ELLIPTIC CURVES AND MORDELL'S THEOREM

HELENA PEREZ-STARK

Abstract. In this paper, we will define the group law for the group of rational points on elliptic curves. Then, we will prove Mordell's theorem, which states that the group of rational points is finitely generated.

Contents

Introduction

Elliptic curves form a substantial field of present-day research, particularly in the field of number theory. Elliptic curves are also useful in the field of cryptography, and were used in Andrew Wiles' proof of Fermat's Last Theorem. First proved in 1922, Mordell's theorem for the group of rational points on elliptic curves is a foundational result in Diophantine geometry. Initially conjectured by Poincare in 1901, Mordell's theorem finds that one can obtain all of the rational points on an elliptic curve from a finite number of such points, just by drawing tangents and chords. This paper adapts the proof from Chapter 3 of [2], which uses only basic group theoretic facts to prove (much of) the theorem. In Section 2, we explore Fermat's method of infinite descent and a notion of *height* to show how Mordell's theorem can be proved. Section 3 establishes that the group of rational points satisfies the conditions for the descent theorem to work.

1. The Group of Rational Points

Definition 1.1. A **cubic curve** over a field K is a curve satisfying the equation

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

Definition 1.2. A cubic curve of the form

$$y^2 = x^3 + ax^2 + bx + c \quad \text{or} \quad y^2 = x^3 + bx + c$$

is said to be in **Weierstrass normal form.**[1]

[1]This applies for fields of characteristic not equal to 2 or 3.

Proposition 1.3. *Any cubic with a rational point $\mathcal{O}$ is isomorphic to a projective cubic curve in $\mathbb{P}_k^2$ in Weierstrass normal form where $\mathcal{O}$ is mapped to* $(0:1:0)$.

As a result of this proposition, we will greatly simplify the machinery of the addition operation by looking only at projective cubic curves in Weierstrass normal form. In addition, we will consider cubic curves as the zero set of the multivariate polynomial $F(x, y)$, where

$$F(x, y) = y^2 - f(x) \quad \text{for} \quad f(x) = x^3 + ax^2 + bx + c.$$

Definition 1.4. A cubic curve in Weierstrass normal form is **nonsingular** if its discriminant

$$D = -4ac^3 + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0.$$

Definition 1.5. An **elliptic curve** E over a field K is a nonsingular, projective cubic curve which satisfies the equation

$$F(x, y) = 0 = y^2 - x^3 - ax^2 - bx - c \text{ for } a,\ b,\ c \in K.$$

and is equipped with a rational base point $\mathcal{O}$ at $(0:1:0)$.

Notation 1.6. We denote $E(K)$ to be the set of (x, y) points where x and y are both in K.

In order to define the addition operation and prove that $E(\mathbb{Q})$ has a group structure, we must first note a few important facts.

Proposition 1.7. *Bezout's Theorem - Suppose X and Y are two projective plane curves over a field K such that X and Y have no common component. Then the number of intersection points - counting multiplicities - of X and Y with coordinates in an algebraically closed field $\overline{K}$ containing K is equal to the product of the degrees of X and Y.*

Remark 1.8. As a result, two cubic curves in the projective plane $\mathbb{P}^2$ will intersect each other at exactly nine points. Then, we state the following theorem, which will allow us to prove the associativity of the group structure:

Proposition 1.9. *Cubic Cayley-Bacharach Theorem - Let C_1 and C_2 be cubic curves in $\mathbb{P}^2$ without common components and assume that C_1 is smooth. Suppose that C_3 is another cubic curve that contains eight of the intersection points of $C_1 \cap C_2$ counting multiplicities. Then C_3 goes through the ninth point of $C_1 \cap C_2$.*

Lemma 1.10. *The point* $(0:1:0)$ *is the only point at which E intersects the line at infinity.*

Proof. This fact follows directly from Proposition 1.7. □

Remark 1.11. Since the coordinates $(0:1:0)$ define all of the lines in the y-direction, $\mathcal{O}$ is the point where are vertical lines on the plane meet.

Remark 1.12. The tangent line at $\mathcal{O}$ well-defined, and is the line at infinity.

First, it is important to note that if a straight line intersects an elliptic curve at two rational points, then the third intersection will also be rational. This is so because any straight line going through two rational points will be a rational line (i.e. it will have rational coefficients).

Knowing this fact, we have a means of obtaining a third rational point from two given ones. Namely, if P and Q are rational points, we can define $P \star Q$ to be

the third intersection point obtained when we draw a line through P and Q. In the case that $Q = P$, then we draw the tangent line at P, which intersects E with multiplicity two, and take the third intersection to be $P \star P$. As it turns out, we can define a valid group structure by taking $P \star Q$ and reflecting it over the x-axis. Since all cubic curves in Weierstrass normal form are symmetrical about the x-axis, the point

$$P + Q = (x, -y), \text{ where } P \star Q = (x, y)$$

is rational as well. Notice that by the previous remarks, the mapping from $P \star Q$ to $P + Q$ is equivalent to drawing a vertical line from $P + Q$ to $\mathcal{O}$ and taking the third intersection point.

$$P + Q = (P \star Q) \star \mathcal{O}.$$

Finally, notice that both operations $+$ and $\star$ must be commutative, since the line through P and Q has the same equation as the line through Q and P.

Proposition 1.13. *The set $E(\mathbb{Q})$ equipped with the binary operation $+$ and the identity element $\mathcal{O}$ forms a group. Therefore, the following are true:*

(a) For all $P \in E(\mathbb{Q})$, $P + \mathcal{O} = \mathcal{O} + P = P$;
(b) For all $P \in E(\mathbb{Q})$, there exists $-P \in E(\mathbb{Q})$ such that $P + (-P) = \mathcal{O}$;
(c) For all P, Q, R, $\in E(\mathbb{Q})$, $(P + Q) + R = P + (Q + R)$.

Proof. Let $P = (x, y) \in E(\mathbb{Q})$. The proof (a) is seen by simply drawing a vertical line through a point and looking at the intersections.

In particular, $(P \star \mathcal{O}) = (x, -y)$, so $(x, y) \star (x, -y) = \mathcal{O}$. So, for any P, we have $-P = (x, -y)$.

The proof of (c) follows from Proposition 1.9. For details, see [2]. □

We conclude the section by providing some explicit formulas for the group law.

Let E be of the form

$$y^2 = x^3 + ax^2 + bx + c, \quad \text{for } a,\, b,\, c \in \mathbb{Q}.$$

Suppose P and Q are two distinct rational points on E which are not additive inverses. Set

$$P = (x_1, y_1),\ Q = (x_2, y_2),\ P \star Q = (x_3, y_3),\ P + Q = (x_3, -y_3).$$

Let $y = \lambda x + \nu$ be the line through P and Q, where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Substituting $\lambda x + \nu$ for y into the equation of the curve and putting all the terms to the right, we obtain the equation

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2). \tag{1.14}$$

Notice that the roots of this cubic are the intersection points x_1, x_2, and x_3. Recall that the x^2 coefficients of both sides of the equation

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

must be equal for the equality to hold. Therefore, we know that

$$a - \lambda^2 = -x_1 - x_2 - x_3$$
$$\text{if and only if} \quad x_3 = \lambda^2 - a - x_1 - x_2 \tag{1.15}$$

and $y_3 = \lambda x + \nu$. Now let $P_0 = (x_0, y_0)$. To find $P_0 + P_0 = 2P_0$ we must use the slope of the tangent line at P_0 given by relation $y^2 = f(x)$. Differentiating, we get

$$\lambda = \left.\frac{dy}{dx}\right|_{P_0} = \frac{f'(x_0)}{2y_0} \tag{1.16}$$

If we plug this value for λ into (1.15) and put everything under a common denominator, we obtain a duplication function for the $x-$value of $2P_0$:

$$x(2P_0) = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}. \tag{1.17}$$

Corollary 1.18. *A point $P = (x, y)$ in $E(\mathbb{Q})$ is a point of order two if and only if $y = 0$.*

Corollary 1.19. *Three points P_1, P_2, and P_3 are colinear if and only if they satisfy*

$$P_1 + P_2 + P_3 = \mathcal{O}$$

2. Fermat's Method of Infinite Descent

In this section we begin the proof of Mordell's Theorem. From now on, let our field K be $\mathbb{Q}$.

Theorem 2.1. *Mordell's Theorem - The group $E(\mathbb{Q})$ is finitely generated.*

To prove Mordell's theorem, we use Fermat's method of infinite descent.

Definition 2.2. We define the height H of a rational number $\frac{m}{n} \in \mathbb{Q}$ to be $H(\frac{m}{n}) = \max\{|m|, |n|\}$. For a rational point $P = (x, y) \in E(\mathbb{Q})$, we let $H(P) = H(x)$. For the base point $\mathcal{O}$ on the curve, we will define $H(\mathcal{O}) = 1$.

We also use a logarithmic definition of height, notated by

$$h(P) = \log H(P).$$

Theorem 2.3. *Infinite Descent Theorem - Let Γ be a abelian group. Suppose there is a function $h : \Gamma \to [0, \infty)$ with the following properties:*

(a) For every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.

(b) For every $P_0 \in \Gamma$ there is a constant κ_0 such that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in \Gamma.$$

(c) There is a constant κ such that

$$h(2P) \geq 4h(P) - \kappa \text{ for all } P \in \Gamma.$$

(d) The subgroup $2\Gamma = \{P \in \Gamma : P = 2P_0 \text{ for } P_0 \in \Gamma\}$ has finite index in Γ.

Then Γ is finitely generated.

Proof. Since 2Γ has finite index in Γ, we know that it must also have finitely many cosets, say n many. Then, we denote coset representatives $Q_1, Q_2, \ldots, Q_n$.

Let $P \in \Gamma$. Since P must be in some coset of 2Γ, we can find a representative Q_{i_1} among our representatives $Q_1, \ldots, Q_n$ such that

$$P - Q_{i_1} = 2P_1 \text{ where } P_1 \in \Gamma. \tag{2.4}$$

Then, by iterating this procedure as many times as we like - say, m times - we have found a method of generating a sequence of points:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m. \end{aligned}$$

Notice that for each P_j in our sequence we can write $P_j = Q_{i_{j+1}} + 2P_{j+1}$. Making this substitution into (2.4) for every P_j, we obtain a formula for P in terms of the coset representatives $Q_1, \ldots, Q_n$ and the terminating point P_m:

$$\begin{aligned} P &= Q_{i_1} + 2(Q_{i_2} + 2(Q_{i_3} + \cdots + 2(Q_{i_m} + 2P_m))) \\ \implies P &= Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} \cdots + 2^{m-1}Q_{m-1} + 2^m P_m. \end{aligned} \tag{2.5}$$

By analyzing the relationship between $h(P_{j-1})$ and $h(P_j)$, we will show that by choosing m large enough, we can get the value of $h(P_m)$ below a certain bounded height. Since there will be finitely many points with height less than this bound, there will be finitely many options for the terminating point P_m. Then, the set of possible P_m's along with the coset representatives $Q_1, \ldots, Q_n$ will generate Γ.

Replacing the P_0 in (b) with $-Q_i$, for $1 \leq i \leq n$, we find that there exists κ_i such that

$$h(P - Q_i) \leq 2h(P) + \kappa_i \text{ for all } P \in \Gamma. \tag{2.6}$$

Evaluating (2.5) for each Q_i, we define $\kappa' = \max\{\kappa_1, \ldots, \kappa_n\}$ so that

$$h(P - Q_i) \leq 2h(P) + \kappa' \text{ for all } P \in \Gamma \text{ and any choice of } -Q_i. \tag{2.7}$$

Now, using the inequality in condition (c) as well as (2.6) we see that there exists κ such that for all P_j, we have the relation

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

Isolating P_j, and doing some algebra, we obtain:

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa + \kappa}{4} \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}[h(P_{j-1}) - (\kappa' + \kappa)] \end{aligned}$$

Notice that if $h(P_{j-1}) > \kappa' + \kappa$, then the quantity $\frac{1}{4}[h(P_{j-1}) - (\kappa' + \kappa)] > 0$. As a result, $h(P_j) < \frac{3}{4}h(P_{j-1})$. Since $\frac{3}{4}$ is less than 1, we know $h(P_j)$ goes to zero as the index j increases. In particular, there exists some index m for which $h(P_m) < \kappa' + \kappa$. Then, as in (2.5), we can write

$$P = Q_{i_1} + 2Q_{i_2} + \cdots + 2^m R$$

where $R = P_m$ is some number in Γ satisfying $h(R) < \kappa' + \kappa$. Summing like terms,

$$P = \alpha_1 Q_1 + \alpha_2 Q_2 + \cdots + \alpha_n Q_n + 2^m R$$

for some $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$. By condition (a) there are only finitely many possibilities for R. Therefore, the finite set

$$\{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) < \kappa' + \kappa\}$$

generates Γ.

□

3. Mordell's Theorem

To actually prove Mordell's Theorem, we have to prove that the group of rational points and the logarithmic height function h satisfy conditions (a) through (d) of Theorem 2.3. If we can show these conditions hold, then we are done. This is accomplished through a series of lemmas of roughly increasing difficulty. The proof of (a) and (b) are quite easy, while the proof of (c) is harder. Proving (d) in full generality for the group $E(\mathbb{Q})$ is beyond the scope of this paper, but we can examine a special case in which we assume the existence of a point of order two.

Lemma 3.1. *For every real number $M > 0$, the set of points in $E(\mathbb{Q})$ with height less than M is finite.*

Proof. The proof follows from the fact that there are finitely many natural numbers less than any positive real number, so therefore only finitely many fractions can be written. □

To prove the next three conditions, we must first look at a few smaller details.

Remark 3.2. If $E(\mathbb{Q})$ is of the form $y^2 + x^3 + ax^2 + bx + c$, where a, b, $c \in \mathbb{Q}$, we can take a, b, and c to be integers through a change in coordinates.

Lemma 3.3. *Let $P = (x, y)$ be a rational point on E. Then, the following hold:*

(a) We can write x and y in the forms

$$x = \frac{m}{e^2} \text{ and } y = \frac{n}{e^3}$$

where m, n and e are integers, e is positive, and $\gcd(m, e) = \gcd(n, e) = 1$. Furthermore, $|m| \leq H(P)$ and $e \leq H(P)^{\frac{1}{2}}$.

(b) There exists a constant $K > 0$ depending on our coefficients a, b, and E such that

$$|n| \leq KH(P)^{\frac{3}{2}} \text{ for all } P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q}).$$

Lemma 3.4. *Let P_0 be a fixed rational point of E. There is a constant κ_0 depending on P_0 and the elliptic curve constants a, b, and E such that*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in E(\mathbb{Q}).$$

Proof. We will prove the lemma for all $P \notin \{P_0, -P_0, \mathcal{O}\}$, since these are either trivial or require the duplication formula. This is excusable since we can check the difference $h(P + P_0) - 2h(P)$ individually for any finite collection of points, and then adjust the value of κ_0 accordingly.

Let $P = (x, y)$, $P_0 = (x_0, y_0)$, and $P + P_0 = (\xi, \eta)$. From (1.15), we have

$$\xi = \lambda^2 - a - x - x_0 \text{ for } \lambda = \frac{y - y_0}{x - x_0}.$$

Isolating ξ on the left, putting everything under a common denominator, and substituting $y^2 - x^3$ for $ax^2 + bx + c$, we are able to find an expression of the form

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

with A, B, C, D, E, F, G being integers expressed in terms of a, b, c and (x_0, y_0).

Using Lemma 3.3, we substitute $\frac{m}{e^2}$ for x and $\frac{n}{e^3}$ for y and clear fractions:

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

Then, since $n, e, m \in \mathbb{Z}$, we have succesfully put ξ in the form of an integer divided by an integer. Therefore we can evaluate the height:

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

Notice that this is not an equality, since the fraction may not be in lowest terms and cancellation would make the height of ξ smaller.

Recall Lemma 3.3, which states that

$$e \leq H(P)^{\frac{1}{2}},\ n \leq KH(P), \quad \text{and } m \leq H(P)$$

where K depends only on a b, and E. Using these inequalities as well as the triangle inequality, we have

$$\begin{aligned} H(\xi) &\leq \max\{|Ane| + |Bm^2| + |Cme^2| + |De^4|,\ |Em^2| + |Fme^2| + |Ge^4|\} \\ &\leq \max\{|AK| + |B| + |C| + |D|,\ |E| + |F| + |G|\}H(P)^2. \end{aligned}$$

Taking the logarithms of both sides, we see

$$h(P + P_0) = h(\xi) \leq 2h(P) + \kappa_0$$

where

$$\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}.$$

Since $A, \ldots, G$ and K depend only on a, b, c and (x_0, y_0), this choice of κ_0 works for all but finitely many P, so we are done. □

Lemma 3.5. *There exists a constant κ, depending on the coefficients a, b, and E such that*

$$h(2P) \geq 4h(P) - \kappa \text{ for all } P \in E(\mathbb{Q}).$$

Proof. We will prove the statement for all points except those which satisfy $2P = \mathcal{O}$. Luckily this set of points is finite, so we can simply take κ to be larger than $4h(P)$ in these cases. Let us write $P = (x, y)$ and $2P = (\xi, \eta)$. To examine the heights of $2P$ and P we will have to compare the heights of ξ and x. we utilize the duplication formula defined earlier on to obtain an explicit formula for ξ. From (1.17), we have

$$\xi = \frac{x^4 - 2bx^2 - \ldots}{4x^3 - 4ax^2 + \ldots}.$$

Because $2P = \mathcal{O}$ if and only if $f(x) = y^2 = 0$ or $P = \mathcal{O}$, by assumption the denominator of this expression is nonzero. Recall that $f(x)$ is also non-singular by assumption, so $f(x)$ and $f'(x)$ have no common complex roots. As a result, the numerator and denominator also have no common complex roots.

The rest of the proof of this lemma relies on the following proposition about the heights and quotients of polynomials with no common complex roots. Because the

proof of this proposition is quite long and does not pertain specifically to elliptic curves, we direct the reader to [2] for the proof.

Proposition 3.6. *Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and no common complex roots. Let d be the maximum of the degrees of ϕ and ψ. Then*

(a) There is an integer $R \geq 1$, depending on ϕ and ψ such that for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\left(\frac{m}{n}\right)\right) \text{ divides } R.$$

(b) There are constants κ_1 and κ_2, depending on ϕ and ψ, such that for all rational numbers $\frac{m}{n}$ that are not roots of ψ,

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

Recall that ξ is a quotient of polynomials of degree 3 and 4. Since $h(P) = h(x)$ and x is rational number, by Proposition 3.6, we see that there exists a constant κ such that $4h(P) - \kappa \leq h(\xi)$, which is exactly what we wanted to show. □

The final lemma is the hardest to show, but the most interesting.

Lemma 3.7. *The subgroup $2E(\mathbb{Q})$ - i.e. the subgroup of rational points which are twice other points - has finite index in $E(\mathbb{Q})$.*

The proof of the general case of this lemma is beyond the scope of this paper. However, we are equipped to prove it given the assumption of one rational root $T = (x_0, 0)$. Since $y^2 = f(x)$ has integer coefficients and leading coefficient 1, x_0 must be an integer, so we can move T to $(0, 0)$ without affecting the group structure. This makes our equation of the form

$$E : y = x^3 + ax^3 + bx$$

First, we will express the multiplication by two map in terms of the composition of two group homomorphisms. Then, by studying the image and kernel of this map, we will be able to show an injection into a finite set and prove that the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Proposition 3.8. *Let E and $\overline{E}$ be elliptic curves given by the equations*

$$E : y^2 = x^3 + ax^2 + bx \quad \text{and} \quad \overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

where $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$. Let $T = (0, 0)$. There exist homomorphisms $\phi : E \to \overline{E}$ and $\psi : \overline{E} \to E$ such that $\psi \circ \phi(P) = 2P$. In addition, the kernels of ϕ and ψ are $\{\mathcal{O}, T\}$ and $\{\overline{\mathcal{O}}, \overline{T}\}$, respectively.

Proof. Define $\overline{\overline{E}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}$, where $\overline{\overline{a}} = -2\overline{a}$ and $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b}$. Notice that $\overline{\overline{E}}$ is isomorphic to E by the transformation $(x, y) \to (\frac{1}{4}x, \frac{1}{8}y)$. Let $P = (x, y) \in E$. If $P \neq \mathcal{O}, T$. Define a map $\phi(x, y) = (\overline{x}, \overline{y})$ by

$$\overline{x} = \frac{y^2}{x^2} \quad \text{and} \quad \overline{y} = y\left(\frac{x^2 - b}{x^2}\right) \tag{3.9}$$

In addition, we have $\phi(\mathcal{O}) = \overline{\mathcal{O}}$ and $\phi(T) = \overline{\mathcal{O}}$. Let $\overline{\phi} : \overline{E} \to \overline{\overline{E}}$ send $(\overline{x}, \overline{y}) \to (\overline{\overline{x}}, \overline{\overline{y}})$ as in (3.9). Similarly, $\overline{\phi}(\overline{\mathcal{O}}) = \overline{\overline{\mathcal{O}}}$ and $\overline{\phi}(T) = \overline{\overline{T}}$. We define $\psi : \overline{E} \to E$ to be the composition of $\overline{\phi}$ with the isomorphism from $\overline{\overline{E}} \to E$. The proof that ψ and ϕ are

well-defined group homomorphisms and that $\psi \circ \phi$ forms the multiplication-by-two map can be found in [2].

□

The image of $E(\mathbb{Q})$ by ϕ forms a subgroup of $\overline{E}(\mathbb{Q})$, which we will denote by $\phi(E(\mathbb{Q}))$. We can describe it as follows:

Proposition 3.10.

(i) $\overline{\mathcal{O}} \in \phi(E(\mathbb{Q}))$.
(ii) $\overline{T} = (0,0) \in \phi(E(\mathbb{Q}))$ *if and only if* $\overline{b} = a^2 - 4b$ *is a perfect square.*
(iii) Let $\overline{P} = (\overline{x}, \overline{y}) \in \overline{E}(\mathbb{Q})$ *with* $\overline{x} \neq 0$. *Then* $\overline{P} \in \phi(E(\mathbb{Q})$ *if and only if* $\overline{x}$ *is the square of a rational number.*

Proof. The proof of (i) follows from the fact that $\phi(\mathcal{O}) = \overline{\mathcal{O}}$. From the definition of ϕ we know that $\overline{T} = (0,0)$ is in the image of ϕ if and only there is some rational point in $E(\mathbb{Q})$ for which $\frac{y^2}{x^2} = 0$ is true. Notice that this point cannot be T itself, since $\phi(T) = \overline{\mathcal{O}}$, so $x \neq 0$. If we set $f(x)$ equal to 0, we have

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b). \tag{3.11}$$

Then, since $x \neq 0$, we want to see if $x^2 + ax + b$ has a rational root. Luckily, we know this occurs if and only if the discriminant $a^2 - 4b$ is a perfect square, which is what we wanted.

For the proof of (iii), suppose that $(\overline{x}, \overline{y})$ is in the image of $\phi(E(\mathbb{Q}))$ and has $\overline{x} \neq 0$. Then by the definition of ϕ, $\overline{x} = \frac{x^2}{y^2}$ must be the square of some rational number. For the only if direction, suppose that $\overline{x} = \omega^2$ for some rational number ω.

Since we have two elements, $\mathcal{O}$ and T, in the kernel of ϕ, we know that two elements of $E(\mathbb{Q})$ will map to $(\overline{x}, \overline{y})$ if it lies in the image of ϕ. We make the substitution

$$x_1 = \frac{1}{2}\left(\omega^2 - a + \frac{\overline{y}}{\omega}\right), \qquad y_1 = x_1\omega$$
$$x_2 = \frac{1}{2}\left(\omega^2 - a - \frac{\overline{y}}{\omega}\right), \qquad y_2 = -x_2\omega.$$

We check that (x_1, y_1) and (x_2, y_2) are on E by substituting b for x_1x_2 in the equation for $\overline{E}$. We check that the points (x_1, y_1) and (x_2, y_2) both map to $(\overline{x}, \overline{y})$ by checking that we can substitute the definitions of x_1 and x_2 into the definition for $\overline{x}$ and $\overline{y}$. □

Now, using what we know about the images of ϕ and ψ, we will find an injective homomorphism from the quotient groups $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q}))$ and $\overline{E}(\mathbb{Q})/\phi(E(\mathbb{Q}))$ into a finite group. It is enough just to show this for the first of these quotients, so we will choose $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q}))$.

Definition 3.12. We define $\mathbb{Q}^*$ to be the multiplicative group of nonzero rational numbers. Furthermore, we define $\mathbb{Q}^{*2}$ to be the group of squares of elements in $\mathbb{Q}^*$,

$$\mathbb{Q}^{*2} = \{r^2 : r \in \mathbb{Q}^*\}.$$

Proposition 3.13. *Define a map* $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ *by*

$$\alpha(P) = \begin{cases} 1 \pmod{\mathbb{Q}^{*2}} & \text{if } P = \mathcal{O} \\ b \pmod{\mathbb{Q}^{*2}} & \text{if } P = T \\ x \pmod{\mathbb{Q}^{*2}} & \text{if } x \neq 0 \end{cases}.$$

Then, the following hold:

(a) *The map* α *is a homomorphism.*

(b) *The kernel of* α *is the image of* $\psi(\overline{E}(\mathbb{Q})$*. Therefore,* α *induces a one-to-one homomorphism*

$$E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$

(c) *Let* $p_1, p_2, \ldots, p_t$ *be the distinct primes dividing* b*. Then, the image of* α *is contained in the subgroup of* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *consisting of*

$$\{\pm p_1^{\beta_1} p_2^{\beta_2} \ldots P_t^{\beta_t} : \beta_i \text{ equals } 0 \text{ or } 1\}$$

(d) *The index* $(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q})))$ *is at most* 2^{t+1}*.*

Proof. To prove (a), we observe that when P is not equal to T or $\mathcal{O}$, we have

$$\alpha(-P) = \alpha(x, -y) = x = \frac{1}{x} \cdot x^2,$$

implying

$$\alpha(-P) \equiv \frac{1}{x} = \frac{1}{\alpha(x, y)} = \alpha(P)^{-1} \qquad (\text{mod } \mathbb{Q}^{*2}).$$

Since $\alpha(\mathcal{O}) = 1 = 1^{-1}$, we have that α sends inverses to inverses except for $P = T$. So, for points distinct from T, it will be enough to prove that whenever $P_1 + P_2 + P_3 = \mathcal{O}$, we have $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$, since that would imply

$$\alpha(P_1 + P_2) = \alpha(-P_3) \equiv \alpha(P_3)^{-1} \equiv \alpha(P_1)\alpha(P_2) \qquad (\text{mod } \mathbb{Q})^{*2}$$

By Corollary 1.18, we know P_1, P_2, P_3 are colinear. So, we have (x_1, y_1), (x_2, y_2), (x_3, y_3) the intersections of E with a line $y = \lambda x + \nu$. We know x_1, x_2, x_3 to be the roots of the polynomial with constant term $(c - \nu^2)$. Equating the constant terms, we obtain $x_1 x_2 x_3 = c - \nu^2$. Since we specify $c = 0$, we have

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1 x_2 x_3 = \nu^2 \equiv 1 \qquad (\text{mod } \mathbb{Q}^{*2}).$$

To check that $\alpha(P + T) = \alpha(P) + \alpha(T)$, we use our formula from (1.15) and substitute y^2 for $x^3 + ax^2 + b$, obtaining

$$\alpha(P + T) = \frac{bx}{x^2} \equiv bx = \alpha(P)\alpha(T) \pmod{\mathbb{Q}^{*2}}.$$

Finally, $\alpha(T + T) = \alpha(\mathcal{O}) \equiv 1 \equiv b^2 = \alpha(T)\alpha(T) \pmod{\mathbb{Q}^{*2}}$. This concludes the proof of (a).

We described the image $\phi(E(\mathbb{Q}))$ in Proposition 3.10, but these statements extend to $\psi(\overline{E}(\mathbb{Q}))$, since ψ is simply the same homomorphism as ϕ applied again. Then, (b) follows easily from directly comparing the requirements from Proposition 3.10 to the definition of α. For example, T is in the image of ψ if and only if b is a perfect square, but $\alpha(T) = b \equiv 1 \pmod{\mathbb{Q}^{*2}}$ if and only if b is a perfect square, and so on. Then, by the first isomorphism theorem for groups, we have that $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q})) \cong Im(\alpha) \subseteq \mathbb{Q}^*/\mathbb{Q}^{*2}$, so there exists some injective homomorphism from $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q})) \to Q^*/Q^{*2}$.

To prove (c), we have to know which rational x-coordinates can show up in the image of α. Using Lemma 3.3, we substitute $\frac{m}{e^2}$ for x and $\frac{n}{e^2}$ for y into the equation for E. Simplifying, we obtain

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$

Let $d = \gcd(m, m^2 + ame^2 + be^4)$. Notice that d divides both m and be^4. However, by definition, m and e are relatively prime, so we must have that d divides b.

Since n^2 is a square, we know that every prime in its prime factorization appears to an even power. By comparing the prime factorizations of m, n^2 and $m^2+ame^2+be^4$, we can conclude that every element of the prime factorization of m occurs to an even power except perhaps those primes which also occur in b. Therefore, we can write m as the product

$$m = \pm(z)^2 \cdot p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_t^{\beta_t},$$

where $p_1, \dots, p_t$ are the distinct primes dividing b, and each ϵ_i is either 0 or 1. As a result, we have that

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_t^{\beta_t} \qquad (\text{mod } \mathbb{Q}^{*2}).$$

Therefore, the image of α is contained within the set defined as

$$\{\pm p_1^{\beta_1} \dots p_t^{\beta_t} : \ \beta_i \text{ equals 0 or 1}\}.$$

If $x = 0$, then $m = 0$, so this argument does not work. However, T is the only point with $x = 0$ and $\alpha(T) = b$, which, dividing out squares, can be written as the product of its prime divisors. This set is clearly a subgroup of $\mathbb{Q}/\mathbb{Q}^{*2}$ since it is closed under multiplication modulo squares, contains 1, and each element is its own inverse.

The subgroup described in c has exactly 2^{t+1} elements, since there are 2^t possible configurations of 0's and 1's in the sequence $\beta_1, \dots, \beta_t$, and each element can be either positive or negative. Therefore the image of α has at most 2^{t+1} elements. By (b), the index $\big(E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q}))\big)$ must be finite as well.

□

Proposition 3.14. *Consider the homomorphisms $\phi : E(\mathbb{Q}) \to \overline{E}(\mathbb{Q})$ and $\psi : \overline{E}(\mathbb{Q}) \to E(\mathbb{Q})$. The indices of $\phi(E(\mathbb{Q}))$ in $\overline{E(\mathbb{Q})}$ and $\psi(E(\mathbb{Q}))$ in $E(\mathbb{Q})$ satisfy the inequality*

$$\big(E(\mathbb{Q}) : 2E(\mathbb{Q})\big) \leq \big(E(\mathbb{Q}) : \psi(\overline{E}(Q))\big)\ \big(\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q})\big)$$

Proof. Since $\psi(\overline{E}(\mathbb{Q}))$ is a subgroup with finite index in $E(\mathbb{Q})$, there exist coset representatives $e_1, \dots, e_n \in E(\mathbb{Q})$ for the finitely many cosets of $\psi(E(\mathbb{Q}))$. In the same fashion, we find coset representatives $\overline{e}_1, \dots, \overline{e}_m$ for the subgroup $\phi(E(\mathbb{Q}))$ in $\overline{E}(\mathbb{Q})$. To prove the claim, it is sufficient to show that the set of $m \cdot n$ elements,

$$\{e_i + \psi(\overline{e}_j) : 1 \leq i \leq n\ 1 \leq j \leq m\},$$

includes the set of coset representatives of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$.

Let $e \in E(\mathbb{Q})$. If we can write e as the sum of an element of $2E(\mathbb{Q})$ as well as an element of the above set, than we are done. Since we already know that each e_i is a coset representative of $\psi(\overline{E}(\mathbb{Q}))$ in $E(\mathbb{Q})$, we can find some e_i such that $e - e_i \in \psi(\overline{E}(\mathbb{Q}))$. Therefore, we write $e - e_i = \psi(\overline{e})$. Similarly, we can find some

$\overline{e}_j$ such that $\overline{e} - \overline{e}_j \in \phi(E(\mathbb{Q}))$. So we write $\overline{e} - \overline{e}_j = \phi(e')$. Utilizing the fact that $\psi \circ \phi$ is the multiplication by two map, we have:

$$\begin{aligned} e = e_i + \psi(\overline{e}) &= e_i + \psi\left(\overline{e}_j + \phi(e')\right) \\ &= e_i + \psi(\overline{e}_j + \psi(\phi(e')) \\ &= e_i + \psi(\overline{e}_j) + 2e' \end{aligned}$$

which is what we wanted. □

This concludes the proof of Lemma 3.7 as well as the proof of Mordell's theorem for elliptic curves containing at least one rational point of order two.

4. Acknowledgments

I would like to thank my advisor Xinchun Ma for helping me understand the subtleties behind the proof, as well as for introducing me to such a fascinating subject. I would also like to thank my fellow REU classmate Connor Lockhart for explaining basic group theory to me when I did not yet know it. Finally, I thank Peter May for giving me the opportunity to participate in the 2020 Apprentice REU Progam.

References

[1] Pinter, Charles C., A Book of Abstract Algebra. Second edition. Mineola, New York : Dover Publications, Inc. 2010

[2] Silverman, Joseph H., and John Torrence Tate. Rational Points On Elliptic Curves. Second edition. Cham: Springer, 2015.

[3] Winter 2005, Elliptic Curves, lecture notes, Delivered July 2020
URL = https://www.dropbox.com/s/urs67ddst1abtdj/ellipticnotes.pdf?dl=0 .