university of groningen

faculty of science and engineering

On Elliptic Curves over the Rationals Containing Points of Order 3

Levi Moes

July 2022

Abstract

In this paper we will discuss the group structure of elliptic curves over $\mathbb{Q}$ which contain a rational point of order 3, namely we will use 3-descent to prove that the group of rational points for such a curve is finitely generated abelian. This shows the methods used to prove the subcase of Mordell's theorem for Elliptic Curves with a rational point of order 2 can be adapted to the case at hand. We shall finish by showing that the methods used in this thesis can provide bounds on the rank of curves of the form $y^2 = x^3 + A^2(ax - b)^2$ where all coefficients are rational.

Supervisors:
Prof. Dr. Jaap Top,
Dr. Pınar Kılıçer

Contents

1 Introduction

At the writing of this thesis it is nearly 100 years ago that Louis Mordell [5] proved that for a ternary homogeneous cubic f the points satisfying $f(x, y, z) = 0$ can be expressed as rational combinations of some finite set of points.

In more digestible terminology we turn to Silverman, who phrases this result as the set of rational points of an elliptic curve

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

being a finitely generated abelian group [7, Theorem 4.1]. This is proven through 2-descent. While the majority of the conditions for 2-descent are fairly elementary to prove in the case of elliptic curves over $\mathbb{Q}$, the condition that the quotient group $E(\mathbb{Q})/mE(\mathbb{Q})$ is finitely generated requires sophisticated tools from Galois Cohomology.

Introductory texts like the book of Tate and Silverman [8] get around this problem by proving only that elliptic curves containing a point of order 2 are finitely generated. Since in this case one is able to define a curve $\bar{E}$ over $\mathbb{Q}$) and maps $\varphi : \bar{E}(\mathbb{Q}) \to E(\mathbb{Q}), \psi : E(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$ such that $[2] = \varphi \circ \psi$ thus

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = [E : \varphi \circ \psi E(\mathbb{Q})] \leq [E : \varphi(\bar{E}(\mathbb{Q}))][\bar{E}(\mathbb{Q}) : \varphi(E(\mathbb{Q}))].$$

Then it is possible to find a map $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ whose image can be shown to be finite and a bound for these the index is then given as

$$[E(\mathbb{Q}) : \varphi(E(\mathbb{Q}))] \leq (\# \operatorname{Im} \alpha)(\# \operatorname{Im} \bar{\alpha})$$

[8, Proposition 3.8]. In our case we will focus on curves which have a point of order 3. This requires us to use 3-descent rather than 2-Descent, and moreover we will have to map to rings which are less friendly than $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, so we will require some more number theory than in the case of a point of order 2.

The first few chapters shall be dedicated to defining elliptic curves and giving examples of points of finite order. The later chapters will be about the proof of this subcase of Mordell's theorem and how it can be used to find bounds for heights, a relation defined in section 5, of certain elliptic curves.

2 Some Prerequisites

2.1 Cubic Polynomials

In this thesis we will be working a lot with cubic polynomials. The particular flavour we will be working with are the monic cubics. These are cubics of the form

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

where $a, b, c \in K$ where K is a field, generally one of characteristic other than 2. Moreover we want f separable, that is, having distinct roots.

When we are working with quadratics we have the discriminant given by the famous $b^2 - 4ac$, which tells us whether a quadratic has distinct roots. For a monic cubic we can similarly define a discriminant.

Definition 2.1. *Let $f \in K[x]$, with K a field and for our purposes typically $\mathbb{Q}$, be monic, and let α_i be the roots of f. The discriminant of f is defined as*

$$D := \prod_{i \neq j} (\alpha_i - \alpha_j)^2.$$

Clearly, if the roots of f are distinct, then $D \neq 0$, and if they are not distinct then some pair of indices $i \neq j$ exists so that $\alpha_i = \alpha_j$ and therefore $D = 0$. Importantly, we can express D as in terms of the coefficients of f.

2.2 Projective Geometry

The following definitions are inspired by [2, Section 3]. Let K be a field. The aim of this section is to define points at infinity on a curve defined over K, which we will require later in this thesis.

Definition 2.2. *Let $n \in \mathbb{N}$ and $u, v \in K^{n+1}$ and view K^{n+1} as a vector space over K. We define an equivalence $\sim_n$ via $u \sim_n v$ if and only if u and v are linearly dependent.*

It should be obvious this indeed defines a family of equivalence relations.

Definition 2.3. *Let $n \in \mathbb{N}$. We define projective n-space over K as*

$$\mathbb{P}^n := \frac{K^{n+1} \setminus \{(0, \dots, 0)\}}{\sim_n}.$$

So one way to view $\mathbb{P}^n$ is as all lines through $(0, \dots, 0)$. Similarly we have the definition of affine space.

Definition 2.4. *Let $n \in \mathbb{N}$, then we define affine n-space as*

$$\mathbb{A}^n(K) := K^n$$

We take some sets in $\mathbb{P}^n$, namely

$$U_i := \{(x_1, \dots x_n, x_{n+1}) \in \mathbb{P}^n : x_i \neq 0\}.$$

We denote an element $P \in U_i$ as

$$P = [x_1 : x_2 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n].$$

And we have a map $\varphi_i : \mathbb{A}^n(K) \hookrightarrow U_i$ via

$$(x_1, \dots x_n) \mapsto (x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n).$$

Since clearly

$$\mathbb{P}^n(K) = \bigcup_{i=1}^{n+1} U_i$$

we can view $\mathbb{P}^n$ as $n+1$ copies of the affine n-space, which are glued together in some way.

Note that $\mathbb{P}^2$ is very close to to $\mathbb{A}^2(K)$, namely,

$$\mathbb{P}^2 = \left\{(x,y,1) : (x,y) \in \mathbb{A}^2(K)\right\} \cup \left\{(x,y,0) : [x:y] \in \mathbb{P}^1\right\}$$

but in $\mathbb{P}^1$ we are much in the same situation as before, namely

$$\mathbb{P}^1 = \left\{(x,1) : x \in \mathbb{A}^1(K)\right\} \cup \{(1,0)\}.$$

So we have a point left, which we view as the *point at infinity.*

Definition 2.5. *Let $F \in K[x,y,z]$, we call F homogeneous if $F(tx,ty,tz) = t^d F(x,y,z)$ for d the degree of F.*

For instance, we can couple a monic cubic with a homogeneous polynomial $f(x) = x^3 + ax^2 + bx + c$ via

$$f(x) \quad \sim \quad F(x,y,z) = z^2 y - (x^3 + azx^2 + bz^2 x + cz^3)$$

and then setting $F(x,y,1) = 0$ yields back the original equation. In general we can find a homogeneous polynomial for every curve defined by the equality of 2 polynomials $g(x,y) = f(x,y)$ we can change a term $x^n y^k$ to a term $x^n y^k z^{d-n-k}$ to get such a polynomial. So for a polynomial $f(x)$ we set f^h to be this homogeneous polynomial, for a homogeneous f we set $f^i(x,y) = f(x,y,1)$. This yields a bijection

$$\{f \in K[x_1,x_2] : \deg f = n\} \leftrightarrow \left\{\text{homogeneous} f \in K[x,y,z] : f(x,y,z) \neq zf'(x,y,z)\, \forall f' \in K[x,y,z]\right\}.$$

We call f^h the projective closure, that is, the projective polynomial which has affine part f.

Definition 2.6. *Let $F \in K[x_1,x_2,x_3]$ be homogeneous of degree n. Then we define the set of points*

$$V(F) := \left\{P \in \mathbb{P}^2 : F(P) = 0\right\}$$

So with the relation we found before, these are all the points on a curve { (x, y) :$g(x,y) = f(x,y)\}$ and we can think of it similarly to the graph

$$\left\{(x,y,f(x,y)) : (x,y) \in \mathbb{Q}^2\right\}.$$

Example 2.7. Consider the following curve over $\mathbb{A}^2(K)$

$$\{(x,y) : f(x,y) = -y^2 + x^3 + ax^2 + bx + c\}$$

so that

$$f^h(x,y,z) = -zy^2 + x^3 + azx^2 + bz^2 x + cz^3.$$

Then we find bijections

$$\begin{aligned} V(f^h) &= \left\{P \in \mathbb{P}^2 : f^h = 0\right\}, \\ &\leftrightarrow \left\{(x,y) \in \mathbb{A}^2(K) : f(x,y) = 0\right\} \cup \left\{(x,y,0) : (x,y) \in \mathbb{P}^1, f^h(x,y,0) = 0\right\}. \end{aligned}$$

The first set is just the set of points on the curve, while for the second we find

$$f^h(x,y,0) = x^3$$

so this set contains just the point $(0,1,0)$, we call this the point at infinity. △

3 Elliptic Curves

The general notion of an elliptic curve shall be the focus for this thesis. For our purposes, a convenient definition is as follows.

Definition 3.1. *Let K be a field of characteristic different from 2 and $f(x) \in K[x]$ be a 3rd degree monic polynomial having distinct roots. An elliptic curve is a curve given by*

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

We denote for a given elliptic curve

$$E(K) := \{(x, y) \in \mathbb{A}^2(K) : y^2 = f(x)\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at $(0, 1, 0)$ from example 2.7.

Since we are talking about an Elliptic *Curve* it is tempting to look at a case where K allows us to graph a function depicting the points on t he elliptic curve.

Example 3.2. Take $K = \mathbb{R}$, $f(x) = x^3 + px^2 + 1$, where we let $p \in \{-2, \ldots, 3\}$. This yields a sequence of elliptic curves E_p, we used python to depict these curves n $[-5, 5] \times [-5, 5]$.

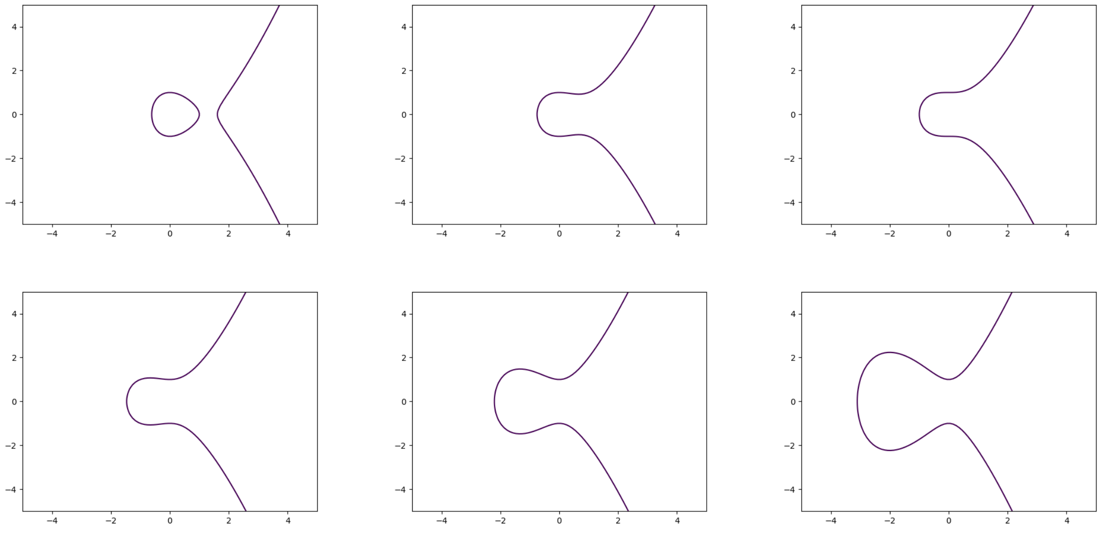

Figure 1: The curves $y^2 = x^3 + px^2 + 1$ for $p \in \{-2, \ldots, 3\}$.

△

It should be noted that an elliptic curve is not always a curve in the Calculus sense, but may also consist of a series of seemingly random points, as is illustrated in the following example.

Example 3.3. Take p a prime with $p \equiv 3 \mod 4$ and take the elliptic curve $y^2 = x^3 + nx$ over $\mathbb{F}_p$ with $n \in \mathbb{F}_p^\times$. To find $E(\mathbb{F}_p)$ we aim to find when $x^3 + nx$ is a square modulo p. Note that -1 is not a square, since the Legendre symbol equals

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{3+4k-1}{2}} = (-1)^{1+2k} = -1.$$

Fix some $a \in \mathbb{F}_p$ which is not a zero of $f := x^3 + nx$, then note $f(-a) = -f(a)$, thus

$$\left(\frac{f(a)}{p}\right)\left(\frac{f(-a)}{p}\right) = \left(\frac{f(a)}{p}\right)^2 \left(\frac{-1}{p}\right) = -1.$$

Hence precisely one of $f(a)$ and $f(-a)$ is a square.

When a is a zero of f we know that $a(a^2 + n) = 0$. Since we are working in a field that means $a = 0$ or $a^2 + n = 0$. So a is not a zero of f unless $a = 0$ or $a = \pm n$. Since we can only factor $x^3 + nx$ into 3 linear factors or a quadratic factor and a linear factor, we have either 1 root ($a = 0$) or 3 roots.

So for half of all residue classes x which are not roots we can find two points $(x, \sqrt{f(\pm x)})$ and $(x, -\sqrt{f(\pm x)})$ on the curve. Hence we have that there are $(p-1)/2$ possible x-coordinates, each corresponding to two y-coordinates. Along with the root 0 and the point at infinity giving

$$\#E(\mathbb{F}_p) = 2(p-1)/2 + 2 = p + 1$$

or we have $(p-3)/2$ x-coordinates corresponding to two points on the curve, along with 3 points corresponding to a root and 1 point at infinity, so

$$\#E(\mathbb{F}_p) = 2(p-3)/2 + 4 = p + 1.$$

For instance when $p = 7$ we can find that on the curve $y^2 = x^3 + x$ we have the points

$$E(\mathbb{F}_p) = \{\mathcal{O}, (0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5)\}.$$

△

The main reason we are interested in elliptic curves is that $E(K)$ is an abelian group. In the case that $K = \mathbb{Q}$ there is a geometric interpretation of what this means, which uses only elementary algebra.

3.1 Elliptic Curves over the Rationals

We take $E : y^2 = f(x)$ to be an elliptic curve over $\mathbb{Q}$. As an example of such a curve we take $f(x) = x^3 - 6x + 9$. Let us take two points on this curve, say $(-3, 0)$ and $(1, 2)$. Then note we can draw a line through both of these points and it intersects the curve at a 3rd point $(9/4, 21/8)$.

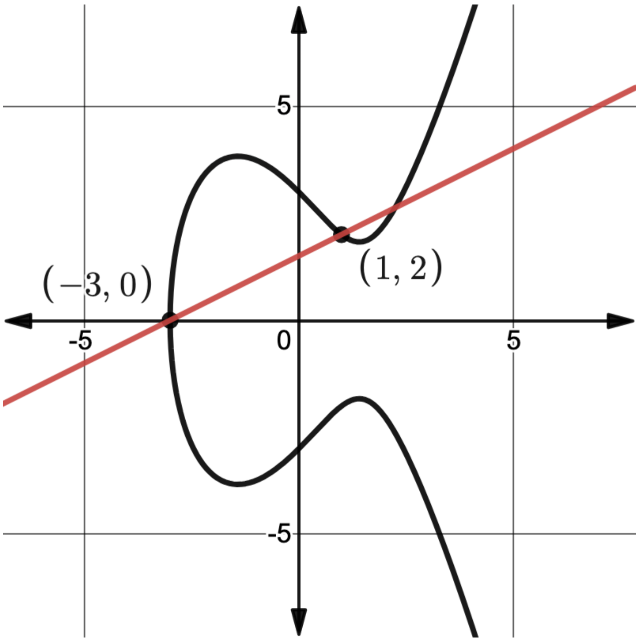

Figure 2: Two points on $y^2 = f(x)$

In fact, barring a few exceptions, we can use this method to obtain a 3rd point when we know two points on the curve.

When we have two distinct points $(x_1, y_1), (x_2, y_2) \in E(\mathbb{Q})$ with $x_1 \neq x_2$, we can use algebra to find a line through both, namely the line

$$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1.$$

Note that this line does not intersect the curve in a 3rd point in $\mathbb{Q}$ when $y_1 = y_2$. Barring this case though, we find via a straightforward computation that

$$x_3 = \left[\frac{y_2 - y_1}{x_2 - x_1}\right]^2 - (x_1 + x_2), \qquad y_3 = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x_3 - x_1) \tag{1}$$

is also a point on this curve.

If the points are not distinct, then [8, Chapter 1.4] describes how we can similarly use the tangent line, which also leads to a point with coordinates in $\mathbb{Q}$.

At this point it is tempting to define a group law by mapping $* : ((x_1, y_1), (x_2, y_2)) \mapsto (x_3, y_3)$. Sadly this is not associative.

Counterexample 3.4. We shall show that taking the 3rd point of intersection as the result of our operation does not yield an associative operation. Namely we consider the curve [1]

$$E : y^2 = x^3 + 113.$$

It is then readily verified that

$$P = (-4, 7), \qquad Q = (2, 11), \qquad R = (8, 25)$$

are points on the curve.

It is moreover verified that

$$\begin{aligned} P * Q &= (22/9, 305/27), \\ Q * R &= (-42/9, -116/27), \end{aligned}$$

and thus

$$\begin{aligned} (P * Q) * R &= (-109/25, -686/125), \\ P * (Q * R) &= (422, 8669). \end{aligned}$$

So indeed $*$ is not associative.

3.1.1 The Group law

Luckily a small modification of $*$ does yield an associative operation, namely when we take the 3rd point of intersection, and replace y by $-y$.

[1] This curve was not picked at random, namely this curve has rank 3, so we can pick 3 distinct elements which have infinite order with respect to the associative operation we shall define later. We picked this since for points of (small) finite order $*$ tends to be associative: none of the curves I tried yielded a counterexample.

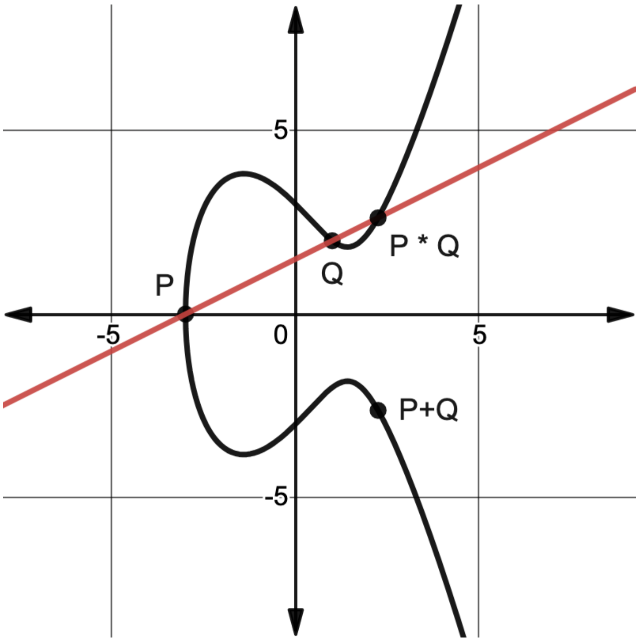

Figure 3: Depiction of the group law

This still leaves a number of edge cases. For instance, when two points are antipodes there is not going to be a 3rd point of intersection in $\mathbb{Q}^2$. Luckily we have a point at infinity, which we will define to be the sum of two antipodes.

After this motivation we introduce the following definition, which is used by [8, Section 1.4].

Definition 3.5. *Let $P = (x_1, y_1), Q = (x_2, y_2)$ be points on an Elliptic curve $y^2 = x^3 + ax^2 + bx + c$ other than $\mathcal{O}$, define an operation $+_E$ as follows.*

1. *If $P \neq Q$ and $x_1 = x_2$ then $P +_E Q = \mathcal{O}$.*
2. *If $P = Q$ and $y_1 = 0$ then $P +_E Q = \mathcal{O}$*

If neither of these are the case we define λ and ν as follows.

1. *if $P \neq Q$ and $x_1 \neq x_2$ then*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

2. *If $P = Q$ and $y_1 \neq 0$ then*

$$\lambda = \frac{3x_1^2 + a}{2y_1}, \qquad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1}$$

then

$$P +_E Q = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu).$$

Finally we define $P +_E \mathcal{O} = \mathcal{O} +_E P = P$. When it is clear from context what the curve is, we will write $+$ instead of $+_E$.

So we have a set, together with a binary operation. This motivates the following theorem.

Theorem 3.6. *Let $E : y^2 = f(x)$ be an elliptic curve. Then $(E(\mathbb{Q}), +_E, \mathcal{O})$ is an abelian group.*

Proof. By construction, we have that $+_E : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q})$ is well defined. Namely, it is clear from equation (1) that when $P, Q \in E(\mathbb{Q})$, then also $P * Q \in E(\mathbb{Q})$. Consequently, the reflection in the y-axis is also in $E(\mathbb{Q})$.

Moreover, if we have a line $y = ax + b$ through $P, Q \in E(\mathbb{Q})$, then this yields an equality

$$\left(\frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1\right)^2 = x^3 + px^2 + qx + r$$

Which yields a root finding problem for $\tilde{f}(x) = 0$. We know that we can factor $\tilde{f}(x) = (x - x_1)(x - x_2)(x - A)$, for some A. We argue A must be rational, since if $A \notin \mathbb{Q}$, then we would have

$$\tilde{f}(x) = -Ax_1x_2 + Ax_1x + Ax_2x - Ax^2 + x_1x_2x - x_1x^2 - x_2x^2 + x^3$$

not having rational coefficients. But clearly $\tilde{f}$ must have rational coefficients, so we conclude A is the x coordinate of a 3rd point of intersection, and moreover there cannot be any more factors, so there are precisely 3 points of intersection. So indeed $+_E$ is well-defined.

It should also be clear that $+_E$ is commutative, since $P +_E Q$ and $Q +_E P$ would yield the same 3rd point of intersection.

Inverses are also straightforward: we think of $\mathcal{O}$ of sitting at infinity, so the line through a point and its antipode (which may be the point itself if we are talking about points like $(-3, 0)$ as in figure 2) will only intersect at infinity.

The proof of $+_E$ being associative can be found in [11, Section 2.4] □

We shall from now on just denote $E(\mathbb{Q})$ to indicate this group.

3.2 Elliptic Curves Over Other Fields

In an arbitrary field of characteristic other than 2 we can define + analogously to definition 3.5. While it is possible to have elliptic curves over a field of characteristic 2 this requires a more subtle definition that we will not go into.

Theorem 3.7. *Let K be a field with characteristic different from 2, and $E : y^2 = f(x)$ an elliptic curve over K. Then $(E(K), +_E, \mathcal{O})$ is an abelian group.*

We expand on this in the following example.

Example 3.8. Let p be a prime and $E : y^2 = f(x)$ an elliptic curve over $\mathbb{F}_{p^n}$. For any finite field $\mathbb{F}_{p^n}$ we surely have $E(\mathbb{F}_{p^n})$ is finite. So by the structure theorem for finitely generated abelian groups [3, Theorem 2.8] there exist finitely many $a_i \in \mathbb{N}_0$ such that

$$E(\mathbb{F}_{p^n}) \simeq \mathbb{Z}/a_0\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}.$$

In Example 3.3 we found that for $p \equiv 3 \mod 4$ a curve $E : y^2 = x^3 + nx$ has $\#E(\mathbb{F}_p) = p + 1$.

When $p = 43$ and $n = 1$ we have $\#E(\mathbb{F}_{43}) = 44 = 2^2 \cdot 11$. The only two Abelian groups of this order are $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It can be verified that $(27, 42)$ is a point of order 4, so

$$E(\mathbb{F}_{43}) \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/44\mathbb{Z}.$$

△

3.3 Isogenies

Since we know that an elliptic curve $E : y^2 = f(x)$ over a field K has an associated abelian group $E(K)$, it is natural to speak about group homomorphisms between these groups. This leads us to the following definition.

Definition 3.9. *Let E_1, E_2 be elliptic curves over a field K. An isogeny $\varphi : E_1(K) \to E_2(K)$ is a group homomorphism that is a rational function in both coordinates, that is*

$$\varphi(x, y) = (\phi(x, y), \psi(x, y))$$

where ϕ and ψ are quotients of polynomials.

The astute reader might notice that this definition is over-engineered, as one can prove that any rational function $\varphi : E_1(K) \to E_2(K)$ satisfying $\varphi : \mathcal{O} \mapsto \mathcal{O}$ would automatically be a group homomorphism. And this is indeed what Silverman proves in the following theorem [8, Theorem III.4.8].

Theorem 3.10. *Let E_1, E_2 be elliptic curves over a field K and $\varphi : E_1(K) \to E_2(K)$ be rational maps such that $\varphi(\mathcal{O}) = \mathcal{O}$, then φ is a group homomorphism.*

Below we shall go into some examples that shall come in useful later.

Example 3.11. Fix some $n \in \mathbb{N}$ then $[n] : P \mapsto nP$ is an isogeny, since it is clearly a rational function, and it is also a homomorphism of groups as by definition $n\mathcal{O} = \mathcal{O}$. And since the group of rational points on an elliptic curve is abelian

$$nA + nB = A + \dots A + B + \dots B = A + B + \dots + A + B = n(A + B).$$

△

The following example is the subject of [10, Chapter 2.2] and will be important later in this thesis.

Example 3.12. Let $A, B \in \mathbb{Q}$ and $\bar{A} = -27A, \bar{B} = 4A + 27B$

$$E : y^2 = x^3 + A(ax - B)^2, \qquad \bar{E} : \eta^2 = \xi^3 + \bar{A}(a\xi - \bar{B})^2$$

so that are elliptic curves, for each pair of parameters A, B we define the map

$$\Phi_{A,B} : (x, y) \mapsto (\xi, \eta),$$

where

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

If we define $\Phi_{A,B} : \mathcal{O} \mapsto \mathcal{O}$ then by theorem 3.10 it follows that $\Phi_{A,B}$ is an isogeny. If we apply the map $\Phi_{\bar{A},\bar{B}} \circ \Phi_{A,B}$ we obtain the curve

$$C : y^2 = x^3 + 3^6 A(ax - 3^6 B)^2.$$

The change of coordinates

$$(x, y) \mapsto (3^6 x, 3^9 y)$$

gives

$$3^{18}y = 3^{18}x^2 + 3^{18}A(ax - B)^2$$

which is the equation of E multiplied by 3^{18}. In conclusion, letting [3] denote the multiplication by 3 map makes the following diagram commute.

$$\begin{tikzcd}
E(\mathbb{Q}) \arrow[r, "\Phi_{A,B}"] \arrow[rr, bend left, "{[3]}"] & \bar{E}(\mathbb{Q}) \arrow[r, "\Phi_{\bar{A},\bar{B}}"] & C(\mathbb{Q})
\end{tikzcd}$$

△

4 Points of Finite Order

We shall introduce the concept of torsion in the context of Abelian groups, after this we will use this to prove properties of the torsion subgroup of the rational points on an elliptic curve.

Definition 4.1. *Let A be an Abelian group. A point of finite order is called a torsion point. We denote the set of all torsion points in A as A_{tors}.*

Theorem 4.2. *A_{tors} is a subgroup of A.*

Proof. Let $(A, e, *)$ be an Abelian group and $H = \{x \in A : |x| < \infty\}$, then $H \leq A$ since clearly $e \in H$ and when $x, y \in H$ then $\operatorname{ord}(xy^{-1}) = \operatorname{lcm}(\operatorname{ord}(x), \operatorname{ord}(y^{-1})) = \operatorname{lcm}(\operatorname{ord}(x), \operatorname{ord}(y)) < \infty$, so $xy^{-1} \in H$. □

Definition 4.3. *Let $(A, e, *)$ be an Abelian group, define*

$$A[n] := \{x \in A : x^n = e\} .$$

Theorem 4.4. *$A[n]$ is a subgroup of A_{tors}.*

Proof. Note that $A[n]$ is precisely the kernel of $f : x \mapsto x^n$, therefore it must be a subgroup, since clearly $e \in \ker f$ and moreover $x, y \in \ker f$ means $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e$. □

Example 4.5. If K is finite then $E(K) = E(K)_{\text{tors}}$ follows by Lagrange's Theorem. △

Example 4.6. A point of order 2 must have a vertical tangent line. Consider the curve $y^2 = x^3 + 6x^2 + 5x$ over $\mathbb{Q}$, the points with such a tangent line are depicted in figure 4.

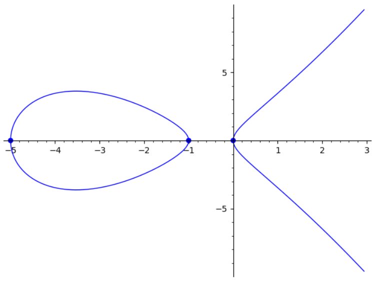

Figure 4: Points of order 2 on $y^2 = x^3 + 6x^2 + 5x$ over $\mathbb{Q}$.

There are three such points, so we have

$$E(\mathbb{Q})[2] = \{\mathcal{O}, (-5, 0), (-1, 0), (0, 0)\} .$$

In particular this tells us $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, since this is a group of 4 elements and all points besides the identity have order 2. △

A deeper result about points of finite order is the following theorem.

Theorem 4.7. *Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$ with integer coefficients. All torsion points of $E(\mathbb{Q})$ have integer coordinates. Moreover if $(x, y) \in E(\mathbb{Q})_{\text{tors}}$ and $y = 0$ then P has order 2, else $y^2 | D$, the discriminant of f.*

The proof of this theorem is outside the scope of this thesis and it can be found in [8, Section 2.5]. This theorem shall be useful when we are trying to find points of finite order.

4.1 Points of Order 2

It is immediately obvious that a point of order 2 must be on the x-axis, since this would mean $P = -P$ thus $(x, y) = (x, -y)$, so this x-coordinate is precisely a root of the corresponding cubic.

Example 4.8. The class of elliptic curves

$$E : y^2 = f(x) = x(x^2 + bx + c)$$

over $\mathbb{Q}$ all have a root $x = 0$, moreover we can use the quadratic formula to factor this as

$$y^2 = x\left(x - \frac{b}{2} + \frac{1}{2}\sqrt{b^2 - 4c}\right)\left(x - \frac{b}{2} - \frac{1}{2}\sqrt{b^2 - 4c}\right).$$

So in fact we can have two additional points of order 2 if $b^2 - 4c$ is a perfect square.

So we can take $b = 5$ and $c = 4$ as then $b^2 - 4c = 25 - 4^2 = 16$ giving us 3 points of order 2 on the curve $y^2 = x(x^2 + 5x + 4)$. △

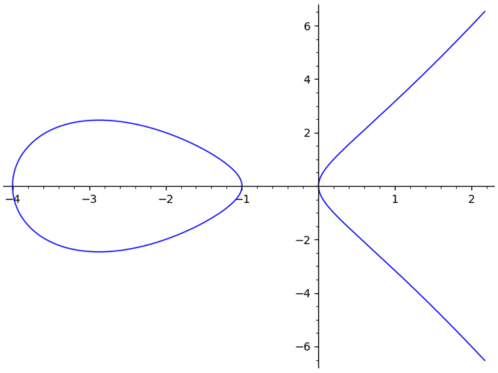

Figure 5: The curve $y^2 = x(x^2 + 5x + 4)$

4.2 Points of Order 3

A point P having order 3 may be phrased as $2P = -P$, so this means that the x coordinates of $-P$ and $2P$ must be the same. For an elliptic curve $y^2 = x^3 + ax^2 + bx + c$ one can find that the x coordinate of $2P$ is given by

$$F(x) = \frac{x^4 - 2bx^2 - 8xcx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{2}$$

So a point of order 3 is a fixed point $F(x) = x$, so

$$\begin{aligned} F(x) = x \iff & \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x \\ \iff & x^4 - 2bx^2 - 8xcx + b^2 - 4ac = 4x^4 + 4ax^3 + 4bx^2 + 4cx \\ \iff & \underbrace{3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2}_{\psi_3} = 0. \end{aligned}$$

Silverman notes that $\psi_3 = 2f(x)f''(x) - f'(x)^2$ [8, Section 2.1]. So points of order 3 are roots of this polynomial.

Theorem 4.9. *Let $E : y^2 = f(x)$ be an elliptic curve. Then $\mathcal{O} \neq P \in E(\mathbb{Q})$ has order 3 if and only if it is a point of infliction.*

This result is an exercise in the book of Tate and Silverman [8, Exercise 2.2].

Proof. We first find the second derivative, using the chain rule

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} = \frac{\mathrm{d}^2\sqrt{y^2}}{\mathrm{d}x^2} = \frac{\mathrm{d}}{\mathrm{d}x}\left[\frac{\mathrm{d}^2\sqrt{y^2}}{\mathrm{d}y^2}\frac{\mathrm{d}y^2}{\mathrm{d}x}\right] = \frac{\mathrm{d}}{\mathrm{d}x}\left[\frac{1}{2\sqrt{y^2}}f'(x)\right] = \left[\frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{2y}\right]f'(x) + \frac{1}{2y}f''(x).$$

Note that

$$\frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{2y} = \frac{\mathrm{d}}{\mathrm{d}y^2}\frac{1}{2y}\frac{\mathrm{d}y^2}{\mathrm{d}x} = -\frac{1}{4y^3}f'(x).$$

Putting this all together we obtain

$$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} = -\frac{1}{4y^3}f'(x)^2 + \frac{1}{2y}f''(x) = \frac{2y^2}{4y^3}f''(x) - \frac{1}{4y^3}f'(x)^2 = \frac{2f(x)f''(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)},$$

since $y^2 = f(x)$. Since a point (x_0, y_0) of order 3 has $\psi_3(x_0) = 0$, it follows that (x_0, y_0) is an infliction point if and only if (x_0, y_0) has order 3. □

So finding a point of order 3 reduces to finding the roots of the quartic polynomial ψ_3. From the fundamental theorem of algebra, it then follows that for every elliptic curve there is a point of order 3 in $E(\mathbb{C})$, but we are interested in rational points. We shall prove several lemmas which lead up to a result about points of order 3.

Lemma 4.10. *ψ_3 has distinct roots in $\mathbb{C}$.*

This is similar to a result in the book by Tate and Silverman [8, Theorem 2.1]

Proof. Recall $\psi_3(x) = 2f(x)f''(x) - f'(x)^2$, so via the product rule

$$\psi_3' = 2\left[f'f'' + f'''f\right] - 2f'f''.$$

But f is monic of order 3, so $f''' = 6$, so $\psi_3' = 12f$. Since f cannot share any roots with f' it follows that ψ_3 and ψ_3' do not share any roots. In conclusion, ψ_3 has distinct complex roots. □

Lemma 4.11. *ψ_3 has precisely 2 real roots.*

This is again an exercise in Tate-Silverman [8, Exercise 2.2b].

Proof. We compute $f''(x) = 6x + 2a$, this has a root $x = -a/3$. Since $f'(x) = 3x^2 + 2ax + b$ we find $f'(-a/3) = -a^2/3 - 2a^2/3 + b = b - a^2$. So

$$\psi_3(-a/3) = -(b - a^2)^2 < 0.$$

But surely the term $3x^4$ is going to be much larger than the lower order terms, so at some point $0 \neq x_0 > -a/3$ it is the case that $\psi_3(x_0) > 0$ and $\psi_3(-x_0) > 0$. So by the intermediate value theorem [9, Theorem 4.35] we get the existence of two real roots.

The coefficients of ψ_3 are all real, so we cannot have precisely 3 real roots, as then we could find $x_4 \notin \mathbb{R}$ and so

$$\psi_3 = \prod_{i=1}^{4}(x - x_i) = x\prod_{i=1}^{3}(x - x_i) - x_4\prod_{i=1}^{3}(x - x_i) \notin \mathbb{R}[x].$$

So we can only have 2 or 4 real roots.

Suppose we have $x_1 < x_2 < x_3 < x_4$ real roots, where x_1 and x_4 are the roots we proved exist. Then at two points between x_1 and x_4: $\psi_3' = 12f$ must change sign. It follows $f''(x_2) > -a/3$. By the same argument applied to x_3 and x_4 we find $x_3 < -a/3$ so $x_2 > x_3$ which contradicts our ordering. Rearranging this argument for all possible orderings of the roots can be done similarly. □

Theorem 4.12. *Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. If $E(\mathbb{Q})$ contains a point of order 3 then E is isogenous to a curve*

$$y^2 = x^3 + A^2(a'x + b')^2,$$

for some constants $A, a', b' \in \mathbb{Q}$.

Proof. Let $P = (a, b)$ have order 3. Without loss of generality we assume $a = 0$, else we define the isogeny $(x, y) \mapsto (x + a, f(x + a))$. And moreover we get that $P = (0, \pm\sqrt{c})$.

Consider the tangent line to P. We know this has form

$$y = \frac{\mathrm{d}y}{\mathrm{d}x} x \pm \sqrt{c}.$$

From 4.9 we know

$$\frac{\mathrm{d}y}{\mathrm{d}x} = \frac{f'(x)}{2y}.$$

So we get the tangent line

$$y = \frac{f'(0)}{2b} x \pm \sqrt{c} = \frac{c}{2b} x \pm \sqrt{c}.$$

Setting this equal to the equation of the curve we obtain

$$\left[\frac{c}{2b} x + \sqrt{c}\right]^2 = x^3 + ax^2 + bx + c.$$

Substituting $x = 0$ in equation 2 shows that $b^2 = 4ac$, continuing with this we obtain that either $b = 0$, in which case we have $E : y^2 = x^3 + c$ and otherwise we can solve this final equation to find constants A, B such that our curve has form $E : y^2 = x^3 + A^2(x - B)^2$. In both cases we have a curve in the promised form. □

4.2.1 Examples of Curves with a Point of Order 3

Example 4.13. When $a = 0$ and $c = 0$ we get an elliptic curve $y^2 = x^3 + bx$ and our ψ_3 can be factored easily, since then the famous quadratic formula can be used to find

$$3x^4 + 6bx^2 - b^2 = 0 \iff x^2 = -b \pm 2/3\sqrt{3}b \iff x = \pm\sqrt{-b \pm 2/3\sqrt{3}b}.$$

So such an elliptic curve never has a rational point of order 3 because this x is never rational unless $b = 0$, which yields a singular curve and hence not elliptic. △

Example 4.14. Consider the curve $E : y^2 = x^3 + x^2 + 2x + 1$ over $\mathbb{Q}$. This gives polynomial

$$\psi_3 = 3x^4 + 4x^3 + 12x^2 + 12x.$$

Which has a rational root $x = 0$. Hence the points $(0, \pm 1)$ are of order 3, and moreover these are the only points of order 3, giving us $E(\mathbb{Q})[3] \simeq \mathbb{Z}/3\mathbb{Z}$.

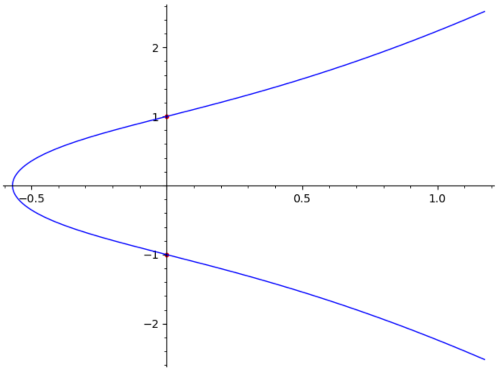

Figure 6: Points of order 3 on $y^2 = x^3 + x^2 + 2x + 1$.

△

For some more general elliptic curves we can find if a point of order 3 exists as follows.

Corollary 4.15. *Suppose the coefficients defining our elliptic curve are integers: $a, b, c \in \mathbb{Z}$. Then any point of order 3 has x-coordinate dividing $4ac - b^2$.*

Proof. From the rational root theorem [1, Section 9.4] any rational root of ψ_3 has the form $x = p/q$ where p, q are coprime integers, moreover theorem 4.7 tells us $q = 1$ so $p|4ac - b^2$. So it follows immediately from the rational root theorem. □

Example 4.16. For the elliptic curve $y^2 = x^3 + 3x^2 + 3x + 2$ we have that any rational x satisfying this equality has $x|15$. By trying all divisors of 15 we find $\psi_3(-1) = 0$ and hence we conclude $(0, -1)$ is a point of order 3. △

Example 4.17. The elliptic curve $y^2 = x^3 - 9x + 9$ has $b^2 - 4ac = -81$, which has divisors $\pm1, \pm3, \pm9, \pm81$. So by trial and error on

$$\psi_3 = 3x^4 - 54x^2 + 108x - 81.$$

wE find that $\psi(3) = 0$. Hence $(3, \pm3)$ are the points of order 3. △

Example 4.18. The curve $y^2 = x^3 + 1$ is quite interesting. Since it contains both a point of order 2 and a point of order 3, clearly -1 is a root of $x^3 + 1$, which corresponds to a point $(-1, 0)$ of order 2, while 0 is a root of ψ_3 so $(0, \pm1)$ are points of order 3. So we multiply a point of order 2 with a point of order 3 to give us a point of order 6, namely the point $(3, 2)$ has order 6. △

4.3 Higher Orders

As was seen between points of order 2 and 3, the amount of computations needed to determine a point of order n quickly increases as n increases. While as we saw it was easy to find a point of order 6 as we could simply add a point of order 2 with one of order 3, it would be much harder to find points whose order has only one prime factor.

A deeper result regarding points of finite order is Mazur's theorem.

Theorem 4.19. *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 12$ with $n \neq 11$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{1, 2, 3, 4\}$.*

Sadly this result is not within our reach to prove, and to anyone interested we refer to [4, Theorem 2]. Another way to phrase this theorem is that the only possible finite orders are the integers 1 through

12 barring 11. We have already seen points of order 2, 3, and 6, so we shall aim to find representatives for most of the other possible orders.

For this we need to expand our definition of an elliptic curve a bit, before we have only talked about curves of the form $y^2 = f(x)$. But we can proceed identically with curves of the form $y^2 + ay + bxy = f(x)$, though we have not done so because this would only serve to increase the amount of computations needed while distracting from the main point, the proof of these curves also forming an abelian group can be found in [7, Chapter III.3].

An integral result needed in computing the order of points is the reduction modulo p theorem.

Theorem 4.20. *Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$ with integer coefficients, take p a prime and $\pi_p : \mathbb{Z} \to \mathbb{F}_p$ the canonical projection. Let the curve $E_p : \bar{y}^2 = \bar{f}(\bar{x})$ be given by applying π_p to both sides of the equation of E. Then unless $p|2D$, where D is the discriminant, we have that the homomorphism $\varphi : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ via*

$$\varphi : \begin{cases} (x, y) & \mapsto (\bar{x}, \bar{y}), \\ \mathcal{O}_{\mathbb{Q}} & \mapsto \mathcal{O}_{\mathbb{F}_p}, \end{cases}$$

induces an isomorphism

$$E(\mathbb{Q})_{\text{tors}} \simeq \operatorname{Im} \varphi \leq E(\mathbb{F}_p).$$

The proof of this statement can be found in [8, Section 4.3]. A helpful consequence of this theorem is that for such φ we have that

$$\#E(\mathbb{Q})_{\text{tors}} | \#E(\mathbb{F}_p).$$

Now we are equipped to find some examples, luckily we need not search far as Tate and Silverman readily provide us with a list of examples to work out in [8, Exercise 2.12].

Example 4.21. We consider the curve

$$E : y^2 = x^3 + 4x.$$

It is immediately clear that this curve has a point of order 2, as $x = 0$ is a root of the polynomial in x.

We note that the curve has discriminant 2, so we are free to conclude that

$$\#E(\mathbb{Q})_{\text{tors}} | \#E_3(\mathbb{F}_3).$$

It is easily found that the latter number is 4. So the only remaining possibilities are 2 and 4. We suspect that the order might be 4, and using a bit of trial and error and remembering points of finite order have integer coefficients, we do indeed get that $(2, 4)$ has order 4, which immediately tells us that

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z}.$$

△

Example 4.22. Now we look at

$$E : y^2 - y = x^3 - x^2.$$

We reduce modulo 3 and immediately find that $\#E(\mathbb{Q})_{\text{tors}} | 5$. Using some trial and error we find the point $P = (0, 1)$ on our curve. And

$$\begin{aligned} P &= (0, 1), \\ 2P &= (1, 0), \\ 4P &= (0, 0). \end{aligned}$$

And then it is clear that $5P = \mathcal{O}$ so indeed we found a point of order 5, and as a group of prime order we have

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}.$$

△

We have already seen a point of order 6 hence we shall skip this order.

Example 4.23. Now we consider the curve

$$y^2 = x^3 - 43x + 166.$$

Which has discriminant $2^{19} \cdot 13$. So we can safely look at the reduction modulo 5. It is easily found that $\#E_5(\mathbb{F}_5) = 7$, so the only possible orders of our torsion group are 1 and 7. Using a bit of trial and error we see that $(3, 8) \in E(\mathbb{Q})$. By taking some inspiration from the methods of [8, Chapter 4.3].

$$\begin{aligned} 1P &= (3, 8), \\ 2P &= (-5, -16), \\ 4P &= (11, 32), \\ 8P &= (3, 8). \end{aligned}$$

So $8P = P$ hence indeed P has order 7 and consequently

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}.$$

△

5 Mordell's Theorem

Our main endeavour will be to prove a subcase of the following statement.

Theorem 5.1. *For any elliptic curve over the rationals $E : y^2 = f(x)$, the group $E(\mathbb{Q})$ is finitely generated.*

This requires results which are beyond the scope of this thesis [7, Section VIII] . We shall prove the weaker version.

Theorem 5.2. *Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{Q}$. If $E(\mathbb{Q})$ contains a point of order 3, then $E(\mathbb{Q})$ is finitely generated.*

As we discussed in the introduction, our method shall be to that of 3-descent, which is explained in chapter 5.1.

By use of the structure theorem for finitely generated abelian groups [3, Theorem 8.5] we see that this theorem says that for any elliptic curve E with a point of order 3 over the rationals there is some $r \in \mathbb{Z}_{\geq 0}$ such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}.$$

Which is a fact we shall later use to find bounds on the rank for some curves.

5.1 The 3-descent Theorem

Our main tool for proving Mordell's Theorem for such curves is the 3-descent theorem, which is as follows.

Theorem 5.3. *Let A be an Abelian group. Suppose there exists a function $h : A \to \mathbb{R}$ such that for all $P \in A$ the following holds.*

1. *Let $Q \in A$ there is $C_1(A, Q) \in \mathbb{R}$ such that*
$$h(P + Q) \leq 2h(P) + C_1(A, Q). \tag{3}$$
2. *There is $C_2(A)$ such that*
$$h(3P) \geq 9h(P) - C_2(A). \tag{4}$$
3. *For every constant C_3 the set*
$$\{Q \in A : h(Q) \leq C_3\} \tag{5}$$
is finite.
4. *The quotient group*
$$A/3A \tag{6}$$
is finite.

Then A is finitely generated.

We call such a function a *height function.* This theorem is the case $m = 3$ of the general descent theorem [7, Theorem 3.1]. After we have this tool, proving theorem 5.2 reduces to proving each of the conditions. The proof of this mirrors the one given by Silverman for the general descent theorem.

Proof. Since we assume $A/3A$ is finite, take representatives $Q_1, \ldots, Q_n \in A$ as representatives of the conjugacy classes. In addition, take arbitrary $P \in A$. Our goal will be to show $P - h(Q)$ where Q is some linear combination of the $Q_1, \ldots, Q_n$ is arbitrarily small, allowing us to conclude the $Q_1, \ldots, Q_n$ together with the points with smaller height are a generating set for $E(\mathbb{Q})$.

We write $P = 3P_1 + Q_{i_1}$ for some $1 \leq i_1 \leq r$. Repeat this for P_1 to obtain a sequence

$$\begin{aligned} P &= 3P_1 + Q_{i_1}, \\ P_1 &= 3P_2 + Q_{i_2}, \\ &\vdots \\ P_{r-1} &= 3P_r + Q_{i_r}. \end{aligned}$$

this gives that for any index j:

$$\begin{aligned} h(P_j) &\leq \frac{1}{3^2}(h(3P_j) + C_2) \\ &= \frac{1}{3^2}\left(h(P_{j-1} - Q_{i_j}) + C_2\right) \\ &\leq \frac{1}{3^2}(2h(P_{j-1} + \underbrace{\max\{-Q_1, \ldots, -Q_n\}}_{C_1'} + C_2)) \end{aligned}$$

Now we apply this inequality repeatedly, and note a geometric series

$$\begin{aligned} h(P_r) &\leq \left(\frac{2}{3^2}\right)^r h(P) + \left[\frac{1}{3^2} + \frac{2}{(3^2)^2} + \cdots + \frac{2^{r-1}}{(3^2)^r}(C_1' + C_2)\right] \\ &< \left(\frac{2}{3^2}\right)^r h(P) + \frac{C_1' + C_2}{3^2 - 2} \\ &\leq \frac{1}{2^r} h(p) + \frac{1}{2}(C_1' + C_2) \end{aligned}$$

so for sufficiently large r

$$h(P_r) \leq 1 + \frac{1}{2}(C_1' + C_2).$$

And because P is a linear combination of P_r and the Q_i we have

$$P = 3^r P_r + \sum_{j=1}^{r} 3^{j-1} Q_{i_j}$$

so any $P \in A$ can be written as a linear combination of

$$\{Q_1, \ldots Q_r\} \cup \{Q \in A : h(Q) \leq 1 + 1/2(C_1' + C_2) :\}$$

which is assumed to be finite. □

5.2 Sketch of the Proof

Now that we have proven the 3-descent theorem we can prove our desired result by finding a function such that each of the conditions in the descent theorem hold. As we shall shortly see, this function is not particularly difficult to define and the first 3 of the conditions are fairly straightforward to prove for elliptic curves over $\mathbb{Q}$ in general, see [7, Lemma 4.1]. Where we run into trouble is in the final condition which does not depend on the height function, the so called *Weak Mordell Weil Theorem.*

Lemma 5.4. *Let E be an elliptic curve over $\mathbb{Q}$ which has a point of order 3. Then $E(\mathbb{Q})/3E(\mathbb{Q})$ is finite.*

This will be the condition for which we will use our assumption that there is a point of order 3 on our curve, since otherwise we will require non-elementary results from cohomology which are beyond the scope of this thesis.

Nevertheless, this proof will require some more skill than the other parts of the 3-descent theorem. We shall have to touch upon some tools relating to algebraic number theory, but no knowledge of this field is assumed and knowledge of the basics of field theory will be sufficient to follow this proof.

As a final note on the remainder of this thesis, we shall prove properties 1, 2, and 3 of the descent theorem are true in Sections 6.1, 6.2, and 6.3 respectively. Property 4 will be shown in section 7. Finally, we shall use the methods from these chapters to discuss some bounds on the ranks of some curves in Section 8

6 Finding a Height Function

This chapter will be about finding a height function suitable for $E(\mathbb{Q})$, and then proving the first 3 properties in theorem 5.3 hold for elliptic curves over $\mathbb{Q}$.

We will first discuss a few examples so as to motivate an intuition behind a height function.

Example 6.1. In the case that $A = \mathbb{Q}$ we can define a function $h_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$

$$h_{\mathbb{Q}} : p/q \mapsto \max\{|p|, |q|\}. \tag{7}$$

And while it is known $\mathbb{Q}$ is not finitely generated as a group, we can still prove one of the properties from the 3-descent theorem holds. Namely, we know that for fixed $m \in \mathbb{R}$ there are only finitely many rational numbers with height bounded by m. If $h(p/q) \leq m$ then both $p, q \leq m$, for which there are only finitely many possibilities. △

Definition 6.2. *(heights on elliptic curves) If $E : y^2 = f(x)$ is an elliptic curve over $\mathbb{Q}$, then we define the height of a point $P = (x, y)$ as $h(P) = \ln h_{\mathbb{Q}}(x)$, where $h_{\mathbb{Q}}$ is as in equation 7.*

The remainder of this section shall be dedicated to proving this notion of height satisfies theorem 5.3.

6.1 Bound on Height

Here we prove the first property of the 3-descent theorem, namely

Lemma 6.3. *Let $E : y^2 = f(x)$ be an elliptic curve. Then if $P \in E(\mathbb{Q})$ then for every $Q \in E(\mathbb{Q})$ there is an integer C_1 such that*

$$h(P + Q) \leq 2h(P) + C_1. \tag{8}$$

This is found in [8, Section 3.2].

Proof. If $Q = \mathcal{O}$ then this is trivial. Suppose $Q \neq \mathcal{O}$, we prove that for all P except for $P \in \{-Q, Q, \mathcal{O}\}$ there is $\tilde{C_1}$ such that 8 holds. Then set $C_1 = \max\{h(-Q), h(Q), h(\mathcal{O}), \tilde{C_1}\}$. This allows us to assume the x coordinates of the points are different.

So write $P = (x, y)$ and $Q = (x_0, y_0)$. So set $P + Q = (\xi, \eta)$. From how we defined the group law on elliptic curve 3.5 we find

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

Where this is the same a as in the definition of an elliptic curve $y^2 = x^3 + ax^2 + \cdots$. Using the relation of the curve we find there are rational numbers $A, \ldots, G$ such that

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

Without loss of generality, these are all integers, else we just multiply with their least common multiple. So note that when we fix P there is no dependence on the coordinates of Q anymore. So this shall serve for our constant C_1.

Using the substitution $x = m/e^2, y = n/e^3$ we simplify

$$\xi = \frac{Ane + Bm^2 + CM^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

So indeed

$$\exp h_{\mathbb{Q}}(\xi) \leq \max\left\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\right\}.$$

Applying the triangle inequality tells us

$$\exp h(P + Q) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\} \exp h(Q)^2$$

taking the log of both sides yields the desired result. □

6.2 Height of 3P

Now that we have proven the first property, we arrive at the second.

Lemma 6.4. *There is a constant C_1 such that*

$$h(3P) \geq 9h(P) - C_1.$$

The proof of this will consist of proving that this reduces to a special case of a lemma in the book by Tate and Silverman [8, Lemma 3.6] and then we prove this lemma. Specifically this lemma is

Lemma 6.5. *Let $\phi, \psi \in \mathbb{Z}[x]$ be coprime polynomials and $d = \max\{\deg\phi, \deg\psi\}$. Then the following are true.*

1. *There is $R \in \mathbb{N}$ depending only on the choice of ϕ and ψ such that for any $m/n \in \mathbb{Q}$*

$$\gcd\left(n^d\phi(m/n), n^d\psi(m/n)\right)$$

divides R.

2. *There are constants κ_1, κ_2 depending only on the choice of ϕ and ψ such that whenever $m/n \in \mathbb{Q}$ is not a root of ψ we have*

$$dh(m/n) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh(m/n) + \kappa_2.$$

Proof. For property a we first note that $n^d\psi(m/n)$ and $n^d\phi(m/n)$ are integers, namely the greatest possible term is $(m/n)^d$ which multiplied with n^d is an integer, and the same goes for all other possible terms. So it does indeed make sense to talk about divisibility.

Without loss of generality we assume $d = \deg\phi$ and $e = \deg\psi$. For ease of notation let us define

$$\Phi(m,n) := n^d\phi(m/n), \qquad \Psi(m,n) := n^d\psi(m/n).$$

So that we only want to find $\gcd(\Phi(m,n), \Psi(m,n))$. Since we assumed ψ, ϕ are coprime we can find $F, G \in \mathbb{Q}[x]$ such that

$$F\phi + G\psi = 1.$$

Moreover we can multiply both sides with the greatest common divisor of all denominators of the coefficients of F and G, which we shall denote as A, to obtain $AF, AG \in \mathbb{Z}[x]$, this gives us A and $D = \gcd(F, G)$ which is independent of m and n. In particular

$$\begin{aligned} An^{D+d}\left(F\left(\frac{m}{n}\right)\phi\left(\frac{m}{n}\right) + G\psi\left(\frac{m}{n}\right)\right) &= An^{D+d}, \\ \Rightarrow n^D AF\left(\frac{m}{n}\right)n^d\phi\left(\frac{m}{n}\right) + n^D AG\left(\frac{m}{n}\right)n^d\psi\left(\frac{m}{n}\right) &= An^{D+d}, \\ \Rightarrow n^D AF\left(\frac{m}{n}\right)\Phi(m,n) + n^D G\left(\frac{m}{n}\right)\Psi(m,n) &= An^{D+d}. \end{aligned}$$

So then the function $\gamma(m,n) := \gcd(\Phi, \Psi)(m,n)$ must divide An^{D+d}.

Since $\gamma|\Phi$ certainly it divides

$$An^{D+d-1}\Phi(m,n)Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}.$$

where the a_i are the coefficients of Φ. So γ must divide

$$\gcd\left(An^{D+d}, Aa_0m^dn^{D+d-1}\right).$$

By assumption of m/n being a reduced fraction, m and n are coprime, therefore $\gamma|Aa_0n^{D+d-1}$. Repeat these steps for $Aa_0n^{D+d-2}\Phi(m,n)$ we eventually obtain $\gamma|Aa_0^{D+d}$ which finished the proof of the first part of the lemma.

Now for the second part. We start with the lower bound, namely

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

for some κ_1 depending only on the choice of polynomials and m/n is not a root of ψ. As in lemma 6.3 we can ignore a finite set of points and simply take a maximum. Namely let m/n not be a root of either polynomial. Note that if $m/n \neq 0$ then $h(m/n) = h(n/m)$, so without loss of generality $d = \deg\phi$ and $e = \deg\psi$. For ease of notation set

$$\xi := \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\psi(m/n)} = \frac{\Phi(m,n)}{\Psi(m,n)}.$$

Where Φ, Ψ are as before. Note that

$$h(\xi) = \max\{|\Phi(m,n)|, |\Psi(m,n)|\},$$

unless these polynomials have a common factor. Using part a we find that $\gcd(\Phi(m,n), \Psi(m,n))$ divides the integer $R \geq 1$ we showed existed. Hence using the well known fact that a maximum is at least the average of its terms

$$h(\xi) \geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \geq \frac{n^d}{2R}\left(|\phi(m/n)| + |\psi(m/n)|\right).$$

So in fact

$$\begin{aligned}\frac{h(\xi)}{h(m/n)^d} &\geq \frac{1}{2R}\frac{1}{\max\{|m|^d, |n|^d\}}\left(|\phi(m/n)| + |\psi(m/n)|\right),\\ &= \frac{1}{2R}\frac{1}{\max\{|m/n|^d, 1\}}\left(|\phi(m/n)| + |\psi(m/n)|\right).\end{aligned}$$

Set

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

Which approaches a non-zero limit as $|t| \to \infty$. Using elementary calculus we find that if $\deg\psi < d$ then $p(t) \to |a_0|$ and if $\deg\psi = d$ then $|a_0| + |b_0|$, where a_0 and b_0 are the final coefficients of ϕ and ψ respectively.

So except for some closed interval I around the points we excluded, p is bounded away from 0. Inside this closed interval we note that it must assume a maximum and minimum value [9, Corollary 13.19]. As it is a bounded continuous function of a compact interval.

So we conclude the existence of some constant $C_1 > 0$ with $p \geq C_1$ for all $t \in \mathbb{R}$. So

$$h(\xi) \geq \frac{C_1}{2R}h(m/n)^d$$

so taking

$$\kappa_1 = \log\left(\frac{2R}{C_1}\right)$$

suffices. The proof of the upper bound is nearly identical to lemma 6.3 □

Now it remains to be shown this indeed implies lemma 6.4, this is shown in a more general case in [10, Appendix b].

Proof of Lemma 6.4. Take some $P \neq \mathcal{O}$ on the curve. We can write this in coordinates as $nP = (x_n, y_n)$. We claim that

$$x_3 = \frac{\phi(x_1)}{\psi(x_1)}$$

for some polynomials in $\mathbb{Z}[x]$ with $\gcd\{\deg\phi, \deg\psi\} = 9$. Then the statement of lemma 6.4 follows immediately by part b of lemma 6.5.

Remember from subsection 4.2 that writing the curve as $y^2 = f(x)$ there is a polynomial

$$\psi_3 = \frac{\mathrm{d}f}{\mathrm{d}x} + f\frac{\mathrm{d}^2 f}{\mathrm{d}x^2}$$

for a curve containing a point of order 3. It can be easily shown using the addition formulas we derived in section 4 that $\gcd(\phi, \psi) = 9$ and

$$\begin{aligned}\phi &= 8f\frac{\mathrm{d}f}{\mathrm{d}x}\psi_3 + 64f^3 + x_1\psi_3^2,\\ \psi &= \psi_3^2\end{aligned}$$

the full derivation can be found in [10, Appendix b]. This immediately shows our lemma in the case that ψ and ϕ are coprime. In the remaining case we have $f'(x_1)^2 = 2f(x_1)f''(x_1)$ which means

$$f'(x_1)^2 = 2f(x_1)f''(x_1) = 0$$

which contradicts f being a nonsingular polynomial hence this case is not possible. □

6.3 Points of Bounded Height

Now for the 3rd property.

Lemma 6.6. *For every constant C_3 the set*

$$\{Q \in A : h(Q) \leq C_3\}$$

is finite.

Note that this exact same reasoning also works over $\mathbb{Q}$.

Proof. Recall

$$h(p/q, y) = \ln\max\{|p|, |q|\}$$

so for any C_1 there are only finitely many options for p and q. □

The final property is significantly harder to prove and we will dedicate an entire chapter to it.

7 The Quotient Group is Finite

Throughout this section it shall be well understood that we are talking about an elliptic curve $E : y^2 = f(x)$ over $\mathbb{Q}$ such that $E(\mathbb{Q})$ has a point of order 3. We shall moreover be using shorthand

$$\Gamma := E(\mathbb{Q}), \qquad \bar{\Gamma} := \bar{E}(\mathbb{Q}).$$

This section shall be dedicated to proving the final part of theorem 5.3, that is

Theorem 7.1. *The index* $[\Gamma : 3\Gamma]$ *is finite.*

Recall that we can find maps such that the diagram

$$\begin{tikzcd} E(\mathbb{Q}) \arrow[r, "\Psi"] \arrow[rr, bend left, "{[3]}"] & \bar{E}(\mathbb{Q}) \arrow[r, "\Phi"] & 3E(\mathbb{Q}) \end{tikzcd}$$

commutes, so that

$$[\Gamma : 3\Gamma] = [\Gamma : \Phi \circ \Psi(\Gamma)] = [\Gamma : \Phi(\bar{\Gamma})][\Phi(\bar{\Gamma}) : \Psi \circ \Phi(\Gamma)].$$

Set $\Psi(\Gamma) = H$ so that $3\Gamma = \Phi(H)$. From the isomorphism theorems it follows

$$\frac{\Phi(\bar{\Gamma})}{\Phi(H)} \simeq \frac{\bar{\Gamma}}{H + \ker \Phi} \simeq \frac{\bar{\Gamma}/H}{(H + \ker \Phi)/H} \simeq \frac{\bar{\Gamma}/H}{\ker \Phi/(\ker \Phi \cap H)}.$$

Thus the index is given as

$$[\Phi(\bar{\Gamma}) : \Phi(H)] = \frac{[\bar{\Gamma} : H]}{[\ker \Phi : (\ker \Phi \cap H)]}.$$

So in conclusion there is some integer $N \in \mathbb{Q}_{\geq 0}$ such that

$$[\Gamma : 3\Gamma] = N[\Gamma : \Phi(\bar{\Gamma})][\bar{\Gamma} : \Psi(\Gamma)].$$

So showing these two indices are finite is sufficient.

This will be achieved by describing two homomorphisms $\alpha : \Gamma \to \mathbb{Q}^\times/\mathbb{Q}^{\times 3}$ and $\bar{\alpha} : \bar{\Gamma} \to \mathbb{Q}(\sqrt{-3})^\times/\mathbb{Q}(\sqrt{-3})^{\times 3}$ such that $\ker \bar{\alpha} = \Psi(\Gamma)$ and $\ker \alpha = \Phi(\bar{\Gamma})$, in other words

$$[\Gamma : 3\Gamma] \leq (\# \operatorname{Im} \alpha)(\# \operatorname{Im} \bar{\alpha}).$$

So it is sufficient to show each of these images is finite. In this chapter we shall be justifying we can indeed define these maps and showing that they have finite image.

7.1 The Rationals Modulo the 3rd Powers

A group which we will need to discuss is $\mathbb{Q}^\times/\mathbb{Q}^{\times 3}$. We can write a typical element $x \in \mathbb{Q}^\times$ as

$$x = \pm \prod_{i=1}^{\infty} p_i^{d_i}$$

where p_i is the $i$the prime, $d_i \in \mathbb{Z}$ and only finitely many d_i are nonzero.

Consider the ith generator

$$e_i := (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \bar{0}, \dots) \in \bigoplus_{i=1}^{\infty} \mathbb{Z}/3\mathbb{Z}.$$

Set $\iota : \mathbb{Q}^{\times 3} \hookrightarrow \mathbb{Q}^{\times}$ to be the inclusion. We find the following sequence is exact.

$$\begin{tikzcd}
\pm \prod_{i=1}^{\infty} p_i^{d_i} \arrow[r, mapsto, "f"] & \sum_i d_i e_i
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q}^{\times 3} \arrow[r, "\iota"] & \mathbb{Q}^{\times} \arrow[r, "f"] & \bigoplus_{\text{primes}}(\mathbb{Z}/3\mathbb{Z}) \arrow[r] & 0.
\end{tikzcd}$$

So from the first isomorphism theorem it follows

$$\mathbb{Q}^{\times}/\mathbb{Q}^{\times 3} \simeq \bigoplus_{\text{primes}} \mathbb{Z}/3\mathbb{Z}.$$

So without loss of generality, we can assume x is an integer times a coset, otherwise we just add 3 to the multiplicity of p^{-d} until we have a positive multiplicity. Moreover, since -1 is a cube we can assume x can be represented as a positive integer.

7.2 Mapping into the Rationals Modulo the Cubes

We define an elliptic curve

$$E : y^2 = x^3 + a^2(x-b)^2.$$

moreover define a map $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^{\times}/\mathbb{Q}^{\times 3}$ by

$$\alpha(P) = \begin{cases} \mathbb{Q}^{\times 3} & \text{if } P = \mathcal{O}, \\ (2ab)^{-1}\mathbb{Q}^{\times 3} & \text{if } P = (0, ab), \\ (y + a(x-b))\mathbb{Q}^{\times 3} & \text{otherwise.} \end{cases}$$

We shall prove this map is a group homomorphism. This map shall be important because we will prove that the image of α is finite.

7.2.1 Proof of Homomorphism Property

We will now show that α is a homomorphism. We shall require two more lemmas.

Lemma 7.2. $\alpha(-P) = \alpha(P)^{-1}$.

Proof. This is obvious if $P = \mathcal{O}$ and if $P = (0, \pm ab)$. So take $P = (x, y)$ with $x \neq 0$, then

$$\begin{aligned} \alpha(x,y)\alpha(x,-y) &= (y + a(x-b))\mathbb{Q}^{\times 3}(-y + a(x-b))\mathbb{Q},^{\times 3} \\ &= (-y^2 + a^2(x-b)^2)\mathbb{Q}^{\times 3}, \\ &= (-x^3 - a^2(x-b)^2 + a^2(x-b^2))\mathbb{Q}^{\times 3}, \\ &= \mathbb{Q}^{\times 3}, \end{aligned}$$

which completes the proof. □

The second lemma is as follows.

Lemma 7.3. *Take $P_i \in \Gamma$, if $P_1 + P_2 + P_3 = \mathcal{O}$ then $\alpha(P_1)\alpha(P_2)\alpha(P_3) = \mathbb{Q}^{\times 3}$.*

The proof is a simpler case of [10, lemma 5].

Proof. If we have a $\mathcal{O}$ among the P_i then this is trivial. The case that one of the P_i equals $(0, ab)$ is somewhat simpler than the remaining, general case which we now consider. If $P_1 + P_2 + P_3 = \mathcal{O}$ then the P_i are on a line. Call this $y = \lambda x + \eta$ for some $\lambda, \eta \in \mathbb{Q}$, this yields

$$(\lambda x + \eta)^2 = x^3 + a^2(x - b)^2,$$

so that

$$x^3 + (a^2 - \lambda^2)x^2 - (2a^2b - 2\lambda\eta)x + (a^2b^2 - \eta^2) = 0.$$

Write $P_i = (x_i, y_i)$, then the equation above has the x_i as roots so

$$x^3 + (a^2 - \lambda^2)x^2 - (2a^2b - 2\lambda\eta)x + (a^2b^2 - \eta^2) = 0 = \prod_{i=1}^{3}(x - x_i).$$

Comparing coefficients shows

$$\begin{cases} x_2x_3 + x_1x_2 + x_1x_3 = -2(a^2b + \lambda\eta), \\ x_1 + x_2 + x_3 = \lambda^2 - a^2, \\ x_1x_2x_3 = \eta^2 - a^2b^2. \end{cases} \tag{9}$$

And since $y_i = \lambda x_i + \eta$, we get

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \prod_{i=1}^{3}((\lambda x_i + \eta) + a^2(x_i - b))\mathbb{Q}^{\times 3}.$$

Since this is going to be a very long equation, we will split it up into the part that has factors a^4 and the part that has not. Starting with the former

$$\begin{aligned}(\lambda x_2 + \eta)(\lambda x_3 + \eta)(x_1 - b) + (\lambda x_1 + \eta)(\lambda x_2 + \eta)(x_3 - b) \\ +(\lambda x_1 + \eta)(\lambda x_3)(x_2 - b) + a^2(x_1 - b)(x_2 - b)(x_3 - b).\end{aligned}$$

By help of a computer, we rewrite this as

$$\begin{aligned}3\lambda^2x_1x_2x_3 + 2\lambda\eta(x_1x_3 + x_2x_3 + x_1x_2) + \eta^2(x_1 + x_2 + x_3) - \lambda^2b(x_1x_3 + x_2x_3 + x_1x_2) \\ -2\lambda\eta b(x_1 + x_2 + x_3) - 3b\eta^3 + a^2(x_1x_2x_3 - b(x_1x_3 + x_2x_3 + x_1x_2) + b^2(x_1 + x_2 + x_3) - b^3).\end{aligned}$$

Substitute our system of equations we find this simplifies to be $-3b\eta^2 - a^2b^3$.

For the other part, we obtain similarly

$$\begin{aligned}\lambda^3x_1x_2x_3 + \lambda^2\eta(x_1x_2 + x_2x_3 + x_1x_3) + \lambda\eta^2(x_1 + x_2 + x_3) + \eta^3 + 3a^2x_1x_2x_3 \\ +a^2(\eta - 2\lambda b)(x_1x_2 + x_2x_3 + x_1x_3) + a^2(\lambda b^2 - 2b\eta)(x_1 + x_2 + x_3) + 3\eta b^2.\end{aligned}$$

Substituting our system of equations this simplifies to $\eta^3 + 3\eta a^2b^2$

Adding these parts together yields a perfect cube. □

Lemma 7.4. *α is a homomorphism.*

Proof. Using the previous 2 lemmas we find that when $P_1 + P_2 + P_3 = \mathcal{O}$ we have $P_1 + P_2 = -P_3$, hence

$$\alpha(P_1 + P_2) = \alpha(-P_3) = \alpha(P_3)^{-1}.$$

But on the other hand

$$\alpha(P_1)\alpha(P_2) = (\alpha(P_1)\alpha(P_2)\alpha(P_3))\alpha(P_3)^{-1} = \alpha(P_3)^{-1}.$$

So $\alpha(P_1 + P_2) = \alpha(P_1)\alpha(P_2)$ □

7.2.2 Proof of Finite Image

Now that we can be sure α is a homomorphism we will set out to prove our desired result.

Lemma 7.5. *$\alpha(E(\mathbb{Q}))$ is finite.*

For this we shall require a number of lemmas, the first of which is.

Lemma 7.6. *A point (x, y) on an elliptic curve $E : y^2 = x^3+a^2(x-b)^2$ can be written as $(m/e^2, n/e^3)$ for some $m, n, e \in \mathbb{Z}$ with e coprime to m and n.*

Proof. We take an arbitrary rational point $(p/q, y)$ on E with p, q coprime integers and $y \in \mathbb{Q}$. Then we should have

$$\begin{aligned} y^2 &= \frac{p^3}{q^3} + a^2\left(\frac{p}{q} - b\right)^2, \\ \Rightarrow y^2 &= \frac{p^3}{q^3} + a^2\left(\frac{p^2}{q^2} - 2b\frac{p}{q} + b^2\right), \\ \Rightarrow y^2 &= \frac{p^3}{q^3} + a^2\frac{p^2 - 2bpq + b^2q^2}{q^2}, \\ \Rightarrow y^2 &= \frac{p^3 + a^2(p^2q - 2bpq + bq^3)}{q^3}. \end{aligned}$$

This tells us that q^3 is a square and that the denominator of y^2 is a cube, and q^3 must equal the denominator of y^2, so the two are equal, allowing us to find the desired integers e, m, n. □

Now we can further expand on this observation, similarly to [10, Section 4.1]. Considering $(m/e^2, n/e^3) \in E$ as above, one obtains

$$n^2 = m^3 + a^2m^2e^2 - 2a^2mbe^4 + a^2b^2e^6, \tag{10}$$

and therefore

$$m^3 = (n + ame - abe^3)(n - ame + abe^3). \tag{11}$$

So if $m \neq 0$ then a small calculation shows that our image under α is given as

$$\alpha(m/e^2, n/e^2) = (n + ame - abe^3)\mathbb{Q}^{\times 3}.$$

Note that if $n + ame - abe^3$ and $n - ame + abe^3$ are coprime then (11) shows that both are perfect cubes and therefore $(m/e^2, n/e^3)$ is contained in $\ker \alpha$.

Now assume $n \pm (ame - abe^3)$ do have prime factors in common. Write this as $n+ame-abe^3 = dp$ where p is coprime to $n - ame + abe^3$ and $d = \gcd(n + ame - abe^3, n - ame + abe^3)$. Now we can follow [10, Section 4.1] to prove a stronger condition from which α having finite image is an easy corollary.

Lemma 7.7. *There is a finite set of primes depending only on a and b such that for any point $(m/e^2, n/e^3)$ with $m \neq 0$ on the curve, $d = \gcd(n + ame - abe^3, n - ame + abe^3)$ has prime factors only from this set.*

Proof. By a standard application of the euclidean algorithm we find

$$\begin{aligned} d &= \gcd(n + ame - abe^3, n - (ame - abe^3)), \\ &= \gcd(n + ame - abe^3, -2ame + 2abe^3), \\ &= \gcd(n + ae(m - be^2), -2ae(m - be^2)). \end{aligned}$$

Recall that $\gcd(n, e) = 1$. Since we only wish to show finitely many prime factors exist we can ignore $-2a$ and simply add these factors to our finite set, so we take

$$d' := \gcd(n + ae(m - be^2), m - be^2),$$

and show it has a finite number of prime factors. Note that we can continue to apply the Euclidean Algorithm to arrive at $d' = \gcd(n, m - be^2)$. So we can find $s, t \in \mathbb{Z}$ such that

$$\begin{aligned} d' &= p_1 \dots p_i, \\ n &= p_1 \dots p_i s, \\ m - be^2 &= p_1 \dots p_i t. \end{aligned}$$

So from equation (10) we obtain that

$$\begin{aligned} p_1^2 \dots p_i^2 s^2 &= m^3 + a^2m^2e^2 - a^2bme^4 - a^2be^4p_1 \dots p_i t, \\ \Rightarrow p_1 \dots p_i(p_1 \dots p_i s^2 + a^2be^4t) &= m^3 + a^2me^2(m - be^2), \\ \Rightarrow p_1 \dots p_i(p_1 \dots p_i s^2 + a^2be^4t - a^2me^2t) &= m^3. \end{aligned}$$

In other words $d'|m^3$ hence each of the p_k divides m. Looking again at equation (10) we find that

$$n^2 - m^3 - a^2m^2e^2 + 2a^2bme^4 = a^2b^2e^6.$$

So since any p_k divides both m and n it must divide e or ab. Recalling the definition of e we conclude that the former isn't possible, so the only prime factors are those in the set

$$\{\text{prime}\, p\,:\, p|ab\}\,.$$

Adding back the factors of d we ignored before we can take our finite set to be

$$\{\text{prime}\, p\,:\, p|2ab\}\,.$$

□

Note that this set depends only on the curve and not on which point we picked on the curve. We deduce Lemma 7.5 from it as follows. Suppose $P = (m/e^2, n/e^3) \in E(\mathbb{Q})$ with $m \neq 0$. If a prime p divides $n + ame - abe^3$ and $p \nmid 2ab$, then the previous argument shows $p \nmid n - ame + abe^3$, hence the multiplicity of p in $n + ame - abe^3$ is a multiple of 3. So p does not contribute to $\alpha(P)$. As a consequence, only primes dividing $2ab$ can contribute to $\alpha(\Gamma)$. This shows lemma 7.5.

7.3 Our Second Homomorphism

Now that we are done with α, we shall need to do something similar for our associated curve $\bar{E}$. Note that we cannot in general map into $\mathbb{Q}^\times$, since we get a term $\bar{a} = -27a$ so we cannot just map to $\sqrt{\bar{a}}$ since this is not necessarily a rational number. This however can be fixed by working in $\mathbb{Q}(\sqrt{-3})$, which as we shall see is fairly nicely behaved.

7.3.1 The Eisenstein Integers

We would like to talk about the decomposition in irreducibles of elements of $\mathbb{Z}[\sqrt{-3}]$, as then we can mirror what we did for $\mathbb{Q}$ earlier. However, $\mathbb{Z}[\sqrt{-3}]$ turns out to not have unique factorisation, since

$$4 = 2^2 = (1 - \sqrt{-3})(1 + \sqrt{-3}).$$

However, we can look at a slightly different ring and still proceed as we wanted. We begin by noting that $\mathbb{Q}(\sqrt{-3})$ is the field of fractions of $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathbb{Z}\left[e^{2i\pi/3}\right]$, which are known as the *Eisenstein Integers*. In this section we shall show that all the algebra we used to prove that α has a finite image is also valid to show $\bar{\alpha}$ has a finite image. For this we shall need to go into some of the properties of the Eisenstein Integers.

Lemma 7.8. *The ring* $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ *is a Euclidean Domain.*

Proof. For ease of notation set ξ to be a 3rd root of unity. So that it satisfies the 3rd cyclotomic polynomial

$$\xi^2 - \xi + 1 = 0.$$

Then it follows

$$\xi\bar{\xi} = 1, \quad \text{and} \quad \xi + \bar{\xi} = 1.$$

We take the norm

$$g : a + b\xi \mapsto a^2 + b^2 + ab,$$

so $g(x) = x\bar{x} = |x|^2$. Given nonzero $\beta, \psi \in \mathbb{Z}[\xi]$ we wish to find $\delta, \varrho \in \mathbb{Z}[\xi]$ with $\beta = \delta\gamma + \varrho$ and $g(\varrho) < g(\gamma)$.

We look at a more general field. Namely we take

$$\beta/\gamma \in \mathbb{Q}(\xi) = \mathbb{Q} + \mathbb{Q}\xi.$$

So that

$$\beta/\gamma = r + s\xi, \quad r, s \in \mathbb{Q}.$$

Then we can find $n, m \in \mathbb{Z}$ such that

$$|r - n| \leq 1/2, \quad |s - m| \leq 1/2.$$

And then we set $\delta = n + m\xi$, since

$$\begin{aligned} g(\beta/\gamma - \delta) &= g(r - n + (s - m)\xi), \\ &= (r - n + (s - m)\xi)(r - n + (s - m)\bar{\xi}), \\ &= (r - n)^2 + (s - n)(s - m)\underbrace{(\bar{\xi} + \xi)}_{1} + (s - m)^2\underbrace{\xi\bar{\xi}}_{1}. \end{aligned}$$

So this can be bounded from above by 3/4. Lastly we set $\varrho := \beta - \gamma\delta$ so that

$$g(\varrho) = g(\gamma(\beta/\gamma - \delta)) = |\gamma|^2|\beta/\gamma - \delta|^2 \leq 3/4g(\gamma).$$

Completing the proof. □

Since being a Euclidean domain implies being a unique factorisation domain, we can approach finding the image of $\bar{\alpha}$ the same way as we found the image of α, except now we talk about ideals. Note however that $\mathbb{Z}[\xi]$ contains nontrivial units namely the 6 points on the unit circle. So the argument we will give in this case will be more intricate than the one we gave for $\mathbb{Q}^\times/\mathbb{Q}^{\times 3}$.

Lemma 7.9. *The group of units in the Eisenstein integers is*

$$\mathbb{Z}[\xi]^\times = \left\{\pm e^{ik\pi/3} : k \in \{0, 1, 2\}\right\}.$$

Proof. Take two elements $x+y\xi$ and $z+w\xi$ in $\mathbb{Z}[\xi]$ and suppose $(x+y\xi)^{-1} = z+w\xi$, then we should have that the norm function g has

$$g(x+y\xi)g(z+w\xi) = g((x+y\xi)(z+w)\xi) = 1.$$

We defined the norm as an integer so either both norms are 1 or both are -1. However this norm is the square of the euclidean norm, which is non-negative, hence both must be 1.

This means $x+y\xi$ and $z+w\xi$ must lie on the unit circle, so the only possibilities are the points

$$\{\pm 1, \pm\xi, \pm\xi^2\}.$$

□

This leaves the question what the irreducible elements are.

Lemma 7.10. *The irreducible elements in $\mathbb{Z}[\xi]$ are*

1. *A product of a unit and a prime congruent to* 2 *mod 3,*
2. *the elements of norm n where n is a prime which is either 3 or congruent to* 1 *mod 3.*

Proof. First note that the norm of an irreducible element must be a prime, unless the element itself is a prime times an element on the unit circle. Otherwise we find there are (non-unit) integers x, y

$$g(a) = xy = g(x)g(y),$$

so $g(a) = g(xy)$. So there is some unit ω such that $a = xy\omega$. So we can get away with only looking at the primes in $\mathbb{Z}$.

Fix $p \in \mathbb{Z}$ a prime and suppose p is irreducible. Then

$$\mathbb{Z}[\xi]/p\mathbb{Z}[\xi] = \mathbb{Z}[X]/(p, x^2 - x + 1) = \mathbb{F}_p[X]/(x^2 - x + 1).$$

This p is irreducible, which means the right hand expression is a field. Which shows that 2 is irreducible, but 3 is not since $3 = -1 \cdot \sqrt{-3} \cdot \sqrt{-3}$. For $p > 3$ we have that any zero n of $x^2 - x + 1$ satisfies $n^6 = 1$, $n^3 = -1$ and $n^2 \neq 1$. This means it must be of order 6. Moreover using the factorisation

$$x^6 - 1 = (x^2 - 1)(x^2 + x + 1)(x^2 - x + 1),$$

shows any element of order 6 is such a zero. So $6|(p-1)$. So for $p \equiv 5 \mod 6$ there is no problem and these elements are irreducible. While for $p \equiv 1 \mod 6$ we have that $x^2 - x + 1$ factorises into two irreducible linear factors.

So p is not irreducible, that means $p = b \cdot c$, where we are forced to have $g(b) = g(c) = p$ and b, c are irreducible. Moreover note that $b \neq \omega c$ for a unit ω, since then $b \mod p$ would be nilpotent in $\mathbb{Z}[\xi]/(p)$ which is not possible as by the chinese remainder theorem

$$\mathbb{F}_p[x]/(x^2 - x + 1) \simeq \mathbb{F}_p^2.$$

And following by the irreducibility we have found all such elements. As for any irreducible d we have that $d\mathbb{Z}[\xi]$ is prime, but this contains the ideal $d\mathbb{Z}$ thus $d|p$ in $\mathbb{Z}[\xi]$. □

7.3.2 Finite Image of the Second Map

So take an elliptic curve $E : y^2 = x^3 + a^2(x+b)^2$ over $\mathbb{Q}$, and take $\bar{E}$ to be the corresponding curve obtained using example 3.11. Recalling what $\bar{E}$ was defined as, we can move constants inside the curve to obtain

$$\bar{E} : y^2 = x^3 - 3(9ax + 9a(4a+27)b)^2.$$

So if we set $\bar{a} = 9a$ and $\bar{b} = 9a(4a^2 + 27b)$ then we can write the associated curve as

$$\bar{E} : x^3 - 3(\bar{a}x + \bar{b})^2.$$

so we take some points $y = n/e^3, x = m/e^2$ and compute

$$\begin{aligned}
\left(\frac{n}{e^3}\right)^2 &= \left(\frac{m}{e^2}\right)^3 - 3\left(\bar{a}\frac{m}{e^2} - \bar{b}\right)^2, \\
\Rightarrow n^2 &= m^3 - 3\left(\bar{a}me - \bar{b}e^3\right)^2, \\
\Rightarrow m^3 &= n^2 - (-3)\left(\bar{a}me - \bar{b}e^3\right)^2, \\
\Rightarrow m^3 &= \left(n + e(\bar{a}m - \bar{b}e^2)\sqrt{-3}\right)\left(n - e(\bar{a}m - \bar{b}e^2)\sqrt{-3}\right).
\end{aligned}$$

So we can connect any point on a curve to an ideal

$$I = \left(n + e(\bar{a}m - \bar{b}e^2)\sqrt{-3}\right).$$

Note that this ideal can be factored into prime ideals, so we can proceed similarly to how we proved the image of α could only contain finitely many prime factors.

This leads us to defining $\bar{\alpha}$ as we did α but into cosets $z\mathbb{Q}(\sqrt{-3})^{\times 3}$ rather than $z\mathbb{Q}^{\times 3}$

The proof of $\bar{\alpha}$ being a homomorphism is similar to that of α being a homomorphism, and it can be found in [10, Section 3.2].

Lemma 7.11. *For a given curve having a point of order 3, there is a finite set of irreducible elements such that all prime ideals in a factorisation of*

$$\left(n + e(\bar{a}m - \bar{b}e^2)\sqrt{-3}\right)$$

are contained in this set for all values of n, e, m that can occur.

Proof. Since we have found that $\mathbb{Q}(\sqrt{-3})$ is the field of fractions of a Euclidean domain, we can proceed similarly as when we were working over $\mathbb{Q}$. Namely, we will show that the image can only contain a finite number of irreducible elements.

Since in a Euclidean domain we are able to use the same language as in $\mathbb{Z}$, we can use the exact same reasoning as in lemma 7.7 to conclude the set $\{p : p\,\text{irreducible}, p|2\bar{a}\bar{b}\}$ suffices. □

7.4 Putting Everything Together

So now we have all the ingredients to prove that $[\Gamma : 3\Gamma]$ is finite. The last thing we shall be needing is the following lemma.

Lemma 7.12. *The sequences*

$$\begin{tikzcd}
\tilde{\Gamma} \arrow[r, "\Phi"] & \Gamma \arrow[r, "\alpha"] & \mathbb{Q}^\times/\mathbb{Q}^{\times 3}
\end{tikzcd}$$

$$\begin{tikzcd}
\Gamma \arrow[r, "\Psi"] & \tilde{\Gamma} \arrow[r, "\bar{\alpha}"] & \mathbb{Q}(\sqrt{-3})^\times/\mathbb{Q}(\sqrt{-3})^{\times 3}
\end{tikzcd}$$

are exact.

Proof. We give the proof for $\bar{\alpha}$ and then the proof for α will be similar. And element is in the kernel of $\bar{\alpha}$ precisely if it is $\mathcal{O}$ or $y + a\sqrt{-3}(x-b)$ is a cube. We recall that $\Phi \circ \Psi = [3]$ so all the points in $\operatorname{Im}\Phi$ are automatically in $\ker\bar{\alpha}$.

Take some $P = (x, y) \in \Gamma$ with $(\xi, \eta) = \Psi(P)$ is a point in $\Psi(\Gamma)$. Since the case that $x = 0$ can be settled with a straightforward calculation, we consider the remaining situation and take

$$\delta = -3y/x, \quad \varepsilon = 1 - 3b/x,$$

then it is clear that

$$\bar{\alpha}(\xi, \eta) = (\delta + \varepsilon\sqrt{-3})^3 = \mathbb{Q}(\sqrt{-3})^{\times 3}.$$

Which is indeed in $\ker\bar{\alpha}$.

The proof of the other inclusion can be found in [10, lemma 7]. □

So now we have properly justified everything we need to prove the index being finite.

Theorem 7.13. *Let $\Gamma = E(\mathbb{Q})$ be the group of points on an elliptic curve over $\mathbb{Q}$ which has a point of order 3. Then*

$$[\Gamma : 3\Gamma]$$

is finite.

Proof. As we justified at the start of this chapter and in the preceding lemma we can find some $N \geq 0$ so that

$$[\Gamma : 3\Gamma] = N(\#\operatorname{Im}\alpha)(\#\operatorname{Im}\bar{\alpha})$$

where α is defined in section 7.2 and $\bar{\alpha}$ in 7.3.2. We showed in lemmas 7.5 and 7.11 that these images are finite. □

This moreover concludes the proof of our subcase of Mordell's theorem, since we showed in section 6 that the first 3 conditions of the 3-descent theorem are satisfied for Elliptic Curves, and in the preceding theorem we showed condition 4.

8 Explicit Computation of the Mordell-Weil group

Now that we know the Mordell-Weil group of certain elliptic curves is finitely generated we can expand on the methods we used to find bounds for the rank of such an elliptic curve. Namely, reuse the terminology from the previous chapter, where we found

$$[\Gamma : 3\Gamma] = \frac{(\#\operatorname{Im}\alpha)(\#\operatorname{Im}\bar{\alpha})}{[\ker\Phi : (\ker\Psi \cap \operatorname{Im}\Phi)]}.$$

But on the other hand, we know from the structure theorem that

$$\frac{\Gamma}{3\Gamma} \simeq \frac{\mathbb{Z}^r \oplus \Gamma_{\text{tors}}}{3(\mathbb{Z}^r \oplus \Gamma_{\text{tors}})}$$

now consider each of the parts of the torsion subgroup

$$\frac{\mathbb{Z}/n\mathbb{Z}}{3(\mathbb{Z}/n\mathbb{Z})}$$

which is a nontrivial if and only if 3 divides n, since $\mathbb{Z}/n\mathbb{Z}$ being a subgroup implies 3 must divide n, call the number such subgroup p then

$$\frac{\Gamma}{3\Gamma} \simeq \left(\frac{\mathbb{Z}}{3\mathbb{Z}}\right)^{r+p}$$

so then we know

$$3^{r+p} = \frac{(\#\operatorname{Im}\alpha)(\#\operatorname{Im}\bar{\alpha})}{[\ker\Psi : (\ker\Psi \cap \operatorname{Im}\Phi)]}$$

Note that $\ker\Psi$ corresponds precisely to the points $\mathcal{O}$ and $(0, \pm ab)$. A further analysis shows in our situation

$$r = \log_3 \frac{(\#\operatorname{Im}\alpha)(\#\operatorname{Im}\bar{\alpha})}{3}.$$

Example 8.1. We take the elliptic curve

$$E : y^2 = x^3 + 4(x-2)^2 = x^3 + 4x^2 - 16x + 16$$

over $\mathbb{Q}$. We shall try to find $E(\mathbb{Q})$ explicitly. We will first find $E(\mathbb{Q})_{\text{tors}}$. Recall that the points of order 2 are the roots of this polynomial. From the rational root theorem we know that any rational solution p/q satisfies $p|16$ and $q|1$, so the possible rational roots are $\{\pm1, \pm2, \pm4, \pm16\}$, straightforward computations show none of these suffice, hence no rational point has order 2.

Similarly, we proved in corollary 4.15 that any rational solution must be an integer p dividing $4 \cdot 4 \cdot 16 - 256 = 0$. Using the tools we derived, we find that indeed 0 is indeed a root of

$$\psi_3 = 3x^4 + 16x^3 + 96x^2 - 192x$$

and by the rational root theorem, no other rational roots exist. Hence the points $(0, \pm 2)$ have order 3.

To exclude any other points of finite order we use [8, Theorem 4.4], which states that for any p other than $2, 5, 7$ there are injective homomorphisms

$$\varphi_p : E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p)$$

where $\tilde{E}$ is the curve given by applying the canonical projection $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ on the coefficients of E and considering it as a curve over $\mathbb{F}_p$. By taking $p = 3$ we find

$$\tilde{E} : y^2 = x^3 + x^2 + \bar{2}x + \bar{1}$$

it is then straightforward to confirm

$$\tilde{E}(\mathbb{F}_3) = \{\mathcal{O}, (\bar{0}, \bar{1}), (\bar{0}, \bar{2})\} \simeq \mathbb{Z}/3\mathbb{Z}$$

This gives us an isomorphism $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}$, which excludes the existence of any other points of finite order. Hence we have that $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \mathbb{Z}/3\mathbb{Z}$ for some $r \in \mathbb{Z}_{\geq 0}$.

To now determine r we look at the images in α and $\bar{\alpha}$. First recall from theorem 7.7 that the only possible prime factors of an element in the image of α are the factors of $2 \cdot 4 \cdot 16$, so only 2 is a possible prime factor. So at most $\operatorname{Im}\alpha = \left\{1, 2, 2^2\right\}$, which is indeed the case, since the point $P = (0, 4)$ yields a common divisor d as in theorem 7.7 of 4, then $\alpha(2P) = \alpha(P)^2 = 4^2\mathbb{Q}^{\times 3} = 2\mathbb{Q}^{\times 3}$, so indeed $\operatorname{Im}\alpha = \{\mathbb{Q}^{\times 3}, 2\mathbb{Q}^{\times 3}, 4\mathbb{Q}^{\times 3}\}$.

This means that

$$r = \log_3 \frac{\# \operatorname{Im}\bar{\alpha}}{3}.$$

We find the equation of the associated curve to be

$$\tilde{E} : \eta^2 = \xi^3 - 108(\xi - 70)^2$$

Using the same methods as before we find that $\tilde{E}(\mathbb{Q})_{\text{tors}} = \tilde{E}(\mathbb{Q})[3]$, and we have the points

$$\{\mathcal{O}, (0, 1), (0, -1)\}$$

so $\bar{\alpha}$ becomes

$$(\xi, \eta) \mapsto \eta + 6\sqrt{-3}(\xi - 70)\mathbb{Q}(\sqrt{-3})^{\times 3}.$$

We require that r is an integer, hence we should find at least 3 points. And indeed

$$\bar{\alpha}(0, 1) = (1 + 6\sqrt{-3}(-69)) = 1 - 414\sqrt{-3} = 1 - 2 \cdot 3^2 \cdot 23\sqrt{-3}$$

Now we also need to bound the rank from above. We have found $\# \operatorname{Im}\alpha$ exactly, so we shall be bounding $\# \operatorname{Im}\bar{\alpha}$. Namely, take a point $P = (t/n^2, s/n^3)$ in $\bar{E}(\mathbb{Q})$. Then

$$\frac{s^2}{n^6} = \frac{t^3}{n^6} - 108\left(\frac{t}{n^2} - 70\right)^2$$
$$\Rightarrow s^2 = t^3 - 108n^2(t - 70n^2)^2$$

Thus we get that

$$P \mapsto (s + 6\sqrt{-3}n(t - 70n^2))\mathbb{Q}(\sqrt{-3})^{\times 3}$$

So we get that if $P \mapsto 0$ then $s = 0$. Therefore, such P correspond to a zero of $x^3 - 108(x - 70)^2$.

But this polynomial is irreducible, since we can reduce it modulo $2, 3, 5$ and 7 to get that a zero must be congruent to: 0 mod 3 and 0 mod 2. So a zero is of the form $x = 6z$. Then we wish to find a solution for

$$6^3z^3 - 108(6z - 70)^2 = 0 \Rightarrow z^3 - 2(z - 35)^2 = 0.$$

But this final polynomial is Eisenstein for 2, and hence irreducible. So no $P \mapsto 0\mathbb{Q}(\sqrt{-3})^{\times}$.

Now lets look at which irreducibles can appear in the factorisation of this ideal. Let us look at a factorisation

$$s + 6\sqrt{-3}n(t - 70n^2) = \omega\pi_1^{m_1} \ldots \pi_k^{m_k}$$

with $m_i \in \mathbb{Z}$, π_i irreducible, and ω a unit. Then consider its conjugate

$$s - 6\sqrt{-3}n(t - 70n^2) = \bar{\omega}\bar{\pi}_i^{m_1} \ldots \bar{\pi}_1^{m_1} \ldots \pi_k^{m_k}) = N(\omega)N(\pi_1^{m_1}) \ldots N(\pi_k^{m_k}).$$

So using unique factorisation in $\mathbb{Z}$ we should have that each π_i has norm a prime $\equiv 1 \mod 3$, or equal to 3.

So, let $N(\pi) = p \equiv 1 \mod 3$. Then

$$p|s + 6\sqrt{-3}n(t - 70n^2)$$

so

$$p|s, \quad p|n(t - 60n^2)$$

since we assumes s and n are coprime we can moreover conclude

$$p|t - 60n^2.$$

In section 7.3.2 we found that the irreducibles which can appear in this image are in the set

$$\{q|2ab\}$$

in our case we know a and b and we can even drop the 2, thus we should have

$$p|108 \cdot 70 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$$

where only $7 \equiv 1 \mod 3$. And we can easily see that $7 = N(1/2 \pm 3/2\sqrt{-3})$, since the units are up to -1 (which is a 3rd power) generated by powers of $\xi = (1/2 + 1/2\sqrt{-3})$, so then something in this image is

$$s + 6\sqrt{-3}n(t - 70n^2) = \xi^A \left(\frac{1}{2} + \frac{3}{2}\sqrt{-3}\right)^B \left(\frac{1}{2} - \frac{3}{2}\sqrt{-3}\right)^C$$

where $A, B, C \in \{0, 1, 2\}$, and moreover if since the norm of the product of irreducibles should be 7, we find that C is determined by B. This gives us 9 choices in total, so $\# \operatorname{Im} \bar{\alpha} \leq 9$ and in conclusion the rank is at most 2.

△

Example 8.2. Take the curve

$$E : y^2 = x^3 + (x - 1)^2$$

over $\mathbb{Q}$. As before the existence of a point of order 2 is quickly excluded by using the rational root theorem on

$$x^3 + x^2 - 2x + 1$$

namely, ± 1 are not zeroes.

We easily find points of order 3 using our ψ_3, namely

$$3x^4 + 4x^3 - 12x^2 + 12x$$

has a root 0. Using the same theorem as before, we find that

$$\bar{E}(\mathbb{F}_3) \simeq \mathbb{Z}/6\mathbb{Z}$$

We find that the point

$$(-2, 1) \mapsto (\bar{4}, \bar{1})$$

which has order 6, and using Mazur's theorem [8, Theorem 2.7] and Sagemath it is easy to find $(-2, 1)$ is not a torsion point. This excludes the existence of any other torsion points. Before we found that the point $(-2, 1)$ has infinite order, and this point gets send to

$$(-2, 1) \mapsto (-2 + (1 - 1)) = (-2) = \left\{\mathbb{Q}^{\times 3}, -2\mathbb{Q}^{\times 3}, 4\mathbb{Q}^{\times 3}\right\}$$

The associated curve is given as

$$\eta^2 = \xi^3 + 27(\xi - 23)^2$$

and we can find a point of infinite order $(69, 621)$. This gives 3 points in $\operatorname{Im}\bar{\alpha}$.

So we have the lower bound

$$r \geq \log_3 \frac{3 \cdot 3}{3} = 1.$$

And thus there are infinitely many rational solutions to

$$y^2 = x^3 + (x-1)^2.$$

△

9 Conclusion

To conclude this thesis we shall discuss possible generalisations of this proof. Namely, are there any other classes of elliptic curves for which we can use these methods to prove the quotient group is finite?

As we saw, we only really need to find maps α and $\bar{\alpha}$ which map into Euclidean Domains. So we would only need to have that for an elliptic curve $y^2 = x^3 + a(x-b)^2$ and the associated curve $y^2 = x^3 - 27a(x - \bar{b})$ the rings $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{-3a})$ are the fields of fractions of Euclidean Domains. While as seen in [10] it is possible to prove the quotient group is finite for other curves, these proofs are far from elementary.

For instance it can be found in [1, Chapter 8] , the Gaussian Integers $\mathbb{Z}[i]$ form a Euclidean Domain, as does $\mathbb{Z}[(1+\sqrt{3})/2]$, so we would expect these methods to work just as well for curves

$$E : y^2 = x^3 - a^2(x-b)^2.$$

With maps $\alpha : E(\mathbb{Q}) \to \mathbb{Q}(i)^\times/\mathbb{Q}(i)^{\times 3}$

$$\alpha(P) = \begin{cases} \mathbb{Q}(i)^{\times 3} & \text{if } P = \mathcal{O}, \\ (2ab)^{-1}\mathbb{Q}(i)^{\times 3} & \text{if } P = (0, |y|), \\ 2ab\mathbb{Q}(i)^{\times 3} & \text{if } P = (0, -|y|), \\ (y + ia(x-b))\mathbb{Q}(i)^{\times 3} & \text{else.} \end{cases}$$

And $\bar{\alpha} : \bar{E}(\mathbb{Q}) \to \mathbb{Q}(\sqrt{3})^\times/\mathbb{Q}(\sqrt{3})^{\times 3}$ by

$$\bar{\alpha}(P) = \begin{cases} \mathbb{Q}(\sqrt{3})^{\times 3} & \text{if } P = \mathcal{O}, \\ (2ab)^{-1}\mathbb{Q}(\sqrt{3})^{\times 3} & \text{if } P = (0, |y|), \\ 2ab\mathbb{Q}(\sqrt{3})^{\times 3} & \text{if } P = (0, -|y|), \\ (y + \sqrt{3}a(x-b))\mathbb{Q}(\sqrt{3})^{\times 3} & \text{else} \end{cases}$$

In fact, from [6, Page 293] we find known integers for which $\mathbb{Q}(\sqrt{d})$ has the desired properties, namely

$$d \in \{-1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Or equivalently, such that either $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[(1+\sqrt{d})/2]$ is a Euclidean domain. A quick search shows that the d for which the squarefree part of $-3d$ is also in this set are

$$d \in \{-1, -2, -7, -11, 3, 6, 21, 33\}$$

so likely for any d in that set we can prove using that same methods that the curves

$$y^2 = x^2 + da^2(x-b)^2$$

have finitely generated groups of points. A new feature in these cases would be that one encounters situations where the group of units of the Euclidean domain is not finite.

References

[1] D. S. Dummit and R. M. Foote. *Abstract Algebra.* Wiley, 2003. ISBN 9780471433347.

[2] A. Gathmann. Plane algebraic curves, class notes, 2018.

[3] S. Lang. *Algebra.* Springer, 2002. ISBN 9780387953854.

[4] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978. URL `http://eudml.org/doc/142524`.

[5] L. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proceedings of the Cambridge Philosophy Society*, 21:179–192, 1922.

[6] P. Samuel. About euclidean rings. *Journal of Algebra*, 19(2):282–301, 1971. ISSN 0021-8693. doi: https://doi.org/10.1016/0021-8693(71)90110-4. URL `https://www.sciencedirect.com/science/article/pii/0021869371901104`.

[7] J. Silverman. *The Arithmetic of Elliptic Curves.* Applications of Mathematics. Springer, 1986. ISBN 9780387962030.

[8] J. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer, 01 2015. ISBN 978-3-319-18587-3. doi: 10.1007/978-3-319-18588-0.

[9] W. A. Sutherland. *Introduction to Metric and Topological Spaces.* Oxford University Press, 2009. ISBN 9780199563081.

[10] M. van Beek. On elliptic curves of the form $y^2 = x^3 + a(x-b)^2$. Thesis at University of Groningen, 2010.

[11] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman and Hall, 2003. ISBN 9781420071467.