university of groningen

faculty of mathematics and natural sciences

The rank of elliptic curves of the form $E_{A,B} : y^2 = x^3 + A(x - B)^2$

Lianne van Timmeren

Master thesis mathematics

July 2015

Supervisor: Prof. dr. J. Top

Second reader: Prof. dr. ir. R.W.C.P. Verstappen

Abstract

The rank of a finitely generated abelian group A is by definition the maximal number of independent points in A. Here we are especially interested in the group, $E_{A,B}(\mathbb{Q})$, of rational points on the elliptic curve $E_{A,B}$. Under the special condition that the multiplication by $3 : E_{A,B} \to E_{A,B}$ factors as a product $3 = \phi \circ \psi$, we compute the rank of $E_{A,B}(\mathbb{Q})$. We need to know something about the torsion points of order 3 that are rational. After introducing a map α we can compute the rank. A computer program will be explained for computing the rank of $E_{A,B}$. We will try to make families of elliptic curves with a higher rank.

Contents

Chapter 1

Introduction

In this thesis we are interested in elliptic curves over $\mathbb{Q}$ of the form

$$E_{A,B} : y^2 = x^3 + A\,(x - B)^2\,.$$

The group of rational points on this elliptic curve will be denoted by $E_{A,B}\,(\mathbb{Q})$. The main goal of this thesis is computing the rank of the group $E_{A,B}\,(\mathbb{Q})$.

In [vB10] there was already a good start with the subject of this thesis. Monique van Beek did a lot of research about the necessary theory on computing the rank of the group $E_{A,B}\,(\mathbb{Q})$. When reading the master thesis [vB10] several questions remained about how this exactly works and how to compute the rank of $E_{A,B}\,(\mathbb{Q})$.

The research of this master thesis started with reading thesis [vB10] and understanding the theory explained there. We started with making a few examples computing the rank. It became clear that some aspects of the theory explained in [vB10] could be stated more precisely and computing the rank by hand was really not doable. Moreover, we wanted to make families of elliptic curves that have higher rank. So we had three goals during this thesis:

1. Making the theory of computing the rank of $E_{A,B}\,(\mathbb{Q})$ more precise and more practical.
2. Making a computer program in magma to compute the rank with help of this theory.
3. Finding families of elliptic curves that have higher rank.

In chapter 2 we start with general theory about elliptic curves. First we define elliptic curves in Weierstrass normal form. We recall the group law and explicit formulas for the group law of elliptic curves. After that we will prove an elliptic curve is an abelian group,

then we explain where the special form

$$E_{A,B} : y^2 = x^3 + A\left(x - B\right)^2 \tag{1.1}$$

comes from. After that more theory about rational points of the elliptic curve $E_{A,B}$ will be discussed. In section 2.2 we will state the definition of rank and some theorems about the rank of elliptic curves. To compute the rank of the group $E_{A,B}\left(\mathbb{Q}\right)$ we need some theory about the points of order dividing 3, this will be explained in section 2.3.
In section 2.4 we define two isogenies ϕ and ψ such that $\phi \circ \psi = [3]$ where [3] is the multiplication by 3 map. We use this multiplication map to compute the rank of $E_{A,B}\left(\mathbb{Q}\right)$. In the next section we will define a homomorphism $\alpha : E_{A,B}\left(\mathbb{Q}\right) \to \mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3}$ which is probably the most important homomorphism in this thesis. With help of α we get an explicit formula for the rank.

Chapter 3 starts with some general algebraic number theory. This is needed to prove that the image of α is contained in a certain set Λ. Then we will derive a formula to compute the rank with help of the image of α. After this we will define the set Λ. We will conclude the chapter with a roadmap to compute the rank.

In chapter 4 the computer program made for computing the rank will be explained. The code can be found in appendix A. In chapter 5 some examples will be given. In chapter 6 we will try to make some families of elliptic curves with higher rank.

Chapter 2

Elliptic curves

In this chapter some general theory about elliptic curves will be explained. In the first section the definition of elliptic curves will be treated. Also the group law will be explained. After that we tell something about our choice of working with elliptic curves of the special form $E_{A,B} : y^2 = x^3 + A(x - B)^2$. We treat some theorems about rational points on this curve. In the next section we tell something about the rank of elliptic curves. Before we can do that, we need to know what the order of a point means, this will also be explained. Section 2.3 of this chapter contains theory about points of order 3 on our elliptic curve. The last two sections contain theory about two different maps, the multiplication map and the map α, respectively.

2.1 Definition of elliptic curves

A general cubic equation is given by

$$ax^3 + bx^2y + cxy + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

A point (x, y) satisfying this cubic equation is rational if $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$. Any cubic equation which contains at least one rational point and which has the property that its homogenization

$$ax^3 + bx^2y + cxyz + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + iyz^2 + jz^3$$

defines a smooth cubic curve in $\mathbb{P}^2$ can be transformed into the Weierstrass normal form. In general this equation is given by

$$y^2 = 4x^3 - g_2x - g_3.$$

The above equation can be transformed into a more general form namely

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

We refer to this equation if we are talking about the Weierstrass normal form.

Definition 1. *Elliptic curves are non-singular curves of the form*

$$F : y^2 = f(x) = x^3 + ax^2 + bx + c \tag{2.1}$$

together with a point at infinity $\mathcal{O}$.

The discriminant of this curve is given by

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

The roots on the right hand side of equation 2.1 must be distinct, which means the discriminant cannot be zero. Elliptic curves can be defined over any field K, however F in the form of equation 2.1 does not define a non-singular curve in case $\text{char}(K) = 2$.

Definition 2. *The group law of elliptic curves is defined as follows: Take two points* P *and* Q *on the elliptic curve, draw a line through* P *and* Q*, this line will intersect with the curve on a third point* $-R$*. Draw a vertical line through* $-R$*, this line will again intersect with the curve. The point where it intersects is the point* $R = P + Q$*. See figure 2.1. Be aware that if* $P = (x, y)$ *then* $-P = (x, -y)$*.*

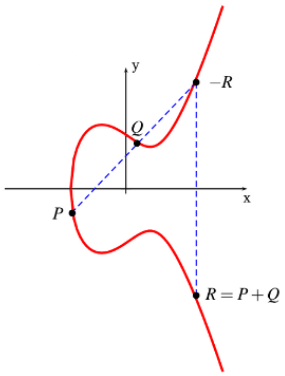

Figure 2.1: Group law elliptic curves

For the next theorem we will use explicit formulas for computing the coordinates of the point $P + Q$ on an elliptic curve. We start with the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_1 + P_2 = (x_3, y_3)$, where $x_1 \neq x_2$. From the group law described above we see we first have to draw a line through P_1 and P_2. So let the equation of this line be $y = \alpha x + \beta$. Then we have $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ and $\beta = y_1 - \alpha x_1 = y_2 - \alpha x_2$. Substituting this in the equation of F, using $y^2 = (\alpha x + \beta)^2$, we get

$$\begin{aligned} (\alpha x + \beta)^2 &= x^3 + ax^2 + bx + c \\ 0 &= x^3 + \left(a - \alpha^2\right) x^2 + (b - 2\alpha\beta)\, x + \left(c - \beta^2\right). \end{aligned}$$

Since this equation has three roots, namely x_1, x_2 and x_3, we have

$$\begin{aligned}
&x^3 + \left(a - \alpha^2\right) x^2 + (b - 2\alpha\beta)\, x + \left(c - \beta^2\right) \\
&= (x - x_1)\,(x - x_2)\,(x - x_3) \\
&= x^3 - (x_1 + x_2 + x_3)\, x^2 + (x_1x_2 + x_1x_3 + x_2x_3) - x_1x_2x_3.
\end{aligned}$$

So we have $\alpha^2 - a = x_1 + x_2 + x_3$. Summarized we get the equations

$$\begin{aligned}
\alpha &= \frac{y_1 - y_2}{x_1 - x_2} \\
\beta &= y_1 - \alpha x_1 \\
x_3 &= \alpha^2 - a - x_1 - x_2 \\
y_3 &= \alpha x_3 + \beta.
\end{aligned}$$

Using this set of equations we can compute the coordinates of $P_1 + P_2 = (x_3, y_3)$ explicitly. If $x_1 = x_2$ and $y_1 = y_2 \neq 0$, the only difference is that $\alpha = \frac{f'(x)}{2y}$.

Theorem 1. *An elliptic curve is an abelian group, consisting of the points given by equation 2.1 and a point $\mathcal{O}$ at "infinity".*

Proof. To prove that an elliptic curve is a commutative group, we have to prove associativity, that a point at infinity exists, that every point has an inverse and that commutativity holds:

- $G1$, associativity: For all $P, Q, R \in F$ we have $(P + Q) + R = P + (Q + R)$. Since this proof is quite lengthy we will not do it here. The proof can be found in [Fri].
- $G2$, point at infinity: For all $P \in F$ we have $P + \mathcal{O} = P = \mathcal{O} + P$. This follows immediately from the definition of the group law on elliptic curves.
- $G3$, inverse: For all $P \in F$ exist a $Q \in F$ such that $P + Q = \mathcal{O} = Q + P$. Since we have to find a point $Q \in F$ such that P and Q lie on a vertical line, we see immediately that this must be the point $Q = -P$. It is easy to see that every point on an elliptic curve has such a point.
- $G4$, commutativity: For all $P, Q \in F$ we have $P + Q = Q + P$. With the formulas given above this property can be checked easily. This is also easy to check geometrically, as can be seen in figure 2.1.

□

This thesis is about the rank of elliptic curves $E_{A,B}$ of the form

$$\begin{aligned}
E_{A,B} : y^2 &= x^3 + A\,(x - B)^2 \\
y^2 &= x^3 + Ax^2 - 2ABx + AB^2,
\end{aligned} \tag{2.2}$$

where A and B are integers. The discriminant then becomes $\Delta = A^2B^3(-4A - 27B)$. Be aware that if A and/or B are not integer, then we can multiply the equation by their denominator(s) and replace the variables x, y to get a new elliptic curve where A, B are integers.

To explain where the form of $E_{A,B}$ comes form, we first need the definition of an isogeny.

Definition 3. *An **isogeny** between two elliptic curves E_1 and E_2 is a morphism that maps $\mathcal{O}_{E_1}$ to $\mathcal{O}_{E_2}$, so*

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

Two elliptic curves are isogenous if there exists an isogeny between E_1 and E_2 such that $\phi(E_1) \neq \{\emptyset\}$.

It is known, see [Sil08], that isogenies are group homomorphism. An important isogeny for this thesis is the multiplication by m map. This will be denoted by $[m]$. In this thesis we are interested in the map [3]. Our goal is to find two isogenies ϕ and ψ that together make the map [3]: $\phi \circ \psi = [3]$.

We start with the elliptic curve F defined over $\mathbb{Q}$. Now we want to define the map [3] and the isogenies ϕ and ψ such that we get figure 2.2.

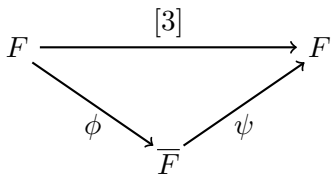

Figure 2.2: The isogenies ϕ and ψ and the map [3].

The isogeny ϕ maps to $\overline{F}$, where $\overline{F}$ is also an elliptic curve defined over $\mathbb{Q}$. Then we have that

$$\text{degree}(\phi) \cdot \text{degree}(\psi) = 9 = \text{degree}([3]).$$

If the degree of ϕ (or ψ) is 1 this isogeny is not interesting. Instead we want both isogenies to have degree 3. We know that the degree(ϕ) = $\ker(\phi)$ where the $\ker(\phi)$ is given by

$$\ker(\phi) = \{P \in F(\mathbb{C}) \mid \phi(P) = \mathcal{O}\}.$$

This gives us a subgroup of order 3, namely $\{P, 2P = -P, \mathcal{O}\}$. Because ϕ is defined over $\mathbb{Q}$ we must have that $\ker(\phi)$ is stable under automorphism. Take the point P in the subgroup as (α, β). We have for all $\sigma \in \text{Aut}(\mathbb{C})$ that

$$\{\sigma(P), \sigma(-P) = -\sigma(P), \sigma(\mathcal{O})\} = \{P, -P, \mathcal{O}\}.$$

So we have $\sigma(P) = \pm P$, and it follows that $\sigma(\alpha) = \alpha$ for all σ. Therefore, we find that $\alpha \in \mathbb{Q}$.

So starting with the equation of $F : y^2 = x^3 + ax^2 + bx + c$ and translating it with $\alpha \in \mathbb{Q}$, so replace x by $x - \alpha$ we get

$$\begin{aligned} y^2 &= (x-\alpha)^3 + a(x-\alpha)^2 + b(x-\alpha) + c \\ &= x^3 - 3\alpha x^3 + 3\alpha^2 x - \alpha^3 + ax^2 - 2a\alpha x + a\alpha^2 + bx - b\alpha + c \\ &= x^3 + (a - 3\alpha)x^2 + \left(3\alpha^2 - 2a\alpha + b\right)x + \left(a\alpha^2 - \alpha^3 - b\alpha + c\right) \\ &= x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c} \end{aligned}$$

with point $\left(0, \sqrt{\tilde{c}}\right)$. Now we want that this point has order 3. We construct a tangent line on F in point P. The equation of the line will be $y = ax + \sqrt{\tilde{c}}$ with

$$a = \left.\frac{dy}{dx}\right|_P = \left.\frac{3x^2 + 2\tilde{a}x + \tilde{b}}{2y}\right|_P = \frac{\tilde{b}}{2\sqrt{\tilde{c}}}.$$

Since the order of P is not equal to 2 we have that $\sqrt{\tilde{c}} \neq 0$, so we can divide by $\sqrt{\tilde{c}}$. Then the tangent line is given by $y = \frac{\tilde{b}}{2\sqrt{\tilde{c}}}x + \sqrt{\tilde{c}}$. Intersecting the tangent line with the elliptic curve gives

$$\frac{\tilde{b}}{4\tilde{c}}x^2 + \tilde{b}x + \tilde{c} = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$$

which has a triple intersection point in $x = 0$ if and only if

$$\tilde{a} = \frac{\tilde{b}}{4\tilde{c}}.$$

This gives two solutions:

1. $\tilde{a} = \tilde{b} = 0$, so $y^2 = x^3 + \tilde{c}$. Indeed $\left(0, \sqrt{\tilde{c}}\right)$ has order 3, but this is not the curve we are interested in in this thesis.

2. $\tilde{a} \neq 0$, then $\tilde{c} = \frac{\tilde{b}^2}{4\tilde{a}}$. The resulting elliptic curve is

$$\begin{aligned} y^2 &= x^3 + \tilde{a}x^2 + \tilde{b}x + \frac{\tilde{b}^2}{4\tilde{a}} \\ &= x^3 + \tilde{a}\left(x^2 + \frac{\tilde{b}}{\tilde{a}} + \frac{\tilde{b}^2}{4\tilde{a}^2}\right) \\ &= x^3 + \tilde{a}\left(x + \frac{\tilde{b}}{2\tilde{a}}\right). \end{aligned}$$

   A change of variables $A := \tilde{a}$ and $B := \frac{-\tilde{b}}{2\tilde{a}}$ gives us the result we wanted: the curve $E_{A,B} : y^2 = x^3 + Ax^2 - 2ABx + AB^2 = x^3 + A(x - B)^2$.

The reader should take note that while in this thesis we derive everything for the elliptic curve $E_{A,B}$ specifically, most of the theorems and definitions used in this thesis are also correct for a general elliptic curve in Weierstrass normal form.

Definition 4. *The set of rational points on $E_{A,B} : y^2 = x^3 + A(x-B)^2$ is given by*

$$E_{A,B}(\mathbb{Q}) := \left\{(x,y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + A(x-B)^2\right\}.$$

In the next section we will see that the group of rational points is a finitely generated abelian group.

Theorem 2. *Any rational point $(x,y) \neq (0,0)$ on the curve 2.1 can be written in the form*

$$(x,y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right).$$

where $m, n, e \in \mathbb{Z}$ and $gcd(m,e) = gcd(n,e) = 1$.

Proof. Since x, y are rational, we can write them as $x = \frac{m}{M}$ and $y = \frac{n}{N}$ where $M, N > 0$ and $\gcd(N,n) = \gcd(M,m) = 1$. Substituting this in the equation of $E_{A,B}$ we get

$$\begin{aligned}
y^2 &= x^3 + A(x-B)^2 \\
\frac{n^2}{N^2} &= \frac{m^3}{M^3} + A\left(\frac{m}{M} - B\right)^2 \\
\frac{n^2}{N^2} &= \frac{m^3}{M^3} + A\frac{m^2}{M^2} - 2AB\frac{m}{M} + AB^2 \\
M^3n^2 &= m^3N^2 + Am^2MN^2 - 2ABmM^2N^2 + AB^2M^3N^2 \quad (*).
\end{aligned}$$

Now we want to show that $M^3 = N^2$, so we have to show $M^3|N^2$ and $N^2|M^3$.

1. The right hand side of the last equation $(*)$ contains in each term N^2 so we have: $N^2|M^3n^2$, and since we have $\gcd(N,n) = 1$ we have $N^2|M^3$.

2. From $(*)$ we have that $M|m^3N^2$, since $\gcd(M,m) = 1$ we have $M|N^2$. Using this back in $(*)$ we have $M^2|N^2m^3$ so $M^2|N^2$ and $M|N$ and again using this back in $(*)$ we have $M^3|N^2m^3$ so $M^3|N^2$.

So now we have proven that $M^3 = N^2$ and shown $M|N$, let $e = \frac{N}{M}$. Then we have:

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M, \; e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N,$$

from which we have the required result

$$(x,y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right),$$

where $m, n, e \in \mathbb{Z}$ and $\gcd(m,e) = \gcd(n,e) = 1$.

□

2.2 Rank of an elliptic curve

Definition 5. *The **order** of a point P of an elliptic curve is the smallest positive integer m, satisfying:*

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ times}} = \mathcal{O}.$$

If no such m exists, we say P has order infinity.

Definition 6. *A **torsion point** is a point with finite order.*

In this thesis we are especially interested in the rank of the elliptic curve $E_{A,B}$.

Definition 7. *The **rank** of an elliptic curve is the maximal number of independent rational points on $E_{A,B}$.*

So for our research about the rank of the elliptic curve $E_{A,B}$ we first need to know all the rational points of $E_{A,B}$. Then we need to check whether they have infinite order or not. To say something about the rank of $E_{A,B}$ we make use of the Mordell's theorem.

Theorem 3. ***Mordell's theorem*** *The group of rational points $E_{A,B}(\mathbb{Q})$ on the elliptic curve $E_{A,B} : y^2 = x^3 + A(x-B)^2$ is a finitely generated abelian group isomorphic to $\mathbb{Z}^r \oplus E_{A,B}(\mathbb{Q})_{tors}$, where $E_{A,B}(\mathbb{Q})_{tors}$ is finite.*

- *r is the rank of the elliptic curve.*
- *$E_{A,B}(\mathbb{Q})_{tors} = \{P \in E_{A,B}(\mathbb{Q}) \mid P \text{ has finite order}\}$.*

Proof. We refer to [vB10] for the proof, since it is derived there explicitly for the same elliptic curve we are discussing. □

There is one more important theorem regarding to points of finite order. We will not use it directly in this thesis, but since we want to set out the complete theory about the order of a point on the elliptic curve $E_{A,B}$ we do mention this theorem. One can use it to compute $E_{A,B}(\mathbb{Q})_{\text{tors}}$.

Theorem 4. ***Nagell-Lutz theorem*** *If $P = (x, y) \in E_{A,B}(\mathbb{Q})$ is a torsion point, then $x, y \in \mathbb{Z}$ and either $y = 0$ (then P has order 2) or $y^2 | \Delta$.*

Proof. The proof can be found in [ST92]. □

This theorem can sometimes be used to prove that a point P has infinite order. Namely compute $2P, 3P, \cdots$ until you get a point nP with coordinates that are not integers. Then you know that nP, and hence P, are of infinite order.

2.3 Points of order 3

Furthermore, we need some theory about the points of order dividing 3 on the elliptic curve 2.2. This can also be found in [ST92] and in [vB10]. Since this is also very important for computing the rank of the elliptic curve $E_{A,B}$, we will set out the theory in this thesis.
We will first derive the theory for the elliptic curve $E_{A,B}$ over a general field. After we have derived the possible points, we will look if they can be rational.

For points to have order 3 we need to have points P on $E_{A,B}$ such that $3P = \mathcal{O}$. To make it slightly easier we look at the points that satisfy $2P = -P$. With use of the group law of elliptic curves we immediately see that $x(2P) = x(-P) = x(P)$. So the points of order 3 satisfy $x(2P) = \pm x(P)$. If we use the group law of elliptic curves in the Weierstrass form $y^2 = x^3 + ax^2 + bx + c$ we can find an explicit formula for the $x-$coordinate of $2P$, namely:

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

If we set this equal to x and do some algebra then we get the following theorem.

Theorem 5. *A point $P = (x, y)$ of the elliptic curve $E_{A,B} : y^2 = x^3 + A(x - B)^2$ has order three if and only if x is a root of the polynomial*

$$g(x) = 3x^4 + 4Ax^3 - 12ABx^2 + 12AB^2x.$$

Proof. The proof is almost worked out in the text above, and can be found by doing some algebra. □

To continue our question: "How many points of order dividing 3 are on the elliptic curve 2.2?" we see from [ST92] that the polynomial of theorem 5 has 4 distinct roots. So we get 8 different points of order 3 on our elliptic curve $E_{A,B}$, namely the 4 roots with positive and the 4 roots with negative $y-$value. Together with the point infinity, which is the only point with order 1 and so the only point with order dividing 3, this gives us in total 9 points of order dividing 3.
It is important for us to know how many of the points of order dividing 3 can be rational and therefore are in $E_{A,B}(\mathbb{Q})$. We notice that there is only one abelian group with nine elements that all have order dividing 3: the product of two cyclic groups of order three, so we see that only 1, 3 or 9 points can be rational.

We immediately see that 1 and 3 points can be rational and order dividing 3, for example

$$\begin{aligned}
&E_{2,1} : y^2 = x^3 + 2\left(x-1\right)^2 \\
&E_{2,1}\left(\mathbb{Q}\right)_{\text{tors}} = \left\{\mathcal{O}\right\}, \\
&E_{1,1} : y^2 = x^3 + \left(x-1\right)^2 \\
&E_{1,1}\left(\mathbb{Q}\right)_{\text{tors}} = \left\{\mathcal{O}, \left(0,1\right), \left(0,-1\right)\right\}.
\end{aligned}$$

These are the only possibilities as we shall prove now. To prove this, we first need the definition of an inflection point on an elliptic curve.

Definition 8. *A nonsingular point P on an elliptic curve is a point of inflection if the tangent line through P has an intersection multiplicity ≥ 3 with $E_{A,B}$ at P.*

Lemma 1. *A point $P \neq \mathcal{O}$ at $E_{A,B}$ is an inflection point if and only if it is of order 3.*

Proof. Let $P \neq \mathcal{O}$ be a point of order 3 on the elliptic curve $E_{A,B}$. Now take the tangent line L through P and call the point of intersection with the elliptic curve Q. Now $P + P = 2P = -Q$. Now take the line through $2P = -Q$ and P. Since P is a third order point we must have that the line through P and Q intersects at $\mathcal{O}$, meaning the line has to be vertical. This means that we have $P = Q$. Now we see that the line L has an intersection multiplicity of 3 with $E_{A,B}$ at P. Therefore, P must be a point of inflection on the elliptic curve $E_{A,B}$. □

Theorem 6. ***Möbius theorem.*** *The graph $y = \sqrt{x^3 + Ax^2 - 2ABx + AB^2}$ contains exactly one point of inflection if $x^3 + Ax^2 - 2ABx + AB^2$ has only simple zeros.*

Proof. Recall that for a twice differentiable function, an inflection point is a point where the graph of the second derivative changes sign. To make the proof slightly easier, we will proof it in general and look at the equation $y = \sqrt{x^3 + ax^2 + bx + c} = \sqrt{f\left(x\right)}$. If we can prove it for this case, then substitute $a = A, b = -2AB$ and $c = AB^2$, we have the result in this special case. The first derivative is

$$\frac{dy}{dx} = \frac{1}{2} f^{-\frac{1}{2}} \cdot \left(3x^2 + 2ax + b\right).$$

And the second derivative

$$\begin{aligned}
\frac{d^2y}{dx^2} &= -\frac{1}{4} f^{-\frac{3}{2}} \cdot \left(3x^2 + 2ax + b\right)^2 + \frac{1}{2} f^{-\frac{1}{2}} \cdot \left(6x + 2a\right) \\
&= -\frac{1}{4} f^{-\frac{3}{2}} \cdot \left(f'\right)^2 + \frac{1}{2} f^{-\frac{1}{2}} \cdot \left(6x + 2a\right) \\
&= -\frac{1}{4} f^{-\frac{3}{2}} \left(\left(f'\right)^2 - 2 \cdot f \cdot f''\right) \\
&= \frac{2f \cdot f'' - \left(f'\right)^2}{4y \cdot f} = \frac{F\left(x\right)}{4y \cdot f}.
\end{aligned}$$

If we differentiate $F(x) = 2f \cdot f'' - \left(f'\right)^2$ we get $F'(x) = 2f' \cdot f'' + 12f - 2f' \cdot f'' = 12f$. So we have $F(x) = 3x^4 + \textit{lower order terms}$ and $\lim_{x\to\pm\infty} = +\infty$. The local extrema of $F(x)$ are at point(s) α with $f(\alpha) = 0$. At these points we have $F(\alpha) = -f(\alpha)^2$. Suppose $f(x)$ only has simple zeros, then $f(x)$ and $f'(x)$ have no zero in common, so $F(\alpha) < 0$. So it follows that $F(x)$ has exactly two zeros. In our case we have $f(x) > 0$, so we have only one zero and therefore one point of inflection. □

Recalling the equation of $E_{A,B}$ to be:

$$\begin{aligned} E_{A,B} : y^2 &= x^3 + A(x-B)^2 \\ &= x^3 + Ax^2 - 2ABx + AB^2 \end{aligned}$$

we see that $E_{A,B}$ consist of two parts,

$$\begin{aligned} y &= \sqrt{x^3 + Ax^2 - 2ABx + AB^2} \\ y &= -\sqrt{x^3 + Ax^2 - 2ABx + AB^2}. \end{aligned}$$

By Möbius' theorem we have that each of these two parts has exactly one point of inflection and by lemma 1 we see we have at most two real points of order 3 on $E_{A,B}$. Since a rational point is real, we have at most two rational points of order 3. With $\mathcal{O}$ included we have at most three rational points of order dividing 3.

For now it is important to determine when $E_{A,B}(\mathbb{Q})$ can contain those two points of order 3. By theorem 5 we have that the $x-$coordinate of a point of order 3 must be a zero of $g(x) = 3x^4 + 4Ax^3 - 12ABx^2 + 12AB^2x$.

One obvious solution for this equation is of course $x = 0$. Therefore we have that the point $(0, y)$ is a point on $E_{A,B}$

$$y^2 = 0^3 + A(0-B)^2 = AB^2.$$

In order to obtain a rational solution we must have that $A = a^2$, for some $a \in \mathbb{Q}$. If A is of this form then we always have 2 points of order 3 in $E_{A,B}(\mathbb{Q})$.

Now we have to look for solutions of $g(x) = 3x^4 + 4Ax^3 - 12ABx^2 + 12AB^2x$ where $x \neq 0$. So we have to solve $3x^3 + 4Ax^2 - 12ABx + 12AB^2 = 0$. If we multiply the equation of $E_{A,B}$ by 3 we get: $3y^2 = 3x^3 + 3A(x-B)^2$. Subtracting these two equations from each other results in:

$$\begin{aligned} 3y^2 &= 3x^3 + 3A(x-B)^2 - 3x^3 - 4Ax^2 + 12ABx - 12AB^2 \\ &= 3x^3 + 3Ax^2 - 6ABx + 3AB^2 - 3x^3 - 4Ax^2 + 12ABx - 12AB^2 \\ &= -Ax^2 + 6ABx - 9AB^2 \\ &= -A(x-3B)^2. \end{aligned}$$

Since $y \neq 0$, this implies $A = -3a^2$ for some $a \in \mathbb{Q}$. If we put $A = -3a^2$ in the equation of $g(x)$ and solve it algebraically (with help of a computer program) for x we get two solutions that can be rational, one is the obvious soltuion $x = 0$ and the other is

$$x = \frac{2}{3}\left(8a^6 - 18Ba^4\right)^{\frac{1}{3}} - \frac{3}{2} \cdot \frac{4Ba^2 - \frac{16}{9}a^4}{\left(8a^6 - 18Ba^4\right)^{\frac{1}{3}}} + \frac{4}{3}a^2.$$

From the above solution for x we see that $8a^6 - 18Ba^4$ has to be a third power to let x be a rational solution. So $8a^6 - 18Ba^4 = a^3\left(8a^3 - 18Ba\right) = m^3$ for a certain $m \in \mathbb{Q}$, $m > 0$. Therefore, we see that we can only have rational points of order dividing 3 if $A = a^2$, $a \in \mathbb{Q}$ or $A = -3a^2$ and $8a^3 - 18Ba = m^3$ for $a, m \in \mathbb{Q}, m > 0$.

Definition 9. $E_{A,B}(\mathbb{Q})[3] = \{$*points of order dividing 3 in* $E_{A,B}(\mathbb{Q})\}$

We have:

$$\#E_{A,B}(\mathbb{Q})[3] = \begin{cases} 3 & \text{if } A = a^2 \text{ or } A = -3a^2 \text{ and } 8a^3 - 18Ba = m^3 \\ & \text{for some } a, m \in \mathbb{Q}, m > 0 \\ 1 & \text{otherwise.} \end{cases}$$

2.4 The multiplication map

In section 2.1 we saw that we used two isogenies and the multiplication by 3 map to get the special form of $E_{A,B}$. Since this is the way $E_{A,B}$ is constructed, we know those isogenies exists. So again we have the isogenies ϕ, ψ and the multiplication by 3 map as in figure 2.3.

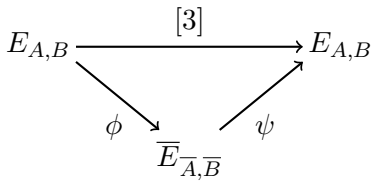

Figure 2.3: The isogenies ϕ and ψ and the map [3].

Here ϕ and ψ are given by:

$$\phi : E_{A,B} \to \overline{E}_{\overline{A},\overline{B}}$$
$$\psi : \overline{E}_{\overline{A},\overline{B}} \to E_{A,B}.$$

From [Top91] we see the elliptic curves $E_{A,B}$ and $\overline{E}_{\overline{A},\overline{B}}$ are given by the equations

$$\begin{aligned} E_{A,B} &: y^2 = x^3 + A\left(x - B\right)^2 \\ \overline{E}_{\overline{A},\overline{B}} &: \eta^2 = \xi^3 + \overline{A}\left(\xi - \overline{B}\right)^2, \end{aligned}$$

where $\overline{A} = -27A$ and $\overline{B} = 4A + 27B$. The two isogenies are defined as follows

$$\phi : E_{A,B} \to \overline{E}_{\overline{A},\overline{B}}, \qquad \phi\left(x, y\right) = \left(\xi, \eta\right)$$

where

$$\begin{aligned} \xi &= \frac{9}{x^2}\left(2y^2 + 2AB^2 - x^3 - \frac{2}{3}Ax^2\right) \\ \eta &= \frac{27y}{x^3}\left(-4ABx + 8AB^2 - x^3\right) \end{aligned}$$

and ψ we split by two maps, namely σ and τ, such that $\psi = \tau \circ \sigma$, where σ is given by

$$\sigma : \overline{E}_{\overline{A},\overline{B}} \to \overline{\overline{E}}_{\overline{\overline{A}},\overline{\overline{B}}}, \qquad \sigma\left(\xi, \eta\right) = \left(x, y\right)$$

where

$$\begin{aligned} x &= \frac{9}{\xi^2}\left(2\eta^2 + 2\overline{AB}^2 - \xi^3 - \frac{2}{3}\overline{A}\xi^2\right) \\ y &= \frac{27\eta}{\xi^3}\left(-4\overline{AB}\xi + 8\overline{AB}^2 - \xi^3\right) \end{aligned}$$

and $\tau : \overline{\overline{E}}_{\overline{\overline{A}},\overline{\overline{B}}} \to E_{A,B}$ is given by replacing y by 3^9y and x by 3^6x and divide the equation by 3^{18}.

If we start with the elliptic curve $E_{A,B}$ and first apply ϕ followed by σ, then we get the resulting elliptic curve $\overline{\overline{E}}_{\overline{\overline{A}},\overline{\overline{B}}} : y^2 = x^3 + 3^6A\left(x - 3^6B\right)^2$. If we replace y by 3^9y and x by 3^6x and divide the equation by 3^{18} then we get our original elliptic curve $E_{A,B}$ back. Thus we see that the group of rational points of $\overline{\overline{E}}_{\overline{\overline{A}},\overline{\overline{B}}}$ is isomorphic to the group of rational points of $E_{A,B}$.

2.5 The map α

To determine the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A\left(x - B\right)^2$ we need to make use of a homomorphism α. Therefore we need to rewrite the equation of $E_{A,B}$:

$$\begin{aligned} x^3 &= y^2 - A\left(x - B\right)^2 \\ &= \left(y + \left(x - B\right)\sqrt{A}\right)\left(y - \left(x - B\right)\sqrt{A}\right). \end{aligned}$$

The map α is defined as follows

$$\alpha : E_{A,B}(\mathbb{Q}) \to \mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3} \tag{2.3}$$

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} & \text{if } P = \mathcal{O} \\ \left(y + (x - B)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} & \text{if } P = (x, y) \in E_{A,B}(\mathbb{Q}) \end{cases}$$

This map α is well-defined if $\left(y + (x - B)\sqrt{A}\right) \neq 0$. This is not the case when $A = a^2$. There are two special points in this case, namely $P = (0, \pm aB)$. We define the image of α for these points separately:

$$\alpha(0, aB) = \frac{1}{2aB} \cdot \mathbb{Q}^{*3}$$
$$\alpha(0, -aB) = 2aB \cdot \mathbb{Q}^{*3}.$$

Since proving that α is a homomorphism is quite lengthy and does not contain any useful theory for this thesis we will not discuss it here. For the interested reader, the complete proof can be found in [vB10] and in a more abstract way in [Top91].

Chapter 3

Computing the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A(x - B)^2$

Although most of this chapters content can be found in [vB10] we will repeat it here for three reasons. First, this chapter is probably the most important for determining the rank of an elliptic curve $E_{A,B}$ of the form: $E_{A,B} : y^2 = x^3 + A(x - B)^2$. Secondly the notation will be slightly different from [vB10], hoping to clarify the theory. At last we will make a roadmap to explain how exactly the rank can be computed, this was not done in [vB10]. In chapter 4 a computer program is made with theory of this chapter.

3.1 Algebraic number theory

Before we can compute the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A(x - B)^2$ we recall some algebraic number theory. This will be stated in this section. The reader who is familiar with algebraic number theory can skip this section.

Write $A = D \cdot n^2$, with $D \in \mathbb{Z}$ square free. In this thesis we work with the quadratic extension of the number field $\mathbb{Q}$, the number field $\mathbb{Q}\left(\sqrt{D}\right) := \left\{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\right\}$. Inside the number field $\mathbb{Q}\left(\sqrt{D}\right)$ we havethe ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, given by

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}\left[\sqrt{D}\right] & \text{if } D \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \mod 4. \end{cases}$$

The following important theorem holds.

Theorem 7. *The ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a Dedekind domain.*

Proof. Since the proof doesn't add anything to this thesis, it will not be included here. The proof can be found in [Ste04]. □

An important property of a Dedekind domain is that every ideal can be written as a unique product of prime ideals. So in the ring of integers of $\mathbb{Q}\left(\sqrt{D}\right)$ we have unique ideal factorization.

Furthermore we need the definition of a prime ideal to be inert, split or ramified. This theory can also be found in [Cha00]. Since we are only working in the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ we will define this only for this number field. So start with $\mathbb{Q}\left(\sqrt{D}\right)$ where $D \not\equiv 1 \mod 4$. Then the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}\left[\sqrt{D}\right]$, where $\sqrt{D}$ has minimum polynomial $X^2 - D$. Given a prime number $p \in \mathbb{Z}$, we have three different cases regarding to the prime ideal factorization of (p):

- **split** primes: The factorization of $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is $P_1 \cdot P_2$ with P_1, P_2 different.
- **inert** primes: $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is prime by itself.
- **ramified** primes: The factorization of $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is P_1^2.

For the units of the ring of integers we make use of the Dirichlet unit theorem. We will only use the Dirichlet unit theorem in the case $\mathbb{Z}\left[\sqrt{D}\right]$, D nonsquare. The complete theoreom can be found in [Ste].

Theorem 8. ***Dirichlet unit theorem, special case.***
$\mathbb{Z}\left[\sqrt{D}\right]$, D nonsquare:

- *$D < 0$: two units, namely $\{\pm 1\}$, $D \neq -1$, $D \neq -3$.*
- *$D > 1$: the units are generated by -1 and a fundamental unit, which has infinity order.*

Finally we recall the definition of the class group.

Definition 10. *The **class group**, Cl, of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ exists of the equivalence classes of ideals not equal to zero, for the equivalence relation we have: $J_1 \sim J_2$ if $\exists a, b \neq 0 \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, such that $aJ_1 = bJ_2$. This is a group with multiplication: $[J_1] \cdot [J_2] = [J_1 J_2]$.*

3.2 Formula for the rank

In chapter 2 we derived the homomorphism α and explained about the isogeny [3]. Recall the isogeny $\phi : E_{A,B} \to \overline{E}_{\overline{A},\overline{B}}$.

$$\phi : E_{A,B} \to \overline{E}_{\overline{A},\overline{B}}, \qquad \phi(x, y) = (\xi, \eta),$$

where

$$\xi = \frac{9}{x^2}\left(2y^2 + 2AB^2 - x^3 - \frac{2}{3}Ax^2\right)$$
$$\eta = \frac{27y}{x^3}\left(-4ABx + 8AB^2 - x^3\right).$$

Together with the isogeny $\psi : \overline{E}_{\overline{A},\overline{B}} \to E_{A,B}$, which is defined in a similar way, we have $\phi \circ \psi = [3]$.

With some knowledge we can derive a formula to compute the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A\left(x - B\right)^2$. Since this theory is exactly the same as in [vB10] we will not derive it again completely, but we will state the most important formulas.
From [vB10] we see that

$$E_{A,B}\left(\mathbb{Q}\right) \cong \mathbb{Z}^r \oplus \left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right) \oplus \ldots \oplus \left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right),$$

where r is the rank of the elliptic curve. Now we have

$$3E_{A,B}\left(\mathbb{Q}\right) \cong 3\mathbb{Z}^r \oplus 3\left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right) \oplus \ldots \oplus 3\left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right).$$

Now it follows

$$\frac{E_{A,B}\left(\mathbb{Q}\right)}{3E_{A,B}\left(\mathbb{Q}\right)} \cong \frac{\mathbb{Z}}{3\mathbb{Z}}^r \oplus \frac{\left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right)}{3\left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z}\right)} \oplus \ldots \oplus \frac{\left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right)}{3\left(\mathbb{Z}/p_s^{\nu_s}\mathbb{Z}\right)},$$

where

$$\frac{\left(\mathbb{Z}/p_j^{\nu_j}\mathbb{Z}\right)}{3\left(\mathbb{Z}/p_j^{\nu_j}\mathbb{Z}\right)} \cong \begin{cases} \mathbb{Z}/3\mathbb{Z} & \text{if } p_j = 3 \\ 0 & \text{if } p_j \neq 3. \end{cases}$$

So we have

$$\left[E_{A,B}\left(\mathbb{Q}\right) : 3E_{A,B}\left(\mathbb{Q}\right)\right] = 3^{r+\text{number of } j \text{ with } p_j=3}.$$

Recall $E\left(\mathbb{Q}\right)[3] = \{\text{points of order dividing 3 in } E_{A,B}\left(\mathbb{Q}\right)\}$. From [vB10] we see

$$\#E\left(\mathbb{Q}\right)[3] = 3^{\text{number of } j \text{ with } p_j=3}.$$

Now we find an important formula for determining the rank of the curve $E_{A,B}$:

$$3^r = \frac{\left[E_{A,B}\left(\mathbb{Q}\right) : 3E_{A,B}\left(\mathbb{Q}\right)\right]}{\#E_{A,B}\left(\mathbb{Q}\right)[3]}.$$

Here comes the point where we will use the isogenies ϕ and ψ. We rewrite

$$\left[E_{A,B}\left(\mathbb{Q}\right) : 3E_{A,B}\left(\mathbb{Q}\right)\right] = \left[E_{A,B}\left(\mathbb{Q}\right) : \psi \circ \phi\left(E_{A,B}\left(\mathbb{Q}\right)\right)\right].$$

Denote $\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})$ as the group of rational points on $\overline{E}_{\overline{A},\overline{B}}$. We have

$$3E_{A,B}(\mathbb{Q}) \subseteq \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) \subseteq E_{A,B}(\mathbb{Q}).$$

So we find

$$[E_{A,B}(\mathbb{Q}) : 3E_{A,B}(\mathbb{Q})] = \left[E_{A,B}(\mathbb{Q}) : \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)\right] \cdot \left[\psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) : \psi \circ \phi\left(E_{A,B}(\mathbb{Q})\right)\right].$$

From elementary group theory we find (the derivation can be found in [vB10]):

$$[E_{A,B}(\mathbb{Q}) : 3E_{A,B}(\mathbb{Q})] = \left[E_{A,B}(\mathbb{Q}) : \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)\right] \cdot \frac{\left[\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q}) : \phi\left(E_{A,B}(\mathbb{Q})\right)\right]}{\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right]}.$$

So in total we get:

$$3^r = \frac{\left[E_{A,B}(\mathbb{Q}) : \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)\right] \cdot \left[\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q}) : \phi\left(E_{A,B}(\mathbb{Q})\right)\right]}{\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right] \cdot \#E_{A,B}(\mathbb{Q})[3]}.$$

Now it is time to simplify the numerator and denominator. We start with the numerator. Recall the map α to be:

$$\alpha : E_{A,B}(\mathbb{Q}) \to \mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3}$$

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} & \text{if } P = \mathcal{O} \\ \left(y + (x - B)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} & \text{if } P = (x, y) \in E_{A,B}(\mathbb{Q}). \end{cases}$$

We have a simular map for $\overline{E}_{\overline{A},\overline{B}}$, called $\overline{\alpha}$:

$$\overline{E}_{\overline{A},\overline{B}} : y^2 = x^3 + \overline{A}\left(x - \overline{B}\right)^2$$
$$\overline{\alpha}(x, y) = \left(y + \left(x - \overline{B}\right)\sqrt{\overline{A}}\right) \cdot \mathbb{Q}\left(\sqrt{\overline{A}}\right)^{*3}$$

with $\overline{A} = -27A$ and $\overline{B} = 4A + 27B$.

Lemma 2. *ker*$(\overline{\alpha}) = \phi\left(E_{A,B}(\mathbb{Q})\right)$.

Proof. The proof can be found in [vB10]. □

From this it follows that

$$\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) \cong \frac{\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})}{\ker(\overline{\alpha})} \cong \frac{\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})}{\phi\left(E_{A,B}(\mathbb{Q})\right)}$$

and now we have the result

$$\left[\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q}) : \phi\left(E_{A,B}(\mathbb{Q})\right)\right] = \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right).$$

In the simular way we have $\ker(\alpha) = \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)$, so we find $\left[E_{A,B}(\mathbb{Q}) : \psi\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)\right] = \#\alpha\left(E_{A,B}(\mathbb{Q})\right)$. Hence we have simplified the numerator.

$$3^r = \frac{\#\alpha\left(E_{A,B}(\mathbb{Q})\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right)}{\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right] \cdot \#E_{A,B}(\mathbb{Q})[3]}.$$

Lets start now with the denominator. From chapter 2 we know everything about the number of points of order dividing 3, namely:

$$\#E_{A,B}(\mathbb{Q})[3] = \begin{cases} 3 & \text{if } A = a^2 \text{ or } A = -3a^2 \text{ and } 8a^3 - 18Ba = m^3 \text{ for some } a, m \in \mathbb{Q} \\ 1 & \text{otherwise.} \end{cases}$$

So the term we are left with is $\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right]$. So our question is of what elements does $\ker(\psi)$ consists. So which elements of $\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})$ are mapped to $\mathcal{O}$ by ψ. For certain we have $\psi\left(\overline{\mathcal{O}}\right) = \mathcal{O}$. So we only have to look at non-trivial points in $\ker(\psi)$. From the map ψ we see that if $\xi \neq 0$ then $(\xi, \eta) \notin \ker(\psi)$. Furthermore the point $(0,0)$ is never an element of $\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})$. So we are left with the points $(0,\eta), \eta \neq 0$. Such a point is only a point of $\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})$ if it satisfies $\eta^2 = \xi^3 + \overline{A}\left(\xi - \overline{B}\right)^2$. Hence we must have $\eta^2 = \overline{A} \cdot \overline{B}^2$, so $\overline{A}$ has to be a perfect square. Since $\overline{A} = -27A$ we must have $A = -3a^2$ for some $a \in \mathbb{Z}$. So

$$\#\ker(\psi) = \begin{cases} 3 & \text{if } A = -3a^2 \\ 1 & \text{otherwise.} \end{cases}$$

So the term $\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right]$ disappears if $A \neq -3a^2$. Because $\phi \circ \psi = [3]$, the only elements of order dividing 3 are sent by ϕ to $\ker(\psi)$. Following [vB10] we see in total:

$$\left[\ker(\psi) : \ker(\psi) \cap \phi\left(E_{A,B}(\mathbb{Q})\right)\right] = \begin{cases} 3 & \text{if } A = -3a^2 \\ & \text{and } E_{A,B}(\mathbb{Q}) \text{ contains no points of order 3} \\ 1 & \text{otherwise.} \end{cases}$$

Combining all the formulas we derived in this section we have a formula for the rank as follows:

$$3^r = \begin{cases} \frac{1}{3} \cdot \#\alpha\left(E_{A,B}(\mathbb{Q})\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) & \text{if } A = -3a^2 \text{ or } A = a^2 \\ \#\alpha\left(E_{A,B}(\mathbb{Q})\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) & \text{otherwise.} \end{cases} \tag{3.1}$$

3.3 Image of α

From the previous chapter we have derived a formula for the rank, namely

$$3^r = \begin{cases} \frac{1}{3} \cdot \#\alpha\left(E_{A,B}(\mathbb{Q})\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) & \text{if } A = -3a^2 \text{ or } A = a^2 \\ \#\alpha\left(E_{A,B}(\mathbb{Q})\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}(\mathbb{Q})\right) & \text{otherwise.} \end{cases}$$

So for now it is important to determine $\#\alpha\left(E_{A,B}\left(\mathbb{Q}\right)\right)$ and $\#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}\left(\mathbb{Q}\right)\right)$. We will do this for the cases where $A \neq -3a^2$ or $A \neq a^2$. Remember the image of α to be

$$\alpha : E_{A,B}\left(\mathbb{Q}\right) \to \mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3}.$$

Define three sets as follows, these sets are fixed for fixed A and B:

$$\begin{aligned}
Q_{A,B} &:= \{Q_1, \ldots, Q_m \subset \mathcal{O}_K \mid Q_i \text{ prime ideals}, Q_i \text{ nonprincipal ramified prime}, A \in Q_i\}, \\
R_{A,B} &:= \{R_1, \ldots, R_t \subset \mathcal{O}_K \mid \ R_i \text{ prime ideals}, R_i \text{ split prime}, AB \in R_i\}, \\
P_{A,B} &:= \{P_1, \ldots, P_n \subset \mathcal{O}_K \mid \ P_i \text{ together with the primes in } Q_{A,B} \text{ generate } Cl\}.
\end{aligned}$$

Theorem 9.

$$\begin{aligned}
\alpha\left(E_{A,B}\left(\mathbb{Q}\right)\right) \subset \Bigg\{ & \beta\mathbb{Q}\left(\sqrt{A}\right)^{*3} \mid \beta \neq 0, \ \beta \in \mathcal{O}_K \text{ and} \\
& \beta\mathcal{O}_K = P_1^{3\epsilon_1} \cdots P_n^{3\epsilon_n} \cdot Q_1^{3\delta_1} \cdots Q_m^{3\delta_m} \cdot R_1^{\gamma_1} \cdots R_t^{\gamma_t} \Bigg\}
\end{aligned}$$

where $P_j \in P_{A,B}$, $Q_i \in Q_{A,B}$ and $R_k \in R_{A,B}$, $\epsilon_j, \delta_i, \gamma_k \in \mathbb{Z}_{\geq 0}$, $\epsilon_j <$ the order of P_j, $\delta_i <$ the order of Q_i and $\gamma_k <$ 3 times the order of R_k .

Proof. We start with the elliptic curve:

$$E_{A,B} : y^2 = x^3 + A\left(x - B\right)^2. \tag{3.2}$$

Like we stated before any rational point of on the curve 3.2 can be written in the form

$$(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right),$$

where $m, n, e \in \mathbb{Z}$ and $\gcd(m, e) = \gcd(n, e) = 1$. We substitute this into the equation 3.2 and find:

$$\begin{aligned}
\left(\frac{n}{e^3}\right)^2 &= \left(\frac{m}{e^2}\right)^3 + A\left(\frac{m}{e^2} - B\right)^2 \\
&= \left(\frac{m}{e^2}\right)^3 + A\left(\frac{m}{e^2}\right)^2 - 2A\frac{m}{e^2}B + AB^2 \\
n^2 &= m^3 + Am^2e^2 - 2AmBe^4 + AB^2e^6.
\end{aligned}$$

This can be factorized into:

$$m^3 = \left(n + \left(me - Be^3\right)\sqrt{A}\right)\left(n - \left(me - Be^3\right)\sqrt{A}\right) = \beta \cdot \overline{\beta}$$

and the map α becomes

$$\begin{aligned}
\alpha\left(\frac{m}{e^2}, \frac{n}{e^3}\right) &= \left(\frac{n}{e^3} + \left(\frac{m}{e^2} - B\right)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} \\
&= \left(n + \left(me - Be^3\right)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} \\
&= \beta \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3}.
\end{aligned}$$

Now we have three important facts about β:

1. $\beta \cdot \overline{\beta} = m^3 \neq 0$
2. $\beta \in \mathcal{O}_K$
3. $\gcd(m, e) = \gcd(n, e) = 1$.

Since the ring of integers of $\mathbb{Q}\left(\sqrt{A}\right)$ is a Dedekind domain we have unique prime ideal factorization.

So we can make a prime ideal factorization of β. This can exsist of 3 different kind of ideals, namely: inert ideals, ramified ideals, and split ideals. So we have:

$$\begin{aligned}\beta\mathcal{O}_K &= V_1^{\zeta_1} \cdots V_u^{\zeta_u} \\ &= V_1^{\zeta_1} \cdots V_i^{\zeta_i} \cdot V_{i+1}^{\zeta_{i+1}} \cdots V_j^{\zeta_j} \cdot V_{j+1}^{\zeta_{j+1}} \cdots V_u^{\zeta_u},\end{aligned}$$

where $V_1 \cdots V_i$ the inert ideals, $V_{i+1} \cdots V_j$ the ramified ideals and $V_{j+1} \cdots V_u$ the split ideals.

The norm of β must be divisible by 3, so we must have:

$$|N(\beta)| = v_1^{3\zeta_1} \cdots v_i^{3\zeta_i} \cdot v_{i+1}^{3\zeta_{i+1}} \cdots v_j^{3\zeta_j} \cdot v_{j+1}^{\zeta_{j+1}} \cdots v_u^{\zeta_u}.$$

By the property of an inert ideal we have that $p^{3\epsilon} = 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)$ for a inert prime p. The same result we have for principal ramified primes. So we are left with:

$$\beta\mathcal{O}_K = V_{i+1}^{3\zeta_{i+1}} \cdots V_j^{3\zeta_j} \cdot V_{j+1}^{\zeta_{j+1}} \cdots V_u^{\zeta_u},$$

where $V_{i+1} \cdots V_j$ the non-principal ramified ideals and $V_{j+1} \cdots V_u$ the split ideals.

Let's have a look at a non-principal ramified prime V that can occur in Λ. From $\beta = \left(n + \left(me - Be^3\right)\sqrt{A}\right)$ we see that $\left(n + \left(me - Be^3\right)\sqrt{A}\right) \in V$, from this it follows that $A \in V$.
A split prime is a prime that satisfies $(V) = P \cdot Q$, where $P \neq Q$. Here we have to consider two possibilities:

1. P and Q appear both in the prime ideal factorization of β. Here we have $\left(n + \left(me - Be^3\right)\sqrt{A}\right) \in V$. This means that V divides n and $\left(me - be^3\right)\sqrt{A} = e\left(m - be^2\right)\sqrt{A}$. One possibility is that V divides both n and e, but since $\gcd(n, e) = 1$ this is not possible. So we must have $V|A$ or $V|\left(m - Be^2\right)$. If $V|\left(m - Be^2\right)$ we have that $V|m$ and $V|B$, since $V|e$ is not possible as we saw before. So if P and Q appear both, we have that $AB \in V$.

2. Only P (or Q) appear in the prime ideal factorization of β. This case needs a little algebraic number theory. The class group C_l of the number field $\mathbb{Q}\left(\sqrt{A}\right)$ is a finite abelian group. Since only P occurs in the prime ideal factorization of β, and because the norm of β is a cube we must have that P occurs to some power 3ϵ with $\epsilon \in \mathbb{N}$. We have $P \sim \prod_i P_i^{\alpha_i} \cdot \prod_j Q_j^{\beta_j}$ since $P_{A,B} \cup Q_{A,B}$ generate the class group. So $P = \prod_i P_i^{\alpha_i} \cdot \prod_j Q_j^{\beta_j} \cdot (\lambda_P)$ where $\lambda_P \in \mathbb{Q}\left(\sqrt{A}\right)^*$. So since we have that P must occur to some power $3\epsilon_i$ this λ_P will disappear modulo third powers. So we only need to consider the P_i that generators the class group together with the elements in the set $Q_{A,B}$.

So we are left with:

$$\beta\mathcal{O}_K = V_{i+1}^{3\zeta_{i+1}} \cdots V_j^{3\zeta_j} \cdot V_{j+1}^{\zeta_{j+1}} \cdots V_u^{\zeta_u},$$

where $V_{i+1} \cdots V_j$ are the non-principal ramified ideals which divide A and $V_{j+1} \cdots V_u$ are the split primes which divide AB or the ideals that generate the class group. So rewriting the prime ideal factorization of β we get the set:

$$\left\{ \beta\mathbb{Q}\left(\sqrt{A}\right)^{*3} \mid \beta \neq 0,\ \beta \in \mathcal{O}_K \text{ and } \beta\mathcal{O}_K = P_1^{3\epsilon_1} \cdots P_n^{3\epsilon_n} \cdot Q_1^{3\delta_1} \cdots Q_m^{3\delta_m} \cdot R_1^{\gamma_1} \cdots R_t^{\gamma_t} \right\}.$$

We still need to prove: $\epsilon_j <$ the order of P_j, $\delta_i <$ the order of Q_i and $\gamma_k < 3$ times the order of R_k.
So start with $\beta\mathcal{O}_K = P_1^{3\epsilon_1} \cdots P_n^{3\epsilon_n} \cdot Q_1^{3\delta_1} \cdots Q_m^{3\delta_m} \cdot R_1^{\gamma_1} \cdots R_t^{\gamma_t}$ in the set above and $\delta = 3 \cdot \text{order}\,[P_j]$. Write $3\epsilon_i = q \cdot \delta + r$ where $r < \delta$. Since $3|\delta$ it follows that $r \equiv 0 \mod 3$.

$$(P_j)^{3\epsilon_i} = \left((P_j)^{\delta}\right)^q \cdot P_j^r = (\lambda)^q \cdot P_j^r = P_j^r \cdot \text{ something in } \mathbb{Q}\left(\sqrt{A}\right)^{*3}.$$

Since $r < \delta$ this proves the claim about the power of P_i. We have the same arguments for the maximum of δ_i and γ_k. □

The large set of the last theorem we give the name Λ, so:

$$\Lambda := \left\{ \beta\mathbb{Q}\left(\sqrt{A}\right)^{*3} \mid \beta \neq 0,\ \beta \in \mathcal{O}_K \text{ and } \beta\mathcal{O}_K = P_1^{3\epsilon_1} \cdots P_n^{3\epsilon_n} \cdot Q_1^{3\delta_1} \cdots Q_m^{3\delta_m} \cdot R_1^{\gamma_1} \cdots R_t^{\gamma_t} \right\}.$$

The following two theorems tells us more about the set Λ.

Theorem 10. *The set Λ is finite.*

Proof. This proof is totally given in the proof of theorem 9. □

Theorem 11. *The set Λ is a group.*

Proof.

- $G1$, associativity: For all $\beta_1, \beta_2, \beta_3 \in \Lambda$ we have $(\beta_1 * \beta_2) * \beta_3 = \beta_1 * (\beta_2 * \beta_3)$. This follows from the definition of the image α en the set Λ.

- $G2$, there exist a unit: For all $\beta \in \Lambda$ we have $\beta * e = \beta = e * \beta$. The unit in Λ is 1, since $\beta \cdot 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} = \beta \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} = 1 \cdot \beta \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3}$.

- $G3$, inverse: For all $\beta \in \Lambda$ exist a $\overline{\beta} \in \Lambda$ such that $\beta * \overline{\beta} = e = \overline{\beta} * \beta$. This follows directly from: $m^3 = \left(n + \left(me - Be^3\right)\sqrt{A}\right)\left(n - \left(me - Be^3\right)\sqrt{A}\right) = \beta \cdot \overline{\beta}$ and $m^3 = 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3}$.

□

Compute the rank

To compute the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A\,(x - B)^2$, in the case A and $-3A$ not a square, we first compute the sets Λ and $\bar{\Lambda}$ for $E_{A,B}$ as $\overline{E}_{\overline{A},\overline{B}}$. This gives an upper bound r_{up} for the rank, namely:

$$r_{\text{up}} = \#\Lambda \cdot \#\overline{\Lambda}. \tag{3.3}$$

After this we search for rational points on the curve $E_{A,B}$ and calculate their image of α in Λ. Doing the same for $\overline{E}_{\overline{A},\overline{B}}$ and combining the results gives a lower bound r_{low} for the rank, in terms of the subgroup of Λ generated by the images.

We know the rank of the elliptic curve $E_{A,B}$ if $r_{\text{up}} = r_{\text{low}}$. In all other cases we have only an upper bound and lower bound for the rank given by $r_{\text{low}} \leq r \leq r_{\text{up}}$.

3.4 Computing the rank

Since there is a lot of theory in the text above, the procedure to compute the upper and lower bound of the elliptic curve $E_{A,B} : y^2 = x^3 + A\,(x - B)^2$ is summarized here.

1. Compute the fundamental unit of the ring of integers $\mathcal{O}$ of the quadratic field $\mathbb{Q}\left(\sqrt{A}\right)$.

2. Compute the ideals P_j, that are the generators of the class group of the ring of integers $\mathcal{O}$.

3. Compute the non-principal ramified primes Q_i such that $A \in Q_i$.

4. Compute the split primes R_k such that $AB \in R_k$.

5. Compute with help of the order of the ideals (see theorem 9) the maximum power to which the ideals P_j, Q_i and R_k can occur.

6. Compute the powers that can occur such that the norm of $\beta \in \Lambda$ is divisible by 3.
7. Compute all possible products of the ideals P_j, Q_i and R_k with all the different powers possible. Call the products β_k.
8. Check from the β_k, that are created with the previous step, whether they are principal or not. The β_k that are not principal can be left out.
9. Compute all the possible combinations of the generators of the β_k that are left and the fundamental unit u to the power $0, 1$ and 2. If there is no fundamental unit, skip this step.
10. Check from all combinations of the previous step if there are generators that are the same upon third powers. If there are two the same, leave one out.
11. The list of generators that are left is the set Λ.
12. Compute all the rational points of $E_{A,B}$ and their image in α.
13. Check of the image of those points is in the set Λ. All those images of those points that satisfy this are in the image of α.
14. Repeat the steps 1 until 13 for $\overline{E}_{\overline{A},\overline{B}}$.
15. Compute $3^{r_{\text{upp}}} = \#\Lambda \cdot \#\overline{\Lambda}$.
16. Compute $3^{r_{\text{low}}} = \#\alpha\left(E_{A,B}\left(\mathbb{Q}\right)\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}\left(\mathbb{Q}\right)\right)$.
17. Compare r_{upp} and r_{low}. If they are the same you have found the rank of the elliptic curve $E_{A,B} : y^2 = x^3 + A\left(x - B\right)^2$, otherwise we have $r_{\text{low}} \leq r \leq r_{\text{up}}$.

In the next chapter we will explain the computer program we made with magma. This program is made with help of the roadmap stated above.

Chapter 4

Explanation of the code for computing the rank

The formulas we derived for computing the rank are not convenient in manual computation. Therefore, we started computing the rank of elliptic curves with help of the computer. Doing this we noticed that computing the rank with the standard function from magma or sage is not that good. The programs do not use the special formulas found in this thesis. That was the point where we decided to make a program of our own to compute the rank of an elliptic curve of the form:

$$E : y^2 = x^3 + A\left(x - B\right)^2. \tag{4.1}$$

In this chapter we explain how this program works. During this chapter the theory set out before is becoming more clear. The total code in magma can be found in appendix A.

In chapter 3 we saw:

$$\alpha\left(E_{A,B}\left(\mathbb{Q}\right)\right) \subset \left\{\beta\mathbb{Q}\left(\sqrt{A}\right)^{*3} \mid \beta \neq 0,\ \beta \in \mathcal{O}_K \text{ and } \beta\mathcal{O}_K = P_1^{3\epsilon_1}\cdots P_n^{3\epsilon_n}\cdot Q_1^{3\delta_1}\cdots Q_m^{3\delta_m}\cdot R_1^{\gamma_1}\cdots R_t^{\gamma_t}\right\},$$

where $P_j \in P_{A,B}$, $Q_i \in Q_{A,B}$ and $R_k \in R_{A,B}$, $\epsilon_j, \delta_i, \gamma_k \in \mathbb{Z}_{\geq 0}$, $\epsilon_j <$ the order of P_j, $\delta_i <$ the order of Q_i and $\gamma_k < 3$ times the order of R_k.

So we need to determine the set Λ. The first step is which P_j, Q_i and $R_k \subset \mathcal{O}_K$ appear in the image of α. Also we have to determine whether there are units that can appear in the image of α.

```
RankComputation := function(A,B)

R<x>:=PolynomialRing(Rationals());
K<c>:=QuadraticField(A);
L<d>:=IntegerRing(K);

ListU:=[];
if Discriminant(L) gt 0 then
   Append(~ListU,FundamentalUnit(L));
else
   Append(~ListU,d^0);
end if;
```

In the above piece of code we determine whether there are fundamental units appearing in the image of alpha. They are stored in `ListU`, otherwise 1 is stored in `ListU`.

```
ListP:=[];

C,c1:=ClassGroup(L);
numC:=# Generators(C);
for i in [1 .. numC] do
   Append(~ListP,c1(C.i));
end for;
```

Here we store in `ListP` the generators of the class group.

```
Id:=Factorization(A);
Id2:=Factorization(A*B);

ListQ:=[];
ListR:=[];

P<x>:=PolynomialRing(Integers());
poly:=P!MinimalPolynomial(d);

for i in [1 .. # Id] do
   g:=Id[i ,1];
   e:=poly mod g;
   Q<y> := PolynomialRing(GF(g));
   for k in [1 .. # Factorization(Q!e)] do
      Ge:=Factorization(Q!e)[k,1];
      pol:=P!Ge;
      GeU:=Evaluate(pol,d);
      I:=ideal< L| GeU,g>;
      if IsRamified(I) eq true and IsPrincipal(I) eq false then
         Append(~ListQ,I);
      end if;
   end for;
end for;

for i in [1 .. # Id2] do
   g:=Id2[i ,1];
   e:=poly mod g;
   Q<y> := PolynomialRing(GF(g));
   for k in [1 .. # Factorization(Q!e)] do
      Ge:=Factorization(Q!e)[k,1];
      pol:=P!Ge;
```

```
        GeU:=Evaluate(pol,d);
        I:=ideal< L| GeU,g>;
        if IsSplit(I) eq true then
            Append(~ListR,I);
        end if;
    end for;
end for;
```

Then we determine the prime ideals Q_i and R_k , where the generators of the ideals can appear in the image of α. Recall that this were the generators of the prime ideals Q_i such that Q_i is non-principal ramified that divides A and that R_k are the prime ideals that are split and divides AB. In the above piece of code we search for those Q_i and R_k and store the R_k in `ListR` and the Q_i in `ListQ`.

The next piece of code can be found in appendix A. It is not repeated here, because it doesn't include any new theory. The only thing it does is checking whether there are double prime ideals in `ListP` and `ListQ`. If there are double ideals this will not bring any more elements in Λ, so one of them can be omitted. So if there are double ideals we will delete them from `ListP`.

```
Listep1:=[];

if # ListP eq 0 then
    n:=0;
    Append(~Listep1,n);
else
    for i in [1 .. # ListP] do
        n:=1; J:=ListP[i];
        while not IsPrincipal(J) do
            n:=n+1; J:=J*ListP[i];
        end while;
        Append(~Listep1,n);
    end for;
end if;
```

In the above piece of code we determine the maximum power of which the generator of the ideal can occur.
In the above code we first make an empty list. Then in the while loop we check what the order of the prime ideal is. The order we save as the number n. We do this for all items in `ListP`, and also in other pieces of code for `ListQ` and `ListR`.

```
Listimagealphaunits:=[];

if ListU[1] eq 1 then
    Append(~Listimagealphaunits,ListU[1]);
end if;
if ListU[1] ne 1 then
    for a in [0 .. 2] do
        Append(~Listimagealphaunits,ListU[1]^a);
```

```
    end for;
end if;
```

Above we are looking at the units that can occur in the image of α. If there exists a fundamental unit then we store in `Listimagealphaunits` $1, u$ and u^2, otherwise we only store 1.

The next piece of code is not that informative, so we do not place it here. This code makes from `ListP`, `ListQ` and `ListR` one list (`Listideals`), and from `Listep1`, `Listep2` and `Listep3` one list (`Listpowers`). The only important thing here is that the order in `Listideals` and `Listpowers` is the same, so we know which power belongs to which ideal.

```
Listnorms:=[];

for i in [1 .. # Listideals] do
    Listnorms:=Append(Listnorms,Norm(Listideals[i]));
end for;

Listhelp :=[];

for i in [1 .. # Listnorms] do
    for j in [1 .. # Listnorms] do
        if i ne j and j ge i then
            if Listnorms[i] eq Listnorms[j] then
                Listhelp:=Include(Listhelp,<i,j>);
            end if;
        end if;
    end for;
end for;
```

Then it is important to look to which power the ideals can occur in the image of α. We already know the maximum powers and they are all stored in `Listpowers`. The first thing is to look whether the norms of two ideals are the same. These are the split ideals. We store this in `Listhelp`.
So with `Listhelp`, as described above, we determine to which powers the ideals P_j and Q_i can occur. All powers we put in a list as follows $[< i_1, j_1 >, \ldots, < i_k, j_n >]$, where $j_1 \ldots j_n$ are powers that can occur on the ideals on place $i_1 \ldots i_k$ in `Listideals`. The code that computes these powers is a little bit long, so we will not place it here. As mentioned before the whole code can be found in appendix A.

```
Listallpowers:=AssociativeArray();

for i in [1 .. # Listideals] do
    Listallpowers[i]:=<>;
    for j in [1 .. # Listrealpowers] do
        if Listrealpowers[j,1] eq i then
            Listallpowers[i]:=Append(Listallpowers[i],Listrealpowers[j,2]) ;
        end if;
    end for;
end for;
```

In the above piece of code we rewrite the list $[< i_1, j_1 >, \ldots, < i_k, j_n >]$, where $j_1 \ldots j_n$ are the powers that can occur on the ideals on place $i_1 \ldots i_k$ in `Listideals`. We make a list `Listallpowers` as long as the number of ideals in `Listideals`. On the first place we write the powers to which the first ideal can occur, on the second place we write the powers to which the second ideal can occur, etcetera. So in total we get a list that looks like this for example: $[< j_1, j_2 >, < j_3 >, \cdots, < j_{n-1}, j_n >]$ where the length is thus k, the number of ideals in `Listideals`. Important is here that if there are split ideals occurring in `Listideals` that in these list the powers that must occur together are on the same place. For example when I, J are split primes with $IJ = (p)$ then $\mathrm{ord}_I(\beta) + \mathrm{ord}_J(\beta) \cong 0 \mod 3$ for any $\beta \mathbb{Q}\left(\sqrt{A}\right)^{*3} \in \Lambda$.

After this there is a code that makes al possible combinations of the `Listallpowers`. So on each place there is a power from each different ideal. So say for example we have 4 ideals then on 1 place there will be 4 numbers, where the first refer to the first ideal, the second to the second ideal etcetera. This list is called `Listpossibilities`.

```
if # Listideals ne 0 then
    Listidealsleft :=[ &*[Listideals[j]^ Listpossibilities [i,j] : j in [1..# Listideals ]] : i in
        [1.. number] ];
else
    Listidealsleft :=[];
end if;
```

In the above piece of code we compute the possible ideals that can occur in the image of α. This looks like the ideal of this form:

$$P_1^{3\epsilon_1} \cdots P_n^{3\epsilon_n} \cdot Q_1^{\delta_1} \cdots Q_m^{\delta_m} cdot R_1^{\gamma_1} \cdots R_z^{\gamma_k}, \tag{4.2}$$

where $P_j, Q_i, R_k \in \mathcal{O}_K$ prime ideals, $\epsilon_j, \delta_i, \gamma_k \in \mathbb{Z}_{\geq 0}$, P_j's are the generators of the class group, the Q_i's de primes that are non-principal ramified and dividing A and the R_k's the split primes where $AB \in Q_i$. So the ideals in `Listidealsleft` are the ideals of the form 4.2.

```
image:=[];
Z<T>:=PolynomialRing(K);

Listimagehelp:=[];
if # Listidealsleft ne 0 then
   for i in [1 .. # Listidealsleft ] do
      b,g:=IsPrincipal( Listidealsleft [i]);
      if b eq true then
         Listimagehelp:=Include(Listimagehelp,g);
      end if;
   end for;
end if;

if # Listimagehelp eq 0 then
```

```
    Listimagehelp:=Include(Listimagehelp,1);
end if;
```

The ideals in 4.2 can only occur in the image of α if they are principal and if they are principal we need a generator. That is what the above code computes. The generators of the principal ideals we put in the `Listimagehelp`. The last three lines are necessary because if there are no ideals in the list, the list will stay empty, but there has to be something in it otherwise we cannot multiply with the generators of the unit group. The first two lines we need later.

```
Listimage:=[];

for i in [1 .. # Listimagealphaunits] do
   for j in [1 .. # Listimagehelp] do
      Listimage:=Include(Listimage,Listimagealphaunits[i]*Listimagehelp[j]);
   end for;
end for;
```

In the above code we multiply the generators of the possible ideals in the image of α with the generators of the unit group we found before.

```
PP<s>:=PolynomialRing(L);
Helplist:=Listimage;

for i in [1 .. # Listimage] do
   for j in [1 .. # Listimage] do
      if i ne j and i gt j then
         if # Factorisation(s^3-(Listimage[i])*(Listimage[j])^2) ge 2 then
            Helplist:=Exclude(Helplist,Listimage[j]);
         end if;
      end if;
   end for;
end for;
```

Here we check whether there are two generators that are the same modulo third powers. This is because

$$\alpha : \Gamma \to \mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3}.$$

So if the generators are the same modulo third powers then they are equal in $\mathbb{Q}\left(\sqrt{A}\right)^* / \mathbb{Q}\left(\sqrt{A}\right)^{*3}$. `Helplist` is the set Λ.

```
Aind:=-Evaluate(Factorization(s^2-A)[1,1],0);
E:=EllipticCurve(x^3+A*(x-B)^2);

PointsE:=RationalPoints(E:Bound:=100000);
PointsE:=PointsE join {P+Q : P in PointsE, Q in PointsE} join {-P + Q : P in PointsE, Q in
    PointsE};
for i in [2 .. # PointsE] do
   P:=PointsE[i];
   aP:=Denominator(P[2])*(P[2]+(P[1]-B)*Aind);
      for j in [1 .. # Helplist] do
         if IsIrreducible (T^3-aP/Helplist[j]) eq false then
```

```
            image:=Include(image,Helplist[j]);
            break;
        end if;
    end for;
end for;

image:=Include(image,1);
agamma:=# image;
lambda:=# Helplist;

return agamma, lambda;

end function;
```

This is the last piece of code concerning the generators of the ideals that can occur in the image of α. Here we look which points lie on the elliptic curve. Then we compute the image of α of those points and check whether they are in Λ. The points that satisfy this will be put in the list named `image`. The only important thing here is how many generators of ideals are in the image, this number we will store in `agamma`.
To compute the rank we follow the same procedure as explained before for the elliptic curve $\overline{E}_{\overline{A},\overline{B}}$. Here the number of generators in the image of alpha we store in `agammastreep`. For computing the rank we use the formula stated before

$$3^r = \begin{cases} \frac{1}{3} \cdot \#\alpha\left(\Gamma\right) \cdot \#\overline{\alpha}\left(\overline{\Gamma}\right) & \text{if } A = -3a^2 \text{ or } A = a^2 \\ \#\alpha\left(\Gamma\right) \cdot \#\overline{\alpha}\left(\overline{\Gamma}\right) & \text{otherwise.} \end{cases}$$

So the last part of the code is

```
A := 8;
B := 1;

agamma, lambda := RankComputation(A, B);
agammastreep, lambdastreep := RankComputation(−27∗A, 4∗A+27∗B);

upperboundrank:=Log(3,lambda∗lambdastreep);
lowerboundrank:=Log(3,agamma∗agammastreep);

"Upperbound rank";
upperboundrank;

"Lowerbound rank";
lowerboundrank;

"Rank of Ellipticcurve E is";
if upperboundrank eq lowerboundrank then
   lowerboundrank;
else
   "Rank not determined";
end if;
```

As explained in section 3.4 we have computed an upper bound and lower bound for the rank. If they are the same we have computed the rank.

Chapter 5

Examples

5.1 Example $E_{8,1} : y^2 = x^3 + 8\,(x-1)^2$

We will derive the rank of this elliptic curve with help of de program explained in chapter 4. This example is also stated in [vB10], but since it was not fully explained there, we will do it here.

We have $A = 8$ and this is not a square or $-3a^2$. So we are working in $\mathbb{Q}\left(\sqrt{2}\right)$ and the ring of integers is $\mathbb{Z}[\sqrt{2}]$. The fundamental unit of $\mathbb{Z}[\sqrt{2}]$ is $1-\sqrt{2}$.

The class number is 1 in this case, so we will not find any generators for the class group. Thus $P_{8,1} = \emptyset$.

Now we have to look whether there are prime ideals Q and R, the primes that are non-principal ramified or split primes respectively and where $A \in Q$ and $AB \in R$. We have that the prime factorization of $AB = 8 \cdot 1 = 2^3$. So we only have to look at prime ideals Q and R that are dividing 2. With help of the program we find that they do not exist. Thus $Q_{8,1} = R_{8,1} = \emptyset$. So in fact we have now completed the computation.

We now know the set $\Lambda = \left\{1, 1-\sqrt{2}, \left(1-\sqrt{2}\right)^2\right\}$.
Computing the rational points on the elliptic curve E gives us a lot of points, and from the program we have made we see that the point $P = (2,4)$ gives after some computation $\alpha\,(2,4) = \left(1-\sqrt{2}\right) \cdot \mathbb{Q}\left(\sqrt{2}\right)^{*3}$ and $2P = \left(\frac{1}{4}, \frac{17}{8}\right)$, so $\alpha\,(2P) = \left(1-\sqrt{2}\right)^2 \cdot \mathbb{Q}\left(\sqrt{2}\right)^{*3}$.
So we see in this case that the number of elements in Λ is equal to the number of elements in the image of α.

For $\overline{E}_{\overline{A},\overline{B}}$ we have that the equation of the curve is given by: $\overline{E}_{-216,59} : y^2 = x^3 - 216\,(x-59)^2$. We are now working in the number field $\mathbb{Q}\left(\sqrt{-6}\right)$. So we have the

ring of integers $\mathbb{Z}\left(\sqrt{-6}\right)$. Since $d < -1$ there is no fundamental unit. We find one ideal that generates the class group, namely $P = \left(2, \sqrt{-6}\right)$. If we factorize $A \cdot B = -216 \cdot 59 = 2^3 \cdot 3^3 \cdot 59$. We find with help of the program $Q_1 = \left(2, \sqrt{-6}\right), Q_2 = \left(3, \sqrt{-6}\right)$, $R_1 = \left(59, \sqrt{-6} + 17\right), R_2 = \left(59, \sqrt{-6} + 42\right)$.
We see that the ideals P and Q_1 are the same, so we don't have to consider P anymore. So we consider (Q_1, Q_2, R_1, R_2). The maximum powers are as follows $(5, 5, 5, 5)$. And the norms of the ideals are given by $(2, 3, 59, 59)$. So we see that for the ideals Q_1 and Q_2 the power must be divisible by 3 and by R_1 and R_2 we must have $3 | (\gamma_1, \gamma_2)$ where γ_i is the power of R_i.

So in total this gives us: $[< 1, 0 >, < 1, 3 >, < 2, 0 >, < 2, 3 >, < 3, 0 >, < 4, 0 >, < 3, 0 >, < 4, 3 >, < 3, 1 >, < 4, 2 >, < 3, 1 >, < 4, 5 >, < 3, 2 >, < 4, 1 >, < 3, 2 >, < 4, 4 >, < 3, 3 >, < 4, 0 >, < 3, 4 >, < 4, 2 >, < 3, 5 >, < 4, 1 >]$ where the first place refers to the ideal, and the second place refers to the possible power of that ideal. Watch out that by the ideals $3 = R_1$ and $4 = R_2$ we have that the two powers in row are together, because together they have to be divisible by 3. (See also the explanation in chapter 4).

Now we will make all the possible combination of these ideals. Since this list is long we will not state it here. After that we check whether they are principal, if they are not principal then they are not in Λ. If they are principal they have a generator which we will denote in a list `Listidealsleft`. From the generators of ideals in `Listidealsleft` we normally have to multiply them with the fundamental unit to the power $0, 1, 2$. Since we don't have a fundamental unit in this case we can skip this step.
From the generators of ideals that are left we check whether they are the same upon third powers, if this is the case we will delete one of them. After this we are left with three generators, which is the set $\overline{\Lambda} = \left\{1, -104430\sqrt{-6} - 3007584, -1214574\sqrt{-6} + 509760\right\}$.

After checking with the rational points of $\overline{E}$ we see that this 3 generators of ideals are indeed in the image of $\overline{\alpha}$.

So in this case we have $3^{r_{\text{upp}}} = 3^{r_{\text{low}}} = 3 * 3 = 3^2$ and the rank is 2.

5.2 Example $E_{79,4} : y^2 = x^3 + 79\,(x-4)^2$

This example can also be found in [vB10], but since there was only an upper bound for the rank found, we can show that the program we made is really an improvement, since we now can find the rank. From the previous example it is already clear how the computer program works, and since the output of this program is already very big we will only state the important things here. Starting with the elliptic curve $E_{79,4} : y^2 = x^3 + 79\,(x-4)^2$,

so $A = 79$ and $B = 4$. We are working in the number field $\mathbb{Q}\left(\sqrt{79}\right)$ with ring of integers $\mathbb{Z}[\sqrt{79}]$ and find:
$\texttt{ListU} = \left\{-9\sqrt{79} + 80\right\}$,
$\texttt{ListP} = \left\{\left(3, \sqrt{79} + 1\right)\right\}$.
Where the element in `ListU` is the fundamental unit and the ideal P_1 in `ListP` is the generator of the class group.

The maximum power of P_1 computed with the program is 8. So since the element $\beta_k \in \Lambda$ has to have a norm divisible by 3 we must have P_1 to a power $0, 3$ or 6. So if we compute the powers of P_1 we get 3 ideals:

$$\left\{\left(27, \sqrt{79} + 22\right), \left(729, 359\sqrt{79} + 266\right), (1)\right\}.$$

All these ideals are principal and their generators are:

$$\left\{2\sqrt{79} + 17, -5\sqrt{79} + 52, 1\right\}.$$

Combining this with the fundamental unit to the power 0,1 and 2 gives the set:

$$\left\{2\sqrt{79} + 17, 5\sqrt{79} - 52, 1, -313\sqrt{79} - 2782, 68\sqrt{79} + 605, -9\sqrt{79} - 80,\right.$$
$$\left. 50078\sqrt{79} + 445103, -10885\sqrt{79} - 96748, 1440\sqrt{79} + 12799\right\}.$$

Checking whether there are double elements up to third power gives us the same set, so we know that the set Λ exists of 9 elements. With the program we checked that those 9 elements are also in the image of α. So the number of elements in the image of α is also 9.

Now we have to follow the same procedure for the curve $\overline{E}_{2133,424} = x^3 - 2133\,(x - 424)^2$. We are working in the number field $\mathbb{Q}\left(\sqrt{-237}\right)$ with ring of integers $\mathbb{Z}[\sqrt{-237}]$. This ring of integers has units $\{\pm 1\}$, so a fundamental unit doesn't exist. We find:

$\texttt{ListP} = \left\{\left(2, \sqrt{-237} + 1\right), \left(7, 48\sqrt{-237} + 1\right)\right\}$,
$\texttt{ListQ} = \left\{\left(2, \sqrt{-237} + 1\right), \left(3, \sqrt{-237}\right), \left(79, \sqrt{-237}\right)\right\}$,
$\texttt{ListR} = \left\{\left(53, \sqrt{-237} + 9\right), \left(53, \sqrt{-237} + 44\right)\right\}$.

The ideals P_i in `ListP` are the generators of the class group together with the elements in `ListQ`. The elements in `ListQ` are the elements which are non-principal, ramified and dividing A and `ListR` are the elements which are split and dividing AB.
Since there is an ideal that appears in `ListP` and in `ListQram` we can ignore the element in the set P. So in total we are left with 6 ideals:

$$\left\{\left(2, \sqrt{-237} + 1\right), \left(7, 48\sqrt{-237} + 1\right), \left(3, \sqrt{-237}\right), \left(79, \sqrt{-237}\right),\right.$$
$$\left.\left(53, \sqrt{-237} + 9\right), \left(53, \sqrt{-237} + 44\right)\right\}$$

with maximum powers $\{5, 17, 5, 5, 5, 5\}$ and norms $\{2, 7, 3, 79, 53, 53\}$. Now we see directly the problem with this elliptic curve, we really get a large amount of possibilities according to this ideals. So we are not able to put all the possibilities here, but with the program we find $\#\overline{\Lambda} = 9$ and $\#\overline{\alpha} = 9$. So in this case we find:

$$3^{r_{\text{upp}}} = 3^{r_{\text{low}}} = 9 * 9 = 3^4$$

so the rank is 4.

5.3 Example $E_{-388728,5184} : y^2 = x^3 - 388728\,(x - 5184)^2$

We start with the elliptic curve $E_{-388728,5184} : y^2 = x^3 - 388728\,(x - 5184)^2$, so $A = -388728$ and $B = 5184$. We are working in the number field $\mathbb{Q}\left(\sqrt{-10798}\right)$ with the ring of integers $\mathbb{Z}[\sqrt{-10798}]$. This ring of integers has units $\{\pm 1\}$, so a fundamental unit doesn't exist. We find:

$\texttt{ListP} = \left\{\left(23, \sqrt{-10798} + 9\right), \left(11, \sqrt{-10798} + 9\right)\right\}$.
$\texttt{ListQ} = \left\{\left(2, \sqrt{-10798}\right), \left(5399, \sqrt{-10798}\right)\right\}$.

The ideals P_i in `ListP` are the generators of the class group together with the elements in `ListQ`. The elements in `ListQ` are the elements which are non-principal, ramified and dividing A.

Those ideals have maximum powers $\{8, 53, 5, 5\}$ and norms $\{23, 11, 2, 5399\}$. Which gives: $[< 1, 0 >, < 1, 3 >, < 1, 6 >, < 2, 0 >, < 2, 3 >, < 2, 6 >, < 2, 9 >, < 2, 12 >, < 2, 15 >, < 2, 18 >, < 2, 21 >, < 2, 24 >, < 2, 27 >, < 2, 30 >, < 2, 33 >, < 3, 0 >, < 3, 3 >, < 4, 0 >, < 4, 3 >]$ as possible powers. In total this gives the set (where $d := \sqrt{-10798}$):

$$\begin{aligned}\Lambda := [&- 399526 \cdot d - 116596804, -101814342 \cdot d + 8628163496,\\ &14567160678 \cdot d - 1288394684200, -1827379629286 \cdot d - 109625597685644,\\ &- 42012551402062 \cdot d + 23788192351399056,\\ &- 5415227091013358 \cdot d + 3476246042123072400,\\ &3676609444490566646 \cdot d - 70147481429791439116,\\ &2061820308759424050 18 \cdot d + 37104571968706855396216, 1].\end{aligned}$$

Thus the number of elements in Λ is 9. With magma we find that the number of elements in the image of α is also 9.

Now we have to follow the same procedure for the curve $\overline{E}_{10495656,-1414944} : y^2 = x^3 + 10495656\,(x + 1414944)^2$. We are working in the number field $\mathbb{Q}\left(\sqrt{32394}\right)$ with ring of

integers $\mathbb{Z}[\sqrt{32394}]$. We find (where $d := \sqrt{32394}$):

$\texttt{ListU} = \{-60 \cdot d + 10799\}$,
$\texttt{ListP} = \{(139, 18188 \cdot d + 9505)\}$,
$\texttt{ListQ} = \{(2, d), (3, d)\}$,
$\texttt{ListR} = \{(17, d + 3,), (17, d + 14)\}$.

The element in `ListU` is the fundamental unit. The ideal P_i in `ListP` is the generator of the class group together with the elements in `ListQ`. The elements in `ListQ` are the elements which are non-principal, ramified and dividing A and `ListR` are the elements which are split and dividing AB.

Those ideals have maximum powers $\{53, 5, 5, 8, 8\}$ and norms $\{139, 2, 3, 17, 17\}$. Which gives: $[< 1, 0 >, < 1, 3 >, < 1, 6 >, < 1, 9 >, < 1, 12 >, < 1, 15 >, < 1, 18 >, < 1, 21 >, < 1, 24 >, < 1, 27 >, < 1, 30 >, < 1, 33 >, < 1, 36 >, < 1, 39 >, < 1, 42 >, < 1, 45 >, < 1, 48 >, < 1, 51 >, < 2, 0 >, < 2, 3 >, < 3, 0 >, < 3, 3 >, < 4, 0 >, < 5, 0 >, < 4, 0 >, < 5, 3 >, < 4, 0 >, < 5, 6 >, < 4, 1 >, < 5, 2 >, < 4, 1 >, < 5, 5 >, < 4, 1 >, < 5, 8 >, < 4, 2 >, < 5, 1 >, < 4, 2 >, < 5, 4 >, < 4, 2 >, < 5, 7 >, < 4, 3 >, < 5, 0 >, < 4, 4 >, < 5, 2 >, < 4, 5 >, < 5, 1 >, < 4, 6 >, < 5, 0 >, < 4, 7 >, < 5, 2 >, < 4, 8 >, < 5, 1 >]$ as possible powers.

In total this gives that the set $\overline{\Lambda}$ exists of 27 elements. With magma we find that the number of elements that can be found in the image of $\overline{\alpha}$ is 3. Namely

$$\begin{aligned}\overline{\alpha} = [1, &-93215149139944502684595153521762639053023933393607054462 2 \cdot d \\ &+ 16777173187439073740843544858252805865151862715229267333574 8, \\ &- 54354393445109837896084189445254365225121122 \cdot d \\ &+ 97828848716183245782227758574688125007033438 12]\end{aligned}$$

We have the following formulas for the upper- and lower bound.

$$\begin{aligned}3^{r_{\text{upp}}} &= \#\Lambda \cdot \#\overline{\Lambda} = 9 \cdot 27 = 3^5 \\ 3^{r_{\text{low}}} &= \#\alpha\left(E_{A,B}\left(\mathbb{Q}\right)\right) \cdot \#\overline{\alpha}\left(\overline{E}_{\overline{A},\overline{B}}\left(\mathbb{Q}\right)\right) = 9 \cdot 3 = 3^3\end{aligned}$$

So for this curve we have $3 \leq r \leq 5$.

Using the standard commands `Rank(E);` and `MordellWeilShaInformation(E);` in magma one finds that in fact the rank of this curve equals 5, and magma is able to find five generators of $E(\mathbb{Q})$. So in principle these could be used to construct the missing elements in the image of $\overline{\alpha}$.

Chapter 6

Families of elliptic curves of higher rank.

In this chapter we try to find families of elliptic curves with higher rank.

6.1 Elliptic curves with at least 2 rational points

Lets start with the elliptic curve $E_{A,B} : y^2 = x^3 + A(x-B)^2$. Now we want that the point $(x, y) = (1, c)$ lies on the curve. So we must have:

$$c^2 = 1^3 + A(1-B)^2.$$

Solving for A gives

$$A = \frac{c^2-1}{(1-B)^2}.$$

We then have a new elliptic curve

$$y^2 = x^3 + \frac{c^2-1}{(1-B)^2}(x-B)^2 \tag{6.1}$$

which contains the point $(1, c)$.

Continuing this, we would like to have a point $(-1, d)$ on the elliptic curve $y^2 = x^3 + \frac{c^2-1}{(1-B)^2}(x-B)^2$. So we have to solve

$$d^2 = -1 + \frac{c^2-1}{(1-B)^2}(1+B)^2$$

which can be written as

$$d^2 + 1 = \left(c^2-1\right)\left(\frac{1+B}{1-B}\right)^2.$$

We define $\alpha := \frac{1+B}{1-B}$, then

$$d^2 + 1 = \left(c^2 - 1\right)\alpha^2$$

which can be rewritten as

$$1 + \alpha^2 = (\alpha c - d)(\alpha c + d).$$

We will now parametrize the solution (c, d) to this equation. We switch to homogeneous coordinates, $(c, d) = (cZ, dZ, Z) = (C, D, Z)$. Filling this out, in equation $1 + \alpha^2 = (\alpha c - d)(\alpha c + d)$, gives

$$(\alpha C - D)(\alpha C + D) = \left(1 + \alpha^2\right) Z^2$$

which contains the points at infinity $(1 : \pm\alpha : 0)$. Consider a line $y = tx + \lambda z$ containing the point $(1 : \alpha : 0)$. Then $\alpha = t \cdot 1 + \lambda \cdot 0 = t$. So the equation of the line is $y = \alpha x + \lambda z$. Intersecting the line with the curve given by $(\alpha x - y)(\alpha x + y) = \left(1 + \alpha^2\right) z$ one obtains two intersection points $(1 : \alpha : 0)$ and $(1 : -\alpha : 0)$. Since we have the equation $d^2 + 1 = \left(c^2 - 1\right)\alpha^2$ it follows that $y^2 + 1 = \left(x^2 - 1\right)\alpha^2$.

$$\begin{aligned}
y^2 + 1 &= \left(x^2 - 1\right)\alpha^2 \\
(\alpha x + \lambda)^2 + 1 &= \alpha^2\left(x^2 - 1\right) \\
\alpha^2 x^2 + 2\alpha x\lambda + \lambda^2 + 1 &= \alpha^2 x^2 - \alpha^2 \\
2\alpha x\lambda &= -\lambda^2 - \alpha^2 - 1.
\end{aligned}$$

So in total we get

$$\begin{aligned}
\alpha &= \frac{1+B}{1-B} \\
c = x &= \frac{-\alpha^2 - \lambda^2 - 1}{2\lambda\alpha} = \frac{-\left(\frac{1+B}{1-B}\right)^2 - \lambda^2 - 1}{2\lambda\frac{1+B}{1-B}} \\
d = y &= \alpha x + \lambda = \frac{-\alpha^2 - \lambda^2 - 1}{2\lambda} + \lambda = \frac{-\left(\frac{1+B}{1-B}\right)^2 + \lambda^2 - 1}{2\lambda}.
\end{aligned}$$

Then the elliptic curve becomes

$$\begin{aligned}
y^2 &= x^3 + \frac{c^2 - 1}{(1-B)^2}(x - B)^2 \\
&= x^3 + \frac{\left(-2\left(\frac{1+B}{1-B}\right)^2\lambda - \left(\frac{1+B}{1-B}\right)^2 - \lambda^2 - 1\right)\left(2\left(\frac{1+B}{1-B}\right)^2\lambda - \left(\frac{1+B}{1-B}\right)^2 - \lambda^2 - 1\right)}{4\left(\frac{1+B}{1-B}\right)^4\lambda^2(1-B)^2}(x - B)^2
\end{aligned}$$

which has points $(1, c(B, \lambda))$ and $(-1, d(B, \lambda))$.

We checked for a lot of values of B, λ that the rank is always 2 or higher. An advantage of such a family is that there appear elliptic curves with higher rank more often. We made a loop which runs over B from 2 to 7 and λ from 1 to 7. Among these 42 elliptic curves there are already 8 with rank 4! The elliptic curves of rank 4 are:

$$\begin{aligned}
&B = 4,\ \lambda = 1,\ y^2 = x^3 + \frac{949}{8100}(x-4)^2,\\
&B = 4,\ \lambda = 3,\ y^2 = x^3 + \frac{205}{2916}(x-4)^2,\\
&B = 4,\ \lambda = 4,\ y^2 = x^3 + \frac{4321}{32400}(x-4)^2,\\
&B = 4,\ \lambda = 5,\ y^2 = x^3 + \frac{44581}{202500}(x-4)^2,\\
&B = 4,\ \lambda = 6,\ y^2 = x^3 + \frac{23941}{72900}(x-4)^2,\\
&B = 4,\ \lambda = 7,\ y^2 = x^3 + \frac{7261}{15876}(x-4)^2,\\
&B = 5,\ \lambda = 6,\ y^2 = x^3 + \frac{19465}{82944}(x-5)^2,\\
&B = 6,\ \lambda = 6,\ y^2 = x^3 + \frac{193069}{1102500}(x-6)^2.
\end{aligned}$$

Since we found that for a lot of curves with rank 4 we have $B := 4$ we fixed this B and let λ run from 1 to 54. Then among these 54 curves we find that there appear 13 curves of rank 3, 25 curves of rank 4, 12 curves of rank 5 and 4 curves of rank 6! The elliptic curves of rank 6 are:

$$\begin{aligned}
&B = 4,\ \lambda = 26,\ y^2 = x^3 + \frac{9205381}{1368900}(x-4)^2,\\
&B = 4,\ \lambda = 37,\ y^2 = x^3 + \frac{6056557}{443556}(x-4)^2,\\
&B = 4,\ \lambda = 49,\ y^2 = x^3 + \frac{466258549}{19448100}(x-4)^2,\\
&B = 4,\ \lambda = 52,\ y^2 = x^3 + \frac{5914633}{219024}(x-4)^2.
\end{aligned}$$

6.1.1 The case $B = 4$

Since in section 6.1 it appears that the elliptic curve

$$y^2 = x^3 + \frac{c^2-1}{(1-B)^2}(x-B)^2, \text{where } c = \frac{-\left(\frac{1+B}{1-B}\right)^2 - \lambda^2 - 1}{2\lambda\frac{1+B}{1-B}}$$

with $B = 4$ gives elliptic curves with rank at least 3, we will show that there are indeed 3 independent points on this curve.

Filling in $B = 4$ into c gives

$$c = \frac{9\lambda^2 + 34}{30\lambda}$$

which gives the elliptic curve:

$$y^2 = x^3 + \frac{81\lambda^4 - 288\lambda^2 + 1156}{8100\lambda^2}(x-4)^2.$$

Multiplying this equation by 90^6 gives

$$\hat{y}^2 = \hat{x}^3 + \frac{81\lambda^4 - 288\lambda^2 + 1156}{\lambda^2}(x-32400)^2.$$

Multiplying by λ^6 gives

$$E : \tilde{y}^2 = \tilde{x}^3 + \left(81\lambda^4 - 288\lambda^2 + 1156\right)\left(x - 32400\lambda^2\right)^2.$$

Looking whether there are points $(x, y) = (a\lambda^4 + b\lambda^2 + c, d\lambda^6 + e\lambda^4 + f\lambda^2 + g)$ on the curve E gives us 4 points:

$$\begin{aligned}
P_1 &= (x_1, y_1) = \left(-8100\lambda^2, 364500\lambda^4 - 1377000\lambda^2\right)\\
P_2 &= (x_2, y_2) = \left(-2160\lambda^2 + 17340, 311040\lambda^4 - 725220\lambda^2 + 2358240\right)\\
P_3 &= (x_3, y_3) = \left(8100\lambda^2, 218700\lambda^4 + 826200\lambda^2\right)\\
P_4 &= (x_4, y_4) = \left(1215\lambda^4 - 2160\lambda^2, 43740\lambda^6 - 191970\lambda^4 + 1175040\lambda^2\right).
\end{aligned}$$

Checking whether these points are independent gives:

$$\begin{aligned}
P_1 + P_2 + P_3 &= \mathcal{O}\\
2P_1 + P_2 - P_4 &= \mathcal{O}.
\end{aligned}$$

So we see that only P_1 and P_2 are independent. If we now replace λ^2 by t we find the curve F, given by

$$F : ty^2 = x^3 + (81t^2 - 288t + 1156)(x - 32400t)^2.$$

Looking whether there are points $(x, y) = (at^4 + bt^2 + c, dt^6 + et^4 + ft^2 + g)$ on the curve F gives us

$$\begin{aligned}
P_5 &= (x_5, y_5) = \left(-81t^2 + 8388t - 1156, 21870t^2 + 651240t + 312120\right)\\
P_6 &= (x_6, y_6) = (32400t, 5832000t)
\end{aligned}$$

Which are also points on E:

$$\begin{aligned}
P_5 &= (x_5, y_5) = \left(-81\lambda^4 + 8388\lambda^2 - 1156, 21870\lambda^5 + 651240\lambda^3 + 312120\lambda\right)\\
P_6 &= (x_6, y_6) = \left(32400\lambda^2, 5832000\lambda^3\right)
\end{aligned}$$

Checking whether P_5 and P_6 are independent gives:

$$P_5 - 2P_6 = \mathcal{O}.$$

So taking P_1, P_2 and P_5 gives us three independent points, which means we have at least rank 3 on this curve.

6.2 Elliptic curves of the form $y^2 = x^3 + a(t)(x-b)^2$

This form of elliptic curves can be found in [Top91]. The family of elliptic curves made there are with $a(t) = t^2 - \left(\beta^2+\beta+1\right)^3$, $b = \left(\beta^2+\beta\right)^2$, $\beta \in \mathbb{Q}$, $\beta \neq 0, -1$. So the curve is:

$$y^2 = x^3 + \left(t^2 - \left(\beta^2+\beta+1\right)^3\right)\left(x - \left(\beta^2+\beta\right)^2\right)^2. \tag{6.2}$$

This curve has over $\mathbb{Q}(t)$ at least rank 3. From [Top91] we see this elliptic curve contains 7 points, namely $(x,y) = \left(\left(\beta^2+\beta\right)^2, \left(\beta^2+\beta\right)^3\right)$ and 6 points $(\text{constant}, \pm\text{constant} \cdot t) = (\tilde{x}, \pm\tilde{y}\cdot t)$. In this paper these points were not determined, so we will do this here. Filling out in the equation of the elliptic curve gives

$$\begin{aligned}(\tilde{y}\cdot t)^2 &= \tilde{x}^3 + \left(t^2 - \left(\beta^2+\beta+1\right)^3\right)\left(\tilde{x} - \left(\beta^2+\beta\right)^2\right)^2 \\ \tilde{y}^2t^2 &= \tilde{x}^3 - \left(\beta^2+\beta+1\right)^3 \cdot \left(\tilde{x} - \left(\beta^2+\beta\right)^2\right)^2 + t^2\left(\tilde{x} - \left(\beta^2+\beta\right)^2\right)^2.\end{aligned}$$

So we have: $\tilde{y} = \tilde{x} - \left(\beta^2+\beta\right)^2$ and $\tilde{x}^3 - \left(\beta^2+\beta+1\right)^3 \cdot \left(\tilde{x} - \left(\beta^2+\beta\right)^2\right)^2 = 0$ so $\tilde{x}^3 = \left(\beta^2+\beta+1\right)^3 \cdot \left(\tilde{x} - \left(\beta^2+\beta\right)^2\right)^2$. Solving this for $\tilde{x}$ with help of maple gives us:

$$\begin{aligned}\tilde{x}_1 &= \beta^2\left(\beta^2+\beta+1\right)(\beta+1)^2 \\ \tilde{x}_2 &= \beta^2\left(\beta^2+\beta+1\right) \\ \tilde{x}_3 &= \left(\beta^2+\beta+1\right)(\beta+1)^2.\end{aligned}$$

So the 7 points on this curve are:

$$\begin{aligned}Q = (x,y) &= \left(\left(\beta^2+\beta\right)^2, \left(\beta^2+\beta\right)^3\right) \\ P_1 = (x,y) &= \left(\tilde{x}_1, \pm\left(\tilde{x}_1 - \left(\beta^2+\beta\right)^2\right)\cdot t\right) \\ P_2 = (x,y) &= \left(\tilde{x}_2, \pm\left(\tilde{x}_2 - \left(\beta^2+\beta\right)^2\right)\cdot t\right) \\ P_3 = (x,y) &= \left(\tilde{x}_3, \pm\left(\tilde{x}_3 - \left(\beta^2+\beta\right)^2\right)\cdot t\right).\end{aligned}$$

With magma we checked whether these points are independent, we saw $P_1 + P_2 + P_3 = \mathcal{O}$, so we can leave P_3 out in our computations.

To check whether a curve has a certain rank over $\mathbb{Q}(\beta, t)$ we have to check if P_1, P_2 and Q are independent.
To prove this we will reduce the curve E to certain primes and look if we can find primes such that the points P_1, P_2 and Q can produce three different vectors modulo those primes. This we will do with help of the image α, which was given by: $\alpha(P) =$

$\left(y + (x - B)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3}$. Doing this we immediately see a problem, namely that the point Q always gives a trivial image of α, since:

$$\begin{aligned}\alpha(Q) = \alpha\left(\left(\beta^2+\beta\right)^2, \left(\beta^2+\beta\right)^3\right) &= \left(\left(\beta^2+\beta\right)^3 + \left(\left(\beta^2+\beta\right)^2 - \left(\beta^2+\beta\right)^2\right)\sqrt{A}\right) \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} \\ &= \left(\beta^2+\beta\right)^3 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3} \\ &= 1 \cdot \mathbb{Q}\left(\sqrt{A}\right)^{*3}.\end{aligned}$$

So we can never prove that those 3 points produce three different vectors modulo certain primes. We tried a lot of different curves to produce 2 different vectors, but we were not successful. After some attempts we succeeded in finding 1 example, which we will show here and explain. We hope that after this the procedure is a little bit more clear.

6.2.1 The case $\beta = 3, t = 2$

So lets start with defining the elliptic curve with $\beta = 3, t = 2$:

$$y^2 = x^3 + \left(t^2 - \left(\beta^2+\beta+1\right)^3\right)\left(x - \left(\beta^2+\beta\right)^2\right)^2 = x^3 - 2193\,(x-144)^2\,. \tag{6.3}$$

On this curve we have the points $P_1 = (1872, 3456)$, $P_2 = (117, -54)$ and $Q = (144, 1728)$. The discriminant of this curve is $\Delta = 2^{14} \cdot 3^9 \cdot 11 \cdot 17^2 \cdot 37 \cdot 43$. So we don't have to reduce modulo the primes $2, 3, 11, 17, 37$ and 43. Since Q is always trivial if we compute $\alpha(Q)$ we don't have to consider this.

- mod 5: the points P_1, P_2 reduce to $P_1 \equiv (2,1) \mod 5$ and $P_2 \equiv (2,1) \mod 5$, so reducing modulo 5 is not interesting, since the two points are the same modulo 5.
- mod 7: the points P_1, P_2 reduce to $P_1 \equiv (3,5) \mod 7$ and $P_2 \equiv (5,2) \mod 7$. Reducing the elliptic curve $y^2 = x^3 - 2193\,(x-144)^2$ gives $\tilde{y}^2 = \tilde{x}^3 + \tilde{5}\left(\tilde{x} + \tilde{3}\right)^2$. We checked with help of maple that 5 is not a square modulo 7. So our image of α becomes $\alpha(x,y) = \left(y + (x+3)\sqrt{5}\right) \cdot \mathbb{Q}\left(\sqrt{5}\right)^{*3}$.

$$\begin{aligned}P_1 : \alpha(3,5) &= 5 + 6 \cdot \sqrt{5} \equiv 1 \cdot \mathbb{Q}\left(\sqrt{5}\right)^{*3} \\ P_2 : \alpha(5,2) &= 2 + 5 \cdot \sqrt{5} \text{ not trivial.}\end{aligned}$$

- mod 13: the points P_1, P_2 reduce to $P_1 \equiv (0,11) \mod 13$ and $P_2 \equiv (0,11) \mod 13$, so reducing modulo 13 is not interesting, since the two points are the same modulo 13.
- mod 19: the points P_1, P_2 reduce to $P_1 \equiv (10,17) \mod 19$ and $P_2 \equiv (3,3) \mod 19$. Reducing the elliptic curve $y^2 = x^3 - 2193\,(x-144)^2$ gives $\tilde{y}^2 = \tilde{x}^3 + \tilde{11}\left(\tilde{x} + \tilde{8}\right)^2$.

We checked with help of maple that $12^2 \equiv 11 \mod 19$. So our image of α becomes $\alpha(x,y) = (y + (x+8)\cdot 12)\cdot \mathbb{Q}^{*3}$.

$$P_1 : \alpha(10,17) = 17 + 18\cdot 12 \equiv 5\cdot \mathbb{Q}^{*3}$$
$$P_2 : \alpha(3,3) = 3 + 11\cdot 12 \equiv 2\cdot \mathbb{Q}^{*3}.$$

In this case we have $\mathbb{F}_{19}^*/\mathbb{F}_{19}^{*3} = \mathbb{F}_{19}^*/_{\{0,1,6\}} \cong \mathbb{Z}/3\mathbb{Z}$. We need to check whether the images of α of P_1 and P_2 are the same or not, so $\frac{5}{2} \mod 19 \equiv 12$ which is not a third power, and thus the images of P_1 and P_2 are different.

So we see:

$$\mathbb{Z}\cdot P_1 + \mathbb{Z}\cdot P_2 \to \mathbb{F}_3 \oplus \mathbb{F}_3$$
$$P_1 \mapsto 0 \oplus 1$$
$$P_2 \mapsto 1 \oplus 2.$$

This is how the method works. For this example we can't prove that we have three different points, since the point Q always maps to a trivial image.

In the next section we will try to make examples for which this method works to show that a curve has a certain rank.

6.2.2 The case $\beta = 9$

We tried to find more examples with the curve

$$y^2 = x^3 + \left(t^2 - \left(\beta^2+\beta+1\right)^3\right)\left(x - \left(\beta^2+\beta\right)^2\right)^2.$$

In the case that $\beta = 9$ we find for t from 1 to 50: 11 curves of rank 3, 31 curves of rank 4, 7 curves of rank 5 and 1 curve with rank 7! The curve of rank 7 is given by

$$y^2 = x^3 - 753247(x-8100)^2.$$

In the case that $\beta = 9$ the family of elliptic curves is given by

$$E : y^2 = x^3 + (t^2 - 753571)(x-8100)^2.$$

With magma we can show that this curve always has 3 independent points:

```
D:=Rationals();
A<a,b,c,d,e,f,g>:=AffineSpace(D,7);
R:=CoordinateRing(A);
P<x,y,z>:=PolynomialRing(R,3);
F:=P!(x^3+(z^2-753571)*(x-8100)^2-y^2);
R<t>:=PolynomialRing(CoordinateRing(A));
pt:=[a*t^2+b*t+c,d*t^3+e*t^2+f*t+g,t];
```

```
ideal:=Ideal( Coefficients (Evaluate(F,pt)));
Z:=Scheme(A,ideal);
points:=Points(Z);
points;
Qt<t>:=FunctionField(Rationals());
R<x>:=PolynomialRing(Qt);
pol:=R!(x^3+(t^2−753571)*(x−8100)^2);
E:=EllipticCurve(pol);
P1:=E![points[2,1]*t^2 + points[2,2]*t+points[2,3],  points[2,4]*t^3 + points[2,5]*t^2+points[2,6]*t
    + points [2,7]]; P1;
P2:=E![points[4,1]*t^2 + points[4,2]*t+points[4,3],  points[4,4]*t^3 + points[4,5]*t^2+points[4,6]*t
    + points [4,7]]; P2;
P3:=E![points[6,1]*t^2 + points[6,2]*t+points[6,3],  points[6,4]*t^3 + points[6,5]*t^2+points[6,6]*t
    + points [6,7]]; P3;
IsLinearlyIndependent([P1,P2,P3]);
```

Which gives output:

```
{@ (−1, 0, 755596, 0, −135, 0, 101640960), (−1, 0, 755596, 0, 135, 0,
−101640960), (−2916000/2989441, 0, 737100, −790236000/5168743489, 0, 2187000/19,
0), (−2916000/2989441, 0, 737100, 790236000/5168743489, 0, −2187000/19, 0),
(−4000/1002001, 0, 9100, −3996000/1003003001, 0, 27000/11, 0), (−4000/1002001,
0, 9100, 3996000/1003003001, 0, −27000/11, 0), (0, −2000, 1738100, 0, −2000,
3730000, −1730729000), (0, −2000, 1738100, 0, 2000, −3730000, 1730729000), (0,
−1458, 1267812, 0, −1458, 2322594, −917601048), (0, −1458, 1267812, 0, 1458,
−2322594, 917601048), (0, −2, 8372, 0, −2, 274, 728728), (0, −2, 8372, 0, 2,
−274, −728728), (0, 0, 7371, 0, 0, −729, 0), (0, 0, 7371, 0, 0, 729, 0), (0, 0,
8100, 0, 0, 0, −729000), (0, 0, 8100, 0, 0, 0, 729000), (0, 0, 9100, 0, 0,
−1000, 0), (0, 0, 9100, 0, 0, 1000, 0), (0, 0, 737100, 0, 0, −729000, 0), (0, 0,
737100, 0, 0, 729000, 0), (0, 2, 8372, 0, −2, −274, 728728), (0, 2, 8372, 0, 2,
274, −728728), (0, 1458, 1267812, 0, −1458, −2322594, −917601048), (0, 1458,
1267812, 0, 1458, 2322594, 917601048), (0, 2000, 1738100, 0, −2000, −3730000,
−1730729000), (0, 2000, 1738100, 0, 2000, 3730000, 1730729000), (729/132496, 0,
7371, −266085/48228544, 0, 10935/4, 0), (729/132496, 0, 7371, 266085/48228544,
0, −10935/4, 0) @}
(−t^2 + 755596 : 135*t^2 − 101640960 : 1)
(−2916000/2989441*t^2 + 737100 : 790236000/5168743489*t^3 − 2187000/19*t : 1)
(−4000/1002001*t^2 + 9100 : 3996000/1003003001*t^3 − 27000/11*t : 1)
true
```

From the output we see that the points:

$$P_1 := (-t^2 + 755596, 135 * t^2 - 101640960)$$

$$P_2 := (-2916000/2989441 * t^2 + 737100, 790236000/5168743489 * t^3 - 2187000/19 * t)$$

$$P_3 := (-4000/1002001 * t^2 + 9100, 3996000/1003003001 * t^3 - 27000/11 * t)$$

are independent. From this we see we have at least rank 3 on this elliptic curve.

6.3 Elliptic curves of the form $y^2 = x^3 + \left(at^2 + b\right)\left(x - \left(ct^2 + dt + e\right)\right)^2$

Our goal with the elliptic curve

$$y^2 = x^3 + \left(at^2 + b\right)\left(x - \left(ct^2 + dt + e\right)\right)^2 \tag{6.4}$$

is to find a point $(x(t), y(t))$ with $x(t)$ a polynomial of degree less than or equal to 2. So $x(t) = ft^2 + gt + h$ and $y(t) = it^3 + jt^2 + kt + l$. If we fill this out in equation 6.4 we get 7 equations of 12 variables $a, b, \ldots, l$. We want to solve this for certain variables such that on the remaining family of elliptic curves there exist as many independent points as possible. We compute this problem with magma as follows:

```
k:=RationalField();
A<a,b,c,d,e,f,g,h,i,j,k,l>:=AffineSpace(k,12);
R:=CoordinateRing(A);
P<x,y,z>:=PolynomialRing(R,3);
F:=P!(x^3+(a*z^2+b)*(x-(c*z^2+d*z+e))^2-y^2);
R<t>:=PolynomialRing(CoordinateRing(A));
pt:=[f*t^2+g*t+h,i*t^3+j*t^2+k*t+l,t];
ideal:=Ideal( Coefficients (Evaluate(F,pt)));
ideal;
```

This gives the output:

```
Ideal of Polynomial ring of rank 12 over Rational Field
Order: Lexicographical
Variables: a, b, c, d, e, f, g, h, i, j, k, l
Basis:
[
b*e^2 - 2*b*e*h + b*h^2 + h^3 - l^2,
2*b*d*e - 2*b*d*h - 2*b*e*g + 2*b*g*h + 3*g*h^2 - 2*k*l,
a*e^2 - 2*a*e*h + a*h^2 + 2*b*c*e - 2*b*c*h + b*d^2 - 2*b*d*g - 2*b*e*f +
    2*b*f*h + b*g^2 + 3*f*h^2 + 3*g^2*h - 2*j*l - k^2,
2*a*d*e - 2*a*d*h - 2*a*e*g + 2*a*g*h + 2*b*c*d - 2*b*c*g - 2*b*d*f +
    2*b*f*g + 6*f*g*h + g^3 - 2*i*l - 2*j*k,
2*a*c*e - 2*a*c*h + a*d^2 - 2*a*d*g - 2*a*e*f + 2*a*f*h + a*g^2 + b*c^2 -
    2*b*c*f + b*f^2 + 3*f^2*h + 3*f*g^2 - 2*i*k - j^2,
2*a*c*d - 2*a*c*g - 2*a*d*f + 2*a*f*g + 3*f^2*g - 2*i*j,
a*c^2 - 2*a*c*f + a*f^2 + f^3 - i^2
]
```

We thus have to solve these 7 equations. Unfortunately we did not manage to do this and so this problem will require additional research.

Chapter 7

Conclusion

As mentioned in the introduction we had three goals during this thesis:

1. Making the theory of computing the rank of $E_{A,B}(\mathbb{Q})$ more precise and more practical.
2. Making a computer program in magma to compute the rank with help of this theory.
3. Finding families of elliptic curves that have higher rank.

We started with the second point, because doing this makes the theory more clear and made it easier to improve the theory about computing the rank of an elliptic curve.

The code we made is explained in chapter 4 and can be found in appendix A in total. This code is useful for computing the rank of an elliptic curve. Unfortunately it does not work as well as expected. Since the code is pretty extensive it uses a lot of memory. The free version of magma limits memory usage. The rank of more complex elliptic curves cannot be computed with this code due to the lack of memory. We also noticed the computing time becomes longer for more complex elliptic curves. One reason for this is that we need to compute all the points of the elliptic curves, which is a very time-consuming process. This causes another problem, since it is not always possible to compute all the points on an elliptic curve. With the program we always get an upper bound and a lower bound for the rank, and if they are not the same we know we have $r_{\text{low}} \leq r \leq r_{\text{upp}}$. So even in this case the code is useful. For continuing research on this subject, a good starting point is making the code more efficient so the rank of more complex elliptic curves can also be computed.

The clarification of the computation of the rank of $E(\mathbb{Q})$ is worked out in chapter 2 and 3. The theory has become more clear and is more comprehensible for further research. In section 3.4 a roadmap can be found that gives a step by step explanation of

how the rank of $E(\mathbb{Q})$ can be computed.

The last goal of this thesis was making families of elliptic curves with higher rank. Unfortunately since the first two points cost a lot of time we didn't have that much time left to find elliptic curves with higher rank. Despite this we had a few tries and managed to find four curves with rank 6 and even one curve with rank 7!

So for making the theory more clear and making a computer program we were pretty successful. Even though the computer program does not always give a good rank, it always gives upper and lower bounds for the rank. Unfortunately we didn't have enough time for making families of elliptic curves.
For further research it would be a good idea to start by making the computer program stated in appendix A more efficient. After that, the improved program can be used to make families of elliptic curves with higher rank. Maybe some ideas to start can be found in chapter 6.

Bibliography

[alg] Dictaat Algebraïsche structuren.

[Cha00] R. Chapman. Algebraic number theory, May 2000. http://empslocal.ex.ac.uk/people/staff/rjchapma/notes/ant.pdf.

[Fri] S. Friedl. An elementary proof of the group law for elliptic curves.

[Sil08] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2008.

[ST92] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer-Verslag, 1992.

[Ste] P. Stevenhagen. Number rings.

[Ste04] W. Stein. Dedekind domains, May 2004. http://modular.math.washington.edu/129/ant/html/node17.html.

[Top91] J. Top. Descent by 3-isogeny and 3-rank of quadratic fields. *Advances in number theory*, Kingston, ON, 1991:303–317, 1991.

[vB10] Monique van Beek. On elliptic curves of the form $y^2 = x^3 + a(x - b)^2$. Master's thesis, University of Groningen, 2010. http://irs.ub.rug.nl/dbi/4c37197241b5a.

Appendix A

Code in magma for computing the rank

```
RankComputation := function(A,B)

R<x>:=PolynomialRing(Rationals());
K<c>:=QuadraticField(A);
L<d>:=IntegerRing(K);

ListU:=[];
if Discriminant(L) gt 0 then
   Append(~ListU,FundamentalUnit(L));
else
   Append(~ListU,d^0);
end if;

ListP:=[];

C,c1:=ClassGroup(L);
numC:=# Generators(C);
for i in [1 .. numC] do
   Append(~ListP,c1(C.i));
end for;

Id:=Factorization(A);
Id2:=Factorization(A*B);

ListQ:=[];
ListR:=[];

P<x>:=PolynomialRing(Integers());
poly:=P!MinimalPolynomial(d);

for i in [1 .. # Id] do
   g:=Id[i,1];
   e:=poly mod g;
   Q<y> := PolynomialRing(GF(g));
   for k in [1 .. # Factorization(Q!e)] do
      Ge:=Factorization(Q!e)[k,1];
      pol:=P!Ge;
```

```
        GeU:=Evaluate(pol,d);
        I:=ideal< L| GeU,g>;
        if IsRamified(I) eq true and IsPrincipal(I) eq false then
            Append(~ListQ,I);
        end if;
    end for;
end for;

for i in [1 .. # Id2] do
    g:=Id2[i ,1];
    e:=poly mod g;
    Q<y> := PolynomialRing(GF(g));
    for k in [1 .. # Factorization(Q!e)] do
        Ge:=Factorization(Q!e)[k,1];
        pol:=P!Ge;
        GeU:=Evaluate(pol,d);
        I:=ideal< L| GeU,g>;
        if IsSplit(I) eq true then
            Append(~ListR,I);
        end if;
    end for;
end for;

ListPhelp:=ListP;

for i in [1 .. # ListPhelp] do
    for j in [1 .. # ListQ] do
        if # ListPhelp ne 0 then
            if ListPhelp[i] eq ListQ[j] then
                ListP:=Exclude(ListP,ListPhelp[i]);
            end if;
        end if;
    end for;
end for;

Listep1:=[];
Listep2:=[];
Listep3:=[];

if # ListP eq 0 then
    n:=0;
    Append(~Listep1,n);
else
    for i in [1 .. # ListP] do
        n:=1; J:=ListP[i];
        while not IsPrincipal(J) do
            n:=n+1; J:=J*ListP[i];
        end while;
        Append(~Listep1,n);
    end for;
end if;

if # ListQ eq 0 then
    m:=0;
    Append(~Listep2,m);
else
    for i in [1 .. # ListQ] do
        m:=1; J:=ListQ[i];
        while not IsPrincipal(J) do
```

```
            m:=m+1; J:=J*ListQ[i];
        end while;
        Append(~Listep2,m);
    end for;
end if;

if # ListR eq 0 then
    z:=0;
    Append(~Listep3,3*z);
else
    for i in [1 .. # ListR] do
        z:=1; J:=ListR[i];
        while not IsPrincipal(J) do
            z:=z+1; J:=J*ListR[i];
        end while;
        Append(~Listep3,3*z);
    end for;
end if;

Listimagealphaunits:=[];
Listideals :=[];
Listpowers:=[];

if ListU[1] eq 1 then
    Append(~Listimagealphaunits,ListU[1]);
end if;
if ListU[1] ne 1 then
    for a in [0 .. 2] do
        Append(~Listimagealphaunits,ListU[1]^a);
    end for;
end if;

for i in [1 .. # ListP] do
    Listideals :=Append(Listideals,ListP[i]);
end for;
for i in [1 .. # ListQ] do
    Listideals :=Append(Listideals,ListQ[i]);
end for;
for i in [1 .. # ListR] do
    Listideals :=Append(Listideals,ListR[i]);
end for;

for i in [1 .. # Listep1] do
    if Listep1[i] ne 0 then
        Listpowers:=Append(Listpowers,Listep1[i]*3-1);
    end if;
end for;
for i in [1 .. # Listep2] do
    if Listep2[i] ne 0 then
        Listpowers:=Append(Listpowers,Listep2[i]*3-1);
    end if;
end for;
for i in [1 .. # Listep3] do
    if Listep3[i] ne 0 then
        Listpowers:=Append(Listpowers,Listep3[i]-1);
    end if;
end for;

Listnorms:=[];
```

```
for i in [1 .. # Listideals] do
   Listnorms:=Append(Listnorms,Norm(Listideals[i]));
end for;

Listhelp :=[];

for i in [1 .. # Listnorms] do
   for j in [1 .. # Listnorms] do
      if i ne j and j ge i then
         if Listnorms[i] eq Listnorms[j] then
            Listhelp:=Include(Listhelp,<i,j>);
         end if;
      end if;
   end for;
end for;

Listrealpowers :=[];

if # Listhelp eq 0 then
   for i in [1 .. # Listpowers] do
      for j in [0 .. Listpowers[i ]] do
         if Gcd(3,j) ne 1 then
            Listrealpowers:=Include(Listrealpowers,<i,j>);
         end if;
      end for;
   end for;
else
   for i in [1 .. # Listpowers] do
      for k in [1 .. # Listhelp] do
         if i ne Listhelp[k,1] and i ne Listhelp[k,2] then
            for j in [0 .. Listpowers[i ]] do
               if Gcd(3,j) ne 1 then
                  Listrealpowers:=Include(Listrealpowers,<i,j>);
               end if;
            end for;
         else
            if i eq Listhelp[k,1] then
               for h in [0 .. Listpowers[Listhelp[k ,1]]] do
                  for l in [0 .. Listpowers[Listhelp[k ,2]]] do
                     if Gcd(3,h+l) ne 1 then
                        if h lt 3 or l lt 3 then
                           Listrealpowers:=Append(Listrealpowers,<Listhelp[k,1],h>);
                           Listrealpowers:=Append(Listrealpowers,<Listhelp[k,2],l>);
                        end if;
                     end if;
                  end for;
               end for;
            end if;
         end if;
      end for;
   end for;
end if;

Listallpowers:=AssociativeArray();

for i in [1 .. # Listideals] do
   Listallpowers[i]:=<>;
   for j in [1 .. # Listrealpowers] do
```

```
        if Listrealpowers[j,1] eq i then
            Listallpowers[i]:=Append(Listallpowers[i],Listrealpowers[j,2]) ;
        end if;
    end for;
end for;

number:=1;
if # Listhelp eq 0 then
    for i in [1 .. # Listideals] do
        number:=number*# Listallpowers[i];
    end for;
else
    for j in [1 .. # Listhelp] do
        for k in [1 .. # Listideals] do
            if k ne Listhelp[j,2] then
                number:=number*# Listallpowers[k];
            end if;
        end for;
    end for;
end if;

state :=[];

if # Listhelp eq 0 then
    for i in [1 .. # Listideals] do
        state:=Append(state,i-i+1);
    end for;
else
    for j in [1 .. # Listhelp] do
        for i in [1 .. # Listideals] do
            if i ne Listhelp[j,2] then
                state:=Append(state,i-i+1);
            end if;
        end for;
    end for;
end if;

 Listpossibilities :=AssociativeArray();

for i in [1 .. number] do
     Listpossibilities [i]:=<>;
end for;

i:=1;
n:=0;

for n in [1 .. number] do
    while i ne # state + 1 and state[i] eq # Listallpowers[i] do
        i := i + 1;
    end while;
    if   i ne # state + 1 then
        state[i] := state[i] + 1;
    end if;
    while i ne 1 do
        i := i - 1;
        state[i] := 1;
    end while;
    if # Listhelp eq 0 then
        for j in [1 .. # state] do
```

```
            Listpossibilities [n]:=Append(Listpossibilities[n], Listallpowers[j,state[j]]);
        end for;
    else
        for k in [1 .. # Listhelp] do
            for j in [1 .. # state] do
                Listpossibilities [n]:=Append(Listpossibilities[n], Listallpowers[j,state[j]]);
                if j eq Listhelp[k,1] then
                    Listpossibilities [n]:=
                    Append(Listpossibilities[n], Listallpowers[Listhelp[k,2], state[Listhelp[k,1]]]);
                end if;
            end for;
        end for;
    end if;
end for;

if # Listideals ne 0 then
    Listidealsleft :=[ &*[Listideals[j]^ Listpossibilities [i,j] : j in [1..# Listideals ]] : i in
        [1.. number] ];
else
    Listidealsleft :=[];
end if;

image:=[];
Z<T>:=PolynomialRing(K);

Listimagehelp:=[];
if # Listidealsleft ne 0 then
    for i in [1 .. # Listidealsleft ] do
        b,g:=IsPrincipal( Listidealsleft [i]);
        if b eq true then
            Listimagehelp:=Include(Listimagehelp,g);
        end if;
    end for;
end if;

if # Listimagehelp eq 0 then
    Listimagehelp:=Include(Listimagehelp,1);
end if;

Listimage:=[];

for i in [1 .. # Listimagealphaunits] do
    for j in [1 .. # Listimagehelp] do
        Listimage:=Include(Listimage,Listimagealphaunits[i]*Listimagehelp[j]);
    end for;
end for;

PP<s>:=PolynomialRing(L);
Helplist:=Listimage;

for i in [1 .. # Listimage] do
    for j in [1 .. # Listimage] do
        if i ne j and i gt j then
            if # Factorisation(s^3-(Listimage[i])*(Listimage[j])^2) ge 2 then
                Helplist:=Exclude(Helplist,Listimage[j]);
            end if;
        end if;
    end for;
end for;
```

```
Aind:=-Evaluate(Factorization(s^2-A)[1,1],0);
E:=EllipticCurve(x^3+A*(x-B)^2);

PointsE:=RationalPoints(E:Bound:=100000);
PointsE:=PointsE join {P+Q : P in PointsE, Q in PointsE} join {-P + Q : P in PointsE, Q in
    PointsE};
for i in [2 .. # PointsE] do
   P:=PointsE[i];
   aP:=Denominator(P[2])*(P[2]+(P[1]-B)*Aind);
   for j in [1 .. # Helplist] do
      if IsIrreducible (T^3-aP/Helplist[j]) eq false then
         image:=Include(image,Helplist[j]) ;
         break;
      end if;
   end for;
end for;

image:=Include(image,1);
agamma:=# image;
lambda:=# Helplist;

return agamma, lambda;

end function;

A := 8;
B := 1;

agamma, lambda := RankComputation(A, B);
agammastreep, lambdastreep := RankComputation(-27*A, 4*A+27*B);

upperboundrank:=Log(3,lambda*lambdastreep);
lowerboundrank:=Log(3,agamma*agammastreep);

"Upperbound rank";
upperboundrank;

"Lowerbound rank";
lowerboundrank;

"Rank of Ellipticcurve E is";
if upperboundrank eq lowerboundrank then
   lowerboundrank;
else
   "Rank not determined";
end if;
```