Mordell's theorem and elliptic curves

Håkon Verås

April 12, 2026

Contents

1 Introduction

This thesis is mainly discussing the group of rational points on an elliptic curve. This includes a brief introduction on affine and projective geometry, with Bezouts theorem and the derivation of the elliptic curve. After proving some smaller results on the group of rational points on the elliptic curve, I state and prove Mordells theorem.

2 Algebraic curves

We first start by discussing the geometry of the elliptic curves. This is important for understanding what elliptic curves are, and how they are derived.

2.1 Projective geometry

The usual cartesian two dimensional plane can be viewed as

$$\mathbb{A}^2(\mathbb{R}) = \{(x, y)|x.y \in \mathbb{R}\}.$$

This is usually called the affine plane over the real numbers. When talking about cubic curves in general, we usually use the notation $\mathbb{A}^2(\mathbb{F}) = \{(a, b)|a, b \in \mathbb{F}\}$, where $\mathbb{F}$ is a field. Algebraic curves in over $\mathbb{A}^2(\mathbb{F})$ is simply defined to be the set of zeros of its polynomial equation $p(x, y)$ over $\mathbb{F}$. Sometimes we want to extend the affine plane to what is called the *projective plane*:

Definition 2.1. *The projective plane $\mathbb{P}^2$ is the set of equivalence classes of $\mathbb{F}^3/(0, 0, 0)$, where $\mathbb{F}$ is a field. Two points (x, y, z) and (x', y', z') are equivalent if there exists some constant λ such that $(x, y, z) = \lambda(x', y', z')$.*

This can also be interpreted as the set of lines in $\mathbb{A}^3$ that passes through $(0, 0, 0)$. It is common to denote the elements of $\mathbb{P}^2$ as $(x : y : z)$. This is interpreted as the ratios between the three coordinates. We see that the elements of $\mathbb{P}^2$ are not well-defined by the coordinates, but rather the ratios between the coordinates. The reason we are considering the projective plane can be illustrated by the following case: Say you want to find the intersection points between the following curves

$$y^2 = \alpha x^2 + 1, \quad y = x. \tag{1}$$

These curves do clearly not intersect in the affine plane over the real numbers, but they are still asymptotic to each other. Intuitively they will *interesect at infinity*. These intersection points can be found by extending the affine plane to the projective plane. A curve

$$f(x, y, z) = 0$$

defined over the projective plane is called a *projective plane curve* and is a homogeneous polynomial. In algebraic geometry the set of zeroes of a polynomial equation is usually

called an *algebraic variety*. Let $U_x = \{(x : y : z) \,|x \neq 0\}$. Then every element $P \in U_x$ can be described as $P = (1 : y : z)$. We define the sets U_y and U_z similarly, and we see that $\mathbb{P}^2 = U_x \cup U_y \cup U_z$. Now we define the *line at infinity* in $\mathbb{P}^2$:

$$L_\infty = \mathbb{P}^2 \setminus U_z = \{(x : y : z) \,|z = 0\}$$

We see that there exists a bijective map $(x : y : 0) \leftrightarrow (x : y)$ between L_∞ and $\mathbb{P}$. It follows that

$$\mathbb{P}^2 = L_\infty \cup U_z$$

We can define a injective map $\mathbb{A}^2(\mathbb{F}) \hookrightarrow U_z$ by mapping $(x, y) \to (x : y : 1)$. This map is obviously not bijective since there are no corresponding element to $(x, y, 0)$ in $\mathbb{A}^2(\mathbb{F})$. We therefore construct a corresponding *point at infinity* to $(x : y : 0)$. We denote this point at infinity as $\mathcal{O}$. We complete the section by considering (1) again. If we consider the equations over the projective plane, we can set denote x and y as $x = X/Z$, $y = Y/Z$ and multiply up the factors of Z. By this we are *homogenizing* the curves. From this we obtain the following set of curves in the projective plane:

$$Y^2 = \alpha X^2 + Z^2, \quad Y = X.$$

For $\alpha = 1$ we get the solution $(0 : 0 : 0)$, and for $\alpha = -1$ we get $(1 : 1 : 0)$. These are our points at infinity.

2.2 Intersection numbers and Bezouts theorem

Let C_1 and C_2 be affine curves of degree d_1 and d_2 respectively over a field k, such that $C_1 : f_1(x, y) = 0$, $C_2 : f_2(x, y) = 0$. Then we set $f_1 = 0 = f_2$ and consider the number of points (x, y) that satisfies these equations. We denote this set of points as $C_1 \cap C_2$. By considering f_1 as a polynomial in y with coefficients in x, we should intuitively get d_1 roots $y_1(x), ..., y_{d_1}(x)$ in the closure of k. Plugging these roots into f_2 should give d_1 polynomials $f_2(x, y_i(x))$. One may intuitively think that this results in $d_1 d_2$ solutions. However, terms may cancel and things may get more complicated. Consider the three following cases:

1. $f_1(x, y) = x + y + 1 = 0, \qquad f_2(x, y) = x^2 + y^2 - 1 = 0,$
2. $f_1(x, y) = x + 1 = 0, \qquad f_2(x, y) = x^2 - y = 0,$
3. $f_1(x, y) = x + y + 1 = 0, \qquad f_2(x, y) = 2x^2 + xy - y^2 + 4x + y + 2 = 0.$

In the first case we substitute $y = -x - 1$ and we get $\{0, -1\}$ as solutions for x in f_2, so we have two solutions. In our second example, substitution $x = -1$ gives only one solution in (x, y). Checking for any solutions in points at infinity, we can *homogenize* the curves by setting $x = X/Z$ and $y = Y/Z$ and multiplying up the factors of Z such that we transform the affine curves into projective plane curves instead:

$$X + Z = 0, \qquad X^2 - YZ = 0$$

This gives solutions $(-1:1:1)$ and $(0:1:0)$. In our last example we have that $2x^2+xy-y^2+4x+y+2=(x+y+1)(2x-y+2)$, so the solutions of f_1 is contained in f_2. Substituting $x=-y-1$ therefore only result in $0=0$. This implies that all points (x,y) that satisfies $f_1(x,y)=0$ will also satisfy $f_2(x,y)=0$.

We now want to define the *intersection number* I between two curves at the origin. Let $f,g\in\mathbb{A}^2(k)$ be two polynomials where f and g have no common factor h such that $h(0,0)=0$. If $\mathcal{F}(k)$ denotes the set of pairs of such polynomials over a field k, then it can be shown that there is a unique map $I:\mathcal{F}(k)\to\mathbb{N}$ such that the following holds

- $I(x,y)=1$,
- $I(f,g)=I(g,f),\quad \forall(f,g)\in\mathcal{F}(k)$,
- $I(f,gh)=I(f,g)+I(f,h),\quad \forall(f,g),(f,h)\in\mathcal{F}(k)$,
- $I(f,g+hf)=I(f,g),\quad \forall(f,g)\in\mathcal{F}(k),h\in\mathbb{A}^2(k)$,
- $I(f,g)=0,\quad g(0,0)\neq 0$.

The proof can be found on p. 9-10 in [2] and is using theory of resultans which I will not go into. We further denote $I(C_1\cap C_2,P)$ to be the *intersection multiplicity* between the curves C_1 and C_2 at a point $P=(a,b)$ that lies on both C_1 and C_2. We define it to be

$$I(C_1\cap C_2,P):=I(f(x-a,y-b),g(x-a,y-b)). \tag{2}$$

Summing all the intersection multiplicities over the points P that lies on both curves, we get the *intersection number*. Since the map I requires that f and g have no common factor, the following theorem will also assume that the projective curves have no common factors.

Theorem 2.2 (Bezouts theorem)**.** *Let C and D be two projective curves with no common factors over an algebraically closed field k. Then we have that*

$$\sum_{P\in C_1\cap C_2} I(C_1\cap C_2,P)=\deg(C_1)\cdot\deg(C_2).$$

The proof of the theorem will follow as the proof of the next five lemmas.

Lemma 2.3. *Consider the following affine curves with no common factors:*

$$C:f_1(x,y)=0,\qquad C:f_2(x,y)=0,$$

with degrees d_1 and d_2 respectively. Let $R=k[x,y]$ and consider the ideal in R generated by f_1 and f_2. Then we have that

$$\#(C_1\cap C_2\cap\mathbb{A}^2)\leq\dim\left(\frac{R}{(f_1,f_2)}\right)\leq d_1d_2, \tag{3}$$

where $\#(C_1\cap C_2\cap\mathbb{A}^2)$ is the number of points in $\mathbb{A}^2$ that coincides with C_1 and C_2.

Proof. Let $P_1, ..., P_m$ be all of the m points in $C_1 \cap C_2$. Then we can construct polynomials h_i such that

$$h_i(P_j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

These polynomials forms a linearly independent set modulo (f_1, f_2):

$$c_1 h_1 + ...c_m h_m \in (f_1, f_2)$$

Plugging in P_i gives that $c_i h_i(P)$ must equal zero, so we have that c_i is zero. Iterating over all P_i where $1 \leq i \leq m$, we get that all c_i equals zero. This proves linear indepence of $\{h_i\}_{i=1}^m$, so we have that

$$m \leq \dim \left(\frac{R}{(f_1, f_2)} \right).$$

The left inequality of (3) follows. To show the right inequality, we define

- $\phi(d) = \frac{(d+1)(d+2)}{2}$,
- $R_d =$ vector space of polynomials $f(x, y)$ of $\deg f \leq d$,
- $W_d = R_{d-d_1} f_1 + R_{d-d_2} f_2$,

for every integer $d \geq 0$. One quickly see that $\dim R_d = \phi(d)$: The intuition behind the following equation is by considering all choices of x, and then iterating over the possible degrees of y, given that $\deg f \leq d$:

$$\dim R_d = \sum_{i=0}^{d} 1 \cdot \left(\sum_{j=0}^{d-i} 1 \right) = d + (d-1) + ...1 = \frac{(d+1)(d+2)}{2} = \phi(d)$$

Since f_1 and f_2 has no common roots, we have that $R_{d-d_1} f_1 \cap R_{d-d_2} f_2$ must contain $f_1 f_2$ in each element of the set. Each element may contain polynomials in the vector space $R_{d-d_1-d_2}$, so we get that

$$R_{d-d_1} f_1 \cap R_{d-d_2} f_2 = R_{d-d_1-d_2} f_1 f_2.$$

We then calculate $\dim W_d$ for $d \geq d_1 + d_2$:

$$\dim W_d = \dim \left(R_{d-d_1} f_1 \cup R_{d-d_2} f_2 \right) = \dim R_{d-d_1} f_1 + \dim R_{d-d_2} f_2 - \dim R_{d-d_1-d_2} f_1 f_2$$

$$= \phi(d-d_1) + \phi(d-d_2) - \phi(d-d_1-d_2),$$

so we get that

$$\dim R_d - \dim W_d = \phi(d) - \phi(d-d_1) - \phi(d-d_2) + \phi(d-d_1-d_2) = d_1 d_2$$

Now consider the elements $g_i \in R$, $1 \leq i \leq d_1 d_2 + 1$. Taking these elements modulo (f_1, f_2), we can find representatives for these elements that has maximal degree less than or equal to $d = d_1 d_2$. This means that those representatives lies in R_d, but we have shown that $\dim R_d - \dim W_d = d_1 d_2$, which implies that the set $\{g_1, ..., g_{d_1 d_2 + 1}\}$ must be linearly dependent. $\square$

Lemma 2.4. *The inequality*

$$\dim\left(\frac{R}{(f_1,f_2)}\right) \leq d_1 d_2$$

can be improved to an equality if C_1 and C_2 does not meet at infinity.

Proof. Let $f(x,y)$ be an arbitrary non-zero polynomial and let f^* be the homogeneous part of highest degree n, such that

$$f(x,y) = \sum_{i,j} c_{i,j} x^i y^j, \qquad f^*(x,y) = \sum_{i+j=n} c_{i,j} x^i y^j$$

Then $f^*(x,y)$ can be factored into linear factors since we are working over the algebraic closure of k:

$$f^*(x,y) = \prod_{i=1}^{n} (a_i x + b_i y)$$

Recall that the the line at infinity is the set of points

$$L_\infty = \{(x:y:z) | z = 0\}.$$

We see that the points $(b_i : -a_i : 0) \in L_\infty$ are the points at infinity on f: Let $x = X/Z$, $y = Y/Z$. Then we have that

$$f(x,y) = \prod_{i=1}^{n} (a_i x + b_i y) + \sum_{i+j<n} c_{i,j} x^i y^j = 0$$

By homogenizing the equation, we get that

$$\prod_{i=1}^{n} (a_i X + b_i Y) + \sum_{i+j<n} Z^{n-i-j} c_{i,j} x^i y^j = 0,$$

so $(b_i : -a_i : 0)$ is clearly the solutions at infinity. Now consider C_1 and C_2 with the corresponding homogeneous parts:

$$f_1^*(x,y) = \prod_{i=1}^{n} (a_{i,1} x + b_{i,1} y), \qquad f_2^*(x,y) = \prod_{i=1}^{m} (a_{i,2} x + b_{i,2} y).$$

Assume C_1 and C_2 does not meet at infinity. Then f_1^* and f_2^* clearly can not have any common roots. We now show that $(f_1, f_2) \cap R_d = W_d$ for $d \geq d_1 + d_2$: Let $f = g_1 f_1 + g_2 f_2$ be an element of R_d where g_1 and g_2 is of lowest possible degree. Then if $\deg g_i > d - d_i$, then $\deg g_i f_i > d$, so it must be the case that $g_1^* f_1^* + g_2^* f_2^* = 0$. Since f_1^* and f_2^* are coprime, we have that $g_1^* = a f_2^*$ and $g_2^* = -a f_1^*$ for some number $a \in k$. Then it follows that

$$\deg(g_1 - a f_2) < \deg(g_1), \qquad \deg(g_2 + a f_1) < \deg(g_2)$$

This contradicts that g_1 and g_2 was of lowest degree. Therefore we have that $\deg g_i \leq d - d_i$ and it follows that $f \in W_d$.

We complete the proof by showing that if $(f_1, f_2) \cap R_d = W_d$ and $d \geq d_1 + d_2$, we have that

$$\dim\left(\frac{R}{(f_1, f_2)}\right) \geq d_1 d_2.$$

From the previous lemma, we know that there are $d_1 d_2$ elements in R_d modulo W_d. If $(f_1, f_2) \cap R_d = W_d$, then they are also linear independent in R modulo (f_1, f_2), so we get that $\dim R/(f_1, f_2) \geq d_1 d_2$. This proves the equality. □

Lemma 2.5. *The following inequality holds*

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P) \leq \dim\left(\frac{R}{(f_1, f_2)}\right)$$

Proof. Let K denote the field of rational functions of x and y. Define the *local ring* $\mathcal{O}_P$ of a point $P = (x, y)$ to be the set

$$\mathcal{O}_P = \left\{ \frac{f(x,y)}{g(x,y)} \,\middle|\, g(P) \neq 0 \right\}$$

We show that $\mathcal{O}_P$ is a subring of K. Let

$$\phi_1(P) = \frac{f_1(P)}{g_1(P)}, \qquad \phi_2(P) = \frac{f_2(P)}{g_1(P)},$$

be arbitrary elements of $\mathcal{O}_P$. $\mathcal{O}_P$ is clearly non-empty, so we have that

$$\phi_1(P) + (-\phi_2(P)) = \frac{f_1(P)}{g_1(P)} + (-\frac{f_2(P)}{g_1(P)}) = \frac{f_1(P)g_2(P) - f_2(P)g_1(P)}{g_1(P)g_2(P)} \in \mathcal{O}_P,$$

$$\phi_1(P)\phi_2(P) = \frac{f_1(P)f_2(P)}{g_1(P)g_2(P)} \in \mathcal{O}_P.$$

It follows from the subring test that $\mathcal{O}_P$ is a subring of K. Now define the map

$$\phi \to \phi(P)$$

We show that the map is a homomorphism. Let $\phi, \varphi \in \mathcal{O}_P$, $a \in k$. Then we have that

$$(\phi\varphi) \to (\phi\varphi)(P) = \phi(P)\varphi(P)$$

$$(\phi + \varphi) \to (\phi + \varphi)(P) = \phi(P) + \varphi(P)$$

$$(k\phi) \to (k\phi)(P) = k\phi(P),$$

which proves the statement. We further define the kernel of the map:

$$M_P = \{\phi \in \mathcal{O}_P | \phi(P) = 0\}.$$

The first isomorphism theorem says that $\mathcal{O}_P/M_P \cong k$, so we have that $\mathcal{O}_P = k + M_P$ is a direct sum.

Now let

$$(f_1, f_2)_P = \mathcal{O}_P f_1 + \mathcal{O}_P f_2 = \{h_1 f_1 + h_2 f_2 | h_1, h_2 \in \mathcal{O}_P\}$$

be the ideal in $\mathcal{O}_P$ generated by f_1 and f_2. It can be shown that our definition of *intersection multiplicity* in Definition 2 coincides with

$$I(C_1 \cap C_2, P) = \dim\left(\frac{\mathcal{O}_P}{(f_1, f_2)_P}\right).$$

From Inequality (3) $I(C_1 \cap C_2, P)$ is clearly finite. We now show the that

$$\dim\left(\frac{\mathcal{O}_P}{(f_1, f_2)}\right) \leq \dim\left(\frac{R}{(f_1, f_2)}\right).$$

Let $g_1/h_1, ..., g_n/h_n$ be linearly independent elements in $\mathcal{O}_P/\left(f_1, f_2\right)_P$. Then you can find the common denominator such that the the linearly independent set becomes $\hat{g}_1/h, ..., \hat{g}_n/h$. Then $g_1, ..., g_n$ forms a linearly independent set in $R/\left(f_1, f_2\right)$. Now assume $g_1/h, ..., g_n/h$ span $\mathcal{O}_P/\left(f_1, f_2\right)_P$. It is clear that $1/h \in \mathcal{O}_P$, so we have that $g_1, ..., g_n$ must span $\mathcal{O}_P/\left(f_1, f_2\right)_P$.

Let now $P \notin C_1 \cap C_2$. Assume without loss of generality that $f_1(P) \neq 0$. Then there exists $g \in \mathcal{O}_P$ such that

$$gf_1 = 1.$$

Hence, 1 is contained in $(f_1, f_2)_P$, so $(f_1, f_2)_P$ generates $\mathcal{O}_P$. It follows that

$$I\left(C_1 \cap C_2, P\right) = \dim\left(\frac{\mathcal{O}_P}{(f_1, f_2)_P}\right) = \dim\left(\frac{\mathcal{O}_P}{\mathcal{O}_P}\right) = 0$$

Let now $P \in C_1 \cap C_2$. Then we have that $f_1(P) = 0$ and $f_2(P) = 0$, so both f_1 and f_2 are contained in M_P. Hence,

$$(f_1, f_2)_P \subset M_P,$$

so (f_1, f_2) is contained in M_P. We then have that

$$I(C_1 \cap C_2, P) = \dim\left(\frac{\mathcal{O}_P}{(f_1, f_2)}\right) = \dim\left(\frac{k + M_P}{(f_1, f_2)}\right)$$

$$= \dim\left(\frac{k}{(f_1, f_2)}\right) + \dim\left(\frac{M_P}{(f_1, f_2)}\right) = 1 + \dim\left(\frac{M_P}{(f_1, f_2)}\right),$$

with equality if and only if $M_P = (f_1, f_2)_P$.

Now we show that for an exponent $r \geq \dim\left(\mathcal{O}_P/(f_1, f_2)_P\right)$, we have that $M_P^r \subset (f_1, f_2)_P$. Let $t_1, ..., t_r$ be a collection of r elements in M_P. Define J_i to be a sequence of ideals in $\mathcal{O}_P$:

$$J_i = t_1 t_2 ... t_i \mathcal{O}_P + (f_1, f_2)_P,$$

where $J_{r+1} = (f_1, f_2)_P$. Then we get that

$$M_P \supset J_1 \supset \cdots \supset J_{r+1} = (f_1, f_2)_P.$$

Since $r > \dim(M_P/(f_1, f_2)_P)$, we must have that $J_i = J_{i+1}$ for some i, $1 \leq i \leq r$. If $i = r$, then we have that $t_1 t_2 ... t_r \in (f_1, f_2)_P$. If $i < r$, we get that

$$t_1 ... t_i = t_1 ... t_i t_{i+1} \phi + \psi, \quad \phi \in \mathcal{O}_P, \psi \in (f_1, f_2)_P$$

From this we have that $t_1...t_i(1-t_{i+1}\phi) = \psi \in \mathcal{O}_P$. Since $(1-t_{i+1}\phi)(P) = 1$, we get that $(1-t_{i+1}\phi)^{-1} \in \mathcal{O}_P$. Then the following holds

$$t_1...t_i...t_r = \psi t_{i+1}...t_r(1-t_{i+1}\phi)^{-1} \in \mathcal{O}_P.$$

Let $P \in C_1 \cap C_2 \cap \mathbb{A}^2$, $\phi \in \mathcal{O}_P$. We show that there exists $g \in R$ such that

$$g \equiv \phi \,(\mathrm{mod}(f_1, f_2)_P), \tag{4}$$

$$g \equiv 0(\mathrm{mod}(f_1, f_2)_Q) \quad \forall\, Q \neq P,\, Q \in C_1 \cap C_2 \cap \mathbb{A}^2. \tag{5}$$

Lemma 2.3 shows that there are at most $d_1 d_2$ points in $C_1 \cap C_2 \cap \mathbb{A}^2$. From the same lemma, we also have that there exists a polynomial $h(x, y) \in R$ such that $h(P) = 1$ and $h(Q) = 0$ for all $Q \in C_1 \cap C_2 \cap \mathbb{A}^2$, $Q \neq P$. It follows that $h^{-1} \in \mathcal{O}_P$ and $h \in M_Q$. For $r \in \mathcal{O}_P$ we have that $h^{-r} \in \mathcal{O}_P$, and we have shown that $h^r \in (f_1, f_2)_Q$ for all other points Q if r is large enough. Then there exists a polynomial $f \in R$ such that $f \equiv \phi h^{-r}(\mathrm{mod}(f_1, f_2)_P)$. Setting $g = fh^r$ gives the desired result.

At last we show that

$$R \longrightarrow \prod_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \frac{\mathcal{O}_P}{(f_1, f_2)_P} \tag{6}$$

is a surjective map given by

$$f \longrightarrow (\ldots, f \bmod (f_1, f_2)_P, \ldots)_{P \in C_1 \cap C_2 \cap \mathbb{A}^2}.$$

Let J be the kernel. Then we have that $(f_1, f_2) \subset J$, so $\dim R/(f_1, f_2) \geq \dim(R/J)$. Surjectivity follows from having showed there exists $g \in R$ with the properties as in Equation (4) and (5). We get that

$$\dim \frac{R}{J} = \sum_P \dim \frac{\mathcal{O}_P}{(f_1, f_2)_P} = \sum_P I(C_1 \cap C_2, P),$$

which proves our inequality. □

Lemma 2.6. *The inequality of Lemma 2.5 can be extended to an equality:*

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P) = \dim\left(\frac{R}{(f_1, f_2)}\right)$$

Proof. Proving this is equivalent with showing that the kernel J is (f_1, f_2). Since we already have that $(f_1, f_2) \subset J$, it remains to show that J is contained in (f_1, f_2). Let $f \in J$. We consider the following set

$$L = \{g \in R | gf \in (f_1, f_2)\}$$

and prove that $1 \in L$. We start by showing that L is an ideal in R and that $(f_1, f_2) \subset L \subset R$. L is clearly non-empty. If $g_1, g_2 \in L$, we have that $g_1 f, g_2 f \in (f_1, f_2)$, so we have that

$$g_1 f + g_2 f = (g_1 + g_2)\, f \in (f_1, f_2)\,,$$

so L is an additive subgroup of R. Now let g be an element of L and h be arbitrary in R, then we get that

$$(hg)f = h(gf) \in (f_1, f_2),$$

so it is an ideal in R. The statement $(f_1, f_2) \subset L \subset R$ follows easily from the definitions of L and R. We now show that for every $P \in \mathbb{A}^2$, there exists $g \in L$ such that $g(P) \neq 0$. If $P \notin C_1 \cup C_2$, then it is trivial. If $P \in C_1 \cap C_2$, then the dimension of the map in the previous lemma is nonzero. Hence, there exists a polynomial $g \in R$ which does not map to zero in Equation (6).

We now prove that $1 \in L$. We know that $(f_1, f_2) \subset L$, so $\dim(R/L)$ is finite. Assume for contradiction that $1 \notin L$. All of the powers of x can not be linearly independent modulo L, so we have that

$$x^n + c_1 x^{n-1} + \cdots + c_n \in L.$$

Since k is algebraically closed, we have that $(x - a_1) \dots (x - a_n) \in L$. If $1 \in L + R(x - a)$, we must have that $1 \in L$, which is a contradiction, so there is an $a \in k$ such that $1 \notin L + R(x-a)$. Similarly, we can show that there is an $b \in k$ such that $1 \notin L + R(x-a) + R(y-b)$. Let $P = (a, b)$. We show that $g(P) = 0$ for all $g \in L$: We have that

$$g(x, y) = g(a + (x - a), b + (y - b)) = g(a, b) + g_1(x, y)(x - a) + g_2(x, y)(y - b),$$

so we have that $g(a, b) \in L$. This contradicts that there always exists $g \in L$ such that $g(P) \neq 0$ for $P \in \mathbb{A}^2$. Hence, our assumption that $1 \notin L$ is false. Since $1 \in L$, we have that $f \in (f_1, f_2)$ and it follows that $J = (f_1, f_2)$. □

Lemma 2.7. *The intersection multiplicity is invariant under projective transformations.*

Proof. We need to describe K, $\mathcal{O}_P$, M_P and $(f_1, f_2)_P$ in terms of homogeneous coordinates. Set

$$x = X/Z, \quad y = Y/Z,$$

and let $k[X/Z, Y/Z]$ be the subring of $k(X, Y, Z)$. Denote $K = k(x, y)$ to be the set of rational functions $\Phi = F/G$ in X, Y, Z, where F and G are homogeneous of same degree. If $\phi \in K$, then we have that

$$\phi = \frac{f(x, y)}{g(x, y)} = \frac{Z^n f(X/Z, Y/Z)}{Z^n g(X/Z, Y/Z)} = \frac{F(X, Y, Z)}{G(X, Y, Z)} = \Phi$$

We say Φ is *defined* at P if $G(P) \neq 0$. Further denote $\mathcal{O}_P$ and M_P as

$$\mathcal{O}_P = \left\{ \Phi = \frac{F}{G} \in K | G(P) \neq 0 \right\},$$

$$M_P = \{ \Phi \in K | \Phi(P) = 0 \}.$$

Let $P = (a, b) = (a : b : 1) \in \mathbb{A}^2$. Then we see that our new definitions of $\mathcal{O}_P$ and M_P coincide with our earlier definitions. Let $C_1 : F_1 = 0$, $C_2 : F_2 = 0$ be two curves in $\mathbb{P}^2$ with no common factor. Then we have that $f_1(x, y) = F_1(x, y, 1)$ and $f_2(x, y) = F_2(x, y, 1)$. Further define

$$(F_1, F_2)_P = \left\{ \frac{F}{G} \in \mathcal{O}_P \middle| F = H_1 F_1 + H_2 F_2 \right\}$$

We then have that $(F_1, F_2)_P = (f_1, f_2)_P$ is the ideal in $\mathcal{O}_P$ generated by f_1 and f_2 for $P \in \mathbb{A}^2$. One may notice that $(F_1, F_2)_P$ can not be the ideal generated by F_1 and F_2 itself, as $F_1(X, Y, 0)$ and $F_2(X, Y, 0)$ is not defined in $\mathcal{O}_P$. Further, define the intersection multiplicity of C_1 and C_2 at $P \in \mathbb{P}^2$ as

$$I(C_1 \cap C_2, P) = \dim \frac{\mathcal{O}_P}{(F_1, F_2)_P},$$

which coincides with our earlier definition of $P \in \mathbb{A}^2$. We now show that $\mathcal{O}_P$ and $(F_1, F_2)_P$ are independent in choice of coordinates in $\mathbb{P}^2$, which further implies $I(C_1 \cap C_2, P)$ is also independent. Let $(x, y, z) \to (a_1x + b_1, a_2y + b_2, a_3z + b_3)$. Then

$$(F_1, F_2) \to (F_1(a_1x + b_1, a_2y + b_2, 1), F_2(a_1x + b_1, a_2y + b_2, 1)$$

As the z-coordinate will be invariant under change of coordinates, we have that $(F_1, F_2)_P$ will remain an ideal in $\mathcal{O}_P$. As P will have the same change of coordinates as the fraction of polynomials in M_P and $\mathcal{O}_P$, we have that the sets must be invariant and equal. We now show that there is a line $L \in \mathbb{P}^2$ which does not meet $C_1 \cap C_2$. We can then set L to be the line at infinity, such that we reduce the case for which Bezout's theorem is already proved. First, let S be a finite set of points in $\mathbb{P}^2$. Since k is an algebraically closed field, it is not finite and we can find such L. We set this L to be the line at infinity. It then follows from Lemma 2.3 that $C_1 \cap C_2$ is finite, which completes the proof. □

2.3 Elliptic curves

We start by considering the general homogeneous cubic curve C in $\mathbb{P}^2(k)$:

$$C : a_0x^3 + a_1x^2y + a_2x^2z + a_3y^3 + a_4xy^2 + a_5y^2z + a_6z^3 + a_7yz^2 + a_8xz^2 + a_9xyz = 0 \quad (7)$$

over a field k. Denote the left hand side as $F(x, y, z)$.

Definition 2.8. *The line*

$$\frac{\partial F(P)}{\partial x}(x - a) + \frac{\partial F(P)}{\partial y}(y - b) + \frac{\partial F(P)}{\partial z}(z - c) = 0$$

is called the tangent line of F at point $P = (a, b, c)$.

We prove that if $F(0, 1, 0) = 0$ and the tangent line to $(0 : 1 : 0)$ is $L_\infty : z = 0$, then we can reduce Equation (7) to

$$y^2z + a_1xyz + a_2yz^2 = x^3 + a_3x^2z + a_4xz^2 + a_5z^3. \quad (8)$$

Proof. We first note that since $(0 : 1 : 0) \in C$, we have that a_3 equals zero. Recall that $U_y = (x : 1 : y)$ and that there exists a bijective mapping $(x : 1 : z) \leftrightarrow (x, z)$ between U_y and $\mathbb{A}^2$. By taking the union of U_y and C, we reduce Equation (7) to the following form

$$\hat{a}_0x^3 + \hat{a}_1x^2 + \hat{a}_2x^2z + \hat{a}_4x + \hat{a}_5z + \hat{a}_6z^3 + \hat{a}_7z^2 + \hat{a}_8xz^2 + \hat{a}_9x = 0, \quad (9)$$

then the tangent line at $(0:1:0)$ is equal to

$$\hat{a}_4 x + \hat{a}_5 z = 0. \tag{10}$$

Since we assumed that the tangent line was equal to $z = 0$, we have that $\hat{a}_4$ is zero and $\hat{a}_5$ being nonzero. It can further be shown using intersection theory that a_1 will equal zero and $\hat{a}_0$ is nonzero, so we get that

$$\hat{a}_0 x^3 + \hat{a}_2 x^2 z + \hat{a}_5 y^2 z + \hat{a}_6 z^3 + \hat{a}_7 y z^2 + \hat{a}_8 x z^2 + \hat{a}_9 xyz = 0, \quad \hat{a}_0, \hat{a}_5 \neq 0.$$

Dividing by $\hat{a}_0$ and mapping z to $-\frac{\hat{a}_0}{\hat{a}_5} z$ gives our result:

$$y^2 z + b_0 xyz + b_1 y z^2 = x^3 + b_2 x^2 z + b_3 x z^2 + b_4 z^3 \tag{11}$$

□

Cubic curves on this form are usually called *elliptic curves*. Since we will primarily be dealing with elliptic curves over $\mathbb{Q}$, we have that $char(k) \neq 2, 3$, so the following mappings are allowed

$$x = x', \qquad y = y' - \frac{b_0}{2} x', \qquad z = z'.$$

We end up cancelling the xyz-term on the left hand side of Equation (11):

$$(y' - \frac{b_0}{2} x')^2 z' + b_0 x'(y' - \frac{b_0}{2} X') z' + b_1 (y' - \frac{b_0}{2} x') z'^2$$

$$= y'^2 z' - b_0 x' y' z' + \frac{b_0^2}{4} x'^2 z' + b_0 x' y' z' - \frac{b_0^2}{2} x'^2 z' + b_1 y' z'^2 - \frac{b_0 b_1}{2} x' z'^2$$

$$= y'^2 z' - \frac{b_0^2}{4} x'^2 z' + b_1 y' z'^2 - \frac{b_0 b_1}{2} x' z'^2$$

By moving the $x'^2 z'$ and $x' z'^2$-terms over to the right side, we have reduced (11) to the following form:

$$y^2 z + b_0 y z^2 = x^3 + b_1 x^2 z + b_2 x z^2 + b_3 z^3$$

We can now cancel the yz^2-term on the left hand by letting $y = y' - \frac{b_0}{2}$:

$$y^2 z = x^3 + b_0 x^2 z + b_1 x z^2 + b_2 z^3 \tag{12}$$

At last, by substituting $x = x' - \frac{b_0}{3}$, we can reduce Equation (12) to

$$y^2 z = x^3 + b_0 x z^2 + b_1 z^3 \tag{13}$$

In the projective space we can dehomogenize, such that $(x : y : z)$ corresponds to $(x/z : y/z : 1)$, for $z \neq 0$. By substituting $(x, y) = (x/z, y/z)$, we get that the previous equation is equivalent to

$$y^2 = x^3 + b_0 x + b_1. \tag{14}$$

This equation is usually denoted as the Weierstrass normal form. When discussing elliptic curves I will usually consider elliptic curves on this form.

2.4 The discriminant

Let $f(x) = x^3 + ax^2 + bx + c$ be a function with the corresponding roots $\alpha_1, \alpha_2, \alpha_3$

$$f(x) = x^3 + ax^2 + bx + c = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3). \tag{15}$$

Then the *discriminant* D of $f(x)$ is defined to be

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2. \tag{16}$$

Using that $f(x) = x^3 + ax^2 + bx + c$, we get the following relations from Equation 15

- $\alpha_1\alpha_2\alpha_3 = -c$,
- $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = b$,
- $\alpha_1 + \alpha_2 + \alpha_3 = -a$.

It can further be shown that the discriminant can be expressed as

$$D = -4a^3 + a^2b^2 + 18abc - 4b^3 - 27c^2 \tag{17}$$

Observe that assuming D is nonzero is equivalent with f only having simple roots. For discriminants restricted to elliptic curves, we only have to cancel the terms containing a.

Definition 2.9. *A point on a cubic curve E is said to be singular at point P if*

$$\frac{\partial F(P)}{\partial x} = 0, \qquad \frac{\partial F(P)}{\partial y} = 0, \qquad \frac{\partial F(P)}{\partial z} = 0$$

A curve that contains no singular points is called a nonsingular curve.

Theorem 2.10. *Every elliptic curve on the form (13) is nonsingular, if $27b_1^2 + 4b_0^2 \neq 0$.*

Proof. We try to find a criterion for a singularity point. Setting the partial derivatives equal to zero, we have that

$$3x^2 + b_0z^2 = 0, \qquad 2yz = 0, \qquad y^2 - 2b_0xz - 3b_1z^2 = 0$$

Since we are in projective geometry, we have that $z \neq 0$. Since the ground field is an integral domain, we have that $y = 0$ from the second equation. We then square the third equation:

$$4b_0^2x^2 = 9b_1^2z^2$$

Using that the first equation equals

$$x^2 = -\frac{b_0z^2}{3}$$

Plugging this into the third equation and dividing by z^2, we get that

$$27b_1^2 + 4b_0^3 = 0,$$

so assuming this is not the case, we have that any elliptic curve on the form as in Equation (13) is nonsingular. This further implies that the curve only has simple roots. □

3 The group law

The group structure on an elliptic curve is often motivated by a geometrical approach: Given that we have two rational points P, Q on a cubic curve, we can consider the line intersecting these points. If $P = Q$, then we consider the tangent line. This line will intersect a third point $R = P \star Q$. Now consider the line connecting $\mathcal{O}$ and R. This will intersect a third point, which we denote by $P+Q$. This way of defining addition is usually referred to as *the composition law.*

Proposition 3.1. *The composition law is an additive group, where the point at infinity is the identity.*

Proof. For $P \in E$, we first show that $P + \mathcal{O} = P$. By how the composition law is defined, we have that $P \star \mathcal{O}$ is the reflection of P along the x-axis. Then $P + \mathcal{O}$ is the reflection of this reflection, which results in

$$P + \mathcal{O} = P$$

Now let P and Q be arbitrary points on a cubic curve E. Then $P + Q$ and $Q + P$ will intersect at the same point R and therefore give the same reflection along the x-axis, so the composition law is commutative. We must now show that for all points P on E, there exists another point R such that $P + R = 0$. Consider the vertical line through P. This line intersects E in the points P, $\mathcal{O}$ and R. Then we have that

$$P + (\mathcal{O} + R) = P + (-P) = \mathcal{O}$$

Proving associativity is the most tedious part. The geometric proof is as follows: Assume that we have a general cubic curve as in Equation (7)

$$F(X, Y, Z) = a_0X^3 + ... + a_9XYZ$$

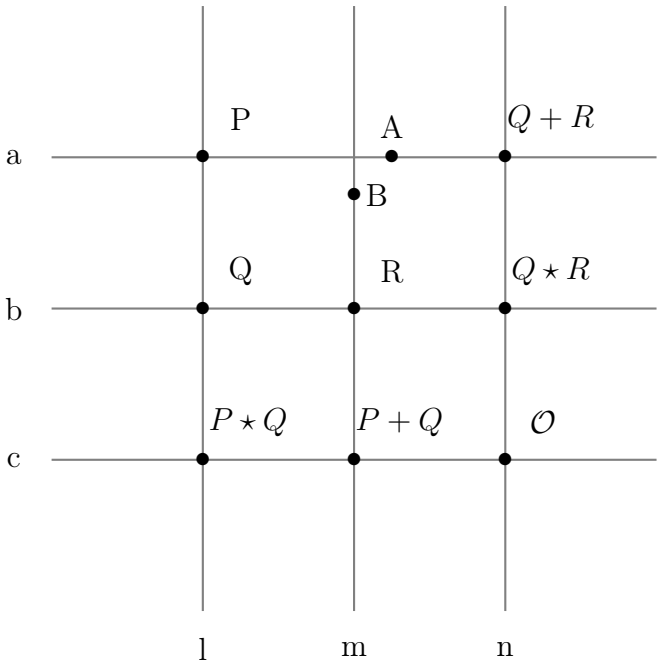
Lemma 3.2. *If two cubic curves in $\mathbb{P}^2$ intersects in nine points, then every cubic curve which passes through eight of those points will also pass through the ninth point.*

Proof. Assume that you have eight points $P_i = (x_i, y_i, z_i)$, $1 \leq i \leq 8$ that are in 'general position', that is, the the vectors $v_i = (x_i^3, x_i^2y_i, ..., x_iy_iz_i)$, $1 \leq i \leq 8$ induces a linearly independent set of vectors. Then the eight points imposes 8 conditions on F. Assume $F_1(X, Y, Z)$ and $F_2(X, Y, Z)$ are two cubic curves that passes through the 8 points, then any other cubic curve F can be expressed as

$$F(X, Y, Z) = \lambda F_1(X, Y, Z) + \mu F_2(X, Y, Z)$$

$F_1 = 0$ and $F_2 = 0$ have 9 points in common including the trivial point, so $F = 0$ obviously passes through all of them. □

Consider then the following diagram



Where a, b, c, l, m, n are lines and the rest are points on a cubic curve C. Observe that when P, Q and R are defined, the rest of the diagram is known. We know that

$$P + (Q + R) = A,$$

$$(P + Q) + R = B,$$

so it remains to show that A and B has to be the same point. Consider now the equations $l(X, Y, Z) = 0, ..., a(X, Y, Z) = 0$. Let

$$F_1(X, Y, Z) = l(X, Y, Z)m(X, Y, Z)n(X, Y, Z) = 0,$$

$$F_2(X, Y, Z) = a(X, Y, Z)b(X, Y, Z)c(X, Y, Z) = 0.$$

Then F_1 and F_2 passes through 8 of the points, and by Lemma 3.2 it must pass through the ninth point. Hence, $A = B$, so we get that

$$P + (Q + R) = (P + Q) + R$$

This completes the proof for associativity. □

4 The duplication formula

Now that we have defined the group operation, we can let a line that intersects the curve generally be defined as

$$L : y = \lambda x + \mu \tag{18}$$

Setting this equal to an elliptic curve C, we can express the coordinates of the third intersection point in terms of the other intersection points betweeen this curve and L:

$$C : y^2 = (\lambda x + \mu)^2 = x^3 + ax^2 + bx + c \tag{19}$$

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\mu)x + (c - \mu^2) = 0$$

If x_1,x_2,x_3 are the three intersection points, we have that

$$x_1 + x_2 + x_3 = \lambda^2 - a,$$

$$x_3 = \lambda^2 - a - x_1 - x_2, \tag{20}$$

and from Equation (18) we get that

$$y_3 = \lambda x_3 + \mu. \tag{21}$$

We want to consider adding two identical points in the group. This will become useful when we later define the *height*. Let

$$y = \lambda x + \mu$$

be the line connecting the two points. Then the slope of the line connecting those points will be the tangent line:

$$\lambda = \frac{dy}{dx} = \frac{3x^2 + 2ax + b}{2y}$$

Define $x(P)$ and $y(P)$ to be the x- and y-coordinate for a point P respectively. From Equation (20) we have that

$$x(2P) = \lambda^2 - 2x - a = \frac{(3x^2 + 2ax + b)^2 - 4y^2(2x + a)}{4y^2}$$

$$= \frac{(3x^2 + 2ax + b)^2 - 8x^4 - 12ax^3 - (4a^2 + 8b)bx^2 - (8c + 4ab)x - 4ac}{4x^3 + 2ax^2 + 4b + 4c}$$

$$= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2} \tag{22}$$

This will be important when using height-functions to prove the Descent- and Mordell's theorem. Next we express $y(2P)$ in terms of x and y:

$$y_3 = y(2P) = -\lambda x_3 - \mu,$$

$$y(2P) = -\lambda \cdot x(2P) - \mu = -\left(\frac{3x^2 + 2ax + b}{2y}\right)\left(\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}\right) - (y - \lambda x)$$

$$= -\frac{(3x^2 + 2ax + b)(x^4 - 2bx^2 - 8cx + b^2 - 4ac) + 8y^4 - 8\lambda xy^3}{8y^3}$$

$$= \frac{x^6 - 2ax^5 + 5bx^4 + 20cx^3 + (20ac - 5b^2)x^2 + (8a^2c - 4bc - 2ab^2)x + 4abc - b^3 - 8c^2}{8y^3} \tag{23}$$

This expression is clearly more complicated to work with than the expression for $x(2P)$. It is therefore natural to consider $x(2P)$ when working with height functions for elliptic curves.

5 The Descent theorem

The descent theorem mainly consists of five different lemmas. If a commutative group satisfies all of these lemmas, the Mordell theorem tells us that the group is finitely generated, which is the main result of this thesis.

We start by defining *height*. The use of height-functions is one of the cornerstones in proving the Descent theorem.

Definition 5.1 (Height)**.** *Let $x = m/n$ written in reduced form, that is,* $\gcd(m, n) = 1$. *Then the height H of x is defined as:*

$$H(x) = \max\{|m|, |n|\}$$

It will often be convenient to compare the height of $H(P + Q)$ with the product $H(P)H(Q)$. We therefore define the logarithm of the height function as h:

$$h(P) = \log H(P) \tag{24}$$

Lemma 5.2. *If (x, y) is a rational point satisfying*

$$y^2 = x^3 + ax^2 + bx + c, \tag{25}$$

then there exists integers m,n and e such that $(x, y) = (m/e^2, n/e^3)$ is the reduced form of (m, n).

Proof. Let $(x, y) = (m/M, n/N), \quad n, M, m, M \in \mathbb{Z}$ be written in reduced form. Substituting this into (25) and multiplying out the denominator gives that

$$n^2M^3 = m^3N^2 + am^2N^2M + bmN^2M^2 + cN^2M^3.$$

Since we can factor out N^2 from the right side and N and n are relatively prime, it follows that N^2 has to divide M^3. Further we see that

$$M(n^2M^2 - am^2N^2 - bmN^2M - cN^2M^2) = m^3N^2.$$

Since m and M are relatively prime, M has to divide N^2. Further we have that

$$M^2(n^2M - bmN^2 - cN^2M) = m^3N^2 + am^2N^2M.$$

We already know that M divides N^2, so we must have that M^2 divides N^2. At last we have from our original equation that M^3 has to divide N^2 since it divides all other terms on the right side. It follows that $N^2 = M^3$. Further let $e = \frac{N}{M}$, then we get that

$$N = N\frac{N^2}{M^3} = \left(\frac{N}{M}\right)^3 = e^3,$$

$$M = M\frac{N^2}{M^3} = \frac{N^2}{M^2} = \left(\frac{N}{M}\right)^2 = e^2,$$

which proves the lemma. □

Now, let $P = (x, y) = (m/e^2, n/e^3)\,, \quad m, e, n \in \mathbb{Z}$ be an arbitrary point on an elliptic curve. Then we have that

$$|m| \leq H(P) \qquad \text{and} \qquad |e^2| \leq |e|^2 \leq H(P).$$

Which leads to the upper bounds of $|e|$ and $|m|$ in terms of $H(P)$:

$$|m| \leq H(P) \qquad \text{and} \qquad |e| \leq H(P)^{\frac{1}{2}}. \tag{26}$$

We can also give an upper bound for $|n|$ in terms of $H(P)$: Substituting $(x, y) = m/e^2, n/e^3)$ into Equation (25) and clear the denominators. This results in the equation

$$n^2 = m^3 + ae^2m^2 + be^4 + ce^6.$$

Taking the the absolute value of both sides gives:

$$|n^2| = |m^3 + ae^2m^2 + be^4 + ce^6|$$

$$\leq |m|^3 + |a||e|^2|m|^2 + |b||e|^4 + |c||e|^6 \leq H(P)^3(1 + |a| + |b| + |c|).$$

Letting K equal $\sqrt{1 + |a| + |b| + |c|}$ results in

$$|n| \leq KH(P)^{\frac{3}{2}}. \tag{27}$$

Lemma 5.3. *For all $M \in \mathbb{R}$, we have that*

$$\{P \in C\,(\mathbb{Q}) \mid h(P) \leq M\}$$

is a finite set.

Proof. Let $X = \lfloor M \rfloor$. Then there are $2X + 1$ integers in the interval $[-X, X]$ for the numerator, including zero. Then the denominator can take on X different positive values. Thus, an upper bound for the number of rational points satisfying the height criterion is $2X^2 + X$, so it is obviously finite. □

Lemma 5.4. *Let $P_0 \in C(\mathbb{Q})$. Then $\exists \kappa_0 \in \mathbb{R}$ dependent on P_0,a,b,c such that*

$$H(P + P_0) \leq 2H(P) + \kappa_0, \qquad \forall P \in C(\mathbb{Q}).$$

Proof. We start by defining $P = (x, y)$, $P_0 = (x_0, y_0)$ and $P + P_0 = (x_3, y_3)$. The proof is trivial for $P_0 = \mathcal{O}$, so let $P \neq \mathcal{O}$. The existence of such a constant follows from assuming there exists one for all but a finite fixed set. Then you can let

$$\kappa_0 = \max_i\{H(P_i + P_0) - 2H(P_i)\},$$

where i iterates over the finite set, so we get a contradiction. Assume now that $P \neq \{P_0, -P_0, 0\}$ and $P = \{x, y\}$. Then we have from Equation (18) and Equation (20) that

$$\lambda = \frac{y - y_0}{x - x_0}, \qquad x_3 = \lambda^2 - a - x - x_0,$$

$$x_3 = \left(\frac{y-y_0}{x-x_0}\right)^2 - a - x - x_0 = \frac{(y-y_0)^2 - (x-x_0)^2(a+x+x_0)}{(x-x_0)^2}.$$

We further have that $y^2 - x^3 = ax^2 + bx + c$, so the expression for x_3 reduces to

$$x_3 = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},$$

for some constants A, B, C, D, E, F, G. By Lemma 5.2, we can transform the expression into

$$x_3 = \frac{Ane + Bm^2 + Ce^2m + De^4}{Em^2 + Fe^2m + Ge^4}.$$

We have now from Definition 5.1 that the height of x_3 is defined to be

$$H(x_3) = \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

Using Equation (26) and Equation (27), we have that

$$|Ane + Bm^2 + Cme^2 + De^4| \leq |A||n||e| + |B||m|^2 + |C||m||e|^2 + |D||e|^4$$

$$\leq H(P)^2(|A|K + |B| + |C| + |D|), \tag{28}$$

$$|Em^2 + Fme^2 + Ge^4| \leq H(P)^2(|E| + |F| + |G|). \tag{29}$$

We see that $H(P + P_0)$ has an upper bounded equal to $H(P)^2$ times a constant. We fix this constant to be equal e^{κ_0}. Taking now the logarithms of both sides gives

$$h(P + P_0) \leq 2h(P) + \kappa_0,$$

which proves the lemma. □

Lemma 5.5. *Let $\phi(X)$, $\psi(X)$ be relatively prime polynomials with coefficients in $\mathbb{Z}$. Let $d = \max\{\deg(\phi(X)), \deg(\psi(X))\}$, then we have that*
a) There is an integer $R \geq 1$ depending on ϕ, ψ, such that for all $\frac{m}{n} \in \mathbb{Q}$, we have that

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) | R$$

b) There exists a constant κ_1 such that for all $\frac{m}{n} \in \mathbb{Q}$, where $\psi\left(\frac{m}{n}\right) \neq 0$, we have that

$$dh(m/n) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right).$$

Proof. We start by proving a). Both ϕ and ψ are polynomials of degree at most d, so $n^d\phi(m/n)$ and $n^d\psi(m/n)$ will both be integers. we have without loss of generality that $\deg(\phi) = d$ and $deg(\psi) = e \leq d$. Then we have that

$$n^d\phi(m/n) = a_0m^d + ... + a_dn^d,$$

$$n^d\psi(m/n) = b_0m^en^{d-e} + ... + b_en^d.$$

$\phi(X)$ and $\psi(X)$ are relatively prime in $\mathbb{Q}[X]$, so they generate the unit ideal. That is, we can find polynomials $F(X)$ and $G(X)$ such that

$$\phi(X)F(X) + \psi(X)G(X) = 1. \tag{30}$$

We can now scale $F(X)$ and $G(X)$ with an integer A such that both $AF(X)$ and $AG(X)$ have integer coefficients. Let $D = \max\{\deg(F(X)), \deg(G(X))\}$. Evaluating Equation (30) at m/n and multiplying by An^{D+d} gives that

$$\left(n^D AF(m/n)\right)\left(n^d\phi(m/n)\right) + \left(n^D AG(m/n)\right)\left(n^D\psi(m/n)\right) = An^{D+d}.$$

Now let $\gamma(m,n)$ be the greatest common divisor of $n^d\phi(m/n)$ and $n^d\psi(m/n)$. Since those two are both integers, we know that γ also divides An^{D+d}. But the integer R that is divisible by $\gcd\left(n^d\phi(m/n), n^d\psi(m/n)\right)$ is supposed to be independent of n. Observe next that since γ divides $n^d\phi(m/n)$, it also divides

$$An^{D+d-1} = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + ... + Aa_dn^{D+2d-1}.$$

Every term except the first one on the right hand side contains An^{D+d}. Since γ divides An^{D+d}, this implies that γ divides $Aa_0m^dn^{D+d-1}$. It follows that $\gcd\left(An^{D+d}, Aa_0m^dn^{D+d-1}\right) = a\gamma$ for some integer a. Since m and n are coprime, we get that γ divides Aa_0n^{D+d-1}. Repeating this argument once more gives that γ divides $Aa_0^2n^{D+d-2}$, so continuing repeating the argument results in γ dividing Aa_0^{D+d}, so a) is proved.

b) As in the previous lemma, we can discard a finite set of points, so let m/n be a rational number that is not a root of of $\phi(X)$, so the denominator is nonzero. We first prove the lower bound. From a) we know there is a fixed integer R that divides the greatest common divisor of $n^d\phi(m/n)$ and $n^d\psi(m/n)$. From this we have that

$$H(x(2P)) \geq \frac{1}{R}\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\} \geq \frac{1}{2R}\left(|n^d\phi(m/n)| + |n^d\psi(m/n)|\right). \quad (31)$$

Further we have that $H\left(\frac{m}{n}\right)^d = \max\{|m|^d, |n|^d\}$. Dividing (31) by this expression gives that

$$\frac{H(x(2P))}{H(m/n)^d} \geq \frac{1}{2R}\frac{\left(|n^d\phi(m/n)| + |n^d\psi(m/n)|\right)}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{(|\phi(m/n)| + |\psi(m/n)|)}{\max\{|m/n|^d, 1\}}.$$

Define the function

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}.$$

We have assumed that ϕ has degree d and ψ has degree $e \leq d$. If $e = d$, we have that if t goes to infinity, then

$$\lim_{t\to\infty} p(t) = |a_0| + |b_0|.$$

Further if $e < d$, $|b_0|$ vanishes and the limit is $|a_0|$. This shows that $p(t)$ is bounded. If we consider $p(t)$ on a closed interval, we have that $p(t)$ is always positive since ϕ and ψ has no common zeros, and thus are never both equal to zero at the same time. Since we are looking at $p(t)$ on a closed interval, there exists a minimum value C for $p(t)$. Since $p(t)$ is strictly positive, C must be larger than zero. From this we have that

$$\frac{H(x(2P))}{H(m/n)^d} \geq \frac{C}{2R},$$

$$H(x(2P)) \geq \frac{C}{2R}H(m/n)^d.$$

Now taking the logarithm of both sides gives that

$$h(x(2P)) \geq dh(m/n) - \kappa_1, \tag{32}$$

where $\kappa_1 = \log \frac{2R}{C}$.

□

Lemma 5.6. *There exists a constant κ dependent on a,b,c such that*

$$H(2P) \geq 4H(P) - \kappa.$$

Proof. As in Lemma 5.4, we can discard a finite set of points, because we can fix a constant κ by iterating over them. Therefore discard all P such that $2P = 0$. Let $y^2 = f(x)$. Now using the duplication formula, we have that

$$x(2P) = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Since $2P \neq 0$, we have that the denominator is nonzero, so $x(2P)$ is the quotient of two polynomials in x with integer coefficients. Since it is assumed that the elliptic curve is non-singular, we know that $f(x)$ and $f'(x)$ have no common roots, so the numerator and the denominator are coprime. We are left with proving that

$$h(x(2P)) \geq 4h(x) - \kappa,$$

but this follows now directly from part b) of Lemma 5.5. □

Lemma 5.7. *Let Γ be the group of rational points over an elliptic curve. Then 2Γ has finite index in Γ.*

Proof. Let

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

be an elliptic curve. Since this lemma in general needs some use of algebraic number theory, I will narrow it down to when $f(x)$ has at least one rational root. Denote one of these roots by x_0. By defining the map

$$y = y', \qquad x = x' - x_0,$$

we move the root to the origin so that the elliptic curve will get transformed to the following form

$$y^2 = x^3 + ax^2 + bx.$$

Further we have that

$$T = (0, 0)$$

is a rational point on E, so we get that $2T = 0$. It can be shown from Equation (17) that the new discriminant equals

$$D = b^2(a^2 - 4b).$$

Since we assume the elliptic curve to be non-singular, we have that $D \neq 0$, so $b \neq 0$ and $a^2 - 4b \neq 0$. We introduce a new curve

$$\overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Note that if we apply the same procedure on $\overline{C}$, we get

$$\overline{\overline{C}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x = x^3 - 2\overline{a}x^2 + (\overline{a}^2 - 4\overline{b})x$$
$$= x^3 + 4ax^2 + (4a^2 - 4a^2 + 16b)x = x^3 + 4ax^2 + 16bx.$$

By mapping y to $8y$, x to $4x$ and dividing by 64 we get C, so we have that $\Gamma \cong \overline{\overline{\Gamma}}$. We are interested in the order of the factor group $\Gamma/2\Gamma$. We will therefore define the map $P \to 2P$ by giving a map $\phi : C \to \overline{C}$ and $\psi : \overline{C} \to \overline{\overline{C}}$ which results in being the duplication map. Let $\phi : C \to \overline{C}$ be defined as

$$\phi(x, y) = (\overline{x}, \overline{y}) = \left(\frac{y^2}{x^2}, y\left(\frac{x^2 - b}{x^2}\right)\right)$$

Then we get that

$$\overline{x}^3 + \overline{ax}^2 + \overline{bx} = \frac{y^2}{x^2}(\overline{x}^2 + \overline{ax} + \overline{b}) = \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\right)$$
$$= \frac{y^2}{x^6}(y^4 - 2ax^2y^2 + x^4a^2 - 4bx^4) = \frac{y^2}{x^6}((y^2 - ax^2)^2 - 4bx^4)$$
$$= \frac{y^2}{x^6}((x^3 + bx)^2 - 4bx^4) = \frac{y^2}{x^6}(x^6 - 2bx^4 + b^2x^2) = \left(\frac{y(x^2 - b)}{x^2}\right)^2$$
$$= \overline{y}^2,$$

so the map ϕ is defined for all points on C except T and $\mathcal{O}$. The map is completed by setting $\phi(T) = \mathcal{O}$ and $\phi(\mathcal{O}) = \overline{\mathcal{O}}$. This is the kernel of ϕ.

Proposition 5.8. *Let C and $\overline{C}$ be the following elliptic curves:*

$$C : y^2 = x^3 + ax^2 + bx, \qquad \overline{C} : y = x^3 + \overline{a}x^2 + \overline{b}x,$$

where

$$\overline{a} = -2a, \qquad \overline{b} = a^2 - 4b, \qquad T = (0, 0) \in C, \tag{33}$$

a) then there is a homomorphism ϕ from C to $\overline{C}$ such that

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & P \neq T, \mathcal{O} \\ \overline{\mathcal{O}} & P = \mathcal{O},\ P = T, \end{cases}$$

where $\ker \phi = \{\mathcal{O}, T\}$.

b) As in a), there is a homomorphism $\psi : \overline{C} \to \overline{\overline{C}}$ together with the map $(x, y) \to \left(\frac{x}{4}, \frac{y}{8}\right)$ such that

$$\psi(\overline{P}) = \begin{cases} \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right) & \overline{P} \neq \overline{T}, \overline{\mathcal{O}} \\ \overline{\mathcal{O}} & \overline{P} = \overline{\mathcal{O}},\ \overline{P} = \overline{T}. \end{cases}$$

The composition $\psi \circ \phi$ yields the duplication formula:

$$(\psi \circ \phi)(P) = 2P.$$

Proof. a) It remains to prove that ϕ is a homomorphism, that is

$$\phi(P+Q) = \phi(P) + \phi(Q) \qquad \forall P, Q \in C.$$

If P or Q are equal to 0, then the proof is trivial so assume it is not the case. If both of P or Q be equal to T, then we must show that

$$\phi(T+T) = \phi(T) + \phi(T).$$

But all of the terms equals 0, so it is obviously true. Further, either P or Q are equal to T, say $P = T$. Then we must calculate $P + T$:

$$x(P+T) = \frac{y^2}{x^2} - x - 0 - a = \frac{y^2 - x^3 - ax^2}{x^2} = \frac{bx}{x^2} = \frac{b}{x},$$

$$y(P+T) = \frac{y}{x}\left(x - \frac{b}{x}\right) - y = -\frac{by}{x^2},$$

so we have that

$$P + T = \left(\frac{b}{x}, -\frac{by}{x^2}\right),$$

$$x(\phi(P+T)) = \frac{\left(-\frac{by}{x^2}\right)^2}{\left(\frac{b}{x}\right)^2} = \frac{y^2}{x^2} = x(\phi(P)),$$

$$y(\phi(P+T)) = \frac{\left(-\frac{by}{x^2}\right)\left(\left(\frac{b}{x}\right)^2 - b\right)}{\left(\frac{b}{x}\right)^2} = \frac{-by(b^2 - bx^2)}{b^2x^2} = \frac{y(x^2-b)}{x^2} = y(\phi(P)).$$

This shows that $\phi(P+T) = \phi(P)$. Since the group is commutative, the same holds when $P = T$.

Now observe that if we have that $P = (x, y)$, then

$$\phi(-P) = \phi(x, -y) = \left(\left(\frac{-y}{x}\right)^2, \left(\frac{-y(x^2-b)}{x^2}\right)\right) = -\phi(x, y) = -\phi(P).$$

Now let P,Q and R be colinear points on C. Then $P + Q + R = 0$, so we have that $P + Q = -R$. It remains to show that $\phi(P)$, $\phi(Q)$ and $\phi(R)$ are the intersection points between $\overline{C}$ and some line. Then we would have that

$$\phi(P+Q) = \phi(-R) = \phi(P) + \phi(Q).$$

The line that intersects $\overline{C}$ is

$$y = \overline{\lambda}x + \overline{\mu},$$

where

$$\overline{\lambda} = \frac{\mu\lambda - b}{\mu}, \quad \overline{\mu} = \frac{\mu^2 - a\mu\lambda + b\lambda^2}{\mu}.$$

We show that $\phi(P) = \phi(x_1, y_1) = (\overline{x_1}, \overline{y_1})$ lies on $y = \overline{\lambda}x + \overline{\mu}$:

$$\overline{\lambda}\overline{x_1} + \overline{\mu} = \frac{\mu\lambda - b}{\mu}\left(\frac{y_1}{x_1}\right)^2 + \frac{\mu^2 - a\mu\lambda + b\lambda^2}{\mu} = \frac{(\mu\lambda - b)y_1^2 + (\mu^2 - a\mu\lambda + b\lambda^2)x_1^2}{\mu x_1^2}$$

$$= \frac{\mu\lambda(y_1^2 - ax_1^2) - b(y_1 - \lambda x_1)(y_1 + \lambda x_1) + \mu^2 x_1^2}{\mu x_1^2}$$
$$= \frac{\lambda(y_1^2 - ax_1^2) - b(y_1 + \lambda x_1) + \mu x_1^2}{x_1^2}$$
$$= \frac{\lambda(x_1^3 + bx_1) - b(y_1 + \lambda x_1) + \mu x_1^2}{x_1^2}$$
$$= \frac{x_1^2(\lambda x_1 + \mu) - by_1}{x_1^2} = \frac{y_1(x_1^2 - b)}{x_1^2} = \overline{y_1}.$$

An identical argument shows that $\phi(Q)$ and $\phi(R)$ lies on $y = \overline{\lambda}x + \overline{\mu}$.

Now one must show that the x-coordinate of $\phi(P)$, $\phi(Q)$ and $\phi(R)$ are the roots of $(\overline{\lambda}x + \overline{\mu})^2 = \overline{f}(x)$. As this will require complex analysis, I will not go into this.

b) Recall that

$$\overline{\overline{C}} : y^2 = x^3 + 4ax^2 + 16bx.$$

The map $(x, y) \to (x/4, y/8)$ is clearly an isomorphism from $\overline{\overline{C}}$ to C, so combining this with a), we have shown that $\psi \circ \phi$ is an homomorphism from C to itself. It remains to show that $\psi \circ \phi$ yields the duplication formula. From Equation (22) and Equation (23) we cancel the terms containing c and we get that

$$2P = \left(\frac{x^4 - 2bx^2 + b^2}{4y^2}, \frac{x^6 - 2ax^5 + 5bx^4 - 5b^2x^2 - 2ab^2x - b^3}{8y^3}\right)$$
$$= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(y^4 - (a^2 - 4b)x^4)}{8y^3x^2}\right)$$

Recalling that

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right), \qquad \psi(\overline{x}, \overline{y}) = \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right),$$

we have that

$$\psi \circ \phi(x, y) = \psi\left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right)$$
$$= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2 - 4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right)$$
$$= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(y^4 - (a^2 - 4b)x^4}{8y^3x^2}\right)$$
$$= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2}{8y^3}\right) = 2P$$

Similarily, we show that $\phi \circ \psi(\overline{x}, \overline{y}) = 2(\overline{x}, \overline{y})$:

$$\phi \circ \psi(\overline{x}, \overline{y}) = \phi\left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right)$$

$$= \left(\frac{\left(\frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right)^2}{\left(\frac{\overline{y}^2}{4\overline{x}^2}\right)^2}, \frac{\left(\frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right)\left(\left(\frac{\overline{y}^2}{4\overline{x}^2}\right)^2 - b\right)}{\left(\frac{\overline{y}^2}{4\overline{x}^2}\right)^2} \right)$$

From Equation (33) we have that $b = \frac{\overline{a}^2 - 4\overline{b}}{16}$:

$$= \left(\frac{(\overline{x}^2-\overline{b})^2}{4\overline{y}^2}, \frac{\left(\frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}\right)\left(\left(\frac{\overline{y}^2}{4\overline{x}^2}\right)^2 - b\right)}{\left(\frac{\overline{y}^2}{4\overline{x}^2}\right)^2} \right)$$

$$= \left(\frac{(\overline{x}^2-\overline{b})^2}{4\overline{y}^2}, \frac{(\overline{x}^2-\overline{b})(\overline{y}^4 - (\overline{a}^2 - 4\overline{b})\overline{x}^4)}{8\overline{y}^3\overline{x}^2} \right)$$

$$= \left(\frac{(\overline{x}^2-\overline{b})^2}{4\overline{y}^2}, \frac{(\overline{x}^2-\overline{b})(\overline{x}^4 + 2\overline{a}\overline{x}^3 + 6\overline{b}\overline{x}^2 + 2\overline{a}\overline{b}x + \overline{b}^2}{8\overline{y}^3} \right) = 2\overline{P}$$

□

This means that we have the curves

$$C : y^2 = x^3 + ax^2 + bx, \qquad \overline{C} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where

$$\overline{a} = -2a, \quad \overline{b} = a^2 - 4b,$$

with the following homomorphisms

$$\phi : C \to \overline{C}, \qquad \psi : \overline{C} \to C,$$

such that $\phi \circ \psi : \overline{C} \to \overline{C}$ and $\psi \circ \phi : C \to C$ are both multiplications by two. It remains to show that this implies that the index $(\Gamma : 2\Gamma)$ is finite. The proof can be found on p. 83-86 in [1]. □

6 The Mordell theorem

Theorem 6.1. *(Descent Theorem) Let* Γ *be a commutative group. Given a mapping*

$$h : \Gamma \to [0, \infty),$$

that satisfies Lemma 5.3, 5.4, 5.6 and 5.7. Then Γ *is finitely generated.*

Proof. Since 2Γ has finite index in Γ, we know there is a finitely many cosets. Let

$$Q = \{Q_1, ..., Q_n\}$$

denote representatives for each coset such that every point P in Γ has a corresponding coset in Q. Then there exists an index i_1 such that

$$P - Q_{i_1} \in 2\Gamma,$$

which is equivalent to

$$P - Q_{i_1} = 2P_1.$$

Further we similarly have

$$P_1 - Q_{i_2} = P_2,$$

$$\vdots$$

$$P_{m-1} - Q_{i_m} = 2P_m.$$

Combining these equations we get that.

$$P = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Applying Lemma 5.4 and replacing P_0 with Q_i, we get that

$$h(P - Q_i) \leq 2h(P) + \kappa_i.$$

Do this for all Q_i, $1 \leq i \leq n$. Then let

$$\kappa' = \max_{1 \leq i \leq n} \kappa_i.$$

Now let κ be the constant from Lemma 5.6. Then we calculate that

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \geq 2h(P_{j-1}) + \kappa' + \kappa.$$

By manipulating this expression we get that

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)).$$

If $h(P_{j-1}) \geq \kappa' + \kappa$, we get that

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}).$$

We have now shown that as long as $h(P_j) \leq \kappa' + \kappa$, there exists a sequence of points $\{P, P_1, ...\}$ such that $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. But if m gets large, we get that $h(P_j) \to 0$, so there must exist some m such that $h(P_m) \leq \kappa' + \kappa$.

This implies that every point P in Γ can be written on the form

$$P = a_1 Q_1 + a_2 Q_2 + ... + a_n Q_n + 2^m R, \tag{34}$$

for some integers $a_1, ..., a_n$ and some point R in Γ such that $h(R) \leq \kappa' + \kappa$. Hence, Γ is finitely generated. $\square$

7 Rank of elliptic curves

From Mordell's theorem, we know that

$$\Gamma \cong \mathbb{Z}^r \oplus \mathbb{Z}_{n_1} \oplus ... \oplus \mathbb{Z}_{n_k}.$$

The rank of Γ is simply the exponent r of $\mathbb{Z}$. The part

$$\mathbb{Z}_{n_1} \oplus ... \oplus \mathbb{Z}_{n_k}$$

is called the *torsion subgroup* of Γ. The torsion subgroup can be calculated quite easily with help from the Nagell-Lutz theorem:

Theorem 7.1 (Nagell-Lutz)**.** *Let*

$$C : y^2 = f(x) = x^3 + ax + b$$

be an elliptic curve with $a, b \in \mathbb{Z}$. If (x, y) is a rational point of finite order, then $x, y \in \mathbb{Z}$ and y either equals zero or the square of y divides the discriminant of C.

The proof can be found in [1] and is not in the scope of this thesis. Calculate the discriminant D of C and consider the possible divisors y of D. The integer roots of $f(x) - y^2$ then becomes a basis for the torsion group.

Example 7.2. *The torsion subgroup of $C : y^2 = x^3 - 43x + 166$ can be found by first calculating the discriminant*

$$D = -4 \cdot (-43)^3 - 27 \cdot 166^2 = -13 \cdot 2^{15}.$$

Going over the possible divisors and checking for integer solutions of $f(x) - y^2$ gives the following basis for the torsion group

$$P = \{\mathcal{O}, (3, \pm 8), (-5, \pm 16), (11, \pm 32)\}.$$

While the torsion group is simple to calculate, no current general algorithm exists for computing the rank of an elliptic curve exactly. The current record for finding an elliptic curve with the highest rank is due to Elkies with rank 28[3]:

$$y^2 + xy + y = x^3 + x^2 - 20067762415575526585033208209338542750930230312178956502x$$
$$+ 3448161179503055646703298569039072037485 5$$
$$94435931918036126600829629193944873224342 9.$$

We will look at a basic approach for determining the rank of some elliptic curves. We start by consider the subgroup 2Γ:

$$2\Gamma \cong 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z} \oplus 2\mathbb{Z}_{n_1} \oplus \cdots \oplus 2\mathbb{Z}_{n_k}$$

We then consider the quotient group $\Gamma/2\Gamma$:

$$\frac{\Gamma}{2\Gamma} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}_{n_1}}{2\mathbb{Z}_{n_1}} \oplus \frac{\mathbb{Z}_{n_k}}{2\mathbb{Z}_{n_k}}.$$

Observe that

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{Z}_2$$

$$\frac{\mathbb{Z}_{n_i}}{2\mathbb{Z}_{n_i}} \cong \begin{cases} Z_2, & \text{if } n_i \equiv 0 \bmod 2. \\ 0, & \text{otherwise,} \end{cases}$$

which results in

$$(\Gamma : 2\Gamma) = 2^{r+(\#\text{ of } n_i \text{ such that } n_i \equiv 0 \bmod 2)} \tag{35}$$

Further let $\Gamma[2]$ denote the subgroup of order 2. Let $Q \in \Gamma[2]$, then we have that

$$Q = 2(a_1P_1 + \cdots + a_rP_r + b_1Q_1 + \cdots + b_sQ_s) = 0$$

This happens when $a_i = 0$ and $2b_i \equiv 0 \bmod n_i$ for all i. If n_i, then we must have that $b_i \equiv 0 \bmod n_i$. If $n_i = 2^{x_i}$, then we only end up with $b_i \equiv 0 \bmod 2^{x_i-1}$. We see that

$$\#\Gamma[2] = 2^{(\text{number of } n_j \text{ with } n_j \equiv 0 \bmod 2)} \tag{36}$$

We then get from Equation (35) and Equation (36) that

$$(\Gamma : 2\Gamma) = 2^r \cdot \#\Gamma[2].$$

Apart from $\mathcal{O}$, the points of order two corresponds to the points having y-coordinate equal to zero. It can be shown that

$$\#\Gamma[2] = \begin{cases} 2, & \text{if } a^2 - 4b \text{ is not a square} \\ 4, & \text{if } a^2 - 4b \text{ is a square.} \end{cases}$$

From Mordell's theorem we have that $2\Gamma = \psi \circ \phi(\Gamma)$. We then get that

$$(\Gamma : 2\Gamma) = (\Gamma : \psi \circ \phi(\Gamma)).$$

Since $2\Gamma \subseteq \psi(\overline{\Gamma}) \subseteq \Gamma$, we get that

$$(\Gamma : 2\Gamma) = (\Gamma : \psi(\overline{\Gamma}))(\psi(\overline{\Gamma}) : \psi \circ \phi(\Gamma)).$$

Now let A be an abelian group, B a subgroup of A with finite index and $\psi : A \to A'$ be a group homomorphism. We then get from group theory that

$$\frac{\psi(A)}{\psi(B)} \cong \frac{A}{(B + \ker(\psi)} \cong \frac{A/B}{(B + \ker(\psi))/B} \cong \frac{A/B}{\ker(\psi)/(\ker(\psi) \cap B)},$$

which results in

$$(\psi(A) : \psi(B)) = \frac{(A : B)}{(\ker(\psi) : \ker(\psi) \cap B)}.$$

Now let $A = \overline{\Gamma}$ and $B = \phi(\Gamma)$. This gives that

$$(\Gamma : 2\Gamma) = \frac{(\Gamma : \psi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \phi(\Gamma))}{(\ker(\psi) : \ker(\psi) \cap \phi(\Gamma))}.$$

We have that $\overline{T} \in \phi(\Gamma)$ iff $\overline{b} = a^2 - 4b$ is a square, so we have that

$$(\ker(\psi) : \ker(\psi) \cap \phi(\Gamma)) = \begin{cases} 2, & \text{if } \overline{b} \text{ is not a square,} \\ 1, & \text{if } \overline{b} \text{ is a square} \end{cases}$$

This gives that

$$2^r = \frac{(\Gamma : 2\Gamma)}{\#\Gamma[2]} = \frac{(\Gamma : \psi(\overline{\Gamma})) \cdot (\overline{\Gamma} : \phi(\Gamma))}{4}. \tag{37}$$

Now let $\mathbb{Q}^*$ be the multiplicative group of non-zero numbers. Let

$$\mathbb{Q}^{*2} = \{x^2 | x \in \mathbb{Q}^*\}.$$

We then give the following mapping $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*\not=}$ by

$$\alpha(P) = \begin{cases} 1 \bmod \mathbb{Q}^{*2}, & P = \mathcal{O} \\ b \bmod \mathbb{Q}^{*2}, & P = T \\ x \bmod \mathbb{Q}^{*2}, & P = (x, y), x \neq 0 \end{cases}$$

It can be shown that α is a homomorphism with the kernel being $\psi(\Gamma)$, so we have that

$$\alpha(\Gamma) \cong \frac{\Gamma}{\psi(\overline{\Gamma})}.$$

Hence, we have that $(\Gamma : \psi(\overline{\Gamma}) = \#\alpha(\Gamma)$. If we define the homomorphism $\overline{\alpha} : \overline{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ similarly, we get that $(\overline{\Gamma} : \phi(\Gamma)) = \#\overline{\alpha}(\overline{\Gamma})$. This results in 37 becomming

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4}. \tag{38}$$

We will compute the rank from this formula by determining the image of $\alpha(\Gamma)$ and $\overline{\alpha}(\overline{\Gamma})$. We know from Lemma 5.2 that $(x, y) = (m/e^2, n/e^3)$. If $m = 0$, then $\alpha(x, y) = \alpha(T) = b$, so $b \bmod \mathbb{Q}^{*2}$ is in $\alpha(\Gamma)$. If $d^2 = a^2 - 4b$, we also have that

$$\left(\frac{-a+d}{2}, 0\right) \in \Gamma, \qquad \left(\frac{-a-d}{2}, 0\right) \in \Gamma,$$

so $\alpha(\Gamma)$ contains $(-a \pm d)/2$.

Now assume $m, n \neq 0$. Then we have from the elliptic curve that

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4). \tag{39}$$

It can be shown that m and $m^2 + ame^2 + be^4$ are relatively prime, so it follows that they are both squares. Let $b_1 = \gcd(m, b)$, then we can write

$$m = b_1 m_1, \qquad b = b_1 b_2, \qquad \text{with } \gcd(m_1, b_2) = 1, \quad m_1 > 0.$$

Substituting this into 39 gives

$$n^2 = b_1^2 m_1 (b_1 m_1^2 + a m_1 e^2 + b_2 e^4)$$

It follows that $b_1|n$, so $n = b_1 n_1$, which gives that

$$n_1^2 = m_1(b_1 m_1^2 + a m_1 e^2 + b_2 e^4).$$

We further have that m_1 and $b_1 m_1^2 + a m_1 e^2 + b_2 e^4$ are coprime, so they are both squares. Let $n_1 = MN$ such that

$$M^2 = m_1 \qquad N^2 = b_1 m_1^2 + a m_1 e^2 + b_2 e^4,$$

which can be narrowed down to the equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4. \tag{40}$$

This means that if you have $(x, y) \in \Gamma$, we have that

$$(x, y) = \left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3} \right)$$

We can now find the order of $\alpha(\Gamma)$ by finding all the different factorizations of b into $b_1 b_2$. For each factor, consider $b \bmod \mathbb{Q}^{*2}$ and $b_1 \bmod \mathbb{Q}^{*2}$ such that Equation 40 has a solution with $M \neq 0$. We also have that $\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = 1$, and assuming $\gcd(b_2, m_1) = 1$ gives that

$$\gcd(b_2, M) = \gcd(M, N) = 1.$$

Now notice that if we have that $a^2 - 4b = d^2$, then we have that $(-a \pm d)/2 \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. From Equation 40 we get that

$$N^2 = \left(\frac{-a \pm d}{2} \right) M^4 + a M^2 e^2 + \left(\frac{-a \mp d}{2} \right) e^4,$$

which has the trivial solution $(M, e, N) = (1, 1, 0)$. We will now look at a couple examples where we determine the rank.

Example 7.3.

$$C : y^2 = x^3 - x, \qquad \overline{C} : y^2 = x^3 + 4x.$$

We see that $b = 1 = (-1) \cdot (1) = (1) \cdot (-1)$ *and* $a = 0$*, so* $b_1 = \pm 1$*. Observing that* $\alpha(T) = b = -1$ *and* $\alpha(\mathcal{O}) = 1$*, we get that*

$$\alpha(\Gamma) = \{\pm 1 \bmod \mathbb{Q}^{*2}\},$$

so $\#\alpha(\Gamma) = 2$*. Further we see that* $\overline{b} = 4$*, so* $b_1 = \{\pm 1, \pm 2, \pm 4\}$*. We have that* $\pm 4 \equiv \pm 1 \bmod \mathbb{Q}^{*2}$*, so the set reduces to* $\{\pm 1, \pm 2\}$*. This gives us the following set of equations:*

- $N^2 = M^4 + 4e^4$
- $N^2 = -M^4 - 4e^4$
- $N^2 = 2M^4 + 2e^4$
- $N^2 = -2M^4 - 2e^4$

Since we assume M is nonzero, it is trivial that the second and the fourth equation has no solutions. The first and the third equation has solutions $(M, e, N) = (1, 0, 1)$ and $(M, e, N) = (2, 1, 1)$ respectively, so $\#\overline{\alpha}(\overline{\Gamma}) = 2$. Hence, it follows from Equation 39 that C_1 has rank zero.

Example 7.4.

$$C : y^2 = x^3 - 5x, \qquad \overline{C} : y^2 = x^3 + 20x.$$

As in the previous example we are determining $\#\alpha(\Gamma)$ and $\#\overline{\alpha}(\overline{\Gamma})$. We see that $b_1 = \{\pm 1, \pm 5\}$, so we get the following set of equations:

- $N^2 = M^4 - 5e^4$
- $N^2 = -M^4 + 5e^4$
- $N^2 = 5M^4 - e^4$
- $N^2 = -5M^4 + e^4$

The first and second equation is the same equations as the third and the fourth, only with M and e reversed. Since we only will find equations such that Me is nonzero, we can consider only the first and the second equation. Some trial-and-error gives the solutions $(M, e, N) = (3, 2, 1)$ and $(M, e, N) = (1, 1, 2)$ to the first and second equation respectively. This corresponds to the solutions $(x, y) = (9/4, 3/8)$ and $(x, y) = (-1, -2)$. Hence, we have that

$$\alpha(\Gamma) = \{\pm 1, \pm 5\} \bmod \mathbb{Q}^{*2},$$

which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

When it comes to $\overline{\alpha}(\overline{\Gamma})$, we see that $\overline{b} = a^2 - 4b = 20$, so

$$\overline{b}_1 = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}.$$

Further we have that $\pm 4 \equiv \pm 1 \bmod \mathbb{Q}^{*2}$ and $\pm 20 \equiv \pm 5 \bmod \mathbb{Q}^{*2}$, so the set reduces to

$$\overline{b}_1 = \{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

Since $\overline{b} = 20$ is positive, we see that $\overline{b}_1$ and $\overline{b}_2$ from the following equation

$$N^2 = \overline{b}_1 M^4 + \overline{b}_2 e^4$$

must have same sign. Since they obviously can not be negative, we can reduce the set to

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{1, 2, 5, 10\} \bmod \mathbb{Q}^{*2}.$$

We then see that $\overline{\alpha}(\overline{\mathcal{O}}) = 1$, $\overline{\alpha}(\overline{T}) \equiv 20 \equiv 5 \bmod \mathbb{Q}^{*2}$. It remains to check if

$$N^2 = 2M^4 + 10e^4$$

has solutions in integers. By considering the number of factors of two, we have that the right hand side must have $4k + 1$ factors of two for $k \in \mathbb{Z}^+$, while the left hand side has $2k$ factors of two for $k \in \mathbb{N} + \{0\}$. Hence, we have that

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 5\} \bmod \mathbb{Q}^{*2},$$

so it follows that

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4} = 2,$$

and we conclude that the rank is 1.

References

[1] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*, Springer 1992.

[2] J. S. Milne, *Elliptic Curves*, Kea Books 2006.

[3] Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007.