university of groningen / faculty of science and engineering / mathematics and applied mathematics

On the rank of $y^2 = x^3 + t^{360} + 1$ over $\mathbb{Q}(t)$

Bachelor's Project Mathematics

November 2024

Student: J.S. Pearson

First supervisor: Jaap Top

Second assessor: Cecília Salgado

1 Introduction

This paper considers the elliptic curve given by

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

It is a result from Shioda [Shi92] that the rank of E_{360} over $\overline{\mathbb{Q}}(t)$ is equal to 68. This is the highest rank elliptic curve over a function field of characteristic 0 that we know of. In this paper we determine the rank of E_{360} over the field it is defined on, $\mathbb{Q}(t)$.

We assume the result, rank $E_{360}(\overline{\mathbb{Q}}(t)) = 68$. We use a vectorspace decomposition to obtain elliptic curves with polynomial coefficients of lower degree, the sum of whose ranks equal the rank of $E_{360}(\overline{\mathbb{Q}}(t))$. We determine the ranks of rational elliptic surfaces, over $\overline{\mathbb{Q}}(t), \mathbb{F}_p(t)$, and $\mathbb{Q}(t)$. The last subsection considers the rank of a K3 surface over $\mathbb{F}_p(t)$ and $\mathbb{Q}(t)$. With this information we conclude the rank of $E_{360}(\mathbb{Q}(t))$.

2 Background

2.1 Algebraic Geometry

Here we briefly review some basic algebraic geometry, from Algebraic Geometry [Har77] Chapter I and The Arithmetic of Elliptic Curves [Sil09] Chapters I and II.

Definition 2.1. An **affine algebraic variety** is an irreducible closed subset of $\mathbb{A}^n$ with the induced topology. A **projective algebraic variety** is an irreducible set in $\mathbb{P}^n$ with the induced topology.

We take algebraic curves to be projective varieties of dimension one.

Definition 2.2. A function $f : Y \to k$ is **regular at a point** $P \in Y$ if there is an open neighbourhood U with $P \in U \subseteq Y$, and polynomials $g, h \in A := k[x_1, ..., x_n]$, such that h is nowhere zero on U, and $f = g/h$ on U. We say that f is **regular on** Y if it is regular at every point of Y.

Definition 2.3. Let k be an algebraically closed field. If X and Y are two varieties, a **morphism** $\phi : X \to Y$ is a continuous map such that for every open set $V \subseteq Y$, and for every regular function $f : V \to k$, the function $f \circ \phi : \phi^{-1}(V) \to k$ is regular.

Definition 2.4. If Y is a variety, we define the **function field** $K(Y)$ of Y as follows. An element of $K(Y)$ is an equivalence class of pairs $< U, f >$ where U is a nonempty open subset of Y, f is a regular function on U, and where we identify two pairs $< U, f >$ and $< V, g >$ if $f = g$ on $U \cap V$. The elements of $K(Y)$ are called **rational functions** on Y.

Theorem 2.1. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Proof. See [Sil09] Theorem II.2.3. □

We state Corollary I.6.12 from [Har77], as it will prove relevant.

Theorem 2.2. *The following three categories are equivalent:*
(i) quasi-projective curves, and dominant rational maps;
(ii) function fields of dimension 1 over k, and k-homomorphisms.
(iii) nonsingular projective curves, and dominant morphisms;

The formal versions of the following definitions require background that is generally not important for the purposes of this paper. Thus we shall give simplified and hopefully more intuitive definitions.

Definition 2.5. The **fibre** over a point $y \in Y$, of a morphism $f : X \to Y$, is the preimage of the singleton set,

$$f^{-1}(\{y\}) = \{x : f(x) = y\}.$$

Definition 2.6. The **genus** of an algebraic variety is a nonnegative integer which is invariant under birational equivalence.

2.2 Elliptic Curves

This paper analyses a particular elliptic curve and the rank of its group. The following background is a summary of the relevant parts of [Sil09] Chapter III.

Definition 2.7. An **elliptic curve** is a smooth projective curve of genus 1 equipped with a chosen point on it.

We usually study elliptic curves by their Weierstrass equations, of the form

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

For convenience we will write the Weierstrass equation using non-homogeneous coordinates,

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

For the purposes of this paper we will be working over fields of characteristic not 2 or 3, which allows us to put any elliptic curve into what is a called **short Weierstrass form**,

$$y^2 = x^3 + Ax + B.$$

Let us set some notation. Considering an elliptic curve E and a field K, when we write,

$$E/K,$$

we are referring to the curve E being defined over K, meaning the coefficients $a_i \in K$. When we write,

$$E(K),$$

we are referring to the set of points on E, whose coordinates are elements of K. The set $E(K)$ forms a group. The identity element of the group is the 'chosen point' the elliptic curve is equipped with. This is the projective point at infinity, that is, the point on every vertical line at which they all intersect. In homogeneous coordinates we write it as $[0 : 1 : 0]$. We will denote it by $\mathcal{O}$.

The addition of two points P and Q on an elliptic curve E is defined as follows. The line through P and Q will intersect E at a third point which we reflect across the axis of symmetry of E. This reflection is what we define to be $P+Q$. The inverse of a point P will be its reflection across the axis of symmetry. For E in short Weierstrass form, the axis of symmetry will be the x-axis. Thus a point $P = (x, y)$ on E will have inverse, $-P = (x, -y)$.

Theorem 2.3. *Let E/K be an elliptic curve. The group law on E defines morphisms,*

$$+ : E \times E \to E \qquad\qquad - : E \to E$$
$$(P_1, P_2) \mapsto P_1 + P_2, \qquad\qquad P \mapsto -P.$$

In this paper we will be considering elliptic curves defined over function fields, and as such cannot be visualised the same as a curve with coefficients over some subset of $\mathbb{R}$. Let K be a number field, that is, a finite degree extension of $\mathbb{Q}$. Let E/K be an elliptic curve.

Theorem 2.4 (Mordell-Weil)**.** *The group $E(K)$ is finitely generated.*

It follows immediately from the fundamental theorem of finitely generated abelian groups that

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

for some powers of primes $q_j = p_j^{e_j}$. The finite part is called the torsion. In this paper we are concerned with determining r, known as the **Mordell-Weil rank**, or just the **rank** of the group $E(K)$.

Let us define some quantities which will be relevant for the study of these curves.

Definition 2.8. The **discriminant** Δ of an elliptic curve in short Weierstrass form is given by,

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

We require that $\Delta \neq 0$, as this is equivalent to the curve being nonsingular.

It is natural to study maps between elliptic curves that preserve the identity element.

Definition 2.9. Let E_1 and E_2 be elliptic curves. An **isogeny** from E_1 to E_2 is a morphism

$$\phi : E_1 \to E_2 \quad \text{satisfying} \quad \phi(\mathcal{O}) = \mathcal{O}.$$

Two elliptic curves E_1 and E_2 are **isogenous** if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{\mathcal{O}\}$. When both elliptic curves E_1, E_2, and the map itself, ϕ, are defined over a field K, we call ϕ a K-isogeny.

Theorem 2.1 implies that either

$$\phi(E_1) = \{\mathcal{O}\} \quad \text{or} \quad \phi(E_1) = E_2.$$

Theorem III.4.8 of [Sil09] tells us that any isogeny is a group homomorphism, and Corollary III.4.9 tells us its kernel is finite when ϕ is not the zero map. Isomorphisms of elliptic curves are given by bijective isogenies. Consider elliptic curves in short Weierstrass form, over a field K with $char \neq 2, 3$. Proposition III.1.4(b) of [Sil09] tells us a map is an isomorphism of elliptic curves if and only if it is a change of coordinates of the form

$$x = u^2 x' \quad \text{and} \quad y = u^3 y' \quad \text{for some } u \in \overline{K}^{\times}.$$

Example 2.1 (Multiplication by m)**.** We call the addition of a point P to itself $m \in \mathbb{Z}_{>0}$ times, a 'multiplication' by m. Consider the map,

$$\begin{aligned}[m] : E &\to E \\ P &\mapsto mP.\end{aligned}$$

We extend this idea to all $m \in \mathbb{Z}$, for negative m defining $[m](P) = [|m|](-P)$, and putting $[0](P) = \mathcal{O}$. Theorem 2.3 allows us to conclude by induction that this map is a morphism. Since $[m](\mathcal{O}) = \mathcal{O}$ for any m, it must also be an isogeny.

As all isogenies are morphisms, they can be written as rational maps of the form

$$(x, y) \mapsto \Big(\frac{g_1(x,y)}{g_2(x,y)}, \frac{h_1(x,y)}{h_2(x,y)}\Big),$$

where g_1, g_2, h_1, h_2 are polynomials with coefficients in the field K which E is defined over. We can assume without loss of generality that the numerators and denominators are coprime. By isogenies being group homomorphisms, for equations in short Weierstrass form we must have,

$$\Big(\frac{g_1(x,-y)}{g_2(x,-y)}, \frac{h_1(x,-y)}{h_2(x,-y)}\Big) = \Big(\frac{g_1(x,y)}{g_2(x,y)}, -\frac{h_1(x,y)}{h_2(x,y)}\Big).$$

This implies g_1 and g_2 do not depend on y, and that $\frac{h_1(x,y)}{h_2(x,y)} = y\frac{f_1(x)}{f_2(x)}$ for some coprime polynomials f_1, f_2. Thus we may write any arbitrary nonzero isogeny as a map of the form

$$(x, y) \mapsto \Big(\frac{g_1(x)}{g_2(x)}, y\frac{f_1(x)}{f_2(x)}\Big).$$

Definition 2.10. The **degree** of an isogeny ϕ, is given by,

$$deg\, \phi = [K(x) : K\Big(\frac{g_1(x)}{g_2(x)}\Big)].$$

Theorem 2.5. *Let $f : E_1 \to E_2$ be an isogeny of degree m. Then there exists a unique isogeny, $\hat{f} : E_2 \to E_1$, called the* ***dual isogeny****, such that $f \circ \hat{f} = [m]$.*

Proof. See [Sil09] section III.6. □

Theorem 2.6. *For two elliptic curves E_1, E_2, if there exists a K-isogeny $f : E_1 \to E_2$, then $E_1(K)$ and $E_2(K)$ have the same rank.*

Proof. By f being an isogeny, it must have finite kernel. This implies f is injective on the torsionfree part, hence $r(E_2(K)) \geq r(E_1(K))$. By Theorem 2.5 we know there exists $\hat{f}$, the dual isogeny of f. Thus the reverse holds, $r(E_1(K)) \geq r(E_2(K))$, and we conclude $r(E_1(K)) = r(E_2(K))$. □

Example 2.2 (Quadratic Twist)**.** Let $L := K(\sqrt{d})$ be a quadratic field extension with $d \in K^\times$. We shall consider an elliptic curve defined over K,

$$E : y^2 = x^3 + Ax + B.$$

The map $(x, y) \mapsto (x, \sqrt{d}y)$ defines an L-isogeny. This gives us the isogenous curve

$$E' : dy^2 = x^3 + Ax + B.$$

By Theorem 2.6 we know rank $(E(L)) =$ rank $(E'(L))$. We can put this back into short Weierstrass form by multiplying across by d^3 and making another change of coordinates (a K-isogeny),

$$d^4y^2 = d^3x^3 + d^3Ax + d^3B,$$
$$(d^2y)^2 = (dx)^3 + d^2A(dx) + d^3B,$$
$$E' : y'^2 = x'^3 + d^2Ax' + d^3B.$$

E' is called the **quadratic twist** of E.

Lemma 2.7.

$$\textit{rank } (E(L)) = \textit{rank } (E(K)) + \textit{rank } (E'(K))$$

Proof. This proof works by vectorspace decomposition, a method which we will study in greater detail in the next section.

Every quadratic extension is Galois. Let us consider $Gal(L/K)$. We know it is cyclic of order 2, and is generated by some element τ which sends $\sqrt{d} \mapsto -\sqrt{d}$.

By $E(L)$ being an abelian group, it is also a $\mathbb{Z}$-module. We can also consider $\mathbb{Q}$ to be a $\mathbb{Z}$-module, and their tensor product $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$ results in another $\mathbb{Z}$-module. We have for any $P \in E(L)$, $r \in \mathbb{Q}$, and $n \in \mathbb{Z}$, that

$$(nP) \otimes r = P \otimes (nr) = n(P \otimes r).$$

Suppose P is a torsion point of order n. Then for any element of $P \otimes r \in E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$, by $r \in \mathbb{Q}$, we can write $r = n\frac{r}{n}$. Then we have,

$$P \otimes r = P \otimes n\frac{r}{n} = nP \otimes \frac{r}{n} = \mathcal{O} \otimes \frac{r}{n} = 0(P \otimes r)$$

This shows that tensoring with $\mathbb{Q}$ sends all torsion points of $E(L)$ to zero. Thus the dimension of the vectorspace $V := E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$ is the rank of the group $E(L)$.

We shall consider the action of the Galois group on this vectorspace. The Galois group acts trivially on the elements of $E(K) \otimes_{\mathbb{Z}} \mathbb{Q} =: V^+$. The only other way the Galois group can act is by sending points to their inverse, $\tau(P) = -P$. We shall call the subspace consisting of points tensor a rational, which are acted upon in this way, V^-. Let us consider an arbitrary element of $P \otimes r \in V^-$. To consider the coordinates of P without r we need to remember we will regain any torsion points which were sent to zero by the tensoring. However, we will see in Section 3.3 that the curves which we deal with are torsion-free, so this need not concern us regarding this paper. We write the following for $P = (x, y)$,

$$(\tau(x), \tau(y)) = (x, -y) \mod \textit{torsion}.$$

Thus we are looking for coordinates satisfying $x \in K$, $y = a\sqrt{d}$ for $a \in K$. The L-isogeny given in the above example gives us a curve with only points of this form. Thus we conclude $V^- = E'(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. The dimension of V is exactly the rank of $E(L)$, and the dimensions of V^+, V^- are rank $(E(K))$ and rank $(E'(K))$ respectively. □

Example 2.3 (Frobenius Endomorphism)**.** Let K be a field of positive characteristic p. Let $q = p^r$ and let E/K be an elliptic curve. We define the curve $E^{(q)}/K$ by raising the coefficients of the equation for E to the power q. Define the Frobenius morphism ϕ_q by,

$$\phi_q : E \to E^{(q)}$$
$$(x, y) \mapsto (x^q, y^q).$$

Note the qth power map $K \to K$ is a homomorphism, so we have,

$$\Delta(E^{(q)}) = 4(A^q)^3 + 27(B^q)^2 = (4A^3)^q + (27B^2)^q = \Delta(E)^q.$$

This tells us the equation for $E^{(q)}$ is nonsingular and thus $E^{(q)}$ is an elliptic curve.

Now let $K = \mathbb{F}_q$. Then the qth power map on K is the identity, so $E^{(q)} = E$. Furthermore ϕ_q is an endomorphism of E, called the **Frobenius endomorphism**. The set of points fixed by ϕ_q is exactly the group $E(\mathbb{F}_q)$.

2.3 Elliptic Surfaces

This section is a summary of relevant parts of Elliptic Surfaces [SS10].

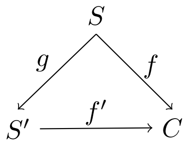
Definition 2.11. Let C be a smooth projective curve over $k = \bar{k}$. An **elliptic surface** S over C is a smooth projective surface S with an elliptic fibration over C, i.e. a surjective morphism

$$f : S \to C,$$

such that,

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

2) the morphism f is 'minimal', meaning; for S' smooth, with f' satisfying 1), there exists no finite morphism g of degree less than or equal to 2 such that the following diagram commutes.



Suppose we have an elliptic curve E over the function field $k(C)$ of a curve C. The **Kodaira Néron model** describes how to associate an elliptic surface $S \to C$ over k to E whose generic fibre returns exactly to E. The model is unique; there is a one-to-one correspondence between elliptic surfaces over C modulo isomorphism, and elliptic curves over $k(C)$ modulo isomorphism,

$$\{\text{elliptic surfaces}/C\}/\cong \;\leftrightarrow\; \{\text{elliptic curves}/k(C)\}/\cong .$$

Any $E/k(C)$ gives rise to a unique elliptic surface with generic fibre E. Any elliptic surface $f : S \to C$ gives rise to a unique $E/k(C)$.

Definition 2.12. Consider an elliptic curve $E/k(t)$ with discriminant Δ. We say that an elliptic curve E is in **minimal Weierstrass form** if all of its coefficients are in $k[t]$ and there does not exist a polynomial u with $deg(u) \geq 1$, such that

$$u^{12} \mid \Delta.$$

Definition 2.13. Consider an elliptic surface given by $f : S \to C$. We have a **rational elliptic surface** if the function field $k(S)$ is isomorphic to the rational function field in two variables, $k(t_1, t_2)$.

Lemma 2.8. *The Kodaira-Néron model of an elliptic curve over $k(t)$ in minimal Weierstrass form $E : y^2 = x^3 + Ax + B$, corresponds to a* ***rational elliptic surface*** *if and only if A and B are not both constants, and*

$$deg(A) \leq 4, \quad \text{and} \quad deg(B) \leq 6.$$

In the previous section, we saw the Mordell-Weil theorem, Theorem 2.4. This is an important result that does not apply to the curves we are studying as they are defined over function fields, not number fields. Luckily, it was generalized to function fields.

Theorem 2.9 (Mordell-Weil Theorem for Function Fields)**.** *Let $\mathcal{E} \to C$ be an elliptic surface defined over a field k, and let E/K be the corresponding elliptic curve over the function field $K = k(C)$. If $\mathcal{E} \not\cong E_0 \times C$ for any elliptic curve E_0/k, then $E(K)$ is a finitely generated abelian group.*

Proof. See [Sil94], Chapter III.6. □

For the most part, in this paper we consider the function field $k(t)$ of the projective line. In Section 4.2 we will utilize function fields over other curves.

3 Rank over $\overline{\mathbb{Q}}(t)$

3.1 Rank bounds and equalities

For the following results, we will consider elliptic curves given by an equation

$$E : y^2 = x^3 + g(t),$$

for polynomials $g(t)$ with coefficients in a field k, so the curve is defined over the function field $K := k(t)$. Denote by

$$r_K(g(t))$$

the rank of E over the field K, i.e. rank $E(K)$. For the rank to be finite, we require that $g(t)$ is not a constant times a sixth power in $k(t)$, see Theorem 2.9.

Lemma 3.1.

$$r_K(g(t)) = r_K(t^6 g(t))$$

Proof. Multiply the equation of the original curve by t^6,

$$t^6 \cdot y^2 = t^6 \cdot x^3 + t^6 \cdot g(t),$$
$$(t^3 y)^2 = (t^2 x)^3 + t^6 g(t).$$

Using the change of coordinates $\eta = t^3 y, \xi = t^2 x$, we get an isomorphic curve

$$\eta^2 = \xi^3 + t^6 g(t).$$

We conclude this curve has the same rank. □

Lemma 3.2.

$$r_K(t^{na} + t^{nb}) \geq r_K(t^a + t^b)$$

Proof. Let $K = k(t)$, and consider a field extension $L = K(s) \supset K$ with $s^n = t$. We have that

$$r_L(s^{na} + s^{nb}) = r_K(t^{na} + t^{nb})$$

because $L = k(s)$ and $K = k(t)$. By $s^n = t$ we have that

$$r_L(s^{na} + s^{nb}) = r_L(t^a + t^b).$$

Finally, we have that the group $E(L)$ must be the same size or bigger than $E(K)$. Thus we can write

$$r_L(t^a + t^b) \geq r_K(t^a + t^b),$$

and we conclude that

$$r_K(t^{na} + t^{nb}) \geq r_K(t^a + t^b).$$

□

Lemma 3.3.

$$r_K(g(t^{2n})) = r_K(g(t^n)) + r_K(t^3 g(t))$$

Proof. To begin let us take a quadratic extension of $K = k(t)$. Let $L = K(s)$ with $s^2 = t$. The *quadratic twist* of $E : y^2 = x^3 + g(t^n)$ is given by

$$E' : ty^2 = x^3 + g(t^n)$$

If we multiply across by t^3,

$$t^4 y^2 = t^3 x^3 + t^3 g(t^n)$$
$$(t^2 y)^2 = (tx)^3 + t^3 g(t^n)$$

by an admissible change of coordinates, $\eta = t^2 y, \xi = tx$, we get an isogenous curve

$$\eta^2 = \xi^3 + t^3 g(t^n).$$

Note that $r_L(g(t^n)) = r_L(g(s^{2n})) = r_K(g(t^{2n}))$. We can now apply Lemma 2.7,

$$\text{rank } E(L) = \text{rank } E(K) + \text{rank } E'(K).$$

We conclude that

$$r_L(g(t^n)) = r_K(g(t^n)) + r_K(t^3 g(t^n))$$
$$r_K(g(t^{2n})) = r_K(g(t^n)) + r_K(t^3 g(t^n)).$$

□

3.2 Vectorspace Decomposition

The following result is from [Mei99], section 2, 'Linear algebra as a tool for decomposition'. It will hopefully shed some light on the proof of Lemma 2.7.

Consider a field k containing a primitive sixth root of unity, $\zeta_6 \in k$. Let $E/k(t)$ be an elliptic curve of the form $y^2 = x^3 + f(t^6)$, where f is a nonconstant polynomial in $k(t)$ with $f(0) \neq 0$. We can tensor this $E(k(t))$ with $\mathbb{Q}$ to obtain a $\mathbb{Q}$ vectorspace,

$$V := E(k(t)) \otimes \mathbb{Q}.$$

The dimension of this vectorspace is equal to the rank of $E(k(t))$. In fact this $\mathbb{Q}$-vectorspace turns out to be a $\mathbb{Q}(\zeta_6)$-vectorspace. We can see this by defining

$$\begin{aligned} \phi &: E(k(t)) \otimes \mathbb{Q} \to E(k(t)) \otimes \mathbb{Q} \\ &(x(t), y(t)) \otimes r \mapsto \zeta_6 \cdot (x(t), y(t)) \otimes r := (\zeta_6^2 x(t), \zeta_6^3 y(t)) \otimes r. \end{aligned}$$

We see that ϕ^6 is identity. Thus we have a $\mathbb{Q}(\zeta_6)$ structure on V by

$$(a + b\zeta_6) \cdot P := a \cdot P + b \cdot \phi(P), \forall a, b, \in \mathbb{Q}, P \in V.$$

Now we define a field automorphism of $k(t)$,

$$\begin{aligned} \Phi &: k(t) \to k(t) \\ &t \mapsto \zeta_6 t. \end{aligned}$$

This automorphism has order 6. Considering $k(t)$ over the fixed field of this automorphism,

$$k(t) \supset k(t)^{<\Phi>} = \{x \in k(t) : \Phi(x) = x\},$$

one obtains a Galois extension with Galois group $< \Phi >$. This means this extension has degree 6. We can see that any rational function in $k(t)$ of the form $f(t^6)$ will be fixed by Φ. We can write

$$k(t^6) \subset k(t)^{<\Phi>}.$$

Let us put $t^6 = s$. Clearly, $[k(t) : k(s)] = 6$. By the tower law, we must have

$$[k(t) : k(s)] = [k(t) : k(t)^{<\Phi>}] \cdot [k(t)^{<\Phi>} : k(s)] = 6.$$

This implies $[k(t)^{<\Phi>} : k(s)] = 1$, so we must have $k(t)^{<\Phi>} = k(s)$.

Now we extend Φ to V, creating a $\mathbb{Q}(\zeta_6)$-linear automorphism of order 6,

$$\begin{aligned} \Phi &: E(k(t)) \otimes \mathbb{Q} \to E(k(t)) \otimes \mathbb{Q} \\ &(x(t), y(t)) \otimes r \mapsto (\Phi x(t), \Phi y(t)) \otimes r. \end{aligned}$$

The following corollary of Maschke's theorem from representation theory is now employed, see Lemma 2.2 of [Mei99].

Lemma 3.4. *Let Ψ be a linear map of finite order acting on a finite dimensional vectorspace. Furthermore suppose Ψ has all its eigenvalues rational. Then Ψ is diagonalizable.*

Φ is order 6, so we must have that for any eigenvalue λ, $\Phi^6(P \otimes r) = \lambda^6(P \otimes r) = P \otimes r$, so the six eigenvalues of Φ are $\{\zeta_6^i\}_{0 \leq i \leq 5}$. These are all in $\mathbb{Q}(\zeta_6)$, thus Φ is diagonalizable and V is spanned by the eigenspaces,

$$V = \oplus_{i=0}^{5} V_{\zeta_6^i}.$$

This means the dimension of V is equal to the sum of the dimensions of these eigenspaces. We can identify each of these eigenspaces with a new elliptic curve $E_i/k(s)$,

$$E_i : y^2 = x^3 + s^i f(s).$$

This also tells us that rank $E(k(t)) = \sum_i$ rank $E_i(k(s))$. Each curve $E_i(k(s))$ is related to the eigenspace with eigenvalue ζ_6^{6-i}. We will prove two cases as examples, the rest follow similarly.

$\underline{i=2}$ Consider the curve $E_2 : y^2 = x^3 + s^2 f(s)$ over the field $k(t)$,

$$y(t^6)^2 = x(t^6)^3 + t^{12} f(t^6).$$

We want to find a map that will take points from this curve to points on our original curve over $k(s)$, $y(t^6)^2 = x(t^6)^3 + f(t^6)$. Write

$$t^{12}\Big(\frac{y(t^6)}{t^6}\Big)^2 = t^{12}\Big(\frac{x(t^6)}{t^4}\Big)^3 + t^{12} f(t^6).$$

The map

$$(x(t), y(t)) \mapsto \Big(\frac{x(t^6)}{t^4}, \frac{y(t^6)}{t^6}\Big),$$

composed with Φ will give us

$$(x(\zeta_6 t), y(\zeta_6 t)) \mapsto \Big(\zeta_6^2 \frac{x(t^6)}{t^4}, \frac{y(t^6)}{t^6}\Big).$$

We also have that

$$\zeta_6^4 \cdot (x(t), y(t)) := \phi^4(x(t), y(t)) = (\zeta_6^2 x(t), y(t)).$$

We see that there is an isomorphism between $E_2(k(s)) \otimes \mathbb{Q}$ and $V_{\zeta_6^4}$.

$\underline{i=5}$ Consider the curve $E_5 : y^2 = x^3 + s^5 f(s)$ over the field $k(t)$,

$$y(t^6)^2 = x(t^6)^3 + t^{30} f(t^6).$$

In the same way as before we write,

$$t^{30}\Big(\frac{y(t^6)}{t^{15}}\Big)^2 = t^{30}\Big(\frac{x(t^6)}{t^{10}}\Big)^3 + t^{30} f(t^6).$$

We have

$$\Big(\frac{x((\zeta_6 t)^6)}{(\zeta_6 t)^{10}}, \frac{y((\zeta_6 t)^6)}{(\zeta_6 t)^{15}}\Big) = \Big(\zeta_6^2 \frac{x(t^6)}{t^{10}}, \zeta_6^3 \frac{y(t^6)}{t^{15}}\Big) = \phi\Big(\frac{x(t^6)}{t^{10}}, \frac{y(t^6)}{t^{15}}\Big) =: \zeta_6\Big(\frac{x(t^6)}{t^{10}}, \frac{y(t^6)}{t^{15}}\Big).$$

We see that there is an isomorphism between $E_5(k(s)) \otimes \mathbb{Q}$ and V_{ζ_6}.

This allows us to state the following result.

Theorem 3.5. *For an elliptic curve $E(k(t))$ of the form $y^2 = x^3 + f(t^6)$, where f is a nonconstant polynomial with $f(0) \neq 0$, we can write*

$$\text{rank } E(k(t)) = \sum_{i=0}^{5} \text{rank } E_i(k(t))$$

for $E_i : y^2 = x^3 + t^i f(t)$.

This immediately gives us

$$r_K(t^{360}+1) = r_K(t^{60}+1) + r_K(t^{61}+t) + r_K(t^{62}+t^2) + r_K(t^{63}+t^3) + r_K(t^{64}+t^4) + r_K(t^{65}+t^5)$$

for any field $K := k(t)$ with $\zeta_6 \in k$. We apply another vectorspace decomposition to the first term in this sum.

$$r_K(t^{60}+1) = r_K(t^{10}+1) + r_K(t^{11}+t) + r_K(t^{12}+t^2) + r_K(t^{13}+t^3) + r_K(t^{14}+t^4) + r_K(t^{15}+t^5)$$

Take the first term in this sum as an example.

Example 3.1. Lemma 3.3 allows us to write

$$r_K(t^{10}+1) = r_K(t^5+1) + r_K(t^8+t^3).$$

Lemma 3.1 allows us to multiply by powers of t^6, giving us

$$r_K(t^8+t^3) = r_K(t^{20}+t^{15}).$$

Lemma 3.2 gives us a bound,

$$r_K(t^{20}+t^{15}) \geq r_K(t^4+t^3).$$

We can thus write

$$r_K(t^{10}+1) \geq r_K(t^5+1) + r_K(t^4+t^3).$$

These methods are applied repeatedly and further examples of their application can be found in [Boo23]and [CMT00]. We arrive at the following collection of lower bounds.

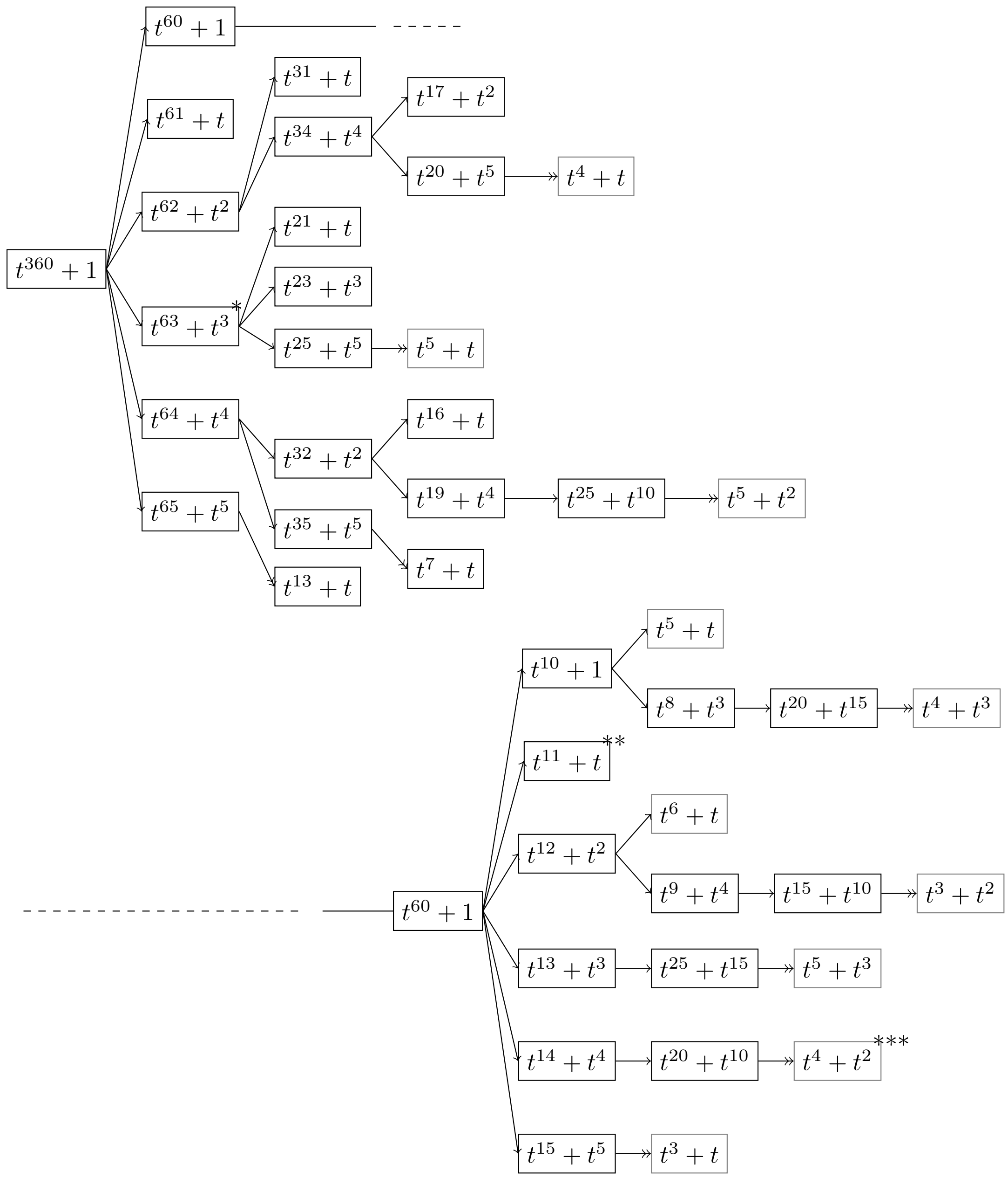


Figure 1: Diagram of constituent ranks.

In the above diagram, each node represents an elliptic curve $y^2 = x^3 + g(t)$, and is denoted by $g(t)$. From the results we have proven, we can say that the rank of each curve is given by the sum of the ranks of each curve it connects to with an arrow. The rank of a curve is bounded below by the rank of the curve to which it is connected by a double headed arrow. The curves for which $g(t)$ has degree less than or equal to 6 have been outlined in grey as these curves will be of note in the next section.

Some notes:

*This curve is decomposed into three by a method entirely analogous to the decomposition in two and six which are already proven. See Theorem A.1.

**This will turn out to be the only curve with $deg(g) \geq 6$ whose rank is non-zero. In Section 4.2 we will determine the rank of this curve over $\mathbb{Q}(t)$.

***In this case, we could remove a factor of 10 from the exponents in order to find a lower bound of $r(t^2+t)$. However, by removing a factor of 5, we are left with a lower bound of $r(t^4+t^2)$ which is greater than $r(t^2+t)$ and thus more helpful.

3.3 Counting Multiplicities

Theorem 3.6. *Consider an algebraically closed field $k = \overline{k}, K = k(t)$. Let E be an elliptic curve of the form $E : y^2 = x^3 + g(t)$, with $g(t)$ a polynomial in K. If g has degree ≤ 6, is nonconstant, and not a power of 6, we have that*

$$r_K(g(t)) = 8 - \sum_{v \in R}(m_v - 2),$$

where $R \subset \mathbb{P}_1(K)$ is the set of zeroes of the discriminant of E, and m_v denotes the multiplicity of the zero v in the discriminant.

Proof. This result follows from Corollary 6.7 of [SS19]. It states

$$\rho(S) = \text{rank } (E(K)) + 2 + \sum_{v \in R}(j_v - 1),$$

where S is the Kodaira-Néron model of E, $\rho(S)$ is the Picard number of this surface, and j_v is the number of irreducible components of the fibre F_v.

As we have seen in Lemma 2.8, the surface is a rational elliptic surface if and only if $\deg(g(t)) \leq 6$ for a curve in minimal Weierstrass form. By Proposition 7.1 of [SS19], the Picard number of a rational elliptic surface is 10. Thus we can write

$$r_K(g(t)) = 8 - \sum_{v \in R}(j_v - 1).$$

As we can see from Table 15.1 of [Sil09], all fibre types bar I_0 and I_n have one less irreducible component than the multiplicity of their zero in the discriminant. For further discussion of why we do not encounter these two types of fibres in the surfaces we study, see Appendix A.1. This gives us the easier to work with formula,

$$r_K(g(t)) = 8 - \sum_{v \in R}(m_v - 2).$$

□

Example 3.2. Let us now apply this theorem. Take for example the curve

$$E_{4,3} : y^2 = x^3 + t^4 + t^3.$$

The discriminant of this curve is given by

$$\Delta = -432 \cdot (t^4 + t^3)^2 = -432 \cdot t^6 \cdot (t+1)^2.$$

Here we can identify a zero of multiplicity 6 at $t = 0$, and another of multiplicity 2 at $t = -1$. We want to check if the point at infinity is also a zero of this discriminant, thus we make the change of coordinates $\eta = \frac{y}{t^3}, \xi = \frac{x}{t^2}, s = \frac{1}{t}$. This gives us a new curve, $\eta^2 = \xi^3 + s^2 + s^3$, with discriminant

$$\Delta_s = -432 \cdot (s^2 + s^3)^2 = -432 \cdot s^4 \cdot (1+s)^2.$$

Here we see a zero at $s = -1$ of multiplicity 2, and equivalent to $t = -1$, which we have already accounted for. Another zero is revealed to us at $s = 0$ corresponding to $t = \infty$, and it has multiplicity 4. We can apply Theorem 3.6 to find the rank of $E_{4,3}$,

$$r_K(t^4 + t^3) = 8 - (4 + 0 + 2) = 2.$$

The rest of these rank calculations follow the same procedure, so the results have been collected in Figure 2. When listing the zeroes, only one of the n zeroes of each $t^n + 1$ is listed, as they all have multiplicity 2 and thus have no bearing on the final rank calculation.

Remark. It is worth noting here that every curve $y^2 = x^3 + g(t)$ appearing in Figure 2 has some zero of its discriminant with multiplicity 2, meaning each curve is related to an elliptic surface which has a type II fibre. This implies the curves are torsion-free. This is Lemma 4.2 of [Mei99], and we will sketch its proof here.

We can see in, for example, Table 15.1 of [Sil09], 'A table of reduction types', that the desingularized Kodaira-Néron model of an elliptic curve, $\tilde{\mathcal{E}}^0(\overline{\mathbb{Q}})$, at a fibre of type II, is isomorphic to the additive group $\overline{\mathbb{Q}}^+$, which is torsion-free. We also have that $\tilde{\mathcal{E}}(\overline{\mathbb{Q}})/\tilde{\mathcal{E}}^0(\overline{\mathbb{Q}})$ is the trivial group (0). We know that $\tilde{\mathcal{E}}(\overline{\mathbb{Q}})/\tilde{\mathcal{E}}^0(\overline{\mathbb{Q}}) \cong E(\overline{\mathbb{Q}}(t))/E_0(\overline{\mathbb{Q}}(t)) \cong (0)$, thus we conclude that $E(\overline{\mathbb{Q}}(t))$ is torsion-free.

$g(t)$	$\Delta_t/27$	$\Delta_s/27$	v	m_v	rank
t^5+1	$(t^5+1)^2$	$s(1+s^5)^2$	$-\zeta_5, \infty$	$2, 2$	8
t^4+t^3	$t^6(t+1)^2$	$s^4(1+s)^2$	$0, -1, \infty$	$6, 2, 4$	2
t^6+t	$t^2(t^5+1)^2$	$(1+s^5)^2$	$0, -\zeta_5$	$2, 2$	8
t^3+t^2	$t^4(t+1)^2$	$s^6(1+s)^2$	$0, -1, \infty$	$4, 2, 6$	2
t^5+t^3	$t^6(1+t^2)^2$	$s^2(1+s^2)^2$	$0, i, \infty$	$6, 2, 2$	4
t^4+t^2	$t^4(t^2+1)^2$	$s^4(1+s^2)^2$	$0, i, \infty$	$4, 2, 4$	4
t^3+t	$t^2(t^2+1)^2$	$s^6(1+s^2)^2$	$0, i, \infty$	$2, 2, 6$	4
t^4+t	$t^2(t^3+1)^2$	$s^4(1+s^3)^2$	$0, -\zeta_3, \infty$	$2, 2, 4$	6
t^5+t	$t^2(t^4+1)^2$	$s^2(1+s^4)^2$	$0, \sqrt{i}, \infty$	$2, 2, 2$	8
t^5+t^2	$t^4(t^3+1)^2$	$s^2(1+s^3)^2$	$0, -\zeta_3, \infty$	$4, 2, 2$	6

Figure 2: Multiplicities

Summing these ranks gives us a bound of $r_{\overline{\mathbb{Q}}(t)}(t^{360}+1) \geq 52 + r_{\overline{\mathbb{Q}}(t)}(t^{11}+t)$. We have the means to find $r_{\overline{\mathbb{Q}}(t)}(t^{11}+t)$, via Shioda's algorithm[Shi92], and in fact it turns out to be exactly 16, telling us $r_{\overline{\mathbb{Q}}(t)}(t^{360}+1) \geq 68$. We know that $r_{\overline{\mathbb{Q}}(t)}(t^{360}+1)$ is indeed 68. This implies that those ranks which we did not include in our sum must be equal to 0. The ranks we have calculated above, as well as $r_{\overline{\mathbb{Q}}(t)}(t^{11}+t)$ are the only ranks contributing to that of E_{360} over $\overline{\mathbb{Q}}(t)$.

Theorem 3.5 holds for any base field containing a primitive sixth root of unity, thus we know all of the relations in Figure 1 hold over $\mathbb{Q}(\zeta_6, t)$. Consider that $\mathbb{Q}(\zeta_6, t) \subset \overline{\mathbb{Q}}(t)$, thus $E(\mathbb{Q}(\zeta_6, t)) \subset E(\overline{\mathbb{Q}}(t))$, so we must have that

$$\text{rank } E(\mathbb{Q}(\zeta_6, t)) \leq \text{rank } E(\overline{\mathbb{Q}}(t)).$$

If rank $E(\overline{\mathbb{Q}}(t)) = 0$, it follows that rank $E(\mathbb{Q}(\zeta_6, t)) = 0$.

4 Rank over $\mathbb{Q}(t)$

4.1 Injectivity, Finite Fields, and Magma

We have that over $\mathbb{Q}(\zeta_6, t)$, the relations in Figure 1 hold, and thus only 11 surfaces have nonzero rank contributing to the rank of E_{360}. However, our question is, what is the rank of E_{360} over $\mathbb{Q}(t)$? The following result simplifies our problem.

Lemma 4.1. *Let $g(t) \in K^\times$ be such that the elliptic curve $E : y^2 = x^3 + g(t)$ has $r_K(g(t)) < \infty$. Put $L := K(\zeta_6)$, for ζ_6 a primitive sixth root of unity. Then we have that*

$$r_L(g(t)) = \begin{cases} r_K(g(t)) & \textit{if } K = L; \\ 2r_K(g(t)) & \textit{otherwise.} \end{cases}$$

Proof. In complex form $\zeta_6 = \frac{1+\sqrt{-3}}{2}$, meaning we can write $K(\zeta_6) = K(\sqrt{-3})$. We have a quadratic extension, and so can apply Lemma 2.7. We take the quadratic twist of $E : y^2 = x^3 + g(t)$ given by

$$E' : y^2 = x^3 - 27g(t).$$

We have that $r_L(g(t)) = r_K(g(t)) + r_K(-27g(t))$. To finish the proof we note that the following isogeny,

$$(x, y) \mapsto \Big(\frac{y^2 + g(t)}{x^2}, \frac{y(x^3 - 8g(t))}{x^3}\Big)$$

tells us that $r_K(g(t)) = r_K(-27g(t))$. Thus we have that $r_L(g(t)) = 2r_K(g(t))$. □

This result tells us that the relations in Figure 1 hold even over $\mathbb{Q}(t)$. The curves which have rank 0 over $\mathbb{Q}(\zeta_6, t)$ will also have rank 0 over $\mathbb{Q}(t)$. Solving the rest of our problem amounts to computing the ranks of the 10 rational elliptic surfaces, and the K3 surface, over $\mathbb{Q}(t)$. Reduction modulo a suitable prime p will be helpful for this.

Theorem 4.2. *Consider an elliptic curve E, with Kodaira Néron model that has a singular fibre. We have that*

$$rank\ E(\mathbb{Q}(t)) \leq rank\ E(\mathbb{F}_p(t))$$

whenever p is such that the number of irreducible components in the fibres of the corresponding elliptic surfaces over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_p}$ is the same.

Proof. We begin by considering Proposition 6.2 of [Lui07]. This paper goes into detail out of the scope of this project, but the following result is highly relevant for us. This proposition considers an 'integral scheme' S, and its base changes, $\bar{S} = S_{\overline{\mathbb{Q}}}$, $\tilde{S} = S_{\overline{\mathbb{F}_p}}$, which are smooth projective surfaces over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_p}$ respectively. It says there are natural injective homomorphisms

$$NS(\bar{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow NS(\tilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow H^2(\tilde{S}, \mathbb{Q}_l)(1)$$

of finite-dimensional vectorspaces over $\mathbb{Q}_l$. Remark 6.3 of the same paper points out that this implies

$$\text{rank } NS(\bar{S}) \leq \text{rank } NS(\tilde{S}).$$

The rank of the Néron-Severi group of S, rank $NS(S)$, is exactly the Picard number of S, $\rho(S)$. Recall the proof of Theorem 3.5, in which we state Corollary 6.7 of [SS19],

$$\rho(S) = \text{rank } E(K) + 2 + \sum_{v \in R} (j_v - 1).$$

By the above, we can write

$$\text{rank } E(\overline{\mathbb{Q}}(t)) + 2 + \sum_{v \in R} (j_v - 1) \leq \text{rank } E(\overline{\mathbb{F}_p}(t)) + 2 + \sum_{v \in T} (h_v - 1)$$

where j_v for $v \in R$ are the number of irreducible components of the fibres over v of the surface over $\overline{\mathbb{Q}}$, and h_v for $v \in T$ considers the surface over $\overline{\mathbb{F}_p}$. Thus, for a p under the assumptions in the statement, we have that

$$\text{rank } E(\overline{\mathbb{Q}}(t)) \leq \text{rank } E(\overline{\mathbb{F}_p}(t)).$$

Since reduction mod p as a map between Néron-Severi groups $\text{NS}(\mathcal{E}/\mathbb{Q}) \to \text{NS}(\mathcal{E}/\mathbb{F}_p)$ is injective, the inequality for the ranks of the corresponding Mordell-Weil groups is a consequence,

$$\text{rank } E(\mathbb{Q}(t)) \leq \text{rank } E(\mathbb{F}_p(t)).$$

□

Calculating ranks of rational elliptic surfaces over finite fields is achievable in Magma, and we do so in the following manner.

Example 4.1. Consider the elliptic curve $E_{5,0} : y^2 = x^3 + t^5 + 1$ over $\mathbb{F}_7(t)$. We can examine it in Magma.

```
p:=7;
k:=GF(p);
K<t>:=FunctionField(k);
E50:=EllipticCurve([K!0, K!(t^5+1)]);
MordellWeilGroup(E50);
```

This input into Magma will output :

```
Abelian Group of order 1
```

This tells us that this surface is isomorphic to the trivial group, and thus has rank 0 over $\mathbb{F}_7$.

Remark. We chose the prime 7 in this example because it is the smallest prime for which we are guaranteed good reduction. All the surfaces we see in our argument have good reduction at any prime $p > 5$, because the multiplicities of the zeroes of their discriminants does not change after reduction modulo p.

$g(t)$	$\mathbb{F}_7(t)$	$\mathbb{F}_{11}(t)$
t^5+1	$Ord1$	$Ord1$
t^4+t^3	$\cong \mathbb{Z}^2$	$\cong \mathbb{Z}$
t^6+t	$Ord1$	$Ord1$
t^3+t^2	$\cong \mathbb{Z}^2$	$\cong \mathbb{Z}$
t^5+t^3	$Ord1$	$\cong \mathbb{Z}^2$
t^4+t^2	$Ord1$	$\cong \mathbb{Z}^2$
t^3+t	$Ord1$	$\cong \mathbb{Z}^2$
t^4+t	$Ord1$	$\cong \mathbb{Z}$
t^5+t	$Ord1$	$\cong \mathbb{Z}^4$
t^5+t^2	$Ord1$	$\cong \mathbb{Z}$

Figure 3: Mordell-Weil Group structures

We can easily repeat this for each of our curves and over other finite fields. Some results have been collected in Figure 3.

Remark. It is interesting to note here that we only see even ranks over $\mathbb{F}_7(t)$ as $\mathbb{F}_7$ contains a primitive sixth root of unity, this follows from Lemma 4.1.

These results only give us upper bounds for the ranks of these curves, so the curves given by constant coefficients t^4+t^3 and t^3+t^2 could have rank 0 or 1. We can see that the point $(-t, t^2)$ satisfies

$$(t^2)^2 = (-t)^3 + t^4 + t^3,$$

and $(-t, t)$ satisfies

$$(t)^2 = (-t)^3 + t^3 + t^2,$$

allowing us to conclude the ranks of these curves are both exactly 1.

This gives us a new upper bound, rank $E_{360}(\mathbb{Q}(t)) = 2 + r_{\mathbb{Q}(t)}(t^{11}+t)$. Using Lemma 4.1, we can write $r_{\mathbb{Q}(t)}(t^{11}+t) \leq \frac{1}{2} r_{\overline{\mathbb{Q}}(t)}(t^{11}+t) = 8$. We conclude this subsection with

$$\text{rank } E_{360}(\mathbb{Q}(t)) \leq 10.$$

4.2 The K3-Surface

So far the methods we have applied have not helped us in calculating the rank of $E_{11,1}(\mathbb{Q}(t))$,

$$E_{11,1} : y^2 = x^3 + t^{11} + t.$$

To tackle this we shall apply the method used in Example 5.1.8 of [Boo23]. We again want to bound the rank of $E_{11,1}(\mathbb{F}_p(t))$ for some prime p such that $E_{11,1}(\mathbb{Q}(t)) \to E_{11,1}(\mathbb{F}_p(t))$ is injective. Let us begin with a finite field $k = \mathbb{F}_7$. As in Bootsma's thesis, we put s^6 equal to our constant coefficient. We could define the curve,

$$C_{11} : s^6 = t^{11} + t,$$

and put $K := k(C)$ the function field of this curve. However the genus of this curve is 25, which is too high for the computations we wish to carry out. Thus, in a method analogous to that of Lemma 3.1, we multiply our constant coefficient by t^{-6} to obtain an elliptic curve with the same rank,

$$E_{5,-5} : y^2 = x^3 + t^5 + t^{-5}.$$

In order to have polynomial coefficients, we define a new variable $u = t + t^{-1}$. This gives us

$$E : y^2 = x^3 + u^5 - 5u^3 + 5u.$$

We want to find the rank of this curve over $k(t)$, rather than $k(u)$. We note that $k(t) \supset k(u)$. The relation between u and t can be given by the quadratic equation $t^2 - ut + 1$, which has roots $t = \frac{u \pm \sqrt{u^2-4}}{2}$. We see that $k(t) = k(u, \sqrt{u^2-4})$. We have a quadratic extension and can apply Lemma 2.7. Our quadratic twist will be given by multiplying our constant coefficient by $(u^2-4)^3$,

$$E' : y^2 = x^3 + (u^2-4)^3(u^5 - 5u^3 + 5u).$$

Thus we have that the rank of $E(k(t))$ is given by

$$r_{k(t)}(u^5-5u^3+5u) = r_{k(u)}(u^5-5u^3+5u) + r_{k(u)}((u^2-4)^3(u^5-5u^3+5u)).$$

We now need to determine the rank of a rational elliptic surface, and a K3 surface over $k(u)$. Using the same Magma code given in Example 4.1, we find that

$$r_{k(u)}(u^5-5u^3+5u) = 0.$$

For the rest of this section we focus on determining $r_{k(u)}((u^2-4)^3(u^5-5u^3+5u))$. This is also a K3 surface, so we continue our attempt to apply the method used in Example 5.1.8 of [Boo23]. Let us define the curve,

$$C : s^6 = (u^2-4)^3(u^5-5u^3+5u).$$

Remark. As we saw in Theorem 2.2, there exists an equivalence of categories between;
(1) Curves over k, and rational maps.
(2) Function fields over k, and field automorphisms that restrict to identity on k.
(3) Curves over k that are projective, smooth, and geometrically irreducible, and morphisms.
This C we have defined is a member of the first category, but its Jacobian and its L-polynomial are only defined for its equivalent, which we denote by $\tilde{C}$, in the third category. Furthermore, due to this equivalence of categories, $k(C) = k(\tilde{C})$.

Theorem 4.3. *Let E be an elliptic curve over k. We have a canonical morphism*

$$E(K) \cong Mor_k(C, E),$$

where Mor_k denotes the group of morphisms over k. Under this isomorphism, $E(K)_{tor}$ injects into the subgroup of constant morphisms.

Corollary 4.4. *Suppose C has genus $g(C) \geq 1$. Then*

$$rank\ E(K) = rank\ Hom_k(JacC, E).$$

For the proofs of the above theorem and corollary, see Theorem 5.1.2 and Corollary 5.1.3 of [Boo23], as the details are outside the scope of this project.

We put E' in this form as follows. Over $K = k(C)$, our curve $E' : y^2 = x^3+(u^2-4)^3(u^5-5u^3+5u)$ is the same as $y^2 = x^3+s^6$. A change of coordinates gives us $\eta^2 = \xi^3+1$. These two curves are isomorphic over K. Call the latter elliptic curve over the base field k, E_0. Now we can write,

$$\begin{aligned} E'(K) &\cong E_0(K) \\ E'(K) &\cong Mor_k(\tilde{C}, E_0), \\ \text{rank } E'(K) &= \text{rank } Hom_k(Jac\tilde{C}, E_0). \end{aligned}$$

The following result is due to Tate[Tat66].

Theorem 4.5. *Let A and B be abelian varieties over a finite field k, and let f_A and f_B be the characteristic polynomials of their Frobenius endomorphisms relative to k. Then*

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

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

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

In order to find the characteristic polynomials of the Frobenius endomorphisms relative to k, we can use L-polynomials, which Magma helps us with. We state some facts about L-polynomials.

Lemma 4.6. *Let L_C denote the L-polynomial of C, χ_C denote the characteristic polynomial of the Frobenius endomorphism on $JacC$, and g the genus of C. Then we have the following,*

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

Theorem 4.7. *Let C be a smooth geometrically irreducible curve of genus $g \geq 1$ defined over $\mathbb{F}_q$. Denote by $L_C(T)$, the L-polynomial of C. Then*

(i) L_C is of the form

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

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

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

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

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

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

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

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

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

$$ia_i = S_ia_0 + S_{i-1}a_1 + ... + S_1\alpha_{i-1}.$$

Proof. See Section 5.1 of [Sti09]. □

Example 4.2. Let us compute the L-polynomial of E_0 over $\mathbb{F}_7$. We have that E_0 is an elliptic curve, and thus has genus 1. This tells us our L-polynomial will have degree 2. Furthermore, we know $a_2 = p = 7$, and $a_0 = 1$. It remains to find a_1, for which we know

$$a_1 = S_1a_0, \quad S_1 = \#(E_0(\mathbb{F}_p)) - (p + 1),$$

$$\implies a_1 = \#(E_0(\mathbb{F}_7)) - 8.$$

There are 12 points in $E_0(\mathbb{F}_7)$. As this elliptic curve is simple and this finite field relatively small this can be computed by hand, but for larger calculations of this sort we can use :

```
p := 7;
k := GF(p);
E0 := EllipticCurve([k!0,k!1]);
#Points(E0);
```

We find the L-polynomial $L_{E_0}(T) = 7T^2 + 4T + 1$. We can also find this directly using Magma.

```
p := 7;
k := GF(p);
E0 := EllipticCurve([k!0,k!1]);
LPolynomial(E0);
```

This gives us the characteristic polynomial,

$$\chi_{E_0}(T) = T^2 + 4T + 7.$$

It remains to determine the L-polynomial of $\tilde{C}$ over $\mathbb{F}_7$. This curve has genus 13, thus we will have a degree 26 polynomial. Let us compute N_r and S_r for as many values of r as Magma can help us with. We do so using the following command.

```
#Places(K, r)
```

We write P_r for the number returned. We have put $K := \mathbb{F}_7(\tilde{C})$. This command outputs the number of Galois orbits of points in $\tilde{C}(\bar{\mathbb{F}}_7)$, consisting of precisely r points. We then have that

$$N_r = \#(\tilde{C}(\mathbb{F}_{7^r})) = \sum_{e|r} e \cdot P_e.$$

Example 4.3. We find the following : $P_1 = 8, P_2 = 69, P_4 = 547$.
This data tells us that $N_4 = \#\tilde{C}(\mathbb{F}_{7^4}) = 8 + 2 \cdot 69 + 4 \cdot 547 = 2334$.

We use this method to find P_r, N_r, and C_r for as high as Magma can compute for us.

r	7^r	P_r	N_r	S_r
1	7	8	8	0
2	49	69	146	96
3	343	112	344	0
4	2401	547	2334	−68
5	16807	3360	16808	0
6	117649	19563	117860	210
7	823543	117648	823544	0

We now apply part (v) of Theorem 4.7.

$$\begin{aligned}
ia_i &= S_i a_0 + S_{i-1}a_1 + ... + S_1\alpha_{i-1}\\
a_1 &= S_1 a_0 = 0\\
2a_2 &= S_2a_0 + S_1a_1 = 96 + 0 = 96\\
3a_3 &= S_3a_0 + S_2a_1 + S_1a_2 = 0\\
4a_4 &= S_4a_0 + S_3a_1 + S_2a_2 + S_1a_3 = -68 + 4608 = 4540\\
5a_5 &= S_5a_0 + S_4a_1 + S_3a_2 + S_2a_3 + S_1a_4 = 0\\
6a_6 &= S_6a_0 + S_5a_1 + S_4a_2 + S_3a_3 + S_2a_4 + S_1a_5 = 210 - 3264 + 108960 = 105906\\
7a_7 &= S_7a_0 + S_6a_1 + S_5a_2 + S_4a_3 + S_3a_4 + S_2a_5 + S_1a_6 = 0
\end{aligned}$$

We use these results and part (ii) of Theorem 4.7 to fill in the following coefficients.

i	a_i	i	a_i	i	a_i	i	a_i
0	1	7	0	14	$7 \cdot a_{12}$	21	0
1	0	8	a_8	15	$7^2 \cdot a_{11}$	22	$7^9 \cdot 1135$
2	48	9	a_9	16	$7^3 \cdot a_{10}$	23	0
3	0	10	a_{10}	17	$7^4 \cdot a_9$	24	$7^{11} \cdot 48$
4	1135	11	a_{11}	18	$7^5 \cdot a_8$	25	0
5	0	12	a_{12}	19	0	26	7^{13}
6	17651	13	a_{13}	20	$7^7 \cdot 17651$		

It remains to compute six coefficients. We take these coefficients, $a_8 = a, a_9 = b, a_{10} = c, a_{11} = d, a_{12} = e, a_{13} = f$, to be variables. Let us consider the L-polynomials (of the smooth, projective, geometrically irreducible equivalents) of the lower genus curves,

$$C_2 : s^2 = (u^2 - 4)^3(u^5 - 5u^3 + 5u),$$

$$C_3 : s^3 = (u^2 - 4)^3(u^5 - 5u^3 + 5u).$$

Magma computes these to be,

$$L_{C_2}(T) = 343T^6 + 77T^4 + 11T^2 + 1,$$

$$L_{C_3}(T) = 2401T^8 + 882T^6 + 175T^4 + 18T^2 + 1.$$

We state Theorem 5 of [Bla+16], known as the Kleiman-Serre theorem.

Theorem 4.8. *If there is a separable morphism of curves $C \to C'$, defined over $\mathbb{F}_q$, then $L_{C'}(T)$ divides $L_C(T)$.*

A morphism $f : X \to Y$ over K is said to be separable if $K(X)$ is a separable extension of $K(Y)$. We see that the following morphisms are separable and defined over $\mathbb{F}_q$ for $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$:

$$C \to C_2 \qquad (u, s) \mapsto (u, \sigma := s^3),$$

$$C \to C_3 \qquad (u, s) \mapsto (u, \tau := s^2).$$

We know that both L_{C_2} and L_{C_3} must divide L_C. By Lemma 4.6, we must also have that χ_{C_2} and χ_{C_3} divide χ_C. We find the following characteristic polynomials,

$$\chi_{C_2}(T) = T^6 + 11T^4 + 77T^2 + 343$$

$$\chi_{C_3}(T) = T^8 + 18T^6 + 175T^4 + 882T^2 + 2401.$$

These are two coprime polynomials, which implies $\chi_{C_2} \cdot \chi_{C_3}$ also divides $\chi_{\tilde{C}}$. Reducing the characteristic polynomial of $\tilde{C}$ modulo $\chi_{C_2} \cdot \chi_{C_3}$, gives us

```
(391*b - 29*d + 165)*$.1^13 + (-2825*a + 391*c - 22*e + 165339560)*$.1^12
+ (8514*b - 401*d - 13662)*$.1^11 + (-76158*a + 8857*c - 450*e +
5500609579)*$.1^10 + (102193*b - 4536*d - 277361)*$.1^9 + (-990311*a +
99792*c - 4536*e + 80924527523)*$.1^8 + (766458*b - 31752*d - 2888550)*$.1^7
+ (-8426285*a + 766458*c - 31752*e + 742491265775)*$.1^6 + (3988747*b -
154350*d - 15473759)*$.1^5 + (-47039706*a + 3988747*c - 154350*e +
4350983109193)*$.1^4 + (13311144*b - 487403*d - 45983952)*$.1^3 +
(-166691826*a + 13311144*c - 487403*e + 16086548095933)*$.1^2 + (23882747*b
- 823543*d - 16470860)*$.1 - 322005313*a + 23882747*c - 823543*e +
32779089198989
```

These coefficients should each be zero as the polynomial is reduced modulo a divisor. Finding a, b, c, d, e, f amounts to solving this linear system. One way to do this in Magma is to define a scheme and find the points in it. We do so as follows.

```
A<a,b,c,d,e,f> := AffineSpace(Rationals(),6);
S := Scheme(A,[(391*b - 29*d + f),(-2825*a + 391*c - 22*e + 165339560),
    (8514*b - 401*d),(-76158*a + 8857*c - 450*e + 5500609579),
    (102193*b - 4536*d),(-990311*a + 99792*c - 4536*e +
    80924527523),(766458*b - 31752*d),(-8426285*a + 766458*c -
    31752*e + 742491265775),(3988747*b - 154350*d),(-47039706*a
    + 3988747*c - 154350*e + 4350983109193),(13311144*b -
    487403*d),(-166691826*a + 13311144*c - 487403*e +
    16086548095933),(23882747*b - 823543*d), - 322005313*a +
    23882747*c - 823543*e + 32779089198989]);
Points(S);
```

We get :

```
{@ (204493, 0, 1907045, 0, 15150065, 0) @}
```

Thus we have computed our characteristic polynomial to be

$$\chi_{\tilde{C}}(T) = T^{26} + 48T^{24} + 1135T^{22} + 17651T^{20} + 204493T^{18} + 1907045T^{16} + 15150065T^{14} + 7 \cdot 15150065T^{12}$$
$$+ 7^3 \cdot 1907045T^{10} + 7^5 \cdot 204493T^8 + 7^7 \cdot 17651T^6 + 7^9 \cdot 1135T^4 + 7^{11} \cdot 48T^2 + 7^{13}.$$

To conclude our investigation, we apply Theorem 4.5. Factorizing $\chi_{\tilde{C}}(T)$ into irreducibles over $\mathbb{Q}$ gives us

$$\chi_{\tilde{C}}(T) = (T^2+7)(T^2-T+7)^2(T^2+T+7)^2(T^4-7T^2+49)(T^4+4T^2+49)(T^4+7T^2+49)(T^4+11T^2+49)$$

We see that it has no common factors with $\chi_{E_0}(T) = T^2 + 4T + 7$, and conclude that rank $E'(K) = 0$. We have now that rank $E'(k(u)) \leq$ rank $E'(k(C)) = 0$, implying we have rank $E'(k(u)) = 0$. This allows us to conclude that

$$r_{k(t)}(u^5 - 5u^3 + 5u) = 0,$$

which means $r_{k(t)}(t^{11} + t) = 0$. As we've already seen, having rank zero over $\mathbb{F}_7(t)$ implies we have rank zero over $\mathbb{Q}(t)$, so we can also write $r_{\mathbb{Q}(t)}(t^{11} + t) = 0$. This was the last relevant rank we needed to compute to conclude that

$$\text{rank } E_{360}(\mathbb{Q}(t)) = 2.$$

A Appendix

A.1 Fibre Types

Tate's algorithm, as outlined in [SS10], considers curves in the form

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

If $t \nmid a_2$, the curve is said to have *multiplicative reduction.* If $t \mid a_2$, the curve is said to have *additive reduction.* As t will always divide 0, we conclude the curves we study have additive reduction.

In the proof of Theorem 3.6, we state that our claim holds because we do not encounter type I_0 or type I_n fibres. Chapter C.16 of [Sil09] states the *exponent of the conductor of* E at v, for a field of characteristic $\neq 2, 3$, is given by

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v, \\ 1 & \text{if } E \text{ has multiplicative reduction at } v, \\ 2 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

We can see from Table C.15.1 of [Sil09], fibres of type I_0 and I_n are the only singular fibres for which $f_v \neq 2$, meaning they do not have additive reduction. Hence we know we will not deal with them in our study of curves in the form $y^2 = x^3 + g(t)$.

A.2 Decomposition in Three

Theorem A.1. *Consider a field k containing a primitive third root of unity ω. For an elliptic curve $E : y^2 = x^3 + f(t^3)$, where f is a nonconstant polynomial with $f(0) \neq 0$, we can write*

$$\textit{rank } E(k(t)) = \textit{rank } E_0(k(t)) + \textit{rank } E_2(k(t)) + \textit{rank } E_4(k(t))$$

for $E_i : y^2 = x^3 + t^i f(t)$.

Proof. We again consider $V := E(K) \otimes \mathbb{Q}$. By defining,

$$\phi : E(\overline{\mathbb{Q}}(t)) \otimes \mathbb{Q} \to E(\overline{\mathbb{Q}}(t)) \otimes \mathbb{Q}$$
$$(x(t), y(t)) \mapsto \omega(x(t), y(t)) := (\omega x(t), y(t)),$$

we see that we have a $\mathbb{Q}(\omega)$ structure on V by

$$(a + b\omega) \cdot v := a \cdot P + b \cdot \phi(P), \forall a, b, \in \mathbb{Q}, P \in V.$$

Define the $k(t)$ automorphism

$$\Phi : k(t) \to k(t)$$
$$t \mapsto \omega t.$$

In the same way as in Section 3.2, We see that $k(t)^{<\Phi>} = k(s)$ with $s = t^3$. The three eigenvalues of Φ extended to V as a $\mathbb{Q}(\omega)$-linear automorphism of order 3 are $1, \omega, \omega^2$. Consider the elliptic curve $E_2 : y^2 = x^3 + s^2 f(s)$ over $k(t)$,

$$y(t^3)^2 = x(t^3)^3 + t^6 f(t^3),$$
$$t^6 \Big(\frac{y(t^3)}{t^3}\Big)^2 = t^6 \Big(\frac{x(t^3)}{t^2}\Big)^3 + t^6 f(t^3).$$

If we apply Φ to coordinates of the form $\Big(\frac{x(t^3)}{t^2}, \frac{y(t^3)}{t^3}\Big)$, we find,

$$\Big(\frac{x((\omega t)^3)}{(\omega t)^2}, \frac{y((\omega t)^3)}{(\omega t)^3}\Big) = \Big(\omega \frac{x(t^3)}{t^2}, \frac{y(t^3)}{t^3}\Big) =: \omega \Big(\frac{x(t^3)}{t^2}, \frac{y(t^3)}{t^3}\Big).$$

We see this coordinate transformation defines an isomorphism between $E_2(k(t))$ and V_ω. The other isomorphisms follow similarly. □

A.3 Curves with Degree 3 Coefficients

In certain situations the following method can be applied to find ranks over $\mathbb{Q}(t)$. Andrew Bremner's paper 'Some simple elliptic surfaces of genus 0' outlines a method to explicitly determine the rank of surfaces in the form we are considering, with degree $g(t) \leq 3$. We have no surfaces given by g with degree less than 3, so only the first theorem of this paper is relevant to us.

We consider curves of the form $y^2 = x^3 + g(t)$, with $g(t)$ a squarefree degree 3 polynomial in $\mathbb{Q}(t)$. Translating and scaling g will leave us with a curve of the same rank. (??) For a polynomial $g(t) = a_3t^3 + a_2t^2 + a_1t + a_0$, the translation $t \mapsto (t - \frac{a_2}{3a_3})$ will remove the 2nd power term,

$$g\Big(t - \frac{a_2}{3a_3}\Big) = a_3t^3 - \Big(\frac{a_2^2}{3a_3} - a_1\Big)t + \frac{2a_2^3}{27a_3^2} - \frac{a_1a_2}{3a_3} + a_0.$$

Sending $t \mapsto \alpha t$ for some $\alpha \in \mathbb{Q}^\times$ will give us a curve of the same rank. Why. We also allow multiplication of the polynomial by a 6th power, $g(t) \mapsto \beta^6 g(t), \beta \in \mathbb{Q}^\times$. This is because we can always make a change of coordinates of the form $\xi = \beta^2 x, \eta = \beta^3 y$. If two polynomials are related by a series of these operations we write $g \sim h$. We cite Theorem 1.1 of [Bre91].

Theorem A.2. *For a polynomial $g(t)$ as described above, the rank r of the curve $E : y^2 = x^3 + g(t)$ is,*
i) $r = 2$ if and only if one of the following :
a) $g \sim -t^3 + 16$
b) $\exists\lambda \in \mathbb{Q}$ s.t. $g \sim -t^3 + 3(\lambda^3 + 1)t + (\frac{1}{4}t^6 + 5\lambda t^3 - 2)$
ii) $r = 1$ if and only if $\exists\lambda \in \mathbb{Q}$ with one of the following :
a) $g \sim -t^3 + \lambda^2, 2\lambda \notin \mathbb{Q}^{\times 3}$
b) $g \sim -t^3 + 3(2\lambda + 1)t + (\lambda^2 + 10\lambda - 2), 2\lambda \notin \mathbb{Q}^{\times 3}$
c) $g \sim \lambda t^3 - \frac{1}{3}\lambda^2(\lambda + 1)t + \lambda^2(8\lambda^2 - 20\lambda - 1)/108, \lambda \notin \mathbb{Q}^{\times 3}$
d) $g \sim \lambda t^3 - 3\lambda^2(\lambda + 1)t + \lambda^2(8\lambda^2 - 20\lambda - 1)/4, \lambda \notin \mathbb{Q}^{\times 3}$
e) $g \sim -t^3 + \frac{1}{3}(2\lambda + 1)t - (\lambda^2 + 10\lambda - 2)/27, 2\lambda \notin \mathbb{Q}^{\times 3}$
f) $g \sim \lambda t^3 - 432\lambda^2, \lambda \notin \mathbb{Q}^{\times 3}$
g) $g \sim \lambda t^3 + 16\lambda^2, \lambda \notin \mathbb{Q}^{\times 3}$
h) $g \sim -t^3 - 27\lambda^2, 2\lambda \notin \mathbb{Q}^{\times 3}$
iii) $r = 0$ if and only if g is not equivalent to any of the above forms.

Example A.1. Consider the curve

$$E : y^2 = x^3 + t^3 + t^2.$$

As we have already computed, its rank over $\overline{\mathbb{Q}}(t)$ is 2. Thus its rank over $\mathbb{Q}(t)$ must be 1 or 0. Let us determine this. First we take a translation $t \mapsto t - \frac{1}{3\cdot 1}$ to eliminate the degree 2 term. This gives us

$$\Big(t - \frac{1}{3}\Big)^3 + \Big(t - \frac{1}{3}\Big)^2 = t^3 - \frac{1}{3}t + \frac{2}{27}.$$

Then we send $t \mapsto -t$ and obtain

$$-t^3 + \frac{1}{3}t + \frac{2}{27}$$

After some trial and error, we check to see if this equation is of the form (e), and find :

$$\frac{1}{3} = \frac{1}{3}(2\lambda + 1) \implies \lambda = 0$$

$$\implies -\frac{1}{27}(\lambda^2 + 10\lambda - 2) = \frac{2}{27}.$$

Furthermore, $2\lambda = 0 \notin \mathbb{Q}^{*3}$. Thus we conclude that the rank is 1.

It is considerably more involved to show that the polynomial does not fit any of the defined cases and thus has rank 0, but it can be done for the curve

$$E : y^2 = x^3 + t^3 + t,$$

allowing us to conclude it has rank 0.

References

[Bla+16] I. Blanco–Chacón et al. "Divisibility of L-polynomials for a family of curves". In: *Contemporary Developments in Finite Fields and Applications*. World Sci. Publ., Hackensack, NJ, 2016, pp. 1–10.

[Boo23] Sven Bootsma. *On Certain Elliptic Surfaces With j-Invariant Zero Over Prime Fields of Positive Characteristic*. Masters Thesis. 2023. URL: `https://fse.studenttheses.ub.rug.nl/id/eprint/29188`.

[Bre91] Andrew Bremner. "Some simple elliptic surfaces of genus zero". In: *Manuscripta Mathematica* 73.1 (1991), pp. 5–37.

[CMT00] Jasbir Chahal, Matthijs Meijer, and Jaap Top. "Sections on Certain $j = 0$ Elliptic Surfaces". In: *Comment. Math. Univ. St. Paul.* 49 (2000), pp. 79–89.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. Springer Verlag, New York, 1977.

[Lui07] Ronald van Luijk. "An elliptic K3 surface associated to Heron triangles". In: *Journal of Number Theory* 123.1 (2007), pp. 92–119.

[Mei99] Matthijs Meijer. *High rank elliptic surfaces*. Masters Thesis. 1999. URL: `https://fse.studenttheses.ub.rug.nl/id/eprint/8622`.

[Shi92] Tetsuji Shioda. "Some remarks on elliptic curves over function fields". In: *Astérisque* 209 (1992), pp. 99–114.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, Heidelberg, 2009.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. Springer Verlag, New York, 1994.

[SS10] Matthias Schütt and Tetsuji Shioda. *Elliptic Surfaces*. 2010. URL: `https://arxiv.org/abs/0907.0298`.

[SS19] Matthias Schütt and Tetsuji Shioda. *Mordell-Weil Lattices*. Vol. 70. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer Verlag, Singapore, 2019.

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Vol. 254. Graduate Texts in Mathematics. Springer Science and Business Media, Berlin, 2009.

[Tat66] John Tate. "Endomorphisms of Abelian Varieties over Finite Fields". In: *Inventiones Mathematicae* 2 (1966), pp. 134–144.