Bachelor Project
Mordell's Theorem for Elliptic Curves with a point of Order 3

Levi Moes

May 27, 2022

Abstract

Tate-Silverman proves Mordell's theorem for curves with a point of order 2, we show this proof generalises to curves with a point of order 3.

Contents

1 Introduction

2 Cubic Polynomials

We expect the reader to be well familiar with methods of finding roots of quadratic polynomials. In particular we have the famous quadratic formula.

In this section we shall discuss some similar concepts of solving cubic polynomials. In particular this thesis will be interested in monic polynomials $f(x) = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{R}$. Firstly, we will generalise the concept of the term $b^2 - 4ac$ in the quadratic formula to such a cubic. Namely, we are looking for a function that takes the coefficients of a polynomial and outputs 0 if and only if it has a double root.

An obvious way to do this is to define

$$\Delta(f) = \prod_{0<i<j\leq 3} (r_i - r_j)^2$$

where r_k is a root of $f(x)$. It can then be seen that $\Delta(f) = 0$ if and only if $r_i = r_j$ for some $i \neq j$, i.e. f has a double root.

We are able to simplify even more because of the following theorem

Theorem 2.1. *For any cubic $f(x) = ax^3 + bx^2 + cx + d$ the change of variables*

$$x \mapsto t - \frac{b}{3a}$$

yields a polynomial $f(t) = t^3 + pt + q$.

Proof. This is a straightforward computation. □

3 Projective Geometry

4 Elliptic Curves

The general notion of an elliptic curve shall be the centre of focus for this thesis. One might define an Elliptic Curve as follows.

Definition 4.1. *Let $f(x)$ be a 3rd degree monic polynomial having distinct roots. An Elliptic Curve is a curve*

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

If K is a field, we denote for a given Elliptic Curve

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

where $\mathcal{O}$ is the point at infinity.

Since we are talking about an Elliptic *Curve* it is tempting to look at a case where K allows us to draw a continuous line to depict an Elliptic Curve.

Example 4.2. Take $K = \mathbb{R}$, $f(x) = x^3 + px^2 + 1$, where we let $r \in \{-2, \ldots, 3\}$. This yields a sequence of Elliptic Curves E_p, we used python to depict these curves on $[-5, 5] \times [-5, 5]$.

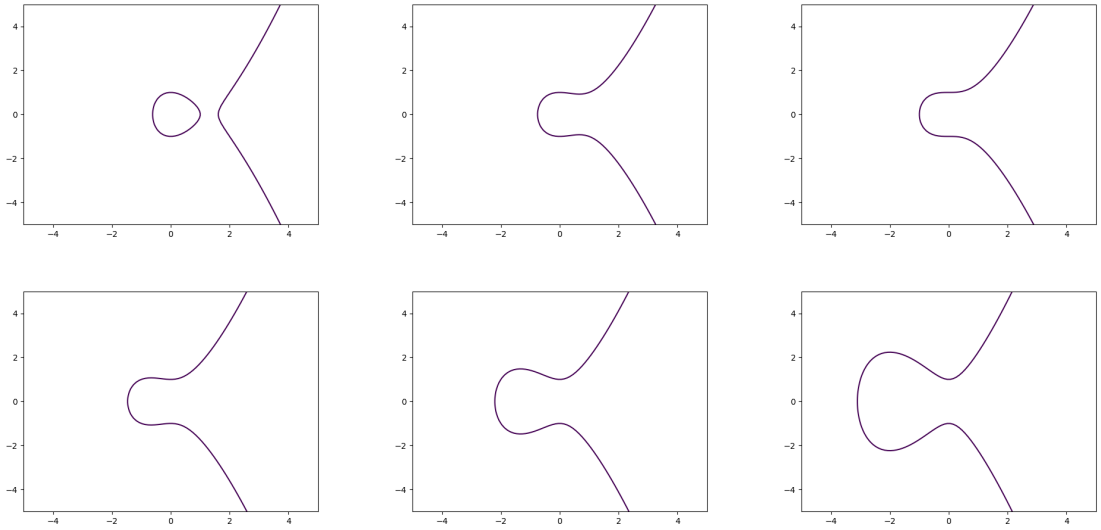

Figure 1: The curves $y^2 = x^3 + px^2 + 1$ for $p \in \{-2, \ldots, 3\}$.

△

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 4.3. Let $K = \mathbb{F}_p$, $p \equiv 3 \mod 4$ a prime and $f(x) = x^3 + nx$ where $\gcd(n, p) = 1$. To find $E(\mathbb{F}_p)$ we wish 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 root of f, then

$$\left(\frac{a^3 + na}{p}\right)\left(\frac{(-a)^3 + n(-a)}{p}\right) = \left(\frac{a}{p}\right)^2\left(\frac{-1}{p}\right)\left(\frac{a^3 + na}{p}\right)^2 = -1.$$

Hence precisely one of $f(a)$ and $f(-a)$ is a square. So for half of all residue classes x we can find two points $(\sqrt{f(\pm x)}, x)$ and $(-\sqrt{f(\pm x)}, x)$ on the curve. Hence including the point at infinity we have

$$\#E(\mathbb{F}_p) = p + 1.$$

For instance when $p = 7$ we have

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

△

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 calculus.

4.1 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 $f(x) = x^3 - 6x + 9$. Say we 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.

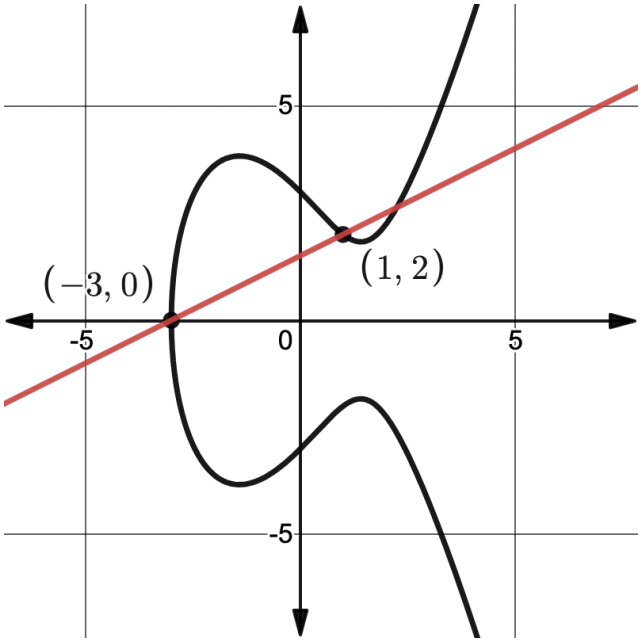

Figure 2: Two points on $y^2 = f(x)$

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 $(x_1, y_1), (x_2, y_2) \in E(\mathbb{Q})$ we can use calculus 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 [5, 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 4.4. Let $E : y^2 = f(x)$ as above over $\mathbb{Q}$. We find the line through $(-3, 0), (1, 2)$ to be

$$y = \frac{x}{2} + \frac{3}{2}.$$

and we solve

$$\left(\frac{x}{2} + \frac{3}{2}\right)^2 = x^3 - 6x + 9$$

which has a solution $9/4$, giving a 3rd point $(9/4, 9/8 + 3/2)$, which we set $(-3, 0) * (1, 2)$. Now similarly we compute $((-3, 0) * (1, 2)) * (-1.414, 3.828) = (-0.727, 3.602)$.

On the other hand, we find $(1, 2) * (-1.414, 3.828) = (0.9879, 2.0092)$ and thus so we find $(-3, 0) * (0.9879, 2.0092) = (2.266, 2.6531)$

4.1.1 The Group law

Luckily a small modification of $*$ does yield an associative operation, namely when we take the 3rd point of intersection, and take its antipode in the y axis.

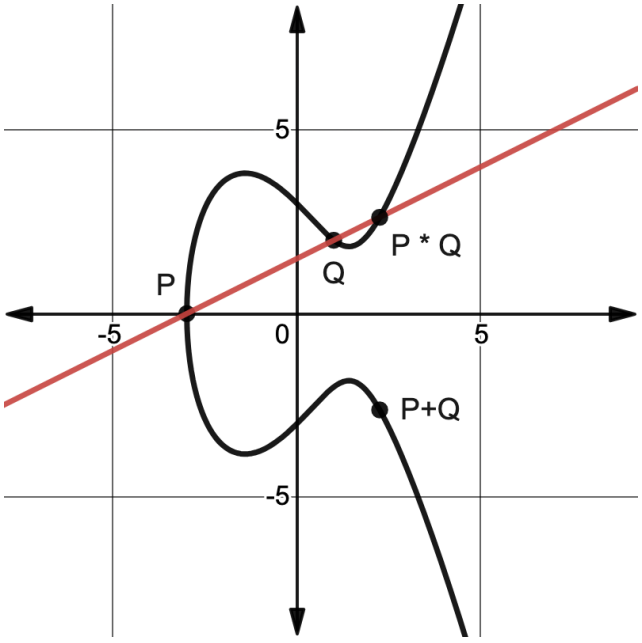

Figure 3: Depiction of the group law

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 [5, section 1.4].

Definition 4.5. *Let $P = (x_1, y_1), Q = (x_2, y_2)$ be points on an Elliptic curve $y^2 = x^3 - ax - b$, 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

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

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 4.6. *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 projection 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 $\tilde{f}(x) = 0$. 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, 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 2) will only intersect at infinity.

The proof of $+_E$ being associative can be found in [8, section 2.4] □

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

Example 4.7. The curve $E : y^2 = x^3 - 6x^2 - 9x + 1$ over $\mathbb{Q}$ is finitely generated. Using SageMath we found

```
sage: E = EllipticCurve([0,-6,0,-9,1]); E
Elliptic Curve defined by y^2 = x^3 - 6*x^2 - 9*x + 1 over Rational Field
sage: E.gens()
[(0 : 1 : 1), (240 : 3671 : 1)]
sage: E.rank()
2
```

Hence using the structure theorem we find there is some Abelian group A such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^2 \times A$$

△

4.2 Elliptic Curves over an Arbitrary Field

In an arbitrary field we can define $+$ analogously to definition 4.5. And again we have

Theorem 4.8. *Let K be a field, and $E : y^2 = f(x)$ an elliptic curve. Then $(E(K), +_E, \mathcal{O})$ is an Abelian Group.*

This yields the following

Example 4.9. Let p be a prime and $E : y^2 = f(x)$ an elliptic curve. For any finite field $\mathbb{F}_{p^n}$ we surely have $E(\mathbb{F}_{p^n})$ is finite. So by the structure theorem [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 4.3 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 $p = 43$ we have $\#E(\mathbb{F}_{43}) = 44 = 2^2 \cdot 11$, hence 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 $(42, 27)$ is a point of order 4, so

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

Numerically, it appears that when n is a square these groups are always cyclic. △

There is a well-known class of primes which have some nice behaviour over these curves

Example 4.10. Let $E : y^2 = f(x)$ over $\mathbb{F}_p$ be as in example 4.9. There is the famous class of Mersenne Primes, which are primes of the form $2^p - 1$, where p is a prime. An efficient algorithm exists to determine the primality of these numbers [1] △

4.3 Isogenies

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

Definition 4.11. *Let E_1, E_2 be Elliptic Curves over a field K. An isogeny $\varphi : E_1(K) \to E_2(K)$ is a rational function that is also a group homomorphism.*

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 [5, Theorem III.4.8] the following theorem.

Theorem 4.12. *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 4.13. 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

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

△

The following example is the subject of [7, chapter 2.2]

Example 4.14. Let $A, B \in \mathbb{Q}$ and $\bar{A} = -27A, \bar{B} = 4A + 27B$

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

be Elliptic Curves, we define the map

$$\Phi_{X,Y} : (x, y) \mapsto (\xi, \eta),$$

where

$$\xi = \frac{9}{x^2}\left(2y^2 + 2XY^2 - x^3 - \frac{2}{3}Xx^2\right),$$
$$\eta = \frac{27y}{x^3}\left(-4XYx + 8XY^2 - x^3\right).$$

If we define $\Phi_{X,Y} : \mathcal{O} \mapsto \mathcal{O}$ then by theorem 4.12 it follows that $\Phi_{X,Y}$ is an isogeny. If we apply the map $\Phi_{\bar{A},\bar{B}} \circ \Phi_{A,B}$ we obtain the curve

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

The change of coordinates

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

gives

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

which is the equation of E multiplied by 3^{18}. In conclusion the following diagram commutes

$$E(\mathbb{Q}) \xrightarrow{\Phi_{A,B}} \bar{E}(\mathbb{Q}) \xrightarrow{\Phi_{\bar{A},\bar{B}}} C(\mathbb{Q}), \qquad E(\mathbb{Q}) \xrightarrow{[3]} E(\mathbb{Q})$$

△

5 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 5.1. *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 5.2. *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 $|xy^{-1}| = \text{lcm}(|x|, |y^{-1}|) = \text{lcm}(|x|, |y|) < \infty$. □

Definition 5.3. *Let $(A, e, *)$ be an Abelian group, define*

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

Theorem 5.4. *$A[n]$ 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 5.5. If K is finite then $E(K) = E(K)_{\text{tors}}$ follows by Lagrange's Theorem. △

Example 5.6. 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.

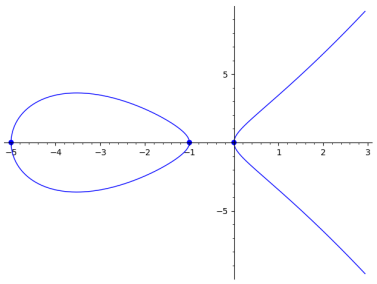

Figure 4: Points of order 2 on $y^2 = x^3 + 6x^2 + 5x$ over $\mathbb{Q}$

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. △

5.1 The Nagell-Lutz Theorem

Theorem 5.7. *Let $E : y^2 = f(x)$ be an Elliptic Curve over $\mathbb{Q}$. 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 $y|D$, the discriminant of f.*

5.2 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 is precisely a root of the corresponding cubic.

Example 5.8. 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

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

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 $y^2 = x(x^2 + 5x + 4)$ △

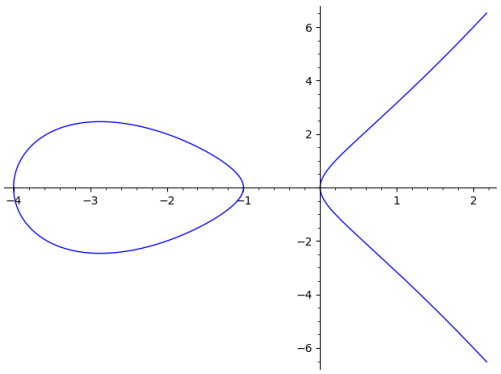

Figure 5: The curve $y^2 = x(x^2 + 5x + 4)$

5.3 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 $\psi_3 = 2f(x)f''(x) - f'(x)^2$ [5, section 2.1]. So points of order 3 are roots of this polynomial.

Theorem 5.9. *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 [5, Exercise 2.2].

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

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

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

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

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

This similar to a result in the book by Tate and Silverman [5, 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 5.11. *ψ_3 has precisely 2 real roots.*

This is again an exercise in Tate-Silverman [5, 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 [6, 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 5.12. *Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\mathbb{Q}$. If $E(\mathbb{Q})$ contains a point of order 3 then E is isogenous to either $E_1 : y^2 = x^3 + A(x - B)^2$ or $E_2 : y^2 = x^3 + D$ for some integers A, B, D. And moreover $A = a^2$ is a square.*

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

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

from 5.9 we know

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

so we get the tangent line

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

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 $E : y^2 = x^3 + d$ and otherwise we can find constants A, B such that our cure has form $E : y^2 = x^3 + A(x - B)^2$. □

5.3.1 Examples of Curves with a Point of Order 3

Example 5.13. When $a = 0$ and $c = 0$ we get an elliptic curve $y^2 = x^3 + bx$ 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 is a singular curve and hence not elliptic. △

Example 5.14. 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 $E(\mathbb{Q})[3] \simeq \mathbb{Z}/3\mathbb{Z}$.

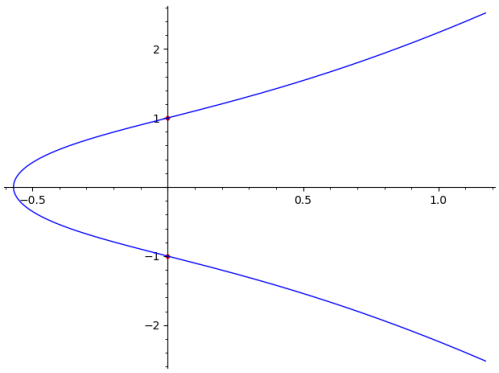

Figure 6: Points of order 3 on $y^2 = x^3 + x^2 + 2x + 1$

△

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

Corollary 5.15. *Suppose the coefficients of 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 [2, Section 9.4] any rational root of ψ_3 has the form $x = p/q$ where $\gcd(p, q) = 1$, $p|4ac - b^2$ and $q|3$, moreover we know from theorem 5.7 that $p/q \in \mathbb{Z}$, so $q|p$. If $q = 3$ then $\gcd(p, q) = 3$ which is not in lowest terms, so we have $q = 1$. For any rational solution x we have $x|4ac - b^2$. □

Example 5.16. For the Elliptic Curve $y^2 = x^3 + 3x^2 + 3x + 2$ we have any rational solution x 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 5.17. The Elliptic Curve $y^2 = x^3 - 9x + 9$ has $b^2 - 4ac = -81$, which has divisors $\pm 1, \pm 3, \pm 9, \pm 81$. So by trial and error on

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

we find that $\psi(3) = 0$. Hence $(3, \pm 3)$ are points of order 3. △

Example 5.18. 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 (0, -1) of order 2, while 0 is a root of ψ_3 so $(\pm 1, 0)$ 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. △

6 Mordell's Theorem

Theorem 6.1. *For any Elliptic Curve $E : y^2 = f(x)$ the group $E(\mathbb{Q})$ is finitely generated.*

Which requires results from cohomology which are beyond the scope of this thesis [4, Section VIII] . We shall prove the weaker version

Theorem 6.2. *Let $E : y^2 = f(x)$ be an Elliptic Curve. If $E(\mathbb{Q})$ contains a point of order 3, then $E(\mathbb{Q})$ is finitely generated.*

6.1 Explicit Computation of Mordell-Weil Groups

If we suppose 6.2 holds, then we can use the structure theorem for finitely generated groups [3, Theorem 8.1] the conclude that an elliptic curve E over $\mathbb{Q}$ has

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})$$

for some integers r, d_i. We can moreover conclude this is the same as

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

We have gone into some examples of computing subgroups of $E(\mathbb{Q})_{\text{tors}}$ in section 5, now we shall give an example of how to compute r for a given curve.

Example 6.3. Let $E : y^2 = x^3 + (x-1)^2$ be an elliptic curve over $\mathbb{Q}$. Recall from example 4.13 that we can find maps Φ, Ψ such that for some elliptic curve $\bar{E}$ the diagram

$$E(\mathbb{Q}) \xrightarrow{\Phi} \bar{E}(\mathbb{Q}) \xrightarrow{\Psi} E(\mathbb{Q}), \qquad [3] : E(\mathbb{Q}) \to E(\mathbb{Q})$$

commutes. As in [7, Section 3.1] we can moreover define a map $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 3}$ by mapping $P = (x, y)$ as

$$\alpha(P) = \begin{cases} \mathbb{Q}^{\times 3} & \text{if } P = \mathbb{Q}, \\ (y + (x-1))\mathbb{Q}^{\times 3} & \text{else.} \end{cases}$$

later on we will verify that this is a homomorphism and $\ker \alpha = \Psi\bar{E}(\mathbb{Q})$, for now we refer to [7, Theorem 5].

Knowing this, we find via the first isomorphism theorem

$$E(\mathbb{Q})/\Psi\bar{E}(\mathbb{Q}) \simeq \alpha(E(\mathbb{Q}))$$

and that $(x, y) \mapsto (x + y - 1) \mod \mathbb{Q}^{\times 3}$.

Now we take an arbitrary rational point p/q on E, then we should have

$$\begin{aligned} \frac{p^2}{q^2} = \frac{p^3}{q^3} + \frac{(p-q)^2}{q^2} &\iff p^3 + q^3 = 2pq^2 \\ &\iff \frac{p^3 + pp^2q - 2pq^2 + q^3}{q^3} = \frac{p^2}{q^2} \end{aligned}$$

These being reduces fractions means that necessarily q^3 is a square, thus $y = m/e^2$ for some $m, e \in \mathbb{Z}$. Giving us

$$m^2 = \frac{p^6}{q^2} + \frac{2p^5}{q} - 3p^4 - 2p^3q + 6p^2q^2 - 4pq^3 + q^4$$

So under α we have

$$\begin{aligned}(p/e^2, m/e^3) &\mapsto p/e^2 + m/e^3 - 1 \mod \mathbb{Q}^{\times 3} \\ &\equiv (pe + m - e^3)/e^3 \mod \mathbb{Q}^{\times 3} \\ &\equiv m + pe - e^3 \mod \mathbb{Q}^{\times 3}\end{aligned}$$

so we can factor

$$\begin{aligned}(-x^2, y^2) &\mapsto -x^2 + y^2 - 1 \mod \mathbb{Q}^{\times 3} \\ &\equiv (y + x - 1)(y - (x - 1)) \mod \mathbb{Q}^{\times 3} \\ &\equiv (m + te - e^3)(m - te + e^3) \mod \mathbb{Q}^{\times 3}\end{aligned}$$

△

7 The 3-Descent Theorem

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

Theorem 7.1. *Let A be an Abelian group. Suppose there exists a function $h : A \to \mathbb{R}$ such that for all $P \in A$*

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 [4, theorem 3.1]. After we have this tool, proving theorem 6.2 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

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

which is assumed to be finite. □

8 Finding a Height Function

The remainder of this project will be about finding a height function suitable for $E(\mathbb{Q})$, and then proving each of the properties in theorem 7.1.

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

Example 8.1. 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 8.2. *(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 7.1.

8.1 Bound on Height

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

Lemma 8.3. *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 [5, 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 4.5 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. □

8.2 Height of 3P

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

Lemma 8.4. *There is a constant C_1 such that*

$$h(3P) \geq 9h(P) - C_2$$

It can be shown [7, Appendix B] that this is just a specific case of a lemma in Silverman's Book [5, Lemma 3.6]. Proving either this lemma or the equivalence is outside the scope of this thesis.

8.3 Points of Bounded Height

Now for the 3rd property.

Lemma 8.5. *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.

9 The Quotient Group is Finite

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

$$\Gamma := C(\mathbb{Q})$$

This section shall be dedicated to proving the final part of theorem 7.1, that is

Theorem 9.1. *The index* $[\Gamma : 3\Gamma]$ *is finite.*

The sketch of our proof will be to define two classes of curves $E : y^2 = g(\xi)$ and $\bar{E} : y^2 = h(x)$ and define two isogenies $\phi : E(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$ along with $\bar{\phi} : \bar{E}(\mathbb{Q}) \to E(\mathbb{Q})$ such that $\phi \circ \varphi = P \mapsto 3P$. This gives us an exact sequence

$$0 \longrightarrow \bar{\phi}\bar{E}/3E \longrightarrow E/3E \longrightarrow E/\bar{\phi}\bar{E} \longrightarrow 0$$

We find an isomorphism $f : \bar{\phi}\bar{E}/3E \to \mathbb{Q}(\sqrt{-3})^\times/(\mathbb{Q}(\sqrt{-3})^\times)^3 =: \mathbb{Q}(\sqrt{-3})_3$ and a homomorphism $g : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 =: \mathbb{Q}_3$ with kernel $\bar{\phi}\bar{E}(\mathbb{Q})$ and show their images are finite. Which means $E/3E$ must be finite as well. Lastly we show that it is sufficient to show any such $3E(\mathbb{Q})$ has finite index to show theorem 9.1, where we recall from theorem 5.12 that there are only two possible forms our equation can have.

9.1 The Rationals Modulo the 3rd Powers

A group which we will need to discuss is $\mathbb{Q}_3 := \mathbb{Q}^\times/\mathbb{Q}^{\times 3}$. We can write a typical element of $x \in \mathbb{Q}^\times$ as

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

where p_i is the $i$the prime, $d_i \in \mathbb{Z}$ and only finitely many d_i are nonzero. Setting e_i as a basis for the infinite product of $\mathbb{Z}/3\mathbb{Z}$ with itself. Then the following sequence is exact

$$p_i^{d_i} \xmapsto{f} e_i d_i$$

$$0 \longrightarrow \mathbb{Q}^{\times 3} \xrightarrow{\iota} \mathbb{Q}^\times \xrightarrow{f} \bigoplus_{\mathbb{N}} (\mathbb{Z}/3\mathbb{Z}) \longrightarrow 0.$$

So from the first isomorphism theorem it follows

$$\mathbb{Q}_3 = \mathbb{Q}^\times/\mathbb{Q}^{\times 3} \simeq \bigoplus_{\mathbb{N}} \mathbb{Z}/3\mathbb{Z}.$$

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.

9.2 Finite Image

We define an elliptic curve

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

Define a map

$$E(\mathbb{Q}) \xmapsto{\quad\alpha\quad} \mathbb{Q}_3$$

$$(x, y) \xrightarrow{\alpha} (y + a(x - b))\mathbb{Q}^{\times 3}.$$

Note that $\ker \alpha = E(\mathbb{Q})[3]$. From the same computation as in example 6.3 we can write a rational point as $(m/e^2, n/e^3)$ and similarly to [7, Section 4.1]

$$\begin{aligned} n^2 &= m^3 + a^2m^2e^2 - 2a^2be^4 + a^2b^2e^6 \\ \therefore m^3 &= (n + ame - abe^3)(n - ame + abe^3). \end{aligned}$$

so 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 this point must be a perfect cube and it is contained in $\ker \alpha$.

Now assume these images 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 [7, Section 4.1].

Theorem 9.2. *There is a finite set of primes depending only on a and b such that for any point on the curve the constant d 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 □

References

[1] J. Bruce. A really trivial proof of the lucas-lehmer test. *The American Mathematical Monthly*, 1993. doi: 10.2307/2324959.

[2] D. S. Dummit. *Abstract Algebra*. Wiley, 2003. ISBN 9780471433347.

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

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

[5] 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.

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

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

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