Technische Universiteit Delft
Faculteit Elektrotechniek, Wiskunde en Informatica
Delft Institute of Applied Mathematics

Elliptische krommen met hoge rang

(Engelse titel: Elliptic curves with high rank)

Verslag ten behoeve van het
Delft Institute of Applied Mathematics
als onderdeel ter verkrijging

van de graad van

BACHELOR OF SCIENCE
in
TECHNISCHE WISKUNDE

door

MICHEL ARTHUR BIK

Delft, Nederland
Juli 2014

BSc verslag TECHNISCHE WISKUNDE

“Elliptische krommen met hoge rang”
(Engelse titel: “Elliptic curves with high rank”)

MICHEL ARTHUR BIK

Technische Universiteit Delft

Begeleiders

Dr. R.M. van Luijk	Dr. K.P. Hart

Overige commissieleden

Dr. C. Kraaikamp	Dr. B. van den Dries

Juli, 2014 Delft

Contents

Chapter 1

Introduction

Consider the set $E_{\mathrm{p}}(\mathbb{Q})$, which is the set of of solutions to the equation $y^2 = x^3 - x + 1$ over $\mathbb{Q}$ together with a special point $\mathcal{O}$. It turns out that $E_{\mathrm{p}}(\mathbb{Q})$ has an natural abelian group structure where $\mathcal{O}$ acts as the zero element.

The curve given by $y^2 = x^3 - x + 1$ is an example of a elliptic curve. In general, an elliptic curve over a field K is a pair $(E_{\mathrm{p}}, \mathcal{O})$, where E_{p} is a smooth projective curve defined over K with genus 1 and $\mathcal{O} \in E_{\mathrm{p}}(K)$. In this case $E_{\mathrm{p}}(K)$ will always have an natural abelian group structure. For K a number field such as $\mathbb{Q}$, the Mordell-Weil theorem tells us that $E_{\mathrm{p}}(K)$ is finitely generated. In this case $E_{\mathrm{p}}(K)$ is isomorphic as a group to $T \times \mathbb{Z}^r$ for some non-negative integer r, where T is the torsion subgroup of $E_{\mathrm{p}}(K)$. We call r the rank of the elliptic curve over K. Now one might ask:

- Do elliptic curves over $\mathbb{Q}$ of arbitrary high rank exist?
- For every integer r, can we find infinite families of elliptic curves over $\mathbb{Q}$ with rank at least r?
- For every finite abelian group T, do elliptic curves over $\mathbb{Q}$ of arbitrary high rank with torsion-subgroup T exist?
- For every r and T, can we find infinite families of elliptic curves over $\mathbb{Q}$ with torsion-subgroup T and rank at least r?

For most T the answer to the third and fourth question is no.

Theorem 1.1 (Mazur's Theorem)**.** Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion-subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:

$$\begin{array}{rll} \mathbb{Z}/N\mathbb{Z} & \text{with} & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{with} & 1 \leq N \leq 4 \end{array}$$

Proof. See Theorem VIII.7.5 of [1]. □

For the finitely many T that can actually occur as torsion subgroups, the answers to these questions are as of this moment unknown. However for each possible torsion-subgroup T (families of) elliptic curves over $\mathbb{Q}$ were found with relatively high rank. The following page lists the world records per T.

`http://web.math.pmf.unizg.hr/~duje/tors/tors.html`

In this thesis we will look at methods for constructing elliptic curves over $\mathbb{Q}$ with high ranks. Using these methods we find an elliptic curve with rank at least 13, an infinite family of elliptic curves with rank at least 9, an elliptic curve with rank at least 10 and torsion-subgroup $\mathbb{Z}/2\mathbb{Z}$ and an infinite family of elliptic curves with rank at least 8 and with torsion point of order 2.

1.1 Conventions

Let $\mathbb{N} = \{1, 2, 3, \dots\}, \mathbb{N}_0 = \{0\} \cup \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ be the sets of positive integers, non-negative integers, integers, rational numbers, real numbers and complex numbers. We will always let K be a perfect field with a fixed algebraic closure $\overline{K}$. Denote the set of units of a ring R by R^*. We will always let n and m be elements of $\mathbb{N}$. The degree of a polynomial $f \in K[x_1, \dots, x_n]$ is its total degree and is denoted by $\deg(f)$.

Chapter 2

Algebraic geometry

To discuss elliptic curves we first need some knowledge from algebraic geometry, which explains the existence of the first two chapters of [1]. For the sake of completeness and to introduce needed notation, which slightly differs from the notation used in [1], we repeat the relevant parts of these two chapters here.

2.1 Affine varieties

Definition 2.1. The affine n-dimensional space over K with coordinates $x_1, \ldots, x_n$ is defined as

$$\mathbb{A}^n_{x_1,\ldots,x_n} = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in \overline{K}\}.$$

The set of K-rational points of $\mathbb{A}^n_{x_1,\ldots,x_n}$ is

$$\mathbb{A}^n_{x_1,\ldots,x_n}(K) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n_{x_1,\ldots,x_n} : x_1, \ldots, x_n \in K\}.$$

Note that $\mathbb{A}^n_{x_1,\ldots,x_n} = \mathbb{A}^n_{x_1,\ldots,x_n}(\overline{K})$.

We write $\mathbb{A}^n$ instead of $\mathbb{A}^n_{x_1,\ldots,x_n}$ when the variables used are $x_1, \ldots, x_n$. However, when for example $n = 2$, we often use the variables x and y instead of x_1 and x_2. So in this case we write $\mathbb{A}^2_{x,y}$, because for example the set of solutions of $x = 0$ is $\overline{K} \times \{0\}$ or $\{0\} \times \overline{K}$ depending on the ordering of x and y.

Definition 2.2. Let $I \subseteq \overline{K}[x_1, \ldots, x_n]$ be an ideal, then define

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Any set V_a of the form V_I is called an affine algebraic set. For an algebraic set V_a we define

$$I(V_\mathrm{a}) = \{f \in \overline{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V_\mathrm{a}\}.$$

We say that V_a is defined over K if $I(V_\mathrm{a})$ can be generated by polynomials in $K[x_1, \ldots, x_n]$.

The subscript a of V_a is notation to show that V_a is an affine algebraic set and we will only give objects subscript a if they are affine algebraic sets, while a subscript p will always indicate a projective algebraic set, which will be defined in the next section. Also when we write V_a/K we will mean that V_a is defined over K.

Definition 2.3. Let V_a/K be an algebraic set. We define the set of K-rational points on V_a as $V_\mathrm{a}(K) = V_\mathrm{a} \cap \mathbb{A}^n(K)$ and we define $I(V_\mathrm{a}/K) = I(V_\mathrm{a}) \cap K[x_1, \ldots, x_n]$.

Note that if $K \subseteq L \subseteq \overline{K}$ is an extension of fields, then V_{a} is also defined over L. In particular, $V_{\mathrm{a}}(L) = V_{\mathrm{a}} \cap \mathbb{A}^n(L)$ and $I(V_{\mathrm{a}}/L) = I(V_{\mathrm{a}}) \cap L[x_1, \ldots, x_n]$.

Definition 2.4. An affine algebraic set V_{a} is called an affine variety if $I(V_{\mathrm{a}})$ is prime. Let V_{a}/K be a variety, i.e., let V_{a} be an affine variety defined over K. Define the coordinate ring of V_{a}/K as $K[V_{\mathrm{a}}] = K[x_1, \ldots, x_n]/I(V_{\mathrm{a}}/K)$. Because $I(V_{\mathrm{a}})$ is prime, $K[V_{\mathrm{a}}]$ is an integral domain. Define the function field $K(V_{\mathrm{a}})$ of V_{a}/K as the field of fractions of $K[V_{\mathrm{a}}]$.

Definition 2.5. Let V_{a} be a variety, then the dimension $\dim(V_{\mathrm{a}})$ of V_{a} is the transcendence degree of $\overline{K}(V_{\mathrm{a}})$ over $\overline{K}$. If $\dim(V_{\mathrm{a}}) = 1$, then V_{a} is called an affine curve.

Definition 2.6. Let V_{a} be a variety, let $P \in V_{\mathrm{a}}(\overline{K})$ and let $f_1, \ldots, f_m \in \overline{K}[x_1, \ldots, x_n]$ be generators of $I(V_{\mathrm{a}})$. Then V_{a} is smooth at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

has rank $n - \dim(V_{\mathrm{a}})$. If V_{a} is not smooth at P, then we call P a singular point of V_{a}. We say that V_{a} is smooth if V_{a} is smooth at every point in $V_{\mathrm{a}}(\overline{K})$.

Next we want to define morphisms of affine varieties. To do so we first need to define the Zariski topology on $\mathbb{A}^n$.

Proposition 2.7 (Proposition I.1.1 of [2])**.** The union of two affine algebraic sets is an affine algebraic set. The intersection of any family of affine algebraic sets is an affine algebraic set. The empty set and $\mathbb{A}^n$ are affine algebraic sets.

Definition 2.8. Define the Zariski topology on $\mathbb{A}^n$ by taking the open subsets to be the complements of the affine algebraic sets of $\mathbb{A}^n$. For every variety V_{a}, define the topology on $V_{\mathrm{a}}(\overline{K})$ as the induced topology.

Definition 2.9. Let V_{a} and $V'_{\mathrm{a}} \subseteq \mathbb{A}^n$ be varieties. For $f_1, \ldots, f_n$ elements of $\overline{K}(V_{\mathrm{a}})$ and $U \subseteq V_{\mathrm{a}}(\overline{K})$ a non-empty open subset of $V_{\mathrm{a}}(\overline{K})$ such that $f_1, \ldots, f_n$ can be evaluated at every point in U and $(f_1(P), \ldots, f_n(P)) \in V'_{\mathrm{a}}(\overline{K})$ for every $P \in U$, a rational map $f : V_{\mathrm{a}} \dashrightarrow V'_{\mathrm{a}}$ is a map $f : U \to V'_{\mathrm{a}}(\overline{K})$ sending $P \mapsto (f_1(P), \ldots, f_n(P))$. We say that f is defined over K if $f_1, \ldots, f_n \in K(V_{\mathrm{a}})$.

Definition 2.10. Let V_{a} and $V'_{\mathrm{a}} \subseteq \mathbb{A}^n$ be varieties. For $U_1, \ldots, U_m \subseteq V_{\mathrm{a}}(\overline{K})$ open in $V_{\mathrm{a}}(\overline{K})$ such that $\bigcup_{i=1}^m U_i = V_{\mathrm{a}}(\overline{K})$ and for $f_1 : U_1 \to V'_{\mathrm{a}}, \ldots, f_m : U_m \to V'_{\mathrm{a}}$ rational maps $V_{\mathrm{a}} \dashrightarrow V'_{\mathrm{a}}$ such that f_i and f_j restrict to the same map on $U_i \cap U_j$ for every i and j, a morphism $f : V_{\mathrm{a}} \to V'_{\mathrm{a}}$ is a map $f : V_{\mathrm{a}} \to V'_{\mathrm{a}}$ sending $P \in U_i$ to $f_i(P)$. We say that f is defined over K if $f_1, \ldots, f_m$ are defined over K.

Definition 2.11. A morphism $f : V_{\mathrm{a}} \to V'_{\mathrm{a}}$ is called an isomorphism is there exists a morphism $g : V'_{\mathrm{a}} \to V_{\mathrm{a}}$ such that $f \circ g$ and $g \circ f$ are the identity maps.

Proposition 2.12. Let $V_{\mathrm{a}} \subseteq \mathbb{A}^n$ be a variety and let $(a_{ij})_{i,j=1}^n$ be an invertible $n \times n$ matrix. Then the rational map

$$\begin{aligned} f : \mathbb{A}^n \quad &\dashrightarrow \quad \mathbb{A}^n \\ (x_1, \ldots, x_n) \quad &\mapsto \quad \left(\sum_{i=1}^n a_{i1} x_i, \ldots, \sum_{i=1}^n a_{in} x_i\right) \end{aligned}$$

restricts to an isomorphism $f^{-1}(V_{\mathrm{a}}) \to V_{\mathrm{a}}$. Any isomorphism of this form is called a linear transformation.

2.2 Projective varieties

It is well known that any two lines in $\mathbb{A}^2$ intersect at one unique point unless the lines are parallel. One can say that even parallel lines intersect at a point, but that this point is just missing in the affine plane. When we add these missing points we get the projective plane.

Definition 2.13. The projective n-dimensional space over K with variables $X_0, \ldots, X_n$ is defined as

$$\mathbb{P}^n_{X_0,\ldots,X_n} = \left(\mathbb{A}^{n+1}_{X_0,\ldots,X_n} \backslash \{(0,\ldots,0)\}\right) / \sim$$

where $(X_0, \ldots, X_n) \sim (Y_0, \ldots, Y_n)$ if and only if there is an $\lambda \in \overline{K}^*$ such that for all $i \in \{0, \ldots, n\}$ hold that $Y_i = \lambda X_i$. We denote the class of $(X_0, \ldots, X_n)$ in $\mathbb{P}^n_{X_0,\ldots,X_n}$ as $(X_0 : \cdots : X_n)$. Define the set of K-rational points of $\mathbb{P}^n_{X_0,\ldots,X_n}$ as

$$\mathbb{P}^n_{X_0,\ldots,X_n}(K) = \{(X_0 : \cdots : X_n) \in \mathbb{P}^n_{X_0,\ldots,X_n} : X_0, \ldots, X_n \in K\}.$$

Just as for $\mathbb{A}^n$ we just write $\mathbb{P}^n$ instead of $\mathbb{P}^n_{X_0,\ldots,X_n}$ when $X_0, \ldots, X_n$ are used as variables.

Note that $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$. Also note that $(X_0 : \cdots : X_n) \in \mathbb{P}^n(K)$ does not imply that $X_0, \ldots, X_n \in K$. For example $(\lambda : 0 : \cdots : 0) = (1 : 0 : \cdots : 0) \in \mathbb{P}^n(K)$ for any $\lambda \in \overline{K}^*$. However for every $(X_0 : \cdots : X_n) \in \mathbb{P}^n$ we can pick an i such that $X_i \neq 0$ and then we see that $(X_0 : \cdots : X_n) \in \mathbb{P}^n(K)$ if and only if $X_0/X_i, \ldots, X_n/X_i \in K$.

Definition 2.14. A polynomial $f \in \overline{K}[X_0, \ldots, X_n]$ is called homogeneous of degree d if

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \text{ for all } \lambda \in \overline{K}.$$

An ideal $I \subseteq \overline{K}[X_0, \ldots, X_n]$ is called homogeneous if it is generated by homogeneous polynomials.

Note that if f is homogeneous and $P \in \mathbb{P}^n$, then whether $f(P)$ is zero or not does not depend on the choice of representatives for P. So it makes sense to ask whether $f(P) = 0$ holds.

Definition 2.15. Let $I \in \overline{K}[X_0, \ldots, X_n]$ be an homogeneous ideal. Then define

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Any set V_p of the form V_I is called a projective algebraic set. For a projective algebraic set V_p we define $I(V_\mathrm{p})$ to be the ideal of $\overline{K}[X_0, \ldots, X_n]$ generated by

$$\{f \in \overline{K}[X_0, \ldots, X_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V_\mathrm{p}\}.$$

We say that V_p is defined over K if $I(V_\mathrm{p})$ can be generated by homogeneous polynomials in $K[X_0, \ldots, X_n]$.

Recall that the subscript a of V_a will always indicate that V_a is an affine algebraic set. In the same way the subscript a of V_p will always indicate that V_p is a projective algebraic set. Also when we write V_p/K we will mean that V_p is defined over K.

Definition 2.16. Let V_p/K be an algebraic set. We define the set of K-rational points on V_p as $V_\mathrm{p}(K) = V_\mathrm{p} \cap \mathbb{P}^n(K)$ and we define $I(V_\mathrm{p}/K) = I(V_\mathrm{p}) \cap K[X_0, \ldots, X_n]$. If $I(V_\mathrm{p})$ is a prime ideal, then V_p is called a projective variety.

Definition 2.17. For every $i \in \{0, \ldots, n\}$ we have an inclusion

$$\begin{array}{rcl}\phi_i : \mathbb{A}^n & \to & \mathbb{P}^n \\ (x_1, \ldots, x_n) & \mapsto & (x_1 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n).\end{array}$$

Using the map we can identify $\mathbb{A}^n$ with the subset of $\mathbb{P}^n$ consisting of all $(X_0 : \cdots : X_n)$ such that $X_i \neq 0$.

Now let V_{p} be a projective algebraic set in $\mathbb{P}^n$ and let $i \in \{0, \ldots, n\}$ be fixed. Then $V_{\mathrm{p}} \cap \mathbb{A}^n$, by which we mean $\phi_i^{-1}(V_{\mathrm{p}})$, is an affine algebraic set and we have

$$I(V_{\mathrm{p}} \cap \mathbb{A}^n) = \{f(x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n) : f \in I(V_{\mathrm{p}})\}.$$

We call $V_{\mathrm{p}} \cap \mathbb{A}^n$ the affine chart of V_{p} corresponding to $X_i = 1$ and $f(x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n)$ is called the dehomogenization of f corresponding to $X_i = 1$.

Definition 2.18. Let V_{a} be an affine algebraic set and let $i \in \{0, \ldots, n\}$ be fixed. Then for every $f \in \overline{K}[x_1, \ldots, x_n]$ write

$$f^*(X_0, \ldots, X_n) = X_i^{\deg(f)} f\left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right).$$

Define the projective closure $\overline{V_{\mathrm{a}}}$ of V_{a} as the projective algebraic set whose homogeneous ideal $I(\overline{V_{\mathrm{a}}})$ is generated by $\{f^* : f \in I(V_{\mathrm{a}})\}$. We can view V_{a} as a subset of $\overline{V_{\mathrm{a}}}$ using the map ϕ_i and we call $\overline{V_{\mathrm{a}}} \backslash V_{\mathrm{a}}$ the points at infinity on $\overline{V_{\mathrm{a}}}$.

Proposition 2.19 (Proposition I.2.6 of [1])**.** Let $\mathbb{A}^n \subseteq \mathbb{P}^n$ be a fixed affine chart.

(a) Let V_{a} be an affine variety, then $\overline{V_{\mathrm{a}}}$ is a projective variety and $V_{\mathrm{a}} = \overline{V_{\mathrm{a}}} \cap \mathbb{A}^n$. Furthermore if V_{a} is defined over K, then so is $\overline{V_{\mathrm{a}}}$.

(b) Let V_{p} be a projective variety, then $V_{\mathrm{p}} \cap \mathbb{A}^n$ is an affine variety and if $V_{\mathrm{p}} \cap \mathbb{A}^n \neq \emptyset$, then $\overline{V_{\mathrm{p}} \cap \mathbb{A}^n} = V_{\mathrm{p}}$. Furthermore if V_{p} is defined over K, then so is $V_{\mathrm{p}} \cap \mathbb{A}^n$.

Proposition 2.20. Let V_{p}/K be a projective variety, then $K[X_0, \ldots, X_n]/I(V_{\mathrm{p}}/K)$ is an integral domain. Let L be the subfield of the field of fractions of $K[X_0, \ldots, X_n]/I(V_{\mathrm{p}}/K)$ consisting of all elements f/g such that

- f and g are homogeneous elements of $K[X_0, \ldots, X_n]/I(V_{\mathrm{p}}/K)$ of the same degree;
- g is non-zero in $K[X_0, \ldots, X_n]/I(V_{\mathrm{p}}/K)$.

Now let $\mathbb{A}^n \subseteq \mathbb{P}^n$ be the affine chart corresponding to $X_i = 1$ for some i such that $V_{\mathrm{p}} \cap \mathbb{A}^n \neq \emptyset$, then the map

$$\begin{array}{rcl}\varphi : K(V_{\mathrm{p}} \cap \mathbb{A}^n) & \to & L \\ \dfrac{f}{g} & \mapsto & \dfrac{X_i^{\max(\deg(f), \deg(g))} f(X_0/X_i, \ldots, X_n/X_i)}{X_i^{\max(\deg(f), \deg(g))} g(X_0/X_i, \ldots, X_n/X_i)}\end{array}$$

is an isomorphism of fields. Furthermore if $P \in (V_{\mathrm{p}} \cap \mathbb{A}^n)(K)$, then φ restricts to an bijective map between the set of the functions in $K(V_{\mathrm{p}} \cap \mathbb{A}^n)$ that are zero at P and the set of the functions in L that are zero at P.

Definition 2.21. Let V_{p}/K be a projective variety and let $\mathbb{A}^n \subseteq \mathbb{P}^n$ be an affine chart such that $V_{\mathrm{p}} \cap \mathbb{A}^n \neq \emptyset$. The dimension of V_{p} is the dimension of $V_{\mathrm{p}} \cap \mathbb{A}^n$ and V_{p} is a projective curve if it has dimension 1. The function field $K(V_{\mathrm{p}})$ of V_{p}/K is the function field of $V_{\mathrm{p}} \cap \mathbb{A}^n$ over K.

Let $P \in V_{\mathrm{p}}(\overline{K})$, then we can choose the affine chart such that $V_{\mathrm{p}} \cap \mathbb{A}^n$ contains P. We say that V_{p} is smooth at P is $V_{\mathrm{p}} \cap \mathbb{A}^n$ is smooth at P and V_{p} is smooth if V_{p} is smooth at every point in $V_{\mathrm{p}}(\overline{K})$. Now consider $\overline{K}[V_{\mathrm{p}} \cap \mathbb{A}^n]$. Since P is contained in $V_{\mathrm{p}} \cap \mathbb{A}^n$, we can evaluate functions in $\overline{K}[V_{\mathrm{p}} \cap \mathbb{A}^n]$ at P. We have a maximal ideal $\mathfrak{m}_P = \{f \in \overline{K}[V_{\mathrm{p}} \cap \mathbb{A}^n] : f(P) = 0\}$ of $\overline{K}[V_{\mathrm{p}} \cap \mathbb{A}^n]$ and we define the local ring of V_{p} at P, denoted as $\overline{K}[V_{\mathrm{p}}]_P$, as the localization of $\overline{K}[V_{\mathrm{p}} \cap \mathbb{A}^n]$ at $\mathfrak{m}_P$.

By Proposition 2.20, the function fields of the affine charts of V_{p} are isomorphic. So the isomorphism class of $K(V_{\mathrm{p}})$ is well defined. For a point $P \in V_{\mathrm{p}}(\overline{K})$, note that $\overline{K}[V_{\mathrm{p}}]_P$ is contained in $K(V_{\mathrm{p}})$ (with the same affine chart). And if P is contained in multiple affine charts of V_{p}, then the isomorphisms between the function field defined by those affine charts restrict to isomorphisms between the local rings of V_{p} at P defined by the same affine charts. This means that the isomorphism class of $\overline{K}[V_{\mathrm{p}}]_P$ is also well defined.

Proposition 2.22 (Proposition I.2.1 of [2])**.** The union of two projective algebraic sets is a projective algebraic set. The intersection of any family of projective algebraic sets is a projective algebraic set. The empty set and $\mathbb{P}^n$ are projective algebraic sets.

Definition 2.23. Define the Zariski topology on $\mathbb{P}^n$ by taking the open subsets to be the complements of the projective algebraic sets of $\mathbb{P}^n$. For every variety V_{p}, define the topology on $V_{\mathrm{p}}(\overline{K})$ as the induced topology.

Definition 2.24. Let V_{p} and $V'_{\mathrm{p}} \subseteq \mathbb{P}^n$ be varieties. A rational map $f : V_{\mathrm{p}} \dashrightarrow V'_{\mathrm{p}}$ is a map $f : U \to V'_{\mathrm{p}}(\overline{K})$ sending $P \mapsto (f_0(P) : \cdots : f_n(P))$ where $f_0, \ldots, f_n$ are elements of $\overline{K}(V_{\mathrm{p}})$ and where $U \subseteq V_{\mathrm{p}}(\overline{K})$ is a non-empty open subset of $V_{\mathrm{p}}(\overline{K})$ such that

- $f_0, \ldots, f_n$ can be evaluated at every point in U;
- $f_0(P), \ldots, f_m(P)$ are not all zero for all $P \in U$;
- and $(f_0(P) : \cdots : f_n(P)) \in V'_{\mathrm{p}}(\overline{K})$ for every $P \in U$.

We say that f is defined over K if $\lambda f_1, \ldots, \lambda f_n \in K(V_{\mathrm{p}})$ for some $\lambda \in \overline{K}$.

Definition 2.25. Let V_{p} and $V'_{\mathrm{p}} \subseteq \mathbb{P}^n$ be varieties. A morphism $f : V_{\mathrm{p}} \to V'_{\mathrm{p}}$ is a map $f : V_{\mathrm{p}} \to V'_{\mathrm{p}}$ sending $P \in U_i$ to $f_i(P)$ where $U_1, \ldots, U_m \subseteq V_{\mathrm{p}}(\overline{K})$ are open in $V_{\mathrm{p}}(\overline{K})$ such that $\bigcup_{i=1}^m U_i = V_{\mathrm{p}}(\overline{K})$ and where $f_1 : U_1 \to V'_{\mathrm{p}}, \ldots, f_m : U_m \to V'_{\mathrm{p}}$ are rational maps $V_{\mathrm{p}} \dashrightarrow V'_{\mathrm{p}}$ such that f_i and f_j restrict to the same map on $U_i \cap U_j$ for every i and j. We say that f is defined over K is $f_1, \ldots, f_m$ are defined over K.

Definition 2.26. A morphism of $f : V_{\mathrm{p}} \to V'_{\mathrm{p}}$ is called an isomorphism is there exists a morphism $g : V'_{\mathrm{p}} \to V_{\mathrm{p}}$ such that $f \circ g$ and $g \circ f$ are the identity maps.

By Theorem II.2.4 of [1] we know that an isomorphism defined over K between projective curves C_{p}/K and C'_{p}/K gives us an isomorphism of the function fields of C_{p} and C'_{p}. Furthermore Proposition I.1.7 of [1] gives a condition for a point P on a curve C_{p} to be smooth in terms of the ideal $\mathfrak{m}_P$ of $\overline{K}[C_{\mathrm{p}}]_P$, which is a subring of $\overline{K}(C_{\mathrm{p}})$. Therefore it is not difficult to prove that isomorphic curves are either both smooth or both not smooth.

By the Riemann-Roch Theorem, for each smooth projective curve C_{p} there is an integer $g \geq 0$ called the genus of C_{p}. The following proposition shows that the genera of isomorphic smooth projective curves are the same.

Proposition 2.27. Let C_{p} and C_{p} be isomorphic smooth projective curves, then the genera of C_{p} and C_{p} are equal.

Proof. An isomorphism of smooth projective curves is a degree 1 map, which is unramified by Proposition II.2.6(a) of [1]. Hence by Theorem II.5.9 of [1] the genera of C_{p} and C_{p} are equal. □

Proposition 2.28. Let $V_{\mathrm{p}} \subseteq \mathbb{P}^n$ be a variety and let $(a_{ij})_{i,j=0}^n$ be an invertible $n+1 \times n+1$ matrix, then the rational map

$$\begin{array}{rcl} f : \mathbb{P}^n & \dashrightarrow & \mathbb{P}^n \\ (X_0 : \cdots : X_n) & \mapsto & \left(\sum_{i=0}^n a_{i0} X_i : \cdots : \sum_{i=0}^n a_{in} X_i \right) \end{array}$$

restricts to an isomorphism $f^{-1}(V_{\mathrm{p}}) \to V_{\mathrm{p}}$. Any isomorphism of this form is called a linear transformation.

2.3 Divisors

Definition 2.29. Let C_{p} be a projective curve, $P \in C_{\mathrm{p}}(\overline{K})$ a smooth point. By Proposition II.1.1 of [1] we know that $\overline{K}[C_{\mathrm{p}}]_P$ is a discrete valuation ring. This means that we have a valuation

$$\begin{array}{rcl} \mathrm{ord}_P : \overline{K}[C_{\mathrm{p}}]_P & \to & \mathbb{N}_0 \cup \{\infty\} \\ \mathrm{ord}_P(f) & = & \sup\{d \in \mathbb{N}_0 : f \in \mathfrak{m}_P^d\} \end{array}$$

If $f \neq 0$, then $\mathrm{ord}_P(f)$ is finite. The field of fractions of $\overline{K}[C_{\mathrm{p}}]_P$ is canonically isomorphic to $\overline{K}(C_{\mathrm{p}})$ and this allows us to define

$$\begin{array}{rcl} \mathrm{ord}_P : \overline{K}(C_{\mathrm{p}}) & \to & \mathbb{Z} \cup \{\infty\} \\ \mathrm{ord}_P(f/g) & = & \mathrm{ord}_P(f) - \mathrm{ord}_P(g) \end{array}$$

We call $\mathrm{ord}_P(f)$ the order of f at P. If $\mathrm{ord}_P(f) > 0$, then we say that f has a zero at P of order $\mathrm{ord}_P(f)$ and if $\mathrm{ord}_P(f) < 0$, then we say that f has a pole at P of order $-\mathrm{ord}_P(f)$.

The following Proposition helps us the calculate the order of a function at a point P.

Proposition 2.30. Let C_{p} be smooth curve and let $P = (a_1, \ldots, a_n) \in (C_{\mathrm{p}} \cap \mathbb{A}^n)(\overline{K})$. Suppose that the ideal $\mathfrak{m}_P \subseteq \overline{K}[C_{\mathrm{p}}]_P$ is generated by $f_1, \ldots, f_m \in \mathfrak{m}_P$, then $\mathrm{ord}_P(f_i) = 1$ for some i. In particular $\mathrm{ord}_P(x_i - a_i) = 1$ some some i.

Proof. By Proposition I.1.7 for [1] we know that $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension 1 as a $\overline{K}$-vectorspace. Suppose that $\mathfrak{m}_P$ is generated by $f_1, \ldots, f_m \in \mathfrak{m}_P$, then $\mathrm{ord}_P(f_i) \geq 1$ for each i. If $\mathrm{ord}_P(f_i) > 1$ for each i, then $f_1, \ldots, f_m \in \mathfrak{m}_P^2$ so

$$\mathfrak{m}_P = (f_1, \ldots, f_m) \subseteq \mathfrak{m}_P^2 \subseteq \mathfrak{m}_P.$$

However $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension 1, so $\mathfrak{m}_P \neq \mathfrak{m}_P^2$. Therefore $\mathrm{ord}_P(f_i) = 1$ for some i. By Hilbert's Nullstellensatz, $\mathfrak{m}_P$ is generated by $x_1 - a_1, \ldots, x_n - a_n$. So we see that in particular $\mathrm{ord}_P(x_i - a_i) = 1$ some some i. □

Definition 2.31. Let C_{p} be a curve, then define the divisor group $\mathrm{Div}(C_{\mathrm{p}})$ of C_{p} to be the free abelian group generated by the points of C_{p}.

$$\mathrm{Div}(C_{\mathrm{p}}) = \bigoplus_{P \in C_{\mathrm{p}}(\overline{K})} \mathbb{Z} \cdot (P)$$

For an element $D = \sum_P n_P \cdot (P) \in \mathrm{Div}(C_{\mathrm{p}})$ we define $\deg(D) = \sum_P n_P$. The divisors of degree 0 form a subgroup of $\mathrm{Div}(C_{\mathrm{p}})$.

$$\mathrm{Div}^0(C_{\mathrm{p}}) = \{D \in \mathrm{Div}(C_{\mathrm{p}}) : \deg(D) = 0\}$$

We say a divisor $\sum_P n_P \cdot (P)$ is effective if $n_P \geq 0$ for all P and for divisors D_1 and D_2 we say that $D_1 \geq D_2$ if $D_1 - D_2$ is effective.

Proposition 2.32. Let C_{p} be a smooth curve, then we have a homomorphism

$$\begin{aligned} \mathrm{div} : \overline{K}(C_{\mathrm{p}})^* &\to \mathrm{Div}^0(C_{\mathrm{p}}) \\ \mathrm{div}(f) &= \sum_P \mathrm{ord}_P(f) \cdot (P) \end{aligned}$$

Proof. By proposition II.1.2 of [1] $\mathrm{ord}_P(f)$ is non-zero for only finitely many $P \in C_{\mathrm{p}}(\overline{K})$. So $\mathrm{div}(f)$ defines an element of $\mathrm{Div}(C_{\mathrm{p}})$. Since ord_P is a valuation, the map $\mathrm{div} : \overline{K}(C_{\mathrm{p}})^* \to \mathrm{Div}(C_{\mathrm{p}})$ is a homomorphism. By Proposition II.3.1(b) of [1], we know that $\deg(\mathrm{div}(f)) = 0$ for every $f \in \overline{K}(C_{\mathrm{p}})^*$. Therefore $\mathrm{div}(f) \in \mathrm{Div}^0(C_{\mathrm{p}})$. □

Definition 2.33. Let C_{p} be a smooth curve and let $f \in \overline{K}(C_{\mathrm{p}})^*$, then the divisor $\mathrm{div}(f)$ is called principal. The set of principal divisors $\mathrm{Princ}(C_{\mathrm{p}})$ forms a subgroup of $\mathrm{Div}^0(C_{\mathrm{p}})$ and we define $\mathrm{Pic}(C_{\mathrm{p}}) = \mathrm{Div}(C_{\mathrm{p}})/\mathrm{Princ}(C_{\mathrm{p}})$ and $\mathrm{Pic}^0(C_{\mathrm{p}}) = \mathrm{Div}^0(C_{\mathrm{p}})/\mathrm{Princ}(C_{\mathrm{p}})$.

Definition 2.34. Let C_{p}/K be a smooth curve and let $G = \mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}/K$, then elements $\sigma \in G$ act on elements of $\mathbb{P}^n$ by acting on its coordinates, i.e. $\sigma(X_0 : \cdots : X_n) = (\sigma X_0 : \cdots : \sigma X_n)$.

Now let $D = \sum_P n_P \cdot (P) \in \mathrm{Div}(C_{\mathrm{p}})$, then we have an action of G on $\mathrm{Div}(C_{\mathrm{p}})$ given by $\sigma D = \sum_P n_P(\sigma P)$. If D is principal, then σD is again principal. Therefore G also acts on $\mathrm{Pic}(C_{\mathrm{p}})$ by acting on the representatives of elements. Clearly $\sigma D \in \mathrm{Div}^0(C_{\mathrm{p}})$ if $D \in \mathrm{Div}^0(C_{\mathrm{p}})$, so the G-actions on $\mathrm{Div}(C_{\mathrm{p}})$ and Pic^0 restrict to actions on $\mathrm{Div}^0(C_{\mathrm{p}})$ and $\mathrm{Pic}^0(C_{\mathrm{p}})$. We define the subgroups of G invariants.

$$\mathrm{Div}_K(C_{\mathrm{p}}) = (\mathrm{Div}(C_{\mathrm{p}}))^G = \{D \in \mathrm{Div}(C_{\mathrm{p}}) : \sigma D = D \ \forall \sigma \in G\}$$

$$\mathrm{Princ}_K(C_{\mathrm{p}}) = (\mathrm{Princ}(C_{\mathrm{p}}))^G = \{D \in \mathrm{Princ}(C_{\mathrm{p}}) : \sigma D = D \ \forall \sigma \in G\}$$

$$\mathrm{Pic}_K(C_{\mathrm{p}}) = \mathrm{Div}_K(C_{\mathrm{p}})/\mathrm{Princ}_K(C_{\mathrm{p}})$$

$$\mathrm{Div}^0_K(C_{\mathrm{p}}) = \left(\mathrm{Div}^0(C_{\mathrm{p}})\right)^G = \{D \in \mathrm{Div}^0(C_{\mathrm{p}}) : \sigma D = D \ \forall \sigma \in G\}$$

$$\mathrm{Pic}^0_K(C_{\mathrm{p}}) = \mathrm{Div}^0_K(C_{\mathrm{p}})/\mathrm{Princ}_K(C_{\mathrm{p}})$$

Note that in general $\mathrm{Pic}^0_K(C_{\mathrm{p}})$ and

$$(\mathrm{Pic}^0(C_{\mathrm{p}}))^G = \{D \in \mathrm{Pic}^0(C_{\mathrm{p}}) : \sigma D = D \ \forall \sigma \in G\}$$

are not necessary equal. However if $C_{\mathrm{p}}(K) \neq \emptyset$, then $\mathrm{Pic}^0_K(C_{\mathrm{p}})$ and $(\mathrm{Pic}^0(C_{\mathrm{p}}))^G$ are isomorphic. So when only considering elliptic curves we could as well define $\mathrm{Pic}^0_K(C_{\mathrm{p}})$ as $(\mathrm{Pic}^0(C_{\mathrm{p}}))^G$ and this is in fact done in [1]. The following proposition proves this in the case of elliptic curves.

Proposition 2.35. Let C_p/K be a smooth curve of genus 1 and let $G = \mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}/K$. Suppose that $C_\mathrm{p}(K) \neq \emptyset$, then the map

$$\begin{array}{rcl} \mathrm{Pic}^0_K(C_\mathrm{p}) & \to & (\mathrm{Pic}^0(C_\mathrm{p}))^G \\ [D] & \mapsto & [D] \end{array}$$

is an isomorphism.

Proof. We prove this by proving that the map

$$\begin{array}{rcl} \pi : \mathrm{Div}^0_K(C_\mathrm{p}) & \to & (\mathrm{Pic}^0(C_\mathrm{p}))^G \\ D & \mapsto & [D] \end{array}$$

is a surjective homomorphism and has kernel $\mathrm{Princ}_K(C_\mathrm{p})$.

Let $D \in \mathrm{Div}^0_K(C_\mathrm{p})$, then $\deg(D) = 0$ and $\sigma D = D$ for every $\sigma \in G$. Therefore $[D]$ is an element of $\mathrm{Pic}^0(C_\mathrm{p})$ and $\sigma[D] = [\sigma D] = [D]$. Hence $[D] \in (\mathrm{Pic}^0(C_\mathrm{p}))^G$ and π is well defined. Clearly π is an homomorphism.

Suppose that $\pi(D) = [0]$, then $D \in \mathrm{Princ}(C_\mathrm{p})$. Since $D \in \mathrm{Div}^0_K(C_\mathrm{p})$, D is G-invariant. Hence $D \in \mathrm{Princ}_K(C_\mathrm{p})$ and $[D] = [0]$. Also clearly if $D \in \mathrm{Princ}_K(C_\mathrm{p})$, then $\pi(D) = [0]$ since $\mathrm{Princ}_K(C_\mathrm{p}) \subseteq \mathrm{Princ}(C_\mathrm{p})$. Hence the kernel of π is $\mathrm{Princ}_K(C_\mathrm{p})$.

Let $O \in C_\mathrm{p}(K)$. Then by the proof of Proposition 3.4 of [1] every element of $(\mathrm{Pic}^0(C_\mathrm{p}))^G$ is of the form $[(P) - (O)]$. Now let $[(P) - (O)] \in (\mathrm{Pic}^0(C_\mathrm{p}))^G$, then for every $\sigma \in G$ we have

$$[(P) - (O)] = \sigma[(P) - (O)] = [(\sigma P) - (\sigma O)].$$

So $(P) - (\sigma P) \in \mathrm{Princ}(C_\mathrm{p})$, because $\sigma O = O$. So $(P) - (\sigma P) = \mathrm{div}(g)$ for some $g \in \overline{K}(C_\mathrm{p})^*$.

By Corollary II.5.5(c) of [1] we see that

$$\mathcal{L}((\sigma P)) = \{f \in \overline{K}(C_\mathrm{p})^* : \mathrm{div}(f) \geq -(\sigma P)\} \cup \{0\}$$

is a one-dimensional vectorspace over $\overline{K}$. Since $\overline{K} \subseteq \mathcal{L}((\sigma P))$ we see that $\overline{K} = \mathcal{L}((\sigma P))$. Now we see that $g \in \overline{K}$, since $(P) - (\sigma P) \geq -(\sigma P)$. Hence $\mathrm{div}(g) = 0$ and $\sigma P = P$. Hence $P \in C_\mathrm{p}(K)$ and we see that $[(P) - (O)] = \pi((P) - (O))$. Hence π is surjective. So we see that the map

$$\begin{array}{rcl} \mathrm{Div}^0_K(C_\mathrm{p})/\mathrm{Princ}_K(C_\mathrm{p}) & \to & (\mathrm{Pic}^0(C_\mathrm{p}))^G \\ [D] & \mapsto & [D] \end{array}$$

is an isomorphism. □

Chapter 3

Elliptic curves

By Theorem II.5.4 of [1] every smooth projective projective has a genus $g \in \mathbb{N}_0$. Elliptic curves are the curves with genus 1 together with a point.

Definition 3.1. An elliptic curve is a pair (E_{p}, O), where E_{p} is a smooth projective curve of genus one and $O \in E_{\mathrm{p}}(\overline{K})$. An elliptic curve (E_{p}, O) is called defined over K if E_{p} is defined over K and $O \in E_{\mathrm{p}}(K)$.

When O is clear from the context we often write just E_{p} instead of (E_{p}, O) and in this case we write E_{p}/K is if the elliptic curve E_{p} is defined over K. We also have a different characterization of when a pair (E_{p}, O) is an elliptic curve.

Proposition 3.2. Let E_{p}/K be a smooth projective curve and let $O \in E_{\mathrm{p}}(K)$, then (E_{p}, O) is an elliptic curve over K if and only if E_{p}/K is isomorphic over K with a smooth projective curve $E'_{\mathrm{p}} \subseteq \mathbb{P}^2_{X,Y,Z}$ defined over K given by a Weierstrass equation

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

with $a_1, a_2, a_3, a_4, a_6 \in K$ such that the isomorphism sends O to $\mathcal{O} = (0 : 1 : 0) \in \mathbb{P}^2_{X,Y,Z}$.

Proof. Suppose that (E_{p}, O) is an elliptic curve over K, then by Proposition II.3.1(a) of [1] we know that E_{p}/K is isomorphic over K with a smooth projective curve E'_{p}/K as above such that the isomorphism sends $\mathcal{O}'$ to $\mathcal{O} = (0 : 1 : 0) \in E_{\mathrm{p}}(K)$.

Now suppose that E_{p}/K is isomorphic over K with a smooth projective curve E'_{p}/K given by a Weierstrass equation. By Proposition II.3.1(c) of [1] $(E'_{\mathrm{p}}, \mathcal{O})$ is an elliptic curve, which means that the genus of E'_{p} is 1. So since E_{p} and E'_{p} are isomorphic, the genus of E_{p} is also 1. Hence (E_{p}, O) is an elliptic curve over K. □

So in particular for any smooth projective curve $E_{\mathrm{p}} \subseteq \mathbb{P}^2$ defined over K given by a Weierstrass equation, $(E_{\mathrm{p}}, \mathcal{O})$ is an elliptic curve where $\mathcal{O} = (0 : 1 : 0) \in \mathbb{P}^2$.

Definition 3.3. Let (E_{p}, O) and (E'_{p}, O') be elliptic curves. We say that (E_{p}, O) and (E'_{p}, O') are isomorphic if there exists an isomorphism $f : E_{\mathrm{p}} \to E'_{\mathrm{p}}$ of projective curves sending O to O'. If (E_{p}, O), (E'_{p}, O') and f are all defined over K, then we say that (E_{p}, O) and (E'_{p}, O') are isomorphic over K.

For elliptic curves over a field K we also have the following results.

Theorem 3.4. Let (E_{p}, O) be an elliptic curve defined over K, then

$$\begin{aligned} \phi : E_{\mathrm{p}}(K) &\rightarrow \mathrm{Pic}^0_K(E_{\mathrm{p}}) \\ P &\mapsto (P) - (O) \end{aligned}$$

is a bijection. Hence $E_{\mathrm{p}}(K)$ has a group structure, where O acts as zero element, such that ϕ is an isomorphism.

Proof. See Remark III.3.5.1 of [1]. □

Theorem 3.5. Let $f : (E_{\mathrm{p}}, O) \rightarrow (E'_{\mathrm{p}}, O')$ be an isomorphism of elliptic curves over K, then f restricts to an isomorphism $E_{\mathrm{p}}(K) \rightarrow E'_{\mathrm{p}}(K)$ of groups.

Proof. Note that f is a function $E_{\mathrm{p}}(\overline{K}) \rightarrow E'_{\mathrm{p}}(\overline{K})$ and since f and its inverse are defined over K, we know that f restricts to a bijective map $E_{\mathrm{p}}(K) \rightarrow E'_{\mathrm{p}}(K)$. By the previous theorem, proving that this is an isomorphism is the same as proving that the map $\mathrm{Pic}^0_K(E_{\mathrm{p}}) \rightarrow \mathrm{Pic}^0_K(E'_{\mathrm{p}})$ sending $\sum_P n_P \cdot (P) \mapsto \sum_P n_P \cdot (f(P))$ is an isomorphism. Define

$$\begin{aligned} \phi : \mathrm{Div}(E_{\mathrm{p}}) &\rightarrow \mathrm{Div}(E'_{\mathrm{p}}) \\ \sum_P n_P \cdot (P) &\mapsto \sum_P n_P \cdot (f(P)) \end{aligned}$$

Clearly ϕ is an homomorphism and if $\deg(D) = 0$, then $\deg(\phi(D)) = 0$. So ϕ restricts to a homomorphism $\mathrm{Div}^0(E_{\mathrm{p}}) \rightarrow \mathrm{Div}^0(E'_{\mathrm{p}})$.

Next suppose that $D \in \mathrm{Div}(E_{\mathrm{p}})$ is principal, then $D = \mathrm{div}(g)$ for some $g \in \overline{K}(E_{\mathrm{p}})$. We know by Remark II.2.5 of [1] that f^{-1} induces an isomorphism $(f^{-1})^* : \overline{K}(E_{\mathrm{p}}) \rightarrow \overline{K}(E'_{\mathrm{p}})$ of the function fields of E_{p} and E'_{p} defined by $(f^{-1})^*(h) = h \circ f^{-1}$. Since f^{-1} is an isomorphism, f^{-1} is unramified. Hence $\mathrm{div}((f^{-1})^*(h)) = \phi(\mathrm{div}(h))$. In particular we see that $\mathrm{div}((f^{-1})^*(g)) = \phi(D)$. Hence ϕ maps principal divisors to principal divisors. So the map

$$\begin{aligned} \mathrm{Pic}(E_{\mathrm{p}}) &\rightarrow \mathrm{Pic}(E'_{\mathrm{p}}) \\ \sum_P n_P \cdot (P) &\mapsto \sum_P n_P \cdot (f(P)) \end{aligned}$$

is well defined and restricts to a map $\mathrm{Pic}^0(E_{\mathrm{p}}) \rightarrow \mathrm{Pic}^0(E'_{\mathrm{p}})$.

Now let $G = \mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}/K$, let $\sigma \in G$ and let $P \in \overline{K}(E_{\mathrm{p}})$. Since f is defined over K, f can be given by rational functions with coefficients in K and therefore $f(\sigma P) = \sigma f(P)$. So we see that $\sigma\phi(D) = \phi(\sigma D)$ for any divisor D. Hence the map $\mathrm{Pic}^0(E_{\mathrm{p}}) \rightarrow \mathrm{Pic}^0(E'_{\mathrm{p}})$ restricts to a map $\mathrm{Pic}^0_K(E_{\mathrm{p}}) \rightarrow \mathrm{Pic}^0_K(E'_{\mathrm{p}})$. This map is a homomorphism of groups and we can find its inverse by replacing f with f^{-1}. Hence it is an isomorphism. □

3.1 Elliptic curves given by a Weierstrass equation

Assume in this section that $\mathrm{char}(K) \neq 2$. Let $h(x) = x^3 + ax^2 + bx + c \in K[x]$ be a polynomial with no double roots in $\overline{K}$. So for all $x \in \overline{K}$ with $h(x) = 0$ we have $h'(x) = 3x^2 + 2ax + b \neq 0$. Now consider the curve $E_{\mathrm{a}} \subseteq \mathbb{A}^2_{x,y}$ given by the equation $y^2 = h(x)$. Clearly E_{a} is defined over K and any singular point of E_{a} satisfies

$$y^2 = h(x), \quad 2y = 0 \quad \text{and} \quad h'(x) = 0.$$

So if $(x, y) \in E_{\rm a}(\overline{K})$ is a singular point of $E_{\rm a}$, then $y = 0$ and $h(x) = h'(x) = 0$. Hence $E_{\rm a}$ is smooth, because h has no double roots.

The projective closure $E_{\rm p} \subseteq \mathbb{P}^2_{X,Y,Z}$ of $E_{\rm a}/K$ is defined by the equation $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. If $Z = 0$, then we see that $X^3 = 0$ and therefore $X = 0$. In this case Y must be non-zero and we may scale Y to be 1. So $\mathcal{O} = (0 : 1 : 0)$ is the only point at infinity on $E_{\rm p}$. To see if $\mathcal{O}$ is a smooth point we take the affine chart corresponding to $Y = 1$ and get the affine curve in $\mathbb{A}^2(u, w)$ defined by $w = u^3 + au^2w + buw^2 + cw^3$. Since $\frac{\partial}{\partial w}(w - u^3 - au^2w - buw^2 - cw^3)$ is non-zero at $(0, 0)$, we see that $(0, 0)$ is smooth. Therefore $\mathcal{O}$ is a smooth point of $E_{\rm p}$ and $E_{\rm p}$ is a smooth curve.

Since $E_{\rm p}/K$ is a smooth curve given by a Weierstrass equation, we know that $E_{\rm p}/K$ is a elliptic curve and if $\mathrm{char}(K) \neq 2$, then every elliptic curve over K is isomorphic to an elliptic curve given by $y^2 = x^3 + ax^2 + bx + c$ for some $a, b, c \in K$.

Proposition 3.6. Let $E_{\rm p} \subseteq \mathbb{P}^2_{X,Y,Z}$ be the projective curve given by

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

with $a_1, a_2, a_3, a_4, a_6 \in K$. Then the rational map $f : \mathbb{P}^2_{X,Y,Z} \dashrightarrow \mathbb{P}^2_{U,V,W}$ given by $(X : Y : Z) \mapsto (X : Y + a_1X/2 + a_3Z/2 : Z)$ induces an isomorphism over K from $E_{\rm p}/K$ to the projective curve $E'_{\rm p} \subseteq \mathbb{P}^2_{U,V,W}$ given by

$$V^2W = U^3 + aU^2W + bUW^2 + cW^3$$

where

$$a = a_2 + \tfrac{1}{4}a_1^2, \quad b = a_4 + \tfrac{1}{2}a_1a_3 \quad \text{and} \quad c = a_6 + \tfrac{1}{4}a_3^2.$$

Furthermore if $E_{\rm p}$ is smooth, then f is an isomorphism over K of the elliptic curves $E_{\rm p}$ and $E'_{\rm p}$.

Proof. Note that

$$(Y + a_1X/2 + a_3Z/2)^2Z - \tfrac{1}{4}a_1^2X^2Z - \tfrac{1}{2}a_1a_3XZ^2 - \tfrac{1}{4}a_3^2Z^3 = Y^2Z + a_1XYZ + a_3YZ^2.$$

So the substitution $(U : V : W) = (X : Y + a_1X/2 + a_3Z/2 : Z)$ gives us

$$V^2W = U^3 + aU^2W + bUW^2 + cW^3.$$

Hence $f(E_{\rm p}) = E'_{\rm p}$. Note that f is a linear transformation defined over K, so f is an isomorphism over K. Therefore $E_{\rm p}/K$ is smooth if and only if $E'_{\rm p}/K$ is smooth and we also have $f(\mathcal{O}) = \mathcal{O}$. Hence if $E_{\rm p}$ is smooth, then f is an isomorphism over K of the elliptic curves $E_{\rm p}$ and $E'_{\rm p}$. □

We also have the following result.

Proposition 3.7. Let $E_{\rm p} \subseteq \mathbb{P}^2_{X,Y,Z}$ be the projective curve given by

$$b_1Y^2Z + a_1XYZ + a_3YZ^2 = b_2X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ and $b_1, b_2 \in K^*$ and let $E'_{\rm p} \subseteq \mathbb{P}^2_{U,V,W}$ be the projective curve given by

$$V^2W + a_1UVW + a_3b_1b_2VW^2 = U^3 + a_2b_1U^2W + a_4b_1^2b_2UW^2 + a_6b_1^3b_2^2W^3.$$

Then the rational map $f : \mathbb{P}^2_{X,Y,Z} \dashrightarrow \mathbb{P}^2_{U,V,W}$ sending $(X : Y : Z) \mapsto (b_1b_2X : b_1^2b_2Y : Z)$ is an isomorphism over K. Furthermore if $E_{\rm p}$ is smooth, then f is an isomorphism over K of the elliptic curves $E_{\rm p}$ and $E'_{\rm p}$.

Proof. We first multiply the equation for E_p by $b_1^3 b_2^2$ and then we use the substitution $(U : V : W) = (b_1 b_2 X : b_1^2 b_2 Y : Z)$ to get

$$V^2W + a_1UVW + a_3b_1b_2VW^2 = U^3 + a_2b_1U^2W + a_4b_1^2b_2UW^2 + a_6b_1^3b_2^2W^3.$$

Hence $f(E_\mathrm{p}) = E'_\mathrm{p}$. Note that f is a linear transformation defined over K, so f is an isomorphism over K. Therefore E_p/K is smooth if and only if E'_p/K is smooth and we also have $f(\mathcal{O}) = \mathcal{O}$. Hence if E_p is smooth, then f is an isomorphism over K of the elliptic curves E_p and E'_p. □

Now let E_p/K be an elliptic curve given by $y^2 = x^3 + ax^2 + bx + c$ for some $a, b, c \in K$. Then we can explicitly describe the group law on $E_\mathrm{p}(K)$. See section III.2 of [1] for this description and see Proposition III.3.4(e) of [1] for the proof that this is in fact a group law. Important to note here is that, counting multiplicities, lines intersect with E_p in three points and the sum of these three points is zero. Also if $(x, y) \in E_\mathrm{a}(K) \subseteq E_\mathrm{p}(K)$, then $-(x, y) = (x, -y)$.

3.2 Elliptic curves given by $y^2 = ax^4 + bx^3 + cx^2 + dx + e$

Assume in this section again that $\mathrm{char}(K) \neq 2$. Let $h(x) = ax^4 + bx^3 + cx^2 + dx + e \in K[x]$ be a polynomial of degree 4 with no double roots in $\overline{K}$. Now consider the affine curve E_a/K in $\mathbb{A}^2_{x,y}$ given by $y^2 = h(x)$. Any singular point of E_a satisfies

$$y^2 = h(x), \quad 2y = 0 \quad \text{and} \quad h'(x) = 0.$$

So if $(x, y) \in E_\mathrm{a}(\overline{K})$ is a singular point of E_a, then $y = 0$ and $h(x) = h'(x) = 0$. Hence E_a is smooth, because h has no double roots.

The projective closure $\overline{E_\mathrm{a}}/K$ in $\mathbb{P}^2_{X,Y,Z}$ of E_a/K is defined by the equation

$$Y^2Z^2 = aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4.$$

Now consider the affine chart in $\mathbb{A}^2_{u,v}$ corresponding to $Y = 1$ given by

$$v^2 = au^4 + bu^3v + cu^2v^2 + duv^3 + ev^4.$$

Note that the ordering of X, Y, Z in $\mathbb{P}^2_{X,Y,Z}$ and u, v in $\mathbb{A}^2_{u,v}$ means that we take $u = X/Y$ and $v = Z/Y$. The point $(0, 0)$ on the affine chart is singular. Therefore $(0 : 1 : 0)$ is a singular point of $\overline{E_\mathrm{a}}$. Hence $\overline{E_\mathrm{a}}$ is not smooth and $(\overline{E_\mathrm{a}}, O)$ is not an elliptic curve for any $O \in \overline{E_\mathrm{a}}(\overline{K})$.

So we see that simply taking the projective closure of E_a will not give us an elliptic curve. However, we will prove in this section that E_a is isomorphic over K with the affine chart of a projective curve. Consider the affine curve $\hat{E}_\mathrm{a}/K$ in $\mathbb{A}^3_{u,v,y}$ given by

$$u = v^2$$

$$y^2 = au^2 + buv + cu + dv + e$$

The rational map $E_\mathrm{a} \dashrightarrow \hat{E}_\mathrm{a}$ sending $(x, y) \mapsto (x^2, x, y)$ is an isomorphism defined over K. So $\hat{E}_\mathrm{a}$ is smooth, because E_a is smooth. We can also check that $\hat{E}_\mathrm{a}$ is smooth directly. The matrix of partial derivatives of the equations for $\hat{E}_\mathrm{a}$ is

$$M = \begin{pmatrix} 1 & -2v & 0 \\ -2au - bv - c & -bu - d & 2y \end{pmatrix}.$$

Now let $P = (u, v, y) \in \hat{E}_{\mathrm{a}}(\overline{K})$. Then P is a singular point of $\hat{E}_{\mathrm{a}}$ if and only if the rank of M evaluated at P is at most 1. Note that the first column is not the zero vector so the rank of M is always at least 1. Also note that $y \neq 0$ if and only if the first and third column are linearly independent and the first and second column are linearly independent if and only if

$$\det \begin{pmatrix} 1 & -2v \\ -2au - bv - c & -bu - d \end{pmatrix} = -bu - d + 2v(-2au - bv - c) \neq 0.$$

So the singular points of $\hat{E}_{\mathrm{a}}$ are precisely the points $(u, v, y) \in \hat{E}_{\mathrm{a}}(\overline{K})$ such that $y = bu + d + 2v(2au + bv + c) = 0$. These conditions correspond to $y = 4ax^3 + 3bx^2 + 2cx + d = 0$ in E_{a} and these are precisely the conditions for a point $(x, y) \in E_{\mathrm{a}}(\overline{K})$ to be singular. Therefore the bijection $E_{\mathrm{a}}(\overline{K}) \to \hat{E}_{\mathrm{a}}(\overline{K})$ restricts to a bijection of the singular points on E_{a} and $\hat{E}_{\mathrm{a}}$. Hence $\hat{E}_{\mathrm{a}}$ is smooth, because E_{a} is smooth.

Now let E_{p}/K in $\mathbb{P}^3_{U,V,W,Y}$ be the curve given by the two equations

$$UW = V^2$$

$$Y^2 = aU^2 + bUV + cUW + dVW + eW^2$$

Note that the affine chart of E_{p} corresponding to $W = 1$ is $\hat{E}_{\mathrm{a}}$. The points at infinity of E_{p} are the points $(U : V : W : Y) \in E_{\mathrm{p}}(\overline{K})$ with $W = 0$. If $W = 0$, then by the first equation $V = 0$ and by the second equation $Y^2 = aU^2$. So the only points at infinity are $(1 : 0 : 0 : \pm\sqrt{a})$. So we see that E_{p} is the union of its affine charts corresponding to $U = 1$ and $W = 1$.

If we take the affine chart in $\mathbb{A}^3_{r,s,t}$ corresponding to $U = 1$, we get the curve $\hat{E}'_{\mathrm{a}}/K$ given by

$$s = r^2$$

$$t^2 = a + br + cs + drs + es^2$$

The points $(0, 0, \pm\sqrt{a})$ are smooth on this curve, so $(1 : 0 : 0 : \pm\sqrt{a})$ are smooth points of E_{p} and E_{p} is smooth. Let E'_{a}/K be the affine curve in $\mathbb{A}^2_{p,q}$ given by

$$q^2 = p^4 h(1/p) = a + bp + cp^2 + dp^3 + ep^4.$$

Then we see that E'_{a} and $\hat{E}'_{\mathrm{a}}$ are isomorphic in the same way that E_{a} and $\hat{E}_{\mathrm{a}}$ are. So we see we can view E_{p} as the union of E_{a} and E'_{a}, where we use the identification $(x, y) = (p, q)$ if $(x^2 : x : 1 : y) = (1 : p : p^2 : q)$.

Note that $(0, 0, \pm\sqrt{a})$ may not lie in $E_{\mathrm{p}}(K)$. So unlike in the previous section, we do not known of any point $O \in E_{\mathrm{p}}(K)$ needed to define an elliptic curve over K. To proceed we need to assume that we have such a point. So we assume that we have a point $(x_0, y_0) \in E_{\mathrm{a}}(K)$, where E_{a}/K was the affine curve given by

$$y^2 = h(x) = ax^4 + bx^3 + cx^2 + dx + e.$$

This means that $(x_0^2 : x_0 : 1 : y_0) \in E_{\mathrm{p}}(K)$ and we will prove that (E_{p}, O) is an elliptic curve using Proposition 3.2. The isomorphism that we want, will be the composition of multiple isomorphisms. For the first one, note that $(0, y_0)$ satisfies $y^2 = h(x + x_0)$. Let $\tilde{h} = h(x + x_0)$, then $(x, y) \mapsto (x - x_0, y)$ is an isomorphism between E_{a} and the curve $\tilde{E}_{\mathrm{a}}/K$ in $\mathbb{A}^2_{x,y}$ given by $y^2 = \tilde{h}(x)$. For $\tilde{E}_{\mathrm{a}}$ we can construct a smooth projective curve $\tilde{E}_p$ such that $\tilde{E}_{\mathrm{a}}$ is isomorphic to an affine chart of $\tilde{E}_{\mathrm{p}}$ in the same way as for E_{a} and we can extend the isomorphism $E_{\mathrm{a}} \to \tilde{E}_{\mathrm{a}}$ to an isomorphism $E_{\mathrm{p}} \to \tilde{E}_{\mathrm{p}}$.

Proposition 3.8. The rational map $f : \mathbb{P}^3_{U,V,W,Y} \dashrightarrow \mathbb{P}^3_{\tilde{U},\tilde{V},\tilde{W},\tilde{Y}}$ sending $(U : V : W : Y) \mapsto (U - 2x_0V + x_0^2W : V - x_0W : W : Y)$ induces to an isomorphism over K from E_p/K to the projective curve $\tilde{E}_\mathrm{p}/K$ defined by

$$\tilde{U}\tilde{W} = \tilde{V}^2$$
$$\tilde{Y}^2 = a\tilde{U}^2 + b'\tilde{U}\tilde{V} + c'\tilde{U}\tilde{W} + d'\tilde{V}\tilde{W} + y_0^2\tilde{W}^2$$

where $\tilde{h}(x) = h(x + x_0) = ax^4 + b'x^3 + c'x^2 + d'x + y_0^2$.

Proof. One can check that substituting $(\tilde{U} : \tilde{V} : \tilde{W} : \tilde{Y}) = (U - 2x_0V + x_0^2W : V - x_0W : W : Y)$ into the equations for $\tilde{E}_\mathrm{p}$ gives us the equations for E_p. This means that $f^{-1}(\tilde{E}_\mathrm{p}) = E_\mathrm{p}$ and therefore f induces a linear transformation $E_\mathrm{p} \to \tilde{E}_\mathrm{p}$. ☐

So after a linear transformation we may assume that $x_0 = 0$ and $e = y_0^2$ and we will do this from now on. For the next part we need a lemma which we will also use later to find curves of the form $y^2 = h(x)$ together with points on that curve.

Lemma 3.9. Let K be a field with $\mathrm{char}(K) \neq 2$. Let $f = \sum_{i=0}^{2n} a_ix^i \in K[x]$ with $a_{2n} = a^2 \in K^{*2}$. Define $b_n = a$ and for $i = n-1, \dots, 0$ define

$$b_i = \frac{1}{2a}\left(a_{n+i} - \sum_{k=i+1}^{n-1} b_kb_{n+i-k}\right)$$

recursively. Next let $g = \sum_{i=0}^{n} b_ix^i \in K[x]$ and $h = g^2 - f$. Then g is of degree n, the degree of h is less than n and $f = g^2 - h$. Furthermore the pair (g, h) is unique with these properties up to multiplication of g by -1.

Proof. Write $g = \sum_{i=0}^{n} b_ix^i$ and let $h = g^2 - f$. We want to the b_i to be such that the degree of h is less than n. This is equivalent to having

$$a_{n+i} = \sum_{k=i}^{n} b_kb_{n+i-k}$$

for $i = 0, \dots, n$, because we want the coefficient of f and g^2 to be equal at x^{n+i} for $i = 0, \dots, n$. For $i = n$ this means that $a^2 = a_{2n} = b_n^2$. Hence $b_n = \pm a$. Now we rewrite the conditions for $i = 0, \dots, n-1$ to

$$a_{n+i} = b_ib_n + \sum_{k=i+1}^{n-1} b_kb_{n+i-k} + b_nb_i.$$

So we have

$$b_i = \frac{1}{2b_n}\left(a_{n+i} - \sum_{k=i+1}^{n-1} b_kb_{n+i-k}\right).$$

Note that only $b_{i+1}, \dots, b_n$ occur on the right hand side. Therefore we can solve these equation recursively in the order $i = n-1, \dots, 0$. We see that $g = \sum_{i=0}^{n} b_ix^i$ and let $h = g^2 - f$ have the desired properties. Furthermore b_n is unique up to multiplication by -1 and b_jb_n for $j < n$ only depends on the a_i. Hence g is unique up to multiplication by -1. So g^2 is unique and therefore so is $h = g^2 - f$. ☐

From now on we will also assume that $y_0 \neq 0$. Note that there are at most four points on E_a such that $y = 0$, namely the roots of h, and we will be looking for elliptic curves with many points. Therefore in practice we will always be able to find a point (x_0, y_0) with $y_0 \neq 0$. Note that E'_a is given by a Weierstrass equation if $(0,0)$ is a point on E_a. So we would still have an elliptic curve if y_0 were 0.

By the previous Lemma we can write

$$p(x) = a + bx + cx^2 + dx^3 + y_0^2x^4 = (y_0x^2 + \gamma x + \delta)^2 - (\alpha x + \beta)$$

for some unique $\gamma, \delta, \alpha, \beta \in K$. Note that $\alpha x + \beta$ is non-zero, because otherwise $p(x)$ would be a square and therefore $h(x) = x^4 p(1/x)$ would also be a square. But $h(x)$ has no double roots, so it is in particular not a square. Using this equality, we can rewrite the equation for E_a and in the same we can rewrite the second equation for E_p.

One can check using $UW = V^2$ that

$$aU^2 + bUV + cUW + dVW + y_0^2W^2 = (y_0W + \gamma V + \delta U)^2 - (\alpha UV + \beta U^2).$$

Therefore we can rewrite the second equation for E_p to

$$\alpha UV + \beta U^2 = (y_0W + \gamma V + \delta U)^2 - Y^2 = (y_0W + \gamma V + \delta U + Y)(y_0W + \gamma V + \delta U - Y).$$

Take $\Theta = y_0W + \gamma V + \delta U + Y$, then this equation becomes

$$\alpha UV + \beta U^2 = \Theta(2y_0W + 2\gamma V + 2\delta U - \Theta).$$

Now define the projective curve E'_p/K in $\mathbb{P}^3_{U,V,W,\Theta}$ by

$$UW = V^2$$

$$\alpha UV + \beta U^2 = \Theta(2y_0W + 2\gamma V + 2\delta U - \Theta)$$

The substitution $\Theta = y_0W + \gamma V + \delta U + Y$ gives the following isomorphism.

Proposition 3.10. The rational map $f : \mathbb{P}^3_{U,V,W,Y} \dashrightarrow \mathbb{P}^3_{U,V,W,\Theta}$ sending $(U : V : W : Y) \mapsto (U : V : W : y_0W + \gamma V + \delta U + Y)$ induces to an isomorphism over K from E_p/K to E'_p/K.

Proof. The substitution $\Theta = y_0W + \gamma V + \delta U + Y$ into the second equation for E'_p gives us the second equation for E_p. Therefore $f^{-1}(E'_\mathrm{p}) = E_\mathrm{p}$. Hence f induces a linear transformation between E_p/K and E'_p/K. □

Next we multiply the second equation for E'_p by $U^3\Theta$ and we use $UW = V^2$ to get

$$\alpha U^4V\Theta + \beta U^5\Theta = 2y_0U^2V^2\Theta^2 + 2\gamma U^3V\Theta^2 + 2\delta U^4\Theta^2 - U^3\Theta^3.$$

Note that we also get this equation if we substitute $(R : S : T) = (U\Theta : V\Theta : U^2)$ in

$$\alpha ST^2 + \beta RT^2 = 2y_0S^2T + 2\gamma RST + 2\delta R^2T - R^3$$

which we can also write as

$$2y_0S^2T + 2\gamma RST - \alpha ST^2 = R^3 - 2\delta R^2T + \beta RT^2.$$

Define the projective curve E''_p/K in $\mathbb{P}^2_{R,S,T}$ by this equation.

Proposition 3.11. Let

$$\begin{array}{rcl} f_1 : \mathbb{P}^3_{U,V,W,\Theta} & \dashrightarrow & \mathbb{P}^2_{R,S,T} \\ (U:V:W:\Theta) & \mapsto & (U\Theta : V\Theta : U^2) \end{array}$$

be the rational map defined for points such that $U \neq 0$. Let

$$\begin{array}{rcl} f_2 : \mathbb{P}^3_{U,V,W,\Theta} & \dashrightarrow & \mathbb{P}^2_{R,S,T} \\ (U:V:W:\Theta) & \mapsto & (V\Theta : W\Theta : UV) \end{array}$$

be the rational map defined for points such that $W\Theta \neq 0$. Let

$$\begin{array}{rcl} f_3 : \mathbb{P}^3_{U,V,W,\Theta} & \dashrightarrow & \mathbb{P}^2_{R,S,T} \\ (U:V:W:\Theta) & \mapsto & (\alpha V + \beta U : \alpha W + \beta V : 2y_0 W + 2\gamma V + 2\delta U - \Theta) \end{array}$$

be the rational map defined for points such that $2y_0W + 2\gamma V + 2\delta U - \Theta \neq 0$. Then together f_1, f_2 and f_3 induce an isomorphism $f : E'_{\mathrm{p}} \to E''_{\mathrm{p}}$ defined over K.

Proof. First we want to show that f is well defined. Suppose that $U \neq 0$ and $W\Theta \neq 0$, then $W \neq 0$, $V^2 = UW \neq 0$ and therefore $V \neq 0$. Hence $V/U \neq 0$. Note that $(V\Theta, W\Theta, UV) = V/U(U\Theta, W\Theta, U^2)$. Hence f_1 and f_2 restrict to the same map.

Next suppose that $U \neq 0$ and $2y_0W + 2\gamma V + 2\delta U - \Theta \neq 0$, then we split into two cases. If $\Theta \neq 0$, then

$$(\alpha V + \beta U : \alpha W + \beta V : 2y_0W + 2\gamma V + 2\delta U - \Theta) = \frac{\alpha V + \beta U}{U\Theta}(U\Theta : V\Theta : U^2)$$

and if $\Theta = 0$, then $(\alpha V + \beta U)U = 0$ so $\alpha V + \beta U = 0$ and $(\alpha W + \beta V)U = V(\alpha V + \beta U) = 0$ so $\alpha W + \beta V = 0$. Therefore

$$(U\Theta : V\Theta : U^2) = (0:0:1) = (\alpha V + \beta U : \alpha W + \beta V : 2y_0W + 2\gamma V + 2\delta U - \Theta).$$

Hence f_1 and f_3 restrict to the same map.

Now suppose that $W\Theta \neq 0$ and $2y_0W + 2\gamma V + 2\delta U - \Theta \neq 0$. Note that if $V = 0$, then $U = 0$ since $UW = V^2 = 0$ and $W \neq 0$. However $\Theta(2y_0W + 2\gamma V + 2\delta U - \Theta) \neq 0$ so $(\alpha V + \beta U)U \neq 0$. Hence $V \neq 0$. We have

$$(\alpha V + \beta U : \alpha W + \beta V : 2y_0W + 2\gamma V + 2\delta U - \Theta) = \frac{\alpha V + \beta U}{V\Theta}(V\Theta : W\Theta : UV).$$

Hence f_2 and f_3 restrict to the same map.

Now note that if $U = 0$, then $V^2 = UW = 0$ so $V = 0$. Hence $\Theta(2y_0W - \Theta) = 0$. So the only points with $U = 0$ are $(0:0:1:0)$ and $(0:0:1:2y_0)$. Hence we see that together f_1, f_2 and f_3 define a morphism.

Note that f_2 and f_3 can be derived from f_1 by multiplying each coordinate with some rational function g. To find the inverse of f we consider the rational map $(R:S:T) \mapsto (R^2T : RST : S^2T : R^3)$ for $S \neq 0$ or $RT \neq 0$. When $S = 0$ and $RT = 0$, we can multiply each coordinate by $g = 1/T$ and $g = (S^2 + \beta T^2 - 2\gamma RT - 2\delta ST)^2/R^2$ to find that there is in fact an inverse morphism. Hence f is an isomorphism. □

So by combining Propositions 3.10 and 3.11, we see that E_p is isomorphic to E''_p and E''_p is isomorphic to a projective curve given by a Weierstrass equation by Proposition 3.7. One can check that this isomorphism sends (x_0, y_0) to $\mathcal{O}$. Hence $(E_\mathrm{p}, (x_0, y_0))$ is an elliptic curve over K by Proposition 3.2. This result is summarised in the following theorem.

Theorem 3.12. Let $h(x) = ax^4 + bx^3 + cx^2 + dx + e \in K[x]$ be a polynomial of degree 4 with no double roots in $\overline{K}$ and let $(x_0, y_0) \in \mathbb{A}^2$ be a point such that $h(x_0) = y_0^2 \neq 0$. Let E_p/K in $\mathbb{P}^3_{U,V,W,Y}$ be the projective curve given by the two equations

$$UW = V^2$$

$$Y^2 = aU^2 + bUV + cUW + dVW + eW^2$$

Let E_a/K in $\mathbb{A}^2_{x,y}$ be the affine curve given by $y^2 = h(x)$ and let E'_a/K be the affine curve in $\mathbb{A}^2_{p,q}$ given by $q^2 = p^4 h(1/p)$. Then we can view E_p as the union of $E_\mathrm{a} \subseteq E_\mathrm{p}$ and $E'_\mathrm{a} \subseteq E_\mathrm{p}$ using the identification $(x, y) = (p, q)$ if $(x^2 : x : 1 : y) = (1 : p : p^2 : q)$ and $(E_\mathrm{p}, (x_0, y_0))$ is an elliptic curve over K.

Note that we know how to add and subtract points in $E_\mathrm{p}(K)$, because we have an isomorphism between $E_\mathrm{p}(K)$ and $E''_\mathrm{p}(K)$ and we know how to add and subtract points in $E''_\mathrm{p}(K)$. See the end of section 3.1.

For example, let $R = (x_0, -y_0)$, $P = (x_1, y_1) \in E_\mathrm{a}(K)$ and $Q = (x_1, -y_1) \in E_\mathrm{a}(K)$ with $x_1 \neq x_0$. Then we can map P, Q and R to E''_p. Let E''_a be the affine chart of E''_p in $\mathbb{A}^2_{r,s}$, which is given by

$$2y_0 s^2 + 2\gamma rs - \alpha s = r^3 - 2\delta r^2 + \beta r.$$

Then we will find that R maps to $-(0, 0) \in E''_\mathrm{a}(K)$ and that P and Q map to points in $E''_\mathrm{a}(K)$ that lie on the line $s = \frac{1}{x_1 - x_0} r$. Hence $P + Q = R$, because the images of P, Q and $-R$ lie on a line in $E''_\mathrm{a}(K)$.

This same statement can be proven using Theorem 3.4. This method requires us to find a function with zeros of order 1 at P and Q and poles of order 1 at O and R. One might think this function is $\frac{x - x_0}{x - x_1}$, which is the correct idea. However it is important to note that $\frac{x - x_0}{x - x_1}$ is not actually an element of the function field of E_p, since E_a is not an affine chart of E_p, but the function field of E_a and the function field of E_p are isomorphic since E_a is isomorphic to an affine chart of E_p that contains a point. So in stead, we have to look at the image of $\frac{x - x_0}{x - x_1}$ in the function field of E_p, which does work.

Chapter 4

The rank of an elliptic curve over $\mathbb{Q}$

Recall that for any elliptic curve E/K the group $E(K)$ is abelian and abelian groups have a unique $\mathbb{Z}$-module structure. This allows us to define the rank of an elliptic curve.

Definition 4.1. Let G be an abelian group and let $g_1, \ldots, g_m \in G$. We call $g_1, \ldots, g_m$ linearly independent (over $\mathbb{Z}$) if for all $k_1, \ldots, k_m \in \mathbb{Z}$

$$k_1 g_1 + k_2 g_2 + \cdots + k_m g_m = 0 \quad \Rightarrow \quad k_1 = k_2 = \cdots = k_m = 0.$$

Definition 4.2. Let G be abelian group. Then the rank $\mathrm{rank}(G)$ of G is defined as

$$\mathrm{rank}(G) = \sup\{n \in \mathbb{N}_0 : \exists g_1, \ldots, g_n \in G \text{ linearly independent}\}.$$

For elliptic curves E_{p} over K, we often say the rank of E_{p}/K when we mean the rank of $E_{\mathrm{p}}(K)$. If K is a number field, then we have the following result.

Theorem 4.3 (Mordell-Weil Theorem)**.** Let K be a number field and let E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.

Proof. See Theorem VIII.6.7 of [1] □

Hence elliptic curves over a number field have a finite rank.

Proposition 4.4. Let G be a finitely generated abelian group with torsion subgroup T, then the rank of G is finite and $G \cong \mathbb{Z}^{\mathrm{rank}(G)} \times T$.

Proof. By the structure theorem of finitely generated abelian groups we know that $G \cong \mathbb{Z}^r \times T$ for some $r \in \mathbb{N}_0$. We see that $\mathrm{rank}(G) \geq r$, because $\mathbb{Z}^r \times T$ contains r linearly independent vectors $e_i = (0, \ldots, 1, \ldots, 0)$ where 1 is at the i'th place.

Now let $(v_1, t_1), \ldots, (v_m, t_m) \in \mathbb{Z}^r \times T$ be linearly independent and write $|T|$ for the order of T. Suppose that $k_1 v_1 + k_2 v_2 + \cdots + k_m v_m = 0$ for some $k_1, \ldots, k_m \in \mathbb{Z}$, then also $|T| k_1 v_1 + |T| k_2 v_2 + \cdots + |T| k_m v_m = 0$. Therefore

$$\begin{aligned} |T|k_1(v_1, t_1) + \cdots + |T|k_m(v_m, t_m) &= k_1(|T|v_1, |T|t_1) + \cdots + k_m(|T|v_m, |T|t_m) \\ &= k_1(|T|v_1, 0) + \cdots + k_m(|T|v_m, 0) \\ &= 0 \end{aligned}$$

Hence since $(v_1, t_1), \ldots, (v_m, t_m)$ are linearly independent and $|T| \geq 1$, we see that $k_1 = \cdots = k_m = 0$. So are $v_1, \ldots, v_m$ also linearly independent. Now consider $v_1, \ldots, v_m$ as elements of $\mathbb{Q}^r$ and suppose that

$$\frac{p_1}{q_1} v_1 + \frac{p_2}{q_2} v_2 + \cdots + \frac{p_m}{q_m} v_m = 0$$

for some $p_1, \dots, p_m \in \mathbb{Z}$ and $q_1, \dots, q_m \in \mathbb{Z}\backslash\{0\}$, then also

$$p_1 q_2 \dots q_m v_1 + q_1 p_2 q_3 \dots q_m v_2 + \dots + q_1 \dots q_{n-1} p_m v_m = 0.$$

Hence $p_1 q_2 \dots q_m = \dots = q_1 \dots q_{m-1} p_m = 0$, because $v_1, \dots, v_m$ are linearly independent over $\mathbb{Z}$. Since $q_1, \dots, q_m \in \mathbb{Z}\backslash\{0\}$, we see $p_1 = p_2 = \dots = p_m = 0$. Hence $v_1, \dots, v_m$ are linearly independent vectors of the $\mathbb{Q}$-vectorspace $\mathbb{Q}^r$. Hence $r \geq m$. □

4.1 Proving the linear independence of points on an elliptic curve over $\mathbb{Q}$

The goal of this thesis is to find elliptic curves $E_\mathrm{p}/\mathbb{Q}$ with a high rank. Therefore we will look for elliptic curves $E_\mathrm{p}/\mathbb{Q}$ with many linearly independent points in $E_\mathrm{p}(\mathbb{Q})$. Now we will look at a method to prove that elements of $E_\mathrm{p}(\mathbb{Q})$ are linearly independent using a bilinear map. In this section, let E_p be an elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + Ax^2 + Bx + C$ for some $A, B, C \in \mathbb{Q}$.

Definition 4.5. The height function $H : \mathbb{Q} \to \mathbb{R}$ on $\mathbb{Q}$ is defined as $h(x) = \max\{|p|, |q|\}$ where $x = p/q$ and $\gcd(p, q) = 1$.

Definition 4.6. The (logarithmic) height $h : E_\mathrm{p}(\mathbb{Q}) \to \mathbb{R}$ on E_p is defined as $h(\mathcal{O}) = 0$ and $h((x, y)) = \log(H(x))$.

Proposition 4.7. Let $P \in E_\mathrm{p}(\mathbb{Q})$. Then $4^{-n}h(2^n P)$ converges as $n \to \infty$.

Proof. Let $f(x) = x$, then the function f is even because $-(x, y) = (x, -y)$ when E_p is given by $y^2 = x^3 + Ax^2 + Bx + C$. Therefore $4^{-n}h(2^n P)$ converges as $n \to \infty$ by Proposition VIII.9.1 of [1]. □

Definition 4.8. The canonical height $\hat{h} : E_\mathrm{p}(\mathbb{Q}) \to \mathbb{R}$ on E_p is the map defined as

$$\hat{h}(P) = \lim_{n\to\infty} 4^{-n} h(2^n P).$$

The canonical height pairing $\langle \cdot, \cdot \rangle : E_\mathrm{p}(\mathbb{Q}) \times E_\mathrm{p}(\mathbb{Q}) \to \mathbb{R}$ on E_p is the map defined as

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Proposition 4.9. The canonical height pairing $\langle \cdot, \cdot \rangle$ on E_p is bilinear.

Proof. See Theorem VIII.9.2 of [1]. □

Proposition 4.10. Let $P_1, \dots, P_m \in E(\mathbb{Q})$ be points such that the matrix $(\langle P_i, P_j \rangle)_{i,j=1}^m$ is invertible, then $P_1, \dots, P_m$ are linearly independent.

Proof. Suppose that $P_1, \dots, P_m$ are linearly dependent, then there exist $k_1, \dots, k_m \in \mathbb{Z}$ not all zero such that $k_1 P_1 + \dots + k_m P_m = 0$. Since $\langle \cdot, \cdot \rangle$ is bilinear, we also have $k_1 \langle Q, P_1 \rangle + \dots + k_m \langle Q, P_m \rangle = 0$ for any $Q \in E(\mathbb{Q})$. Take $Q = P_1, \dots, P_m$, then we see that

$$(\langle P_i, P_j \rangle)_{i,j=1}^m (k_1, \dots, k_m)^T = (0, \dots, 0)^T.$$

Since $k_1, \dots, k_m$ are not all zero, we see that $(\langle P_i, P_j \rangle)_{i,j=1}^m$ is not invertible. Hence $P_1, \dots, P_m$ are linearly independent if $(\langle P_i, P_j \rangle)_{i,j=1}^m$ is invertible. □

Note that the matrix $(\langle P_i, P_j\rangle)_{i,j=1}^m$ can only be approximated and the determinant of $(\langle P_i, P_j\rangle)_{i,j=1}^m$ can be 0 while the determinant of its approximation is close to but not equal to zero. Therefore we cannot conclude that $P_1, \dots, P_m$ are linearly independent when all we know is that the approximated determinant is non-zero.

We can however give an approximation of the determinant of $(\langle P_i, P_j\rangle)_{i,j=1}^m$ using the division-free method built into SAGE. This method uses only addition, subtraction and multiplication and the number of operations used is bounded by a polynomial in m. See [3] for more details. Hence if we approximate $(\langle P_i, P_j\rangle)_{i,j=1}^m$ well enough, which we can do using the `height_pairing_matrix` command of SAGE, then we can also approximate its determinant such that the difference between the approximation and the real value is at most some $\varepsilon > 0$.

Also note that this method to determine if points are linearly independent is for an elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + Ax^2 + Bx + C$ only. So we have to convert elliptic curves to that form.

Chapter 5

Infinite families of elliptic curves over $\mathbb{Q}$ with high rank

Assume that $\mathrm{char}(K) \neq 2$ and take $k \in \mathbb{N}$. Let $b_1, \ldots, b_{2k}$ be elements of K and take $b = (b_1, \ldots, b_{2k}) \in \mathbb{A}^{2k}(K)$. Consider $f_b = \prod_{i=1}^{2k}(x - b_i) \in K[x]$. By Lemma 3.9, there are unique $g_b, h_b \in K[x]$ such that $f_b = g_b^2 - h_b$, $\deg(g_b) = k$ and $\deg(h_b) < k$. Note we can view the coefficients of h_b as elements of $K[b_1, \ldots, b_{2k}]$, since we can find them from $b_1, \ldots, b_{2k}$ using only addition, multiplication and division by 2. Write

$$h_b = \sum_{i=0}^{k-1} h_{bi}(b_1, \ldots, b_{2k}) x^i$$

with $h_{bi} \in K[b_1, \ldots, b_n]$. Now let $d \in \{3, 4\}$ and let $\mathcal{A}_{kd}$ in $\mathbb{A}^{2k}_{b_1,\ldots,b_{2k}}$ be the affine set given by the equations $h_{bi}(b_1, \ldots, b_{2k}) = 0$ for $i = d+1, \ldots, k-1$. Then $\mathcal{A}_{kd}(K)$ is the set of all b such that $\deg(h_b) \leq d$. Let $\mathcal{B}_{kd}(K) \subseteq \mathcal{A}_{kd}(K)$ be the set of all b such that

- the b_i are all distinct;
- $\deg(h_b) = d$;
- h_b has no double roots in $\overline{K}$;
- and $g_b(b_1) \neq 0$ if $d = 4$.

Note that if $\deg(h_b) = 4$ and $g_b(b_i) = 0$, then $h_b(b_i) = g_b(b_i)^2 = 0$. So in this case there are at most four b_i such that $g_b(b_i) = 0$ since the b_i are all different. Since $\deg(h_b) = 4 < k$ we have at least ten b_i. Therefore $g_b(b_1) \neq 0$ after a possible re-ordering of the b_i, which does not change g_b and h_b.

Note that the first condition can be expressed as $b_i - b_j \neq 0$ for all $i \neq j$. The second condition can be expressed as $h_{bd}(b_1, \ldots, b_{2k}) \neq 0$. Let Δ_d be the discriminant of a degree d polynomial viewed as an element of $K[b_1, \ldots, b_{2k}]$. Then the third condition is equivalent to $\Delta_d(b_1, \ldots, b_{2k})$ being non-zero. Lastly, $g_b(b_1)$ can be viewed as an element of $K[b_1, \ldots, b_{2k}]$. So $\mathcal{B}_{kd}(K)$ is the subset of $\mathcal{A}_{kd}(K)$ consisting of all elements b such that a finite set of polynomial are all non-zero at b. This means that that $\mathcal{B}_{kd}(K)$ is an open set in $\mathcal{A}_{kd}(K)$ with the induced topology of $\mathbb{A}^{2k}_{b_1,\ldots,b_{2k}}$.

Now let $b = (b_1, \ldots, b_{2k}) \in \mathcal{B}_{k3}(K)$. Then let E_{a}/K be the curve in $\mathbb{A}^2_{x,y}$ defined by $y^2 = h_b(x)$ and let E_{p}/K be its projective closure. Take $P_i = (b_i, g_b(b_i))$ and $Q_i = (b_i, -g_b(b_i))$ for

$i = 1, \ldots, 2k$, then we see that $P_i, Q_i \in E_{\mathrm{a}}(K)$ for all i. By Proposition 3.7, E_{p}/K is K-isomorphic to a projective curve given by a Weierstrass equation and therefore $(E_{\mathrm{p}}, \mathcal{O})$ is an elliptic curve over K by Proposition 3.2. We say that E_{p} is the elliptic curve corresponding to b.

Next let $b = (b_1, \ldots, b_{2k}) \in \mathcal{B}_{k4}(K)$, again let E_{a}/K be the curve in $\mathbb{A}^2_{x,y}$ defined by $y^2 = h_b(x)$ and take $P_i = (b_i, g_b(b_i))$ and $Q_i = (b_i, -g_b(b_i))$ for $i = 1, \ldots, 2k$. Take $(x_0, y_0) = Q_1$, then $y_0 \neq 0$, because $g_b(b_1) \neq 0$. Let E_{p}/K and E'_{a} be as in Theorem 3.12. Then E_{a} is K-isomorphic with the affine chart corresponding to $W = 1$ of E_{p}, which is the smooth projective curve given by

$$UW = V^2$$

$$Y^2 = aU^2 + bUV + cUW + dVW + eW^2$$

By Theorem 3.12, we know that (E_{p}, Q_1) is an elliptic curve over K. We say that (E_{p}, Q_1) is the elliptic curve corresponding to b.

So if we pick a $b \in \mathcal{B}_{kd}(\mathbb{Q})$, we find an elliptic curve E_{p} over $\mathbb{Q}$ together with $4k$ points on E_{p} that are $\mathbb{Q}$-rational. Note that for all i, $P_i + Q_i = \mathcal{O}$ if $d = 3$. Also we showed that $P_i + Q_i = P_1$ if $d = 4$ at the end of section 3.2. Hence Q_i can always be expressed in terms of P_i and P_1. So we know that at best $2k$ of the points we get are linearly independent. However by the following Proposition we know this will not be true for any b.

Proposition 5.1. Let $b = (b_1, \ldots, b_{2k}) \in \mathcal{B}_{kd}(\mathbb{Q})$, let (E_{p}, O) be the elliptic curve corresponding to b, let $P_i = (b_i, g_b(b_i)) \in E_{\mathrm{p}}(\mathbb{Q})$ and let $Q_i = (b_i, -g_b(b_i)) \in E_{\mathrm{p}}(\mathbb{Q})$, then $\sum_{i=1}^{2k} P_i = k(P_1 + Q_1)$.

Proof. By Theorem 3.4 we know that $\sum_{i=1}^{2k} P_i = k(P_1 + Q_1)$ holds if and only if

$$\sum_{i=1}^{2k} (P_i) - k((P_1) + (Q_1))$$

is a principal divisor. Consider the function $f = \frac{y - g_b(x)}{(x - b_1)^k} \in K(E_{\mathrm{p}})$. We know that $\mathrm{div}(f) = \mathrm{div}(y - g_b(x)) - k \cdot \mathrm{div}(x - b_1)$, so first look at the functions $y - g_b(x)$ and $x - b_1$.

Note that $y - g_b(x)$ has no poles in $E_{\mathrm{a}}(\overline{K})$. Suppose that $(x, y) \in E_{\mathrm{a}}(\overline{K})$ is a zero of $y - g_b(x)$, then $g_b(x)^2 = y^2 = h_b(x)$. So $f_b(x) = 0$ and $x = b_i$ for some i. Now we see that $y = g_b(b_i)$ and $(x, y) = P_i$.

Now consider $x - b_1$. It also has no poles in $E_{\mathrm{a}}(\overline{K})$ and we see that P_1 and Q_1 are the only zeros of $x - b_1$. To calculate the order of $x - b_1$ at P_1 and Q_1, first recall that $Q_1 = (b_1, -g_b(b_1))$ with $g_b(b_1) \neq 0$. Then note that

$$(y - g_b(b_1))(y + g_b(b_1)) = y^2 - g_b(b_1)^2 = h_b(x) - g_b(b_1)^2 = (x - b_1)r(x)$$

for some $r(x) \in K[x]$, because $h_b(x) - g_b(b_1)^2$ has a zero at b_1. So we see that $(y - g_b(b_1)) = (x - b_1)\frac{r(x)}{y + g_b(b_1)}$ and $\frac{r(x)}{y + g_b(b_1)} \in K[E_{\mathrm{p}}]_{P_1}$ since $y + g_b(b_1)$ is non-zero at P_1. Therefore $x - b_1$ generates the ideal $(x - b_1, y - g_b(b_1)) = \mathfrak{m}_{P_1} \subseteq K[E_{\mathrm{p}}]_{P_1}$ and $x - b_1$ has a zero of order 1 at P_1. In the same way we see that $x - b_1$ has a zero of order 1 at Q_1.

Now we know that f has zeros at $P_1, \ldots, P_{2k}$ of still unknown order and we know that f has poles of order k at P_1 and Q_1. Now we will consider what happens at infinity.

Suppose that $\deg(h_b) = 3$ and write $h_b(x) = h_3x^3 + h_2x^2 + h_1x + h_0$, then E_{p} is given by

$$Y^2Z = h_3X^3 + h_2X^2Z + h_1XZ^2 + h_0Z^3$$

and $O = \mathcal{O} = (0 : 1 : 0)$ is the only point at infinity. To calculate the order of f at $\mathcal{O}$, we need to go the affine chart of E_{p} corresponding to $Y = 1$. So we take $x = X/Y$ and $z = Z/Y$ and get the affine curve given by

$$z = h_3x^3 + h_2x^2z + h_1xz^2 + h_0z^3.$$

Note that $\mathcal{O}$ is $(0, 0)$ and f is $\frac{z^{k-1}-z^k g_b(x/z)}{(x-b_1z)^k}$ in this affine chart. We have

$$z(1 - h_0z^2) = z - h_0z^3 = h_3x^3 + h_2x^2z + h_1xz^2 = x(h_3x^2 + h_2xz + h_1z^2).$$

Therefore the ideal $(x, z) = \mathfrak{m}_{\mathcal{O}}$ of $K[E_{\mathrm{p}}]_{\mathcal{O}}$ is generated by x. Hence x has a zero of order 1 at $\mathcal{O}$. Write $\tau(x, z) = \frac{h_3x^2+h_2xz+h_1z^2}{1-h_0z^2}$, then we have

$$z = h_3x^3 + h_2x^2z + h_1xz^2 + h_0z^3 = x^3(h_3 + h_2\tau(x, z) + h_1\tau(x, z)^2 + h_0\tau(x, z)^3).$$

Note that $h_3 + h_2\tau(0, 0) + h_1\tau(0, 0)^2 + h_0\tau(0, 0)^3 = h_3 \neq 0$. This means that z, as a function, has a zero of order 3 at $\mathcal{O}$, because z is the product of x^3, which has a zero of order 3 at $\mathcal{O}$, and a function that has neither a zero nor a pole at $\mathcal{O}$.

Now we can go back to f. Note that $z^{k-1} - z^k g_b(x/z)$ has a zero of order k at $\mathcal{O}$, because $z^{k-1} - z^k g_b(x/z)$ contains a term x^k, which has a zero of order k at $\mathcal{O}$, and all other terms have a zero of higher order at $\mathcal{O}$. Similarly $(x - b_1z)^k$ has a zero of order k at $\mathcal{O}$. This means that f has order 0 at $\mathcal{O}$.

Next suppose that $\deg(h_b) = 4$. Recall that in this case, E_{p} has the two points $(1 : 0 : 0 : \pm\sqrt{a})$ at infinity, which correspond to the points $(0, \pm\sqrt{a})$ on the affine curve E'_{a} given by $q^2 = p^4h(1/p)$. One can check that f corresponds to the function $\frac{p^{2k-2}q-p^{2k}g_b(1/p)}{(p-b_1p^2)^k} = \frac{p^{k-2}q-p^k g_b(1/p)}{(1-b_1p)^k}$ in the function field of E'_{a}. We see that we get the top coefficient of g_b if we evaluate this function at the points $(0, \pm\sqrt{a})$. Therefore f has neither a zero or pole at these points.

So in both cases f has no zeros or poles at infinity. So since the degree of $\mathrm{div}(f)$ must be 0, since f has zeros at $P_1, \ldots, P_{2k}$ and since f has poles of order k at P_1 and Q_1, we now see that the zeros of f all have order 1. Hence

$$\mathrm{div}(f) = \sum_{i=1}^{2k}(P_i) - k((P_1) + (Q_1))$$

and $\sum_{i=1}^{2k} P_i = k(P_1 + Q_1)$. □

Corollary 5.2. Let $b = (b_1, \ldots, b_{2k}) \in \mathcal{B}_{kd}(\mathbb{Q})$, let (E_{p}, O) be the elliptic curve corresponding to b and let $G \subseteq E_{\mathrm{p}}(\mathbb{Q})$ be the subgroup of $E_{\mathrm{p}}(\mathbb{Q})$ generated by $P_i = (b_i, g_b(b_i))$ and $Q_i = (b_i, -g_b(b_i))$ for $i = 1, \ldots, 2k$. Then the rank of G is at most $2k - 1$.

Proof. Suppose that $\deg(h_b) = 3$, then $P_i + Q_i = \mathcal{O}$ for any i. Hence G is generated by $P_1, \ldots, P_{2k}$. By the previous Proposition, we know that $\sum_{i=1}^{2k} P_i = k(P_1 + Q_1) = \mathcal{O}$. Therefore $P_{2k} = -\sum_{i=1}^{2k-1} P_i$ and G is generated by $P_1, \ldots, P_{2k-1}$. So since G is generated by $2k - 1$ elements, the rank of G is at most $2k - 1$.

Suppose that $\deg(h_b) = 4$, then $Q_i = P_1 - P_i$ for any i, since Q_1 is the zero element. Hence G is generated by $P_1, \ldots, P_{2k}$. By the previous Proposition, we know that $\sum_{i=1}^{2k} P_i = kP_1$. Therefore $P_{2k} = kP_1 - \sum_{i=1}^{2k-1} P_i$ and G is generated by $P_1, \ldots, P_{2k-1}$. So again we see that the rank of G is at most $2k - 1$. □

We are looking for families of elliptic curves over $\mathbb{Q}$ with high rank. We will find such families by finding elliptic curves over $\mathbb{Q}(t)$ with high rank. Consider $b(t) = (b_1(t), \ldots, b_{2k}(t)) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$ as a function of t and let $b(t_0) = (b_1(t_0), \ldots, b_{2k}(t_0))$ for any $t_0 \in \mathbb{Q}$ such that $b_1(t_0), \ldots, b_{2k}(t_0)$ are all well defined. The next proposition will show that, in most cases, we will have $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$.

In these cases, we get the equations defining the elliptic curve corresponding to $b(t_0)$ by replacing t by t_0 in the equations that define the elliptic curve corresponding to $b(t)$. Also, we can try to evaluate points on the elliptic curve corresponding to $b(t)$ at t_0 to get points on the elliptic curve corresponding to $b(t_0)$. Since the coordinates of points on the elliptic curve corresponding to $b(t)$ are rational functions, we see that for any point there can only be finitely many $t_0 \in \mathbb{Q}$ where we fail to evaluate the point.

In general, we call an elliptic curve E over $\mathbb{Q}$, which we get by evaluating an elliptic curve E' over $\mathbb{Q}(t)$ at some $t_0 \in \mathbb{Q}$, the specialisation of E' at t_0. And we call the map sending points on E' to their evaluation at t_0, when it exists, the specialisation map.

Proposition 5.3. Let $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$, then there are only finitely many $t_0 \in \mathbb{Q}$ such that either $b(t_0)$ is not defined or $b(t_0) \notin \mathcal{B}_{kd}(\mathbb{Q})$.

Proof. First note that $b_1(t), \ldots, b_{2k}(t)$ are rational functions. So for each i we can write $b_i(t) = f(t)/g(t)$ for some $f, g \in \mathbb{Q}[t]$ with $g \neq 0$. Since $g \in \mathbb{Q}[t]$ is non-zero, there are only finitely many $t_0 \in \mathbb{Q}$ such that $g(t_0) = 0$. So for only finitely many t_0, $b_i(t_0)$ is not well defined. Hence there are also only finitely many t_0 such that $b(t_0)$ is not well defined.

Now consider the $t_0 \in \mathbb{Q}$ such that $b(t_0)$ is well defined. Note that we get $h_{b(t_0)}$ and $g_{b(t_0)}$ if we replace t in $h_{b(t)}$ and $g_{b(t)}$ by t_0. This means that we get

- $h_{b(t_0)i}(b_1(t_0), \ldots, b_{2k}(t_0))$ for $i = 0, \ldots, k-1$,
- $b_i(t_0) - b_j(t_0)$ for all $i \neq j$,
- $\Delta_d(b_1(t_0), \ldots, b_{2k}(t_0))$
- and $g_{b(t_0)}(b_1(t_0))$

by evaluating the corresponding rational function at t_0. Since $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$, we know that

- $b(t) \in \mathcal{A}_{kd}(\mathbb{Q}(t))$,
- $b_i(t) - b_j(t) \neq 0$ for all $i \neq j$,
- $h_{bd}(b_1(t), \ldots, b_{2k}(t)) \neq 0$,
- $\Delta_d(b_1(t), \ldots, b_{2k}(t)) \neq 0$
- and $g_{b(t)}(b_1(t)) \neq 0$.

This means that $b(t_0) \in \mathcal{A}_{kd}(\mathbb{Q})$, because $h_{b(t_0)i}$ is the zero function for $i = d+1, \ldots, k-1$. Since $b_i(t) - b_j(t)$, $h_{bd}(b_1(t), \ldots, b_{2k}(t))$, $\Delta_d(b_1(t), \ldots, b_{2k}(t))$ and $g_{b(t)}(b_1(t))$ are non-zero, there are only finitely many $t_0 \in \mathbb{Q}$ such that they are 0 at t_0. Hence there are only finitely many $t_0 \in \mathbb{Q}$ such that $b(t_0) \notin \mathcal{B}_{kd}(\mathbb{Q})$. □

Theorem 5.4. Let $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$. If $R_1(t), \ldots, R_m(t)$ are linearly independent $\mathbb{Q}(t)$-rational points on the elliptic curve over $\mathbb{Q}(t)$ corresponding to $b(t)$, then there are only finitely many $t_0 \in \mathbb{Q}$ with $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$ such that $R_1(t_0), \ldots, R_m(t_0)$ are not well-defined linearly independent $\mathbb{Q}$-rational points on the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$.

Proof. When $b(t_0) \in \mathcal{B}(\mathbb{Q})$, we get the elliptic curve corresponding to $b(t_0)$ by evaluating the elliptic curve corresponding to $b(t)$ at t_0. Note that $Q(t) = \mathbb{Q}(\mathbb{P}^1)$. Theorem C.20.3 of [1] now tells us that for all but finitely many t_0 the specialisation map is injective on the points where it is defined. So for all but finitely many $t_0 \in \mathbb{Q}$ the points $R_1(t_0), \ldots, R_m(t_0)$ are linearly independent when they are well defined, which they are at all but finitely many t_0. □

So from a $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$ such that its corresponding elliptic curve has a high rank, we get an infinite family of elliptic curves with at least the same rank. We have similar statements in the other direction.

Proposition 5.5. Let $b_1(t), \ldots, b_{2k}(t) \in \mathbb{Q}(t)$ and $d \in \{3, 4\}$. Take $b(t) = (b_1(t), \ldots, b_{2k}(t))$ and $t_0 \in \mathbb{Q}$. Suppose that $b(t) \in \mathcal{A}_{kd}(\mathbb{Q}(t))$, that $b_i(t_0)$ is well defined for each i and that $b(t_0) = (b_1(t_0), \ldots, b_{2k}(t_0)) \in \mathcal{B}_{kd}(\mathbb{Q})$. Then $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$.

Proof. Note that $b_1(t_0), \ldots, b_{2k}(t_0)$ are all different, because $b(t_0) \in \mathcal{B}(\mathbb{Q})$. So we see that $b_1(t), \ldots, b_{2k}(t)$ must also be all different. Next note that the coefficient of $h_{b(t)}$ at x^d evaluated at t_0 is the leading coefficient of $h_{b(t_0)}$, which is non-zero. Therefore the coefficient of $h_{b(t)}$ at x^d is a non-zero rational function and we have $\deg(h_{b(t)}) = d$. The discriminant Δ of $h_{b(t)}$ is an element of $\mathbb{Q}(t)$, which is the discriminant of $h_{b(t_0)}$ when evaluated at t_0. Hence Δ is non-zero as rational function, because $b(t_0) \in \mathcal{B}(\mathbb{Q})$ and therefore Δ evaluated at t_0 is non-zero. Lastly $g_{b(t)}(b_1(t))$ is non-zero if $d = 4$, since $g_{b(t_0)}(b_1(t_0))$ is non-zero if $d = 4$. Hence $b(t) \in \mathcal{B}(\mathbb{Q}(t))$. □

Proposition 5.6. Let $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$ and let $t_0 \in \mathbb{Q}$ such that $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$. Suppose that $R_1(t), \ldots, R_m(t)$ are $\mathbb{Q}(t)$-rational points on the elliptic curve over $\mathbb{Q}(t)$ corresponding to $b(t)$ such that $R_1(t_0), \ldots, R_m(t_0)$ are well-defined linearly independent $\mathbb{Q}$-rational points on the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$. Then $R_1(t), \ldots, R_m(t)$ are linearly independent.

Proof. Suppose that $k_1R_1(t) + \cdots + k_mR_m(t) = O$ for some $k_1, \ldots, k_m \in \mathbb{Z}$. Note that if $P(t)$ and $Q(t)$ are $\mathbb{Q}(t)$ rational points on the elliptic curve over $\mathbb{Q}(t)$ corresponding to $b(t)$ such that $P(t_0)$ and $Q(t_0)$ are well-defined, then $(P+Q)(t_0) = P(t_0) + Q(t_0)$, i.e. the specialisation is a homomorphism. This means that $k_1R_1(t_0) + \cdots + k_mR_m(t_0) = O$. Therefore $k_1 = \cdots = k_m = 0$, because $R_1(t_0), \ldots, R_m(t_0)$ are linearly independent. Hence $R_1(t), \ldots, R_m(t)$ are linearly independent. □

So we can find infinite families of elliptic curves with high rank by finding a $b(t) \in \mathcal{A}_{kd}(\mathbb{Q}(t))$ and a $t_0 \in \mathbb{Q}$ such that $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that $\{P_1(t_0), \ldots, P_{2k-1}(t_0)\}$ has a big independent subset. Then using Proposition 5.5, we get an elliptic curve over $\mathbb{Q}(t)$, which has a independent subset of the same size by Proposition 5.6. This gives us an infinite family of elliptic curves using Proposition 5.3 and by Theorem 5.4 all but finitely many of these elliptic curves again have an independent subset of the same size. First we will choose k to be 4 or 5, because then $b(t) \in \mathcal{A}_{kd}(\mathbb{Q}(t))$ will always hold for $d = k-1$. However with some more work, we can also choose k to be 6 or 8.

Note that in general, having an infinite family of elliptic curves does not mean that we we have infinitely many elliptic curves that are pairwise not isomorphic. However, in our case we can prove relatively simply that we do. More precisely, we can prove that an elliptic curve within our family can only be isomorphic to finitely many other elliptic curves within our family.

Definition 5.7. Let E_{p} be an elliptic curve over K given by a Weierstrass equation

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

for some $a_1, a_2, a_3, a_4, a_6 \in K$. Take

$$\begin{aligned} b_2 &= a_1^2 + 4a_4 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned}$$

and define

$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \end{aligned}$$

By Proposition III.1.4(a)(i) of [1], we know that $\Delta \neq 0$, because E_{p} is smooth. So j is well defined. We call j the j-invariant of the elliptic curve E_{p}. By Proposition III.1.4(b), we know that two elliptic curves are isomorphic over $\overline{K}$ if and only if their j-invariants are equal. We can use this to get the following result.

Proposition 5.8. Let $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$, let $t_0 \in \mathbb{Q}$ such that $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$ and let E_{p} be the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$. Then either all elliptic curves corresponding to $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ for some $t_1 \in \mathbb{Q}$ have the same j-invariant or there are only finitely many $t_1 \in \mathbb{Q}$ such that $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the j-invariant of the elliptic curve corresponding to $b(t_1)$ is equal to the j-invariant of E_{p}.

Proof. From the definition of the j-invariant, we see that we can view the j-invariant of E_{p} as a rational function of t evaluated at t_0. Either $j(t)$ is constant or not. If $j(t)$ is constant, then all elliptic curves corresponding to $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ for some $t_1 \in \mathbb{Q}$ must have the same j-invariant. If not, then for all $\lambda \in \mathbb{Q}$ there are only finitely many $t_1 \in \mathbb{Q}$ such that $j(t_1) = \lambda$. Hence in this case, there are only finitely many $t_1 \in \mathbb{Q}$ such that $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the elliptic curve corresponding to $b(t_1)$ has the same j-invariant as E_{p}. □

Corollary 5.9. Let $b(t) \in \mathcal{B}_{kd}(\mathbb{Q}(t))$, let $t_0 \in \mathbb{Q}$ such that $b(t_0) \in \mathcal{B}_{kd}(\mathbb{Q})$ and let E_{p} be the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$. If there is a $t_1 \in \mathbb{Q}$ such that $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the elliptic curve corresponding to $b(t_1)$ has a different j-invariant than E_{p}, then there are infinitely many $t_2 \in \mathbb{Q}$ such that $b(t_2) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the elliptic curves corresponding to the $b(t_2)$ are pairwise not isomorphic.

Proof. Again view the j-invariant as a rational function of t. If there is an $t_1 \in \mathbb{Q}$ such that $b(t_1) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the elliptic curve corresponding to $b(t_1)$ has a different j-invariant as E_{p}, then $j(t)$ is not constant. So each $\overline{\mathbb{Q}}$-isomorphic class of elliptic curves can only occur finitely many times within the family of elliptic curve corresponding to $b(t_2) \in \mathcal{B}_{kd}(\mathbb{Q})$ for some

$t_2 \in \mathbb{Q}$. Note that if elliptic curves over some field K are isomorphic over any subfield L of $\overline{K}$ containing K, then they are also isomorphic over $\overline{K}$. So we also know that each $\mathbb{Q}$-isomorphism class of elliptic curves can only occur finitely many times within the family of elliptic curve corresponding to $b(t_2) \in \mathcal{B}_{kd}(\mathbb{Q})$ for some $t_2 \in \mathbb{Q}$. Hence there must be infinitely many $t_2 \in \mathbb{Q}$ such that $b(t_2) \in \mathcal{B}_{kd}(\mathbb{Q})$ and such that the elliptic curves corresponding to the $b(t_2)$ are pairwise not isomorphic. □

So by finding a second elliptic curve in a family with a different j-invariant, we can prove that we have infinitely many truly different elliptic curves. Since we will be using Theorem 5.4, the families that we find will contain finitely many elliptic curves where we do not have an lower bound on the rank. Therefore note that we are not interested in the rank of the second elliptic curve that has a different j-invariant, because we only want to prove that the j-invariant is non-constant as a rational function.

5.1 Construction 1

Let $b = (1, 2, 3, 4, 5, 6, 7, 9)$, then one can check that $b \in \mathcal{B}_{43}(\mathbb{Q})$ and the elliptic curve E_{p} corresponding to b is given by

$$y^2 = \tfrac{7875}{128}x^3 - \tfrac{285193}{512}x^2 + \tfrac{1304393}{1024}x - \tfrac{1868711}{16384}.$$

Using Propositions 3.7 and 4.10 we can check that

$$\begin{aligned} P_1 &= (1, 3299/128, 1) & P_2 &= (2, -3381/128, 1) & P_3 &= (3, -2413/128, 1) \\ P_4 &= (4, -325/128, 1) & P_5 &= (5, -573/128, 1) & P_6 &= (6, -3541/128, 1) \\ P_7 &= (7, -6541/128, 1) \end{aligned}$$

are linearly independent. Hence $E_{\mathrm{p}}(\mathbb{Q})$ has rank at least 7.

Now take $b(t) = (1, 2, 3, 4, 5, 6, 7, t)$. Since $\deg(h_{b(t)}) < k = 4$, we see that $b(t) \in \mathcal{A}_{43}(\mathbb{Q}(t))$. So $b(t) \in \mathcal{B}_{43}(\mathbb{Q}(t))$ by Proposition 5.5 and the points $P_1(t), \ldots, P_7(t)$ are linearly independent by Proposition 5.6. Hence the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$ exists and has rank at least 7 for all but finitely many $t_0 \in \mathbb{Q}$. The elliptic curves corresponding to $b(9)$ and $b(10)$ have different j-invariants. Hence we have infinitely many non-isomorphic elliptic curves over $\mathbb{Q}$ with rank at least 7 by Corollary 5.9.

5.2 Construction 2

Let $b = (1, 2, 3, 4, 5, 6, 7, 8, 9, 12)$, then one can check that $b \in \mathcal{B}_{54}(\mathbb{Q})$. The affine chart E_{a} of the elliptic curve E_{p} corresponding to b is given by

$$y^2 = \tfrac{1231757}{512}x^4 - \tfrac{11034561}{256}x^3 + \tfrac{4453331697}{16384}x^2 - \tfrac{11370142773}{16384}x + \tfrac{39865067649}{65536}$$

Now one can check that

$$\begin{aligned} P_1 &= (1, -97625/256) & P_2 &= (2, 9005/256) & P_3 &= (3, -15597/256) \\ P_4 &= (4, -50279/256) & P_5 &= (5, -56833/256) & P_6 &= (6, -49275/256) \\ P_7 &= (7, -63125/256) & P_8 &= (8, -124687/256) & P_9 &= (9, -220329/256) \end{aligned}$$

are linearly independent by mapping these points to the elliptic curve given by $y^2 = h(x)$ for some monic h of degree 3 using Propositions 3.8, 3.10, 3.11, 3.7 and 3.6 and then using Proposition 4.10. Hence $E_{\mathrm{p}}(\mathbb{Q})$ has rank at least 9.

Now take $b(t) = (1, 2, 3, 4, 5, 6, 7, 8, 9, t)$. Since $\deg(h_{b(t)}) < k = 5$, we see that $b(t) \in \mathcal{A}_{54}(\mathbb{Q}(t))$. So $b(t) \in \mathcal{B}_{54}(\mathbb{Q}(t))$ by Proposition 5.5 and the points $P_1(t), \ldots, P_9(t)$ are linearly independent by Proposition 5.6. Hence the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$ exists and has rank at least 9 for all but finitely many $t_0 \in \mathbb{Q}$. The elliptic curves corresponding to $b(12)$ and $b(13)$ have different j-invariants. Hence we have infinitely many non-isomorphic elliptic curves over $\mathbb{Q}$ with rank at least 9 by Corollary 5.9.

5.3 Construction 3

Let $\beta = (b_1^2, \ldots, b_6^2)$ with $b_1, \ldots, b_6 \in K$, then there are $g_\beta, h_\beta \in K[x]$ such that $\prod_{i=1}^6 (x - b_i^2) = g_\beta(x)^2 - h_\beta(x)$ and $\deg(h_\beta) < 3$. Now consider $b = (b_1, \ldots, b_6, -b_1, \ldots, -b_6)$. We also have $g_b, h_b \in K[x]$ such that $\prod_{i=1}^6 (x - b_i)(x + b_i) = g_b(x)^2 - h_b(x)$ and $\deg(h_b) < 6$, but since

$$g_b(x)^2 - h_b(x) = \prod_{i=1}^{6} (x^2 - b_i^2) = g_\beta(x^2)^2 - h_\beta(x^2).$$

we see that $g_b(x) = \pm g_\beta(x^2)$ and $h_b(x) = h_\beta(x^2)$, because (g_b, h_b) is unique up to multiplication of g_b by -1. We will always choose the leading terms g_b and g_β to be 1. So we have $g_b(x) = g_\beta(x^2)$. We see that $\deg(h_b) = 2\deg(h_\beta) \leq 4$.

If we apply this to $K = \mathbb{Q}$ and $K = \mathbb{Q}(t)$, then we see that any b of the form

$$(b_1, \ldots, b_6, -b_1, \ldots, -b_6)$$

will be contained in $\mathcal{A}_{64}(\mathbb{Q})$ and any $b(t)$ of the form

$$(b_1(t), \ldots, b_6(t), -b_1(t), \ldots, -b_6(t))$$

will be contained in $\mathcal{A}_{64}(\mathbb{Q}(t))$. So we can use Proposition 5.5. Take

$$b = (1, 2, 3, 4, 5, 8, -1, -2, -3, -4, -5, -8).$$

Then one can check that $b \in \mathcal{B}_{64}(\mathbb{Q})$. The affine chart E_{a} of the elliptic curve E_{p} corresponding to b is given by

$$y^2 = \tfrac{34655789}{64} x^4 - \tfrac{344443001}{64} x^2 + \tfrac{11347641529}{256}$$

and the points

$$\begin{array}{lll} P_1 = (1, -100541/16) & P_2 = (2, -89747/16) & P_3 = (3, -100877/16) \\ P_4 = (4, -157451/16) & P_5 = (5, -252077/16) & P_6 = (8, 700693/16) \end{array}$$

are linearly independent. So the rank of the elliptic curve over $\mathbb{Q}$ corresponding to b is at least 6. Take

$$b(t) = (1, 2, 3, 4, 5, t, -1, -2, -3, -4, -5, -t).$$

We know that $b(t) \in \mathcal{A}_{64}(\mathbb{Q}(t))$. So $b(t) \in \mathcal{B}_{64}(\mathbb{Q}(t))$ by Proposition 5.5 and the points $P_1(t), \ldots, P_6(t)$ are linearly independent by Proposition 5.6. Hence the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$ exists and has rank at least 6 for all but finitely many $t_0 \in \mathbb{Q}$. The elliptic curves corresponding to $b(7)$ and $b(8)$ have different j-invariants. Hence we have infinitely many non-isomorphic elliptic curves over $\mathbb{Q}$ with rank at least 6 by Corollary 5.9. Unfortunately the following proposition shows that this is the best result we can get using this construction. We will however always have a point of order 2 in $E_{\mathrm{p}}(\mathbb{Q})$.

Proposition 5.10. Let (E_p, O) be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = h(x^2)$ as in Theorem 3.12 for some $h \in \mathbb{Q}[x]$ with $\deg(h) = 2$. Let $P = (x_1, y_1)$, $P' = (-x_1, y_1)$, $Q = (x_2, y_2)$ and $Q' = (-x_2, y_2)$ be $\mathbb{Q}$-rational points on E_p, then $P + P' = Q + Q'$.

Proof. Write $h(x) = h_2x^2 + h_1x + h_0$. Let $E_\mathrm{a}/\mathbb{Q}$ be the smooth affine curve in $\mathbb{A}^2_{x,y}$ given by $y^2 = h(x^2)$ and let $C_\mathrm{a}/\mathbb{Q}$ be the affine curve in $\mathbb{A}^2_{x,y}$ given by $y^2 = h(x)$. Note that C_a is smooth, because otherwise $h(x)$ would have a double zero in $\overline{\mathbb{Q}}$. But then $h(x^2)$ would also have a double zero in $\overline{\mathbb{Q}}$, which is impossible since E_a is smooth. We have a morphism $\pi : E_\mathrm{a} \to C_\mathrm{a}$ sending $(x, y) \mapsto (x^2, y)$. Note that $\pi^{-1}(x_1^2, y_1) = \{P, P'\}$ and $\pi^{-1}(x_2^2, y_2) = \{Q, Q'\}$.

Now let $C_\mathrm{p}/\mathbb{Q}$ in $\mathbb{P}^2_{X,Y,Z}$ be the projective closure of C_a given by

$$Y^2 = Z^2h(X/Z) = h_2X^2 + h_1XZ + h_0Z^2.$$

The points at infinity of C_p are $(1 : \pm\sqrt{h_2} : 0)$. If we take the affine chart corresponding to $X = 1$, we get the affine curve in $\mathbb{A}^2_{s,t}$ given by $s^2 = t^2h(1/t)$. This affine curve is smooth, because h has no double roots. Therefore C_p is a smooth projective curve.

We can extend π to a morphism $E_\mathrm{p} \to C_\mathrm{p}$. Recall that E_p is given by the equations

$$UW = V^2$$

$$Y^2 = h_2U^2 + h_1UW + h_0W^2$$

since $h(x^2) = h_2x^4 + h_1x^2 + h_0$. Now consider the rational map

$$\begin{array}{rcl} \pi : \mathbb{P}^3_{U,V,W,Y} & \dashrightarrow & \mathbb{P}^2_{X,Y,Z} \\ (U : V : W : Y) & \mapsto & (U : Y : W) \end{array}$$

If $(U : V : W : Y) \in E_\mathrm{p}(\overline{\mathbb{Q}})$, then we see that $(U : Y : W) \in C_\mathrm{p}(\overline{\mathbb{Q}})$. So π is in fact a morphism. Furthermore if $(x, y) \in E_\mathrm{a}(\overline{\mathbb{Q}}) \subseteq E_\mathrm{p}(\overline{Q})$, then we see that

$$\pi((x, y)) = \pi((x^2 : x : 1 : y)) = (x^2 : y : 1).$$

So we see that we have indeed extended π.

Note that for any point $(X : Y : Z) \in C_\mathrm{p}(\overline{\mathbb{Q}})$ we have $\pi^{-1}((X : Y : Z)) = \{(X : \pm\sqrt{XZ} : Z : Y)\}$ and $XZ = 0$ for only finitely many points on C_p. So the morphism π is a degree 2 map by Proposition II.2.6(b) of [1]. So by Proposition II.2.6(a), we know that $e_\pi((U : V : W : Y)) = 1$ if $V \neq 0$ and $e_\pi((U : V : W : Y)) = 2$ if $V = 0$. Now consider the maps

$$\begin{array}{rcl} \pi^* : \mathbb{Q}(C_\mathrm{p}) & \to & \mathbb{Q}(E_\mathrm{p}) \\ f(x, y) & \mapsto & f(x^2, y) \end{array}$$

$$\begin{array}{rcl} \pi^* : \mathrm{Div}(C_\mathrm{p}) & \to & \mathrm{Div}(E_\mathrm{p}) \\ (Q) & \mapsto & \displaystyle\sum_{P \in \pi^{-1}(Q)} e_\pi(P) \cdot (P) \end{array}$$

which are induced by π. By Proposition II.3.6(b), we know that $\pi^*(\mathrm{div}(f)) = \mathrm{div}(\pi^*(f))$. This means that if $(\pi(P)) - (\pi(Q))$ is principal, then $(P) + (P') - (Q) - (Q')$ is principal.

One can consider the rational map $C_\mathrm{p} \dashrightarrow \mathbb{P}^1$ sending $(X:Y:Z) \mapsto (X:Z)$ for $X \neq 0$ or $Z \neq 0$ and use Theorem II.5.9 of [1] to prove that C_p has genus 0. Now consider the divisor $D = (\pi(Q)) - (\pi(P))$. By Corollary II.5.5(c) of [1], we know that $\ell(D) = 1$. Therefore there must be an $f \in \overline{\mathbb{Q}}(C_\mathrm{p})^*$ such that $\mathrm{div}(f) \geq -D$. This f must have a zero of order 1 at $\pi(P)$ and has at most a pole of order 1 at $\pi(Q)$. So $\mathrm{div}(f) = -D$, because $\deg(\mathrm{div}(f)) = 0$. Hence $-D = (\pi(P)) - (\pi(Q))$ is principal. Therefore $(P) + (P') - (Q) - (Q')$ is also principal. So by Theorem 3.4, we have $P + P' = Q + Q'$. □

Corollary 5.11. Let $b = (b_1, \ldots, b_6, -b_1, \ldots, -b_6) \in \mathcal{B}_{64}(\mathbb{Q})$. Let

$$\begin{aligned} P_i &= (b_i, g_b(b_i)) \\ P'_i &= (-b_i, g_b(b_i)) \\ Q_i &= (b_i, -g_b(b_i)) \\ Q'_i &= (-b_i, -g_b(b_i)) \end{aligned}$$

for $i = 1, \ldots, 6$ and let (E_p, Q_1) be the elliptic curve over $\mathbb{Q}$ corresponding to b. Then the subgroup G of $E_\mathrm{p}(\mathbb{Q})$ generated by $P_1, \ldots, P_6, P'_1, \ldots, P'_6, Q_1, \ldots, Q_6, Q'_1, \ldots, Q'_6$ is generated by $P_1, \ldots, P_6, P'_1$. Furthermore $2P'_1 = Q_1$ and the rank of G is at most 6.

Proof. We proved at the end of section 3.2 that

$$P_i + Q_i = P'_i + Q'_i = P_1$$

for all i. By Proposition 5.1, we know that

$$\sum_{i=1}^{6} (P_i + P'_i) = 6P_1$$

and by Proposition 5.10, we know that

$$P_i + P'_i = Q_i + Q'_i = P_1 + P'_1$$

for any i. The first equality tells us that the subgroup of $E_\mathrm{p}(\mathbb{Q})$ generated by $P_1, \ldots, P_6, P'_1, \ldots, P'_6$ contains $Q_1, \ldots, Q_6, Q'_1, \ldots, Q'_6$. Using the last equality we see that the subgroup of $E_\mathrm{p}(\mathbb{Q})$ generated by $P_1, \ldots, P_6, P'_1$ also contains $P'_2, \ldots, P'_6$. Hence G is generated by $P_1, \ldots, P_6, P'_1$.

Next note that $P_1 + P'_1 = Q_1 + Q'_1$ and $P'_1 + Q'_1 = P_1 + Q_1$. So $P_1 + 2P'_1 + Q'_1 = 2Q_1 + Q'_1 + P_1$ and hence $2P'_1 = 2Q_1 = Q_1$, because Q_1 is the zero element. Since G is generated by 7 elements, one of which has finite order, we see that the rank of G is at most 6. □

This construction does not give a record, but it does give us a family of elliptic curves with a 2-torsion point and we have been able to choose $k = 6$. The next construction generalizes this idea by replacing x^2 in $y^2 = h_\beta(x^2)$ with a polynomial $p(x) \in \mathbb{Q}[x]$.

5.4 Construction 4

Let $\beta = (b_1, b_2, b_3, b_4)$ with $b_1, b_2, b_3, b_4 \in \mathbb{Q}$. Then there are $g_\beta, h_\beta \in \mathbb{Q}[x]$ such that $\prod_{i=1}^{4}(x - b_i) = g_\beta(x)^2 - h_\beta(x)$ and $\deg(h_\beta) < 2$. Let $p(x) \in \mathbb{Q}[x]$ be a monic polynomial of degree d and let $c_{ij} \in \mathbb{Q}$ for $i = 1, 2, 3, 4$ and $j = 1, \ldots, d$ be such that $p(c_{ij}) = b_i$ for every i and j. Then

$$\prod_{i=1}^{4} \prod_{j=1}^{d} (x - c_{ij}) = \prod_{i=1}^{4} (p(x) - b_i) = g_\beta(p(x))^2 - h_\beta(p(x)).$$

Now let $b = (c_{11}, c_{12}, \dots, c_{4d})$, then we see that $h_b = h_\beta(p(x))$ and therefore $\deg(h_b) \leq d$. So we might be able to use this method to find elliptic curves. However, to do this we need to be able to find $b_1, b_2, b_3, b_4 \in \mathbb{Q}$, $p(x) \in \mathbb{Q}[x]$ and $c_{ij} \in \mathbb{Q}$ that satisfy these conditions. For $d = 3$ we have been able to find all possible b_1, b_2, b_3, b_4, $p(x)$ and c_{ij}.

We are looking for $b_1, b_2, b_3, b_4 \in \mathbb{Q}$, $p(x) \in \mathbb{Q}[x]$ and $c_{ij} \in \mathbb{Q}$ such that

$$\begin{aligned} p(x) - b_1 &= (x - c_{11})(x - c_{12})(x - c_{13}) \\ p(x) - b_2 &= (x - c_{21})(x - c_{22})(x - c_{23}) \\ p(x) - b_3 &= (x - c_{31})(x - c_{32})(x - c_{33}) \\ p(x) - b_4 &= (x - c_{41})(x - c_{42})(x - c_{43}) \end{aligned}$$

Note that if we fix the c_{ij}, then b_1, b_2, b_3, b_4 and $p(x)$ will not unique if they exist, because we can add $\lambda \in \mathbb{Q}$ to $p(x)$ and b_1, b_2, b_3, b_4 to get a different solution. Also, b_1, b_2, b_3, b_4 and $p(x)$ will exist if and only if we choose the c_{ij} such that the four polynomials on the right hand side have the same coefficients at x^2 and x. Then we can simply choose $p(x)$ to be $(x-c_{11})(x-c_{12})(x-c_{13})$ and find $b_1, \dots, b_4$.

So we have the conditions that $c_{i1} + c_{i2} + c_{i3}$ and $c_{i1}c_{i2} + c_{i1}c_{i3} + c_{i2}c_{i3}$ are both independent of i. We have the following equality of symmetric polynomials in 3 variables:

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$$

This means that the previous conditions are equivalent to the conditions that $c_{i1} + c_{i2} + c_{i3}$ and $(c_{i1} + c_{i2} + c_{i3})^2$ are independent of i. These conditions can be viewed as equations that define a plane and a sphere in $\mathbb{A}^3$. So what we are actually looking for are four points $(c_{11}, c_{12}, c_{13}), \dots, (c_{41}, c_{42}, c_{43}) \in \mathbb{A}^3_{x,y,z}(\mathbb{Q})$, that lie on the intersection of a plane given by $x + y + z = \lambda_1$ and a sphere given by $x^2 + y^2 + z^2 = \lambda_2$ for some $\lambda_1, \lambda_2 \in \mathbb{Q}$, such that all coordinates are different.

Now let $c_{11}, c_{12}, c_{13} \in \mathbb{Q}$ be all different. Take $\lambda_1 = c_{11} + c_{12} + c_{13}$ and $\lambda_2 = c_{11}^2 + c_{12}^2 + c_{13}^2$. Note that the intersection of a plane and a sphere is either empty, a point or a circle. The first is obviously not the case here. The second would only be the case if the tangent-plane of (c_{11}, c_{12}, c_{13}) on the sphere is the plane. However the tangent plane of (c_{11}, c_{12}, c_{13}) on the sphere is given by $2c_{11}x+2c_{12}y+2c_{13}z = 2\lambda_2$ and the c_{1j} are all different. So $2c_{11}x+2c_{12}y+2c_{13}z = 2\lambda_2$ and $x + y + z = \lambda_1$ do not define the same plane. Hence the intersection of the plane and the sphere is a circle.

Now consider this circle inside the plane given by $x + y + z = \lambda_1$. It is well known that, if we know a rational point on a circle, we can find every rational point on that circle by looking at the lines in the plane through the know rational point. Hence we have found all possible solutions.

To recap: We first choose a point $(c_{11}, c_{12}, c_{13}) \in \mathbb{A}^3_{x,y,z}(\mathbb{Q})$ with all different coordinates. Then the intersection of the corresponding plane and sphere is a circle and we find (c_{i1}, c_{i2}, c_{i3}) for $i = 2, 3, 4$ by intersecting a line in the plane that goes through (c_{11}, c_{12}, c_{13}) with this circle. Next we choose $p(x) = (x - c_{11})(x - c_{12})(x - c_{13})$ and then there are $b_1, b_2, b_3, b_4 \in \mathbb{Q}$ with the required properties. Note that every solution can be found in this way.

Just like with the previous construction, we have a morphism

$$\begin{aligned} \pi : E_{\mathrm{a}} &\to C_{\mathrm{a}} \\ (x, y) &\mapsto (p(x), y) \end{aligned}$$

where $C_{\rm a}$ is the curve given by $y^2 = h_\beta(x)$ and again we could prove that the sum of all elements that map to the same point is always the same.

However in this case this is much simpler to prove: if (x_1, y_1) satisfies $y^2 = h_\beta(x)$, then $\pi^{-1}((x_1, y_1))$ consists of the points in $E_{\rm a}$ that also lie on the line $y = y_1$. Recall that $E_{\rm a}$ is given by $y^2 = h_b(x)$ with $\deg(h_b) = 3$ and therefore the sum of any three points connected by a line is zero when we count multiplicities. Hence $P_{3k+1} + P_{3k+2} + P_{3k+3} = \mathcal{O}$ for $k = 0, 1, 2, 3$, because P_{3k+1}, P_{3k+2} and P_{3k+3} have the same y-coordinate. So we see that the subgroup of $E_{\rm p}(\mathbb{Q})$ generated by $P_1, \ldots, P_{12}$ is also generated by $P_1, P_2, P_4, P_5, P_7, P_8, P_{10}, P_{11}$, which means that we will not improve our record using this construction.

5.5 Construction 5

Now suppose that $d = 4$. Then we are looking for $b_1, b_2, b_3, b_4 \in \mathbb{Q}$, $p(x) \in \mathbb{Q}[x]$ and $c_{ij} \in \mathbb{Q}$ for $i, j = 1, \ldots, 4$ such that

$$\begin{aligned} p(x) - b_1 &= (x - c_{11})(x - c_{12})(x - c_{13})(x - c_{14}) \\ p(x) - b_2 &= (x - c_{21})(x - c_{22})(x - c_{23})(x - c_{24}) \\ p(x) - b_3 &= (x - c_{31})(x - c_{32})(x - c_{33})(x - c_{34}) \\ p(x) - b_4 &= (x - c_{41})(x - c_{42})(x - c_{43})(x - c_{44}) \end{aligned}$$

Similar to the case where $d = 3$, we see that for given c_{ij} such $b_1, b_2, b_3, b_4 \in \mathbb{Q}$ and $p(x) \in \mathbb{Q}[x]$ exist if and only if

$$\begin{gathered} c_{i1} + c_{i2} + c_{i3} + c_{i4} \\ c_{i1}^2 + c_{i2}^2 + c_{i3}^2 + c_{i4}^2 \\ c_{i1}^3 + c_{i2}^3 + c_{i3}^3 + c_{i4}^3 \end{gathered}$$

do not depend on i or equivalently if for every i, $(c_{i1}, c_{i2}, c_{i3}, c_{i4})$ is a $\mathbb{Q}$-rational point on the affine variety in $\mathbb{A}^4$ given by

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= \lambda_1 \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 &= \lambda_2 \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 &= \lambda_3 \end{aligned}$$

for some $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$. Finding all points on a variety given by a degree 3 polynomial is generally quite hard. However, we have been able to find infinitely many points when $\lambda_1 = \lambda_3 = 0$.

Suppose that $c_{i1} + c_{i2} = c_{i3} + c_{i4} = 0$ for every i, then

$$c_{i1} + c_{i2} + c_{i3} + c_{i4} = c_{i1}^3 + c_{i2}^3 + c_{i3}^3 + c_{i4}^3 = 0$$

for every i and $c_{i1}^2 + c_{i2}^2 + c_{i3}^2 + c_{i4}^2 = 2\left(c_{i1}^2 + c_{i3}^2\right)$. So if we let (c_{i1}, c_{i3}) be points on a circle given by $x^2 + y^2 = r^2$, then

$$\begin{gathered} c_{i1} + c_{i2} + c_{i3} + c_{i4} \\ c_{i1}^2 + c_{i2}^2 + c_{i3}^2 + c_{i4}^2 \\ c_{i1}^3 + c_{i2}^3 + c_{i3}^3 + c_{i4}^3 \end{gathered}$$

do not depend on i. We have

$$(x - c_{11})(x - c_{12})(x - c_{13})(x - c_{14}) = (x^2 - c_{i1}^2)(x^2 - c_{13}^2) = x^4 - r^2x^2 + c_{11}^2 c_{13}^3$$

for every i. So we choose $p(x) = x^4 - r^2x^2$ and $b_i = -c_{i1}^2 c_{i3}^3$. Note that $p(x)$ is a polynomial in x^2. This unfortunately means that we can apply Proposition 5.10 to see that the rank of the subgroup G generated by $P_1, \ldots, P_{16}, Q_1, \ldots, Q_{16}$ of elliptic curve we get with this construction will be at most 8. However at the same time we can also say that we might be able the find a family of elliptic curve with a 2-torsion point of higher rank than before and this is indeed the case.

Take $r = 1$, then all rational points on the circle are of the form

$$\phi(t) = (\phi_1(t), \phi_2(t)) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$$

for some $t \in \mathbb{Q}$. We have $\phi(2) = (4/5, 3/5)$, $\phi(4) = (8/17, 15/17)$, $\phi(5) = (5/13, 12/13)$ and $\phi(6) = (12/37, 35/37)$. So we can take

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \\ c_{31} & c_{42} & c_{43} & c_{44} \end{pmatrix} = \begin{pmatrix} 4/5 & -4/5 & 3/5 & -3/5 \\ 8/17 & -8/17 & 15/17 & -15/17 \\ 5/13 & -5/13 & 12/13 & -12/13 \\ 12/37 & -12/37 & 35/37 & -35/37 \end{pmatrix}.$$

and $b = (c_{11}, c_{12}, c_{13}, c_{14}, c_{21}, c_{22}, c_{23}, c_{24}, c_{31}, c_{32}, c_{33}, c_{34}, c_{31}, c_{42}, c_{43}, c_{44})$. One can check that $b \in \mathcal{B}_{84}(\mathbb{Q})$. The elliptic curve E_{p} corresponding to b is given by

$$\begin{aligned} y^2 \quad = \quad & -\tfrac{116720828701679553996426885874076326170336000 6686208}{218156433534458127997812001450129844514892000783691 40625}x^4 \\ & +\tfrac{1167208287016795539964268858740763261703360006686208}{21815643353445812799781200145012984451489200078369140625}x^2 \\ & -\tfrac{224275198145333065377472136956185833445682417680839317405113993501696}{6095706293185439848493565125013831389866758303531219357211464859008789 0625} \end{aligned}$$

and we have the independent points:

$$\begin{aligned} P_1 &= \left(\tfrac{4}{5}, \tfrac{22959788490364212047915268436421856}{78075004279125338056867795867503906 25}\right) \\ P_3 &= \left(\tfrac{3}{5}, \tfrac{22959788490364212047915268436421856}{7807500427912533805686779586750390625}\right) \\ P_5 &= \left(\tfrac{8}{17}, -\tfrac{18385559754456311996728580997473952}{7807500427912533805686779586750390625}\right) \\ P_7 &= \left(\tfrac{15}{17}, -\tfrac{18385559754456311996728580997473952}{7807500427912533805686779586750390625}\right) \\ P_9 &= \left(\tfrac{5}{13}, -\tfrac{13667901667303973649566974071473952}{7807500427912533805686779586750390625}\right) \\ P_{11} &= \left(\tfrac{12}{13}, -\tfrac{13667901667303973649566974071473952}{7807500427912533805686779586750390625}\right) \\ P_{13} &= \left(\tfrac{12}{37}, \tfrac{9093672931396073598380286632526048}{7807500427912533805686779586750390625}\right) \\ P_{15} &= \left(\tfrac{35}{37}, \tfrac{9093672931396073598380286632526048}{7807500427912533805686779586750390625}\right). \end{aligned}$$

Now let $b(t)$ be

$$\begin{array}{llll} (\phi_1(t), & -\phi_1(t), & \phi_2(t), & -\phi_2(t), \\ \phi_1(t+2), & -\phi_1(t+2), & \phi_2(t+2), & -\phi_2(t+2), \\ \phi_1(t+3), & -\phi_1(t+3), & \phi_2(t+3), & -\phi_2(t+3), \\ \phi_1(t+4), & -\phi_1(t+4), & \phi_2(t+4), & -\phi_2(t+4)). \end{array}$$

One can check that $b(t) \in \mathcal{A}_{84}(\mathbb{Q}(t))$. So $b(t) \in \mathcal{B}_{84}(\mathbb{Q}(t))$ by Proposition 5.5 using $t_0 = 2$ and the points $P_1(t), P_3(t), \ldots, P_{15}(t)$ are linearly independent by Proposition 5.6. Hence the elliptic curve over $\mathbb{Q}$ corresponding to $b(t_0)$ exists, has a 2-torsion point and has rank at least 8 for all but finitely many $t_0 \in \mathbb{Q}$. The elliptic curves corresponding to $b(2)$ and $b(3)$ have different j-invariants. Hence we have infinitely many non-isomorphic elliptic curves over $\mathbb{Q}$ with a 2-torsion point and rank at least 8 by Corollary 5.9.

Chapter 6

Finding elliptic curves with relatively high rank within families

In section 5.2 we found an infinite family of elliptic curves over $\mathbb{Q}$ with rank at least 9 and in section 5.5 we found an infinite family of elliptic curves with a 2-torsion point and rank at least 8. The next step is to find elliptic curves within these families that have a higher rank. We do this using a conjecture that relates the rank of an elliptic curve over $\mathbb{Q}$ to the number of points on its reduction, which we will define now.

Definition 6.1. Let E_{p} be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Let $p > 0$ be a prime number and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field with p elements. Since $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, we can consider the Weierstrass equation modulo p. If it defines an elliptic curve $\hat{E}_{\text{p}}$ over $\mathbb{F}_p$, then $\hat{E}_{\text{p}}$ is called the reduction of E_{p} at p. In this case we say that E_{p} has a good reduction at p and we will define $E_{\text{p}}(\mathbb{F}_p)$ to be the set of $\mathbb{F}_p$-rational points on $\hat{E}_{\text{p}}$, i.e.

$$E_{\text{p}}(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : F(x, y) \equiv 0 \mod p\} \cup \{\hat{\mathcal{O}}\}$$

where $\hat{\mathcal{O}}$ is the point $(0 : 1 : 0)$ in the 2-dimensional projective space over $\mathbb{F}_p$ and where

$$F(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6).$$

Let E_{p} be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Then as a projective curve E_{p} is given by the equation

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

Recall that the $\mathbb{Q}$-rational points on E_{p} are of the form $(X : Y : Z)$ where X, Y, Z are defined up to scaling by a non-zero element of $\overline{\mathbb{Q}}$. Hence we may scale X, Y, Z such that $X, Y, Z \in \mathbb{Z}$. So every $\mathbb{Q}$-rational point on E_{p} gives a rational point on each reduction of E_{p} by scaling the point to integer coordinates with greatest common divider 1 and then reducing modulo the prime we are working with. So when E_{p} has many $\mathbb{Q}$-rational point, we expect its reduction to also have many rational points. Therefore we expect the rank of $E_{\text{p}}(\mathbb{Q})$ to be high when the size of $E_{\text{p}}(\mathbb{F}_p)$

is big for many primes p. While this idea is a conjecture at most, it has been shown to work when looking for elliptic curves with high rank by Mestre [5] and others.

With this idea as starting point, we can find candidates for elliptic curves with relatively high rank. The following theorem gives us an indication of when we should call $E_\mathrm{p}(\mathbb{F}_p)$ big.

Theorem 6.2 (Hasse)**.** Let $\hat{E}_\mathrm{p}$ be an elliptic curve defined over the finite field $\mathbb{F}_q$ with q elements. Then $|\#\hat{E}_\mathrm{p}(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

Proof. See Theorem V.1.1 of [1]. □

To prove that an elliptic curve indeed has a high rank, we need to find extra linearly independent points. For this, we use Michael Stoll's ratpoints program. See [4]. This program requires as input the coefficients of an equation of the form $y^2 = a_n x^n + \cdots + a_0$ with $a_0, \cdots a_n$ integers and it generally works faster if those coefficients are small in absolute value and if n is small. We will first apply these ideas to the family of elliptic curves that are given by $y^2 = x^3 + a$ for some $a \in \mathbb{Z}\backslash\{0\}$, because it is easy to find elliptic curves in this family with a given reduction.

6.1 Elliptic curves given by $y^2 = x^3 + a$

For all $a \in \mathbb{Z}\backslash\{0\}$, let E_p^a be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + a$. We want to find candidates for a that have a small absolute value such that the reduction of E_p^a has many points for many primes. By Theorem 6.2, the reduction of E_p^a at a prime p can have at most $p+1+2\sqrt{p}$ point. So since $p + 1 + 2\sqrt{p}$ is relatively big compared to p when p is small, we will focus on a such that E_p^a has many points in its reductions at small primes.

For $p = 2$ or $p = 3$, the curve over $\mathbb{F}_p$ given by $y^2 = x^3 + \hat{a}$ has a singular point for all $\hat{a} \in \mathbb{F}_p$. So E_p^a never has a good reduction at 2 or 3. However, for $p = 2$ note that if $y^2 = x^3 + a$, then also

$$\left(\frac{y-4}{8}\right)^2 + \frac{y-4}{8} = \left(\frac{x}{4}\right)^3 + \frac{a-16}{64}$$

So if $a \equiv 16 \mod 64$, then E_p^a is isomorphic to the elliptic curve given by the equation $y^2 + y = x^3 + a'$ with $a' = (a-16)/64$ and this elliptic curve has a good reduction at 2. This reduction will always have three $\mathbb{F}_2$-rational points: the point at infinity and the two points with x-coordinate $a' \mod 2$, which is at least not a small amount. So we will require a to be $16 \mod 64$.

For $p > 3$ prime, the curve over $\mathbb{F}_p$ given by $y^2 = x^3 + \hat{a}$ is an elliptic curve if and only if $\hat{a}$ is non-zero in $\mathbb{F}_p$. So E_p^a has a good reduction at p if and only if $a \not\equiv 0 \mod p$ and if $a \not\equiv 0 \mod p$, then the reductions of E_p^a and E_p^{a+p} at p are the same. We see that, when considering one prime, it only matters what a is modulo p.

Our algorithm for finding candidates for a has two parts. For the first part, let $n \in \mathbb{N}$ and let $p_1, \ldots, p_n$ be the first n primes greater than 3 such that for each prime p_i there is an $a \in \mathbb{Z}$ such that E_p^a has a good reduction at p with at least $p + 1$ rational points. Then for each p_i, we calculate what a should be modulo p_i in order for E_p^a to have a good reduction at p_i with as many rational points as possible. Then using the Chinese remainder theorem, we create a list of what a should be modulo $N = 64\prod_{i=1}^n p_i$ such that E_p^a has a good reduction with as many points as possible at every prime p_i and such that $a \equiv 16 \mod 64$. Since we want to keep the absolute value of a small, we will consider for each a in our list both a and $a - N$ to be candidates for the elliptic curve with high rank. We use $n = 9$ and get a list with millions of possible a's modulo $N = 2^6 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$.

In the second part, we will reduce the number of candidates by looking at primes higher than p_n. Suppose that we have more than 250 candidates remaining. Let p be the next prime for which there is an $a \in \mathbb{Z}$ such that E_{p}^a has a good reduction at p with more than $p + 1 + \sqrt{p}$ rational points. For every remaining candidate a, we will no longer consider a to be a candidate if E_{p}^a does not have a good reduction at p with more than $p + 1 + \sqrt{p}$ rational points. If we still have more than 250 candidates remaining after that, we repeat this process with the next prime. We relaxed the condition from having as many points as possible to having more than $p+1+\sqrt{p}$ points, because we consider reductions at individual primes less important as primes grow bigger.

Now we use the ratpoints program in SAGE to search for independent $\mathbb{Q}$-rational points on E_{p}^a for each remaining candidate a. For $a = 933491313296$, we find the following linearly independent points.

$$\begin{array}{rrr} (-9640, 194036) & (-9416, 314100) & (-9368, 333708) \\ (-35839/4, 3702785/8) & (-8320, 597964) & (-8216, 615540) \\ (-6560, 806964) & (-4583, 915003) & (1009, 966705) \end{array}$$

This means that the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + 933491313296$ has rank at least 9.

6.2 Elliptic curves corresponding to $b \in \mathcal{B}_{54}(\mathbb{Q})$

In section 5.2 we proved that there are infinitely many $b \in \mathcal{B}_{54}(\mathbb{Q})$ such that their corresponding elliptic curves have rank at least 9. Now we will search for $b \in \mathcal{B}_{54}(\mathbb{Q})$ that give an elliptic curve with higher rank. First note that we will need an equation of the form $y^2 = a_n x^n + \cdots + a_0$ with integer coefficients to use the ratpoints program. In our case, we can choose $n = 3$ or $n = 4$, because we have the equation $y^2 = h_b(x)$ with $\deg(h_b) = 4$ and we have an Weierstrass equation. In practice, using the Weierstrass equation seems to be the faster choice. Given a Weierstrass equation with coefficients in $\mathbb{Q}$, we can multiply the equation by the denominators of all coefficients and then use Proposition 3.7 to find an isomorphic elliptic curve given by a Weierstrass equation with integer coefficients. However, note that such an elliptic curve is not unique and it might not be the best isomorphic elliptic curve there is to use the ratpoints program on. We use the `minimal_model` command of SAGE to find for each elliptic curve an isomorphic elliptic curve given by a Weierstrass equation with integer coefficients, which is as suggested minimal in the sense that Δ as defined in Definition 5.7 is an integer of minimal absolute value. The `minimal_model` command returns an elliptic curve given by the equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with $a_1, a_2, a_3 \in \{-1, 0, 1\}$ and $a_4, a_6 \in \mathbb{Z}$. Using Propositions 3.6 and 3.7, we can then get an equation in the required form.

In practice, we only find new independent points on such elliptic curves when $|a_4| \leq 10^{22}$ and $|a_6| \leq 10^{27}$. So we try to make sure that the elliptic curves we will get satisfy these conditions by considering the $(b_1, \ldots, b_{10}) \in \mathcal{B}_{54}(\mathbb{Q})$ with $|b_1|, \ldots, |b_{10}| \leq 15$. Note that if (E_{p}, Q) is the elliptic curve corresponding to some $b \in \mathcal{B}_{54}(\mathbb{Q})$, then changing the order of b (in a way such that the result is still an element of $\mathcal{B}_{54}(\mathbb{Q})$) only changes Q and not E_{p}. And by Theorem 3.4, the isomorphism class of the group $E_{\mathrm{p}}(\mathbb{Q})$ does not depend of Q. Hence we may (in most cases) reorder b. So we will only look at the $(b_1, \ldots, b_{10}) \in \mathcal{B}_{54}(\mathbb{Q})$ that satisfy $0 \leq b_1 < b_2 < \cdots < b_{10} \leq 15$. This makes it much simpler to go through all possibilities.

So for all $b = (b_1, \ldots, b_{10})$ with $b_1, \ldots, b_{10} \in \mathbb{Z}$ such that $0 \leq b_1 < b_2 < \cdots < b_{10} \leq 15$ we check if $b \in \mathcal{B}_{54}(\mathbb{Q})$, if the `minimal_model` command returns an elliptic curve with $|a_4| \leq 10^{22}$ and $|a_6| \leq 10^{27}$ and if the points $P_1, \ldots, P_9$ as in section 5.2 are linearly independent. We also check if the reduction of our elliptic curve at p exists and has at least $p + 1 + \sqrt{p}$ points for at least 9 primes $p < 50$. The reason that we do not focus on small primes is that we cannot be sure that our elliptic curve has a good reduction at those primes. After all this, we get a list of elliptic curves that we all search using the ratpoints program.

For $b = (0, 1, 3, 6, 7, 10, 11, 12, 14, 15)$ we find elliptic curve that is isomorphic to the elliptic curve given by

$$y^2 + xy = x^3 - 55234491932639620x + 4558178199992994234882416$$

This second elliptic curve has the following linearly independent points.

$$\begin{array}{rr} (4308782, 2078522517224) & (86989586714, 25656569172315416) \\ (8015499410, 717312855401624) & (26294774, 1767465373736) \\ (46910978, 1438833150488) & (282663782, 3395427645224) \\ (195211634, 1102084840856) & (67567838, -1065199529752) \\ (-19716394, -2374761442264) & (-11258468, 2275660900624) \\ (-7453570, 2229231903464) & (-1364326, 2152565086286) \end{array}$$

$$\left(-\tfrac{884633627853364642}{865124569}, \tfrac{76917829732353145250863688}{25445908947997}\right)$$

This means that the elliptic curve over $\mathbb{Q}$ given by

$$y^2 + xy = x^3 - 55234491932639620x + 4558178199992994234882416$$

has rank at least 13.

6.3 Elliptic curves corresponding to $b \in \mathcal{B}_{84}(\mathbb{Q})$

We will also try to improve our record for the rank of elliptic curves over $\mathbb{Q}$ with a 2-torsion point. In section 5.5, we found an infinite family of such curves with rank at least 8. However, one can imagine from the elliptic curve we gave explicitly that the coefficients will not be small enough for ratpoints to find new points. One way to solve this problem is to let the b_i be small integers. This means that we have to find four points with different integer coordinates on the same circle. Equivalently, we have to write integers N, which represent the radius of the circle squared, as the sum of two squares in four different ways.

We will try to limit the size of the coefficients of the elliptic curve by restricting to $N \leq 20000$. We again use the `minimal_model` command to get an elliptic curve to use as input for the ratpoints program and check the same conditions as in the previous section (where we in this case check the linear independence of $P_1, P_3, \ldots, P_{15}$ as in section 5.5). Again we get a list of elliptic curves, which we all search using the ratpoints program.

For $b = (21, 118, 37, 114, 54, 107, 69, 98, -21, -118, -37, -114, -54, -107, -69, -98)$ we get an elliptic curve which is isomorphic to the elliptic curve given by

$$y^2 + xy + y = x^3 + 1493264593028517x + 219319624323468643478002$$

This second elliptic curve has the following linearly independent points.

$$\begin{array}{rr}
(13391150, -210553204599) & (311129025377/64, -173551219073551755/512) \\
(156029008, -2013398349559) & (1177929422, -40450296532599) \\
(734379911/4, -20372550261291/8) & (-67671023/64, -73041625702373/512) \\
(327208184/49, -61551570214161/343) & (-1128934, 142284528585) \\
(-10195999, 75149482110) & (-\frac{5528023603116623995}{539948675344}, -\frac{29611075829087199554022683061}{396760766026875328})
\end{array}$$

This means that the elliptic curve over $\mathbb{Q}$ given by

$$y^2 + xy + y = x^3 + 1493264593028517x + 2193196243234686434780 2$$

has rank at least 10.

Bibliography

[1] J.H. Silverman: The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics 106. Springer-Verlag, New York, 1992.

[2] R. Hartshorne: Algebraic Geometry. 1st edition. Corr. 8th printing. Graduate Texts in Mathematics 52. Springer-Verlag, New York, 1997.

[3] T. R. Seifullin: Computation of determinants, adjoint matrices, and characteristic polynomials without division. Cybernetics and Systems Analysis, Vol. 38, No. 5, 2002.

[4] `http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html`

[5] J.-F. Mestre: Construction d'une courbe elliptique de rang ≥ 12. C. R. Acad. Sci. Paris Sér. I Math., 295(12): 643-644, 1982

[6] An, S.-Y., Kim, S.-Y., Marshall, D., Marshall, S., McCallum, W., Perlis, A.: Jacobians of Genus One Curves. J. Number Theory 90, 304315 (2001)