An elliptic surface of rank 15

Frank de Zeeuw

July 6, 2006

Contents

1 Introduction

1.1 Elliptic Curves

In general, an elliptic curve is an algebraic curve of genus one with a distinguished point $\mathcal{O}$ on it. Here, it will be enough to think of an equation

$$y^2 = x^3 + ax + b$$

with a, b in a field k of characteristic not 2 or 3, such that $16a^3 + 27b^2 \neq 0$. Such an equation defines a set $E(K)$ over any field extension K of k, namely the set of $(x, y) \in K^2$ that satisfy the equation, together with a point $\mathcal{O}$ at infinity.
The main tool for analyzing the arithmetic of such curves, i.e. the existence of points other than $\mathcal{O}$ in $E(K)$ for different K, is the fact that the set of points on E forms an abelian group. The group law is defined geometrically, as illustrated in the following picture:

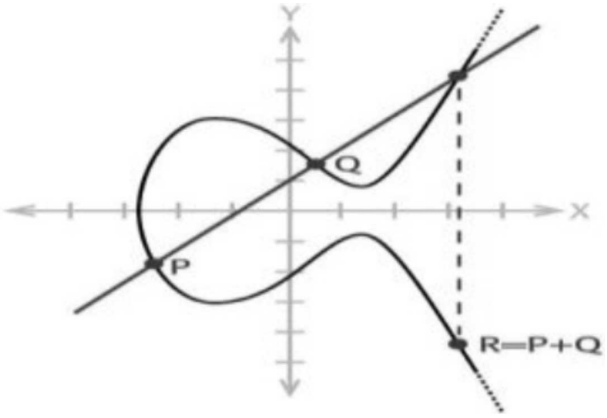


Figure 1: The group law on an elliptic curve.

Given two points P and Q on the elliptic curve, we can consider a straight line through them, which will intersect the curve in a third point. Then we take the reflection of that point in the x-axis as the sum of P and Q. To get $P+P$, we do the same for the tangent line at P, which will also intersect the curve in one other point. Finally $-P$ is the reflection of P in the x-axis. In this way we get a group law, with the point at infinity as the zero element. It has the property that if P and Q are in $E(K)$, then so are $P + Q$ and $-P$, making every $E(K)$ into a group.
Most of the research on elliptic curves has focused on the algebraic structure of this group, called the Mordell-Weil group. The name comes from the most important result on it:

Theorem 1 (Mordell-Weil)**.** *For any elliptic curve E defined over a number field K, the Mordell-Weil group $E(K)$ is finitely generated.*

This implies that $E(K) \cong \mathbb{Z}^r \oplus E_{\text{tor}}$, where E_{tor} is the finite group of all points of finite order, and r is called the rank of the group $E(K)$. The structure of E_{tor} is usually easy to determine. Over $\mathbb{Q}$, for instance, Mazur proved that its order is at most 16, and the torsion points can be efficiently determined by the Nagell-Lutz theorem [Si0].
The free part, specifically the rank r, has proved to be a tougher nut to crack. The rank is conjectured to be unbounded, but at the time of writing the highest known rank of an explicit example over $\mathbb{Q}$ is 28, recently found by Elkies (May 2006). Furthermore, no finite algorithm or method is known which can determine the rank for every elliptic curve (say, over $\mathbb{Q}$), much less for finding explicit generators. In short, determining ranks of elliptic curves is a big open problem in number theory today.

1.2 Elliptic Curves over Function Fields

We now consider elliptic curves over, for instance, $\mathbb{Q}(t)$. Then an equation like

$$y^2 = x^3 - t^2x + t^2$$

defines an elliptic curve over $\mathbb{Q}(t)$. Its points are pairs $(x(t), y(t))$ with $x(t), y(t)$ rational functions in $\mathbb{Q}(t)$ satisfying the equation. In this case we have for example the point (t, t).
The proof of the Mordell-Weil theorem can also be extended to elliptic curves over function fields (see [Si2, Ch. III]):

Theorem 2 (Mordell-Weil over function fields)**.** *Let E be an elliptic curve defined over $k(t)$, with k a finite extension of its prime field. Assume there is no elliptic curve E_0 over k such that $E \cong E_0 \otimes k(t)$.*
Then $E(k(t))$ is finitely generated.

It is also conjectured that the rank of $E(k(t))$ can be arbitrarily high, and an example over $\overline{\mathbb{Q}}(t)$ has been found with rank 68 (see [Sh2]). When such curves are defined over $\mathbb{Q}(t)$, they can be helpful in finding elliptic curves over $\mathbb{Q}$ of high rank.

1.3 Elliptic Surfaces

There is another way to look at an elliptic curve over a function field. Since its equation contains three variables, it defines a surface in three-dimensional space. We call this an *elliptic surface*, a notion we will define exactly in the next chapter. For now, the point is that the geometry of the surface can be used to investigate the arithmetic structure of the elliptic curve, in particular the rank.

For instance, algebraic surfaces are classified by their geometric genus p_g, and per class the Mordell-Weil rank is known to satisfy $r \leq 10p_g + 8$. If $p_g = 0$, the surfaces are called *rational*, and the upper bound for the rank is 8. For all $r \leq 8$, explicit examples with that rank can easily be found. For $p_g = 1$, the surfaces are called *K3 surfaces* and finding such examples is already harder.
In 1982, Cox [Cox] proved that examples exist for all $r \leq 18$, but his proof was not constructive. In 2000, Kuwata [Kuw] gave explicit examples for all $r \leq 18$, except for the case $r = 15$. In his thesis [Kl1], Kloosterman constructed a family of elliptic K3 surfaces with generic rank 15. After this, in [Kl2] he proved the rank of one member of this family to be exactly 15, thereby completing the list of Kuwata. In his proof he used the difficult Artin-Tate conjecture, which has been proved for K3 surfaces, but is still a conjecture for most other classes of varieties. It is this I seek to improve upon, by redoing his proof using more elementary, though somewhat lengthier, computations. This could prove useful for cases in which the Artin-Tate conjecture is not known to hold.

1.4 Outline

In chapter 2 I will define elliptic surfaces and most of the tools I will need. Chapter 3 will explain the method used to determine the rank. The method stems mostly from Kloosterman and is based on work of Van Luijk [Lu1], but is made more elementary, and hopefully more general. Chapter 4 will then apply the method to a family of elliptic surfaces of rank 2. The result was already known and can be proved in an easier way, but I could not find it in the literature. Therefore it seemed useful to record it here, especially since it provided a good test case for this method, and a practice case for me. In chapter 5 I finally apply the method to a member of Kloosterman's family, to show that it has rank 15.

2 Elliptic Surfaces

2.1 Definitions

Let k be a perfect field of characteristic not 2 or 3, and let $\mathbb{P}^1 = \mathbb{P}^1(k)$.

Definition 1. *An* elliptic surface *is a smooth projective surface $\mathcal{E}$, such that:*

- *There is a morphism $\pi : \mathcal{E} \to \mathbb{P}^1$, such that for all but finitely many points $t \in \mathbb{P}^1$, the fiber $\mathcal{E}_t := \pi^{-1}(t)$ is a non-singular curve of genus 1.*
- *There is a distinguished section to π, i.e. a map $\sigma_0 : \mathbb{P}^1 \to \mathcal{E}$ such that $\pi \circ \sigma_0 = id_{\mathbb{P}^1}$. We call this the zero section.*
- *The surface $\mathcal{E}$ is minimal with the properties above.*

For example, the equation $y^2 = x^3 - t^2x + t^2$ defines an elliptic surface $\mathcal{E}$, by first taking the Zariski closure of the set

$$\{\, ([X, Y, Z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 \mid t \neq \infty, Y^2Z = X^3 - t^2XZ^2 + t^2Z^3 \,\},$$

and then resolving the two singular points, by repeatedly blowing them up. From now on, when we talk about an elliptic surface given by some equation, we will mean the variety resulting from taking the affine surface defined by the equation, projectivizing it, and resolving the singular points.
The morphism $\pi : \mathcal{E} \to \mathbb{P}^1$ in the example then corresponds to the projection

$$(x, y, t) \mapsto t,$$

and the zero section is

$$\sigma_0 \colon t \mapsto ([0, 1, 0], t).$$

We call this the zero section because it is the zero element in the group of sections, defined as

$$\mathcal{E}(\mathbb{P}^1/k) := \{\, k\text{-morphisms } \sigma \colon \mathbb{P}^1 \to \mathcal{E} \text{ such that } \pi \circ \sigma = id_{\mathbb{P}^1} \,\}.$$

To define the addition of this group, we can use the fact that almost every fiber $\mathcal{E}_t = \pi^{-1}(t)$ is an elliptic curve, so we can add sections fiber-by-fiber. Let $\sigma_1, \sigma_2 \in \mathcal{E}(\mathbb{P}^1)$ be sections. Then for all t such that $\mathcal{E}_t$ is non-singular, we can define

$$(\sigma_1 + \sigma_2)(t) := \sigma_1(t) + \sigma_2(t),$$

where the '+' on the right is addition on $\mathcal{E}_t$. Defined this way, $\sigma_1 + \sigma_2$ is a rational map $\mathbb{P}^1 \to \mathcal{E}$. Since $\mathbb{P}^1$ is non-singular and $\mathcal{E}$ is projective, this is a morphism, hence an element of $\mathcal{E}(\mathbb{P}^1/k)$.
Note that this does not define a group structure on the set of points of the

surface, but on the set of sections. In fact, a section $t \mapsto (x(t), y(t), t)$ could just as well be viewed as a point $(x(t), y(t))$ on the elliptic curve over $k(t)$ defined by the same equation. See [Si2, p. 210] for an exact proof of the isomorphism $\mathcal{E}(\mathbb{P}^1/k) \cong E(k(t))$. So actually this group of sections is just another instance of a Mordell-Weil group, and it follows from the Mordell-Weil theorem for elliptic curves over function fields (Theorem 2) that it is finitely generated.

2.2 An example

Let's look at the example $y^2 = x^3 - t^2x + t^2$ in more detail.
In the picture on the left you see the affine surface defined by this equation, with the t-axis oriented vertically. The horizontal contour lines are the fibers $\pi^{-1}(t)$, for t an integer. On the right you see the surface with several sections drawn on it.

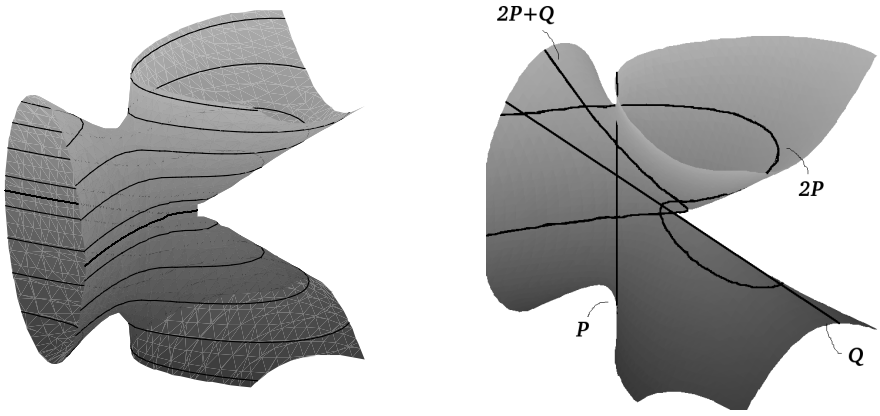


Figure 2: The surface $y^2 = x^3 - t^2x + t^2$.

Two of those sections are easy to find right away:

$$P = (1, 1) \text{ and } Q = (t, t).$$

In the picture, P is the vertical line down the middle, and Q is the line going from the top left to bottom right corner. Both of these are straight lines, but by applying the group law we obtain sections $mP + nQ$, most of which will be rational functions of higher degree. For instance,

$$2P + Q = \left(\frac{t^3 + 2t^2 - 3t}{t^2 + 2t + 1}, -\frac{t^4 - t^3 - 9t^2 + t}{t^3 + 3t^2 + 3t + 1} \right)$$

Below we will see that the Mordell-Weil group of this surface has rank 2. It seems plausible to guess that P and Q are generators, since they are linear, and the addition usually increases degree. To prove this, we will have to look more closely at the geometry of the surface.

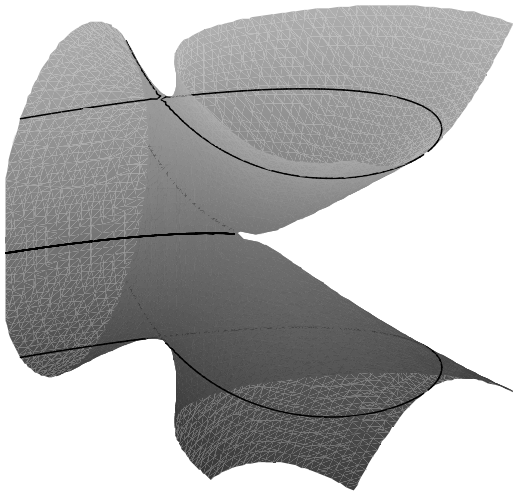


Figure 3: Three singular fibers on $y^2 = x^3 - t^2x + t^2$.

2.3 Singular fibers

First of all, consider the fibers on the surface. We know that almost all are elliptic curves, but which ones are not? In other words, which ones are singular curves? Visually, we can make out that $\mathcal{E}_0$ is a cusp, and that above and below that there are two nodes.

To determine these exactly, we look at the discriminant of the equation. Since an elliptic curve $y^2 = x^3 + ax + b$ is singular if and only if its discriminant $4a^3 + 27b^2$ vanishes, the singular fibers of our surface are given by the t for which

$$\Delta_t = t^4(-4t^2 + 27)$$

vanishes, i.e. $t = 0$ and $t = \pm\sqrt{27}/2$. But we must not forget to check the fiber at $t = \infty$! To inspect that one we first change coordinates to $s = 1/t$, so that the equation becomes, after substituting $\xi = s^2x$, $\eta = s^3y$ and multiplying by s^6:

$$\eta^2 = \xi^3 - s^2\xi + s^4,$$

which has discriminant

$$\Delta_s = s^6(-4 + 27s^2).$$

Hence there is also a singular fiber at $t = \infty$, where $s = 0$.
Each of the singular fibers contains a point that is singular on that fiber. However, those points are not necessarily singular points on the surface. In fact, only the points $(x, y, t) = (0, 0, 0)$ and $(\xi, \eta, s) = (0, 0, 0)$ are singular

points on the surface; the other two are smooth.
It is these singular points on the surface that are blown up to make the surface smooth. The minimality then means that the surface is not blown up too far, i.e. after any blow-down the surface would be singular, or π would no longer be a morphism. We will just look at the resulting surface set-theoretically: $\mathcal{E}$ consists of the set of points on the affine surface defined by the equation, except that all singular points on singular fibers are replaced by certain curves.
This may seem a bit mysterious, but the good thing is that the possible structures that can occur for the blown-up singular fibers on such a model, have been completely classified by Kodaira [Kod], and Tate [Tat] has given an algorithm to determine the structure in any given case. The results of Tate's algorithm are summarized in table 1.

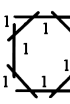
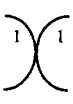
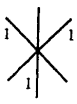
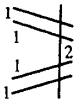
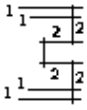
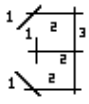
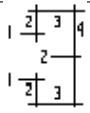
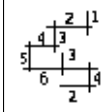
type	I_0	I_k	II	III	IV	I_0^*	I_k^*	IV^*	III^*	II^*
										
#components	1	k	1	2	3	5	5+k	7	8	9
$v(\Delta)$	0	k	2	3	4	6	6+k	8	9	10
j-invariant	$v(j)\geq 0$	$v(j)=-k$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$	$v(j)\geq 0$	$v(j)=-k$	$\tilde{j}=0$	$\tilde{j}=1728$	$\tilde{j}=0$

Table 1: All possible singular fiber structures with their properties.

Determining the structure of a singular fiber at t now comes down to computing the order of vanishing of the discriminant t and seeing which structure in the table matches that. If there are more possibilities, the order of vanishing of the j-invariant will solve that.
Let's work this out for our example. We see that the discriminant vanishes to order 1 if we take $t = \pm\sqrt{27}/2$, which only happens for a fiber of type I_1, i.e. a node. That makes sense, because the singular points on the fibers $\pi^{-1}(\pm\sqrt{27}/2)$ were smooth points on the surface, so didn't have to be blown up.
The fiber $\pi^{-1}(0)$ could be of type IV or I_4. So we have to look at the j-invariant, which is

$$j(\mathcal{E}) = 2^8 3^3 \frac{a(t)^3}{4a(t)^3 + 27b^2} = 2^8 3^3 \frac{t^2}{4t^2 - 27}.$$

Since at $t = 0$ this vanishes to order 2, we have a fiber of type IV.
Finally, for the fiber at $t = \infty$ the discriminant vanishes to order 6, so we could have type I_6 or I_0^*. The j-invariant does not have a pole there, so we have type I_0^*.

2.4 The Néron-Severi Lattice

Following Shioda [Shi], we will introduce a larger group related to the Mordell-Weil group, called the Néron-Severi group, for which some very useful theorems hold.

Definition 2. *The* Néron-Severi group $\mathrm{NS}(\mathcal{E})$ *of a surface* $\mathcal{E}$ *is the group of divisors on* $\mathcal{E}$ *modulo algebraic equivalence.*

This definition is not so easy to understand, but luckily we will not need it explicitly here. We will just state the results that Shioda derived, and work from those. To at least explain what the words mean: a *divisor* on a surface is a finite $\mathbb{Z}$-linear combination of irreducible curves on S. For an exact definition of algebraic equivalence, see [Har, exercise V.1.7].
In [Shi], the following properties of the Néron-Severi group $\mathrm{NS}(\mathcal{E})$ of an elliptic surface are proven:

- Let T be the subgroup of $\mathrm{NS}(\mathcal{E})$ generated by the zero section, one smooth fiber and all the irreducible components of singular fibers that do not meet the zero section. Then
$$\mathrm{NS}(\mathcal{E})/T \cong \mathcal{E}(\mathbb{P}^1/k) \cong E(k(t)).$$
- The rank of T is $2 + \sum_{t\in S}(m_t - 1)$, where S is the set of t such that the fiber $\pi^{-1}(t)$ is singular, and m_t is the number of components of $\pi^{-1}(t)$. It follows that
$$\operatorname{rank} E(k(t)) = \operatorname{rank} \mathrm{NS}(\mathcal{E}) - 2 - \sum_{t\in S}(m_t - 1). \tag{1}$$
This formula is called the Shioda-Tate formula.

As the title of this section already gives away, the Néron-Severi group has a lattice structure. Since there are several variants of the definition of a lattice, we give the appropriate one here:

Definition 3. *A* lattice *is a free* $\mathbb{Z}$*-module* L *of finite rank, together with a symmetric non-degenerate bilinear pairing*
$$\langle \cdot, \cdot \rangle \colon L \times L \to \mathbb{Q}.$$

Since we already know $\mathrm{NS}(\mathcal{E})$ to be a finitely generated abelian group without torsion, all we need is a pairing of this kind. It turns out that the intersection pairing will do.

Definition 4. *The* intersection pairing *is the unique symmetric bilinear pairing*
$$\mathrm{Div}(\mathcal{E}) \times \mathrm{Div}(\mathcal{E}) \to \mathbb{Z} \tag{2}$$
$$(D_1, D_2) \mapsto (D_1 \cdot D_2), \tag{3}$$
where $(D_1 \cdot D_2)$*, called the* intersection number*, is such that*

- *If Γ_1 and Γ_2 are irreducible curves on $\mathcal{E}$ that meet everywhere transversally, we have*
$$(\Gamma_1 \cdot \Gamma_2) = \#(\Gamma_1 \cap \Gamma_2).$$
- *If D_1 is linearly equivalent to D_2, then $(D \cdot D_1) = (D \cdot D_2)$ for any divisor D.*

If the two divisors D_1, D_2 meet in a single point P the intersection paring can be computed as

$$(D_1 \cdot D_2) = \dim_k \mathcal{O}_{\mathcal{E},P}/(f_1, f_2),$$

where $\mathcal{O}_{\mathcal{E},P}$ is the local ring at P, and f_1, f_2 are local equations for D_1 resp. D_2 (see [Si2, III.7]).
It can be proven that $(D_1 \cdot D_2)$ depends only on the algebraic equivalence classes of D_1 and D_2, so that this pairing on $\mathrm{Div}(\mathcal{E})$ induces a well-defined pairing on $\mathrm{NS}(\mathcal{E})$. By [Shi, Th. 3.1], it is non-degenerate, so that it makes $\mathrm{NS}(\mathcal{E})$ into a lattice.
Shioda goes on to show that

$$E(k(t))/E(k(t))_{\mathrm{tor}} \cong \mathrm{NS}(\mathcal{E}) \otimes \mathbb{Q}.$$

This means that we also have a lattice structure on the Mordell-Weil group modulo torsion (which explains the title of Shioda's article, "On the Mordell-Weil lattices").
We will denote the resulting pairing on $E(k(t))$, multiplied by -1, by $\langle \cdot, \cdot \rangle$. It is called the *height pairing* and is related to the arithmetic height funtion on an elliptic curve. The important thing for us is that Shioda ([Shi, Th. 8.6]) gives an explicit formula for the height pairing.

Theorem 3. *For $P, Q \in E(k(t))$,*

$$\langle P, Q \rangle = \chi + (P \cdot O) + (Q \cdot O) - (P \cdot Q) - \sum_{t \in S} \mathrm{contr}_t(P, Q) \tag{4}$$

$$\langle P, P \rangle = 2\chi + 2(P \cdot O) - \sum_{t \in S} \mathrm{contr}_t(P, P), \tag{5}$$

where S is the set of $t \in \mathbb{P}^1$ such that $\mathcal{E}_t$ is singular.

Here χ is the arithmetical genus of the surface (see next section), and the contr_t are contributions of the singular fibers, which can be determined as follows. For each singular fiber $\mathcal{E}_t$, if P or Q intersects $\mathcal{E}_t$ in the same component as the zero section intersects, then $\mathrm{contr}_t(P, Q) = 0$. Otherwise, see if P and Q intersect the **same** component (or $P = Q$), or **different** components, and read off $\mathrm{contr}_t(P, Q)$ from table 2 (where we only show the cases that we will need in this text).

fiber type:	III	III^*	IV	I_0^*
same:	$\frac{1}{2}$	$\frac{3}{2}$	$\frac{2}{3}$	1
different:	—	—	$\frac{1}{3}$	$\frac{1}{2}$

Table 2: The contributions at some singular fibers.

We could use this, for instance, to determine if a number of points $\{P_i\}_{i\in I}$ are independent in the Mordell-Weil group of an elliptic surface. That is equivalent to the points being independent in the lattice, which is true if and only if their discriminant

$$\mathrm{D} = \det(\langle P_i, P_j\rangle)_{i,j\in I}$$

is non-zero.
Let's apply this to our example $y^2 = x^3 - t^2x + t^2$. To show that the points $P = (1, 1)$ and $Q = (t, t)$ are independent, we have to show that

$$\det\begin{pmatrix}\langle P,P\rangle & \langle P,Q\rangle\\ \langle Q,P\rangle & \langle Q,Q\rangle\end{pmatrix} \neq 0.$$

Now we have to compute several things.

- $\chi = 1$, see the next section
- $(P \cdot O) = 0$, $(Q \cdot O) = 0$
- $(P \cdot Q) = \dim k[t]_{(t-1)}/t = 1$
- The contributions (the I_1 fiber always has contribution 0):
  - contr(P): At $t = 0$, we have a fiber of type IV, and P intersects $\mathcal{E}_0$ away from the singular point, so in the same component as the zero section, which gives a contribution 0. At $t = \infty$, we have a fiber of type I_0^*, and there P does intersect the fiber in the singular point, so that we get a total contribution of 1.
  - contr(Q): At both $t = 0$ and $t = \infty$, Q intersects the fiber in its singular point, which gives a total contribution of 5/3.
  - contr(P, Q): The total contribution is 1/2.

This give us the following results

$$\langle P, P\rangle = 2 + 0 - 1 = 1 \tag{6}$$

$$\langle Q, Q\rangle = 2 + 0 - \frac{5}{3} = \frac{1}{3} \tag{7}$$

$$\langle P, Q\rangle = \langle Q, P\rangle = 1 + 0 + 0 - 1 - \frac{1}{2} = -\frac{1}{2}, \tag{8}$$

with which we can compute the determinant:

$$D = \det \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{3} \end{pmatrix} = \frac{1}{12}.$$

Therefore P and Q are independent. In the next section we will see that the Mordell-Weil group has rank 2 in this example, so we have almost proven that P and Q form a basis, except that the subgroup generated by P and Q could be of finite index.
Suppose the subgroup generated by P and Q has index n in $E(k(t))$. Since its determinant is $1/12$, it follows from basic lattice theory that $E(k(T))$ has determinant $\frac{1}{12n^2}$. But if we look more closely at the formulas (4) and (5), we see that all terms are integers, except for the contributions. In Table 2 we can see that the only possible denominators (in this example) are 2 and 3. It follows that the denominator of a determinant of two points in $E(k(t))$ could be at most 36. That means that the only index that can occur is $n = 1$. We can conclude:

Theorem 4. *The points $P = (1, 1)$ and $Q = (t, t)$ form a basis for the Mordell-Weil group of the elliptic surface defined by $y^2 = x^3 - t^2x + t^2$.*

2.5 Classification of Surfaces

We will quickly introduce some invariants of elliptic surfaces that will be useful in this text.
Let $\mathcal{E}$ be defined by an equation

$$y^2 = x^3 + a(t)x + b(t), \qquad a(t), b(t) \in k[t] \text{ not both constant,}$$

which is minimal, i.e. there is no non-constant $f \in k[t]$ such that $f^4 \mid a(t)$ and $f^6 \mid b(t)$ (otherwise we could make the equation simpler by putting $x(t) = f^2x'(t)$, $y(t) = f^3y'(t)$ and dividing by f^6).
Let N be the minimal integer such that

$$\deg(a(t)) \leq 4N \text{ and } \deg(b(t)) \leq 6N.$$

Fact. The surface $\mathcal{E}$ is called *rational* if $N = 1$, and it is called a *K3* surface if $N = 2$.

Fact. The Euler characteristic χ of $\mathcal{E}$ equals N, and the geometric genus p_g equals $N - 1$.

Our example has $a(t) = -t^2$ and $b(t) = t^2$, so that $N = \chi = 1$, $p_g = 0$, and the surface is rational.
Recall that in the introduction we gave a relation between the geometric genus and the highest possible rank of an elliptic surface; we can expand a

little on that now. A general cohomology argument shows that the Néron-Severi rank of an elliptic surface is 10, so that the Shioda-Tate formula (1) gives us the Mordell-Weil rank

$$r = 8 - \sum (m_t - 1),$$

where the sum is over the singular fibers. In the example, the fibers of type IV, I_0^* and I_1 have m_t equal to 3, 5, and 1. So we get

$$r = 8 - 2 - 4 = 2,$$

as we desired.

3 Strategy

We will outline our method for determining the rank of an elliptic surface in certain cases.
Let $\mathcal{E}$ be the elliptic surface over k and E the corresponding elliptic curve over $k(t)$. Since we will be looking at the lattice structure of $E(k(t))$, we will have to disregard the torsion subgroup. We will do this by tensoring with $\mathbb{Q}$, and abbreviating as follows:

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

Clearly the rank of E_k equals that of $E(k(t))$.
First of all we need the following lemma, true for every prime p where E has good reduction:

Lemma 1. *The reduction map $E_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{F}}_p}$ is injective.*

Proof. See [Lu1, Proposition]. □

If we can determine the rank n of $E_{\overline{\mathbb{F}}_p}$ for a prime p of good reduction, this lemma says that n is an upper bound for the rank of $E_{\overline{\mathbb{Q}}}$. Suppose we can also prove $n-1$ to be a lower bound. This could be done by finding $n-1$ independent points on $E_{\overline{\mathbb{Q}}}$, or it could simply be zero if $n = 1$. Then consider the following lemma:

Lemma 2. *If $E_{\overline{\mathbb{Q}}}$ has the same rank as $E_{\overline{\mathbb{F}}_p}$, then the determinants of the lattices $E_{\overline{\mathbb{Q}}}$ and $E_{\overline{\mathbb{F}}_p}$ differ only by a square.*

Proof. If $E_{\overline{\mathbb{Q}}}$ has the same rank as $E_{\overline{\mathbb{F}}_p}$, then the injection $E_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{F}}_p}$ makes $E_{\overline{\mathbb{Q}}}$ into a sublattice of $E_{\overline{\mathbb{F}}_p}$. Basic lattice theory then tells us that it has a finite index $[E_{\overline{\mathbb{F}}_p} : E_{\overline{\mathbb{Q}}}]$ and that

$$\det(E_{\overline{\mathbb{Q}}}) = [E_{\overline{\mathbb{F}}_p} : E_{\overline{\mathbb{Q}}}]^2 \cdot \det(E_{\overline{\mathbb{F}}_p}),$$

which proves the lemma. □

The first thing to try would be to compute both these determinants, see if they differ by a square, and if not, conclude that $E_{\overline{\mathbb{Q}}}$ and $E_{\overline{\mathbb{F}}_p}$ do not have the same rank. However, to compute the determinant of $E_{\overline{\mathbb{Q}}}$ we would have to know its rank, which is what we are trying to find. We can work around this as follows.
Suppose we have two primes p, q of good reduction, such that both $E_{\overline{\mathbb{F}}_p}$ and $E_{\overline{\mathbb{F}}_q}$ have rank equal to the upper bound n, and suppose we can find n independent points for both. Then we can calculate the determinant of each, and see if they differ by a square. If they do not, they cannot both differ by a square from the determinant of $E_{\overline{\mathbb{Q}}}$. Hence by Lemma 2, the rank of $E_{\overline{\mathbb{Q}}}$ is not n, so must be $n-1$.

Note that it is enough to find independent points on $E_{\overline{\mathbb{F}}_p}$ and $E_{\overline{\mathbb{F}}_q}$, instead of a basis, since the determinant of n independent points will differ from the determinant of a basis by a square, which we can ignore, since we consider the determinants modulo squares anyway.

4 The curve $f(t)y^2 = f(x)$

We will now apply the method from the previous chapter to a specific example.

4.1 The curve

Let $f(x) = x^3 + ax + b$ for $a, b \in \mathbb{Q}$, and let $E'/\mathbb{Q}$ be the elliptic curve given by a Weierstrass equation $y^2 = f(x)$. We can consider it as a curve over the function field $\mathbb{Q}(t)$, but also as a curve over the extension $\mathbb{Q}(t, s)$, obtained by adjoining s satisfying $s^2 = t^3 + at + b$.
Over $\mathbb{Q}(t, s)$, we can make a coordinate change $\eta = \frac{y}{s}$, which gives $y^2 = s^2\eta^2 = (t^3 + at + b)\eta^2$, to get a new elliptic curve (replacing η by y again):

$$E : (t^3 + at + b)y^2 = x^3 + ax + b$$

defined over $\mathbb{Q}(t)$. Writing $f(u) = u^3 + au + b$, we can shorten it to

$$E : f(t)y^2 = f(x).$$

Over $\mathbb{Q}(t, s)$, the two curves E' and E are isomorphic, since there is a coordinate change between them. However, because the coordinate change involves s, they are not isomorphic over $\mathbb{Q}(t)$. In the following we will try to determine some of the structure of E over $\mathbb{Q}(t)$, in particular the rank.
We have chosen this curve because its structure can be determined in an elementary way, using an isomorphism

$$E(k(t))/E[2](k(t)) \;\cong\; \mathrm{End}_k(E'),$$

where k is any field of characteristic not 2 or 3.
We will try to calculate the rank of E by our method from chapter 3, which will actually be harder to work out. Nevertheless, we will use it as a test case, with the comfort of being able to check the result via the isomorphism. The isomorphism follows from the following proposition:

Proposition 1. *Let α and β be the maps*

$$\begin{array}{ccccc} E(k(t)) & \xrightarrow{\alpha} & Mor_k(E', E') & \xrightarrow{\beta} & End_k(E') \\ (x(t), y(t)) & \longmapsto & ((u, v) \mapsto (x(u), v \cdot y(u))) & & \\ & & \psi & \longmapsto & \tau_{-\psi(\mathcal{O})}\psi. \end{array}$$

The map $\varphi = \beta \circ \alpha$ is an onto group homomorphism with kernel $E[2](k(t))$.

The main idea here is the definition of α. It would be very convenient if α would just map to $\mathrm{End}_k(E')$, and it almost does. However, the points of order 2 in $E(k(t))$, i.e. the points $(t_i, 0)$ with t_i a root of f, are sent to the maps $(u, v) \mapsto (x(t_i), 0)$, which do not map $\mathcal{O}$ to $\mathcal{O}$, so are not

endomorphisms. Because of this little problem, the proof requires a lot of detail, so we will work it out separately, in section 4.5.
Now we state our main theorem, and give a relatively simple proof of it, using the isomorphism from the proposition.

Theorem 5. *The rank of $E(\mathbb{Q}(t))$ is 1.*

Proof. We will show that $\mathrm{End}_{\mathbb{Q}}(E')$ has rank 1, so that the theorem follows from the proposition.
The identity on E' is in $\mathrm{End}_{\mathbb{Q}}(E')$ and has infinite order, so we have inclusions

$$\mathbb{Z} \subseteq \mathrm{End}_{\mathbb{Q}}(E') \subseteq \mathrm{End}_{\overline{\mathbb{Q}}}(E').$$

By Silverman (1986, Th.VI.6.1b, p.165), $\mathrm{End}_{\overline{\mathbb{Q}}}(E')$ is either $\mathbb{Z}$ or an order in a quadratic imaginary extension of $\mathbb{Q}$. In the first case we are done, in the second case we have $\mathrm{End}_{\mathbb{Q}}(E') \subseteq \mathbb{Z}[\alpha]$ with $\alpha \in \mathbb{C} - \mathbb{R}$ satisfying $\alpha^2 - t\alpha + d = 0$.
Now the morphisms in $\mathrm{End}_{\overline{\mathbb{Q}}}(E')$ that are in $\mathrm{End}_{\mathbb{Q}}(E')$ are precisely the ψ that satisfy $\psi^*\omega = \lambda_\psi \omega$ with $\lambda_\psi \in \mathbb{Q}$, where $\omega = dx/2y$ is the invariant differential on E'. But α, and similarly any multiple of α, has $\alpha^*\omega = \lambda_\alpha$ with $\lambda_\alpha \notin \mathbb{R}$. Therefore $\mathrm{End}_{\mathbb{Q}}(E')$ does not contain any multiple of α, so has rank 1.

□

As we said, we will ignore this proof, and try to reach the result by our method from chapter 3.
We will use the following two propositions, true for every prime p such that E' has good reduction at p:

Proposition 2. *The rank of $E(\mathbb{F}_p(t))$ is 2.*

Proof. We again use the isomorphism from above, now for $k = \mathbb{F}_p$, so that we only have to show that $\mathrm{End}_{\mathbb{F}_p}(E')$ has rank 2.
On the one hand, $\mathrm{End}_{\mathbb{F}_p}(E')$ contains the module $\mathbb{Z}[\phi]$, generated by the identity on E' and the Frobenius morphism $\phi : (x, y) \mapsto (x^p, y^p)$. This has rank 2 since ϕ satisfies $\phi^2 - t\phi + p \cdot id = 0$. On the other hand, it is contained in $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$, so we have:

$$\mathbb{Z}[\phi] \subseteq \mathrm{End}_{\mathbb{F}_p}(E') \subseteq \mathrm{End}_{\overline{\mathbb{F}}_p}(E').$$

From Silverman (1986, Th.. V.3.1, p. 137) we know that $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$ is an order in either a quadratic imaginary field, or in a quaternion algebra. In the first case it has rank 2, which would imply that $\mathrm{End}_{\mathbb{F}_p}(E')$ has rank 2 as well. In the second case, we observe that the morphisms of $\mathrm{End}_{\overline{\mathbb{F}}_p}(E')$ that are in $\mathrm{End}_{\mathbb{F}_p}(E')$ are precisely the ones that commute with ϕ. Now, in a quaternion algebra, there are at most two independent elements that commute with

one another. Hence $\mathrm{End}_{\mathbb{F}_p}(E')$ cannot contain an element independent from id and ϕ, for that would give three commuting independent elements in a quaternion algebra. Therefore $\mathrm{End}_{\mathbb{F}_p}(E')$ must have rank 2 in this case as well, finishing our proof.

□

Remark. We can also use the isomorphism to pinpoint two independent elements of $E(\mathbb{F}_p(t))$, by finding inverse images for the two independent elements $id_{E'}$ and the Frobenius ϕ in $\mathrm{End}_{\mathbb{F}_p}(E')$. The first is clearly $\varphi(P)$ for $P = (t, 1) \in E(\mathbb{F}_p(t))$. The second is given by $(t, s) \mapsto (t^p, s^p)$, so suppose $\varphi(x(t), y(t)) = (t^p, s^p)$. Then $x(t) = t^p$ and $sy(t) = s^p$, so

$$y(t) = s^{p-1} = (s^2)^{\frac{p-1}{2}} = f(t)^{\frac{p-1}{2}}.$$

The point $Q = (t^p, f(t)^{\frac{p-1}{2}})$ is indeed in $E(\mathbb{F}_p(t))$ since

$$f(t)(f(t)^{\frac{p-1}{2}})^2 = f(t)^p = (t^3 + at + b)^p = (t^p)^3 + at^p + b = f(t^p).$$

It follows that P and Q are independent points of infinite order. However, it is not necessarily true that P and Q form a basis for $E(\mathbb{F}_p(t))$, because $\mathbb{Z}[\phi]$ might have a finite index in $\mathrm{End}_{\mathbb{F}_p}(E')$.
For example, consider the curve $y^2 = x^3 - x$ over $\mathbb{F}_5$. Then $\overline{2} \in \mathbb{F}_5$ is a square root of -1, and there is an endomorphism

$$i : (x, y) \mapsto (-x, \overline{2}y)$$

which is not in $\mathbb{Z}[\phi]$. In fact, the Frobenius ϕ satisfies

$$\phi = [-1] + [2] \circ i,$$

which can be proven with some (computer) algebra. It follows that $\mathbb{Z}[\phi]$ has index 2 in $\mathbb{Z}[i]$, so it also has index greater than two in $\mathrm{End}_{\mathbb{F}_p}(E')$.

Since $E(\mathbb{Q}(t))$ injects into $E(\mathbb{F}_p(t))$, it follows that

$$\text{rank } E(\mathbb{Q}(t)) \leq 2.$$

Furthermore, in the remark after Proposition 2 we saw the point $P = (t, 1)$ in $E(\mathbb{F}_p)$, which can easily be checked to be in $E(\mathbb{Q}(t))$, and that its image under the group homomorphism

$$E(\mathbb{Q}(t)) \longrightarrow E(\mathbb{F}_p(t)) \longrightarrow \mathrm{End}_{\mathbb{F}_p}(E')$$

is $id_{E'}$. It follows that $(t, 1)$ is a point of infinite order, so that

$$\text{rank } E(\mathbb{Q}(t)) \geq 1.$$

Our goal in this chapter will be to prove the following claim, which will complete the argument:

Proposition 3. *The rank of $E(\mathbb{Q}(t))$ is not 2.*

We will explicitly calculate the determinant of $E(\mathbb{F}_p(t))$ for two prime numbers p_1, p_2 not equal to 2 or 3. We hope to see that these determinants do not differ by a square, for then by chapter 3 it would follow that $E(\mathbb{Q}(t))$ has rank 1.

4.2 Calculating the intersection numbers

4.2.1 The intersection number of P and O

As sections, we will write P as $([t,1,1],t)$, and O as $([0,1,0],t)$, with $t \in \mathbb{P}^1$. For $t \neq \infty$, these two will clearly not intersect, since their third homogeneous coordinates are never equal. To see what happens at $t = \infty$, we have to change variable to $s = \frac{1}{t}$. Setting $g(s) = 1 + as^2 + bs^3 = s^3 f(\frac{1}{s})$, we get $\frac{g(s)}{s^3} y^2 = f(x)$, which we multiply by s^3 to get

$$g(s)y^2 = s^3x^3 + as^3x + bs^3.$$

In the new variables $s = \frac{1}{t}, u = sx$ and y we have

$$E_\infty : g(s)y^2 = u^3 + as^2u + bs^3.$$

Here we will use a notation like E_∞ (or later $\widetilde{E}$ and E^w) to represent the curve E in different variables, and write for instance P_∞ for a point P in those variables.
On E_∞, we have $P_\infty = ([s \cdot t, 1, 1], s) = ([1,1,1], s)$ and $O_\infty = ([0,1,0], s)$. Hence the points P and O do not intersect at $t = \infty$ either, so their intersection number is 0, i.e.

$$(PO) = 0.$$

4.2.2 The intersection number of Q and O

As sections, $Q = ([t^p, f(t)^{\frac{p-1}{2}}, 1], t)$ and $O = ([0,1,0],t)$. So again for $t \neq \infty$, they do not intersect. However, for $t = \infty$ we have $O_\infty = ([0,1,0], s)$ and

$$\begin{aligned} Q_\infty &= ([s \cdot (1/s)^p, f(1/s)^{\frac{p-1}{2}}, 1], s) \\ &= ([s^{-(p-1)}, (g(s)/s^3)^{\frac{p-1}{2}}, 1], s) \\ &= ([s^{\frac{p-1}{2}}, g(s)^{\frac{p-1}{2}}, s^{3\frac{p-1}{2}}], s). \end{aligned}$$

So since $p \neq 2$, these two intersect for $s = 0$ in the point $R = ([0,1,0], 0)$.
To calculate the intersection number we homogenize the equation for E_∞:

$$g(s)y^2z = x^3 + as^2xz^2 + bs^3z^3$$

and then dehomogenize it again with respect to y, by dividing by y^3 and setting $u = \frac{x}{y}$, $v = \frac{z}{y}$, giving us

$$\widetilde{E} : g(s)v = u^3 + as^2uv + bs^3v^3$$

and the sections O and Q become

$$\widetilde{O} = ((0,0),s) \text{ and } \widetilde{Q} = \left(\left(\left(\frac{s}{g(s)}\right)^{\frac{p-1}{2}}, \left(\frac{s^3}{g(s)}\right)^{\frac{p-1}{2}}\right), s\right).$$

Viewing $\widetilde{O}$ locally as $\mathbb{P}^1$, the coordinate ring there is $\mathbb{F}_p[s]_{(0)}$, so that intersecting with $\widetilde{Q}$ gives the ring

$$\mathbb{F}_p[s]_{(0)}/\left(\left(\frac{s}{g(s)}\right)^{\frac{p-1}{2}}, \left(\frac{s^3}{g(s)}\right)^{\frac{p-1}{2}}\right) = (\mathbb{F}_p[s]/(s^{\frac{p-1}{2}}))_{(0)},$$

using that $g(s)$ is a unit in $\mathbb{F}_p[s]_{(0)}$, since $g(0) = 1$.
Then the intersection number is

$$(QO) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[s]/(s^{\frac{p-1}{2}}))_{(0)} = \frac{p-1}{2}.$$

4.2.3 The intersection number of P and Q

First of all, for $t = \infty$ they do not intersect, since we have already seen that for $t = \infty$, Q intersects O, but P does not. Since Q has only one point on the fiber at $t = \infty$, P and Q cannot also meet there.
As sections we have $P = ([t,1,1],t)$ and $Q = ([t^p, f(t)^{\frac{p-1}{2}}, 1], t)$. So these will intersect if

$$t = t^p \text{ and } f(t)^{\frac{p-1}{2}} = 1.$$

Since we know that

$$t^p - t = \prod_{x \in \mathbb{F}_p} (t - x),$$

P and Q will intersect for all $t = x \in \mathbb{F}_p$ satisfying $f(x)^{\frac{p-1}{2}} = 1$. This happens if and only if $f(x)$ is a nonzero square in $\mathbb{F}_p$, i.e. if and only if there is a $y \in \mathbb{F}_p^*$ such that $f(x) = y^2$. In other words, P and Q intersect for $t = x$ if and only if there is a point $(x,y) \in E'(\mathbb{F}_p) - E'[2](\mathbb{F}_p)$.
For each such x, the local intersection index is

$$\dim_{\mathbb{F}_p}\mathbb{F}_p[t]_{(t-x)}/(t^p - t, f(t)^{\frac{p-1}{2}} - 1) = \dim_{\mathbb{F}_p}\mathbb{F}_p[t]_{(t-x)}/(t-x) = 1,$$

using that $(t^p - t)/(t - x)$ is a unit in $\mathbb{F}_p[t]_{(t-x)}$, since x is a simple zero of $(t^p - t)$.
It follows that

$$(PQ) = \sum_{\text{such } x} 1 = \frac{\#E'(\mathbb{F}_p) - \#E'[2](\mathbb{F}_p)}{2},$$

where we divide by 2 because for $y \neq 0$ the points (x, y) and $(x, -y)$ in $E'(\mathbb{F}_p)$ give the same x.

4.3 Calculating the contributions

4.3.1 Preparations

Next we want to determine the contributions $\mathrm{contr}_v(P)$, $\mathrm{contr}_v(Q)$ and $\mathrm{contr}_v(P,Q)$ for $v \in S := \{t_1, t_2, t_3, \infty\}$, where the t_i are roots of f. For this we will first have to determine the structure of the singular fibers on the surface $\mathcal{E}$ over k corresponding to the curve E over $k(t)$.
To do this we need the discriminant of the elliptic curve. For an elliptic curve in Weierstrass form (in characteristic not 2 or 3),

$$y^2 = x^3 + A(t)x + B(t),$$

the discriminant is given by $\Delta_t = -16(4A(t)^3 + 27B(t)^2)$, and the j-invariant by $j_t = -1728(4A(t))^3/\Delta_t$.
In our case we first need to bring $f(t)y^2 = x^3 + ax + b$ into Weierstrass form, which we can do by multiplying by $f(t)^3$, and then applying the transformation $u = f(t)x$, $v = f(t)^2 y$. This gives

$$E^w : v^2 = u^3 + af(t)^2 u + bf(t)^3.$$

The discriminant and j-invariant are then

$$\Delta_t = -16(4a^3 + 27b^2)f(t)^6 \quad \text{and} \quad j_t = \frac{4 \cdot 1728 \cdot a^3}{4a^3 + 27b^2}.$$

Here $4a^3 + 27b^2$ is the discriminant of the original elliptic curve, hence is not zero. It is also (up to sign) the discriminant of $f(x)$, so $f(t)$ has three distinct zeroes, which we will call t_1, t_2 and t_3. It follows that there are three singular fibers $F_{t_i} = \pi^{-1}(t_i)$, and for each the valuation of the discriminant is 6 and the valuation of the j-invariant is non-negative. From Table 1 it follows that all three are of type I_0^*.
We also have to check the fiber at infinity, for which we have to change variable to $s = \frac{1}{t}$. Setting $g(s) = 1 + as^2 + bs^3 = s^3 f(\frac{1}{s})$, we get

$$v^2 = u^3 + a\frac{g(s)^2}{s^6}u + b\frac{g(s)^3}{s^9},$$

which we multiply by s^{12},

$$s^{12}v^2 = s^{12}u^3 + as^6 g(s)^2 u + bs^3 g(s)^3,$$

and then transform by $\xi = s^4 u$, $\eta = s^6 v$, which finally gives

$$E^w_\infty : \eta^2 = \xi^3 + as^2 g(s)^2 \xi + bs^3 g(s)^3.$$

In these variables, the discriminant and j-invariant are

$$\Delta_s = -16(4a^3 + 27b^2)g(s)^6 s^6 \quad \text{and} \quad j_s = \frac{4 \cdot 1728 \cdot a^3}{4a^3 + 27b^2}.$$

This tells us that the fiber at infinity, where $s = 0$, is singular, the valuation of its discriminant is again 6 (since $g(0) = 1$), and the valuation of the j-invariant is 0. So this fiber, which we will call F_∞, is also of type I_0^*.

4.3.2 The contributions of P and of Q at F_{t_i}

First we look for the points of intersection of the sections P and Q with the singular fibers F_{t_i}, $i = 1, 2, 3$.
We need to do this on the curve in Weierstrass form, E^w, where P and Q are given respectively by

$$([tf(t), f(t)^2, 1], t) \quad \text{and} \quad ([t^p f(t), f(t)^{\frac{p+3}{2}}, 1], t).$$

These will both intersect the curve $E^w_{t=t_i}$, which is given by $v^2 = u^3$, in the point $U = ([0, 0, 1], t_i)$, since $f(t_i) = 0$. Now U is the singular point on the fiber that is blown up when $\mathcal{E}$ is constructed, so P and Q intersect F_{t_i} in one of the components that is created in the blowing up, while O intersects it in the component existing before the blowup. Using that the fiber is of type I_0^*, it follows from Table 2 that

$$\text{contr}_{t_i}(P, P) = \text{contr}_{t_i}(Q, Q) = 1.$$

4.3.3 The contributions of P and of Q at F_∞

Now for the other fiber, F_∞.
We have to consider the curve E^w_∞, where P is given by $([g(s), g(s)^2, 1], s)$ and Q by $([g(s)s^{\frac{p-1}{2}}, g(s)^{\frac{p+3}{2}}, s^{3\frac{p-1}{2}}], s)$. The fiber $\pi^{-1}(\infty)$ is given by $s = 0$, so P intersects it in $([1, 1, 1], 0)$ and Q intersects it in $([0, 1, 0], 0)$, using that $g(0) = 1$. Viewing $\pi^{-1}(\infty)$ as the curve $y^2 = x^3$, we see that P and Q intersect it away from its cusp. Therefore P and Q intersect F_∞ on the same component as O. Table 2 then tells us that

$$\text{contr}_\infty(P, P) = \text{contr}_\infty(Q, Q) = 0.$$

4.3.4 The contributions of P and Q together

Finally we consider $\text{contr}_v(P, Q)$. Let Θ_0 be the component of F_v that O intersects, and let Θ_i, $i \geq 1$ be the other components. Then we have the following values for this contribution:

$$\begin{aligned} \text{contr}_v(P, Q) &= 0 \quad \text{if } P \text{ or } Q \text{ intersect } F_v \text{ in } \Theta_0 \\ &= 1 \quad \text{if } P \text{ and } Q \text{ intersect } F_v \text{ in the same } \Theta_i \text{ , for } i \geq 1 \\ &= \tfrac{1}{2} \quad \text{if } P \text{ and } Q \text{ intersect } F_v \text{ in different } \Theta_i \text{ , for } i \geq 1. \end{aligned}$$

For F_∞, we have already seen that both P and Q intersect it in Θ_0, so

$$\text{contr}_\infty(P, Q) = 0.$$

For the F_{t_i}, we know that P and Q do not intersect it in Θ_0 so we can exclude the first case. However, we do not know yet if they intersect it in the same or in different Θ_i. One way to do this would be by going through

the steps in Tate's algorithm and see what happens to the sections after each blowup. But we will use the following trick.
We will look at the curve over an extension of $\overline{\mathbb{F}_p}(t)$ such that the fiber $\pi^{-1}(t_i)$ is smooth. The different components of $\pi^{-1}(t_i)$ will then correspond to distinct points of order 2 on this fiber. To see which components P and Q intersect, we only have to see which of the corresponding points over the extension the corresponding sections intersect, and in particular if they intersect in the same point or in different points.
Fix a t_i, let us say t_1, and consider $f(t)y^2 = f(x)$ over the extension $\mathbb{F}_p(s) = \mathbb{F}_p(t,s)$ of $\mathbb{F}_p(t)$ given by $s = \sqrt{t-t_1}$, so $t = s^2 + t_1$. Then the equation for the curve can be written

$$f(x) = f(t)y^2 = (t-t_1)(t-t_2)(t-t_3)y^2 = s^2(s^2+t_1-t_2)(s^2+t_1-t_3)y^2 \ / \ \mathbb{F}_p(s),$$

so by transforming with $v = sy$ we get

$$(s^2 + t_1 - t_2)(s^2 + t_1 - t_3)v^2 = x^3 + ax + b \ / \ \mathbb{F}_p(s).$$

Here the fiber over by $s = 0$ is non-singular, since t_1, t_2 and t_3 are distinct. The point $P = (t, 1)$ is transformed to $(s^2 + t_1, s)$ and $Q = (t^p, f(t)^{\frac{p-1}{2}})$ to $Q = ((s^2 + t_1)^p, sf(s^2 + t_1)^{\frac{p-1}{2}})$. Hence they intersect the fiber given by $s = 0$ at respectively $(t_1, 0)$ and $(t_1^p, 0)$. It follows that P and Q intersect the fiber in the same point if and only if $t_i \in \mathbb{F}_p$.
But zeroes of $f(t)$ lying in $\mathbb{F}_p$ correspond exactly to points of exact order 2 on the curve $E' : y^2 = f(x)$, i.e. points in $E'[2](\mathbb{F}_p) - \mathcal{O}$. For those zeroes the contribution is 1, while for the others it is $\frac{1}{2}$, i.e.

$$\begin{aligned}\sum_{t_i} \mathrm{contr}_{t_i}(P,Q) &= 1 \cdot (\#E'[2](\mathbb{F}_p) - 1) + \frac{1}{2} \cdot (3 - (\#E'[2](\mathbb{F}_p) - 1)) \\ &= 1 + \frac{\#E'[2](\mathbb{F}_p)}{2}.\end{aligned}$$

4.4 Putting everything together

Recall that we wanted to calculate the pairings $\langle P,P\rangle$, $\langle P,Q\rangle = \langle Q,P\rangle$ and $\langle Q,Q\rangle$, using the following formulas:

$$\begin{aligned}\langle P,P\rangle &= 4 + 2(PO) - \sum_{t\in S} \mathrm{contr}_t(P,P),\\ \langle P,Q\rangle &= 2 + (PO) + (QO) - (PQ) - \sum_{t\in S} \mathrm{contr}_t(P,Q).\end{aligned}$$

In the two preceding sections we have calculated the following:

- $(PO) = 0,\ (QO) = \frac{p-1}{2}$,
- $(PQ) = \frac{1}{2}(\#E'(\mathbb{F}_p) + \#E'[2](\mathbb{F}_p))$,
- $\mathrm{contr}_{t_i}(P,P) = \mathrm{contr}_{t_i}(Q,Q) = 1, \quad i = 1,2,3$,
- $\mathrm{contr}_\infty(P) = \mathrm{contr}_\infty(Q) = \mathrm{contr}_\infty(P,Q) = 0$,
- $\sum_{t_i} \mathrm{contr}_{t_i}(P,Q) = 1 + \frac{1}{2}\#E'[2](\mathbb{F}_p)$.

Putting these into the formulas we get:

$$\begin{aligned}\langle P,P\rangle &= 4 + 0 - 3 = 1,\\ \langle Q,Q\rangle &= 4 + p - 1 - 3 = p,\\ \langle P,Q\rangle &= 2 + 0 + \frac{p-1}{2} - \frac{1}{2}(\#E'(\mathbb{F}_p) - \#E'[2](\mathbb{F}_p)) - 1 - \frac{1}{2}\#E'[2](\mathbb{F}_p)\\ &= \frac{1}{2} + \frac{p}{2} - \frac{1}{2}\#E'(\mathbb{F}_p)\\ &= \frac{1 + p - \#E'(\mathbb{F}_p)}{2}.\end{aligned}$$

As an aside, we observe that $\deg(id) = 1 = \langle P,P\rangle$ and $\deg(\phi) = p = \langle Q,Q\rangle$, so that we have proven the following:

Proposition 4. *Consider the lattice $\Lambda = \mathrm{End}_{\mathbb{F}_p}(E')$, with quadratic form defined by $[\varphi,\varphi] = \deg(\varphi)$. Then $E(\mathbb{F}_p(t))$ and Λ are isomorphic as lattices.*

We have shown that the determinant of the lattice $E(\mathbb{F}_p(t))$ will be (up to multiplication by squares, which does not matter)

$$\det_p = p - \left(\frac{1 + p - \#E'(\mathbb{F}_p)}{2}\right)^2.$$

We wanted to use this by, given an elliptic curve, finding two p's such that the corresponding $\det_p$'s do not differ by a square. For a given case, this will not be very hard.
For instance, take $E' : y^2 = x^3 + x + 1$. Using a computer algebra system, or

even by hand, it is easily checked that $\#E'(\mathbb{F}_p)$ has 9 points for $p = 5$, and 5 points for $p = 7$. Then we can calculate that $\det_5 = \frac{11}{4}$ and $\det_7 = \frac{19}{4}$. These clearly do not differ by a square, so for this E' we have proved that $E(\mathbb{Q}(t))$ has rank 1.
To prove this in general by the same method, however, is not easy at all. All we can do is bring out the big guns and use a theorem of Elkies [Elk], which says that for any elliptic curve over $\mathbb{Q}$, there are infinitely many p such that $\#E'(\mathbb{F}_p) = p + 1$. Thus for every elliptic curve there are two primes such that $\det_p = p$, and of course these do not differ by a square. With that our main theorem is proven.

4.5 Proof of Proposition 1

Because of its length we relegated the elementary proof of Proposition 1 to this section. We restate it here:

Proposition. *Let $E : f(t)y^2 = f(x)$ be an elliptic curve over $k(t)$, and $E' : v^2 = u$ an delliptic curve over k.*
Let α and β be the maps

$$\begin{array}{ccccc} E(k(t)) & \xrightarrow{\alpha} & Mor_k(E', E') & \xrightarrow{\beta} & End_k(E') \\ (x(t), y(t)) & \longmapsto & ((u, v) \mapsto (x(u), v \cdot y(u))) & & \\ & & \psi & \longmapsto & \tau_{-\psi(\mathcal{O})}\psi, \end{array}$$

where $\alpha([0, 1, 0])$ is the map $P \mapsto \mathcal{O}$.
Then the map $\varphi = \beta \circ \alpha$ is a surjective group homomorphism with kernel $E[2](k(t))$.

Proof. First we will show that α and β are well-defined group homomorphisms, and then that $\beta \circ \alpha$ is surjective with kernel $E[2](k(t))$.
To show that α is a well-defined group homomorphism, we observe that $x(u)$ and $v \cdot y(u)$ are rational functions on E' since

$$v^2 y(u)^2 = f(u)y(u)^2 = f(x(u)).$$

Hence $(u, v) \mapsto (x(u), v \cdot y(u))$ defines a rational map $E' \to E'$, which is then a morphism since E' is smooth and projective.
Now fix $P = (u, v) \in E'$. Then $\alpha_P : (x(t), y(t)) \to (x(u), v \cdot y(u))$ is a morphism from $E \to E'$ that maps $\mathcal{O}_E$ to $\mathcal{O}'_E$. From Silverman (1986, Th.III.4.8, p.75) it then follows that α_P is a group homomorphism for each P. Hence α itself is a group homomorphism.
To see that β is well-defined we observe that $\beta(\psi)$ is in $\mathrm{End}_k(E')$ (which consists of all morphisms $E' \to E'$ mapping $\mathcal{O}$ to itself), since

$$(\tau_{-\psi(\mathcal{O})} \circ \psi)(\mathcal{O}) = \psi(\mathcal{O}) - \psi(\mathcal{O}) = \mathcal{O}.$$

It is a group homomorphism since

$$\begin{aligned}\beta(\psi_1+\psi_2)(P) &= (\tau_{-\psi_1(\mathcal{O})-\psi_2(\mathcal{O})}\circ(\psi_1+\psi_2))(P)\\ &= \psi_1(P)+\psi_2(P)-\psi_1(\mathcal{O})-\psi_2(\mathcal{O})\\ &= (\beta(\psi_1)+\beta(\psi_2))(P)\end{aligned}$$

for all $P \in E'$.
The kernel of β consists of the ψ such that

$$\mathcal{O} = \tau_{-\psi(\mathcal{O})}(\psi(P)) = \psi(P) - \psi(\mathcal{O})$$

for all $P \in E'$, i.e. of all constant morphisms ψ.
The kernel of φ is

$$\begin{aligned}\ker(\beta\circ\alpha) &= \{P\in E(k(t))|\alpha(P)\in\ker(\beta)\}\\ &= \{(x(t),y(t)) \mid (u,v)\mapsto(x(u),v\cdot y(u)) \text{ is constant}\}\cup\mathcal{O}_E\\ &= \{(x,0)\in E(k(t)) \mid x\in k\}\cup\mathcal{O}_E\\ &= E[2](k(t)).\end{aligned}$$

Finally we show that $\varphi = \beta\circ\alpha$ is surjective. The map β is surjective, since it is the identity on

$$\mathrm{End}_k(E') \subseteq \mathrm{Mor}_k(E',E').$$

We can write any $\psi \in \mathrm{Mor}_k(E',E')$ as

$$\psi : (u,v) \mapsto (a(u)+v\cdot b(u), c(u)+v\cdot d(u)).$$

Suppose that $\psi \in \mathrm{End}_k(E')$, so that ψ is a homomorphism. Then we have $\psi(u,-v) = -\psi(u,v)$, which implies

$$(a-bv, c-dv) = (a+bv, -c-dv),$$

so that $b = c = 0$ and $\psi(u,v) = (a(u), v\cdot d(v))$. Hence $\psi = \alpha(a(t),d(t))$ and it follows that $\mathrm{End}_k(E')$ is contained in the image of α, so that φ is surjective. □

5 An elliptic surface of rank 15

5.1 Introduction

Our aim in this chapter will be to show that the $K3$ surface

$$Y : y^2 = x^3 + (9v^8 - 14v^4 + 9)x + 4v^2(3v^8 - 10v^4 + 3)$$

has Mordell-Weil rank 15 over $\overline{\mathbb{Q}}$.
The first step will be reducing this problem to showing that the $K3$ surface

$$X : y^2 = x^3 + t^3(t+3)(t+1)^2(t+4)^2x + t^5(t+1)^3(t+4)^3$$

has rank 0 over $\overline{\mathbb{Q}}$. We will show that $X \bmod p$ has rank 1 over $\overline{\mathbb{F}}_p$ for two primes of good reduction, find a point of infinite order for each of those primes, and calculate the determinants of the corresponding lattices. If the determinants do not differ by a square, we will know by chapter 3 that the rank of X is 0, from which it will follow that Y has rank 15.

5.2 The surfaces

Theorem 6. *The ranks over $\overline{\mathbb{Q}}$ of Y and X satisfy*

$$\mathit{rank}\, Y = 15 + \mathit{rank}\, X,$$

Hence the surface Y has rank 15 if and only if X has rank 0.

Proof. We will build Y from X in several steps, and show that there is a rational map $X \to Y$ of finite degree. Then we use a lemma from [Ino, Kuw] which says that if V and W are $K3$ surfaces together with a rational map $V \to W$ of finite degree, then their Néron-Severi groups have the same rank. Applying the Shioda-Tate formula twice gives

$$\operatorname{rank} Y + \sum_{t \in S_Y} (m_t - 1) = \operatorname{rank} X + \sum_{t \in S_X} (m_t - 1),$$

where S_Z is the set of singular fibers on the surface Z.
The theorem then follows from the fact that $\sum_{t \in S_X}(m_t - 1) = 15$ while $\sum_{t \in S_Y}(m_t - 1) = 0$. In fact, the surfaces were constructed with that in mind: the singular fibers of X have a lot of components, and in each step towards Y we try to break those singular fibers up into ones that have fewer components.
We will walk through the construction to show that a rational map of finite degree exists, and keep track of the singular fibers to illustrate what happens. We start with X, which has one fiber of type III^* with $m_t = 8$, two fibers of type I_0^* with $m_t = 5$, and three of type I_1 with $m_t = 1$. Hence

$$\sum_{t \in S_X} (m_t - 1) = (8 - 1) + 2 \times (5 - 1) = 15.$$

name	equation
X	$y^2 = x^3 + t^3(t+3)(t+4)^2(t+1)^2x + t^5(t+4)^3(t+1)^3$
W_1	$y^2 = x^3 + t^3(t+3)x + t^5$
W_2	$y^2 = x^3 + s^3(9s^2 - 14s + 9)x + 4s^5(3s^2 - 10s + 3)$
W_3	$y^2 = x^3 + u^2(9u^4 - 14u^2 + 9)x + 4u^4(3u^4 - 10u^2 + 3)$
Y	$y^2 = x^3 + (9v^8 - 14v^4 + 9)x + 4v^2(3v^8 - 10v^4 + 3)$

Table 3: Surfaces used in the proof and their equations.

Let W_1 be the twist of X by $(t+1)(t+4)$, and let W_2 be the surface obtained from W_1 by putting

$$t = f(s) := \frac{16s}{3s^2 - 10s + 3}.$$

Inspecting the determinant of W_2 tells us that it has 2 III^* and six I_1 fibers, which means

$$\sum_{t \in S_{W_2}} (m_t - 1) = 2 \times (8 - 1) = 14.$$

Let W_3 be obtained from W_2 by putting $s = u^2$. Then it has 2 fibers of type I_0^* and 12 of type I_1, so

$$\sum_{t \in S_{W_3}} (m_t - 1) = 2 \times (5 - 1) = 8.$$

Finally we put $u = v^2$ in W_3 to reach Y, and see that it only has 24 I_1 fibers, so that

$$\sum_{t \in S_Y} (m_t - 1) = 0.$$

Since each step consisted of a rational map of finite degree, there is also a rational map of finite degree between X and Y, finishing our proof. $\square$

5.3 Calculating the determinants

First we will have to find points on X over two primes of good reduction. A simple computer search over the lowest primes gives the following points over 11 and 17:

$$\begin{aligned} P_{11} = \big(&10(t+1)(t^2+7t+2)(t+4)\ , \\ &8(t+1)^2(t^2+5t+10)(t+4)^2\big) \ \text{ over } \mathbb{F}_{11} \\ P_{17} = \big(&(t+2)(t+4)(t^2+3t+8), \\ &6(t^4+13t^3+7t^2+12t+11)(t+4)^2\big) \ \text{ over } \mathbb{F}_{17} \end{aligned}$$

Both primes are easily checked to be of good reduction.
In the next section we will show that $X \bmod 11$ and $X \bmod 17$ have rank 1 over $\overline{\mathbb{F}}_p$, so that their determinants are just $\langle P_{11}, P_{11}\rangle$ and $\langle P_{17}, P_{17}\rangle$. We calculate these by working through the terms in the formula from chapter 2:

$$\langle P_q, P_q\rangle = 2\chi + (P_q \cdot O) - \sum \mathrm{contr}_t(P_q).$$

We'll do this step-by-step again.

- The genus $\chi = 2$ since X is a $K3$ surface.
- We easily compute $(P_{11} \cdot O) = 0$, $(P_{17} \cdot O) = 0$.
- The contributions at the singular fibers:
  - III^* fiber $\Rightarrow$ contr $= 3/2$
  - two I_1 fibers $\Rightarrow$ contr $= 0$
  - two I_0^* fibers $\Rightarrow$ contr $= \begin{cases} 0 & \text{if } P \text{ meets } \Theta_0; \\ 1 & \text{otherwise.} \end{cases}$
    - $P_{11} \mid_{t=-4} = (0,0)$, $\quad P_{11} \mid_{t=-1} = (0,0) \quad \Rightarrow \quad 2 \times \mathrm{contr} = 1$;
    - $P_{17} \mid_{t=-4} = (0,0)$, $\quad P_{17} \mid_{t=-1} = (1,8) \quad \Rightarrow \quad \mathrm{contr} = 1$;

Together these give

$$\begin{aligned} \langle P_{11}, P_{11}\rangle &= 4 - \frac{3}{2} - 2 = \frac{1}{2} \\ \langle P_{17}, P_{17}\rangle &= 4 - \frac{3}{2} - 1 = 1\frac{1}{2}, \end{aligned}$$

and

$$\frac{\langle P_{17}, P_{17}\rangle}{\langle P_{11}, P_{11}\rangle} = 3,$$

so they do not differ by a square. By chapter 3 this implies that

$$\operatorname{rank} X(\overline{\mathbb{Q}}) = 0$$

and by section 2 we have that

$$\operatorname{rank} Y(\overline{\mathbb{Q}}) = 15.$$

5.4 The ranks of $X \bmod 11$ and $X \bmod 17$

The only loose end left to tie is proving that $X \bmod 11$ and $X \bmod 17$ have rank 1 over $\overline{\mathbb{F}}_p$. The method used in this section is perhaps more difficult than the techniques above, but has been used in the literature several times before [Kl2, Lu1, Lu2].
The crucial theorem is this:

Theorem 7. *Let S be a smooth projective surface over $\mathbb{F}_p$ and φ_p^* the action of Frobenius on $H^2_{\acute{e}t}(S_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$. Then the rank of NS$(S)$ is bounded from above by the number of eigenvalues λ of φ^* for which λ/p is a root of unity, counted with multiplicity.*

Proof. See [Lu1, Cor. 6.4]. □

The Tate conjecture, which predicts equality in the theorem above, is known for $K3$ surfaces, but here we will only need the inequality.
Let $\overline{X} = X \bmod p$ be the surface defined above modulo p, let ρ be the rank of NS(X) and r the Mordell-Weil rank of $\overline{X}$ over $\overline{\mathbb{F}}_p$. Since

$$\rho = 2 + r + \sum (m_t - 1) = 17 + r,$$

we would like to show that for $p = 11, 17$ there are 18 or less eigenvalues λ for which λ/p is a root of unity, because then

$$18 \geq \rho = 17 + r$$

implies $r \leq 1$. We have already found points on $X \bmod 11$ and $X \bmod 17$, which were non-torsion since their determinants were non-zero, so this means that $r = 1$ in each case, as we desired.
So we want to determine the eigenvalues of φ_p^*, i.e. the roots of its characteristic polynomial $\psi_p(X)$. By the Weil conjectures, $\psi_p(X)$ is in $\mathbb{Z}[X]$ and its roots have absolute value p. We can determine its coefficients by using the Lefschetz Trace Formula. This will enable us to compute $\mathrm{Tr}((\varphi_p^*)^m)$ for enough m to allow us to find the coefficients of $\psi_p(X)$ with basic algebra. However, H^2 has dimension 22, so this would be impractical to compute. Luckily, we can split it up into

$$H^2 = V \oplus W,$$

with V the 18-dimensional subspace generated by the zero section, a smooth fiber, the 15 components of singular fibers and the one section we have found above. Since we want to show that $\rho \leq 18$, it will be enough to show that none of the eigenvalues coming from W are p times a root of unity.
This reduces the problem to computing the degree 4 characteristic polynomial of $\varphi_p^*|_W$, which we will write as

$$f_p = X^4 + c_1 X^3 + c_2 X^2 + c_3 X + c_4. \quad \in \mathbb{Z}[X]$$

Since we already know that all roots have absolute value p, we know that $c_4 = \pm p^4$. The Weil conjectures also give a functional equation $p^{22}\psi_p(x) = \pm x^{22}\psi_p(p^2/x)$. From the Tate algorithm it can be seen that the generators of V are all defined over $\mathbb{F}_{p^2}$, which means that the roots of ψ_p/f_p are all p or $-p$, so that the functional equation is also true for ψ_p/f_p. It follows that the functional equation holds for f_p, so

$$p^4 f_p(x) = \pm x^4 f_p(p^2/x).$$

Writing this out, we get

$$f_p(X) = \pm(p^4 + c_1 p^2 X + c_2 X^2 + \frac{c_3}{p^2}X^3 + \frac{c_4}{p^4}X^4),$$

from which we deduce that

$$c_3 = \text{sign}(c_4) p^2 c_1.$$

Furthermore, we see that if $c_2 \neq 0$, then $\text{sign}(c_4) = +1$.
Finally, we can compute c_1 and c_2 by

$$c_1 = -t_1 \tag{9}$$

$$c_2 = \frac{1}{2}(t_1^2 - t_2), \tag{10}$$

where $t_m = \text{Tr}((\varphi_p^*)^m|_W)$ is computed by the Lefschetz Trace Formula. In this case that gives

$$\begin{aligned} \#X(\mathbb{F}_{p^m}) &= 1 + p^{2m} + \text{Tr}(\varphi_p^*)^m|_V + \text{Tr}(\varphi_p^*)^m|_W \\ &= 1 + p^{2m} + (k+3)p^m + t_m, \end{aligned} \tag{11}$$

where k is the number of components of singular fibers not meeting the zero section that are defined over $\mathbb{F}_{p^m}$, and the 3 comes from the zero section, fiber and found section, which are all rational. On the other hand, we can explicitly count the points on $X(\mathbb{F}_{p^m})$ by

$$\begin{aligned} \#X(\mathbb{F}_{p^m}) &= \#\{\text{affine pts on } X \text{ before blow-up}\} + \#\{\text{pts at } \infty\} \\ &\quad + \#\{\text{pts over } t = \infty\} + \#\{\text{pts on blown-up singular fibers}\} \\ &= \#X_{\text{aff}}(\mathbb{F}_{p^m}) + \#A(\mathbb{F}_{p^m}) + p^m + kp^m. \end{aligned} \tag{12}$$

Here X_{aff} is the affine part of the not-blown-up surface, i.e. the number of $(x, y, t) \in \mathbb{F}_{p^m}^3$ satisfying the defining equation of the surface. Further A is the fiber over $t = \infty$ and the last term counts the new points on the blow-ups of singular fibers. In total there are k new components defined over $\mathbb{F}_{p^m}$, each containing $p^m + 1$ points, and there are k intersection points

we have to subtract again, giving kp^m.
Putting (11) and (12) together, we get

$$t_m = \#X_{\text{aff}}(\mathbb{F}_{p^m}) + \#A(\mathbb{F}_{p^m}) + p^m + kp^m - 1 - p^{2m} - (k+3)p^m \quad (13)$$
$$= \#X_{\text{aff}}(\mathbb{F}_{p^m}) + \#A(\mathbb{F}_{p^m}) - 2p^m - p^{2m} - 1. \quad (14)$$

So for 11 and 17 we use the computer to do the following counts:

$$\begin{aligned}
\#X_{\text{aff}}(\mathbb{F}_{11}) &= 120\\
\#X_{\text{aff}}(\mathbb{F}_{11^2}) &= 14488\\
\#X_{\text{aff}}(\mathbb{F}_{17}) &= 318\\
\#X_{\text{aff}}(\mathbb{F}_{17^2}) &= 83540,
\end{aligned}$$

and each time the curve A becomes $y^2 = x^3 + x$, giving

$$\begin{aligned}
\#A(\mathbb{F}_{11}) &= 12\\
\#A(\mathbb{F}_{11^2}) &= 144\\
\#A(\mathbb{F}_{17}) &= 16\\
\#A(\mathbb{F}_{17^2}) &= 320.
\end{aligned}$$

For $p = 11$ the traces and coefficients are then

$$\begin{aligned}
t_1 &= 120 + 12 - 2 \cdot 11 - 11^2 - 1 = -12,\\
t_2 &= 14488 + 144 - 2 \cdot 11^2 - 11^4 - 1 = -252,\\
c_1 &= 12,\\
c_2 &= (12^2 + 252)/2 = 198,
\end{aligned}$$

and for $p = 17$

$$\begin{aligned}
t_1 &= 318 + 16 - 2 \cdot 17 - 17^2 - 1 = 10,\\
t_2 &= 83540 + 320 - 2 \cdot 17^2 - 17^4 - 1 = -240\\
c_1 &= -10,\\
c_2 &= (10^2 + 240)/2 = 170.
\end{aligned}$$

Since $c_2 \neq 0$, we know from above that $c_3 = p^2 c_1$ and $c_4 = p^4$, so the polynomials are:

$$\begin{aligned}
f_{11} &= X^4 + 12X^3 + 198X^2 + 12 \cdot 11^2 X + 11^4\\
f_{17} &= X^4 - 10X^3 + 170X^2 - 10 \cdot 17^2 X + 17^4.
\end{aligned}$$

To apply theorem 7 we have to see if these polynomials have roots of the form $p\zeta$ with ζ a root of unity. Therefore we change variable to $Y = X/11$ resp. $Y = X/17$, and divide by 11^3 resp. 17^3. Then we want to show that the roots of

$$11Y^4 + 12Y^3 + 18Y^2 + 12Y + 11,$$

$$17Y^4 - 10Y^3 + 10Y^2 + 10Y + 17$$

are roots of unity. That follows from the fact that both are irreducible over $\mathbb{Z}$, and are clearly not cyclotomic. Irreducibility of the second polynomial can be proved by reducing modulo 7. For the first it can be shown by checking that it has a prime value for $Y = -12, -8, -6, -2, 0, 2, 4, 6, 10$, and then arguing that if it factors as $g(Y)h(Y)$, at each of those nine values either g or h must be ± 1. However, if g and h were nonconstant they could attain -1 or 1 at most $2 \times (\deg g + \deg h) = 8$ times.
This finishes our proof that $\rho \leq 18$, and that

$$\operatorname{rank} X = 1$$

over $\overline{\mathbb{F}}_p$ for $p = 11, 17$.

References

[Cox] Cox, D., Mordell-Weil groups of elliptic curves over $\mathbb{C}(t)$ with $p_g = 0$ or 1. *Duke Math. J.*, **49** (1982), 677–689.

[Elk] Elkies, N., The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$, *Invent. Math.*, **89** (1987), 561–568.

[Har] Hartshorne, R., *Algebraic Geometry*, GTM **52**, Springer-Verlag, New York, 1977.

[Ino] Inose, H., On certain Kummer surfaces which can be realized as non-singular quartic surfaces in $\mathbb{P}^3$, *J. Fac. Sci. Univ. Tokyo*, **23** (1976), 545-560.

[Kl1] Kloosterman, R., *Arithmetic and moduli of elliptic surfaces*, PhD thesis, University of Groningen, 2005.

[Kl2] Kloosterman, R., *Elliptic $K3$ surfaces with Mordell-Weil rank 15*, Preprint, 2005, available at `arXiv:math.AG/0502439`.

[Kod] Kodaira, K., On compact analytic surfaces II-III, *Ann. of Math.*, **77** (1963), pp.563–626; **78** (1963), pp. 1–40.

[Kuw] Kuwata, M., Elliptic $K3$ surfaces with given Mordell-Weil rank, *Comm. Math. Univ. Sancti. Pauli*, **49** (2000), pp. 91–100.

[Lu1] Van Luijk, R., *An elliptic $K3$ surface associated to Heron triangles*, Preprint, 2005, available at `arXiv:math.AG/0411606`.

[Lu2] Van Luijk, R., *$K3$ surfaces with Picard number one and infinitely many rational points*, Preprint, 2005, available at `arXiv:math.AG/0506416`.

[Nag] Nagao, K., An example of elliptic curve over $\mathbb{Q}(T)$ with rank ≥ 13, *Proc. of the Japan Acad.*, **70** (1994), 152–153.

[Shi] Shioda, T., On the Mordell-Weil Lattices, *Comm. Math. Univ. Sancti. Pauli*, **39**, 2 (1990), pp. 211–240.

[Sh2] Shioda, T., Some remarks on elliptic curves over function fields, *Astérisque*, **209** (1992), 211–240.

[Si0] Silverman, J. H. and Tate, J., *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[Si1] Silverman, J.H., *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New York, 1986.

[Si2] Silverman, J.H., *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer-Verlag, New York, 1994.

[Tat] Tate, J., Algorithm for determining the type of a singular fiber in an elliptic pencil, *Modular functions of one variable IV*, Lect. Notes in Math. **476**, Springer-Verlag, Berlin (1975), pp. 33–52.