rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Notes on Elliptic Delsarte Surfaces

Master's Thesis Mathematics

July 2014

Student: L.J. Disselhorst

First Supervisor: Dr. J. Top

Second Supervisor: Dr. H.W. Broer

Abstract

In this thesis, we try to find the generators of the Mordell-Weil group a particular elliptic K3 surface. We first determine the rank of the Mordell-Weil group and describe the relation between its generators. Next we determine a point in a finite field, which we will lift to a field with characteristic zero.

Contents

1 Introduction

In the PhD. thesis of Bas Heijne ([2]), Heijne has described the generators of the Mordell-Weil groups of several Elliptic Delsarte surfaces. The only unsolved problem in the thesis, is to find the generators of the Mordell-Weil group of the surface defined by the equation $y^2 = x^3 + t^7x + 1$. In this master's thesis, I attempt to solve the problem. First, we discuss the method to determine the rank of a Mordell-Weil group, then we use Galois theory to describe the relation between the Mordell-Weil group's generators. Finally, we determine a point on the elliptic surface in a finite field, which will be lifted to a field with characteristic zero. Throughout the thesis, the algebraic computing program magma is used.

2 The rank of a surface and types of points

In this section, we discuss a geometric approach to determine the group of rational points on an elliptic curve E defined over $\overline{\mathbb{Q}}(t)$. Throughout, it is assumed that no elliptic curve E_0 over $\overline{\mathbb{Q}}$ exists such that $E \cong E_0$ over $\overline{\mathbb{Q}}(t)$. Under this condition, we first observe that the Mordell-Weil group $E(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}^r \times \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$ for some integers $r \geq 0$ and $a > 0, b > 0$ (See [9, p. 109] and [8, p. 242]). The number r is called the rank of E over $\overline{\mathbb{Q}}(t)$ and the subgroup $E_{\text{tors}}(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$, consisting of all points of finite order in $E(\overline{\mathbb{Q}}(t))$, is called the torsion subgroup.

2.1 The rank

An elliptic curve E over $\overline{\mathbb{Q}}(t)$ is given by an equation $y^2 = x^3 + ax + b$, for certain $a, b \in \overline{\mathbb{Q}}(t)$. Any $u \in \overline{\mathbb{Q}}(t)^*$ gives rise to a coordinate change

$$\eta := u^3 y, \xi := u^2 x, \tag{1}$$

which transforms the equation into

$$\eta^2 = \xi^3 + u^4 a\xi + u^6 b.$$

In this way, one can clear the denominators of a, b, leading to an equation with $a, b \in \overline{\mathbb{Q}}[t]$.

Now $x^3 + ax + b - y^2$ is a polynomial in $\overline{\mathbb{Q}}[x, y, t]$, so its zeroes define a surface over $\overline{\mathbb{Q}}$. Moreover, this surface is equipped with a morphism to $\mathbb{A}^1$, namely $(x, y, t) \mapsto t$. The elliptic surface $\mathcal{E}$ associated to E is a smooth, projective surface which is birational to the surface above, such that the

given morphism defines a morphism $\pi : \mathcal{E} \to \mathbb{P}^1$, and $\mathcal{E}$ is "minimal" for these properties. For details, see section 8.8 of [8], which describes the more difficult situation where $\overline{\mathbb{Q}}(t)$ and the principal ideal doman $\overline{\mathbb{Q}}[t]$ are replaced by an arbitrary number field K and its ring of integers R.

The surface $\mathcal{E}$ has a "second Betti number", $b_2 = \dim_{\mathbb{C}} H^2(\mathcal{E}(\mathbb{C}), \mathbb{C})$, which is a topological invariant of the space $\mathcal{E}(\mathbb{C})$.

Another invariant of $\mathcal{E}$ is its "Picard number", ρ, which can be defined as the dimension over $\mathbb{Q}$ of the vector space $H^{1,1}(\mathcal{E}(\mathbb{C}), \mathbb{C}) \cap H^2(\mathcal{E}(\mathbb{C}), \mathbb{Q})$.

A third invariant of $\mathcal{E}$ is its "Lefschetz number" λ, which is defined as:

$$\lambda := b_2 - \rho. \tag{2}$$

There is a relation between the rank r of $E(\overline{\mathbb{Q}}(t))$ and these invariants. To state this, we will introduce one more invariant, called ρ_{triv}.

The morphism $\pi : \mathcal{E} \to \mathbb{P}^1$ is in fact an extention of the map $(x, y, t) \mapsto t$. For given $t_0 \in \mathbb{P}^1$, the inverse image $\pi^{-1}(t_0) \subset \mathcal{E}$ is closely related to the curve with equation $y^2 = x^3 + a(t_0)x + b(t_0)$. If this curve is an elliptic curve, then so is $\pi^{-1}(t_0)$. Otherwise, $\pi^{-1}(t_0)$ turns out to be a union of finitely many rational curves, which is called a singular fibre (for more information, see [4])

A method to determine the the rational curves, is explained in [6, p. 11] by Schuett and Shioda. We denote the surface's equation by $\mathcal{E} : y^2 = x^3 + ax + b$ and determine its discriminant $\Delta(\mathcal{E}(t_0))$ at t_0. If $\Delta = 0$, then our cubic curve is singular at t_0. Next, we verify the vanishing orders v of a and b. On [6, p. 16], there is a table which provides the types of fibres corresponding to $v(a_4)$ and $v(a_6)$. A comprehensive image of the types of curves can be found on [6, p. 13], so that we can determine the number of rational curves at t_0. We denote this number by ν_{t_0}, then:

$$\rho_{\text{triv}} := 2 + \sum_{\substack{t_0 \in \mathbb{P}^1 \text{ s.t.} \\ \pi^{-1}(t_0) \text{ is} \\ \text{not ellilptic}}} (\nu_{t_0} - 1) \tag{3}$$

We now state the following theorem:

Theorem 2.1. $r = \rho - \rho_{triv}$.

This theorem is proven in e.g. [7]

We combine this theorem with equations 3 and 2, to obtain a formula for computing the rank:

Corollary 1. *The rank of an elliptic surface is given by*

$$r = b_2 - \lambda - \rho_{triv} \tag{4}$$

We will now discuss the second betti number $b_2(S)$ of an elliptic surface, by combining some sections of [6].

On [6, p. 28], we obtain an equation for b_2:

$$b_2(S) = e(S) - 2(1 - b_1(C)),$$

where $e(S)$ is the Euler number of an elliptic surface and $b_1(C)$ is the first Betti number of its base curve C. In our case $C \cong \mathbb{P}^1$, hence $b_1 = 0$.

Denote the elliptic surface in the usual Weierstrass form: $y^2 = x^3 + ax + b$, with $a, b \in \overline{\mathbb{Q}}[t]$, as on [6, p. 16], then we define "minimal polynomials" as follows:

Definition 1. *$a(t)$ and $b(t)$ are minimal polynomials if there is no $c(t) \in \overline{\mathbb{Q}}[t] \setminus \overline{\mathbb{Q}}$ with the property that $c^4|a$ and $c^6|b$.*

Assuming we have an elliptic surface with minimal polynomials, we determine the smallest $n \in \mathbb{N}$ that satisfies the following three conditions (see [6, p. 37]:

1. $\deg(a_i) \leq ni$ for all i.
2. there is some i such that $\deg(a_i) \geq (n-1)i$.
3. For any finite place on $\mathbb{P}^1$ with valuation v, there is some i such that $v(a_i) < i$.

In the minimal Weierstrass form, the latter two conditions are always met, the first reduces to finding the smallest n such that $\deg(a) \leq 4n$ and $\deg(b) \leq 6n$. Using [6, p. 38], we see that $e(S) = 12\chi(S) = 12n$. We combine this with what we know about b_2 to obtain:

$$b_2 = 12n - 2. \tag{5}$$

Finally, we discuss the algorithm for obtaining the Lefschetz number, which can also be found in [2]. The Lefschetz number can not always be determined, but it is possible for Delsarte surfaces. These have the property that, when homogenized, they are of the form

$$\sum_{i=0}^{3} T^{a_{i0}} X^{a_{i1}} \tilde{Y}^{a_{i2}} Z^{a_{i3}}. \tag{6}$$

With all exponents a_{ij} nonnegative. This homogeneous form is obtained from the standard form of an elliptic curve by the variable change $y \mapsto i \cdot y$. We

place the exponents in a matrix as follows:

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Take the additive group $(\mathbb{Q}/\mathbb{Z})^4$ and construct a subgroup L by choosing the following generators:

$$\begin{aligned} l_1 &:= (1,0,0,-1)A^{-1} \\ l_2 &:= (0,1,0,-1)A^{-1} \\ l_3 &:= (0,0,1,-1)A^{-1} \end{aligned}$$

Next, we define $\Lambda \subset L$. Λ is the set of all elements $v = (b_1, b_2, b_3, b_4) \in L$ that satisfy:

1. v only has nonzero components.
2. There exists a "good" $t \in \mathbb{Z}$ such that $\text{ord}(tv) = \text{ord}(v)$, where ord is the order in the additive group $(\mathbb{Q}/\mathbb{Z})^4$.
3. If such "good" t exist, we also need that $\sum_{i=0}^{3} \{t \cdot b_i\} = 1$ or 3 for at least one t. $\{b_i\}$ refers to the natural bijection between $(\mathbb{Q}/\mathbb{Z})$ and $[0,1)$.

The Lefschetz number is defined to be $\lambda := \#\Lambda$.

2.2 Torsion points

To determine the torsion points of an elliptic curve, one can apply the Nagell-Lutz theorem:

Theorem 2.2. *Let $\mathcal{E}(\overline{\mathbb{Q}}(t))$ be an elliptic surface with Weierstrass equation $y^2 = x^3 + a(t)x + b(t)$, with $a(t), b(t) \in \overline{\mathbb{Q}}[t]$ and suppose that $P = (\alpha, \beta) \in E(\overline{\mathbb{Q}}(t))$ is a nonzero torsion point. Then:*

$$\begin{cases} \textit{either } \beta = 0 & P \textit{ has order 2 and } \alpha \in \overline{\mathbb{Q}}[t] \textit{ satisfies } \alpha^3 + a(t)\alpha + b(t) = 0, \\ \textit{or } \beta^2 | \Delta(E) & \textit{order } \geq 3. \end{cases}$$

In [8], the proof has been given for elliptic curves of the form $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. This proof can be adapted to our case.

An alternative way to find torsion points, or prove in some cases that they do not exist, will be explained in section 3.2.

3 Application of the theory

In this section, we apply the theory of section 1 to our surface.

3.1 The rank

We wish to determine the rank of the surface defined by:

$$y^2 = x^3 + t^7 x + 1, \tag{7}$$

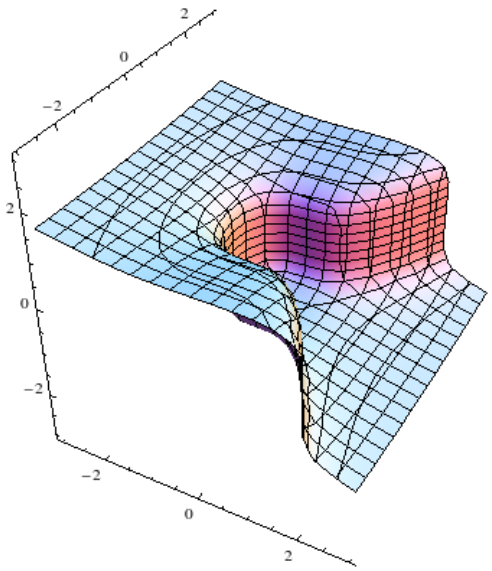


Figure 1: The surface $E : y^2 = x^3 + t^7 x + 1$

To determine the Lefschetz number of the our surface, we first need to transform it so that it can be homogenized into the form of equaiton 6, we first apply the variable change $y \mapsto (iy) = \tilde{y}$. Then our surface is defined by the equation $x^3 + t^7 x + \tilde{y}^2 + 1 = 0$.

Theorem 3.1. *The Lefschetz number of the surface defined by* $x^3 + t^7 x + \tilde{y}^2 + 1 = 0$ *equals* 6.

Proof. We write the homogenized equation in the form as in equation 6, so $\sum_{i=0}^{3} T^{a_{i0}} X^{a_{i1}} \tilde{Y}^{a_{i2}} Z^{a_{i3}} = X^3 Z^5 + T^7 X + \tilde{Y}^2 Z^6 + Z^8$ and put the exponents in a matrix A, so we get:

$$A = \begin{pmatrix} 0 & 3 & 0 & 5 \\ 7 & 1 & 0 & 0 \\ 0 & 0 & 2 & 6 \\ 0 & 0 & 0 & 8 \end{pmatrix} \quad \text{with inverse:} \quad A^{-1} = \frac{1}{168} \begin{pmatrix} -8 & 24 & 0 & 5 \\ 56 & 0 & 0 & -35 \\ 0 & 0 & 84 & -63 \\ 0 & 0 & 0 & 21 \end{pmatrix}.$$

Then $L \subset (\mathbb{Q}/\mathbb{Z})^4$ is generated by:

$$\begin{aligned} l_1 &= (1,0,0,-1)A^{-1} = \frac{1}{42}(-2,6,0,-4), \\ l_2 &= (0,1,0,-1)A^{-1} = \frac{1}{42}(14,0,0,-14), \\ l_3 &= (0,0,1,-1)A^{-1} = \frac{1}{42}(0,0,21,-21). \end{aligned}$$

Claim: $L \cong \mathbb{Z}/42\mathbb{Z}$, with generator $l := l_1 + l_3$.

In $(\mathbb{Q}/\mathbb{Z})^4$, $\mathrm{ord}(l_1) = 21$, $\mathrm{ord}(l_3) = 2$ and $14 \cdot l_1 = \frac{1}{42}(-28, 84, 0, -56) = \frac{1}{42}(14, 0, 0, -14) = l_2$. Now let $l := l_1 + l_3 = \frac{1}{42}(-2, 6, 21, 17)$, which clearly has order 42. Then $22 \cdot l = l_1$ and $21 \cdot l = l_3$. The relation between l_1 and l_2 shows that $22 \cdot 14 \cdot l = l_2$. We conclude that $L \cong \mathbb{Z}/42\mathbb{Z}$ and that $l := l_1 + l_3$ is its generator, which proves the claim.

To describe all elements in L, let $v_n := n \cdot l$, for $n \in \{0, \ldots, 41\}$. We need to find all v_n that are elements of Λ. First, observe that v_n has only nonzero elemenhts if $2 \nmid n$ and $7 \nmid n$. Next, for $t \in \mathbb{Z}$, $\mathrm{ord}(t \cdot v_n) = \mathrm{ord}(v_n)$ if t is coprime with 42 and finally, we determine for which fully nonzero v_n, there exists a t such that $\sum_{i=1}^{4} \{t \cdot a_i\} = 1$ or 3. For six v_n, this is the case (the smallest t is given):

n	v_n	t	$\mathrm{ord}(v_n)$	$\sum$
3	$(-\frac{3}{21}, \frac{3}{7}, \frac{3}{2}, \frac{51}{42})$	5	42	1
9	$(-\frac{9}{21}, \frac{9}{7}, \frac{9}{2}, \frac{153}{42})$	11	42	1
15	$(-\frac{15}{21}, \frac{15}{7}, \frac{15}{2}, \frac{255}{42})$	1	42	1
27	$(-\frac{27}{21}, \frac{27}{7}, \frac{27}{2}, \frac{459}{42})$	1	42	3
33	$(-\frac{33}{21}, \frac{33}{7}, \frac{33}{2}, \frac{561}{42})$	11	42	3
39	$(-\frac{39}{21}, \frac{39}{7}, \frac{39}{2}, \frac{663}{42})$	5	42	3

So $\lambda = \#\Lambda = 6$. □

Next, we wish to determine the Betti number b_2.

Theorem 3.2. *the Betti number b_2 of the surface defined by $y^2 = x^3 + t^7x + 1$ equals 2.*

Proof. We recall the Weierstrass equation $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Q}[t]$. With our equation (7), we have that $a(t) = t^7$ and $b(t) = 1$. The polynomials are clearly minimal and not both are constant, so we can immediately compute n:

$$n = \max(\lceil \frac{\deg(a)}{4} \rceil, \lceil \frac{\deg(b)}{6} \rceil) = 2,$$

so $b_2 = 22$. □

Finally, we will prove the following about the number ρ_{triv} of $\mathcal{E}$:

Theorem 3.3. *The surface defined by $y^2 = x^3 + t^7x + 1$ has $\rho_{triv} = 3$.*

Proof. As we have seen in section 2.1, ρ_{triv} is the sum of the components of all rational fibres. We find the rational fibres by fixing $t = t_0$ and determining for which t_0 our curve $E_{t_0}/\mathbb{Q}$ is not an elliptic curve. For finite t_0, the singular curves can be found at the t_0 for which $\Delta(E_{t_0}) = 0$. For our curve, we have that

$$\Delta(E_{t_0}) = -4t^{21} - 27. \tag{8}$$

So Δ has 21 simple roots, which means that E has 21 singular fibres of type I_1, which have one component.

For infinite t, let $t = \frac{1}{s}$ and apply the coordinate change as stated in equation 1, for $u \in \overline{\mathbb{Q}}(s)^*$, to obtain $E' : \eta^2 = \xi^3 + s\xi + s^{12}$. This equation is minimal at $s = 0$ and $E'_{s=0}$ is clearly not an elliptic curve. From [6, p. 14], we get that $E_{t=\infty}$ is a singular fibre of type III, which has $\nu_\infty = 2$.

Recall equation 3:

$$\rho_{\text{triv}} = 2 + \sum(\nu_{t_0} - 1) = 2 + 21 \cdot (1 - 1) + (2 - 1) = 3$$

□

We can now determine the rank of our surface by equation 4:

$$r = b_2 - \lambda - \rho_{\text{triv}} = 22 - 6 - 3 = 13$$

We conclude that there are thirteen solutions $(x_i(t), y_i(t))$, with $i \leq 13$ of equation 7, that are independent in the group $E(\overline{\mathbb{Q}}(t))$.

3.2 Torsion Points

We will now show that the elliptic curve E over $\overline{\mathbb{Q}}(t)$ defined by equation 7 has no nontrivial torsion points.

Theorem 3.4. *The elliptic curve $E : y^2 = x^3 + t^7x + 1$ has no torsion points other than $\mathcal{O}$*

Proof. Our surface is defined by the Weierstrass equation $y^2 = x^3 + t^7x + 1$. Use theorem 2.2 and assume that $P = (\alpha, \beta) \in E(\overline{\mathbb{Q}}(t))$ is a nonzero torsion point. $\Delta(\mathcal{E}) = -4t^{21} - 27$, which has no double roots in $\overline{\mathbb{Q}}$, so β must be constant. First, assume $\beta = 0$, then $\alpha(\alpha^2 + t^7) = -1$, so $\alpha \in \overline{\mathbb{Q}}[t]^* = \overline{\mathbb{Q}}^*$. However, this contradicts that α must have a t component, because $\alpha^3 + t^7\alpha + 1$ has a degree of 7 in t. So $\beta \neq 0$ and therefore $\beta \in \overline{\mathbb{Q}}^*$. We have a $\beta \in \overline{\mathbb{Q}}^*$ and we wish to determine if there is an α such that $(\alpha, \beta) \in E(\overline{\mathbb{Q}}(t))$. Assume there is, then α satisfies the equation

$$\alpha^3 + t^7\alpha + 1 - \beta^2 = 0.$$

Then $\alpha \in \overline{\mathbb{Q}}[t]$ and $\alpha | 1 - \beta^2$. If $\beta^2 \neq 1$, then α is a nonzero constant. However, $\alpha^3 + t^7\alpha + 1 - \beta^2$ has degree 7 in t, so no such α can exist in this case. If $\beta = \pm 1$, then $\alpha^3 + t^7\alpha = 0$, so $\alpha = 0$ or $\alpha^2 = t^7$. In the latter case, we have that $\alpha \notin \overline{\mathbb{Q}}[t]$, which contradicts an earlier finding. This means that α must be zero, so the only two candidate torsion points that we have left, are $(0, \pm 1)$. Let $P = (0, \pm 1)$, then $2 \cdot P = (\frac{t^{14}}{4}, \mp\frac{t^{21}}{8} \mp 1)$, which shows that $\beta^2 \nmid \Delta(E)$, so P is not a torsion point. We conclude that there are no torsion points. □

We will now prove Theorem 3.4 in an alternative way, using reduction theory.

Proof. Use the fact that $\overline{\mathbb{Q}}(t) = \overline{\mathbb{Q}}(\frac{1}{t})$ and let $\frac{1}{t} = s$. Then the elliptic curve is described as follows:

$$\begin{aligned} E : y^2 &= x^3 + t^7x + 1 \\ &= x^3 + s^{-7}x + 1 \end{aligned} \tag{9}$$

We multiply with s^{12} and use the standard coordinate change (see equation 1, with $u = s^2$. Then

$$E : \eta^2 = \xi^3 + s\xi + s^{12} \tag{10}$$

which is another equation defining the curve E.

Define $\overline{E} = E \bmod (s)$, then $\overline{E} : \eta^2 = \xi^3$ over $\overline{\mathbb{Q}}$.

$$\begin{array}{ccc} E(\overline{\mathbb{Q}}(s)) \subset E(\overline{\mathbb{Q}}((s))) & \xrightarrow{\bmod s} & \overline{E}(\overline{\mathbb{Q}}) \\ \cup & & \\ E_0(\overline{\mathbb{Q}}((s))) & \xrightarrow{\phi:\ \bmod s} & \overline{E_{ns}}(\overline{\mathbb{Q}}) \end{array} \tag{11}$$

The map mod s is defined as follows. Since $E \subset \mathbb{P}^2$, every point $P \in E(\overline{\mathbb{Q}}((s)))$ can be written as $(a(s) : b(s) : c(s))$ with $a, b, c \in \overline{\mathbb{Q}}[[s]]$ and at least one of them in $\overline{\mathbb{Q}}[[s]]^*$. Now $P \mod s$ is defined as $(a(0) : b(0) : c(0)) \in \overline{E}(\overline{\mathbb{Q}})$. This is analogous to section 7.2 of [8].

The set E_0 consists of the points that are not singular when mapped by mod s, so in this case, $(0, 0)$ is the only point that can be found in $\overline{E}(\overline{\mathbb{Q}})$ but not in $\overline{E}_{ns}(\overline{\mathbb{Q}})$.

$\overline{E}$ clearly has a cusp at $(0, 0)$, so we may apply proposition 2.5b of chapter III of [8], which tells us that E_{ns} is isomorphic to an additive group, in our case with the structure $(\mathbb{Q}, +, 0)$.

Assume that $P \in E(\overline{\mathbb{Q}}((s)))$ is a torsion point not equal to $\mathcal{O}$. Because there is a type III fibre at $s = 0$, the table 15.1 at [8, p. 448] tells us that $E_0(\overline{\mathbb{Q}}((s)))$ is a subgroup of $E(\overline{\mathbb{Q}}((s)))$ of index 2. So $2P = \mathcal{O}$, which we know to be impossible.

□

3.3 The Galois action on the rational points

From sections 3.1 and 3.2, we know that the Mordell-Weil group $E(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}^{13}$.

E over $\overline{\mathbb{Q}}(t)$ has j-invariant $1728\frac{4t^{21}}{4t^{21}+27}$, so there is a curve over $\overline{\mathbb{Q}}(t^{21})$ with a j-invariant that has the same value. Some calculations, by the use of equation 1, show that $E \cong (\eta^2 = \xi^3 + t^{-21}\xi + t^{-42})$.

Let $t^{21} = T$, then we have the following construction:

$$\begin{array}{ccc} \mathbb{Z}^{13} \cong E(\overline{\mathbb{Q}}(t)) & \circlearrowleft & \mathrm{Gal}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(t^{21})) \cong \mathbb{Z}/21\mathbb{Z} \\ \cup & & \\ \mathbb{Z} \cong E(\overline{\mathbb{Q}}(T)). & & \end{array}$$

The group $\mathrm{Gal}(\overline{\mathbb{Q}}(t)/\overline{\mathbb{Q}}(t^{21}))$ acts on $E(\overline{\mathbb{Q}}(t))$: for $\tau \in$Gal and $P = (x_0, y_0) \in E(\overline{\mathbb{Q}}(t))$ one takes $\tau(P) := (\tau(x_0), \tau(y_0))$. This action is linear in the sense that $\tau(P + Q) = \tau(P) + \tau(Q)$ and $\tau(\mathcal{O}) = \mathcal{O}$. Moreover, the Galois group is cyclic, by σ with $\sigma(t) = \zeta t$ with $\zeta \in \overline{\mathbb{Q}}$ a primitive 21^{tst} root of unity. If we fix a basis for $E(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z}^{13}$, then the action of σ on $E(\overline{\mathbb{Q}}(t))$ is given by an

invertible matrix $A \in \mathbb{Z}^{13}$. As $\sigma^{21} = id, A^{21} = I$, so A is diagonalizable over $\mathbb{C}$. This tells that the eigenvalues of A form a satisfy $\lambda^{21} - 1 = 0$, so they can only be 21^{st}, 7^{th}, 3^{rd} roots of unity or 1.

Now let k be a field that contains the 21^{st} roots of unity, then we have the following construction:

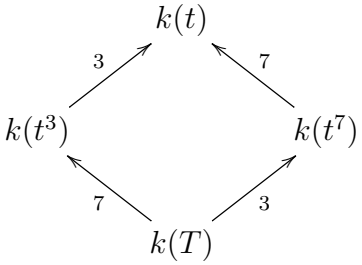
$$\begin{array}{c} k(t) \\ \Big\downarrow \text{Galois, degree 21} \\ k(T) \end{array}$$

Denote the Galois group by $G = \langle\sigma\rangle$, where σ has the property that $\sigma(t) = \zeta t$, with ζ a primitive 21^{st} root of unity.

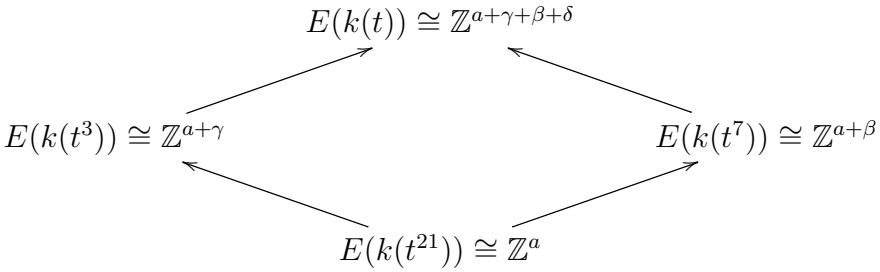
Non-trivial subgroups of G can be found by factoring 21 in its primes, so one can see that $H_3 = \{id, \sigma^7, \sigma^{14}\} = \langle\sigma^7\rangle$ and $H_7 = \{id, \sigma^3, \ldots, \sigma^{18}\} = \langle\sigma^3\rangle$ are the only subgroups of G. Next, we determine $k(t)^{H_3}$:

$$\begin{aligned} k(t)^{H_3} &= \{f \in k(t) | \tau(f) = f \forall \tau \in H_3\} \\ &= \{f \in k(t) | \sigma^7(f) = f\} \\ &= \{f \in k(t) | f(\zeta^7 t) = f(t)\} \\ &= k(t^3). \end{aligned}$$

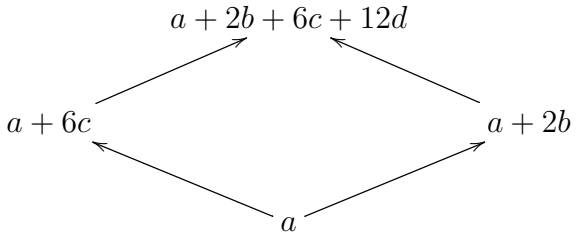
Similarly, we get that $k(t)^{H_7} = k(t^7)$, so we can find subfields of $k(t)$ as follows:



The Mordell-Weil groups of E over these function fields then have the same construction:



To determine β, γ and δ, we note that the third roots of unity (which exist in $k(t^7)$), come in pairs. $\beta = 2b$. Similarly, the seventh roots of unity come in sets of six, so $\gamma = 6c$. Finally, the primitive 21^{st} roots of unity (in $k(t)$), show that $\delta = 12d$. Then the rank of the Mordell-Weil groups of E over its respective function field, is determined to be the following:



If 1 is an eigenvalue of A, then there is a $v \in \mathbb{Z}^{13}$ that is a solution to $(A - I)v = 0$ for nonzero v. The point $P = (0, 1)$ satisfies $\sigma(P) = P$, so 1 is indeed an eigenvalue of A.

The third roots of unity satisfy $\sigma^3 = id$, so we look at $E(\overline{\mathbb{Q}}(t)^{\langle\sigma^3\rangle}) = E(\overline{\mathbb{Q}}(t^7))$. We determine the rank of $E(\overline{\mathbb{Q}}(t^7))$ to see that it is isomorphic with $\mathbb{Z}$ (for the proof, see section 6), so the third roots of unity do not contribute to the set of eigenvalues or to the set of points (Means that we only have id as contribution, why?). Similarly, we can prove that $E(\overline{\mathbb{Q}}(t)^{\langle\sigma^7\rangle}) = E(\overline{\mathbb{Q}}(t^3)) \cong \mathbb{Z}$, so the 7^{th} roots of unity also do not contribute.

What remains are the 21^{st} roots of unity: these are roots of the minimal cylcotomic polynomial $\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$. So $\mathbb{Q}[\sigma] \cong \mathbb{Q} \times \mathbb{Q}(\zeta_{21})$.

Matrix A works over $\mathbb{Q}$ and has its characteristic polynomial $\det(A - \lambda I)$ in $\mathbb{Z}[\lambda]$, so the minimal polynomial of ζ_{21} divides the characteristic polynomial:

$$A \sim \begin{pmatrix} 1 & & & & & & & & & & & & \\ & \zeta_{21} & & & & & & & & & & & \\ & & \zeta_{21}^2 & & & & & & & & & & \\ & & & \ddots & & & & & & & & & \\ & & & & \zeta_{21}^i & & & & & & & & \\ & & & & & \ddots & & & & & & & \\ & & & & & & \zeta_{21}^{20} & & & & & & \end{pmatrix}$$

where i is coprime with 21. So

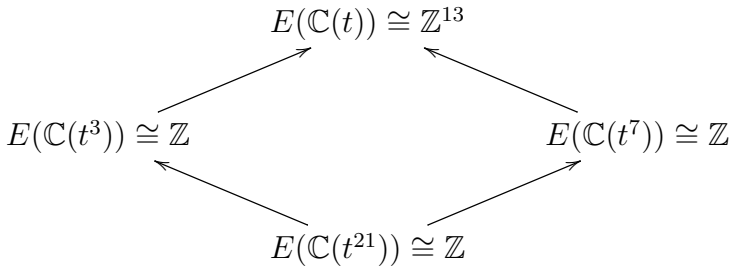
$$(A - I) \cdot (A - \zeta_{21} I) \cdot \ldots \cdot (A - \zeta_{21}^{20} I) = (A - I) \cdot (\Phi_{21}(A)) = 0. \qquad (12)$$

This tells us that $\mathbb{Q}[A] \cong \mathbb{Q} \times \mathbb{Q}(\zeta_{21})$ and even $\mathbb{Z}[A] \cong \mathbb{Z}[x]/(x \cdot \Phi_{21}(x)) \cong \mathbb{Z} \times \mathbb{Z}[\zeta_{21}]$.

In [10, p. 205], it is stated that $\mathbb{Q}(\zeta_{21})$ has class number 1, so $\mathbb{Z}[\zeta_{21}]$ is a principal ideal ring. Let τ be the generator of $\mathrm{Gal}(\mathbb{C}(t)/\mathbb{C}(t^{21}))$ and Φ the minimal polynomial of the 21^{st} roots of unity. Denote the Mordell-weil group of E by M. $x-1$ and $\Phi(x)$ generate $\mathbb{Z}[x]$, so we have that $\phi(\tau)M \oplus (\tau-1)M = M$.

Let $P \in \Phi(\tau)M$, then we have $(\tau-1)P = O$, or $\tau(P) = P$, so $\Phi(\tau)M$ is the part of M that is invariant under τ, i.e. the group with generator $P = (0,1)$. $(\tau-1)M$ is the kernel of $\Phi(\tau)$ and a module over $\mathbb{Z}[\zeta_{21}]$. To show that his module is torsion free, let $P \in (\tau-1)M$ and $\alpha \in \mathbb{Z}[\zeta_{21}]$, such that $\alpha P = O$. Then we also have that $|\alpha|P = O$, but M is torsion free, so $\alpha = 1$ for all cases. Since $\mathbb{Z}[\zeta_{21}]$ is a principal ideal ring, we have that $(\tau-1)M$ is free over $\mathbb{Z}[\zeta_{21}]$. Then we conclude that $(\tau-1)M = \mathbb{Z}[\zeta_{21}] \cdot P$ for a $P \in M$.

Recall the image of the subfields of the Mordell-Weil groups over $k(t)$ and its subfields (12). The ranks are now provided.



4 Determining a point

In this section, we will try to find a nontrivial point $P \in E$, that is a generator of $E(\overline{\mathbb{Q}}(t))$. We let $x(t)$ and $y(t)$ be polynomials in $\overline{\mathbb{Q}}(t)$. In [5], M. Kuroda determined a form of $x(t)$ and $y(t)$, as well as the constraints of their coefficients, we will give a more detailled description. First, we will derive a relation between the degree of x at a point P and the height pairing $\langle P, P\rangle$, which will help us choose the form of the polynomials. Then we use these polynomials to find a point solution to E over a finite field. Finally, we apply Hensel's lemma (see [1]) to lift this solution to $\overline{\mathbb{Q}}$.

4.1 Height Pairing

Theorem 4.1. *If $P \in E(k(t))$ satisfies $\langle P, P\rangle \leq 4$ (but nonzero), then $x(P)$ is a polynomial of degree ≤ 4. Moreover, $deg(x(P)) = 4$ if and only if $\langle P, P\rangle = 4$ and $deg(x(P)) \leq 3$ if and only if $\langle P, P\rangle = \frac{7}{2}$.*

Proof. To show this, we turn to [7, p. 21], where the height paring is discussed.

Let $P \in E(\overline{\mathbb{Q}})$, then $\langle P, P\rangle = 2\chi + 2(PO) - \sum_{v\in R} contr_v(P)$. For us, $\chi = 2$ and $(PO) = k$ with $k \in \mathbb{Z}_{\geq 0}$. Moreover, $contr_v(P)$ is the local contrivution at a bad fibre of E. We determine which componen ts P and O intersect at a bad fibre and what contribution they have. In section 2.1, we determined that E has 21 fibres of type I_1 and one of type III (at ∞). Fibres of type I_1 have no contribution but:

$$contr_v(P) = \begin{cases} \frac{1}{2} & \text{if } P \text{ and } O \text{ intersect different components at } \infty \\ 0 & \text{if } P \text{ and } O \text{ intersect the same components at } \infty \end{cases} \tag{13}$$

To look at the curve at $t = \infty$, recall equations 9 and 10:

$$\begin{aligned} E &: y^2 = x^3 + t^7 x + 1 \\ &\downarrow \\ E' &: \eta^2 = \xi^3 + s\xi + s^{12}, \end{aligned}$$

so we determine its behaviour at $s = 0$.

A point $P = (x(t), y(t))$ in E is equivalent to $P = (s^4 x(\frac{1}{s}), s^6 y(\frac{1}{s}))$. Equivalently, the x-coordinate described by:

$$x(t) = \frac{a_d t^d + \ldots + a_0}{b_e t^e + \ldots + b_0},$$

is the following in s:

$$s^4 \cdot x(s^{-1}) = s^4 \frac{a_d s^{-d} + \ldots + a_0}{b_e s^{-e} + \ldots + b_0}. \tag{14}$$

In the latter case, the degree of the numerator equals $4 - d$ and the degree of the denominator equals $-e$. We now have two cases.

Case 1: $-e \leq 4 - d$. We multiply the rational function by s^e, to get

$$s^4 \cdot x(s^{-1}) = \frac{a_d s^{4-d+e} + \ldots + a_0 s^e}{b_e + \text{h.o.t.}}.$$

We substitute $s = 0$ to see that

$$s^4 \cdot x(s^{-1}) = \begin{cases} 0 & \text{if } 4 - d + e > 0, \\ \frac{a_d}{b_e} & \text{if } 4 - d + e = 0. \end{cases}$$

$P(\infty) = (0 : 0 : 1)$ if $d < 4 + e$ and a smooth point if $d = 4 + e$.

Case 2: $4 - d < -e$, then:

$$s^4 \cdot x(s^{-1}) = \frac{a_d + \text{h.o.t.}}{b_e s^{d-4-e} + \text{h.o.t.}}.$$

At $s = 0$, the point is at ∞, and the curve is reduced to $\eta^2 = \xi^3$, which provides a smooth point. This means that equation 13 reduces to:

$$contr_v(P) = \begin{cases} \frac{1}{2} & \text{if deg(numerator of } x(t)) \\ & \quad < 4 + \deg(\text{denominator of } x(t)) \\ 0 & \text{otherwise} \end{cases}$$

The minimality of $\langle P, P \rangle$ is reached when $(PO) = 0$, so $P(t_0) \neq O = \infty$ must hold for finite t_0 and infinity. This means that $x(P)$ must be a polynomial, i.e. of the form $a_d t^d + \ldots a_0$, for finite t_0. If $t_0 = \infty$, or $s_0 = 0$, we require $s_0^4 \cdot x(s_0^{-1})$ to be a polynomial (as shown by equation 14). So $x(P)$ must be a polynomial with $\deg(x(P)) \leq 4$.

The following table gives the degree in t of the right hand side of $y^2 = x^3 + t^7 x + 1$, depending on the degree of $(x(t))$, and what the resulting degree of $y(t)$ is:

$\deg(x(t))$	deg r.h.s.	$\deg(y(t))$
0	0 (if $x = 0$), 7 (if $x \neq 0$)	0 (cannot exist if $x \neq 0$)
1	8	4
2	9	cannot exist
3	10	5
4	12	6

This concludes the proof that $\deg(x(t)) \leq 4$ and that $\deg(y(t)) \leq 6$. $\square$

In our search for points $P = (x(t), y(t))$ on E, we will first try to find points with the property $\langle P, P \rangle \leq 4$. The correspoding $x(t)$ and $y(t)$ are then denoted as follows:

$$x(t) = \sum_{m=0}^{4} a_m t^m,$$
$$y(t) = \sum_{n=0}^{6} b_m t^m.$$

By comparing coefficients in the equality $y(t))^2 = (x(t))^3 + x(t)t^7 + 1$, we obtain the following set of equations that $(a_0, \ldots, a_4, b_1, \ldots, b_6)$ must satisfy for the pair $(x(t), y(t))$ to be a point P on E:

$$\begin{aligned}
a_4^3 &= b_6^2 \\
3a_3a_4^2 + a_4 &= 2b_5b_6, \\
3a_2a_4^2 + 3a_3^2a_4 + a_3 &= 2b_4b_6 + b_5^2, \\
3a_1a_4^2 + 6a_2a_3a_4 + a_2 + a_3^3 &= 2b_3b_6 + 2b_4b_5, \\
3a_0a_4^2 + 6a_1a_3a_4 + a_1 + 3a_2^2a_4 + 3a_2a_3^2 &= 2b_2b_6 + 2b_3b_5 + b_4^2, \\
6a_0a_3a_4 + a_0 + 6a_1a_2a_4 + 3a_1a_3^2 + 3a_2^2a_3 &= 2b_1b_6 + 2b_2b_5 + 2b_3b_4, \\
6a_0a_2a_4 + 3a_0a_3^2 + 3a_1^2a_4 + 6a_1a_2a_3 + a_2^3 &= 2b_0b_6 + 2b_1b_5 + 2b_2b_4 + b_3^2, \\
6a_0a_1a_4 + 6a_0a_2a_3 + 3a_1^2a_3 + 3a_1a_2^2 &= 2b_0b_5 + 2b_1b_4 + 2b_2b_3, \\
3a_0^2a_4 + 6a_0a_1a_3 + 3a_0a_2^2 + 3a_1^2a_2 &= 2b_0b_4 + 2b_1b_3 + b_2^2, \\
3a_0^2a_3 + 6a_0a_1a_2 + a_1^3 &= 2b_0b_3 + 2b_1b_2, \\
3a_0^2a_2 + 3a_0a_1^2 &= 2b_0b_2 + b_1^2, \\
3a_0^2a_1 &= 2b_0b_1, \\
a_0^3 + 1 &= b_0^2,
\end{aligned}$$

The code to obtain this set can be found in 7.2. Should we try to find a solution depending only on $(a_0, \ldots, a_3, b_0, \ldots b_5)$, i.e. a point P with height pairing $\frac{7}{2}$, then magma is quick to find out that only the trivial soulutions can exist (see 7.4 for the code). A nontrivial solution depending on all twelve variables cannot be found by magma, but a different approach is discussed in the next sections.

4.2 A point over $\mathbb{F}_{41}$

Magma cannot find a set $(a_0, \ldots, a_4, b_0, \ldots, b_6)$ that corresponds to a non-trivial point of E over $\overline{\mathbb{Q}}(t)$, but when solving the problem over $\mathbb{F}_p$, solutions can be found in a reasonable time. This is what we will now do, with $p = 41$. When we have found points $P \in E(\mathbb{F}_{41})$, we will use Hensel's lemma (as explained in section 4.3) to lift P to a point in $\mathbb{Q}_p(t)$, the function field over the field of p-adic numbers.

The magma code which determines the equations in the previous section, is adapted to find solutions to this set, and can be found in 7.3. Using this code, we find 48 points (24 pairs of P and $-P$) in $E(\mathbb{F}_{41}(t))$.

An example of such a solution is $a = (0, -5, 4, 7, -8, 1, 0, 0, -1, 27, -1, 29)$. This corresponds to $P = (x(t), y(t)) = (-5t + 4t^2 + 7t^3 - 8t^4, 1 - t^3 + 27t^4 - t^5 + 29t^6) \in E(F_{41}(t))$, with $E : y^2 + x^3 + t^7x + 1$.

The field extension $\mathbb{F}_{41}(t^{21})$ is not Galois, since the minimal polynomial of t over $\mathbb{F}_{41}(t^{21})$ is $x^{21} - t^{21}$, which does not split over $\mathbb{F}_{41}(t)$. To obtain a splitting field, we need a primitive 21^{st} root of unity. Since $21|41^2 - 1 = (41-1)(41+1)$, such a root ζ exists in $\mathbb{F}_{41^2}$, and we see that $\mathbb{F}_{41^2}(t)/\mathbb{F}_{41^2}(t^{21})$ is Galois, with group $\text{Gal}(\mathbb{F}_{41^2}(t)/\mathbb{F}_{41^2}(t^{21}))$ generated by σ, which is defined by $\sigma(t) = \zeta t$.

The curve $\tilde{E} : y^2 = x^3 + t^{-21}x + t^{-42}$ is defined over $\mathbb{F}_{41^2}(t^{21})$, so σ generates an automorphism of the group

$$\tilde{E}(\mathbb{F}_{41^2}(t)) \cong E(\mathbb{F}_{41^2}(t)),$$

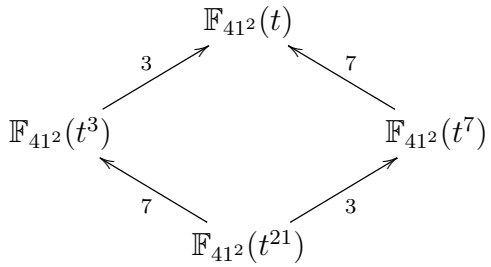
with isomorphism:

$$\begin{aligned} P = \big(\frac{x(t)}{t^{14}}, \frac{y(t)}{t^{21}}\big) &\mapsto (x(t), y(t)) \\ \sigma(P) = \big(\frac{x(\zeta t)}{(\zeta t)^{14}}, \frac{y(\zeta t)}{(\zeta t)^{21}}\big) &\mapsto (\zeta^7 x(\zeta t), y(\zeta t). \end{aligned} \tag{15}$$

$\sigma^{21} = \text{id}$ in $\text{Gal}(\overline{\mathbb{F}}_{41}(t)/\overline{\mathbb{F}}_{41^2}(t))$, so we also have:

$$\begin{gathered} (\sigma^{21} - \text{id}) \in \text{End}(E(\mathbb{F}_{41^2}(t))) \\ \shortparallel \\ (\sigma - \text{id})\Phi_3(\sigma)\Phi_7(\sigma)\Phi_{21}(\sigma) \end{gathered}$$

Recall the image of the subfields of $k(t)$, on page 12. With $k = \mathbb{F}_{41}$, we get the following construction of subfields:



Using magma (see 7.5 for the code), we determine $(1-\sigma(P))(\Phi_{21}(\sigma(P)) \neq O$. This is different from the situation over $\overline{\mathbb{Q}}$, where $(1-\sigma)(\Phi_{21}(\sigma)) = O$ in $\mathrm{End}(E(\overline{\mathbb{Q}}(t))$.

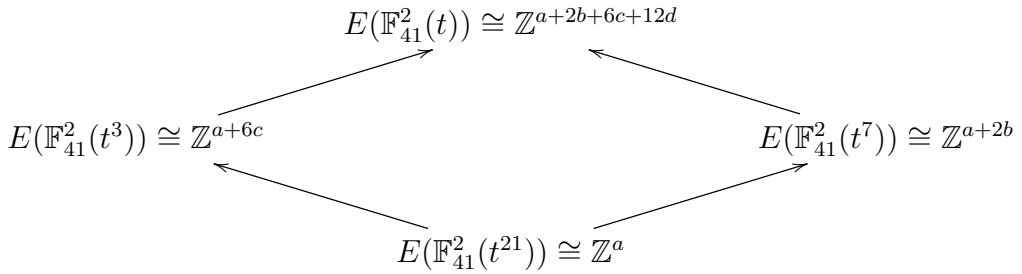
Equation 15 shows that $\sigma^3(P) = P$, so

$$E(\mathbb{F}_{41^2}(t)) \supset E(\mathbb{F}_{41^2}(t))^{\langle\sigma^3=\mathrm{id}\rangle} = E(\mathbb{F}_{41^2}(t^7) = E(\mathbb{F}_{41^2}(t^{21})) = E(\mathbb{F}_{41^2}(t))^{\langle\sigma=\mathrm{id}\rangle},$$

then $E(\mathbb{F}_{41^2}(t^7))$ has rank 1. We deduce that $(\sigma - \mathrm{id})\Phi_7(\sigma)\Phi_{21}(\sigma) = O$ in $\mathrm{End}(E(\mathbb{F}_{41^2}(t)))$. This means that $E(\mathbb{F}_{41^2}(t))^{\langle\sigma^7=\mathrm{id}\rangle} = E(\mathbb{F}_{41^2}(t^3))$ must have rank at least 7.

To check if $(\sigma-\mathrm{id})\Phi_7(\sigma) = O$, assume that there is a $P \in E(\mathbb{F}_{41^2}(t))^{\langle\sigma^7=\mathrm{id}\rangle}$. Then $\sigma^7(P) = P$, so $(\zeta^7 x(\zeta^7 t), y(\zeta^7 t)) = P$. However, take $P = (-5t + 4t^2 + 7t^3 - 8t^4, 1 - t^3 + 27t^4 - t^5 + 29t^6)$, then $\sigma^7(x(P))$ has first coeficient equal to $\zeta^{14}(-5) \neq -5$, contradicting the assumption. So P is not exclusively found in $E(\mathbb{F}_{41^2}(t))^{\langle\sigma^7=\mathrm{id}\rangle}$. Then $(\sigma - \mathrm{id})\Phi_7(\sigma) \neq O$.

As in the case of a field with characteristic 0, we have the following construction of the Mordell-Weil group of E over the different finite function fields:



We have established that $\mathrm{rank}(E(\mathbb{F}_{41^2}(t^7))) = 1$, so $b = 0$. Similarly, $c \geq 1$ and $d \geq 1$. E is a K3 surface, so it has rank at most 20. We conclude that $c = d = 1$. Since $E(\mathbb{F}_{41^2}(t))^{\langle\sigma=\mathrm{id}\rangle}$ has rank 1, $\mathrm{rank}(E(\mathbb{F}_{41^2}(t))) = 19$.

As an example, let $P = (-5t + 4t^2 + 7t^3 - 8t^4, 1 - t^3 + 27t^4 - t^5 + 29t^6)$ and apply the magma code from section 7.5. Then we indeed have:

$$\begin{aligned}
&\Phi_{21}(\sigma(P))\Phi_7(\sigma(P))(1-\sigma(P)) \\
&\quad = -P + \sigma(P) - \sigma^3(P) + \sigma^4(P) - \sigma^6(P) + \sigma^7(P) - \sigma^9(P) + \sigma^{10}(P) \\
&\qquad - \sigma^{12}(P) + \sigma^{13}(P) - \sigma^{15}(P) + \sigma^{16}(P) - \sigma^{18}(P) + \sigma^{19}(P) \\
&\quad = O.
\end{aligned}$$

4.3 Hensel lifting

In this section, we will lift the point $P = (x(t), y(t))$ from the previous section from $\mathbb{F}_p(t)$ to $\mathbb{Q}_p(t)$, the function field over the field of p-adic numbers. To do so, we first discuss Hensel's lemma:

Theorem 4.2. *If $f(X) \in \mathbb{Z}_p[X]$ and a $a \in \mathbb{Z}_p$ satisfies*

$$f(a) \equiv 0 \mod p, f'(a) \neq 0 \mod p, \tag{16}$$

then there is an $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0 \in \mathbb{Z}_p$ and $\alpha \equiv a \mod p$.

The theorem and proof can be found in [1]. It is also the case $n = 1$ of theorem 4.3 below.

While this theorem helps us find a zero in $\mathbb{Z}_p$ of a polynomial $f(x)$, we need an analog for a system of polynomial equations in more variables. This is stated as follows:

Theorem 4.3. *Let $f_1, \ldots f_n$ be a system of n polynomials in $\mathbb{Z}_p[x_1, \ldots, x_n]$ and let $(a_1, \ldots, a_n)$ be a vector in $\mathbb{Z}_p^n$ with:*

$$f_i(a) \equiv 0 \mod p \text{ for all } i \in \{1, \ldots, n\}$$

and

$$\det(\frac{\partial}{\partial x_j} f_i)(a) \neq 0 \mod p$$

Then $\alpha \in \mathbb{Z}_p^n$ exists such that $f_i(\alpha) = 0$ for all i and $\alpha \equiv a \mod p$.

Proof. We will construct a Cauchy sequence $a^{(1)} = a, a^{(2)}, \ldots, a^{(m)}, \ldots$ in $\mathbb{Z}_p^n$, such that $f_j(a^{(m)}) \equiv 0 \mod p^m$ for all j and m. Then $\alpha := \lim_{m\to\infty} a^{(m)}$ is the desired solution.

Suppose $m \geq 1$ and $a^{(1)} \ldots, a^{(m)}$ have been constructed satisfying $a^{(j)} \equiv a^{(j-1)} \mod p^{j-1}$, for all $j \leq m$, and $f_i(a^{(j)}) \equiv 0 \mod p^j$ for all i. To determine $a^{(m+1)}$, try $a^{(m+1)} := a^{(m)} + p^m \cdot \lambda$ for some $\lambda \in \mathbb{Z}_p^n$. Write $f_i(a^{(m)}) = p^m \cdot b_i$ with $b_i \in \mathbb{Z}_p$, and $i = 1, \ldots, n$.

Then

$$\begin{aligned} f_i(a^{(m+1)}) \mod p^{m+1} \\ &= f_i(a^{(m)}) \mod p^{m+1} + p^m(\nabla f_i(a^{(m)}))\lambda \mod p^{m+1} \\ &= p^m(b_i + (\nabla f_i)\lambda) \mod p^{m+1} \end{aligned}$$

This is $0 \mod p^{m+1}$ for every $i = 1, \ldots, n$, precisely when $b_i + (\nabla f_i)\lambda \equiv 0 \mod p$. Since $a^{(m)} \equiv a^{(1)} \mod p$, this means λ should satisfy:

$$\begin{pmatrix} \nabla f_1(a) \\ \nabla f_2(a) \\ \vdots \\ \nabla f_n(a) \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} -b_1 \\ -b_2 \\ \vdots \\ -b_n \end{pmatrix} \mod p.$$

By assumption, the matrix presented here is nonsingular modulo p, hence such a λ exists. □

We will now use theorem 4.3 to show the following:

Proposition 1. *There exist* $\alpha = (\alpha_0, \ldots, \alpha_4, \beta_0, \ldots, \beta_6) \in \mathbb{Z}_{41}^{12}$, *with* $\alpha \neq (0, \ldots, 0, \pm 1, 0, \ldots, 0)$ *such that* $f_i(a) = 0$ *for all* $1 \leq i \leq 13$, *with:*

$$\begin{aligned} f_1 &= a_4^3 - b_6^2 \\ f_2 &= 3a_3a_4^2 + a_4 - 2b_5b_6, \\ f_3 &= 3a_2a_4^2 + 3a_3^2a_4 + a_3 - 2b_4b_6 + b_5^2, \\ f_4 &= 3a_1a_4^2 + 6a_2a_3a_4 + a_2 + a_3^3 - 2b_3b_6 + 2b_4b_5, \\ f_5 &= 3a_0a_4^2 + 6a_1a_3a_4 + a_1 + 3a_2^2a_4 + 3a_2a_3^2 - 2b_2b_6 + 2b_3b_5 + b_4^2, \\ f_6 &= 6a_0a_3a_4 + a_0 + 6a_1a_2a_4 + 3a_1a_3^2 + 3a_2^2a_3 - 2b_1b_6 + 2b_2b_5 + 2b_3b_4, \\ f_7 &= 6a_0a_2a_4 + 3a_0a_3^2 + 3a_1^2a_4 + 6a_1a_2a_3 + a_2^3 - 2b_0b_6 + 2b_1b_5 + 2b_2b_4 + b_3^2, \\ f_8 &= 6a_0a_1a_4 + 6a_0a_2a_3 + 3a_1^2a_3 + 3a_1a_2^2 - 2b_0b_5 + 2b_1b_4 + 2b_2b_3, \\ f_9 &= 3a_0^2a_4 + 6a_0a_1a_3 + 3a_0a_2^2 + 3a_1^2a_2 - 2b_0b_4 + 2b_1b_3 + b_2^2, \\ f_{10} &= 3a_0^2a_3 + 6a_0a_1a_2 + a_1^3 - 2b_0b_3 + 2b_1b_2, \\ f_{11} &= 3a_0^2a_2 + 3a_0a_1^2 - 2b_0b_2 + b_1^2, \\ f_{12} &= 3a_0^2a_1 - 2b_0b_1, \\ f_{13} &= a_0^3 - b_0^2 + 1. \end{aligned}$$

Proof. For the moment, only consider the system $f_1 = f_2 = \ldots = f_{12} = 0$, then $a := (0, -5, 4, 7, -8, 1, 0, 0, -1, 27, -1, 29)$ satisfies

$$\det(\frac{\partial}{\partial x_j} f_i)(a) \neq 0 \mod 41.$$

Namely,

$$\det(\frac{\partial}{\partial x_j} f_i)(a) = \begin{vmatrix} 0 & 0 & 0 & 0 & 28 & 0 & 0 & 0 & 0 & 0 & 0 & 24 \\ 0 & 0 & 0 & 28 & -8 & 0 & 0 & 0 & 0 & 0 & 24 & 2 \\ 0 & 0 & 28 & -8 & -4 & 0 & 0 & 0 & 0 & 24 & 2 & 28 \\ 0 & 28 & -8 & -4 & -2 & 0 & 0 & 0 & 24 & 2 & 28 & 2 \\ 28 & -8 & -4 & -2 & 2 & 0 & 0 & 24 & 2 & 28 & 2 & 0 \\ -8 & -4 & -2 & 2 & 3 & 0 & 24 & 2 & 28 & 2 & 0 & 0 \\ -4 & -2 & 2 & 3 & -7 & 24 & 2 & 28 & 2 & 0 & 0 & -2 \\ -2 & 2 & 3 & -7 & 0 & 2 & 28 & 2 & 0 & 0 & -2 & 0 \\ 2 & 3 & -7 & 0 & 0 & 28 & 2 & 0 & 0 & -2 & 0 & 0 \\ 3 & -7 & 0 & 0 & 0 & 2 & 0 & 0 & -2 & 0 & 0 & 0 \\ -7 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}$$

$= 2 \mod 41.$

By theorem 4.3, we now know that $\alpha' \in \mathbb{Z}_{41}^{12}$ exists such that $f_i(\alpha') = 0$ for $1 \leq i \leq 12$, and $\alpha' \equiv a \mod 41$. Put

$$\xi(t) := \alpha_0 + \alpha_1 t + \ldots + \alpha_4 t^4,$$
$$\eta(t) := \alpha_5 + \alpha_6 t + \ldots + \alpha_{11} t^6.$$

By construction, $\xi(t)^3 + t^7\xi(t) + 1 - \eta(t)^2$ is a constant $c \in 41\mathbb{Z}_{41}$, so $\eta^2 = \xi^3 + t^7\xi + 1 - c$, with $1 - c \neq 0$ and $\deg(\xi) = 4$, $\deg(\eta) = 6$. Applying Hensel's lemma (see theorem 4.2) to the polynomials $x^2 - 1 + c$ and $x^3 - 1 + c$, we obtain $\lambda, \mu \in \mathbb{Z}_{41}$ with $\lambda \equiv \mu \equiv 1 \mod 41$ and $\lambda^2 = 1 - c = \mu^3$. Now $\eta_1(t) := \frac{\eta(t)}{\lambda}$ and $\xi_1(t) := \frac{\xi(t)}{\mu}$ satisfy $\eta_1^2 = \xi_1^3 + \frac{t^7}{\mu^2}\xi_1 + 1$.

Apply Hensel's lemma to $x^7 - \mu^2$, which yields $\nu \in \mathbb{Z}_{41}$ with $\nu \equiv 1 \mod 41$ and $\nu^7 = \mu^2$. Finally, write

$$s := \frac{t}{\nu},$$
$$\xi_2(s) := \xi_1(s\nu) = \xi_1(t),$$
$$\eta_2(s) := \eta_1(s\nu) = \eta_1(t).$$

Then ξ_2, η_2 are polyonomials of degree 4 resp. 6, and $\eta_2^2 = \xi_2^3 + s^7\xi_2 + 1$. The coefficients of ξ_2, η_2 provide the solution $\alpha \in \mathbb{Z}_{41}^{12}$.

□

Fix a field homomorphism $\mathbb{Q}_p \to \mathbb{C}$, this embeds $Z(\mathbb{Q}_p) \to Z(\mathbb{C})$.
Claim: $Z(\mathbb{C})$ is finite, hence $Z(\mathbb{C}) = Z(\overline{\mathbb{Q}})$.

Proof. By construction, every point in $Z(\mathbb{C})$ corresponds to a point $P \in E(\mathbb{C})(t))$ of height $\langle P, P\rangle \in \{\frac{7}{2}, 4\}$. Since $E(\mathbb{C}(t))$ contains only finitely many points of bounded height, this shows that $Z(\mathbb{C})$ is finite. Suppose $\alpha \in Z(\mathbb{C}) \setminus Z(\overline{\mathbb{Q}})$. Then at least one of the coordinates of α is transcendental over $\mathbb{Q}$. Specializing this coordinate to elements of $\overline{\mathbb{Q}}$ then yields infinitely many points in $Z(\overline{\mathbb{Q}})$. □

Since we showed $\#Z(\mathbb{Q}_{41}) \geq 3$, it follows that $Z(\mathbb{C}) = Z(\overline{\mathbb{Q}})$ also has at least 3 elements. So indeed a point $P \in E(\overline{\mathbb{Q}}(t))$ exists with the x-coordinate a polynomial of degree 4.

5 Conclusion

In this thesis, we have tried to find the generators of the Mordell-Weil group of the elliptic curve $E/\overline{\mathbb{Q}}(t)$ defined by the equation $y^2 = x^3 + t^7x + 1$. We used a geometric approach to show that the Mordell-Weil group has rank 13, and showed that the group has no nontrivial torsion by using either the Nagell-Lutz theorem or reduction theory. By determing the Galois action on the rational points, we have shown that the thirteen generators are two sets: one only containing the trivial generator and one containing the twelve nontrivial generators. If we find one nontrivial generator, we can then apply the Galois action to find the other eleven.

So far, it is impossible to find a point on the curve over a function field with characteristic zero, but the computing software is able to determine a point on the curve over a finite field. We can then lift the point to a p-adic field using Hensel's lemma. Using some transformations, we then proved that a solution $\alpha \in \mathbb{Z}_{41}^{12}$ exists. Finally, a homomorphism is fixed to embed $Z(\mathbb{Q}_p)$ in $Z(\mathbb{C})$ and the fact that $Z(\mathbb{C}) = Z(\overline{\mathbb{Q}})$ tells us that there is a point $P \in E(\overline{\mathbb{Q}}(t))$ with the x-coordinate a polynomial of degree 4.

6 Additional proofs

In this section, we prove that rank$E/\overline{\mathbb{Q}}(t^3) = 1$ and that rank$E/\overline{\mathbb{Q}}(t^7) = 1$, facts we used in section 3.3.

Theorem 6.1. *Let $E : y^2 = x^3 + t^{-21}x + t^{-42}$ be an elliptic curve over $\overline{\mathbb{Q}}(t^7)$. Then this curve has rank equal to 1.*

Proof. Let $u = t^{-7}$, so $\overline{\mathbb{Q}}(t^7) = \overline{\mathbb{Q}}(u^{-1}) = \overline{\mathbb{Q}}(u)$, the rank of $E/\overline{\mathbb{Q}}(t^7)$ is obviously the same as the rank of $E/\overline{\mathbb{Q}}(u)$:

$$\begin{aligned} E : y^2 &= x^3 + t^{-21}x + t^{-42} \\ &\downarrow \\ E : \eta^2 &= \xi^3 + u^3\xi + u^6 \end{aligned}$$

This curve is a rational elliptic curve, so equation 4 reduces to $r = b_2 - \rho_{\text{triv}}$ (cite?), with $b_2 = 10$. To determine ρ_{triv}, we apply the same method as we did in theorem 3.1.

$\Delta(E/\overline{\mathbb{Q}}(u)) = 4u^9 + 27u^{12} = u^9(4 + 27u^3)$, so E has three singular fibres of type I_1 at finite nonzero u. For $u = 0$, we find a fibre of type III^* (which has eight components). In the case that $u = \infty$, let $v = \frac{1}{u}$, to find that the curve defined by $y^2 = x^3 + vx + 1$ has a curve of type I_0 (See [6, p. 14]). Then $\rho_{\text{triv}} = 2 + 7 = 9$ and $r = 10 - 9 = 1$. □

Theorem 6.2. *Let $E : y^2 = x^3 + t^{-21}x + t^{-42}$ be an elliptic curve over $\overline{\mathbb{Q}}(t^3)$. Then this curve has rank equal to 1*

Proof. Let $s = t^{-3}$, so $\overline{\mathbb{Q}}(t^3) = \overline{\mathbb{Q}}(s^{-1}) = \overline{\mathbb{Q}}(s)$. We transform E to a minimal curve in s:

$$\begin{aligned} E : y^2 &= x^3 + t^{-21}x + t^{-42} \\ &\downarrow \\ E : \eta^2 &= \xi^3 + s^3\xi + s^8 \end{aligned}$$

This is a K3 surface, so we have to determine the Lefschetz number.

The homogenized form of the equation is $X^3Z^5 + S^3XZ^5 - Y^2Z^6 + S^8$ and exponents form the following matrix:

$$A = \begin{pmatrix} 0 & 3 & 0 & 5 \\ 3 & 1 & 0 & 4 \\ 0 & 0 & 2 & 6 \\ 8 & 0 & 0 & 0 \end{pmatrix} \quad \text{with inverse:} \quad A^{-1} = \frac{1}{56}\begin{pmatrix} 0 & 0 & 0 & 7 \\ 32 & -40 & 0 & 15 \\ 24 & -72 & 28 & 27 \\ -8 & 24 & 0 & -9 \end{pmatrix}.$$

Then : $L \subset (\mathbb{Q}/\mathbb{Z})^4$ is generated by:

$$l_1 = (1,0,0,-1)A^{-1} = \frac{1}{14}(2,-6,0,4),$$
$$l_2 = (0,1,0,-1)A^{-1} = \frac{1}{14}(10,-2,0,6),$$
$$l_3 = (0,0,1,-1)A^{-1} = \frac{1}{14}(8,-10,7,9).$$

Claim: L is generated by $l = l_3$.

In $(\mathbb{Q}/\mathbb{Z})^4$, we have that $2l = \frac{1}{14}(2,-6,0,4) = l_1$, $10l = \frac{1}{14}(10,-2,0,6) = l_2$, which proves the claim.

In this additive group, l clearly has order 14, so let $v_i := i \cdot l$ for $i \in \{1,\ldots,14\}$. v_i has only nonzero elements if i is coprime with 2 and 7 and $\mathrm{ord}(t \cdot v_i) = \mathrm{ord}(v_i)$ only for t coprime to 2 and 7. The following "good" t have the property that $\sum_{j=1}^{4}\{a_{ij}\} = 1$ or 3, were a_{ij} is the j^{th} component of v_i:

n	v_n	t	$\mathrm{ord}(v_n)$	$\sum$
1	$\frac{1}{14}(8,-10,7,9)$	3	14	3
3	$\frac{1}{14}(10,-2,7,13)$	1	14	3
5	$\frac{1}{14}(12,-8,7,3)$	9	14	3
9	$\frac{1}{14}(2,-6,7,11)$	5	14	3
11	$\frac{1}{14}(4,-12,7,1)$	13	14	3
13	$\frac{1}{14}(6,-4,7,5)$	11	14	3

So $\lambda = 6$.

Next, $b_2 = 12n - 2$, with $n = \max(\lceil \frac{\deg(a)}{4} \rceil, \lceil \frac{\deg(b)}{6} \rceil = 2$, so $b_2 = 22$.

Finally, we count the components of bad fibres to determine ρ_{triv} (see [6, p. 13]). $E : y^2 = x^3 + s^3x + s^8$ has discriminant $4s^9 + 27s^{16} = s^9(4 + 27s^7)$, so E has seven fibres of type I_1, which have one component. At $s = 0$, we find a component of type III^*, which has 8 components. Let $w = \frac{1}{s}$ to see that the minimal curve $E : y^2 = x^3 + w^5x + w^4$ has a fibre of type IV^*, which has 7 components, at $w = 0$, or $s = \infty$.

Then $\rho_{\text{triv}} = 2 + 7 + 6 = 15$ and so $r = b_2 - \lambda - \rho_{\text{triv}} = 22 - 6 - 15 = 1$, which finishes the proof. □

Alternatively, we can apply the theorem of Inose (Source [3]): there is a mapping $(x, y, t^{-3}) \mapsto (\xi, \eta, s)$ of $E : y^2 = x^3 + t^7x + 1 \to \underline{E} : \eta^2 = \xi^3 + s^3\xi + s^8$. Both curves are K3, over a field with characteristic 0 ($\overline{\mathbb{Q}}(t^3)$). Applying the theorem of Inose, we see that both have the same Picard number $\rho = 16$. We have determined that the curve $E : \eta^2 = \xi^3 + s^3\xi + s^8$ over $\overline{\mathbb{Q}}(s)$ has $\rho_{\text{triv}} = 15$, so $r = 1$.

7 Appendix Magma Code

In this section, we display the code used to compute the various results given in the thesis.

7.1 Torsion Points

The following code is used to determine $2 \cdot P$, where $P = (0, 1)$ is a candidate torsion point in section 3.2.

```
K<t>:=FunctionField(Rationals());

E:=EllipticCurve([t^7,1]);

P:=E!([0,1]);

P;
2*P;
```

7.2 Equations for the polynomial coefficients

The following code determines what equations the coefficients of the polynomials $x(t)$ and $y(t)$ (as denoted in section 4) must satisfy for the point $P = (x(t), y(t))$ to be on the curve E over $\overline{\mathbb{Q}}(t)$.

```
K<t>:=FunctionField(Rationals());
t:=1;
E:=EllipticCurve([K|t,1]);

R<xi>:=PolynomialRing(K);
A<a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6>:=AffineSpace(K,12);
S:=CoordinateRing(A);
U<t>:=PolynomialRing(S);
x:=a0+a1*t+a2*t^2+a3*t^3+a4*t^4;
y:=b0+b1*t+b2*t^2+b3*t^3+b4*t^4+b5*t^5+b6*t^6;
f:=x^3+t^7*x+1-y^2;
I:=ideal<S | Coefficients(f)>;

B:=Scheme(A,I);
B;
```

7.3 Points on a finite field

The following code determines which pionts exist in $E(\mathbb{F}_p(t))$, in this case for $E : y^2 = x^3 + t^7x + 1$ and $p = 41$.

```
K<t>:=FunctionField(Rationals());
Q:=Rationals();
p:=41;
t:=1;
F:=GF(p);
E:=EllipticCurve([F|t,1]);

R<xi>:=PolynomialRing(F);
A<a0,a1,a2,a3,a4,b0,b1,b2,b3,b4,b5,b6>:=AffineSpace(F,12);
S:=CoordinateRing(A);
U<t>:=PolynomialRing(S);
x:=a0+a1*t+a2*t^2+a3*t^3+a4*t^4;
y:=b0+b1*t+b2*t^2+b3*t^3+b4*t^4+b5*t^5+b6*t^6;
f:=x^3+t^7*x+1-y^2;
I:=ideal<S | Coefficients(f)>;

B:=Scheme(A,I);
Points(B);
```

7.4 Points of height pairing less than 4

The following code determines which points exist in $E(\mathbb{Q}_p(t))$, with height pairing $\langle P, P\rangle < 4$

```
K:=RationalField();
X<x,y,z>:=AffineSpace(K,3);
F:=x^3+z^7*x+1-y^2;
A<a0,a1,a2,a3,b0,b1,b2,b3,b4,b5>:=AffineSpace(K,10);
R<t>:=PolynomialRing(CoordinateRing(A));
pt:=[a0+a1*t+a2*t^2+a3*t^3,
     b0+b1*t+b2*t^2+b3*t^3+b4*t^4+b5*t^5,t];
I:=Ideal(Coefficients(Evaluate(F,pt)));
Z:=Scheme(A,I);
Points(Z);
```

7.5 Code to show that rank$(E/\mathbb{F}_{41}(t)) = 19$

The following code computes that $\Phi_{21}(\sigma(P))\Phi_7(\sigma(P))(1-\sigma(P)) = O$, used in section 4.2. Here `P[21]`$= \sigma^{21}(P) = P$. This is chosen for computational methods.

```
Fq<a>:=GF(41^2);
K<t>:=FunctionField(Fq);
P<x>:=PolynomialRing(K);
Order(a);
z:=a^80; z;
E:=EllipticCurve([t^7,1]);

P:=[];

for i:=1 to 21 do
P[i]:=E![z^(7*i)*(0+(-5)*(z^i*t)+4*(z^i*t)^2+
 7*(z^i*t)^3+(-8)*(z^i*t)^4),1+0*(z^i*t)+
 0*(z^i*t)^2+(-1)*(z^i*t)^3+27*(z^i*t)^4+
 (-1)*(z^i*t)^5+29*(z^i*t)^6];
end for;

-P[21]+P[1]-P[3]+P[4]-P[6]+P[7]-P[9]+P[10]
-P[12]+P[13]-P[15]+P[16]-P[18]+P[19];
```

References

[1] K. Conrad. Hensel's Lemma. 2013. http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/hensel.pdf.

[2] B.L. Heijne. *Elliptic Delsarte Surfaces*. PhD thesis, Rijksuniversiteit Groningen, 2011. http://irs.ub.rug.nl/ppn/339372087.

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

[4] K Kodaira. On compact analytic surfaces ii. *Ann. of Math. (2) 77*, 1963.

[5] Masamichi Kuroda. Q-bases of the Neron-Severi groups of certain elliptic surfaces. 2013. http://arxiv.org/pdf/1307.5650v3.pdf.

[6] M. Schuett and T. Shioda. Elliptic Surfaces. *Adv. Stud. Pure Math., 60,*, 2009.

[7] T. Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul. 39 (1990), no. 2,*, pages 211–240, 2010. http://www2.rikkyo.ac.jp/ shioda/papers/mwl.pdf used in the page references, accessed July 2014.

[8] J.H Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2008.

[9] J. Top. *Groepentheorie*. http://www.math.rug.nl/ top/alg1.pdf.

[10] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 1997.