mathematics, and by extension, about life.

Over the past year, I have enjoyed sharing the struggle of learning mathematics with the honours students in the MSI basement. I feel privileged to belong to this close community. In particular, I would like to thank Hannah, my dual space, for helping me appreciate challenges and for providing me with much needed distractions.

My university experience would have been vastly different, had I not had the opportunity to spend three semesters in Singapore, so I would like to thank the incredible USP community at NUS for making me feel welcome and for exposing me to many new perspectives.

I would also like to thank my family, as well as Jannik and Claudia, who have supported me in various ways throughout my university studies.

Abstract

The existence of elliptic curves over the rational numbers of arbitrarily large rank is an open problem; however, it is known that elliptic curves over function fields of finite fields can have arbitrarily large rank. By associating elliptic curves over function fields of finite fields with elliptic surfaces over finite fields, and then associating elliptic surfaces with Fermat surfaces, it is possible to reduce the problem of determining the rank of an elliptic curve over a function field of a finite field to evaluating the zeta function of a Fermat surface. We explain how to do this for a particular family of elliptic curves, whose members may have arbitrarily large rank.

Contents

Chapter 0

Preliminaries

It is unknown whether elliptic curves over the rational numbers can have arbitrarily large Mordell-Weil rank, but it is possible to construct elliptic curves over function fields of finite fields with arbitrarily large rank. We would like to explore the theory of elliptic curves over $\mathbb{F}_q(t)$, where q is a prime power, $\mathbb{F}_q$ is the finite field with q elements and t is a transcendental element.

In some ways, the field $\mathbb{F}_q(t)$ is analogous to the field $\mathbb{Q}$. The fraction field of $\mathbb{Z}$ is $\mathbb{Q}$ and the fraction field of $\mathbb{F}_q[t]$ is $\mathbb{F}_q(t)$. Both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ contain infinitely many elements, are principal ideal domains and the quotient of each of these rings by a non-zero prime ideal is a finite field. As a result, elliptic curves over $\mathbb{F}_q(t)$ share some common properties with elliptic curves over $\mathbb{Q}$. Therefore, the existence of elliptic curves with arbitrarily large rank over $\mathbb{F}_q(t)$ suggests the existence of elliptic curves of arbitrarily large rank over $\mathbb{Q}$.

The j-invariant can be used to determine isomorphism classes of elliptic curves over an algebraically closed field. Over $\mathbb{F}_q(t)$, elliptic curves with the same j-invariant are not necessarily isomorphic, but those with different j-invariants certainly are not. In [ST67], Shafarevich and Tate construct examples of elliptic curves over $\mathbb{F}_p(t)$, where p is prime, of arbitrarily large rank and whose j-invariant lies in $\mathbb{F}_p$. For an elliptic curve E over $\mathbb{F}_p(t)$ with j-invariant in $\mathbb{F}_p$, there exists a finite extension $L/\mathbb{F}_p$ such that over L, there exists an isomorphism between $E/\mathbb{F}_p(t)$ and an elliptic curve defined over $\mathbb{F}_p$. This property is called *isotriviality*.

Over $\mathbb{Q}$, there is no analogous property to isotriviality, so finding an elliptic curve with arbitrarily large rank over $\mathbb{F}_q(t)$ with j-invariant not in $\mathbb{F}_q$ is stronger evidence towards the existence of elliptic curves over $\mathbb{Q}$ of arbitrarily large rank than the examples of Shafarevich and Tate. In [Ulm02], Ulmer constructs examples of non-isotrivial elliptic curves of arbitrarily large rank. By associating

elliptic curves over $\mathbb{F}_q(t)$ with elliptic surfaces over $\mathbb{F}_q$, and then associating elliptic surfaces with Fermat surfaces over $\mathbb{F}_q$, Ulmer reduces the problem of determining the rank of an elliptic curve over a function field of a finite field to evaluating the zeta-function of a Fermat surface over a finite field. This project seeks to explain Ulmer's construction.

Chapter 0 covers definitions and basic theorems in preparation for later chapters. We introduce elliptic curves, surfaces, divisors, Galois cohomology and Gauss and Jacobi sums. In chapter 1, we prove that the Mordell-Weil rank is finite for elliptic curves over $\mathbb{F}_q(t)$. Although we can associate elliptic curves over $\mathbb{F}_q(t)$ to elliptic surfaces over $\mathbb{F}_q$, we cannot define the Mordell-Weil rank of an elliptic surface. Instead, we define the Néron-Severi group of a surface, and find a relationship between the Néron-Severi group of an elliptic surface and the Mordell-Weil group of the corresponding elliptic curve. This relationship is due to Shioda, and can be found in [Shi72].

From chapter 2 onwards, we specialise to a particular sequence of elliptic curves. Chapter 2 is dedicated to understanding the geometrical properties of these elliptic curves and the corresponding elliptic surfaces. We then construct birational maps relating our elliptic surfaces to Fermat surfaces. Chapter 3 deals with zeta-functions, the Weil conjectures, the Tate conjecture and the Birch and Swinnerton-Dyer conjecture, which we use to connect the problem of finding the rank of an elliptic curve to the problem of finding the zeta-function of a Fermat surface. In chapter 4, we explicitly calculate the zeta-function of a quotient group of a Fermat surface, which provides an expression for the rank of our elliptic curve. Finally, we explicitly construct elliptic curves over functions fields of finite fields of arbitrarily large rank.

The theory of elliptic curves is developed in [Sil86] and that of elliptic surfaces in [Sil94]. These are the principal references for chapters 0 and 1. We do not include a complete theory of elliptic curves and surfaces in chapter 0, but cite some of the main results used later in the paper. In chapters 2, 3 and 4, the principal reference is Ulmer's paper [Ulm02]. Basic knowledge of algebraic geometry is assumed, for example the content of [FW89], and we cite a number of theorems from commutative algebra and algebraic geometry without proof from [Har77].

0.1 Notation

For easy reference, here is a list of frequently used notation. Other symbols are defined along the way.

$\Bbbk = \mathbb{F}_q = \mathbb{F}_{p^f}$, where $q = p^f$ is a power of a prime $p \neq 2, 3$ and $\mathbb{F}_q$ is the finite field with q elements. Many of the propositions in this paper also hold for fields of characteristic 2 and 3, but for simplicity we do not consider these special cases.

$\mathbb{K} = \Bbbk(t) = \mathbb{F}_q(t) = \mathbb{F}_{p^f}(t)$

K is an arbitrary field, not necessarily algebraically closed nor of characteristic 0.

$\overline{K}$ denotes the algebraic closure of K.

K^* denotes the set of invertible elements of K.

E/K is an elliptic curve over K. We usually consider elliptic curves $E/\mathbb{K}$.

$E(K)$ denotes the set of points on an elliptic curve E/K with coordinates in K.

$[m]$ is the multiplication by m map on an elliptic curve (using the group law).

$E[m]$ denotes the set of points on an elliptic curve E/K in $E(\overline{K})$ of order dividing m.

$\mathcal{E}/K$ is an elliptic surface over K. We usually consider $\mathcal{E}/\Bbbk$ and we often abbreviate this to $\mathcal{E}$.

$\mathcal{F}/K$ is a Fermat surface over K. We usually consider $\mathcal{F}/\Bbbk$ and we abbreviate this to $\mathcal{F}$. Where the degree d of the Fermat surface is important, we write $\mathcal{F}_d$.

$\mathcal{W}$ is a Weierstrass model of an elliptic surface.

$\mathcal{S}$ denotes an arbitrary surface.

C denotes an arbitrary curve.

$G_{L/K}$ is the Galois group of a Galois extension $K \subset L$.

μ_n denotes the group of n^{th} roots of unity in a field K.

$\#(X)$ denotes the number of points in X, where X is some variety or algebraic set.

Square brackets are used for projective coordinates, for example $[X, Y, Z]$, round brackets are used for affine coordinates, for example (x, y, z).

Fr denotes the Frobenius endomorphism of a variety X over $\mathbb{F}_q$ given by sending $[X_0, ..., X_n] \in X$ to $[X_0^q, ..., X_n^q] \in X$.

0.2 Elliptic Curves

Definition 0.1. A *curve* over a field K is a projective variety of dimension 1 whose defining polynomials have coefficients in K.

Definition 0.2. An *elliptic curve* E over a field K is a non-singular curve of genus 1 over K with a K-rational point $\mathcal{O}$.

All elliptic curves over K, where K is a field not of characteristic 2, can be written in the form

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

where $a_1, a_2, a_3, a_4, a_6 \in K$. This is known as *Weierstrass form* [Sil86, III §3]. Let

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

The discriminant Δ and the j-invariant j of $E/\mathbb{K}$ are given by

$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + -b_2b_4b_6 \\ j &= \frac{(b_2^2 - 24b_4)^3}{\Delta} \end{aligned}$$

In this paper, we assume that $\mathbb{K}$ is not of characteristic 2 or 3, so we can write $E/\mathbb{K}$ in the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a, b \in \mathbb{K}$.

Proposition 0.3. [Sil86, III §1] *The discriminant Δ is not the zero polynomial.*

Definition 0.4. A $\mathbb{K}$-*valued point* on $E/\mathbb{K}$ is a point with coordinate values in the field $\mathbb{K}$. The set of $\mathbb{K}$ valued points is denoted $E(\mathbb{K})$, and in chapter 1 we show that this is a finitely generated Abelian group.

0.3 Elliptic Surfaces

Definition 0.5. A *surface* over a field K is a projective variety of dimension 2 whose defining polynomials have coefficients in K.

We wish to define elliptic surfaces in an analogous way to elliptic curves. Given an elliptic curve $E/\mathbb{K}$, we want to be able to associate $E/\mathbb{K}$ to an elliptic surface $\mathcal{E}/\Bbbk$. The Weierstrass equation for $E/\mathbb{K}$ lies in $\mathbb{K}[X,Y,Z]$, but by eliminating denominators, we can also consider this Weierstrass equation as a polynomial in $\Bbbk[X,Y,Z,t]$. We can write $E/\mathbb{K}$ in Weierstrass form as

$$E_t : Y^2Z + A_1(t)XYZ + A_3(t)YZ^2 = X^3 + A_2(t)X^2Z + A_4(t)XZ^2 + A_6(t)Z^3$$

where $A_i(t)$ is considered as a rational function in $\Bbbk(t)$ for $i = 1,2,3,4,6$. Suppose v is an element of $\overline{\Bbbk} \cup \{\infty\}$. Then we can consider E_v as a non-singular elliptic curve over $\overline{\Bbbk}$ for almost all values of $v \in \overline{\Bbbk} \cup \{\infty\}$, specifically, for all values of v such that the discriminant $\Delta \neq 0$ and such that $A_i(v)$ does not have a pole at v for $i = 1,2,3,4,6$. As Δ is a non-zero polynomial in $\Bbbk[t]$ (after eliminating denominators), there are finitely many roots of the polynomial $\Delta = 0$.

Definition 0.6. Suppose $E/\mathbb{K}$ is an elliptic curve given by the Weierstrass equation

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

Then write $A_i(t) = a_i$ for $i = 1,2,3,4,6$, where $A_i(t)$ is considered as a rational function in $\Bbbk(t)$. We define the corresponding *Weierstrass model* $\mathcal{W}/\Bbbk$ to be the Zariski closure of the set

$$\{([X,Y,Z],t) \in \mathbb{P}^2 \times \mathbb{P}^1 \mid A_i \text{ does not have a pole at } t \text{ for all } i \text{ and}$$
$$Y^2Z + A_1(t)XYZ + A_3(t)YZ^2 = X^3 + A_2(t)X^2Z + A_4(t)XZ^2 + A_6(t)Z^3\}$$

where $t \in \mathbb{P}^1$ can be considered as an element of $\overline{\Bbbk} \cup \{\infty\}$.

Note that the Weierstrass model is equipped with a non-constant map $\pi : \mathcal{W} \to \mathbb{P}^1$ given by projection onto the last coordinate. The Weierstrass model $\mathcal{W}/\Bbbk$ is a *fibred surface*, where the fibres are given by $E_t = \pi^{-1}(t)$. Each fibre of $\mathcal{W}$ has one irreducible component, either a nodal, cuspidal or non-singular cubic curve.

Definition 0.7. [Sil94, III §7] A surface $\mathcal{S}$ is *relatively minimal* if

1. $\mathcal{S}$ is a non-singular projective surface
2. If there exists a birational morphism ϕ from $\mathcal{S}$ to a non-singular projective surface $\mathcal{S}'$, then ϕ is an isomorphism.

Theorem 0.8. [Har77, V] *Every non-singular surface is birationally equivalent to a relatively minimal surface.*

By blowing up singular points on $\mathcal{W}$, we can find a non-singular surface birationally equivalent to $\mathcal{W}$. Thus we can find a relatively minimal surface $\mathcal{E}$ which is birationally equivalent to $\mathcal{W}$.

Definition 0.9. Let $E/\mathbb{K}$ and $\mathcal{W}/\Bbbk$ be as before. The *elliptic surface* $\mathcal{E}/\Bbbk$ associated to $E/\mathbb{K}$ is the unique non-singular and relatively minimal surface birationally equivalent to $\mathcal{W}$ and equipped with a non-constant map $\pi' : \mathcal{E} \to \mathbb{P}^1$.

The map $\pi' : \mathcal{E} \to \mathbb{P}^1$ is induced by the birational map $\mathcal{E} \to \mathcal{W}$.

$$\begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{W} \\ {\scriptstyle \pi'}\downarrow & \swarrow {\scriptstyle \pi} & \\ \mathbb{P}^1 & & \end{array}$$

The elliptic surface $\mathcal{E}/\Bbbk$ equipped with the map $\pi' : \mathcal{E} \to \mathbb{P}^1$ is also a fibred surface, where the fibres are given by $E_t = \pi'^{-1}(t)$. There are only finitely many singular fibres of $\mathcal{W}$ and so the blow up of $\mathcal{W}$ also has only finitely many singular fibres. The fibres of $\mathcal{E}$ may have multiple components, as the blow up of $\mathcal{W}$ is obtained by deleting points and adding curves to $\mathcal{W}$.

Theorem 0.10. [Sil94, III §3] $\Bbbk(\mathcal{E}) \cong \Bbbk(\mathbb{P}^1)(E)$ *as* $\Bbbk(\mathbb{P}^1)$*-algebras.*

Definition 0.11. The *generic fibre* of $\mathcal{E}/\Bbbk$ is $E/\mathbb{K}$.

0.4 Divisors

Definition 0.12. A *divisor* on a variety defined over K is a formal sum of subvarieties defined over K of codimension 1 with coefficients in $\mathbb{Z}$.

For example, a divisor D on a curve C/K is a formal sum

$$\sum_i n_i(P_i)$$

where the P_i are points in $C(\overline{K})$ and the n_i are in $\mathbb{Z}$. (It is always possible to write a divisor D on a curve C/K in this form, but it is necessary to take points P_i in $C(\overline{K})$, not in $C(K)$.) Similarly, a divisor $\mathcal{D}$ on a surface $\mathcal{S}/K$ is a formal sum of curves on $\mathcal{S}/K$ defined over K. The set of divisors on a variety X is denoted $\mathrm{Div}(X)$; and $\mathrm{Div}(X)$ has a natural group structure by taking formal sums. If the coefficients in the formal sum of subvarieties of codimension 1 are all

non-negative, then we say the divisor is an *effective divisor*. We can thus impose a partial order on the group of divisors by writing $D \geq 0$ if and only if D is an effective divisor.

Definition 0.13. The *degree* of a divisor is the sum of the coefficients in $\mathbb{Z}$. For example, if $D = \sum_i n_i(P_i)$, then $\deg(D) = \sum_i n_i$.

Definition 0.14. A *principal divisor* of a variety X/K is a divisor of the form (f), where $f \in K(X)^*$. If D_1 and D_2 are two divisors on X/K, we say that D_1 and D_2 are *linearly equivalent* if $D_1 - D_2$ is a principal divisor.

For example, if C is a curve and $f \in K(C)^*$, then

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

Note that the set of principal divisors of a variety X/K form a subgroup of $\mathrm{Div}(X)$.

Proposition 0.15. [Har77, II 6.10] *All principal divisors on a projective curve C/K have degree 0.*

Proposition 0.16. [Sil86, II §3] *On $\mathbb{P}^1$, D is a principal divisor if and only if the degree of D is 0.*

Definition 0.17. The *Picard group* is the quotient group of divisors modulo linear equivalence. If X is a variety, we denote this group by $\mathrm{Pic}(X)$.

If X is a curve, we use $\mathrm{Pic}^0(X)$ to denote the subgroup of the Picard group containing only divisors of degree 0. (Though not immediately obvious, this definition is consistent with the usual definition of $\mathrm{Pic}^0(X)$ of a variety X: the subgroup of divisors in $\mathrm{Pic}(X)$ algebraically equivalent to 0.)

Theorem 0.18. *Let C be an irreducible curve on a surface $\mathcal{S}$ and let $\phi : C \dashrightarrow \mathbb{P}^1$ be a rational map. Then ϕ is constant or surjective.*

Proof. Let U be an open subset of C. As ϕ is a rational map, we can write $\phi(x) = [\phi_0(x), ..., \phi_n(x)]$ for $x \in U$, where ϕ_i is a rational map for all i. If we clear denominators, then ϕ is defined everywhere on U except for at points x such that $\phi_0(x) = ... = \phi_n(x) = 0$. If we remove all the common components of $\phi_0(x), ..., \phi_n(x)$, then $V(\phi_0(x), ..., \phi_n(x))$ is a closed subvariety of codimension strictly greater than 1. However, U is an open subset of a curve C, which has

dimension 1, so there are no points in $V(\phi_0(x), ..., \phi_n(x))$ and ϕ must be defined everywhere on U. This holds for all $U \subset C$. A rational map defined everywhere on C is a morphism, so ϕ is a morphism.

As ϕ is continuous, the image of ϕ must be closed in the Zariski topology. C is irreducible so $\phi(C)$ is irreducible. Thus $\phi(C)$ must be a single point on $\mathbb{P}^1$ or the whole of $\mathbb{P}^1$. □

Definition 0.19. Let $\mathcal{D}$ be a divisor on a fibred surface $\mathcal{S}$ with a morphism $\pi : \mathcal{S} \to \mathbb{P}^1$. When $\pi : \mathcal{D} \to \mathbb{P}^1$ is constant, call $\mathcal{D}$ *fibral*. When $\pi : \mathcal{D} \to \mathbb{P}^1$ is surjective, call $\mathcal{D}$ *horizontal*.

If $\pi(\mathcal{D}) = \{t\}$, then π is constant and $\mathcal{D}$ lies in the fibre $S_t = \pi^{-1}(t)$.

Definition 0.20. If $\mathcal{D}$ is a horizontal divisor on a surface $\mathcal{S}$, we say $\mathcal{D}$ *meets the generic fibre* of $\mathcal{S}$. If $\mathcal{D}$ is a fibral divisor on $\mathcal{S}$, we say $\mathcal{D}$ does not meet the generic fibre.

(This interpretation of 'meets the generic fibre' is consistent with the usual scheme-theoretic understanding.)

Theorem 0.21. [Har77, V 1.1] *Let $\mathcal{S}/K$ be a surface. There is a unique symmetric bilinear pairing* $\mathrm{Div}(\mathcal{S}) \times \mathrm{Div}(\mathcal{S}) \to \mathbb{Z}$ *given by* $(D_1, D_2) \mapsto D_1 \cdot D_2$ *which has the following three properties*

1. If C_1 and C_2 are two irreducible curves on a surface S that meet everywhere transversally, then $(C_1) \cdot (C_2) = \#(C_1 \cap C_2)$.

2. (numerical equivalence) If $D_1, D_2 \in \mathrm{Div}(\mathcal{S})$ are divisors such that D_1 is linearly equivalent to D_2, then for all $D \in \mathrm{Div}(\mathcal{S})$, $D \cdot D_1 = D \cdot D_2$.

3. For divisors $D_1, D_2, D_3 \in \mathrm{Div}(\mathcal{S})$,

$$(D_1 + D_2) \cdot D_3 = D_1 \cdot D_3 + D_2 \cdot D_3.$$

Definition 0.22. We call $D_1 \cdot D_2$ the *intersection number* of D_1 and D_2.

0.4.1 The Riemann-Roch Theorem

Definition 0.23. [Sil86, II §5] Let C be a curve and let Ω_C be the space of differential forms on C. Let $\omega \in \Omega_C$ and define

$$(\omega) = \sum_{P \in C(\overline{K})} \mathrm{ord}_P(\omega)(P).$$

As $(\omega) \in \mathrm{Div}(C)$, we can also consider (ω) as an equivalence class of divisors in $\mathrm{Pic}(C)$.

Definition 0.24. A *canonical divisor* is a divisor of the form $(\omega) \in \mathrm{Pic}(C)$, where $\omega \in \Omega_C$ is a non-zero differential form.

Theorem 0.25 (Riemann-Roch)**.** [FW89, Ch.7] *Let*

$$\mathcal{L}(D) = \{f \in K(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Let $l(D) = \dim_K \mathcal{L}(D)$*. Let* K_C *be a canonical divisor on* C*. Then there is an integer* g*, called the* genus *of* C*, such that for every divisor* $D \in \mathrm{Div}(C)$*,*

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

Corollary 0.26. *If* $C = E$ *is an elliptic curve, then*

1. $l(K_E) = 1$
2. $\deg(K_E) = 0$
3. *If* $\deg(D) > 0$*, then* $l(D) = \deg(D)$*.*

Proof. (1) comes from substituting $D = 0$ and $g = 1$ into the Riemann-Roch theorem and (2) comes from substituting $D = K_E$ and $g = 1$ into the Riemann-Roch theorem and using the fact that $l(K_E) = 1$.

(3) We want to show $l(K_E - D) = 0$. We know $\deg(K_E - D) < 0$. Suppose $f \in \mathcal{L}(K_E - D)$. Then $0 = \deg(\mathrm{div}(f)) \geq -\deg(K_E - D)$. However, $-\deg(K_E - D) > 0$, so $f = 0$. Thus $l(K_E - D) = 0$. □

0.4.2 The Group Law on Elliptic Curves

Definition 0.27. The *rank* of an Abelian group A is the minimum number of generators of the largest torsion-free subgroup of A.

We wish to consider K-rational points on an elliptic curve E/K as a group, so that we can study the properties of this group. It turns out that the K-valued points on E form a finitely generated Abelian group, hence $E(K)$ is isomorphic to a product of copies of $\mathbb{Z}$ and torsion quotient groups of $\mathbb{Z}$. The rank of this group is then the number of torsion-free copies of $\mathbb{Z}$ and can be thought of as the number of independent points in $E(K)$ which have infinite order. We use the group structure of $\mathrm{Pic}^0(E)$ to define a group law on E.

Lemma 0.28 (Abel's theorem on an elliptic curve)**.** *The map* $\phi : E(K) \to \mathrm{Pic}^0(E)$ *given by* $P \mapsto (P) - (\mathcal{O})$ *is a bijection.*

Proof. (Injectivity) Suppose $(P)-(\mathcal{O}) \sim (Q)-(\mathcal{O})$, where $\sim$ denotes linear equivalence. Then $(P) \sim (Q)$. By definition of linear equivalence, we can find an $f \in K(E)$ such that $(f) = (P) - (Q)$. As $(f) \geq -(Q)$, $f \in \mathcal{L}((Q))$. By the Riemann-Roch theorem, $l((Q)) = \deg((Q)) = 1$. This implies $f \in K$. By proposition 0.15, all principal divisors on E have degree 0, so $P = Q$.

(Surjectivity) Suppose $D \in \mathrm{Pic}^0(E)$. By the Riemann-Roch theorem,

$$l(D + (\mathcal{O})) = \deg(D + (\mathcal{O})) = 1.$$

Let $g \in \mathcal{L}(D + (\mathcal{O}))$ be a generator of $\mathcal{L}(D + (\mathcal{O}))$. We know $\mathrm{div}(g)$ is a divisor of degree 0, so $\mathrm{div}(g) + D + (\mathcal{O}) \geq 0$. As $\deg(\mathrm{div}(g) + D + (\mathcal{O})) = 1$, there exists a point $Q \in E(K)$ such that $\mathrm{div}(g) + D + (\mathcal{O}) \sim (Q)$. Thus $\mathrm{div}(g) = -D - (\mathcal{O}) + (Q)$ and $D \sim (Q) - (\mathcal{O})$. □

For every $D \in \mathrm{Pic}^0(E)$, we can find a unique $Q \in E(K)$ such that $D = (Q) - (\mathcal{O})$. Define $P_1 + P_2$ to be the unique element $R \in E(K)$ such that $(R) = (P_1) + (P_2) - (\mathcal{O})$. Thus the group structure of $\mathrm{Pic}^0(E)$ defines a group law on $E(K)$. Also note that the group of points on E under this group law is Abelian.

Proposition 0.29. [Sil86, III §3] *Let $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then D is a prinicipal divisor if and only if $\sum n_P = 0$ and $\sum [n_P]P = \mathcal{O}$, where the second summation is the group law on elliptic curves.*

0.5 The Tate Module

We later use the Tate module to evaluate the zeta-function of an elliptic curve over $\mathbb{F}_q$ and we use the Weil paring to prove the weak Mordell-Weil theorem. The theory behind these ideas is covered in detail in [Sil86], but only the main propositions and results needed in this paper are included here.

Definition 0.30. Let I be a partially ordered set, let $(A_i)_{i \in I}$ be a family of groups and let $f_{ij} : A_j \to A_i$ for $i \leq j$ be a family of homomorphisms with the following properties

1. $f_{ii} : A_i \to A_i$ is the identity on A_i for all $i \in I$
2. $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$.

Then the *inverse limit* is defined to be

$$\varprojlim_{i \in I} A_i = \left\{ \vec{a} \in \prod_i A_i \mid a_i = f_{ij}(a_j) \text{ for all } i \leq j \text{ such that } i, j \in I \right\}$$

Definition 0.31. The *l-adic integers*, $\mathbb{Z}_l$, are constructed by taking the inverse limit of $A_i = \mathbb{Z}/l^i\mathbb{Z}$, where $i \in \mathbb{N}$ has the natural order, and with respect to the natural maps $f_{ij} : \mathbb{Z}/l^j\mathbb{Z} \to \mathbb{Z}/l^i\mathbb{Z}$. Thus

$$\mathbb{Z}_l = \varprojlim_{i \in \mathbb{N}} \mathbb{Z}/l^i\mathbb{Z}$$

Therefore, an l-adic integer can be considered as a sequence $(a_i)_{i\geq 1}$ such that $a_i \in \mathbb{Z}/l^i\mathbb{Z}$ and if $i \leq j$, then $a_i \equiv a_j \mod l^i$.

Definition 0.32. The field of *l-adic numbers* $\mathbb{Q}_l$ is the fraction field of the l-adic integers $\mathbb{Z}_l$.

Definition 0.33. [Sil86, III §7] Let E/K be an elliptic curve and let l be a prime. The *l-adic Tate module of* E, denoted $T_l(E)$ is constructed by taking the inverse limit of $A_i = E[l^i]$, where $i \in \mathbb{N}$ has the natural order and with respect to the natural 'multiplication by l' maps $[l] : E[l^{i+1}] \to E[l^i]$. We define

$$T_l(E) = \varprojlim_{i \in \mathbb{N}} E[l^n].$$

Note that the Tate module has a natural structure as a $\mathbb{Z}_l$-module.

Proposition 0.34. [Sil86, III §7] *If* $l \neq \mathrm{char}(K)$, *then* $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$.

Definition 0.35. [Sil86, III §8] Let E/K be an elliptic curve. Let $f \in \overline{K}(E)$ be a function such that

$$\mathrm{div}(f) = m(T) - m(\mathcal{O})$$

where $T \in E[m]$. Let g be a function such that $g^m = f \circ [m]$. The *Weil pairing* is a map $e_m : E[m] \times E[m] \to \mu_m$ given by

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

where $X \in E(\overline{K})$ is any point such that $g(X+S)$ and $g(X)$ are both defined and non-zero.

Proposition 0.36. [Sil86, III §8] *The Weil pairing has the following properties:*

1. *(Bilinear)* $e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T)$ *and* $e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$.
2. *(Alternating)* $e_m(S,T) = e_m(T,S)^{-1}$.
3. *(Non-degenerate) If* $e_m(S,T) = 1$ *for all* $S \in E[m]$, *then* $T = \mathcal{O}$.
4. *(Galois invariant) For all* $\sigma \in G_{\overline{K}/K}$, $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$.

Definition 0.37. [Sil86, III §4] An *isogeny* between two elliptic curves E_1/K and E_2/K is a non-constant morphism $\phi : E_1 \to E_2$ which sends $\mathcal{O}_{E_1}$ to $\mathcal{O}_{E_2}$.

Proposition 0.38. [Sil86, III §6] *Suppose $\phi : E_1 \to E_2$ is an isogeny of degree m. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$.*

Proposition 0.39. [Sil86, III §6] *Suppose $\phi : E_1 \to E_2$ is an isogeny such that $\deg(\phi) = m$. Then*

1. *$\hat{\phi} \circ \phi = [m]$ on E_1, $\phi \circ \hat{\phi} = [m]$ on E_2.*
2. *$\hat{\hat{\phi}} = \phi$.*

Proposition 0.40. [Sil86, III §6] *Let E be an elliptic curve over a field K and let m be a non-zero integer. Then*

1. *$\deg([m]) = m^2$.*
2. *If $\mathrm{char}(K) = 0$ or if $\gcd(\mathrm{char}(K), m) = 1$, then*

$$E[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

3. *If $\mathrm{char}(K) = p$, then $E[p^e] \cong \{\mathcal{O}\}$ for all positive integers e or $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.*

Definition 0.41. Let L/K be a field extension. Then the *separable degree* of L/K is the degree of the largest intermediate field J such that J/K is a separable extension.

Proposition 0.42. [Sil86, III §4] *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\#(\ker(\phi)) = \deg_s(\phi)$, where $\deg_s(\phi)$ denotes the separable degree of ϕ.*

0.6 Group Cohomology

In this section, we merely state a few central ideas of group cohomology and Galois cohomology. A thorough treatment of the theory can be found in [Ser02].

Suppose M is a G-module, where G is a finite group.

Definition 0.43. The *zeroth cohomology group* $H^0(G, M)$ is the submodule of M containing G-invariant elements.

Definition 0.44. A *crossed homomorphism* $f : G \to M$ is a map such that $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ for all $\sigma, \tau \in G$. A *principal crossed homomorphism* $f : G \to M$ is a map such that $f(\sigma) = \sigma c - c$ for some fixed $c \in M$ and for all $\sigma \in G$.

The set of crossed homomorphisms form a group under addition and the set of principal crossed homomorphisms are a subgroup of the group of crossed homomorphisms.

Definition 0.45. The *first cohomology group* $H^1(G, M)$ is the group of all crossed homomorphisms $f : G \to M$ modulo principal crossed homomorphisms.

Remark 0.46. If G acts trivially on M, then $H^1(G, M) \cong \mathrm{Hom}(G, M)$.

Definition 0.47. $C^n(G, M)$ is the group of all continuous maps from G^n to M. Let the *coboundary map* $d^n : C^n(G, M) \to C^{n+1}(G, M)$ be given by

$$\begin{aligned} d^n(\eta)(\sigma_1, ..., \sigma_{n+1}) &= \sigma_1 \eta(\sigma_2, ..., \sigma_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i \eta(\sigma_1, ..., \sigma_{i-1}, \sigma_i \circ \sigma_{i+1}, \sigma_{i+2}, ..., \sigma_{n+1}) + (-1)^{n+1} \eta(\sigma_1, ..., \sigma_n) \end{aligned}$$

Note that $d^{n+1} \circ d^n = 0$.

Definition 0.48. We call $C^0(G, M) \to C^1(G, M) \to C^2(G, M)...$ a *cochain complex* and we define cohomology groups

$$H^n(G, M) = \frac{\ker(d^n)}{\mathrm{im}(d^{n-1})}$$

for $n \geq 1$.

Proposition 0.49. [Sil86, App. B] *Suppose* $0 \to P \to M \to N \to 0$ *is an exact sequence of* G*-modules. Then there exists a long exact sequence*

$$\begin{aligned} 0 \to H^0(G, P) \to H^0(G, M) \to H^0(G, N) \to \\ H^1(G, P) \to H^1(G, M) \to H^1(G, N) \to H^2(G, P) \to ... \end{aligned}$$

This is a result of the snake lemma.

0.6.1 Galois Cohomology

We usually consider G to be a Galois group acting on a field K. The Galois group $G_{\overline{K}/K}$ is the inverse limit of the Galois group $G_{L/K}$ with respect to finite extensions L of K. The coboundary maps are continous with respect to the profinite topology on $G_{\overline{K}/K}$ and the discrete topology on M.

Let M be a $G_{\overline{K}/K}$-module.

Definition 0.50. The *zeroth cohomology group* $H^0(G_{\overline{K}/K}, M)$ is the submodule of M containing $G_{\overline{K}/K}$-invariant elements.

Proposition 0.51. [Sil86, App. B] *Suppose* $0 \to P \to M \to N \to 0$ *is an exact sequence of* $G_{\overline{K}/K}$*-modules. Then there exists a long exact sequence*

$$0 \to H^0(G_{\overline{K}/K}, P) \to H^0(G_{\overline{K}/K}, M) \to H^0(G_{\overline{K}/K}, N) \to$$
$$H^1(G_{\overline{K}/K}, P) \to H^1(G_{\overline{K}/K}, M) \to H^1(G_{\overline{K}/K}, N) \to H^2(G_{\overline{K}/K}, P) \to ...$$

Theorem 0.52 (Hilbert's Theorem 90)**.** [Ser02, X] $H^1(G_{\overline{K}/K}, \overline{K}^*) = 0$

0.7 Gauss and Jacobi Sums

This section contains a number of elementary proofs explaining the properties of Gauss and Jacobi sums. We later use Gauss and Jacobi sums to evaluate the zeta-function of a Fermat surface.

Definition 0.53. A *multiplicative character* is a homomorphism from a multiplicative group to the multiplicative group of a field (usually $\overline{\mathbb{Q}}^\times$).

Definition 0.54. An *additive character* is a homomorphism from an additive group to the multiplicative group of a field (usually $\overline{\mathbb{Q}}^\times$).

We will generally denote multiplicative characters by χ and additive characters by ψ. The *trivial multiplicative character* ε maps every element of $\mathbb{F}_q^\times$ to the identity on $\overline{\mathbb{Q}}$.

Definition 0.55. Let $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ and $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}^\times$. Then a *Gauss sum* is given by

$$g(\chi, \psi) = -\sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x).$$

Definition 0.56. Let $\chi_1, ..., \chi_n$ be multiplicative characters $\mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$. Then the *Jacobi sums* $J_0(\chi_1, ..., \chi_n)$ and $J(\chi_1, ..., \chi_n)$ are given by

$$J_0(\chi_1, ..., \chi_n) = \sum_{x_1+...+x_n=0} \chi_1(x_1)...\chi_n(x_n)$$

where the sum is over all elements $x_1, ..., x_n \in \mathbb{F}_q^\times$ such that $x_1 + ... + x_n = 0$ and

$$J(\chi_1, ..., \chi_n) = \sum_{x_1+...+x_n=1} \chi_1(x_1)...\chi_n(x_n)$$

where where the sum is over all elements $x_1, ..., x_n \in \mathbb{F}_q^\times$ such that $x_1 + ... + x_n = 1$.

Proposition 0.57. [IR82, 8 §1] *Let χ be a multiplicative character. Then*

$$\sum_{x\in\mathbb{F}_q^\times}\chi(x)=\begin{cases} q-1 & \text{if } \chi=\varepsilon \\ 0 & \text{if } \chi\neq\varepsilon \end{cases}$$

Proof. If $\chi=\varepsilon$, then $\chi(x)=1$ for all $x\in\mathbb{F}_q^\times$. There are $q-1$ elements in $\mathbb{F}_q^\times$, so if $\chi=\varepsilon$ the sum is $q-1$.

Suppose $\chi\neq\varepsilon$. There exists an $x'\in\mathbb{F}_q^\times$ such that $\chi(x')\neq 1$. We have the identity

$$\sum_{x\in\mathbb{F}_q^\times}\chi(x)=\chi(x')\sum_{x\in\mathbb{F}_q^\times}\chi(x)$$

as multiplying by x' will permute the elements of $\mathbb{F}_q^\times$. As $\chi(x')\neq 1$, the only way this equality can hold is if $\sum_{x\in\mathbb{F}_q^\times}\chi(x)=0$. □

Similarly, if ψ is a non-trivial additive character, then

$$\sum_{x\in\mathbb{F}_q}\psi(x)=0.$$

Gauss and Jacobi sums are used to determine numbers of solutions of particular equations in finite fields, thus they are useful in understanding the zeta-functions of varieties. We will not use this theorem, but include it to motivate the use of Gauss and Jacobi sums in counting rational points on surfaces, particularly Fermat surfaces.

Theorem 0.58. [IR82, 8. §7] *Let $\chi_i:\mathbb{F}_p^\times\to\overline{\mathbb{Q}}^\times$ be multiplicative characters. The number of solutions N in $\mathbb{F}_p$ to the equation*

$$a_1x_1^{d_1}+\ldots+a_rx_r^{d_r}=b$$

is given by

$$N=\begin{cases} \sum_{\text{each }\chi_i^{d_i}=\varepsilon}\chi_1(a_1^{-1})\ldots\chi_r(a_r^{-1})J_0(\chi_1,\ldots,\chi_r) & \text{if } b=0 \\ \sum_{\text{each }\chi_i^{d_i}=\varepsilon}\chi_1(a_1^{-1})\ldots\chi_r(a_r^{-1})(\chi_1\ldots\chi_r)(b)J(\chi_1,\ldots,\chi_r) & \text{if } b\neq 0 \end{cases}$$

where the sums are taken over all χ_i such that $\chi_i^{d_i}=\varepsilon$.

We aim to prove general results about Gauss and Jacobi sums used in [Ulm02]. We extend the definition of multiplicative characters to allow $\chi(0)=0$, where χ is non-trivial. This allows us to write $\sum_{x\in\mathbb{F}_{p^f}}$ instead of $\sum_{x\in\mathbb{F}_{p^f}^\times}$.

Proposition 0.59. [IR82, 8. §2] *Let χ (multiplicative) and ψ (additive) be non-trivial characters mapping into $\overline{\mathbb{Q}}^\times$. Then $|g(\chi,\psi)|=p^{f/2}$.*

Proof. We want to compute $g(\chi,\psi)\overline{g(\chi,\psi)}$. If $\chi(x) = y$, then let $\overline{\chi}(x) = y^{-1} = \chi(x^{-1})$. Note that $\overline{\chi}$ is a character.

$$\begin{aligned} g(\chi,\psi)g(\overline{\chi},\psi) &= \sum_{x\in\mathbb{F}_{pf}^{\times}} \chi(x)\psi(x) \sum_{y\in\mathbb{F}_{pf}^{\times}} \overline{\chi}(y)\psi(y) \\ &= \sum_{x\in\mathbb{F}_{pf}} \sum_{y\in\mathbb{F}_{pf}} \chi(xy^{-1})\psi(x+y) \\ &= \sum_{x\in\mathbb{F}_{pf}} \chi(x) \sum_{y\in\mathbb{F}_{pf}} \psi((1+x)y) \\ &= \chi(-1)p^f \end{aligned}$$

The third equality is a result of making the substitution $x \to xy$ and the last equality is due to the fact that the second sum is equal to 0 by proposition 0.57 for all x such that $x \neq -1$. When $x = -1$, the second sum is equal to p^f. We also have

$$\begin{aligned} g(\overline{\chi},\psi) &= -\sum_{y\in\mathbb{F}_{pf}^{\times}} \overline{\chi}(y)\psi(y) \\ &= -\overline{\chi}(-1) \sum_{y\in\mathbb{F}_{pf}^{\times}} \overline{\chi}(-y)\psi(y) \\ &= -\chi(-1) \sum_{y\in\mathbb{F}_{pf}^{\times}} \overline{\chi(-y)\psi(-y)} \\ &= \chi(-1)\overline{g(\chi,\psi)} \end{aligned}$$

As $g(\overline{\chi},\psi) = \chi(-1)\overline{g(\chi,\psi)}$ and $g(\chi,\psi)g(\overline{\chi},\psi) = \chi(-1)p^f$, we have $g(\chi,\psi)\overline{g(\chi,\psi)} = p^f$ and so $|g(\chi,\psi)| = p^{f/2}$. □

Definition 0.60. A *quadratic Gauss sum* $g(\chi,\psi)$ is given by

$$g(\chi,\psi) = -\sum_{x\in\mathbb{F}_q^{\times}} t(x)^{\frac{q-1}{2}}\psi(x)$$

where t is a multiplicative character.

Proposition 0.61. [IR82, 6 §4] *If $g(\chi,\psi)$ is a quadratic Gauss sum, then*

$$g(\chi,\psi) = \begin{cases} \pm\sqrt{p} & \text{if } q \equiv 1 \mod 4 \\ \pm i\sqrt{p} & \text{if } q \equiv 3 \mod 4 \end{cases}$$

Proposition 0.62. [IR82, 8 §5] *Let $J_0(\chi_1,...,\chi_n)$ and $J(\chi_1,...,\chi_n)$ be Jacobi sums, where $\chi_1,...,\chi_n$ are multiplicative characters and are not all trivial, but $\chi_1...\chi_n = \varepsilon$. Then*

$$J(\chi_1,...,\chi_n) = \begin{cases} \frac{(-1)^n}{p^f} g(\chi_1,\psi)...g(\chi_n,\psi) & \text{if all } \chi_i \text{ are non-trivial} \\ 0 & \text{otherwise} \end{cases}$$

Also, $J(\chi_1, ..., \chi_n) = \frac{1}{p^f - 1} J_0(\chi_1, ..., \chi_n)$.

Proof. Suppose one of the characters is trivial. Let $\chi_1 = \varepsilon$ be the trivial character. Then

$$\begin{aligned} J_0(\chi_1, ..., \chi_n) &= \sum_{x_1 + ... + x_n = 0} \chi_1(x_1) ... \chi_n(x_n) \\ &= N \sum_{x_2 \in \mathbb{F}_{p^f}^\times} \chi_2(x_2) ... \sum_{x_n \in \mathbb{F}_{p^f}^\times} \chi_n(x_n) \\ &= 0 \end{aligned}$$

where $N \in \mathbb{N}$. This is because we can freely choose $x_2, ..., x_n$ and then let $x_1 = -(x_2 + ... + x_n)$ so that $x_1 + .. + x_n = 0$.

Suppose all of the characters are non-trivial. Then

$$\begin{aligned} J_0(\chi_1, ..., \chi_n) &= \sum_{x_1 + ... + x_n = 0} \chi_1(x_1) ... \chi_n(x_n) \\ &= \sum_{x_1 \in \mathbb{F}_{p^f}^\times} \chi_1(x_1) \left(\sum_{x_2 + ... + x_n = -x_1} \chi_2(x_2) ... \chi_n(x_n) \right) \\ &= (\chi_2 ... \chi_n)(-1) J(\chi_2, ..., \chi_n) \sum_{x_1 \in \mathbb{F}_{p^f}^\times} (\chi_1 ... \chi_n)(x_1) \\ &= \chi_1(-1) J(\chi_2, ..., \chi_n)(p^f - 1) \end{aligned}$$

where the last equality is due to the fact that $\chi_1 ... \chi_n = \varepsilon$. We compute $J_0(\chi_2, ..., \chi_n)$. If all of the characters are non-trivial and $\chi_1 ... \chi_n = \varepsilon$, then $\chi_2 ... \chi_n \neq \varepsilon$.

$$\begin{aligned} J_0(\chi_2, ..., \chi_n) &= \sum_{x_2 + ... + x_n = 0} \chi_2(x_2) ... \chi_n(x_n) \\ &= \sum_{x_2 \in \mathbb{F}_{p^f}^\times} \chi_2(x_2) \left(\sum_{x_3 + ... + x_n = -x_2} \chi(x_3) ... \chi_n(x_n) \right) \\ &= (\chi_3 ... \chi_n)(-1) J(\chi_3, ..., \chi_n) \sum_{x_2 \in \mathbb{F}_{p^f}^\times} (\chi_2 ... \chi_n)(x_2) \\ &= 0 \end{aligned}$$

Here the last equality is due to the proposition 0.57, as we know $\chi_2 ... \chi_n \neq \varepsilon$.

Assembling the previous calculations gives

$$\begin{aligned} g(\chi_1,\psi)...g(\chi_n,\psi) &= (-1)^n \sum_{x_1,...,x_n \in \mathbb{F}_{p^f}} \chi_1(x_1)...\chi_n(x_n)\psi(x_1+...+x_n) \\ &= (-1)^n \sum_{y\in\mathbb{F}_{p^f}} \sum_{x_1+...+x_n=y} \chi_1(x_1)...\chi_n(x_n)\psi(y) \\ &= (-1)^n \left(J_0(\chi_1,...,\chi_n) + J(\chi_1,...,\chi_n) \sum_{y\in\mathbb{F}_{p^f}^\times} \varepsilon(y)\psi(y) \right) \\ &= (-1)^n \left(J_0(\chi_1,...,\chi_n) + J(\chi_1,...,\chi_n)(-1) \right) \end{aligned}$$

Similarly, $g(\chi_2,\psi)...g(\chi_n,\psi) = (-1)^{n-1}\left(J_0(\chi_2,...,\chi_n) - J(\chi_2,...,\chi_n)g(\chi_2...\chi_n,\psi)\right)$. However, as $J_0(\chi_2,...,\chi_n) = 0$, we have

$$J(\chi_2,...,\chi_n) = (-1)^n \frac{g(\chi_2,\psi)...g(\chi_n,\psi)}{g(\chi_2...\chi_n,\psi)}.$$

Therefore,

$$\begin{aligned} J_0(\chi_1,...,\chi_n) &= \chi_1(-1)J(\chi_2,...,\chi_n)(p^f-1) \\ &= \chi_1(-1)(p^f-1)(-1)^n \frac{g(\chi_2,\psi)...g(\chi_n,\psi)}{g(\chi_2...\chi_n,\psi)} \\ &= \chi_1(-1)(p^f-1)(-1)^n \frac{g(\chi_1,\psi)...g(\chi_n,\psi)}{g(\chi_1,\psi)g(\overline{\chi_1},\psi)} \\ &= \chi_1(-1)(p^f-1)(-1)^n \frac{g(\chi_1,\psi)...g(\chi_n,\psi)}{\chi_1(-1)p^f} \\ &= (-1)^n \frac{p^f-1}{p^f} g(\chi_1,\psi)...g(\chi_n,\psi) \end{aligned}$$

Using the fact that $g(\chi_1,\psi)...g(\chi_n,\psi) = (-1)^n\left(J_0(\chi_1,...,\chi_n) - J(\chi_1,...,\chi_n)\right)$ gives

$$J(\chi_1,...,\chi_n) = \frac{(-1)^n}{p^f} g(\chi_1,\psi)...g(\chi_n,\psi)$$

$$J(\chi_1,...,\chi_n) = \frac{1}{p^f-1} J_0(\chi_1,...,\chi_n).$$

□

0.7.1 The Hasse-Davenport Relation

Definition 0.63. The *field trace* of a finite Galois field extension L/K is given by

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma\in G_{L/K}} \sigma(\alpha)$$

where $\alpha \in L$. In particular, if $K = \mathbb{F}_{p^f}$ and L is a finite field extension, then $L = \mathbb{F}_{p^{if}}$ where $(i \geq 1)$ and

$$\mathrm{Tr}_{L/K}(\alpha) = \alpha + \alpha^{p^f} + \alpha^{p^{2f}} ... + \alpha^{p^{(i-1)f}}$$

Definition 0.64. The *field norm* of a finite Galois field extension L/K is given by

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in G_{L/K}} \sigma(\alpha)$$

where $\alpha \in L$. In particular, if $K = \mathbb{F}_{p^f}$ and L is a finite field extension, then $L = \mathbb{F}_{p^{if}}$ where $(i \geq 1)$ and

$$\mathrm{N}_{L/K}(\alpha) = \alpha\alpha^{p^f}\alpha^{p^{2f}}...\alpha^{p^{(i-1)f}} = \alpha^{(p^{if}-1)/(p^f-1)}$$

Proposition 0.65 (Properties of the field trace)**.** *Let L/K be a separable extension.*

1. $\mathrm{Tr} : L \to K$ *is a K-linear map.*
2. $\mathrm{Tr} : L \to K$ *is a surjective map.*
3. *Suppose $K \subset J \subset L$ is a tower of fields. Then* $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{J/K} \circ \mathrm{Tr}_{L/J}$.

Proof. Although these properties hold in general for separable field extensions L/K, we prove them only for the simple case where $L = \mathbb{F}_{p^{if}}$ and $K = \mathbb{F}_{p^f}$. Clearly L/K is a Galois extension. Note $\mathrm{Tr} : L \to K$ as for all $x \in L$ and for all $\sigma_{L/K}$, we have $\mathrm{Tr}(x) = \sigma(\mathrm{Tr}(x))$.

(1) We want to show that

$$\mathrm{Tr}_{L/K}(\alpha x + \beta y) = \alpha \mathrm{Tr}_{L/K}(x) + \beta \mathrm{Tr}_{L/K}(y)$$

for all $\alpha, \beta \in K$ and for all $x, y \in L$. This follows from the definition of the field trace:

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha x + \beta y) &= \sum_{\sigma \in G_{L/K}} \sigma(\alpha x + \beta y) \\ &= \alpha \sum_{\sigma \in G_{L/K}} \sigma(x) + \beta \sum_{\sigma \in G_{L/K}} \sigma(y) \\ &= \alpha \mathrm{Tr}_{L/K}(x) + \beta \mathrm{Tr}_{L/K}(y) \end{aligned}$$

(2) Suppose $x \in \ker(\mathrm{Tr})$. Then x is a root of the polynomial

$$\alpha + \alpha^{p^f} + \alpha^{p^{2f}} ... + \alpha^{p^{f(i-1)}}$$

Therefore, there are at most $p^{f(i-1)}$ elements in the kernel of the trace map. Thus there are at least $\frac{p^{if}}{p^{f(i-1)}} = p^f$ elements in the image of the trace map, and as $\mathrm{im}(\mathrm{Tr}) \subset \mathbb{F}_{p^f}$, we conclude that $\mathrm{im}(\mathrm{Tr})$ contains p^f elements and the trace map is surjective. This implies that there are $p^{f(i-1)}$ elements in the kernel of the trace map. Thus the kernel of the trace map must have dimension $i-1$ as a $\mathbb{F}_{p^f}$-linear space.

(3) We use the fact that $G_{L/K}/G_{L/J} = G_{J/K}$.

$$\begin{aligned}
\mathrm{Tr}_{J/K}(\mathrm{Tr}_{L/J}(x)) &= \mathrm{Tr}_{J/K}\left(\sum_{\sigma\in G_{L/J}} \sigma(x)\right) \\
&= \sum_{\tau\in G_{J/K}} \tau\left(\sum_{\sigma\in G_{L/J}} \sigma(x)\right) \\
&= \sum_{\tau\in G_{L/K}/G_{L/J}} \sum_{\sigma\in G_{L/J}} \tau(\sigma(x)) \\
&= \sum_{\rho\in G_{L/K}} \rho(x) \\
&= \mathrm{Tr}_{L/K}(x)
\end{aligned}$$

□

We can define additive characters using the field trace and multiplicative characters using the field norm. Suppose we have a field extension $K \subset L$. Then if $\psi_0 : K \to \overline{\mathbb{Q}}^\times$ is an additive character on K, then we can define an additive character $\psi : L \to \overline{\mathbb{Q}}^\times$ by letting $\psi = \psi_0 \circ \mathrm{Tr}_{L/K}$. Similarly, if $\chi_0 : K \to \overline{\mathbb{Q}}^\times$, then we can define a multiplicative character $\chi : L \to \overline{\mathbb{Q}}^\times$ by $\chi = \chi_0 \circ \mathrm{N}_{L/K}$.

Theorem 0.66 (Hasse-Davenport relation)**.** [IR82, 11. §4] *Let K be a finite field with q elements and let $K \subset L$ be a finite Galois extension. Let $\chi(x) = \chi_0(\mathrm{N}_{L/K}(x))$ and $\psi(x) = \psi_0(\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(x))$, where χ is a multiplicative character and ψ is an additive character. Then*

$$g(\chi_0, \psi_0) = g(\chi, \psi)^n$$

where $n = [L : K]$.

Chapter 1

The Rank of Elliptic Curves

In this chapter, we relate the rank of an elliptic curve $E/\mathbb{K}$ to the rank of the Néron-Severi group of the associated elliptic surface $\mathcal{E}/\Bbbk$. Firstly, we prove the Mordell-Weil theorem, which states that $E(\mathbb{K})$ is a finitely generated Abelian group. Then we prove a theorem by Shioda relating the rank of $E(\mathbb{K})$ to the rank of the Néron-Severi group of $\mathcal{E}/\Bbbk$. We adapt Silverman's proof of the Mordell-Weil theorem given in [Sil94, III §2] to account for functions fields of the form $k(t)$, where $k = \Bbbk$ is a non-algebraically closed finite field of characteristic $p \neq 0$.

The group structure of $\mathrm{Pic}(E)$ can be used to impose a group structure on points in $E(\mathbb{K})$; however, this group structure does not directly provide a group structure on the associated elliptic surface $\mathcal{E}/\Bbbk$. The Néron-Severi group of a surface is somewhat analogous to the Mordell-Weil group of a curve, in that the group structure of the Néron-Severi group comes from the group structure of $\mathrm{Pic}(\mathcal{E})$. The Néron-Severi group of $\mathcal{E}$ is the Picard group of $\mathcal{E}$ modulo algebraic equivalence. We aim to write the rank of $E(\mathbb{K})$ in terms of the rank of the Néron-Severi group of $\mathcal{E}/\Bbbk$.

1.1 The Mordell-Weil Theorem

Theorem 1.1 (The Mordell-Weil theorem)**.** *The group $E(\mathbb{K})$ is a finitely generated Abelian group.*

The proof of this theorem is an application of the descent procedure on Abelian groups. We prove $E(\mathbb{K})/mE(\mathbb{K})$ is finite when $m = 2$, although this is true for all $m \in \mathbb{Z}$. We then define the 'height' of a point on an elliptic curve, which satisfies the conditions of the descent theorem (theorem 1.11).

1.1.1 The Weak Mordell-Weil Theorem

Theorem 1.2 (The Weak Mordell-Weil theorem)**.** *The group $E(\mathbb{K})/2E(\mathbb{K})$ is finite.*

We let $E/\mathbb{K}$ be the elliptic curve given by $y^2 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$ for distinct $\lambda_1, \lambda_2, \lambda_3 \in \overline{\mathbb{K}}$. All non-singular elliptic curves over a field not of characteristic 2 or 3 can be written in this form. We firstly demonstrate that we can assume without loss of generality $E[2] \subset E(\mathbb{K})$, then we show that $E(\mathbb{K})/2E(\mathbb{K})$ injects into a finite set.

Lemma 1.3. [Sil86, VIII §1] *Let $\mathbb{L} = \mathbb{K}([2]^{-1}E(\mathbb{K}))$, where $\mathbb{K}([2]^{-1}E(\mathbb{K}))$ is the field $\mathbb{K}$ adjoin all the coordinate values of all elements Q such that $2Q \in E(\mathbb{K})$. Then $\mathbb{L}/\mathbb{K}$ is a Galois extension.*

Sketch of proof. There are four elements of order dividing 2 in $E(\overline{\mathbb{K}})$, which form a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This follows from proposition 0.40, but can be seen by writing explicit equations for E as well as for the group law on E. As $\mathbb{K}$ is not of characteristic 2 or 3, we can write $E : y^2 = x^3 + ax + b$ for $a, b \in \mathbb{K}$. Explicit equations for the group law on elliptic curves show that if (x, y) has order 2, then $y = 0$. There are 3 points of order 2, corresponding to the three roots of $x^3 + ax + b = 0$, as well as the point $\mathcal{O}$ of order 1. (The roots of $x^3 + ax + b = 0$ must be distinct if $E/\mathbb{K}$ is a non-singular curve.) The group $E[2] = \ker([2])$, and $\#(\ker([2])) = \deg([2]) = 4$, so by proposition 0.42, the field extension $\mathbb{L}/\mathbb{K}$ must be separable. We show $\mathbb{L}$ is normal by showing that $G_{\overline{\mathbb{K}}/\mathbb{L}}$ is the kernel of a homomorphism.

Definition 1.4. [Sil86, VIII §1] The *Kummer Pairing* is a pairing

$$\kappa : E(\mathbb{K}) \times G_{\overline{\mathbb{K}}/\mathbb{K}} \to E[2]$$

given by $(P, \sigma) \mapsto Q^\sigma - Q$, where $E[2]$ is the set of points on E of order 2 and $2Q = P$ for some $Q \in E(\overline{\mathbb{K}})$. The action of $\sigma \in G_{\overline{\mathbb{K}}/\mathbb{K}}$ on Q is the action of σ on each of the coordinate values of Q.

This map is well-defined and independent of the choice of Q. We show that the kernel on the right is $G_{\overline{\mathbb{K}}/\mathbb{L}}$.

Suppose $\sigma \in G_{\overline{\mathbb{K}}/\mathbb{L}}$. Then $\kappa(P, \sigma) = Q^\sigma - Q$, but $Q \in E(\mathbb{L})$, so $\kappa(P, \sigma) = Q - Q = \mathcal{O}$. Thus σ is in the kernel of κ on the right.

Suppose $\sigma \in G_{\overline{\mathbb{K}}/\mathbb{K}}$ is in the kernel of κ on the right. Then $\kappa(P, \sigma) = \mathcal{O}$ for all $P \in E(\mathbb{K})$ and so $Q^\sigma - Q = \mathcal{O}$ for all choices of Q such that $2Q = P \in E(\mathbb{K})$. By

definition of $\mathbb{L}$, σ fixes all elements in $\mathbb{L}$, so the kernel on the right is a subset of $G_{\overline{\mathbb{K}}/\mathbb{L}}$. Thus $G_{\overline{\mathbb{K}}/\mathbb{L}}$ is normal and so $\mathbb{L}/\mathbb{K}$ is normal and hence Galois. □

Remark 1.5. The Galois group $G_{\mathbb{L}/\mathbb{K}}$ is Abelian, as there exists an injection $G_{\mathbb{L}/\mathbb{K}} \to \mathrm{Hom}(E(\mathbb{K}), E[2])$ given by $\sigma \mapsto \kappa(\cdot, \sigma)$. Additionally, $\sigma \in G_{\mathbb{L}/\mathbb{K}}$ has order 2. Thus $\mathbb{L}$ is a Abelian extension of exponent 2. (See [Sil86, VIII §1].)

Proposition 1.6. *Let $\mathbb{L}$ and $\mathbb{K}$ be as before. Then the extension $\mathbb{L}/\mathbb{K}$ is finite.*

Proof. We use the fact that $\mathbb{L}/\mathbb{K}$ is unramified outside of S, where

$$S = \left\{ v \;\middle|\; \begin{array}{l} \lambda_1, \lambda_2 \text{ or } \lambda_3 \text{ has a pole at } v \text{ or} \\ \quad \Delta = (\lambda_1 - \lambda_2)^2(\lambda_2 - \lambda_3)^2(\lambda_3 - \lambda_1)^2 \text{ vanishes at } v \end{array} \right\}$$

and where $\lambda_i \in \mathbb{L}$ is viewed as a map from $\mathbb{P}^1$ to $\mathbb{P}^1$ by considering λ_i as a rational function in t for $i = 1, 2, 3$. Note that there are finitely many elements in S. The proof of this fact for number fields L and K is given in [Sil86, VIII §1], but carries over word-for-word to the case where $\mathbb{L}$ and $\mathbb{K}$ are function fields.

We know that $\mathbb{L}$ is an Abelian extension of $\mathbb{K}$ of exponent 2. The characteristic of $\mathbb{K}$ is coprime to 2, so the maximal Abelian extension of exponent 2 of $\mathbb{K}$ is obtained by adjoining the square roots of all the elements in $\mathbb{K}$. This is a main result in Kummer theory, and can be found in [Lan02, VI §9].

Let $L/\mathbb{K}$ be the maximal Abelian extension of $\mathbb{K}$ of exponent 2 which is unramified outside of S. Then L is obtained by adjoining square roots of elements in $\mathbb{K}$. As L is unramified outside of S, we only need to adjoin the square roots of elements $f \in \mathbb{K}$ such that $\mathrm{ord}_v(f) \equiv 0 \mod 2$ for all $v \notin S$. (Here we are viewing f as a rational function $\mathbb{P}^1 \to \mathbb{P}^1$.) Additionally, we only need to adjoin the square roots of elements in $\mathbb{K}$ which are not in $\mathbb{K}^2$. Therefore,

$$L = \mathbb{K}(\sqrt{f} \mid f \in \mathbb{K}(S, 2))$$

where

$$\mathbb{K}(S, 2) = \{f \in \mathbb{K}^*/\mathbb{K}^{*2} \mid \mathrm{ord}_v(f) \equiv 0 \mod 2 \ \forall v \notin S\}.$$

We prove $\mathbb{K}(S, 2)$ is a finite set of points in order to conclude that $L/\mathbb{K}$ is finite. Let

$$\mathbb{K}(\varnothing, 2) = \{f \in \mathbb{K}^*/\mathbb{K}^{*2} \mid \mathrm{ord}_v(f) \equiv 0 \mod 2 \ \forall v \in \mathbb{P}^1\}.$$

Let $\#S$ be the (finite) number of elements of S and let α be the map given by $\alpha : f \mapsto (\mathrm{ord}_v(f) \mod 2)_{v \in S}$. By the exact sequence,

$$0 \longrightarrow \mathbb{K}(\varnothing, 2) \longrightarrow \mathbb{K}(S, 2) \xrightarrow{\alpha} (\mathbb{Z}/2\mathbb{Z})^{\#S}$$

if $\mathbb{K}(\varnothing, 2)$ is finite, then $\mathbb{K}(S, 2)$ is finite. Suppose $f \in \mathbb{K}(\varnothing, 2)$. We consider f as a map from $\mathbb{P}^1 \to \mathbb{P}^1$. By proposition 0.16,

$$\mathrm{div}(f) = 2a_1(P_1) + ... + 2a_n(P_n)$$

for some $a_1, ..., a_n \in \mathbb{Z}$ such that $a_1 + ... + a_n = 0$. Thus $\mathrm{div}(f) = 2\mathrm{div}(g)$ for some $g \in \mathbb{K}^*/\mathbb{K}^{*2}$. We have $\mathrm{div}(fg^{-2}) = 0$, so $f = cg^2$ for some $c \in \mathbb{F}_q$ and $f \equiv 0 \mod \mathbb{K}^{*2}$. Therefore $\mathbb{K}(\varnothing, S)$ is trivial and $\mathbb{K}(S, 2)$ is finite. As L is the maximal Abelian extension of $\mathbb{K}$ of exponent 2 which is unramified outside of S, $\mathbb{L} \subseteq L$. Therefore, $\mathbb{L}/\mathbb{K}$ is finite. □

Lemma 1.7. [Sil86, VIII §1] *Let $\mathbb{L}$ and $\mathbb{K}$ be as before. If $E(\mathbb{L})/2E(\mathbb{L})$ is finite, then $E(\mathbb{K})/2E(\mathbb{K})$ is finite.*

Proof. Consider the natural map $\phi : E(\mathbb{K})/2E(\mathbb{K}) \to E(\mathbb{L})/2E(\mathbb{L})$. The sequence

$$0 \longrightarrow \ker(\phi) \longrightarrow E(\mathbb{K})/2E(\mathbb{K}) \xrightarrow{\phi} E(\mathbb{L})/2E(\mathbb{L})$$

is exact. To show that $E(\mathbb{K})/2E(\mathbb{K})$ is finite, we need to show that $\ker(\phi)$ is finite. We have

$$\ker(\phi) = \frac{E(\mathbb{K}) \cap 2E(\mathbb{L})}{2E(\mathbb{K})}.$$

Let $\varphi_P : G_{\mathbb{L}/\mathbb{K}} \to E[2]$ be given by $\sigma \mapsto Q^\sigma - Q$, where $Q \in E(\overline{\mathbb{K}})$ is such that $2Q = P$. This map is independent of choice of Q. Let $G : \ker(\phi) \to Map(G_{\mathbb{L}/\mathbb{K}}, E[2])$ be given by $P \mapsto \varphi_P$. This map is well-defined. We show that it is an injection.

Suppose $\varphi_P = \varphi_{P'}$ for some $P, P' \in \ker(\phi)$. Then $Q^\sigma - Q = Q'^\sigma - Q'$ for all $\sigma \in G_{\mathbb{L}/\mathbb{K}}$ and for some choice of Q and Q' such that $2Q = P$ and $2Q' = P'$. Thus $(Q - Q')^\sigma = Q - Q'$ for all $\sigma \in G_{\mathbb{L}/\mathbb{K}}$, so $(Q - Q') \in E(\mathbb{K})$. Therefore,

$$P - P' = [2](Q - Q') \in 2E(\mathbb{K})$$

and so $P \equiv P'$ in $\ker(\phi)$. The map G is an injective map from $\ker(\phi)$ into $Map(G_{\mathbb{L}/\mathbb{K}}, E[2])$, a finite set. Thus $\ker(\phi)$ is finite and so $E(\mathbb{K})/2E(\mathbb{K})$ is finite. □

Lemma 1.8. *[Sil86, VIII §1] The Kummer pairing induces an injective map*

$$E(\mathbb{K})/2E(\mathbb{K}) \times G_{\mathbb{L}/\mathbb{K}} \to E[2].$$

Proof. We have shown that the kernel of the Kummer pairing on the right is $G_{\overline{\mathbb{K}}/\mathbb{L}}$. It remains to show that the kernel of the Kummer pairing on the left is $2E(\mathbb{K})$.

Suppose $P \in 2E(\mathbb{K})$. Then $P = 2Q$ for some $Q \in E(\mathbb{K})$. Then $\kappa(P,\sigma) = Q^\sigma - Q = \mathcal{O}$, as $Q \in E(\mathbb{K})$ so Q is fixed under $\sigma \in G_{\overline{K}/\mathbb{K}}$.

Suppose $\kappa(P,\sigma) = \mathcal{O}$ for all $\sigma \in G_{\overline{K}/\mathbb{K}}$. Then if $Q \in E(\overline{\mathbb{K}})$ is such that $2Q = P$, then Q is fixed by all $\sigma \in G_{\overline{\mathbb{K}}/\mathbb{K}}$. Therefore, $Q \in E(\mathbb{K})$, so $P \in 2E(\mathbb{K})$.

Therefore, there exists an injection $E(\mathbb{K})/2E(\mathbb{K}) \times G_{\mathbb{L}/\mathbb{K}} \to E[2]$. □

Proof of the weak Mordell-Weil theorem. We know from proposition 1.6 and lemma 1.3 that $\mathbb{L}/\mathbb{K}$ is a finite Galois extension. Therefore, $G_{\mathbb{L}/\mathbb{K}}$ is finite. We also know from lemma 1.8 that there exists an injection $E(\mathbb{K})/2E(\mathbb{K}) \to \mathrm{Hom}(G_{\mathbb{L}/\mathbb{K}}, E[2])$. As $\mathrm{Hom}(G_{\mathbb{L}/\mathbb{K}}, E[2])$ is finite, $E(\mathbb{K})/2E(\mathbb{K})$ is finite. □

Using Galois cohomology, it is possible to give a more explicit proof of the weak Mordell-Weil theorem, by giving an injective map

$$F : E(\mathbb{K})/2E(\mathbb{K}) \to (\mathbb{K}^*/\mathbb{K}^{*2}) \times (\mathbb{K}^*/\mathbb{K}^{*2})$$

such that the image of F is a finite set. We give a second proof of the weak Mordell-Weil theorem by constructing F. By lemma 1.7, we can assume without loss of generality that $E[2] \subseteq E(\mathbb{K})$.

Lemma 1.9. [Sil86, VIII §3] *There exists an injective map*

$$F : E(\mathbb{K})/2E(\mathbb{K}) \to (\mathbb{K}^*/\mathbb{K}^{*2}) \times (\mathbb{K}^*/\mathbb{K}^{*2}).$$

Proof. The sequence

$$0 \longrightarrow E[2] \longrightarrow E(\overline{\mathbb{K}}) \xrightarrow{[2]} E(\overline{\mathbb{K}}) \longrightarrow 0$$

is exact. From this, we get the exact sequence of cohomology

$$E(\mathbb{K}) \xrightarrow{[2]} E(\mathbb{K}) \xrightarrow{\delta} H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2])$$

and so the map $E(\mathbb{K})/2E(\mathbb{K}) \to H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2])$ is an injection. The coboundary map δ is by definition the map $\delta : P \mapsto \kappa(P,\sigma)$, where κ is the Kummer pairing. As the Galois group $G_{\overline{\mathbb{K}}/\mathbb{K}}$ acts trivially on $E[2]$, we have

$$\begin{aligned} H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2]) &\cong \mathrm{Hom}(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2]) \\ &\cong \mathrm{Hom}(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \\ &\cong \mathrm{Hom}(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mathbb{Z}/2\mathbb{Z})^2 \\ &\cong \mathrm{Hom}(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)^2 \\ &\cong H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)^2 \end{aligned}$$

where μ_2 is the group of second roots of unity in $\mathbb{K}$. The sequence:

$$1 \longrightarrow \mu_2 \longrightarrow \overline{\mathbb{K}}^* \xrightarrow{2} \overline{\mathbb{K}}^* \longrightarrow 1$$

is exact. Thus

$$1 \longrightarrow \mathbb{K}^*/\mathbb{K}^{*2} \xrightarrow{\delta'} H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2) \longrightarrow H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \overline{\mathbb{K}}^*)$$

is exact. By Hilbert's Theorem 90, $H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \overline{\mathbb{K}}^*) = 0$, so the middle map is an isomorphism and $\mathbb{K}^*/\mathbb{K}^{*2} \cong H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)$. Therefore,

$$H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2]) \cong (\mathbb{K}^*/\mathbb{K}^{*2}) \times (\mathbb{K}^*/\mathbb{K}^{*2}).$$

The coboundary map $\delta' : \mathbb{K}^*/\mathbb{K}^{*2} \to H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)$ is given by $\delta'(b)(\sigma) = \frac{\beta^\sigma}{\beta}$, where $\beta^2 = b$. If F is the map

$$E(\mathbb{K})/2E(\mathbb{K}) \xrightarrow{\delta} H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2]) \cong H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)^2 \xrightarrow{\delta'^{-1} \times \delta'^{-1}} \left(\frac{\mathbb{K}^*}{\mathbb{K}^{*2}}\right) \times \left(\frac{\mathbb{K}^*}{\mathbb{K}^{*2}}\right)$$

then F is an injection. □

Lemma 1.10. [Sil86, X §1] *The image of F is finite.*

Sketch of proof. We sketch the main ideas of this proof, but more verification is required to check the maps are as claimed. See [Sil86, X §1] for details.

Let T_1, T_2 and T_3 correspond to the points of order 2 $(\lambda_1, 0)$, $(\lambda_2, 0)$ and $(\lambda_3, 0)$ respectively. We want to figure out exactly what the map F is. We have the following maps

$$\begin{array}{ccc} E(\mathbb{K})/2E(\mathbb{K}) & \xrightarrow{\delta} & H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2]) \\ \downarrow F & & \downarrow e \\ (\mathbb{K}^*/\mathbb{K}^{*2}) \times (\mathbb{K}^*/\mathbb{K}^{*2}) & \xrightarrow{(\delta', \delta')} & H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, \mu_2)^2 \end{array}$$

where e is induced by some isomorphism between $E[2]$ and $\mu_2 \times \mu_2$. We claim $F : P = (x, y) \mapsto (x - \lambda_1, x - \lambda_2)$ for all $P \neq T_i$ for $i = 1, 2$ and for $P \neq \mathcal{O}$.

We let e be induced by the Weil pairing $e_2 : E[2] \times E[2] \to \mu_2$. Suppose $h \in H^1(G_{\overline{\mathbb{K}}/\mathbb{K}}, E[2])$. Then let $e(h) = (e_2(h, T_1), e_2(h, T_2))$. It can be checked that e is in fact an isomorphism. We want to show $\delta' \circ F = e \circ \delta$.

Let $i = 1, 2$. Let $Q \in E(\overline{\mathbb{K}})$ be an element such that $2Q = P \in E(\mathbb{K})$. By definition of the Weil pairing,

$$e_2(Q^\sigma - Q, T_i) = \frac{g_i(X + Q^\sigma - Q)}{g_i(X)}$$

for some $f_i, g_i \in \overline{\mathbb{K}}(\mathbb{P}^1)$ such that $g_i^2 = f_i \circ [2]$ and $\mathrm{div}(f_i) = 2(T_i) - 2(\mathcal{O})$, and at a place X such that $g_i(X)$ is defined and non-zero. Letting $X = Q$, we have

$$e_2(Q^\sigma - Q, T_i) = \frac{g_i(Q)^\sigma}{g_i(Q)}.$$

We know $\delta'(x - \lambda_i) = \beta_i^\sigma/\beta_i$ for some β_i such that $\beta_i^2 = x - \lambda_i$. The divisor of $x - \lambda_i$ is $2(T_i) - 2(\mathcal{O})$, so we can let $f_i(P) = x - \lambda_i$, for $P = (x, y)$. Then $(g_i(Q))^2 = f_i(2Q) = x - \lambda_i$, where $2Q = P = (x, y)$. Therefore, we can let $\beta_i = g_i(Q)$.

Thus for $P = 2Q$,

$$\begin{aligned}
(\delta'(F(P)), \delta'(F(P))) &= (\delta'(x - \lambda_1), \delta'(x - \lambda_2)) \\
&= \left(\frac{\beta_1^\sigma}{\beta_1}, \frac{\beta_2^\sigma}{\beta_2}\right) \\
&= \left(\frac{g_1(Q)^\sigma}{g_1(Q)}, \frac{g_2(Q)^\sigma}{g_2(Q)}\right) \\
&= (e_2(Q^\sigma - Q, T_1), e_2(Q^\sigma - Q, T_2)) \\
&= (e_2(\kappa(P, \sigma), T_1), e_2(\kappa(P, \sigma), T_2)) \\
&= e(\delta(P))
\end{aligned}$$

and so the claimed maps commute. We conclude F is the map

$$F : P = (x, y) \mapsto (x - \lambda_1, x - \lambda_2)$$

for $x \neq \lambda_1, \lambda_2$ and $P \neq \mathcal{O}$. Moreover, we can show $F(P) \in \mathbb{K}(S, 2) \times \mathbb{K}(S, 2)$, a finite set. We want to show that $\mathrm{ord}_v(x - \lambda_i) \equiv 0 \mod 2$ for all $v \notin S$ and for $i = 1, 2$. Let $n = \mathrm{ord}_v(x - \lambda_i)$ and suppose j and k are such that i, j and k are distinct.

1. Suppose $n = 0 = \mathrm{ord}_v(x - \lambda_i)$. Then clearly $\mathrm{ord}_v(x - \lambda_i) \equiv 0 \mod 2$.
2. Suppose $n < 0$. Then $(x - \lambda_i)$ has a pole at v. Also

$$n = \mathrm{ord}_v(x - \lambda_i) = \mathrm{ord}_v(x - \lambda_j) = \mathrm{ord}_v(x - \lambda_k) = \mathrm{ord}_v(x)$$

Thus $2\mathrm{ord}_v(y) = 3n$ and so $n \equiv 0 \mod 2$.

3. Suppose $n > 0$. Then $(x - \lambda_i)$ has a zero at v.

$$\min\{\mathrm{ord}_v(x - \lambda_i), \mathrm{ord}_v(x - \lambda_j)\} \leq \mathrm{ord}_v((x - \lambda_i) - (x - \lambda_j)) = \mathrm{ord}_v(\lambda_j - \lambda_i) = 0$$

as $\lambda_1, \lambda_2, \lambda_3$ do not have poles at t and Δ does not vanish at v. Therefore, $\mathrm{ord}_v(x - \lambda_j) = 0$ and $\mathrm{ord}_v(x - \lambda_k) = 0$, which implies

$$2\mathrm{ord}_v(y) = \mathrm{ord}_v((x - \lambda_i)(x - \lambda_j)(x - \lambda_k)) = \mathrm{ord}_v(x - \lambda_i)$$

and $\mathrm{ord}_v(x-\lambda_i) \equiv 0 \mod 2$. Thus F is injective and $F(P) \in \mathbb{K}(S,2) \times \mathbb{K}(S,2)$, a finite set, for all $P \in E(\mathbb{K})/2E(\mathbb{K})$ such that $P \neq (\lambda_1, 0), (\lambda_2, 0), \mathcal{O}$.

F is not defined at $(\lambda_1, 0), (\lambda_2, 0)$ and at $\mathcal{O}$. However, this is a finite number of points, so does not affect the finiteness of $E(\mathbb{K})/2E(\mathbb{K})$. F can be extended to send $(\lambda_1, 0), (\lambda_2, 0)$ and $\mathcal{O}$ to points in $\mathbb{K}(S,2) \times \mathbb{K}(S,2)$ (see [Sil86, X §1]).

Hence we have shown that $F : E(\mathbb{K})/2E(\mathbb{K}) \to (\mathbb{K}^*/\mathbb{K}^{*2}) \times (\mathbb{K}^*/\mathbb{K}^{*2})$ is injective and the image of F is finite. □

1.1.2 Heights and Descent

Theorem 1.11 (Descent Theorem)**.** [Sil86, VIII §3] *Let A be an Abelian group such that A/mA is finite for some $m \in \mathbb{Z}$. Suppose there exists a height function $h : A \to \mathbb{R}$ satisfying the following three properties:*

1. Suppose $Q \in A$. Then there exists a constant C_1 depending on A and Q such that for all $P \in A$, $h(P+Q) \leq 2h(P) + C_1$

2. There is an integer $m \geq 2$ and a constant C_2 depending on A such that for all $P \in A$, $h(mP) \geq m^2 h(P) - C_2$

3. For every constant C_3, $\{P \in A \mid h(P) \leq C_3\}$ is a finite set

Then A is finitely generated.

Proof. [Sil86, VII §4] □

We apply the descent theorem to prove that $E(\mathbb{K})$ is finitely generated. By the weak Mordell-Weil theorem, $E(\mathbb{K})/2E(\mathbb{K})$ is finite. We need to define some notion of height on $E(\mathbb{K})$ which satifies the properties of the descent theorem. Elements of $\mathbb{K}$ can be considered as rational functions in t, so if $f \in \mathbb{K}$, then we can consider f as a rational function $f : \mathbb{P}^1 \to \mathbb{P}^1$.

Definition 1.12. The *height of an element $f \in \mathbb{K}$* is the maximal degree of the numerator and the denominator of f, when considered as a rational function in t, and is denoted $h(f)$. Suppose $E/\mathbb{K}$ is given by a Weierstrass equation. The *height of a point $P = (x, y) \neq \mathcal{O}$* is given by $h(x)$ and is denoted by $h(P)$. Define $h(\mathcal{O}) = 0$.

For $\mathbb{K} = \mathbb{F}_q(t)$, the number of elements of $\mathbb{K}$ with height less than a given $n \in \mathbb{Z}$ is finite. Thus if $A = E(\mathbb{K})$, then property (3) of the descent theorem holds. The first two properties of the descent theorem can be proved by arithmetic manipulation of the group law.

Theorem 1.13. [Sil94, III §4] *Let $E/\mathbb{K}$ be an elliptic curve and h as before. Then*

1. *$h(P+Q)+h(P-Q)=2h(P)+2h(Q)+C_1$ for all $P,Q\in E(\mathbb{K})$*
2. *$h(2P)=4h(P)+C_2$ for all $P\in E(\mathbb{K})$*

where C_1 and C_2 depend on the elliptic curve $E/\mathbb{K}$.

Proof. [Sil94, III §4] □

Proof of the Mordell-Weil theorem. If $A=E(\mathbb{K})$, the conditions of the descent theorem hold. In subsection 1.1.1, we showed that $E(\mathbb{K})/2E(\mathbb{K})$ is finite. Therefore by the descent theorem, $E(\mathbb{K})$ is a finitely generated Abelian group. □

By the Mordell-Weil theorem, we know that $E(\mathbb{K})$ is a finitely generated Abelian group. Thus

$$E(\mathbb{K})\cong\mathbb{Z}^r\oplus\mathbb{Z}/q_1\mathbb{Z}\oplus...\oplus\mathbb{Z}/q_n\mathbb{Z}$$

where $q_1,...,q_n$ are powers of primes.

Definition 1.14. The *rank* of an elliptic curve $E/\mathbb{K}$ can be considered as the number of independent points in $E(\mathbb{K})$ of infinite order. If

$$E(\mathbb{K})\cong\mathbb{Z}^r\oplus\mathbb{Z}/q_1\mathbb{Z}\oplus...\oplus\mathbb{Z}/q_n\mathbb{Z}$$

then $\mathrm{Rank}(E(\mathbb{K}))=r$.

We also have

$$\begin{aligned}E(\mathbb{K})/2E(\mathbb{K})&\cong(\mathbb{Z}/2\mathbb{Z})^r\oplus(\mathbb{Z}/q_1\mathbb{Z})/2(\mathbb{Z}/q_1\mathbb{Z})\oplus...\oplus(\mathbb{Z}/{p_n}^{a_n}\mathbb{Z})/2(\mathbb{Z}/{p_n}^{a_n}\mathbb{Z})\\&\cong(\mathbb{Z}/2\mathbb{Z})^r\oplus(\mathbb{Z}/2\mathbb{Z})^N\end{aligned}$$

where if $E[2]\subseteq E(\mathbb{K})$, then $N=2$, otherwise $N=0$ or 1. To calculate the rank of $E/\mathbb{K}$, one could potentially look at the number of copies of $\mathbb{Z}/2\mathbb{Z}$ in $E(\mathbb{K})/2E(\mathbb{K})$ and the number of points of order 2 in $E(\mathbb{K})$.

Definition 1.15. If $E(\mathbb{K})\cong\mathbb{Z}^r\oplus\mathbb{Z}/q_1\mathbb{Z}\oplus...\oplus\mathbb{Z}/q_n\mathbb{Z}$, then the torsion subgroup of $E(\mathbb{K})$ is given by

$$E(\mathbb{K})_{\mathrm{tor}}\cong\mathbb{Z}/q_1\mathbb{Z}\oplus...\oplus\mathbb{Z}/q_n\mathbb{Z}$$

where $q_1,...,q_n$ are powers of primes.

Proposition 1.16. *$E(\mathbb{K})_{tor}$ is generated by 2 elements.*

Proof. By proposition 0.40, if

$$E(\mathbb{K}) \cong \mathbb{Z}^r \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/q_n\mathbb{Z}$$

where $q_1, ..., q_n$ are powers of primes, then for every prime p, p divides at most two elements of the set $\{q_1, ..., q_n\}$. Therefore, we can write the set $\{q_1, ..., q_n\}$ as a disjoint union of two sets $A = \{q_{a,1}, ..., q_{a,n_a}\}$ and $B = \{q_{b,1}, ..., q_{b,n_b}\}$, such that if q_i and q_j (where $i \neq j$) are elements of the same set, then q_i and q_j are coprime. Therefore

$$\mathbb{Z}/q_{a,1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/q_{a,n_a}\mathbb{Z}$$

is a cyclic group with one generator, call this α, and

$$\mathbb{Z}/q_{b,1}\mathbb{Z} \oplus ... \oplus \mathbb{Z}/q_{b,n_b}\mathbb{Z}$$

is a cyclic group with one generator, call this β. The group $E(\mathbb{K})_{\text{tor}}$ is thus generated by α and β. □

Note that for a function field $K = k(C)$, where k is an infinite field, the group $E(K)$ is not necessarily finitely generated.

1.1.3 An Upper Bound on Rank$(E(\mathbb{K}))$

During the proof of the weak Mordell-Weil theorem, we used the fact that the following sequence is exact and proved that $\mathbb{K}(\varnothing, 2)$ is trivial. We have

$$0 \longrightarrow \mathbb{K}(\varnothing, 2) \cong 0 \longrightarrow \mathbb{K}(S, 2) \xrightarrow{\alpha} (\mathbb{Z}/2\mathbb{Z})^{\#S}$$

where $\#S$ is the number of elements of S and $\alpha : f \mapsto (\text{ord}_u(f) \mod 2)_{u \in S}$. Thus the map $\alpha : \mathbb{K}(S, 2) \to (\mathbb{Z}/2\mathbb{Z})^{\#S}$ is an injection. Also, we proved that the map $F : E(\mathbb{K})/2E(\mathbb{K}) \to \mathbb{K}(S, 2) \times \mathbb{K}(S, 2)$ is an injection. So there exists an injection $E(\mathbb{K})/2E(\mathbb{K}) \to (\mathbb{Z}/2\mathbb{Z})^{\#S} \times (\mathbb{Z}/2\mathbb{Z})^{\#S}$. Supposing $E[2] \subseteq E(\mathbb{K})$, then $\text{Rank}(E(\mathbb{K})) \leq 2\#S - 2$. Thus to find elliptic curves with large rank, we must increase the number of points in S.

1.2 The Néron-Severi group

Definition 1.17. The *Néron-Severi group* of a variety X is the group of divisors on X modulo algebraic equivalence. We denote this group by $\text{NS}(X)$.

1.2.1 Algebraic Equivalence of Divisors

Definition 1.18. [Har77, V Ex.1.7] Let D_0 and D_1 be two divisors on a surface $\mathcal{S}$. Then D_0 and D_1 are *prealgebraically equivalent* if there exists a non-singular curve C and a divisor D on $\mathcal{S} \times C$ such that no irreducible component of D is contained in $\mathcal{S} \times \{t\}$ for all closed points t on C, and such that there exist closed points t_0 and t_1 on C such that D_0 and D_1 correspond to the divisor D on $\mathcal{S} \times \{t_0\}$ and $\mathcal{S} \times \{t_1\}$ respectively.

Proposition 1.19. *If two divisors are linearly equivalent, then they are algebraically equivalent.*

Proof. We show that for any prinicipal divisor $\mathrm{div}(f)$ on a surface $\mathcal{S}$, $\mathrm{div}(f) \sim 0$, where $\sim$ denotes algebraic equivalence. Consider the principal divisor $(Xf - Y)$, where $[X, Y] \in \mathbb{P}^1$. The points $[0, 1]$ and $[1, 0]$ are closed points on $\mathbb{P}^1$ so (f) and (1) are prealgebraically equivalent. The divisor (1) on $\mathcal{S}$ is algebraically equivalent to 0 by the parametrisation of the principal divisor (X), where $[X, Y] \in \mathbb{P}^1$. Thus $\mathrm{div}(f) \sim 0$. □

By this proposition, the Néron-Severi group of a surface $\mathcal{S}$ is a quotient group of $\mathrm{Pic}(\mathcal{S})$.

Suppose $\mathcal{E}$ is an elliptic surface with a map $\mathcal{E} \to \mathbb{P}^1$. Divisors corresponding to fibres on $\mathcal{E}$ can be parametrised by $\mathbb{P}^1$. By definition, any two divisors corresponding to two fibres E_r and E_s are algebraically equivalent. This is because r and s are closed points in $\mathbb{P}^1$, thus E_r and E_s are prealgebraically equivalent.

Definition 1.20. Two divisors D_1 and D_2 are *numerically equivalent* if for every divisor D, $D_1 \cdot D = D_2 \cdot D$.

Proposition 1.21. [Har77, V Ex.1.7] *If two divisors are algebraically equivalent, then they are numerically equivalent.*

1.2.2 The Rank of Elliptic Curves and Surfaces

We wish to find a relationship between the rank of an elliptic curve $E/\mathbb{K}$ and the rank of the Néron-Severi group of the corresponding elliptic surface $\mathcal{E}/\Bbbk$. Firstly, we sketch a proof of the fact that the smooth part of the Picard variety of an elliptic surface $\mathcal{E}/\Bbbk$ is trivial.

Definition 1.22. $\mathrm{PicVar}_{\mathcal{E}}$ is the smooth (reduced) part of the Picard variety $\mathrm{Pic}^0(\mathcal{E}/\Bbbk)$.

Definition 1.23. [Shi99] The K/k-trace of an Abelian variety A is a pair (τ, B) where B is an Abelian variety over k and $\tau : B \to A$ is a homomorphism with the property that if (τ', B') is a pair such that B' is an Abelian variety over k and $\tau' : B' \to A$ is a homomorphism, then there exists a unique homomorphism $\phi : B' \to B$ such that $\tau' = \tau \circ \phi$.

The K/k-trace exists for every Abelian variety and is an invariant [Cho55].

Theorem 1.24. [Shi99] *Let $\mathcal{S}$ be a surface defined over a field k equipped with a non-constant map $f : \mathcal{S} \to C$, where C is a non-singular projective curve. The map $f^* : \mathrm{Pic}^0(C) \to \mathrm{PicVar}_{\mathcal{S}}$ is an isomorphism if and only if the $k(C)/k$-trace of $\mathrm{Pic}^0_K(\mathcal{S})$ is trivial.*

We give a sketch of the proof of a weaker claim.

Proposition 1.25. *Let $\mathcal{E}$ be an elliptic surface defined over a field k and equipped with a non-constant map $\pi : \mathcal{E} \to C$, where C is a non-singular projective curve, such that $\mathcal{E}$ corresponds to an elliptic curve $E/k(C)$ whose j-invariant does not lie in k. Then $PicVar_{\mathcal{E}} \cong Pic^0(C)$.*

Sketch of proof. The $k(C)/k$ trace of $A = \mathrm{Pic}^0(E/k(C))$ is a pair (τ, B) such that B is an Abelian variety defined over $\Bbbk$ and $\tau : B \to \mathrm{Pic}^0(E/k(C))$ is a homomorphism. We know B must be either $\mathrm{Pic}^0(E/k(C))$ or trivial. This is because B must be a variety of dimension 0 or 1, and if B is a variety of dimension 1, then it must be equal to the whole of $\mathrm{Pic}^0(E/k(C))$ as $E/k(C)$ is irreducible. If B is $\mathrm{Pic}^0(E/k(C))$, then the j-invariant of $E/k(C)$ must lie in k. By assumption, the j-invariant of $E/k(C)$ does not lie in k, so B is trivial. Therefore, the $k(C)/k$-trace (τ, B) is trivial (τ is the zero map and $B = 0$).

There exist maps

$$0 \longrightarrow \mathrm{Pic}^0(C) \xrightarrow{\alpha} \mathrm{PicVar}_{\mathcal{E}} \xrightarrow{\beta} \mathrm{Pic}^0(E/k(C))$$

where α is the pullback map of $\pi : \mathcal{E} \to C$ and β is restriction to the generic fibre. We know that α maps into $\mathrm{PicVar}_{\mathcal{E}}$, as $\mathrm{PicVar}_{\mathcal{E}}$ is the smooth part of $\mathrm{Pic}^0(\mathcal{E}/k)$. The pullback map $\alpha : \mathrm{Pic}^0(C) \to \mathrm{PicVar}_{\mathcal{E}}$ maps divisors on C to fibral divisors on $\mathcal{E}$.

Restriction to the generic fibre gives a homomorphism

$$\beta : \mathrm{PicVar}_{\mathcal{E}} \to \mathrm{Pic}^0(E/k(C)).$$

By the property of the $k(C)/k$-trace, there exists a unique homomorphism ϕ : $\mathrm{PicVar}_{\mathcal{E}} \to 0$ such that $\beta = \tau \circ \phi$. We know that ϕ and τ are the zero maps, so β is also the zero map. Thus we have the sequence

$$0 \longrightarrow \mathrm{Pic}^0(C) \xrightarrow{\alpha} \mathrm{PicVar}_{\mathcal{E}} \xrightarrow{\beta} 0$$

and wish to show that it is exact. We know that β is the restriction to the generic fibre of divisors in $\mathrm{PicVar}_{\mathcal{E}}$, and as β is the 0 map, all divisors in $\mathrm{PicVar}_{\mathcal{E}}$ must be fibral divisors. We also know that all divisors in the image of α are fibral divisors, so the image of α is in the kernel of β. The image of α contains the irreducible component of all non-singular fibres, but exactness takes more verification, as one needs to also check all irreducible components of singular fibres of $\mathcal{E}$ are in the image of α. Details are given in [Shi99]. The sequence is exact and $\mathrm{Pic}^0(C) \cong \mathrm{PicVar}_{\mathcal{E}}$. □

Corollary 1.26. *If $\mathcal{E}/\Bbbk$ is the elliptic surface corresponding to the elliptic curve $E/\mathbb{K}$, where the j-invariant of $E/\mathbb{K}$ does not lie in $\Bbbk$, then $PicVar_{\mathcal{E}} \cong Pic^0(\mathbb{P}^1) \cong 0$.*

Let $E/\mathbb{K}$ be a non-isotrivial elliptic curve and let $\mathcal{E}/\Bbbk$ be the corresponding elliptic surface. By the Mordell-Weil theorem, $E(\mathbb{K})$ is a finitely generated Abelian group and is generated by $r = \mathrm{Rank}(E(\mathbb{K}))$ elements plus up to two torsion elements in $E(\mathbb{K})_{\mathrm{tor}}$. Let $s_1, ..., s_r \in E(\mathbb{K})$ be r independent points of infinite order and let t_1, t_2 be generators of $E(\mathbb{K})_{\mathrm{tor}}$ of order r_1 and r_2 such that $r_1, r_2 \geq 1$, $r_2 | r_1$ and $\#(E(\mathbb{K})_{\mathrm{tor}}) = r_1 r_2$. Let S be the set of points $v \in \mathbb{P}^1$ such that E_v is a singular fibre.

Theorem 1.27. [Shi72] *The Néron-Severi group $\mathrm{NS}(\mathcal{E})$ is generated by the following divisors*

E_{u_0}, a non-singular fibre (i.e. $u_0 \notin S$).

$(\mathcal{O})$, the divisor corresponding to the zero section of the elliptic surface $\mathcal{E}$. When $E/\mathbb{K}$ is written in Weierstrass form, the zero section is the curve $([0,1,0],t) \in \mathbb{P}^2 \times \mathbb{P}^1$.

$\Lambda_{v,i}$, where $(1 \leq i \leq n_v - 1, v \in S)$, the divisors corresponding to the irreducible components of the bad fibres of $\mathcal{E}$ which do not intersect $(\mathcal{O})$.

$D^1_\alpha = (s_\alpha) - (\mathcal{O})$, where $(1 \leq \alpha \leq r)$ and,

$D^2_\beta = (t_\beta) - (\mathcal{O})$, where $\beta = 1, 2$

Addtionally, there are at most two fundamental relations between these divi-

sors. For $\beta = 1, 2$,

$$r_\beta D_\beta^2 \sim r_\beta (D_\beta^2 \cdot (\mathcal{O}))E_{u_0} + \sum_v [\Lambda_{v,1} \quad \cdots \quad \Lambda_{v,n_v-1}] r_\beta A_v^{-1} \begin{bmatrix} (D_\beta^2 \cdot \Lambda_{v,1}) \\ \vdots \\ (D_\beta^2 \cdot \Lambda_{v,n_v-1}) \end{bmatrix}$$

where A_v *is the* $(n_v - 1 \times n_v - 1)$ *matrix given by* $[(\Lambda_{v,i} \cdot \Lambda_{v,j})]_{1 \le i,j \le n_v - 1}$.

Note that r_β is a positive integer, A_v is a matrix with integral entries, the dot $\cdot$ represents the intersection number of two divisors and D_β^2, $(\mathcal{O})$ and $\Lambda_{v,i}$ are divisors.

Corollary 1.28. $\mathrm{Rank}(\mathrm{NS}(\mathcal{E})) = \mathrm{Rank}(E(\mathbb{K})) + 2 + \sum_{v \in S}(n_v - 1)$.

This follows directly from theorem 1.27. $\mathrm{NS}(\mathcal{E})$ is generated by $\mathrm{Rank}(E(\mathbb{K}))$ divisors of the form D_α^1, the divisors $(\mathcal{O})$ and E_{u_0}, as well as $\sum_{v \in S}(n_v - 1)$ divisors of the form $\Lambda_{v,i}$.

Lemma 1.29. *[Shi72] Suppose that a divisor* D *on* $\mathcal{E}$ *does not meet the generic fibre. Then*

$$D \sim (D \cdot (\mathcal{O}))E_{u_0} + \sum_v [\Lambda_{v,1} \quad \cdots \quad \Lambda_{v,n_v-1}] A_v^{-1} \begin{bmatrix} (D \cdot \Lambda_{v,1}) \\ \vdots \\ (D \cdot \Lambda_{v,n_v-1}) \end{bmatrix}$$

where A_v *is the* $(n_v - 1 \times n_v - 1)$ *matrix given by* $[(\Lambda_{v,i} \cdot \Lambda_{v,j})]_{1 \le i,j \le n_v - 1}$.

Proof. If D does not meet the generic fibre, then each component of D is contained in a fibre. Let $\Lambda_{v,0}$ denote the irreducible component of the fibre at v with non-zero intersection with $(\mathcal{O})$. Then $D = \sum_v \sum_{i=0}^{n_v-1} \lambda_{v,i}\Lambda_{v,i}$, for some integers $\lambda_{v,i}$. We have

$$\sum_v \lambda_{v,0}\Lambda_{v,0} \sim (D \cdot (\mathcal{O}))E_{u_0}$$

This is by definition of $\Lambda_{v,0}$ and by the fact that all fibral divisors are algebraically equivalent. Also

$$\begin{aligned} D \cdot \Lambda_{v,j} &= \sum_{i=1}^{n_v-1} \lambda_{v,i}\Lambda_{v,i} \cdot \Lambda_{v,j} \\ &= e_j A_v \begin{bmatrix} \lambda_{v,1} \\ \vdots \\ \lambda_{v,n_v-1} \end{bmatrix} \end{aligned}$$

where e_j is the $(1 \times n_v - 1)$ matrix with j^{th} entry 1 and 0s elsewhere. Thus we have

$$\begin{bmatrix} (D \cdot \Lambda_{v,1}) \\ \vdots \\ (D \cdot \Lambda_{v,n_v-1}) \end{bmatrix} = A_v \begin{bmatrix} \lambda_{v,1} \\ \vdots \\ \lambda_{v,n_v-1} \end{bmatrix}$$

So

$$\sum_v [\Lambda_{v,1} \quad \cdots \quad \Lambda_{v,n_v-1}] A_v^{-1} \begin{bmatrix} (D \cdot \Lambda_{v,1}) \\ \vdots \\ (D \cdot \Lambda_{v,n_v-1}) \end{bmatrix} = \sum_v [\Lambda_{v,1} \quad \cdots \quad \Lambda_{v,n_v-1}] \begin{bmatrix} \lambda_{v,1} \\ \vdots \\ \lambda_{v,n_v-1} \end{bmatrix}$$

if A_v is invertible. However, A_v is symmetric and is negative-definite [Sil94, III §8]. Thus A_v has negative eigenvalues and is hence invertible. □

Proof of theorem 1.27. [Shi72] We can now assume without loss of generality that no component of D is contained in a fibre. Let $d = D \cdot E_{u_0}$. Then $D - d(\mathcal{O})$ meets the generic fibre at a divisor $\mathcal{D}$ of degree zero, where $\mathcal{D}$ is considered as a divisor on $E/\mathbb{K}$. We consider the sum $S(\mathcal{D})$ of the components of the divisor $\mathcal{D}$, where the sum is taken using the group law on the elliptic curve $E/\mathbb{K}$. By the group law, we obtain a point $s \in E(\mathbb{K})$. As $E(\mathbb{K})$ is finitely generated, we can express s in the form

$$s = \sum_{\alpha=1}^{r} a_\alpha s_\alpha + b_\beta t_\beta$$

for some integers a_α and b_β. Let

$$D' = \sum_{\alpha=1}^{r} a_\alpha D_\alpha^1 + b_\beta D_\beta^2$$

Then $S(\mathcal{D}) = S(D' \cdot E)$, where $D' \cdot E$ is the intersection of D' with the generic fibre.

Let $P = S(\mathcal{D}) - S(D' \cdot E) = \mathcal{O}$. Then by Abel's theorem,

$$\mathcal{O} = P \mapsto 0 = (P) - (\mathcal{O}) = \mathcal{D} - (\mathcal{O}) - D' \cdot E + (\mathcal{O}) = \mathcal{D} - D' \cdot E$$

and so $\mathcal{D}$ is linearly equivalent to $D' \cdot E$. Therefore, $D - d(\mathcal{O}) - D'$ does not intersect the generic fibre and hence $D - d(\mathcal{O}) - D'$ can be written in the form stated in lemma 1.29. Thus D is linearly equivalent to a combinations of the divisors E_{u_0}, $(\mathcal{O})$, $\Lambda_{v,i}$, D_α^1, D_β^2.

We now show that that there are at most two relations between these divisors. Suppose there is a relation

$$\sum_\alpha a_\alpha D_\alpha^1 + \sum_\beta b_\beta D_\beta^2 + cE_{u_0} + \sum_v \sum_{i \geq 1} d_{v,i} \Lambda_{v,i} + e(\mathcal{O}) \sim 0 \tag{1.1}$$

where $a_\alpha, b_\beta, c, d_{v,i}, e$ are integers.

If the left side of the above equation is algebraically equivalent to 0, then it must be numerically equivalent to 0 and have intersection number 0 with E_{u_0}. Thus $e = 0$. We know from corollary 1.26 that $\mathrm{PicVar}_{\mathcal{E}} \cong \mathrm{Pic}^0(C) \cong 0$, so the left hand side of 1.1 is linearly equivalent to a fibral divisor. Restriction to the generic fibre gives

$$\sum_\alpha a_\alpha D^1_\alpha + \sum b_\beta D^2_\beta \equiv 0$$

By proposition 0.29, $\sum_\alpha a_\alpha s_\alpha + \sum b_\beta t_\beta = 0$. This implies $a_\alpha = 0$ for all α and $b_1, b_2 \equiv 0 \mod 2$. So the left hand side of equation 1.1 is a divisor of the form

$$\sum_\beta b_\beta D^2_\beta + cE_{u_0} + \sum_v \sum_{i\geq 1} d_{v,i}\Lambda_{v,i} \sim 0$$

We now know $-\sum_\beta b_\beta D^2_\beta \sim cE_{u_0} + \sum_v \sum_{i\geq 1} d_{v,i}\Lambda_{v,i}$ and also that the intersection of $b_\beta D^2_\beta$ with the generic fibre is 0. By lemma 1.29, we can write

$$r_\beta D^2_\beta \sim r_\beta (D^2_\beta \cdot (\mathcal{O}))E_{u_0} + \sum_v [\Lambda_{v,1} \quad \cdots \quad \Lambda_{v,n_v-1}] r_\beta A_v^{-1} \begin{bmatrix} (D^2_\beta \cdot \Lambda_{v,1}) \\ \vdots \\ (D^2_\beta \cdot \Lambda_{v,n_v-1}) \end{bmatrix}$$

Lemma 1.29 implies that this is the only relation between divisors, as there is no relation between E_{u_0} and $\Lambda_{v,i}$ for all $1 \leq i \leq n_v - 1$.

Chapter 2

Elliptic Surfaces and Fermat Surfaces

In this chapter, we analyse the elliptic curve $E/\mathbb{K}$ given by the Weierstrass equation

$$E : y^2z + xyz = x^3 - t^dz^3$$

where d is a positive integer. For the elliptic curve E, the discriminant is $\Delta = t^d(1 - 2^43^3t^d)$ and the j-invariant is $j = (t^d(1 - 2^43^3t^d))^{-1}$. As the j-invariant of E does not lie in $\mathbb{F}_q$, E is a non-isotrivial elliptic curve. We associate $E/\mathbb{K}$ to the unique elliptic surface $\mathcal{E}/\Bbbk$ such that $\mathcal{E}$ is non-singular and relatively minimal and such that $\mathcal{E}$ is equipped with a non-constant map $\pi' : \mathcal{E} \to \mathbb{P}^1$.

Considering t as a variable, let $\mathcal{W} \subset \mathbb{P}^2 \times \mathbb{P}^1$ be the Zariski closure of the surface over $\Bbbk$ given by the equation

$$\mathcal{W} : y^2z + xyz = x^3 - t^dz^3.$$

The surface $\mathcal{W}/\Bbbk$ is the Weierstrass model of the elliptic curve $E/\mathbb{K}$. The Weierstrass model is equipped with a non-constant map $\pi : \mathcal{W} \to \mathbb{P}^1$ given by projection onto the t coordinate. The problem with letting $\mathcal{E} = \mathcal{W}$ is that $\mathcal{W}$ has singular points for some values of d. We blow up $\mathcal{W}$ at a 'minimal' number of places and a 'minimal' amount of times to obtain the non-singular and relatively minimal surface $\mathcal{E}$.

We also aim to understand the geometric properties of the elliptic surface $\mathcal{E}/\Bbbk$ associated to $E/\mathbb{K}$. We look at the structure of the singular fibres of $\mathcal{E}$ and count the number of $\Bbbk$-valued points on each type of singular fibre. This will later allow us to evaluate the zeta-functions of the fibres of $\mathcal{E}$. We then relate the elliptic surface $\mathcal{E}$ to a Fermat surface $\mathcal{F}_d$.

2.1 Resolution of Singularities

We consider $\mathcal{W} \subset \mathbb{P}^2 \times \mathbb{P}^1$ as the gluing together of two surfaces U and U' in $\mathbb{P}^2 \times \mathbb{A}^1$. Let

$$U = \{([x, y, z], t) \in \mathbb{P}^2 \times \mathbb{A}^1 \mid y^2z + xyz = x^3 - t^d z^3\}.$$

We analyse the behaviour at $t = \infty$ via a change of coordinates. Let $x = t^{2a}x'$, $y = t^{3a}y'$ and $t = t'^{-1}$, where $d = 6a - b$ and $0 \leq b < 6$. Then let

$$U' = \{([x', y', z'], t') \in \mathbb{P}^2 \times \mathbb{A}^1 \mid y'^2z' + t'^a x'y'z' = x'^3 - t'^b z'^3\}.$$

We glue $U \setminus \{t = 0\}$ to $U' \setminus \{t' = 0\}$ by identifying $([x, y, z], t) \in U \setminus \{t = 0\}$ with $([t'^{-2a}x', t'^{-3a}y', z'], t') \in U' \setminus \{t' = 0\}$ to obtain the Weierstrass model $\mathcal{W} \subset \mathbb{P}^2 \times \mathbb{P}^1$. By blowing up singular points on $\mathcal{W}$, we can find a non-singular surface birationally equivalent to $\mathcal{W}$.

Let $u = y^2z + xyz - x^3 + t^d z^3$ and let $u' = y'^2z' + t'^a x'y'z' - x'^3 + z'^3 t'^b$. Then U is the set of points $([x, y, z], t) \in \mathbb{P}^2 \times \mathbb{A}^1$ such that $u = 0$. Similarly, U' is the set of points $([x', y', z'], t') \in \mathbb{P}^2 \times \mathbb{A}^1$ such that $u' = 0$.

2.1.1 Singularities of U

The partial derivatives of $u = y^2z + xyz - x^3 + t^d z^3$ are

$$\begin{aligned}
\frac{\partial u}{\partial x} &= yz - 3x^2 \\
\frac{\partial u}{\partial y} &= 2yz + xz \\
\frac{\partial u}{\partial z} &= y^2 + xy + 3t^d z^2 \\
\frac{\partial u}{\partial t} &= dt^{d-1} z^3
\end{aligned}$$

Thus u has just one singular point at $([0, 0, 1], 0)$ when $d > 1$. When $d = 1$, then there are no singular points. The surface U has a finite number of singular points, thus we can blow up U a finite number of times to resolve all singularities. The blow-up of U will be birationally equivalent to U. Blowing up U at $([0, 0, 1], 0)$ will not introduce any additional singularities, thus we only need to consider the region of U around $([0, 0, 1], 0)$. As $z \neq 0$ near the singular point, we can dehomogenise u by setting $z = 1$ and write $v = y^2 + xy - x^3 + t^d$, where v is a curve in $\mathbb{A}^3$.

Let U_{x_i} denote the i^{th} blow-up of U in the x_i^{th} affine coordinate chart. Similarly, let U_{y_i} and U_{z_i} denote the i^{th} blow-up in the y_i^{th} and z_i^{th} affine coordinate charts respectively.

Suppose $d > 1$. We blow up v at the origin by associating $(x, y, t) \in \mathbb{A}^3$ with $[x_1, y_1, z_1] \in \mathbb{P}^3$ by the following equations

$$\begin{aligned} xy_1 &= x_1 y \\ xz_1 &= x_1 t \\ yz_1 &= y_1 t \end{aligned}$$

Suppose $x_1 = 1$. Then $y = xy_1$ and $t = xz_1$. Substituting into v and reducing gives the first blow-up in the affine coordinate chart $x_1 = 1$

$$U_{x_1} : y_1^2 + y_1 - x + x^{d-2} z_1^d = 0.$$

By checking partial derivatives, it is evident that the first blow-up in the affine coordinate chart $x_1 = 1$ has no singularities. Similarly, the first blow-up in the affine coordinate chart $y_1 = 1$ is given by

$$U_{y_1} : 1 + x_1 - x_1^3 y + y^{d-2} z_1^d = 0.$$

This also has no singularities. If $z_1 = 1$, then $x = x_1 t$ and $y = y_1 t$ and

$$U_{z_1} : y_1^2 + x_1 y_1 - x_1^3 t + t^{d-2} = 0.$$

The partial derivatives of $v_1 := y_1^2 + x_1 y_1 - x_1^3 t + t^{d-2}$ are

$$\begin{aligned} \frac{\partial v_1}{\partial x_1} &= y_1 - 3x_1^2 t \\ \frac{\partial v_1}{\partial y_1} &= 2y_1 + x_1 \\ \frac{\partial v_1}{\partial t} &= -x_1^3 + (d-2)t^{d-3} \end{aligned}$$

When $d = 2$, then the partial derivatives are all equal to zero at $(x_1, y_1, t) = (0, 0, 0)$, but $(0, 0, 0)$ is not a point on the surface $y_1^2 + x_1 y_1 - x_1^3 t + t^{d-2} = 0$. When $d = 3$, then there are also no singular points. For $d > 3$, there is one singular point at $(x_1, y_1, t) = (0, 0, 0)$.

Assume the i^{th} blow-up in the z_i^{th} coordinate chart U_{z_i} is given by

$$U_{z_i} : y_i^2 + x_i y_i - x_i^3 t^i + t^{d-2i} = 0$$

for $d \geq 2i$. The partial derivatives of $v_i := y_i^2 + x_i y_i - x_i^3 t^i + t^{d-2i}$ are

$$\begin{aligned}\frac{\partial v_i}{\partial x_i} &= y_i - 3x_i^2 t^i \\ \frac{\partial v_i}{\partial y_i} &= 2y_i + x_i \\ \frac{\partial v_i}{\partial t} &= -ix_i^3 t^{i-1} + (d-2i)t^{d-2i-1}\end{aligned}$$

For $d > 2i+1$, there is one singular point at $(x_i, y_i, t) = (0,0,0)$. For $d = 2i$, the partial derivatives are all 0 at $(0,0,0)$, but $(0,0,0)$ is not a point on v_i. For $d = 2i+1$, there are also no singular points. Assume there are no singular points in U_{x_i} and U_{y_i}.

The blow-up of v_i at $(x_i, y_i, t) = (0,0,0)$ is given by making the substitution

$$\begin{aligned}x_i y_{i+1} &= x_{i+1} y_i \\ x_i z_{i+1} &= x_{i+1} t \\ y_i z_{i+1} &= y_{i+1} t\end{aligned}$$

In the coordinate chart $z_{i+1} = 1$, the blow-up is given by the surface

$$v_{i+1} := y_{i+1}^2 + x_{i+1} y_{i+1} - x_{i+1}^3 t^{i+1} + t^{d-2(i+1)}$$

Similarly, this blow-up has one singular point when $d > 2(i+1)+1$ and has no singular points in $U_{x_{i+1}}$ and $U_{y_{i+1}}$. Thus we have shown that the singularity in U can be resolved after $\left\lfloor \frac{d}{2} \right\rfloor$ blow-ups.

Example 2.1. We wish to understand how blowing up points on $\mathcal{W}$ affects the singular fibres of $\mathcal{W}$. We will do this in the next section by using Tate's algorithm. The proof of Tate's algorithm essentially involves understanding the blow-ups of an arbitrary Weierstrass model, so we demonstrate the idea behind Tate's algorithm by looking at the fibre at $t = 0$ on $\mathcal{W}$.

The fibre of $\mathcal{W}$ at $t = 0$ is given by the equation $y^2 z + xyz - x^3 = 0$. This is a nodal cubic curve and is thus a singular fibre. Let i be a positive integer such that $i < \lfloor \frac{d}{2} \rfloor$. In the z_i^{th} affine coordinate chart of the i^{th} blow-up, the fibre at $t = 0$ appears to have 2 irreducible components, as it is given by the equation $y_i^2 + x_i y_i = 0$.

Let $j = \lfloor \frac{d}{2} \rfloor$. In the z_j^{th} affine coordinate chart of the j^{th} blow-up, the fibre at $t = 0$ appears to have 1 or 2 irreducible components, depending on whether d is even (1 irreducible component), or odd (2 irreducible components). If d is even, then $d = 2j$ and in the z_j^{th} affine coordinate chart of the j^{th} blow-up, the fibre at

$t = 0$ is given by $y_i^2 + x_i y_i + 1 = 0$. If d is odd, then $d = 2j + 1$ and in the z_j^{th} affine coordinate chart of the j^{th} blow-up, the fibre at $t = 0$ is given by $y_j^2 + x_j y_j = 0$.

Thus, it seems that each blow-up of $\mathcal{W}$ adds 2 irreducible components to the singular fibre at $t = 0$, and the last necessary blow-up adds 1 component to the singular fibre at $t = 0$ if d is even and 2 components to the singular fibre at $t = 0$ if d is odd. Therefore, it seems that the blow-up of $\mathcal{W}$ adds $d - 1$ components to the singular fibre at $t = 0$ and so the fibre of $\mathcal{E}$ at $t = 0$ should have d components.

This idea clearly takes more verification, as it is necessary to understand how the affine coordinate charts after each blow-up are glued together and how new irreducible components are added to the fibre. However, this is the basic idea behind Tate's algorithm, and using Tate's algorithm we will show that the fibre of $\mathcal{E}$ at $t = 0$ does indeed have d irreducible components.

2.1.2 Singularities of U'

The partial derivatives of $u' = y'^2 z' + t'^a x' y' z' - x'^3 + t'^b z'^3$ are

$$\begin{aligned}
\frac{\partial u'}{\partial x'} &= t'^a y' z' - 3x'^2 \\
\frac{\partial u'}{\partial y'} &= 2y' z' + t'^a x' z' \\
\frac{\partial u'}{\partial z'} &= y'^2 + t'^a x' y' + 3t'^b z'^2 \\
\frac{\partial u'}{\partial t'} &= a t'^{a-1} x' y' z' + b t'^{b-1} z'^3
\end{aligned}$$

For $b \neq 0$, there is just one singular point at $([x', y', z'], t') = ([0, 0, 1], 0)$. We will resolve this singularity in the next section by using Tate's algorithm. Tate's algorithm produces a non-singular and relatively minimal elliptic surface. Moreover, it classifies the possible geometric structures of the fibres of the elliptic surface.

2.2 Tate's Algorithm

On the Weierstrass model $\mathcal{W}$, for all but finitely many $t \in \mathbb{P}^1$, $E_t = \pi^{-1}(t)$ is a non-singular fibre. We say that the elliptic curve $E/\mathbb{K}$ has *bad reduction* at points t such that E_t is a singular fibre and has *good reduction* at points t such that E_t is a non-singular fibre. Note that $E/\mathbb{K}$ has bad reduction at points t such that the discriminant of E is 0 and possibly at $t = \infty$. As $\Delta = t^d(1 - 2^4 3^3 t^d)$, the points of bad reduction are at $t = 0$, roots of $(1 - 2^4 3^3 t^d)$ and possibly at $t = \infty$.

The blow-up of $\mathcal{W}$ does not affect the fibres at points of good reduction, but may change the fibres at points of bad reduction. A *special fibre* of $\mathcal{E}$ is a fibre of $\mathcal{E}$ at a place $t \in \mathbb{P}^1$. For example, at a point t with good reduction, the special fibre of $\mathcal{E}$ consists of one irreducible curve (an elliptic curve). We use the term 'special fibre' out of tradition and use the term synonymously with 'fibre', although 'special fibre' has a scheme-theoretic interpretation.

Kodaira and Néron classify the possible types of special fibres of a elliptic surface. We identify the possible types of special fibres of the elliptic surface $\mathcal{E}$ associated to $E : y^2z + xyz = x^3 - t^dz^3$ by using Tate's algorithm. A detailed description of Tate's algorithm and the classification of special fibres is given in [Tat75] and [Sil94]. After applying Tate's algorithm, we will be able to understand the geometric properties of the elliptic surface $\mathcal{E}$.

For the elliptic curve $E : y^2z + xyz = x^3 - t^dz^3$, the constants a_i and b_j for $i = 1, 2, 3, 4, 6$ and $j = 2, 6, 8$ defined in section 0.2 are

$$a_1 = 1, \quad a_2 = a_3 = a_4 = 0, \quad a_6 = -t^d, \quad b_2 = 1, \quad b_6 = -4t^d, \quad b_8 = -t^d.$$

Let π be a uniformiser at a place t. Let $v(\Delta)$ be the valuation of Δ with respect to the uniformiser π. We denote the number of irreducible components of the special fibre defined over $\Bbbk$ by n and the number of components of the special fibre defined over $\Bbbk$ of multiplicity 1 by c. Note that throughout this paper, we consider the number of irreducible components of the special fibre defined over $\Bbbk$ to be the number of Galois orbits of roots of the defining polynomial of the special fibre.

The elliptic curve $E/\mathbb{K}$ has *split reduction* at a place t if the number of irreducible components of the special fibre at t defined over $\overline{\Bbbk}$ is the same as n, the number of irreducible components of the special fibre defined over $\Bbbk$, and has *non-split reduction* otherwise. $E/\mathbb{K}$ has *multiplicative reduction* at t if the fibre E_t on the Weierstrass model $\mathcal{W}$ is a nodal cubic and has *additive reduction* at t if the fibre E_t on the Weierstrass model $\mathcal{W}$ is a cuspidal cubic. The fibre E_0 on $\mathcal{W}$ is given by the equation $y^2z + xyz = x^3$, which is a nodal cubic, so $E/\mathbb{K}$ has multiplicative reduction at 0. When $b \neq 0$, the fibre E_∞ is a cuspidal cubic given by the equation $y'^2z' = x'^3$, so E_∞ has additive reduction at ∞ when $b \neq 0$.

Definition 2.2. [Sil94, Ex.3.36] The *conductor divisor* of an elliptic curve E is an effective divisor on $\mathbb{P}^1$ given by $\mathcal{F}_{E/K} = \sum_{t\in\mathbb{P}^1} f_t(t) \in \mathrm{Div}(\mathbb{P}^1)$. The *conductor*

f_t is given by:

$$f_t = \begin{cases} 0, & \text{if } E_t \text{ is non-singular (has good reduction)} \\ 1, & \text{if } E_t \text{ has a node (has multiplicative reduction)} \\ 2, & \text{if } E_t \text{ has a cusp (has additive reduction)} \end{cases}$$

For all $t \in \mathbb{P}^1$, we find c and n, as well as the reduction type of the special fibres of $E/\mathbb{K}$ at t. We follow Tate's algorithm as given in [Sil94, IV §9].

Case 1: $\pi \nmid \Delta$

If $\pi \nmid \Delta$, then E has reduction type I_0 (good reduction) at t. Also, $n = 1$ and $c = 1$.

Case 2: $\pi | t^d$

Suppose $\pi | t^d$ and hence $\pi | \Delta$. We can assume without loss of generality that $\pi = t$. The fibre at $t = 0$ has a singular point at $(x, y) = (0, 0)$. As $\pi \nmid b_2 = 1$ and $v(\Delta) = d$, the special fibre at $t = 0$ is of type I_d. Over a field of characteristic not equal to 2, the polynomial $T^2 + a_1T - a_2 = T^2 + T$ splits. Thus $n = d$ and $c = d$ and the special fibre at $t = 0$ has split multiplicative reduction.

The special fibre consists of d non-singular curves (copies of $\mathbb{P}^1$) defined over $\Bbbk$ arranged in a d-gon. If $d = 1$, then the special fibre is a curve defined over $\Bbbk$ with a node.

Case 3: $\pi | (1 - 2^4 3^3 t^d)$

Suppose $\pi | (1 - 2^4 3^3 t^d)$. We have $\pi \nmid b_2 = 1$ and $v(\Delta) = 1$, so E has reduction type I_1. Consider the polynomial $T^2 + a_1T - a_2 = T^2 + T$. Over a field of characteristic not equal to 2, this polynomial splits. Thus $n = 1$ and $c = 1$ and the special fibre has split multiplicative reduction.

The special fibre is a curve defined over $\Bbbk$ with a node.

Case 4: $t = \infty$

Suppose $t = \infty$. We apply a change of coordinates to identify the possible reduction types at $t = \infty$. Let $t = t'^{-1}$, $x = t^{2a}x'$ and $y = t^{3a}y'$, where $a, b \in \mathbb{Z}$ and $d = 6a - b > 0$. We apply Tate's algorithm to the elliptic curve

$$y'^2z' + t'^a x'y'z' = x'^3 - t'^b z'^3 \tag{2.1}$$

For this elliptic curve,

$$a_1 = t'^a, \quad a_2 = a_3 = a_4 = 0, \quad a_6 = -t'^b, \quad b_2 = t'^{2a}, \quad b_6 = -4t'^b, \quad b_8 = -t'^{2a+b}.$$

The discriminant $\Delta = t'^{6a+b} - 2^4 3^3 t'^{2b}$. If the following conditions hold for a uniformiser π, then the original Weierstrass equation is not minimal

$$\pi|\Delta, \quad \pi|a_1 = t'^a, \quad \pi^2|a_2 = 0, \quad \pi^3|a_3 = 0, \quad \pi^4|a_4 = 0, \quad \pi^6|a_6 = -t'^b$$

$$\pi|b_2 = t'^{2a}, \quad \pi^3|b_6 = -4t'^b, \quad \pi^3|b_8 = -t'^{2a+b}.$$

These conditions hold for $a \geq 1$, $b \geq 6$ and $\pi = t'$. Without loss of generality, we can thus choose $a \geq 1$ and $0 \leq b < 6$, and write $d = 6a - b$.

Case 4a: $b = 0$

Suppose $b = 0$. Equation 2.1 has no singular points. Thus for $b = 0$, E has good reduction (type I_0) at $t = \infty$. Also, $c = 1$ and $n = 1$.

Case 4b: $b = 1$

Suppose $b = 1$. Then for $\pi = t'$, we have $t' = \pi|\Delta$, $\pi|a_6 = -t'$ and $\pi|b_2 = t'^{2a}$, but $\pi^2 \nmid a_6 = -t'$, thus at $t = \infty$ and for $b = 1$, the special fibre is type II, where $n = 1$ and $c = 1$. The special fibre has split additive reduction and is a cuspidal cubic defined over $\Bbbk$.

Case 4c: $b = 2$

Suppose $b = 2$. The following relations hold for $\pi = t'$

$$\pi|\Delta, \quad \pi|b_2 = t'^{2a}, \quad \pi^2|a_6 = -t'^2, \quad \pi^3|b_8 = -t'^{2a+2}.$$

However, $\pi^3 \nmid b_6 = -4t'^2$. By Tate's algorithm, the reduction type is IV. Consider the polynomial $F(T) = T^2 + \pi^{-2}t'^2 = T^2 + 1$. Let $\Bbbk'$ be the splitting field of this polynomial over $\Bbbk$. If $\Bbbk$ contains μ_4, then $\Bbbk' = \Bbbk$ and $c = 3$. If not, then $\Bbbk \subset \Bbbk'$ and $c = 1$. Thus the special fibre has split additive reduction when $\mu_4 \subset \Bbbk$ and non-split additive reduction otherwise.

The special fibre is given by an equation of the form

$$(Y^2 + Z^2)Z = 0$$

so has 2 components defined over $\Bbbk$ ($n = 2$) when $\mu_4 \notin \Bbbk$ and 3 components defined over $\Bbbk$ ($n = 3$) when $\mu_4 \subset \Bbbk$.

Case 4d: $b = 3$

Suppose $b = 3$. The following relations hold for $\pi = t'$

$$\pi|\Delta, \quad \pi|b_2 = t'^{2a}, \quad \pi^2|a_6 = -t'^3, \quad \pi^3|b_8 = -t'^{2a+3},$$

$$\pi^3|b_6 = -4t'^3, \quad \pi|a_1 = t'^a, \quad \pi^3|a_6 = -t'^3.$$

Consider the polynomial $F(T) = T^3 - \pi^{-3}t'^3 = T^3 - 1$. $F(T)$ splits into either 2 or 3 irreducible components when $\Bbbk$ is not a field of characteristic 2 or 3, so E has reduction type I_0^* at $t = \infty$ and $c = 1 + \#\{\alpha \in \Bbbk \mid F(\alpha) = 0\}$. Thus $c = 2$ if $\mu_3 \notin \Bbbk$ and $c = 4$ if $\mu_3 \subset \Bbbk$. The special fibre at $t = \infty$ has split additive reduction when $\mu_3 \subset \Bbbk$ and non-split additive reduction otherwise.

The special fibre consists of up to four lines of multiplicity 1 intersecting a line of multiplicity 2 ($Y^2 = 0$). One of the lines of multiplicity 1 is given by an equation of the form $Z = 0$ and the other lines of multiplicity 1 correspond to the roots of the equation $T^3 + 1 = 0$. Thus the number of components of the special fibre defined over $\Bbbk$ is 4 when $\mu_3 \notin \Bbbk$ and is 5 when $\mu_3 \subset \Bbbk$.

Case 4e: $b = 4$

Suppose $b = 4$. The following relations hold for $\pi = t'$

$$\pi|\Delta, \quad \pi|b_2 = t'^{2a}, \quad \pi^2|a_6 = -t'^4, \quad \pi^3|b_8 = -t'^{2a+4},$$

$$\pi^3|b_6 = -4t'^4, \quad \pi|a_1 = t'^a, \quad \pi^3|a_6 = -t'^4.$$

Consider the polynomial $F(T) = T^3 - \pi^{-3}t'^4 = T^3 - \pi$. Modulo π, this polynomial has a triple root at $T = 0$. Also $\pi^4|a_6 = -t'^4$. Thus the special fibre is of type IV^*. Consider the polynomial $F(T) = T^2 + \pi^{-4}t'^4 = T^2 + 1$. Let $\Bbbk'$ be the splitting field of this polynomial. Then $c = 3$ if $\Bbbk' = \Bbbk$, otherwise $c = 1$. Thus the special fibre has split additive reduction when $\mu_4 \subset \Bbbk$ and non-split additive reduction otherwise.

The special fibre contains a line given by an equation of the form $Z = 0$, a line given by an equation of the form $Y^2 = 0$ and a line of the form $X^3 = 0$. There are 2 additional singular points on the special fibre, whose blow-ups each add 1 or 2 additional components defined over $\Bbbk$ to the special fibre, depending on whether or not $\mu_4 \subset \Bbbk$. If $\mu_4 \subset \Bbbk$, then $n = 7$, and if $\mu_4 \notin \Bbbk$, then $n = 5$.

Case 4f: $b = 5$

Suppose $b = 5$. Similar to $b = 4$, the following relations hold for $\pi = t'$

$$\pi|\Delta, \quad \pi|b_2 = t'^{2a}, \quad \pi^2|a_6 = -t'^5,$$

$$\pi^3|b_8 = -t'^{2a+5}, \quad \pi^3|b_6 = -4t'^5, \quad \pi|a_1 = t'^a, \pi^3|a_6 = -t'^5.$$

The polynomial $F(T) = T^3 - \pi^{-3}t'^5 = T^3 - \pi^2$ has a triple root modulo π at $T = 0$. Also $\pi^4|a_6 = -t'^5$. Consider the polynomial $F(T) = T^2 + \pi^{-4}t'^5 = T^2 + \pi = 0$. This polynomial has a double root modulo π at $T = 0$. We have $\pi^5|a_6 = -t'^5$ and $\pi^4|a_4 = 0$, however $\pi^6 \nmid a_6 = -t'^5$. Thus the special fibre is of type II^*, where $n = 9$ and $c = 1$, and E has split additive reduction at $t = \infty$. The special fibre consists of 9 curves defined over $\Bbbk$.

2.2.1 The Special Fibres of $\mathcal{E}$

By Tate's algorithm, we can construct a non-singular and relatively minimal surface $\mathcal{E}$ by resolving the singularities in $\mathcal{W}$ such that $\mathcal{E}$ is birationally equivalent to $\mathcal{W}$. The projection map $\pi : \mathcal{W} \to \mathbb{P}^1$ induces a non-constant map $\pi' : \mathcal{E} \to \mathbb{P}^1$. Therefore, $\mathcal{E}$ is the unique elliptic surface corresponding to $E/\mathbb{K}$. The fibres of $\mathcal{E}$ have the reduction types given in the table below. Blank entries of the table correspond to no restrictions on b or on $\Bbbk = \mathbb{F}_q$, aside from the ongoing assumption that $\Bbbk$ is not characteristic 2 or 3. Recall c is the number of components of the special fibre of multiplicity 1 defined over $\Bbbk$ and n is the number of irreducible components of the special fibre defined over $\Bbbk$. We also write π for a uniformiser at a place t and note the conductor of each special fibre.

Reduction Type	Fibre (E_t)	b	$\Bbbk$ such that	c	n	f_t
I	E_t, for $\pi \nmid \Delta$			1	1	0
I	E_∞	0		1	1	0
I_1	E_t, for $\pi \mid (1 - 2^4 3^3 t^d)$			1	1	1
I_d (split)	E_0			d	d	1
II	E_∞	1		1	1	2
IV (split)	E_∞	2	$\mu_4 \subset \Bbbk$	3	3	2
IV (non-split)	E_∞	2	$\mu_4 \notin \Bbbk$	1	2	2
I_0^* (split)	E_∞	3	$\mu_3 \subset \Bbbk$	4	5	2
I_0^* (non-split)	E_∞	3	$\mu_3 \notin \Bbbk$	2	4	2
II^*	E_∞	5		1	9	2
IV^* (split)	E_∞	4	$\mu_4 \subset \Bbbk$	3	7	2
IV^* (non-split)	E_∞	4	$\mu_4 \notin \Bbbk$	1	5	2

On $\mathcal{W}$, the singular fibres are nodal or cuspidal cubic curves and consist of one component defined over $\Bbbk$. On $\mathcal{E}$, the properties of the singular fibres are given by Tate's algorithm. The blow-up of $\mathcal{W}$ does not affect the non-singular fibres of $\mathcal{W}$. Blowing up $\mathcal{W}$ involves deleting singular points and adding curves. If n_v is the number of irreducible components on a singular fibre E_v of $\mathcal{E}$, then the blow-up of $\mathcal{W}$ must add $n_v - 1$ irreducible components to the singular fibre.

2.2.2 Counting Points on the Special Fibres

We count the number of $\Bbbk_i = \mathbb{F}_{q^i}$ valued points on each special fibre in preparation for understanding the L-function of $E/\mathbb{K}$. Let $\mathcal{V}$ denote a special fibre and let $\#(\mathcal{V}(\mathbb{F}_{q^i}))$ denote the number of $\mathbb{F}_{q^i}$-valued points on $\mathcal{V}$.

For all the split additive reduction types,

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = nq^i + 1$$

where n is the number of components of the special fibre defined over $\Bbbk$. This is due to the special fibre consisting of n components, each with $q^i + 1$ non-singular

points, however the fibres intersect $n-1$ times, so $\#(\mathcal{V}(\mathbb{F}_{q^i})) = nq^i + n - (n-1) = nq^i + 1$.

For reduction type I_d where $d \geq 2$, the special fibre consists of d copies of $\mathbb{P}^1$ arranged in a d-gon. Thus there are $q^i + 1$ non-singular points on each copy of $\mathbb{P}^1$ minus d intersection points. So

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = dq^i.$$

In particular, if $d = 1$, the special fibre consists of a curve with a nodal singular point. Thus

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = q^i.$$

It now remains to understand the non-split additive reduction types.

Type IV, non-split additive reduction

The special fibre is given by an equation of the form

$$(Y^2 + Z^2)Z = 0$$

and consists of 1 or 3 components containing $\mathbb{F}_{q^i}$ valued points, depending on whether or not $\mu_4 \subset \mathbb{F}_{q^i}$. If $q \equiv 1 \mod 4$, then $\mu_4 \subset \mathbb{F}_{q^i}$, and so the special fibre has split reduction. Otherwise, if $q \equiv 3 \mod 4$, then $\mu_4 \subset \mathbb{F}_{q^i}$ when i is even and $\mu_4 \not\subset \mathbb{F}_{q^i}$ when i is odd. Thus

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = 2q^i + (-1)^i q^i + 1.$$

Type I_0^*, non-split additive reduction

The special fibre consists of 3 or 5 components containing $\mathbb{F}_{q^i}$ valued points, depending on whether or not $\mu_3 \subset \mathbb{F}_{q^i}$. As q is not of characteristic 3, $q \equiv 1 \mod 3$ or $q \equiv 2 \mod 3$. If $q \equiv 1 \mod 3$, then $\mu_3 \subset \Bbbk$ and so the special fibre has split reduction. Assume $q \equiv 2 \mod 3$. Then when i is even, the special fibre splits over $\mathbb{F}_{q^i}$ and consists of 5 components containing $\mathbb{F}_{q^i}$-valued points. When i is odd, the special fibre consists of 3 components containing $\mathbb{F}_{q^i}$-valued points. Thus

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = 4q^i + (-1)^i q^i + 1.$$

Type IV^*, non-split additive reduction

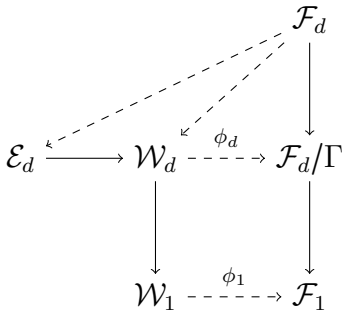
The special fibre consists of 3 or 7 components containing $\mathbb{F}_{q^i}$ valued points, depending on whether or not $\mu_4 \subset \mathbb{F}_{q^i}$. If $q \equiv 1 \mod 4$, then $\mu_4 \subset \mathbb{F}_{q^i}$, and so the special fibre has split reduction. Otherwise, if $q \equiv 3 \mod 4$, then $\mu_4 \subset \mathbb{F}_{q^i}$ when i is even and $\mu_4 \notin \mathbb{F}_{q^i}$ when i is odd. Thus

$$\#(\mathcal{V}(\mathbb{F}_{q^i})) = 5q^i + (-1)^i 2q^i + 1.$$

A summary of the number of $\mathbb{F}_{q^i}$-valued points on each special fibre is given in section 3.2.3 when we evaluate the zeta-function of $\mathcal{E}$.

2.3 Fermat Surfaces

The aim of this section is to relate the Weierstrass model $\mathcal{W}$ of the elliptic curve E to a Fermat surface over $\Bbbk$. We will explain the following diagram and show that it commutes.



(2.2)

Let $\mathcal{W}_d$ be the Weierstrass model of the elliptic curve $E/\mathbb{K}$ and let $\mathcal{W}_1$ be the Weierstrass model of E when $d = 1$. We know there exists a birational map $\mathcal{E}_d \to \mathcal{W}_d$ resulting from the blow-up of $\mathcal{W}_d$.

Definition 2.3. A *Fermat surface* $\mathcal{F}_d$ of degree $d \geq 1$ is a hypersurface in $\mathbb{P}^3$ defined by the equation

$$x_0^d + x_1^d + x_2^d + x_3^d = 0$$

We consider the Fermat surface to be defined over the field $\Bbbk$. The Fermat surface is non-singular and there exists a surjective morphism of degree d^3 from $\mathcal{F}_d$ to $\mathcal{F}_1$ given by $[x_0, x_1, x_2, x_3] \mapsto [x_0^d, x_1^d, x_2^d, x_3^d]$.

Let H be the group of automorphisms of the Fermat surface $\mathcal{F}_d/\Bbbk$ given by

$$H = \{[\zeta_i, \zeta_j, \zeta_k, \zeta_l] \in \mu_d^4 \subset \overline{\Bbbk}\}$$

where the ζs are d^{th} roots of unity in $\overline{\mathbb{k}}$ and the group action is coordinate-wise multiplication. Elements of H act on points $[x_0, x_1, x_2, x_3]$ on the Fermat surface $\mathcal{F}_d$ by coordinate-wise multiplication. Let $\text{Diag} \subset H$ be the group of trivial automorphisms of the Fermat surface $\mathcal{F}_d$ given by

$$\text{Diag} = \{[\zeta, \zeta, \zeta, \zeta] \in \mu_d^4 \subset \overline{\mathbb{k}}\} \subset H.$$

Let $G = H/\text{Diag}$. Note that $\mathcal{F}_d/G \cong \mathcal{F}_1$. Let Γ be the subgroup of G given by

$$\Gamma = \{[\zeta_0, \zeta_1, \zeta_2, \zeta_3] \in G \mid \zeta_0^3\zeta_1^{-6}\zeta_2^2\zeta_3 = 1\}.$$

As $\Gamma \subset G$, the map $\mathcal{F}_d \to \mathcal{F}_1$ factors through $\mathcal{F}_d/\Gamma$. We also have a morphism $\mathcal{W}_d \to \mathcal{W}_1$ given by $([x, y, z], t) \mapsto ([x, y, z], t^d)$. This map has degree d.

Let $\mathcal{W}_d \dashrightarrow \mathcal{F}_1$ be the dominant rational map defined by

$$([x, y, z], t) \mapsto [y^2z, xyz, -x^3, z^3t^d].$$

This map factors through $\mathcal{W}_1$ and the map $\phi_1 : \mathcal{W}_1 \dashrightarrow \mathcal{F}_1$ is given by

$$([x, y, z], t) \mapsto [y^2z, xyz, -x^3, z^3t].$$

This is a birational map with inverse $\mathcal{F}_1 \dashrightarrow \mathcal{W}_1$ given by

$$[x_0, x_1, x_2, x_3] \mapsto \left([x_0x_1x_2, x_0^2x_2, -x_1^3], \frac{x_0x_2^2x^3}{x_1^6}\right)$$

Thus the degree of the map $\mathcal{W}_d \dashrightarrow \mathcal{F}_1$ is the same as the degree of the map $\mathcal{W}_d \to \mathcal{W}_1$ and so has degree d.

Let $\mathcal{F}_d \dashrightarrow \mathcal{W}_d$ be the dominant rational map defined by

$$[x_0, x_1, x_2, x_3] \mapsto \left([(x_0x_1x_2)^d, (x_0^2x_2)^d, -x_1^3d], \frac{x_0^3x_2^2x_3}{x_1^6}\right).$$

This map also factors through $\mathcal{F}_d/\Gamma$.

Applying the map $\mathcal{F}_d \dashrightarrow \mathcal{W}_d$ followed by the map $\mathcal{W}_d \dashrightarrow \mathcal{F}_1$ is just the morphism $\mathcal{F}_d \to \mathcal{F}_1$. The map $\mathcal{F}_d \to \mathcal{F}_1$ has degree d^3, so the map $\mathcal{F}_d \dashrightarrow \mathcal{W}_d$ has degree d^2. The map $\mathcal{F}_d \to \mathcal{F}_d/\Gamma$ is of degree d^2, as Γ contains d^2 elements. Therefore, the map $\phi_d : \mathcal{W}_d \to \mathcal{F}_d/\Gamma$ is a birational map. We further investigate this map in section 2.3.1.

The surface $\mathcal{W}_d$ is normal by the Serre criterion, as it only contains finitely many singular points (regular in codimension 1) and is locally a hypersurface in $\mathbb{A}^3$ (see [Har77, II 8.23]). The Fermat surface $\mathcal{F}_d$ is also normal by the Serre criterion, as it is a non-singular hypersurface. The quotient $\mathcal{F}_d/\Gamma$ is normal as $\mathcal{F}_d$ is normal.

Summary

We provide a description of diagram 2.2 here for quick reference.

$\mathcal{W}_d$ is the Weierstrass model of the elliptic curve $E/\mathbb{K}$ and $\mathcal{W}_1$ is the Weierstrass model of E when $d = 1$. $\mathcal{F}_d$ is the Fermat surface of degree d, and $\mathcal{F}_1$ is the Fermat surface of degree 1. Γ is a group of automorphisms of points in $\mathcal{F}_d$ by multiplication by d^{th} roots of unity.

$\mathcal{W}_d$ and $\mathcal{F}_d/\Gamma$ are normal.

The horizontal arrows are birational maps, the diagonal arrows are dominant rational maps and the vertical arrows are finite surjective morphisms.

$\mathcal{E}_d \to \mathcal{W}_d$ is the birational map resulting from the blow-up of $\mathcal{W}_d$.

$\mathcal{F}_d \to \mathcal{F}_1$ is given by $[x_0, x_1, x_2, x_3] \mapsto [x_0^d, x_1^d, x_2^d, x_3^d]$ and factors through $\mathcal{F}_d/\Gamma$.

$\mathcal{W}_d \to \mathcal{W}_1$ is given by $([x, y, z], t) \mapsto ([x, y, z], t^d)$.

$\mathcal{F}_d \dashrightarrow \mathcal{W}_d$ is given by $[x_0, x_1, x_2, x_3] \mapsto \left([(x_0x_1x_2)^d, (x_0^2x_2)^d, -x_1^3 d], \frac{x_0^3x_2^2x_3}{x_1^6}\right)$ and factors through $\mathcal{F}_d/\Gamma$. There exists an inverse map $\mathcal{W}_d \dashrightarrow \mathcal{F}_d/\Gamma$.

$\mathcal{W}_1 \dashrightarrow \mathcal{F}_1$ is given by $([x, y, z], t) \mapsto [y^2z, xyz, -x^3, z^3t^d]$.

2.3.1 An Isomorphism

Ulmer proves the following lemma, which is then used to find an isomorphism between a subset of $\mathcal{W}_d$ and the quotient of a Fermat surface $\mathcal{F}_d/\Gamma$.

Lemma 2.4. [Ulm02] *Let W, X, Y and Z be varieties over k and assume that X is normal. Let $g : X \dashrightarrow Y$ be a rational map, let $f : W \to X$ be a finite surjective morphism and let $h : Y \to Z$ be a finite morphism. Then*

1. *$g \circ f$ is defined at $w \in W$ if and only if g is defined at $f(w)$.*
2. *g is defined at $x \in X$ if and only if $h \circ g$ is defined at x.*

Corollary 2.5. [Ulm02] *Consider the following commutative diagram of varieties:*

$$\begin{array}{ccc} \tilde{X} & \overset{\tilde{\phi}}{\dashrightarrow} & \tilde{Y} \\ \downarrow{\scriptstyle \pi_X} & & \downarrow{\scriptstyle \pi_Y} \\ X & \overset{\phi}{\dashrightarrow} & Y \end{array}$$

where π_X and π_Y are finite surjective morphisms, $\tilde{\phi}$ and ϕ are dominant rational maps and $\tilde{X}$ and $\tilde{Y}$ are normal. Then if $V \subset X$ and $V' \subset Y$ are open subsets and the induced map ϕ on V is an isomorphism $\phi : V \to V'$, then $\tilde{\phi}$ induces an isomorphism from $\tilde{V} = \pi_X^{-1}(V)$ to $\tilde{V'} = \pi_Y^{-1}(V')$.

Proof. By part 1 of the lemma, $\phi \circ \pi_X$ is defined on $\tilde{V}$ if and only if ϕ is defined on $\pi_X(\tilde{V})$. As $\pi_X(\tilde{V}) = V$ and ϕ is defined on the open subset $V \subset X$, $\phi \circ \pi_X$ is defined on $\tilde{V}$.

By part 2 of the lemma, $\pi_Y \circ \tilde{\phi}$ is defined on $\tilde{V}$ if and only if $\tilde{\phi}$ is defined on $\tilde{V}$. By commutativity of the diagram, $\pi_Y \circ \tilde{\phi} = \phi \circ \pi_X$, so $\tilde{\phi}$ is defined on $\tilde{V}$.

By the surjectivity of π_X and π_Y, $\tilde{\phi}(\tilde{V}) \subset \tilde{V}'$ and $\tilde{\phi}(\tilde{V}')^{-1} \subset \tilde{V}$. By the commutativity of the diagram, $\tilde{\phi}^{-1} \circ \tilde{\phi}$ is the identity map on $\tilde{V}$ and $\tilde{\phi} \circ \tilde{\phi}^{-1}$ is the identity map on $\tilde{V}'$. Thus $\tilde{\phi}$ induces an isomorphism from $\tilde{V}$ to $\tilde{V}'$. □

We apply this lemma to the commutative diagram in equation 2.2.

$$\begin{array}{ccc} \mathcal{W}_d & \overset{\phi_d}{\dashrightarrow} & \mathcal{F}_d/\Gamma \\ \downarrow & & \downarrow \\ \mathcal{W}_1 & \overset{\phi_1}{\dashrightarrow} & F_1 \end{array}$$

The surfaces $\mathcal{W}_d$ and $\mathcal{F}_d/\Gamma$ are normal, ϕ_d and ϕ_1 are dominant rational maps and the maps $\mathcal{W}_d \to \mathcal{W}_1$ and $\mathcal{F}_d/\Gamma \to \mathcal{F}_1$ are finite surjective morphisms. Thus this diagram satisfies the conditions of corollary 2.5.

Let $V \subset \mathcal{W}_1$ be the subset of $\mathcal{W}_1$ such that $t \neq \infty$ and $xyz \neq 0$. Let $V' \subset \mathcal{F}_1$ be the subset of $\mathcal{F}_1$ such that $x_0x_1x_2 \neq 0$.

$$\phi_1([x,y,z],t) = [y^2z, xyz, -x^3, z^3t]$$

$$\phi_1^{-1}([x_0,x_1,x_2,x_3]) = \left([x_0x_1x_2, x_0^2x_2, -x_1^3], \frac{x_0^3x_2^2x_3}{x_1^6}\right)$$

Thus $\phi_1 : V \to V'$ is an isomorphism.

By corollary 2.5, ϕ_d induces an isomorphism from a subset $\tilde{V}$ of $\mathcal{W}_d$ to a subset $\tilde{V}'$ of $\mathcal{F}_d/\Gamma$. The subset $\tilde{V} \subset \mathcal{W}_d$ is obtained from $\mathcal{W}_d$ by removing the subset of $\mathcal{W}_d$ where $t = \infty$, as well as the subset of $\mathcal{W}_d$ where $xyz = 0$. The subset $\tilde{V}' \subset \mathcal{F}_d/\Gamma$ is obtained by removing the subset of $\mathcal{F}_d/\Gamma$ where $x_0x_1x_2 = 0$. We know $\mathcal{F}_d \setminus V(x_0x_1x_2)$ corresponds to removing the following 3 Fermat curves from $\mathcal{F}_d$:

$$x_1^d + x_2^d + x_3^d = 0$$
$$x_0^d + x_2^d + x_3^d = 0$$
$$x_0^d + x_1^d + x_3^d = 0$$

The image of these three Fermat curves under the map $\mathcal{F}_d \to \mathcal{F}_d/\Gamma$ also consists of three irreducible curves in $\mathcal{F}_d/\Gamma$. Thus $\tilde{V}'$ is obtained by removing 3 irreducible curves from $\mathcal{F}_d/\Gamma$.

Let $u = y^2z + xyz - x^3 + t^dz^3$ and $u' = y'^2z' + t'^ax'y'z' - x'^3 + z'^3t'^b$. To obtain $\tilde{V}$, we must remove the following subvarieties from $\mathcal{W}_d$:

1. $V(y'^2z' - x'^3, t')$, the subset of $\mathcal{W}_d$ where $t = \infty$ (or $t' = 0$). This consists of one irreducible curve.

2. $V(y^2z + t^dz^3, x)$, the subset of $\mathcal{W}_d$ where $x = 0$ and $t \neq \infty$. This algebraic set can be factored into 2 or 3 irreducible varieties, $V(z)$ and the irreducible components of $V(y^2 + t^dz^2, x)$. If d is odd or $\mu_4 \notin k$, then $V(y^2 + z^2t^d, x)$ is irreducible. If d is even and $\mu_4 \in k$, then $V(y^2 + z^2t^d, x)$ can be factored into two irreducible components, $V(y + izt^{\frac{d}{2}}, x)$ and $V(y - izt^{\frac{d}{2}}, x)$. Note that $V(x^3, z)$, the subset of $\mathcal{W}_d$ where $z = 0$, is a subset of $V(y^2z + t^dz^3, x)$, the subset of $\mathcal{W}_d$ where $x = 0$.

3. $V(x^3 - t^dz^3, y)$, the subset of $\mathcal{W}_d$ where $y = 0$ and $t \neq \infty$. This is irreducible if $3 \nmid d$. If $3|d$ and $\mu_3 \notin k$, then this splits into two irreducible components, $V(x - t^{\frac{d}{3}}z, y)$ and $V(x^2 + xt^{\frac{d}{3}}z + t^{\frac{2d}{3}}z^2, y)$. If $3|d$ and $\mu_3 \subset k$, then $V(x^3 - t^dz^3, y)$ splits into 3 irreducible components.

Thus, $\tilde{V}$ is obtained from $\mathcal{W}_d$ by removing a union of curves. The number of irreducible curves in this union is given by:

$$\alpha = 1 + \begin{cases} 2 & \text{if } 2 \nmid d \text{ or } \mu_4 \notin k \\ 3 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 1 & \text{if } 3 \nmid d \\ 2 & \text{if } 3|d \text{ and } \mu_3 \notin k \\ 3 & \text{if } 3|d \text{ and } \mu_3 \subset k \end{cases}$$

The Weierstrass model $\mathcal{W}_d$ minus α irreducible curves is isomorphic to $\mathcal{F}_d/\Gamma$ minus 3 irreducible curves. We will later use this information to compare the zeta-function of $\mathcal{W}_d$ to the zeta-function of $\mathcal{F}_d/\Gamma$. We also know that the elliptic surface $\mathcal{E}$ is obtained from $\mathcal{W}_d$ by adding $\sum_v n_v - 1$ irreducible curves, where n_v is the number of irreducible components in each fibre E_v of $\mathcal{E}$.

Chapter 3

Enter Zeta-Functions

3.1 Zeta-Functions

We provide three expressions of zeta-functions and show that they are equivalent.

Definition 3.1. The *zeta-function* of a variety X over $\mathbb{F}_q$ is given by

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} \frac{(\#X(\mathbb{F}_{q^n}))T^n}{n}\right)$$

where $\#X(\mathbb{F}_{q^n})$ is the number of points in $X(\mathbb{F}_{q^n})$.

Example 3.2. We compute the zeta-function of $\mathbb{P}^1$, considered over the field $\mathbb{F}_q$. The number of $\mathbb{F}_{q^i}$-valued points on $\mathbb{P}^1$ is $q^i + 1$.

$$\begin{aligned} Z(\mathbb{P}^1,T) &= \exp\left(\sum_{i=1}^{\infty} \frac{(q^i+1)T^i}{i}\right) \\ &= \exp\left(\sum_{i=1}^{\infty}\left(\frac{q^iT^i}{i} + \frac{T^i}{i}\right)\right) \\ &= \exp\left(\ln(1-T)^{-1} + \ln(1-qT)^{-1}\right) \\ &= \frac{1}{(1-T)(1-qT)} \end{aligned}$$

Definition 3.3. To avoid scheme theory, we consider a *closed point* x in the variety X to be the Galois orbit of $x \in X(\overline{\mathbb{F}_q})$ and the *degree* of x to be the number of elements in the Galois orbit.

Definition 3.4. The *Euler factorisation* of the zeta-function $Z(X, q^{-s})$ is given by

$$\zeta(X,s) = \prod_x \frac{1}{1 - q^{-\deg(x)s}}$$

where the product is over all closed points in the variety X.

We now show that $\zeta(X,s) = Z(X,q^{-s})$, by first explaining the following lemma.

Lemma 3.5. *$\#X(\mathbb{F}_{q^n}) = \sum_x \deg(x)$, where the sum is taken over all closed points x in X such that $\deg(x)|n$.*

Sketch of proof. Suppose $x \in X(\mathbb{F}_{q^n})$. The field extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ is of degree n, so any intermediate field must have order dividing n by the tower law. Thus x is the root of a unique minimal polynomial of degree dividing n, so the number of elements in the Galois orbit of x divides n. The right hand side counts the number of elements in each Galois orbit contained in an intermediate field K where $\mathbb{F}_q \subset K \subset \mathbb{F}_{q^n}$, so the equality holds. □

Proposition 3.6. *$\zeta(X,s) = Z(X,q^{-s})$*

Proof. From lemma 3.5,

$$\#X(\mathbb{F}_{q^n}) = \sum_x \deg(x)$$

where the sum is taken over all closed points x such that $\deg(x)|n$.

Let $\sum_x$ denote the sum over all closed points $x \in X$. The coefficients of T^n are the same for all n in the following equality

$$\begin{aligned}
\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})T^n &= \sum_x \sum_{m=1}^{\infty} \deg(x) T^{\deg(x)m} \\
\implies \sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})T^n \frac{dT}{T} &= \sum_x \sum_{m=1}^{\infty} \deg(x) m \frac{T^{\deg(x)m}}{m} \frac{dT}{T} \\
\implies \sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})T^n}{n} &= \sum_x \sum_{m=1}^{\infty} \frac{T^{\deg(x)m}}{m} \\
\implies \sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})T^n}{n} &= \sum_x -\ln(1 - T^{\deg(x)}) \\
\implies \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})T^n}{n}\right) &= \prod_x \frac{1}{1 - T^{\deg(x)}}
\end{aligned}$$

Note that the product is taken over all closed points $x \in X$. Let $T = q^{-s}$. Then $\zeta(X,s) = Z(X,q^{-s})$. □

Remark 3.7. If X is a variety defined over a finite field and X' is a closed subvariety of X, then $\zeta(X,s) = \zeta(X',s)\zeta(X \setminus X',s)$ and

$$\operatorname{ord}_{s=1}(\zeta(X,s)) = \operatorname{ord}_{s=1}(\zeta(X',s)) + \operatorname{ord}_{s=1}(\zeta(X \setminus X',s)).$$

This is clear by the definition of the zeta-function.

3.1.1 Cohomological Description of Zeta-Functions

The cohomological description of zeta-functions uses theory outside the scope of this project. Without sufficient explanation, we will use l-adic étale cohomology groups, denoted $H^i_{\text{ét}}(X, \mathbb{Q}_l)$, where X is a variety defined over a finite field. We also use the result $H^i_{\text{ét}}(\mathbb{F}_d/\Gamma, \mathbb{Q}_l) = H^i_{\text{ét}}(\mathbb{F}_d, \mathbb{Q}_l)^\Gamma$, which is given in [Mil80, III Th. 2.20].

We begin by recalling a theorem from algebraic topology.

Theorem 3.8 (Lefschetz fixed-point theorem)**.** [Hat02, 2.C] *Let $f : X \to X$ be a continuous map from a finite CW complex X to itself. Let $H_i(X, \mathbb{Q})$ be the i^{th} singular homology group of X with coefficients in $\mathbb{Q}$. Let*

$$\Lambda_f = \sum_{i=0}^{2\dim(X)} (-1)^i \mathrm{Tr}(f_* | H_i(X, \mathbb{Q})).$$

Then $\#X^f = \Lambda_f$, where $\#X^f$ is the number of points in X fixed by f. Thus if $\Lambda_f \neq 0$, then f has a fixed point.

The Lefschetz fixed-point theorem is a generalisation of the Brouwer fixed-point theorem, which states that every continuous function from the closed unit disk D^n to itself must have a fixed point. D^n is a finite CW complex and $H_i(D^n) = 0$ for all $i > 0$. If $f : D^n \to D^n$ is a continuous map, then $f_* : H_0(D^n, \mathbb{Q}) \to H_0(D^n, \mathbb{Q})$ is a non-zero map. Thus $\Lambda_f \neq 0$ for all continuous f, so $f : D^n \to D^n$ has a fixed-point. We apply the Lefschetz fixed-point theorem to the Frobenius map on a variety defined over a field of characteristic not equal to 0.

Theorem 3.9 (Lefschetz fixed-point theorem for the Frobenius)**.** [Mil80, VI §12] *Let X be a variety defined over $\mathbb{F}_q$. Then the fixed points of the Frobenius endomorphism are precisely the points in $X(\mathbb{F}_q)$, and*

$$\#X(\mathbb{F}_q) = \sum_{i=0}^{2\dim(X)} (-1)^i \mathrm{Tr}(\mathrm{Fr}^* | H^i_{\text{ét}}(X, \mathbb{Q}_l))$$

where Fr^* is the Frobenius map on $H^i_{\text{ét}}(X, \mathbb{Q}_l)$.

Note that Tr here denotes the matrix trace. We use the Lefschetz fixed-point theorem for the Frobenius to find a cohomological description of zeta-functions.

Definition 3.10. The *cohomological* description of the zeta-function $Z(X, T)$ is given by

$$Z(X, T) = \prod_{i=0}^{2\dim X} \det(1 - T\mathrm{Fr}^* | H^i_{\text{ét}}(X, \mathbb{Q}_l))^{(-1)^{i+1}}.$$

Definition 3.11. The *characteristic polynomial* of the Frobenius map Fr^* on the i^{th} cohomology group $H^i_{\text{ét}}(X, \mathbb{Q}_l)$ is given by

$$P_i(X,T) = \det(1 - T\mathrm{Fr}^* | H^i_{\text{ét}}(X, \mathbb{Q}_l)).$$

Note that this definition of the characteristic polynomial is slightly different to the usual definition, as the roots of this characteristic polynomial are the inverses of the eigenvalues of the Frobenius map. We can rewrite the cohomological description of the zeta-function $Z(X,T)$ as

$$Z(X,T) = \prod_{i=0}^{2\dim X} P_i(X,T)^{(-1)^{i+1}}$$

We prove that this definition is consistent with previous descriptions of the zeta-function.

Proposition 3.12.

$$Z(X,T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})T^n}{n}\right) = \prod_{i=0}^{2\dim X} \det(1 - T\mathrm{Fr}^* | H^i_{\text{ét}}(X, \mathbb{Q}_l))^{(-1)^{i+1}}$$

Proof. Let Fr_i^n denote $((\mathrm{Fr}^*)^n | H^i_{\text{ét}}(X, \mathbb{Q}_l))$, the Frobenius map Fr^* on the cohomology group $H^i_{\text{ét}}(X, \mathbb{Q}_l)$ applied n times. The Frobenius map is a linear transformation on $H^i_{\text{ét}}(X, \mathbb{Q}_l)$, so we can express Fr_i as a matrix in Jordan normal form with eigenvalues along the diagonal. Let the eigenvalues of Fr_i be $\alpha_{i,j}$. Then

$$\begin{aligned}
\prod_j (1 - \alpha_{i,j}T) &= \det(1 - T\mathrm{Fr}_i) \\
\implies \exp\left(\sum_{n=1}^{\infty} \sum_j -\frac{\alpha_{i,j}^n T^n}{n}\right) &= \det(1 - T\mathrm{Fr}_i) \\
\implies \exp\left(\sum_{n=1}^{\infty} -\frac{\mathrm{Tr}(\mathrm{Fr}_i^n)T^n}{n}\right) &= \det(1 - T\mathrm{Fr}_i) \\
\implies \exp\left(\sum_{n=1}^{\infty} \frac{\sum_{i=0}^{2\dim(X)} (-1)^i \mathrm{Tr}(\mathrm{Fr}_i^n)T^n}{n}\right) &= \prod_{i=0}^{2\dim X} \det(1 - T\mathrm{Fr}_i)^{(-1)^{i+1}}
\end{aligned}$$

As $\#X(\mathbb{F}_{q^n}) = \sum_i^{2\dim(X)} (-1)^i \mathrm{Tr}(\mathrm{Fr}_i^n)$, this gives us the desired equality

$$\exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})T^n}{n}\right) = \prod_{i=0}^{2\dim X} \det(1 - T\mathrm{Fr}^* | H^i_{\text{ét}}(X, \mathbb{Q}_l))$$

□

3.1.2 The Zeta-Function of an Elliptic Curve

Proposition 3.13. *The* zeta-function *of an elliptic curve $E/\mathbb{F}_q$ is given by*

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)}$$

where $\alpha_1, \alpha_2 \in \overline{\mathbb{F}_q}$ are such that $|\alpha_1| = |\alpha_2| = \sqrt{q}$, $\alpha_1\alpha_2 = q$ and $\alpha_1 + \alpha_2 \in \mathbb{Z}$.

In order to compute the zeta-function of $E/\mathbb{F}_q$, we need to find an expression for the number of points in $E(\mathbb{F}_{q^n})$. We relate the degree of endomorphisms in $\mathrm{End}(E)$ to the determinant and trace of endomorphisms in $\mathrm{End}(T_l(E))$, when considered as linear maps from $\mathbb{Z}_l \times \mathbb{Z}_l \to \mathbb{Z}_l \times \mathbb{Z}_l$. We show that for $\psi_l \in \mathrm{End}(T_l(E))$, $\det(\psi_l)$ and $\mathrm{Tr}(\psi_l)$ are independent of l.

Lemma 3.14. [Sil86, V §2] *Let $\phi \in \mathrm{End}(E)$ and let $\phi_l \in \mathrm{End}(T_l(E))$ be the image of ϕ under the map $\mathrm{End}(E) \to \mathrm{End}(T_l(E))$. Then*

$$\det(\phi_l) = \deg(\phi) \text{ and } \mathrm{Tr}(\phi_l) = 1 + \deg(\phi) - \deg(1-\phi).$$

Proof. We know that $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ by proposition 0.34. Let $v_1 = (a, b)$ and $v_2 = (c, d)$ be a basis for $T_l(E)$. Then ϕ_l can be expressed by the matrix

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

Using the properties of the Weil paring (proposition 0.36), $e : T_l(E) \times T_l(E) \to T_l(\mu)$, we show that $e(v_1, v_2)^{\deg(\phi)} = e(v_1, v_2)^{\deg(\phi_l)}$.

$$\begin{aligned} e(v_1, v_2)^{\deg(\phi)} &= e([\deg(\phi)]v_1, v_2) \\ &= e((\hat{\phi}_l \circ \phi_l)v_1, v_2) \\ &= e(\phi_l(v_1), \phi_l(v_2)) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(av_1, bv_1)e(cv_2, bv_1)e(av_1, dv_2)e(cv_2, dv_2) \\ &= e(v_1, v_2)^{-bc}e(v_1, v_2)^{ad} \\ &= e(v_1, v_2)^{\det(\phi_l)} \end{aligned}$$

Thus $\det(\phi_l) = \deg(\phi)$. Also,

$$1 + \det(A) - \det(1-A) = 1 + ad - bc - ((1-a)(1-d) - bc) = a + d = \mathrm{Tr}(A)$$

so $\mathrm{Tr}(\phi_l) = 1 + \deg(\phi) - \deg(1-\phi)$. □

We can now apply this lemma to the Frobenius endomorphism, as the Frobenius automorphism is an element of $\mathrm{End}(E)$. Note that Fr_l, the image of Fr under the map $\mathrm{End}(E) \to \mathrm{End}(T_l(E))$ can be considered as a 2×2 matrix.

Lemma 3.15. [Sil86, III §4-5] $\#E(\mathbb{F}_{q^n}) = \deg(1 - \mathrm{Fr}^n)$

We wish to relate $\deg(1 - \mathrm{Fr}^n)$ to the determinant of an endomorphism in $\mathrm{End}(T_l(E))$.

Lemma 3.16. [Sil86, V §2]

$$\#E(\mathbb{F}_{q^n}) = 1 - \alpha_1^n - \alpha_2^n + q^n$$

where $\alpha_1, \alpha_2 \in \overline{\mathbb{F}_q}$ *are such that* $|\alpha_1| = |\alpha_2| = \sqrt{q}$, $\alpha_1\alpha_2 = q$ *and* $\alpha_1 + \alpha_2 \in \mathbb{Z}$.

Proof. By lemma 3.14, the polynomial

$$\det(T - \mathrm{Fr}_l) = T^2 - \mathrm{Tr}(\mathrm{Fr}_l)T + \det(\mathrm{Fr}_l)$$

has integer coefficients, as $\mathrm{Tr}(\mathrm{Fr}_l), \det(\mathrm{Fr}_l)$ are elements of $\mathbb{Z}$. Also, if $T = \frac{r}{s} \in \mathbb{Q}$, then

$$\det\left(\frac{r}{s} - \mathrm{Fr}_l\right) = \frac{\det(r - s\mathrm{Fr}_l)}{s^2} = \frac{\deg(r - s\mathrm{Fr})}{s^2} \geq 0$$

Therefore, the polynomial $\det(T - \mathrm{Fr}_l)$ must have two complex conjugate roots, call these α_1 and α_2. We know that $\det(\mathrm{Fr}_l) = \deg(\mathrm{Fr}) = q$, so $\alpha_1\alpha_2 = q$ and $|\alpha_1| = |\alpha_2| = \sqrt{q}$. Thus

$$\det(T - \mathrm{Fr}_l) = (T - \alpha_1)(T - \alpha_2).$$

By the same reasoning,

$$\det(T - \mathrm{Fr}_l^n) = (T - \alpha_1^n)(T - \alpha_2^n).$$

So

$$\begin{aligned}\#E(\mathbb{F}_{q^n}) &= \deg(1 - \mathrm{Fr}^n) \\ &= \det(1 - \mathrm{Fr}_l^n) \\ &= (1 - \alpha_1^n)(1 - \alpha_2^n) \\ &= 1 - \alpha_1^n - \alpha_2^n + q^n\end{aligned}$$

□

Proof of proposition 3.13. By lemma 3.16,

$$\begin{aligned}
Z(E/\mathbb{F}_q, T) &= \exp\left(\sum_{n=1}^{\infty} \frac{(\#E(\mathbb{F}_{q^n}))T^n}{n}\right) \\
&= \exp\left(\sum_{n=1}^{\infty} \frac{(1-\alpha_1^n-\alpha_2^n+q^n)T^n}{n}\right) \\
&= \exp\left(\sum_{n=1}^{\infty} \left(\frac{T^n}{n} - \frac{\alpha_1^n T^n}{n} - \frac{\alpha_2^n T^n}{n} + \frac{q^n T^n}{n}\right)\right) \\
&= \exp\left(-\ln(1-T) + \ln(1-\alpha_1 T) + +\ln(1-\alpha_2 T) + \ln(1-qT)\right) \\
&= \frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)}
\end{aligned}$$

□

3.2 The Weil Conjectures

The Weil conjectures are statements about the zeta-function of a variety X defined over a finite field $\mathbb{F}_q$. The first Weil conjecture states that the zeta-function $Z(X,T)$ should be a rational function of T, and was proven by Dwork in 1960. The second Weil conjecture states that the zeta-function $Z(X,T)$ satisfies a functional equation and was proven by Grothendieck in 1965. The third Weil conjecture is an analogue of the Riemann hypothesis for varieties over finite fields, and was proven by Deligne in 1974.

Theorem 3.17 (Weil conjectures)**.** [Mil80, VI §12] *Suppose X is a smooth projective variety of dimension n over a finite field $\mathbb{F}_q$. Then*

1. (Rationality) $Z(X,T)$ is a rational function of T. Moreover, we can write $Z(X,T)$ as:

$$\frac{P_1(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$$

where $P_i(T) \in \mathbb{Z}[T]$ for all i and n is the dimension of X. Furthermore, $P_0(T) = (1-T)$ and $P_{2n}(T) = (1-q^nT)$.

2. (Functional equation and Poincaré duality) There exists an integer ε (the Euler characteristic) such that $Z(X, q^{-n}T^{-1}) = \pm q^{\frac{n\varepsilon}{2}} T^{\varepsilon} Z(X,T)$.

3. (Riemann hypothesis) By 1., we can write $Z(X,T) = \frac{P_1(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$. Additionally, $P_i(T) = \prod_j (1-\alpha_{i,j}T)$ where $\alpha_{i,j} \in \mathbb{C}$ and $|\alpha_{i,j}| = q^{\frac{i}{2}}$ for all i and j.

If X is an elliptic curve E over a finite field $\mathbb{F}_q$, then we can prove the Weil conjectures for $E/\mathbb{F}_q$. Specifically, we can show that $Z(E/\mathbb{F}_q, T)$ is a rational function of T, that $Z(E/\mathbb{F}_q, T) = Z(E/\mathbb{F}_q, q^{-1}T^{-1})$ and the Riemann hypothesis.

Proof of the Weil conjectures for $X = E/\mathbb{F}_q$. (1) Let α_1, α_2 be as in proposition 3.13. Let $P_1(T) = (1-\alpha_1 T)(1-\alpha_2 T) = 1 - aT + qT^2$, where $a = \alpha_1 + \alpha_2 \in \mathbb{Z}$. Let $P_0(T) = (1-T)$ and let $P_2(T) = (1-qT)$. Then by proposition 3.13,

$$Z(E/\mathbb{F}_q, T) = \frac{P_1(T)}{P_0(T)P_2(T)}$$

and so $Z(E/\mathbb{F}_q, T)$ is a rational function.

(2) Let $\varepsilon = 0$.

$$\begin{aligned} Z(E/\mathbb{F}_q, q^{-1}T^{-1}) &= \frac{1 - \frac{a}{qT} + \frac{1}{qT^2}}{(1-\frac{1}{qT})(1-\frac{1}{T})} \\ &= \frac{qT^2 - aT + 1}{(qT-1)(T-1)} \\ &= Z(E/\mathbb{F}_q, T) \end{aligned}$$

(3) We have $P_0(T) = (1-T)$, so $|\alpha_{0,1}| = 1 = q^0$. Also $P_2(T) = (1-qT)$, so $|\alpha_{2,1}| = q = q^1$. We have $P_1(T) = (1-\alpha_1 T)(1-\alpha_2 T)$, so $|\alpha_1| = |\alpha_{1,1}| = \sqrt{q} = q^{\frac{1}{2}}$ and $|\alpha_2| = |\alpha_{1,2}| = \sqrt{q} = q^{\frac{1}{2}}$. Thus the Riemann hypothesis holds for $E/\mathbb{F}_q$. □

To see why the third Weil conjecture is the Riemann hypothesis, we can look at the roots of $Z(E/\mathbb{F}_q, q^{-s})$.

$$Z(E/\mathbb{F}_q, q^{-s}) = \frac{(1-\alpha_1 q^{-s})(1-\alpha_2 q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

If $Z(E/\mathbb{F}_q, q^{-s}) = 0$, then $\alpha_1 q^{-s} = 1$ or $\alpha_2 q^{-s} = 1$. So $|q^s| = |\alpha_1| = |\alpha_2| = \sqrt{q}$. Thus the real part of s is $\frac{1}{2}$.

The rationality of the zeta-function for projective curves was proven by F.K. Schmidt in 1931 using the Riemann-Roch theorem. The analogue of the Riemann hypothesis for curves was proven by Weil himself.

3.2.1 The Tate Conjecture

By the first and third Weil conjectures, we can write the zeta-function of a variety X over $\mathbb{F}_q$ as a rational function

$$Z(X,T) = \frac{P_1(T)...P_{2n-1}(T)}{P_0(T)P_2(T)...P_{2n}(T)}$$

where n is the dimension of X. This is equivalent to the cohomological description of $Z(X,T)$, where we let $P_i(T) = P_i(X,T)$ and

$$Z(X,T) = \prod_{i=0}^{2\dim X} P_i(X,T)^{(-1)^{i+1}}$$

By the third Weil conjecture, $P_i(X,T) = P_i(T) = \prod_j (1 - \alpha_{i,j}T)$ where $\alpha_{i,j} \in \mathbb{C}$ and $|\alpha_{i,j}| = q^{\frac{i}{2}}$ for all i and j. As $|\alpha_{i,j}| = q^{i/2}$, only the polynomial $P_2(X,T)$ can contribute to the order of the pole at $T = q^{-1}$ of $Z(X,T)$. Letting $T = q^{-s}$, this corresponds to the order of the pole at $s = 1$ of $\zeta(X,s)$. This gives the inequality

$$\dim_{\mathbb{Q}_l}(H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q} \leq -\text{ord}_{s=1}\zeta(X,s)$$

where $(H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q}$ is the subset of $(H^2_{\text{ét}}(X,\mathbb{Q}_l))$ such that the Frobenius map Fr^* on $(H^2_{\text{ét}}(X,\mathbb{Q}_l))$ acts by multiplication by q. (If X is smooth and projective, this is an equality.)

We claim without proof that there exists a cycle class map

$$\text{NS}(X) \to (H^2_{\text{ét}}(X,\mathbb{Q}_l))$$

which induces an injection $\text{NS}(X) \otimes \mathbb{Q}_l \to (H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q}$. This gives the inequality

$$\text{Rank}(\text{NS}(X)) \leq \dim_{\mathbb{Q}_l}(H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q}.$$

Thus

$$\text{Rank}(\text{NS}(X)) \leq \dim_{\mathbb{Q}_l}(H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q} \leq -\text{ord}_{s=1}\zeta(X,s).$$

Conjecture A (Tate conjecture)**.**

$$\text{Rank}(\text{NS}(X)) = \dim_{\mathbb{Q}_l}(H^2_{\text{ét}}(X,\mathbb{Q}_l))^{\text{Fr}^*=q} = -\text{ord}_{s=1}\zeta(X,s).$$

The Tate conjecture holds for curves defined over $\mathbb{F}_q$. By the Weil conjectures, if C is a smooth projective curve defined over $\mathbb{F}_q$, then $-\text{ord}_{s=1}\zeta(C,s) = 1$.

If C is a smooth, projective curve, then two divisors are algebraically equivalent if and only if they are of the same degree. This is because a product of d copies of C can be used to parametrise effective divisors of degree d. If there exists one effective divisor on C degree $s \neq 0$, then there exist divisors on C of degree ns for every $n \in \mathbb{Z}$. We can always find an effective divisor on C by using another curve C' to cut out on C a divisor. Therefore, the Néron-Severi group of C is isomorphic to $\mathbb{Z}$ and $\text{Rank}(\text{NS}(C)) = 1$.

In [Tat94], Tate proves that if the Tate conjecture holds for X and $X \dashrightarrow Y$ is a dominant rational map, then the Tate conjecture holds for Y. Tate also proves that if the Tate conjecture holds for X and Y, then it also holds for $X \times Y$. We now specialise to our elliptic surface $\mathcal{E}$ corresponding to the elliptic curve $E/\mathbb{K}$ given by

$$E : y^2z + xyz = x^3 - t^dz^3$$

We want to show that the Tate conjecture holds for the elliptic surface $\mathcal{E}$. We know that there exists a dominant rational map $\mathcal{F}_d \dashrightarrow \mathcal{E}$, so the Tate conjecture for the Fermat surface $\mathcal{F}_d$ would imply the Tate conjecture for $\mathcal{E}$. We show that there exists a dominant rational map from the product of two Fermat curves to the Fermat surface $\mathcal{F}_d$, so the Tate conjecture holds for $\mathcal{F}_d$.

Proposition 3.18. [SK79] *The Fermat surface $\mathcal{F}_d$ is dominated by a product of Fermat curves F_d.*

Proof. The Fermat surface $\mathcal{F}_d$ consists of the set of points in $\mathbb{P}^3$ such that $z_0^d + z_1^d + z_2^d + z_3^d = 0$. The Fermat curve F_d consists of the set of points in $\mathbb{P}^2$ such that $x_0^d + x_1^d + x_2^d = 0$. We show that the map $f : F_d \times F_d \to \mathcal{F}_d$ given by

$$([x_0, x_1, x_2], [y_0, y_1, y_2]) \mapsto [x_0y_2, x_1y_2, \zeta x_2y_0, \zeta x_2y_1]$$

is a dominant rational map, where ζ is a root of unity such that $\zeta^d = -1$. Note $[x_0y_2, x_1y_2, \zeta x_2y_0, \zeta x_2y_1] \in \mathcal{F}_d$ as

$$(x_0y_2)^d + (x_1y_2)^d + (\zeta x_2y_0)^d + (\zeta x_2y_1)^d = y_2^d(x_0^d + x_1^d) - x_2^d(y_0^d + y_1^d) = y_2^dx_2^d - x_2^dy_2^d = 0.$$

We consider f to be dominant if the map from $F_d \times F_d$, viewed as a product of curves defined over $\overline{\Bbbk}$, to $\mathcal{F}_d$, viewed as a surface defined over $\overline{\Bbbk}$, is dominant. This map is well-defined at all points of F_d where $x_2 \neq 0$ and $y_2 \neq 0$, and so it is rational.

Suppose $[z_0, z_1, z_2, z_3] \in \mathcal{F}_d$. Suppose $z_2^d + z_3^d \neq 0$. Then we can assume without loss of generality that $z_2^d + z_3^d = 1$. Thus $z_0^d + z_1^d + 1 = 0$. Then $[z_0, z_1, 1] \in F_d$ and $[\zeta^{-1}z_2, \zeta^{-1}z_3, 1] \in F_d$ and

$$\big([z_0, z_1, 1], [\zeta^{-1}z_2, \zeta^{-1}z_3, 1]\big) \mapsto [z_0, z_1, z_2, z_3].$$

Suppose $z_2^d + z_3^d = 0$ and hence $z_0^d + z_1^d = 0$. We know at least two of coordinates of $[z_0, z_1, z_2, z_3]$ must be non-zero. Thus $[z_0, z_1, z_2, z_3] \sim [1, \zeta_1, Z, \zeta_2 Z]$ or $[z_0, z_1, z_2, z_3] \sim [Z, \zeta_1 Z, 1, \zeta_2]$, where ζ_1 and ζ_2 are some roots of unity such that $\zeta_1^d = \zeta_2^d = -1$ and $Z \in \overline{\Bbbk}$. The locus of points of this form on the Fermat surface is a finite number of curves, thus the image of f dominates the Fermat surface. □

By the Tate conjecture (conjecture A),

$$\mathrm{Rank}(\mathrm{NS}(\mathcal{E})) = -\mathrm{ord}_{s=1}\zeta(\mathcal{E}, s). \tag{3.1}$$

We have reduced the problem of evaluating the rank of the Néron-Severi group of $\mathcal{E}$ to computing the zeta-function of $\mathcal{E}$.

3.2.2 The Zeta-Function of a Fermat Surface

We can further reduce the problem of computing the rank of $E/\mathbb{K}$ to evaluating the order of vanishing of the zeta-function of $\mathcal{F}_d/\Gamma$. In section 2.3.1, we found a subset of $\mathcal{W}_d$ isomorphic to a subset of $\mathcal{F}_d/\Gamma$. The zeta-functions of isomorphic varieties are equal. Also, the zeta-function of any curve defined over a finite field has order of vanishing at $s = 1$ of -1 by the Weil conjectures; therefore, by remark 3.7, removing a curve from a variety of dimension 2 will increase the order of vanishing at $s = 1$ of the zeta-function of the variety by 1.

In section 2.3.1, we proved that the Weierstrass model $\mathcal{W}_d$ minus α irreducible curves is isomorphic to $\mathcal{F}_d/\Gamma$ minus 3 irreducible curves, where

$$\alpha = 1 + \begin{cases} 2 & \text{if } 2 \nmid d \text{ or } \mu_4 \notin k \\ 3 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 1 & \text{if } 3 \nmid d \\ 2 & \text{if } 3|d \text{ and } \mu_3 \notin k \\ 3 & \text{if } 3|d \text{ and } \mu_3 \subset k \end{cases}$$

Thus

$$\begin{aligned} &-\operatorname{ord}_{s=1}(\zeta(W_d, s)) - 4 - A = -\operatorname{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) - 3 \\ \implies &-\operatorname{ord}_{s=1}(\zeta(W_d, s)) = -\operatorname{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) + 1 + A \end{aligned} \tag{3.2}$$

where

$$A = \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } \mu_4 \notin k \\ 1 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3|d \text{ and } \mu_3 \notin k \\ 2 & \text{if } 3|d \text{ and } \mu_3 \subset k \end{cases}$$

Additionally, we can evaluate the zeta-function of $\mathcal{W}_d$ in terms of the zeta-function of $\mathcal{E}$. The good fibres of $\mathcal{W}_d$ are the same as the good fibres of $\mathcal{E}$, however bad fibres of $\mathcal{W}_d$ are affected by the blow-up. Using Tate's algorithm, we know the geometric structure of the bad fibres of $\mathcal{E}$. Specifically, we know how many irreducible components (dimension 1 varieties) are in each bad fibre. Bad fibres of W_d all have one irreducible component (a nodal or a cuspidal cubic curve), so the order of vanishing of the zeta-functions of $\mathcal{W}_d$ and $\mathcal{F}_d/\Gamma$ will differ by the number of irreducible components added to each bad fibre during the blow-up. Let n_v be the number of irreducible components in a bad fibre at v of $\mathcal{E}$. Therefore,

$$\begin{aligned} &-\operatorname{ord}_{s=1}(\zeta(\mathcal{E}, s)) - \sum_v (n_v - 1) = -\operatorname{ord}_{s=1}(\zeta(W_d, s)) \\ \implies &-\operatorname{ord}_{s=1}(\zeta(\mathcal{E}, s)) = -\operatorname{ord}_{s=1}(\zeta(W_d, s)) + \sum_v (n_v - 1). \end{aligned} \tag{3.3}$$

From corollary 1.28,

$$\mathrm{Rank}(\mathrm{NS}(\mathcal{E})) = \mathrm{Rank}(E(\mathbb{K})) + 2 + \sum_v (n_v - 1).$$

Substituting equations 3.1, 3.2 and 3.3 into the above equation gives

$$\mathrm{Rank}(E(\mathbb{K})) = -\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) - 1 + A \tag{3.4}$$

where A is as before. Note that A is a number between 0 and 3.

We have now reduced the problem of computing the rank of an elliptic curve over $\mathbb{K}$ to computing the zeta-function of a Fermat surface over $\Bbbk$. This zeta-function will reduce to evaluating some Gauss and Jacobi sums, and will be explained in the next chapter.

3.2.3 The Birch and Swinnerton-Dyer Conjecture

As a side note, we show that the Tate conjecture for $\mathcal{E}/\Bbbk$ is equivalent to the Birch and Swinnerton-Dyer conjecture for the associated elliptic curve E over $\mathbb{K}$.

Definition 3.19. [Ulm09] The *L-series* of an elliptic curve over $\mathbb{F}_q$ is given by

$$L(E,T) = \prod_{\text{good } v} (1 - a_v T^{\deg(v)} + q_v T^{2\deg(v)})^{-1} \prod_{\text{bad } v} (1 - a_v T^{\deg(v)})^{-1}$$

where $q_v = q^{\deg(v)}$ and

$$a_v = \begin{cases} q_v + 1 - \#(E_v(\mathbb{F}_{q^i})), & \text{if } E_v \text{ is non-singular (has good reduction)} \\ 1, & \text{if } E_v \text{ has split multiplicative reduction} \\ -1, & \text{if } E_v \text{ has non-split multiplicative reduction} \\ 0, & \text{if } E_v \text{ has additive reduction} \end{cases}$$

and where the products are over closed points $v \in \mathbb{P}^1$ with good and bad reduction.

Remark 3.20. When we consider the order of vanishing at $s = 1$ of the L-function, this is the order of vanishing of the L-function at $s = 1$ of $L(E,T)$ where $T = q^{-s}$. (This is analogous to the zeta-function and its Euler factorisation.)

Conjecture B (Birch and Swinnerton-Dyer Conjecture)**.**

$$\mathrm{ord}_{s=1}(L(E,s)) = \mathrm{Rank}(E(\mathbb{K}))$$

In section 2.2.2, we found expressions for the number of $\mathbb{F}_{q^i}$-valued points in each bad fibre for each i. Using this information, we can calculate the zeta-function for each bad fibre of $\mathcal{E}$. Let $b = -1$ if the conductor of the fibre is 2 (additive reduction), let $b = 0$ if the conductor of the fibre is 1 (multiplicative reduction). Let n be the number of irreducible components of the special fibre defined over $\Bbbk = \mathbb{F}_q$ (as before). Let M be the number of irreducible components of the special fibre defined over $\overline{\Bbbk}$, and let $m = M - n$.

Reduction Type	$\#E_t(\mathbb{F}_{q^i})$	$Z(E_t, T)$	n	m	b
I_d (split)	$1 + 5q^i$	$\frac{1}{(1-qT)^d}$	d	0	0
II	$1 + q^i$	$\frac{1}{(1-T)(1-qT)}$	1	0	-1
IV (split)	$1 + 3q^i$	$\frac{1}{(1-T)(1-qT)^3}$	3	0	-1
IV (non-split)	$1 + 2q^i + (-1)^i q^i$	$\frac{1}{(1-T)(1-qT)^2(1+qT)}$	2	1	-1
I_0^* (split)	$1 + 5q^i$	$\frac{1}{(1-T)(1-qT)^5}$	5	0	-1
I_0^* (non-split)	$1 + 4q^i + (-1)^i q^i$	$\frac{1}{(1-T)(1-qT)^4(1+qT)}$	4	1	-1
II^*	$1 + 9q^i$	$\frac{1}{(1-T)(1-qT)^9}$	9	0	-1
IV^* (split)	$1 + 7q^i$	$\frac{1}{(1-T)(1-qT)^7}$	7	0	-1
IV^* (non-split)	$1 + 5q^i + (-1)^i 2q^i$	$\frac{1}{(1-T)(1-qT)^5(1+qT)^2}$	5	2	-1

Note b is the degree of $(1-T)$ in the zeta-function, n is the degree of $(1-qT)$ and m is the degree of $(1+qT)$. Thus the zeta-function of a bad fibre on the elliptic surface $\mathcal{E}$ is given by

$$Z(\pi^{-1}(v), T) = \frac{(1-T)^{b_v}}{(1-q_vT)^{n_v}(1+q_vT)^{m_v}}$$

where $q_v = q^{\deg(v)}$.

Proposition 3.21. *The L-function of the elliptic curve $E/\mathbb{K}$ is given by*

$$L(E,T) = \frac{Z(\mathbb{P}^1,T)Z(\mathbb{P}^1,qT)}{Z(\mathcal{E}/\Bbbk,T)} \prod_{\text{bad } v} \frac{Z(\pi^{-1}(v), T^{\deg(v)})(1-T^{\deg(v)})(1-q_vT^{\deg(v)})}{(1-a_vT^{\deg(v)})}.$$

where

$$a_v = \begin{cases} q_v + 1 - \#(E_v(\mathbb{F}_{q^i})), & \text{if } E_v \text{ is non-singular (has good reduction)} \\ 1, & \text{if } E_v \text{ has split multiplicative reduction} \\ -1, & \text{if } E_v \text{ has non-split multiplicative reduction} \\ 0, & \text{if } E_v \text{ has additive reduction} \end{cases}$$

Proof.

$$\begin{aligned} Z(\mathcal{E}, T) &= \prod_{\text{closed } x \in \mathcal{E}} \left(1 - T^{\deg(x)}\right)^{-1} \\ &= \prod_{\text{closed } v \in \mathbb{P}^1} \prod_{x \in \pi^{-1}(v)} \left(1 - T^{\deg(x)}\right)^{-1} \\ &= \prod_{\text{closed } v \in \mathbb{P}^1} Z(\pi^{-1}(v), T^{\deg(v)}) \\ &= \prod_{\text{good } v} Z(\pi^{-1}(v), T^{\deg(v)}) \prod_{\text{bad } v} Z(\pi^{-1}(v), T^{\deg(v)}) \end{aligned}$$

where the final products are over points $v \in \mathbb{P}^1$ with good and bad reduction. In section 3.1.2, we calculated the zeta-function of an elliptic curve over $\mathbb{F}_q$. Thus if E has good reduction at v,

$$Z(\pi^{-1}(v), T^{\deg(v)}) = \frac{\left(1 - a_v T^{\deg(v)} + q_v T^{2\deg(v)}\right)}{\left(1 - T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)}.$$

We also know that at a bad fibre v,

$$Z(\pi^{-1}(v), T^{\deg(v)}) = \frac{\left(1 - T^{\deg(v)}\right)^{b_v}}{\left(1 - q_v T^{\deg(v)}\right)^{n_v}\left(1 + q_v T^{\deg(v)}\right)^{m_v}}.$$

Putting this together,

$$\begin{aligned} Z(\mathcal{E}, T) &= \prod_{\text{good } v} \frac{\left(1 - a_v T^{\deg(v)} + q_v T^{2\deg(v)}\right)}{\left(1 - T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)} \prod_{\text{bad } v} \frac{\left(1 - T^{\deg(v)}\right)^{b_v}}{\left(1 - q_v T^{\deg(v)}\right)^{n_v}\left(1 + q_v T^{\deg(v)}\right)^{m_v}} \\ &= \frac{Z(\mathbb{P}^1, T) Z(\mathbb{P}^1, qT)}{L(E, T)} \prod_{\text{bad } v} \frac{\left(1 - T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)\left(1 - T^{\deg(v)}\right)^{b_v}}{\left(1 - a_v T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)^{n_v}\left(1 + q_v T^{\deg(v)}\right)^{m_v}} \\ &= \frac{Z(\mathbb{P}^1, T) Z(\mathbb{P}^1, qT)}{L(E, T)} \prod_{\text{bad } v} \frac{\left(1 - T^{\deg(v)}\right)^{b_v + 1}}{\left(1 - a_v T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)^{n_v - 1}\left(1 + q_v T^{\deg(v)}\right)^{m_v}} \end{aligned}$$

Rearranging gives the result

$$L(E, T) = \frac{Z(\mathbb{P}^1, T) Z(\mathbb{P}^1, qT)}{Z(\mathcal{E}/\mathbb{k}, T)} \prod_{\text{bad } v} \frac{Z(\pi^{-1}(v), T^{\deg(v)})\left(1 - T^{\deg(v)}\right)\left(1 - q_v T^{\deg(v)}\right)}{\left(1 - a_v T^{\deg(v)}\right)}.$$

□

Thus

$$\mathrm{ord}_{s=1}(L(E,T)) = -\mathrm{ord}_{s=1}\zeta(\mathcal{E},s) - 2 - \sum_{v}(n_v - 1) = \mathrm{Rank}(E(\mathbb{K}))$$

where n_v is the number of irreducible components of the special fibre at v and the second equality is from corollary 1.28. Therefore, the Birch and Swinnerton-Dyer conjecture holds for $E/\mathbb{K}$.

Remark 3.22. In [Ulm09], Ulmer omits the $(1 - a_v T^{\deg(v)})$ component of the L-function of $E/\mathbb{K}$. Additionally, n and m for non-split reduction type IV^* are given as 3 and 4, as opposed to 5 and 2.

Chapter 4

Elliptic Curves of Arbitrarily Large Rank

The previous chapter reduced the problem of calculating the rank of $E(\mathbb{K})$ to evaluating the order of vanishing at $s = 1$ of the zeta-function of a quotient of a Fermat surface by a group. Recall equation 3.4,

$$\text{Rank}(E(\mathbb{K})) = -\text{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) - 1 + A$$

where A depends on q and d and is a number between 0 and 3. In this chapter, we find an expression for $-\text{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s))$ in terms of q and d. Therefore, we will be able to control the rank of $E(\mathbb{K})$ by varying q and d.

Due the Weil conjectures, only the polynomial $P_2(\mathcal{F}_d/\Gamma, T)$ contributes to the order of vanishing of $Z(\mathcal{F}_d/\Gamma, T)$ at $T = q^{-1}$ (i.e. at $s = 1$). By the cohomological description of zeta-functions,

$$P_2(\mathcal{F}_d/\Gamma, T) = \det(1 - T\text{Fr}^* | H^2_{\acute{e}t}(\mathcal{F}_d/\Gamma, \mathbb{Q}_l))$$

so we need to understand how the Frobenius map acts on $H^2_{\acute{e}t}(\mathcal{F}_d/\Gamma, \mathbb{Q}_l)$. In [Ulm02], Ulmer proves a theorem by Shioda stating that the Frobenius map acts on a particular subgroup of $H^2_{\acute{e}t}(\mathcal{F}_d, \mathbb{Q}_l)$ by multiplication by a Jacobi sum. The proof of this theorem is outside the scope of this project, so we merely provide an explanation of its assumptions and consequences. We begin this chapter by understanding the Gauss and Jacobi sums use in Shioda's theorem.

In this chapter, we will assume that q is a power of p and that $d|p^n + 1$ for some positive integer n.

4.1 Evaluating Gauss and Jacobi Sums

Let G, H, Diag and Γ be as defined in section 2.3.

Let n be an integer coprime to p. Let t be a character which sends n^{th} roots of unity in $\overline{\mathbb{k}}$ to n^{th} roots of unity in $\overline{\mathbb{Q}}^\times$. As n and p are coprime, the group of n^{th} roots of unity in $\overline{\mathbb{k}}$ is isomorphic to the group of n^{th} roots of unity in $\overline{\mathbb{Q}}^\times$, thus it is possible to find such a character.

We firstly consider the group $\hat{H}$ of characters acting on elements of H. Elements of $\hat{H}$ are homomorphisms sending elements of H to $\overline{\mathbb{Q}}^\times$. We consider the action of an element of $\hat{H}$ coordinate-wise. The d^{th} roots of unity are a cyclic group isomorphic to $\mathbb{Z}/d\mathbb{Z}$, so any homomorphism on the d^{th} roots of unity in $\overline{\mathbb{k}}$ is completely determined by where the generator is sent. Moreover, 1 must be sent to $1 \in \overline{\mathbb{Q}}^\times$, so any character must send d^{th} roots of unity in $\overline{\mathbb{k}}$ to d^{th} roots of unity in $\overline{\mathbb{Q}}^\times$. Therefore, the group of characters from d^{th} roots of unity in $\overline{\mathbb{k}}$ to $\overline{\mathbb{Q}}^\times$ is isomorphic to $\mathbb{Z}/d\mathbb{Z}$ and so the group of characters $\hat{H}$ must be isomorphic to $(\mathbb{Z}/d\mathbb{Z})^4$.

We can hence express the action of $h \in \hat{H}$ on $z = [\zeta_0, \zeta_1, \zeta_2, \zeta_3] \in H$ by

$$h(z) = t(\zeta_0)^{a_0} t(\zeta_1)^{a_1} t(\zeta_2)^{a_2} t(\zeta_3)^{a_3}$$

where (a_0, a_1, a_2, a_3) is some element in $(\mathbb{Z}/d\mathbb{Z})^4$. Note that d and p are coprime. As G is a quotient group of H, the group of characters $\hat{G}$ sending elements of G to elements of $\overline{\mathbb{Q}}^\times$ must be a subgroup of $\hat{H}$. Elements of $\hat{G}$ must send elements of Diag to $1 \in \overline{\mathbb{Q}}^\times$, so if $[\zeta, \zeta, \zeta, \zeta] \in \text{Diag}$, then

$$t(\zeta)^{a_0} t(\zeta)^{a_1} t(\zeta)^{a_2} t(\zeta)^{a_3} = 1.$$

Therefore, the group of characters $\hat{G}$ precisely corresponds to the subgroup of $(\mathbb{Z}/d\mathbb{Z})^4$ given by

$$\{a = (a_0, a_1, a_2, a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 \mid \sum_i a_i = 0\}$$

and the pairing $G \times \hat{G} \to \overline{\mathbb{Q}}^\times$ is given by

$$a(z) = \langle [\zeta_0, \zeta_1, \zeta_2, \zeta_3], (a_0, a_1, a_2, a_3) \rangle = \prod_{i=0}^{3} t(\zeta_i)^{a_i}.$$

Let $\hat{G}' \subset \hat{G}$ be the set of characters

$$\hat{G}' = \{a = (a_0, a_1, a_2, a_3) \in \hat{G} \mid \text{either } a = 0 \text{ or } a_i \neq 0 \text{ for all } i\}$$

Suppose $a \in \hat{G}$. We define $qa = (qa_0, qa_1, qa_2, qa_3)$ and we define $u(a)$ to be the smallest positive integer such that $q^{u(a)}a = a$.

4.1.1 A Jacobi Sum

Fix $a \in \hat{G}$.

Definition 4.1. Let $\psi_0 : \mathbb{F}_p \to \overline{\mathbb{Q}}^\times$ be a non-trivial character. For each finite extension $\mathbb{F}_{p^m}$ of $\mathbb{F}_p$, let $\psi : \mathbb{F}_{p^m} \to \overline{\mathbb{Q}}^\times$ be given by $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}$.

Definition 4.2. Let t and $\hat{G}$ be as before. Let $\chi_i : \mathbb{F}^\times_{q^{u(a)}} \to \overline{\mathbb{Q}}^\times$ be a multiplicative character given by $\chi_i = t^{\frac{(q^{u(a)}-1)a_i}{d}}$.

This is well defined, as $u(a)$ is chosen to be the smallest positive integer such that $q^{u(a)}a_i - a_i \equiv 0 \mod d$ for all i. Also, χ_i is independent of the choice of representative of $a_i \in \mathbb{Z}$. This is because different choices of a_i differ by a multiple of d, so the power of t will differ by a multiple of $(q^{u(a)}-1)$, which will not change the multiplicative character. We define a Gauss sum in the usual way

$$g(\chi_i, \psi) = -\sum_{x \in \mathbb{F}^\times_{q^{u(a)}}} \chi_i(x)\psi(x)$$

where $\psi : \mathbb{F}_{q^{u(a)}} \to \overline{\mathbb{Q}}^\times$. We define a Jacobi sum

$$J(a) = J(\chi_0, \chi_1, \chi_2, \chi_3) = \sum_{x_0+x_1+x_2+x_3=1} \chi_0(x_0)\chi_1(x_1)\chi_2(x_2)\chi_3(x_3)$$

where the sum is over all elements $x_0, x_1, x_2, x_3 \in \mathbb{F}^\times_{q^{u(a)}}$ such that $x_1 + ... + x_n = 1$. We define $J(0) = q$. Suppose $a \neq 0$. Then the characters χ_i are not all trivial as t is a non-trivial character. However, for any $x \in \mathbb{F}^\times_{q^{u(a)}}$,

$$(\chi_0\chi_1\chi_2\chi_3)(x) = t^{\frac{(q^{u(a)}-1)(a_0+a_1+a_2+a_3)}{d}}(x) = t^{(q^{u(a)}-1)c}(x) = t(x^{q^{u(a)}-1})^c = t(1)^c = 1$$

where $c \in \mathbb{Z}$. Therefore, the product $\chi_0\chi_1\chi_2\chi_3$ is a trivial character. By proposition 0.62, we can write

$$J(a) = \frac{1}{q^{u(a)}} g(\chi_0, \psi)g(\chi_1, \psi)g(\chi_2, \psi)g(\chi_3, \psi)$$

and

$$J(a) = \frac{1}{q^{u(a)} - 1} \sum_{x_0+x_1+x_2+x_3=0} \chi_0(x_0)\chi_1(x_1)\chi_2(x_2)\chi_3(x_3)$$

where the sum is over all elements $x_0, x_1, x_2, x_3 \in \mathbb{F}^\times_{q^{u(a)}}$ such that $x_1 + ... + x_n = 0$.

Additionally, $J(qa) = J(a)$ for all $a \in \hat{G}$. For $a = 0$, clearly this is true. Suppose $a \neq 0$. We know $u(qa)$ is the smallest integer $u(qa)$ such that $q^{u(qa)}qa = qa$, which

is the smallest integer $u(a)$ such that $q^{u(a)}a = a$, so $u(qa) = u(a)$. Thus

$$\begin{aligned} J(qa) &= \frac{1}{q^{u(qa)}-1} \sum_{x_0+x_1+x_2+x_3=0} \chi_0(x_0)^q\chi_1(x_1)^q\chi_2(x_2)^q\chi_3(x_3)^q \\ &= \frac{1}{q^{u(a)}-1} \sum_{x_0+x_1+x_2+x_3=0} \chi_0(x_0^q)\chi_1(x_1^q)\chi_2(x_2^q)\chi_3(x_3^q) \\ &= \frac{1}{q^{u(a)}-1} \sum_{x_0+x_1+x_2+x_3=0} \chi_0(x_0)\chi_1(x_1)\chi_2(x_2)\chi_3(x_3) \\ &= J(a) \end{aligned}$$

where the sums are over all elements $x_0, x_1, x_2, x_3 \in \mathbb{F}^\times_{q^{u(a)}}$ such that $x_1 + ... + x_n = 0$. The third equality is due to the fact that $x_0, x_1, x_2, x_3 \in \mathbb{F}^\times_{q^{u(a)}}$, so taking q^{th} powers is an automorphism of $\mathbb{F}^\times_{q^{u(a)}}$. We will prove that the Jacobi sum $J(a)$ is just $q^{u(a)}$, where $d|p^n + 1$ for some positive integer n, and $q = p^f$ is a prime power. We first prove two lemmas.

Lemma 4.3. [Ulm02] *Let b be a rational number between 0 and 1 such that $b \neq \frac{1}{2}$ and suppose that there exist positive integers n and f such that $(p^n + 1)b \in \mathbb{Z}$ and $(p^f - 1)b \in \mathbb{Z}$. Then f is even and $(p^e + 1)b \in \mathbb{Z}$, where $e = gcd(n, f/2)$.*

Proof. Let $b = \frac{c}{d}$, where $\gcd(c, d) = 1$. By the assumptions of the lemma, $d > 2$, $d|p^n + 1$ and $d|p^f - 1$. As $p^n \equiv -1 \mod d$ and $p^f \equiv 1 \mod d$, where $d > 2$, we know f must be even. Additionally,

$$\gcd(p^{2n} - 1, p^f - 1) = p^{\gcd(2n,f)} - 1 = p^{2e} - 1$$

as $p^{2n} - 1 = (p^{2e} - 1)(1 + p + ... + p^{2n-2e})$ and $p^f - 1 = (p^{2e} - 1)(1 + p + ... + p^{f-2e})$. We have $p^{2n} \equiv 1 \mod d$ and $p^f \equiv 1 \mod d$, so $p^{2e} \equiv 1 \mod d$. As $p^n = (p^e)^{\frac{n}{e}} \equiv -1 \mod d$, we know that $\frac{n}{e}$ is odd and so $p^e \equiv -1 \mod d$. So $(p^e + 1)b \in \mathbb{Z}$. □

Lemma 4.4. [Ulm02] *Let $\chi : \mathbb{F}^\times_{p^{2f}} \to \overline{\mathbb{Q}}^\times$ be a non-trivial multiplicative character which is trivial on $\mathbb{F}^\times_{p^f}$. Then $g(\chi, \psi) = -\chi(x)p^f$, where $x \in \mathbb{F}^\times_{p^{2f}}$ is any element such that $Tr_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0$.*

Proof. We first show

$$\sum_{y \in \mathbb{F}^\times_{p^f}} \psi(xy) = \begin{cases} p^f - 1 & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0 \\ -1 & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) \neq 0 \end{cases}$$

where ψ is an additive character such that $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_p}$. By the properties of the field trace (proposition 0.65),

$$\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_p} = \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}.$$

Suppose $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0$. Then if $y \in \mathbb{F}^\times_{p^f}$,

$$\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_p}(xy) = \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(y\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x)) = \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(0) = 0.$$

Therefore

$$\sum_{y\in\mathbb{F}^\times_{p^f}} \psi(xy) = \sum_{y\in\mathbb{F}^\times_{p^f}} \psi_0(0) = p^f - 1.$$

Suppose $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) \neq 0$. Then if $y \in \mathbb{F}^\times_{p^f}$,

$$\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(xy)) = \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(y\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x)) = \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(x'y)$$

where $x' = \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) \neq 0$. We know multiplication by x' permutes the elements in $\mathbb{F}^\times_{p^f}$. Therefore,

$$\sum_{y\in\mathbb{F}^\times_{p^f}} \psi_0(\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(x'y)) = \sum_{y'\in\mathbb{F}^\times_{p^f}} \psi_0(\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(y')) = -1$$

by proposition 0.57, because $\psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}$ is a non-trivial character and because $\psi_0(\mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}(0)) = 1$.

We now have

$$\begin{aligned}
g(\chi,\psi) &= -\sum_{x\in\mathbb{F}^\times_{p^{2f}}} \chi(x)\psi(x) \\
&= -\sum_{x\in\mathbb{F}^\times_{p^{2f}}/\mathbb{F}^\times_{p^f}} \left(\chi(x) \sum_{y\in\mathbb{F}^\times_{p^f}} \psi(xy)\right) \\
&= -\sum_{x\in\mathbb{F}^\times_{p^{2f}}/\mathbb{F}^\times_{p^f}} \chi(x) \begin{cases} p^f - 1 & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0 \\ -1 & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) \neq 0 \end{cases} \\
&= -\chi(x)p^f
\end{aligned}$$

where the second line is due to the fact that χ is trivial on $\mathbb{F}^\times_{p^f}$ and the last line is due to the fact that there is one element x such that $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0$. This is because the dimension of the kernel of $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}$ as a $\mathbb{F}_{p^f}$-linear space is 1. Also we use proposition 0.57, as we use the fact that $\sum_{x\in\mathbb{F}^\times_{p^{2f}}/\mathbb{F}^\times_{p^f}} \chi(x) = 0$ for a non-trivial character χ. □

Proposition 4.5. [Ulm02] *Let $J(a)$ be as before. Suppose $d|p^n + 1$ for some positive integer n and let $q = p^f$. Then for all $a \in \hat{G}'$, $J(a) = q^{u(a)}$.*

Proof. Suppose $a = 0$. Then $J(a) = q$ and as $u(a) = 1$, so the proposition holds.

Suppose $a = (d/2, d/2, d/2, d/2)$. As $\frac{q-1}{2}d \equiv 0 \mod d$, we know $u(a) = 1$ and $J(a) = (1/q)g(t^{\frac{q-1}{2}}, \psi)^4$. The Gauss sum $g(t^{\frac{q-1}{2}}, \psi)$ is by definition a quadratic Gauss sum and so by proposition 0.61, $g(t^{\frac{q-1}{2}}, \psi)^4 = q^2$, so $J(a) = q$ and the proposition holds.

Suppose $a \neq 0$ and $a \neq (d/2, d/2, d/2, d/2)$. We know that $0 < \frac{a_i}{d} < 1$ and so by lemma 4.3, $u(a)$ is even. Also by lemma 4.3, if we let $e = \gcd(n, u(a)/2)$, then $(p^e + 1)(a_i/d) \in \mathbb{Z}$ and $p^{2e} \equiv 1 \mod d$.

We firstly show that we can write $t^{\frac{\left(q^{u(a)}-1\right)a_i}{d}}$ as $t^{\frac{\left(q^{2e}-1\right)a_i}{d}} \circ N_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}$ where N is the field norm.

$$\begin{aligned} t^{\frac{\left(q^{2e}-1\right)a_i}{d}}\left(N_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}(x)\right) &= t^{\frac{\left(q^{2e}-1\right)a_i}{d}}\left(x x^{q^{2e}} x^{q^{2\cdot 2e}} x^{q^{3\cdot 2e}} \ldots x^{q^{u(a)-2e}}\right) \\ &= t^{\frac{\left(q^{2e}-1\right)\left(q+q^{2e}+q^{2\cdot 2e}+\ldots+q^{u(a)-2e}\right)a_i}{d}}(x) \\ &= t^{\frac{\left(q^{u(a)-1}\right)a_i}{d}}(x) \end{aligned}$$

Let $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}$, where $\psi_0 : \mathbb{F}_{q^{2e}} \to \overline{\mathbb{Q}}^{\times}$ is a non-trivial additive character. Then

$$\begin{aligned} g\left(t^{\frac{\left(q^{u(a)}-1\right)a_i}{d}}, \psi\right) &= -\sum_{x \in \mathbb{F}^{\times}_{q^{u(a)}}} t^{\frac{\left(q^{u(a)}-1\right)a_i}{d}}(x)\psi(x) \\ &= -\sum_{x \in \mathbb{F}^{\times}_{q^{u(a)}}} t^{\frac{\left(q^{2e}-1\right)a_i}{d}}\left(N_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}(x)\right)\psi_0\left(\mathrm{Tr}_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}(x)\right) \\ &= \left(-\sum_{x \in \mathbb{F}^{\times}_{q^{2e}}} t^{\frac{\left(q^{2e}-1\right)a_i}{d}}(x)\psi_0(x)\right)^{\frac{u(a)}{2e}} \end{aligned}$$

where the last line is due to the Hasse-Davenport relation (theorem 0.66). Additionally, the character $t^{\frac{\left(q^{2e}-1\right)a_i}{d}}$ acts trivially on $\mathbb{F}^{\times}_{q^e}$. Suppose $x \in \mathbb{F}^{\times}_{q^e}$. Then

$$t^{\frac{\left(q^{2e}-1\right)a_i}{d}}(x) = t^{\frac{\left(q^{e}+1\right)a_i}{d}}\left(x^{q^e-1}\right) = t(1) = 1$$

as $(p^e + 1)\frac{a_i}{d} \in \mathbb{Z}$. By lemma 4.4, if we choose $y \in \mathbb{F}^{\times}_{q^{2e}}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^{2e}}/\mathbb{F}_{q^e}}(y) \neq 0$, then

$$\left(-\sum_{x \in \mathbb{F}^{\times}_{q^{2e}}} t^{\frac{\left(q^{2e}-1\right)a_i}{d}}(x)\psi_0(x)\right)^{\frac{u(a)}{2e}} = \left(-t^{\frac{\left(q^{2e}-1\right)a_i}{d}}(y)q^e\right)^{\frac{u(a)}{2e}} = \left(-t^{\frac{\left(q^{2e}-1\right)a_i}{d}}(y)\right)^{\frac{u(a)}{2e}} q^{\frac{u(a)}{2}}$$

The Jacobi sum $J(a)$ is $J(a) = \frac{1}{q^{u(a)}}q^{2u(a)} = q^{u(a)}$. □

We relate this Jacobi sum to the action of the Frobenius map on $H^2_{\text{ét}}(\mathcal{F}_d/\Gamma, \mathbb{Q}_l)$.

4.1.2 The Action of the Frobenius on $H^2_{\text{ét}}(\mathcal{F}_d, \mathbb{Q}_l)$

Let $H^2(X) = H^2_{\text{ét}}(X, \mathbb{Q}_l)$ for a variety X over a field K.

Suppose $a \in \hat{G}$, where $\hat{G}$ is as before. Let $H^2(\mathcal{F}_d)(a) \subset H^2(\mathcal{F}_d)$ be the space of classes $c \in H^2(\mathcal{F}_d)$ such that $z^*(c) = a(z)c$ for all $z \in G$, where G is as before. Let $qa = (qa_0, qa_1, qa_2, qa_3)$ and let $z^q = [\zeta_0^q, \zeta_1^q, \zeta_2^q, \zeta_3^q]$.

Lemma 4.6. *Let $u(a)$ be as before, the smallest positive integer such that $q^{u(a)}a = a$. Then $(Fr^{u(a)})^*$ sends $H^2(\mathcal{F}_d)(a)$ to itself for each $a \in \hat{G}$.*

Proof. We firstly show $\mathrm{Fr}^*(H^2(\mathcal{F}_d)(a)) \subset H^2(\mathcal{F}_d)(qa)$.

Suppose $c \in H^2(\mathcal{F}_d)(a)$. Then

$$\begin{aligned} z^*(\mathrm{Fr}^*(c)) &= (\mathrm{Fr} \circ z)^*(c) \\ &= (z^q \circ \mathrm{Fr})^*(c) \\ &= \mathrm{Fr}^*((z^q)^*(c)) \\ &= \mathrm{Fr}^*(a(z^q)c) \\ &= \mathrm{Fr}^*((qa)(z)c) \\ &= (aq)(z)\mathrm{Fr}^*(c) \end{aligned}$$

where the last equality is due to the linearity of Fr^*. Therefore, Fr^* sends $H^2(\mathcal{F}_d)(a)$ to $H^2(\mathcal{F}_d)(qa)$ and so $(\mathrm{Fr}^{u(a)})^*$ sends $H^2(\mathcal{F}_d)(a)$ to $H^2(\mathcal{F}_d)(q^{u(a)}a) = H^2(\mathcal{F}_d)(a)$. □

We do not prove the following theorem of Shioda, as it requires knowledge of a number of topics outside the scope of this project. Specifically, the proof uses étale cohomology theory. We explain why statements 1 and 2 imply statement 3 and explain a corollary of this theorem.

Theorem 4.7. [Ulm02] *Let $\mathcal{F}_d$ be the Fermat surface of degree d over $\mathbb{F}_q$ and let $\hat{G}'$ and $J(a)$ be as before.*

1. $H^2(\mathcal{F}_d)(a) = 0$ if $a \notin \hat{G}'$ and is 1-dimensional if $a \in \hat{G}'$.

2. If $a \in \hat{G}'$, then $(Fr^{u(a)})^*$ acts on $H^2(\mathcal{F}_d)(a)$ by multiplication by $J(a)$.

3. If $a \in \hat{G}'$, then the characteristic polynomial of Fr^* on $\bigoplus_{i=1}^{u(a)-1} H^2(\mathcal{F}_d)(q^i a)$ is equal to $(1 - J(a)T^{u(a)})$.

Proof of 1 and 2 $\implies$ 3. Suppose $a \in \hat{G}'$. The Frobenius map is a linear transformation on

$$\bigoplus_{i=0}^{u(a)-1} H^2(\mathcal{F}_d)(q^i a).$$

By (1), each $H^2(\mathcal{F}_d)(q^i a)$ is a 1-dimensional space. Therefore, the Frobenius map $\mathrm{Fr}^* : H^2(\mathcal{F}_d)(q^i a) \to H^2(\mathcal{F}_d)(q^{i+1}a)$ must be an isomorphism. By (2), $(\mathrm{Fr}^{u(a)})^*$ acts on $H^2(\mathcal{F}_d)(a)$ by multiplication by $J(a)$. Therefore, the Frobenius map Fr^* can be represented by the $(u(a)-1 \times u(a)-1)$ matrix

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & J(a) \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

The characteristic polynomial of this matrix is $(1 - J(a)T^{u(a)})$. □

This proposition allows us to relate the zeta-function of the Fermat surface to Jacobi sums, and by proposition 4.5, we know that if $d|p^n + 1$ for some positive integer n, then the Jacobi sum $J(a) = q^{u(a)}$.

Corollary 4.8. [Ulm02] *Let $\Gamma^\perp \subset \hat{G}$ be the set of characters trivial on $\Gamma \subset G$. Let $A_1, ..., A_k$ be the orbits of multiplication by q on $\Gamma^\perp \cap \hat{G}'$ and choose $a_i \in A_i$. Then*

$$P_2(\mathcal{F}_d/\Gamma, T) = \prod_{i=1}^{k}(1 - J(a_i)T^{u(a_i)}).$$

Proof. We know $H^i(\mathcal{F}_d/\Gamma) = H^i(\mathcal{F}_d)^\Gamma$ by [Mil80, III Th. 2.20]. By the first part of proposition 4.7, we only need to consider $H^2(\mathcal{F}_d)(a)$ where $a \in \Gamma^\perp \cap \hat{G}'$ when evaluating the characteristic polynomial

$$P_2(\mathcal{F}_d/\Gamma, T) = \det(1 - T\mathrm{Fr}^* | H^2(\mathcal{F}_d)^\Gamma).$$

However, proposition 4.7 tells us that

$$P_2(\mathcal{F}_d/\Gamma, T) = \prod_{i=1}^{k}(1 - J(a_i)T^{u(a_i)})$$

where the a_is are representatives of each orbit of multiplication by q in $\Gamma^\perp \cap \hat{G}'$. □

By proposition 4.5 and corollary 4.8, we can write

$$P_2(\mathcal{F}_d/\Gamma, T) = \prod_{i=1}^{k}(1 - q^{u(a_i)}T^{u(a_i)}).$$

Therefore

$$-\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) = -\mathrm{ord}_{s=1}\left(\frac{1}{\prod_{i=1}^{k}(1 - q^{u(a_i)}q^{-s(u(a_i))})}\right) = k \qquad (4.1)$$

as only the order of vanishing of $P_2(\mathcal{F}_d/\Gamma, T)$ contributes to the order of vanishing at $s = 1$ of the zeta-function of $\mathcal{F}_d/\Gamma$. Note that k is the number of orbits in $\Gamma^\perp \cap \hat{G}'$ of multiplication by q. Therefore, it is possible to express the order of vanishing of the zeta-function of $\mathcal{F}_d/\Gamma$ in terms of only q and d. We now find an expression for the rank of $E(\mathbb{K})$ is terms of q and d.

4.2 A Lower Bound for the Rank of $E(\mathbb{K})$

Theorem 4.9. [Ulm02] *Let p be a prime, n a positive integer and d a divisor of $p^n + 1$. Let q be a power of p and let E be the elliptic curve over $\mathbb{F}_q(t)$ defined by*

$$y^2z + xyz = x^3 - t^d z^3.$$

Then the j-invariant of E is not in $\mathbb{F}_q$, the conjecture of Birch and Swinnerton-Dyer holds for E and the rank of $E(\mathbb{F}_q(t))$ is

$$\sum_{\substack{e|d \\ e\nmid 6}} \frac{\varphi(e)}{o_e(q)} + \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } \mu_4 \notin k \\ 1 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3|d \text{ and } \mu_3 \notin k \\ 2 & \text{if } 3|d \text{ and } \mu_3 \subset k \end{cases}$$

Here $\varphi(e)$ is the cardinality of $(\mathbb{Z}/e\mathbb{Z})^\times$ and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

Proof. The j-invariant of E is $1/(t^d(1 - 2^4 3^3 t^d))$, so is not in $\mathbb{F}_q$, therefore E is not isotrivial. In section 3.2.3, we proved that the Birch and Swinnerton-Dyer conjecture holds for E. It remains to evaluate the rank of $E(\mathbb{F}_q(t))$. We know by corollary 4.1 that $-\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s))$ is just the number of orbits of multiplication by q in $\Gamma^\perp \cap \hat{G}'$ and we know by equation 3.4

$$\mathrm{Rank}(E(\mathbb{K})) = -\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) - 1 + A$$

where A depends on q and d and is a number between 0 and 3. Therefore, it remains only to compute the number of orbits of multiplication by q in $\Gamma^\perp \cap \hat{G}'$.

The set of characters $\Gamma^\perp$ is the cyclic subgroup of $\hat{G}$ generated by $(3, -6, 2, 1)$, because

$$\Gamma = \left\{ [\zeta_0, \zeta_1, \zeta_2, \zeta_3] | \zeta_0^3 \zeta_1^{-6} \zeta_2^2 \zeta_3 = 1 \right\} \subset G.$$

Moreover,

$$\hat{G}' = \{ a \in \hat{G} \mid a = 0 \text{ or } a = (a_0, a_1, a_2, a_3) \text{ with } a_i \neq 0 \}.$$

so the set $\Gamma^\perp \cap \hat{G}'$ is in bijective correspondence with

$$\{ a_3 \in \mathbb{Z}/d\mathbb{Z} \mid 6a_3 \neq 0 \} \cup \{0\}$$

The size of the orbit of a_3 in $(\mathbb{Z}/d\mathbb{Z})^\times$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$, where $e = \frac{d}{\gcd(d,a_3)}$. So

$$-\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) = \sum_{\substack{e|d \\ e\nmid 6}} \frac{\varphi(e)}{o_e(q)} + 1$$

where $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$ and φ is the Euler totient function, so $\varphi(e)$ is the number of elements in $(\mathbb{Z}/e\mathbb{Z})^\times$. Adding 1 in this equation corresponds to the orbit of $a = 0$.

By equation 3.4,

$$\begin{aligned} \mathrm{Rank}(E(\mathbb{K})) &= -\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) - 1 + A \\ &= \sum_{\substack{e|d \\ e\nmid 6}} \frac{\varphi(e)}{o_e(q)} + A \end{aligned} \tag{4.2}$$

where

$$A = \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } \mu_4 \notin k \\ 1 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3|d \text{ and } \mu_3 \notin k \\ 2 & \text{if } 3|d \text{ and } \mu_3 \subset k \end{cases}$$

□

We now specialise to particular choices of q and d, to provide some simple, explicit calculations of the rank of $E(\mathbb{K})$. In all the following examples, assume q is a power of p and $d|p^n + 1$ for some positive integer n.

Example 4.10. Assume $q = p$. As $p^n + 1 \equiv 0 \mod d$, $p^n \equiv -1 \mod d$ and so $p^{2n} \equiv 1 \mod d$. Thus the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$ is less than or equal to $2n$. For all e such that $e|d$, the order of p in $(\mathbb{Z}/e\mathbb{Z})^\times$ must also be less than or equal to $2n$. The Euler totient function $\varphi(e)$ outputs the number of integers coprime to e and by Euler's formula

$$\sum_{e|d} \varphi(e) = d.$$

As the sum in equation 4.2 is over all e such that $e \nmid 6$,

$$\sum_{\substack{e|d \\ e\nmid 6}} \varphi(e) = d - 2 = p^n - 1$$

as $1, 2|d$ and $\varphi(1) + \varphi(2) = 2$. This gives the inequality

$$-\mathrm{ord}_{s=1}(\zeta(\mathcal{F}_d/\Gamma, s)) = \sum_{\substack{e|d \\ e\nmid 6}} \frac{\varphi(e)}{o_e(q)} + 1 \geq \frac{p^n - 1}{2n} + 1.$$

By equation 4.2,

$$\begin{aligned}\text{Rank}(E(K)) &= \sum_{\substack{e|d \\ e\nmid 6}} \frac{\varphi(e)}{o_e(q)} + A \\ &\geq \frac{p^n - 1}{2n}\end{aligned}$$

remembering that A is a number between 0 and 3. This is a lower bound for the rank of $E(\mathbb{F}_p(t))$, where p is prime and $d|p^n + 1$.

Example 4.11. Assume $q = (p^{2n})^f$. Then $q \equiv 1 \mod d$ so $o_e(q) = 1$. Additionally, assume $6|d$. Using Euler's formula,

$$\sum_{\substack{e|d \\ e\nmid 6}} \varphi(e) = d - 6 = p^n - 5$$

Also, if $6|d$, then $2|d$ and $(p^{2n})^f \equiv 1 \mod 4$, so $4|(p^{2n})^f - 1$. We have $3|d$ and $(p^{2n})^f \equiv 0$ or $1 \mod 3$, but as $p \neq 3$, $(p^{2n})^f \equiv 1 \mod 3$. Thus $3|(p^{2n})^f - 1$. Hence $A = 3$ and

$$\text{Rank}(E(K)) = p^n - 2.$$

Example 4.12. Assume $q = (p^{2n})^f$ and $6 \nmid d$. Using Euler's formula,

$$\sum_{\substack{e|d \\ e\nmid 6}} \varphi(e) = d - 2 = p^n - 1$$

As $2|d$ and $(p^{2n})^f \equiv 1 \mod 4$, we know $4|(p^{2n})^f - 1$. However, $3 \nmid d$ and so $A = 1$. Thus

$$\text{Rank}(E(K)) = p^n.$$

If $E : y^2 + xy = x^3 - t^d$ is an elliptic curve defined over $\mathbb{F}_q(t)$, where q is a power of $p \neq 2, 3$ and for some positive integer n, $d|p^n + 1$, then we can find a lower bound for the rank of $E(\mathbb{F}_q(t))$ in terms of q and d. Thus clever choices of q and d will give elliptic curves of arbitrarily large rank. For example, if $6 \nmid d$ and $q = (p^{2n})^f$ for $p \neq 2, 3$, then $\text{Rank}(E(\mathbb{F}_q(t))) = p^n$.

4.3 Remarks

In [Ulm02], Ulmer proves that there exist non-isotrivial elliptic curves of arbitrarily large rank over function fields of finite fields. We follow Ulmer's construction for elliptic curves over $\mathbb{F}_q(t)$, where q is not of characteristic 2 or 3. Ulmer showed

that the problem of evaluating the rank of a specific type of elliptic curve $E(\mathbb{K})$ could be reduced to evaluating the order of vanishing of the zeta-function of some quotient of a Fermat surface by a group. Potentially the same technique could be used for other elliptic curves defined over $\mathbb{K}$. Any elliptic curve $E/\mathbb{K}$ can be associated to an elliptic surface $\mathcal{E}/\mathbb{k}$. Tate's algorithm can be used to understand the geometric properties of $\mathcal{E}/\mathbb{k}$, particularly the structure of the bad fibres of $\mathcal{E}$. There is a relation between the Néron-Severi group of $\mathcal{E}$ and the Mordell-Weil group of E, thus understanding the rank of one of these groups is understanding the rank of the other.

The special property of Ulmer's choice of elliptic curve is that there exists a dominant rational map from a Fermat surface to the associated elliptic surface. This implies that the Tate conjecture as well as the Birch and Swinnerton-Dyer conjecture hold for the elliptic curve. The zeta-functions of Fermat surfaces are well-known, though the zeta-function of a quotient of a Fermat surface by a group may be difficult to explicitly compute.

The existence of an explicit lower bound for the rank of $E(\mathbb{F}_q(t))$ suggests something similar may be true for the rank of an elliptic curve E defined over $\mathbb{Q}$. The lower bound for the elliptic curve $E : y^2z + xyz = x^3 - t^dz^3$ over $\mathbb{F}_q(t)$ suggests two ways to increase the rank of E. One way is to increase the value of q, and the other way is to increase the value of d. Increasing the value of q to find elliptic curves over $\mathbb{F}_q(t)$ does not really have a direct analogue for elliptic curves over $\mathbb{Q}$, as we do not wish to change the ground field $\mathbb{Q}$. However, changing the value of the coefficients of an elliptic curve over $\mathbb{Q}$ is a direct analogue of increasing the value of d. Increasing the value of d increases the number of divisors of the discriminant and hence the number of points of bad reduction on $E/\mathbb{K}$. This suggests elliptic curves over $\mathbb{Q}$ of large rank have large discriminants with many divisors.

Bibliography

[Cho55] Wei-Liang Chow, *Abelian varieties over function fields*, Trans. Am. Math. Soc. **78** (1955), 237–275.

[FW89] William Fulton and Richard Weiss, *Algebraic curves: an introduction to algebraic geometry*, vol. 3, Addison-Wesley Redwood City California, 1989.

[Har77] Robin Hartshorne, *Algebraic geometry*, no. 52, Springer, 1977.

[Hat02] Allen Hatcher, *Algebraic topology*, Cambridge University Press, 2002.

[IR82] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1982.

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math **78** (1956), no. 3, 555–563.

[Lan02] ———, *Algebra revised third edition*, Springer-Verlag, New York, 2002.

[Mil80] James S. Milne, *Étale cohomology*, no. 33, Princeton University Press, New Jersey, 1980.

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Springer-Verlag, 2002.

[Shi72] Tetsuji Shioda, *On elliptic modular surfaces*, Journal of the Mathematical Society of Japan **24** (1972), no. 1, 20–59.

[Shi99] ———, *Mordell-weil lattices for higher genus fibration over a curve*, London Mathematical Lecture Note Series (1999), 359–374.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[SK79] Tetsuji Shioda and Toshiyuki Katsura, *On fermat varieties*, Tohoku Mathematical Journal **31** (1979), no. 1, 97–115.

[ST67] Igor R. Shafarevich and John Tate, *The rank of elliptic curves*, AMS Transl **8** (1967), 917–920.

[Tat75] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable IV, Springer, 1975, pp. 33–52.

[Tat94] ———, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991) **55** (1994), 71–83.

[Ulm02] Douglas Ulmer, *Elliptic curves with large rank over function fields*, Annals of mathematics (2002), 295–315.

[Ulm09] ———, *Elliptic curves over function fields*, IAS/Park City Math. Ser **18** (2009), 211–280.