ELLIPTIC CURVES AND THE MORDELL-WEIL THEOREM

KAREN BUTT

Abstract. Our goal is to prove the Mordell-Weil theorem for elliptic curves over $\mathbb{Q}$, which states that the group of rational points $E(\mathbb{Q})$ is finitely generated. The key tool used is the deep fact that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, the proof of which is the primary focus of this paper.

Contents

1. Introduction

Understanding the rational and integer solutions to seemingly simple Diophantine equations - polynomial equations with integer coefficients - often involves unexpectedly advanced tools. For example, Fermat's Last Theorem took almost 400 years to solve, and led to the development of a lot of interesting mathematics.

Rational solutions to polynomial equations in one variable are easy to understand. If r/s in lowest terms solves $a_n x^n + \cdots + a_1 x + a_0 = 0$ then $r \mid a_0$ and $s \mid a_n$. Linear equations in two variables are also easy. The equation $ax + by = c$ for nonzero $a, b, c \in \mathbb{Z}$ always has infinitely many rational solutions. As for integer solutions, there are infinitely many if $\gcd(a, b) \mid c$ and none otherwise. For quadratic polynomials, it is very helpful to think geometrically. The zero sets of such polynomials are conic sections. Given one rational solution, we can show there are infinitely many using a geometric procedure. Given a rational point on a conic and any rational line, we can define a bijection between the rational points on the line and the rational points on the conic. This is discussed in detail in Section 1.1 of [3]. The question of how to determine whether or not a given conic has a rational solution is much more difficult, but well-understood nonetheless.

On the other hand, there is no known algorithm to determine in general if a cubic equation has a rational solution. In this paper, we will consider sets of solutions

Date: August 29, 2016.

to equations of the form $y^2 = f(x) = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Q}$ and $f(x)$ separable, called *elliptic curves* over $\mathbb{Q}$. To understand if there are infinitely many rational solutions, we can try to come up with a geometric procedure to find more rational solutions from known ones. We cannot simply project onto a line as we can with conics. The construction of a bijection between rational points on a line and rational points on a conic relies heavily on the fact that a line intersects a conic in at most two points, whereas a line can intersect a cubic curve in three points. Given two rational points on an elliptic curve, we can draw the line through them and see if that line intersects the curve somewhere else. If it does, this gives another rational point on the curve and now we have two new pairs of points to which we can apply this process. It turns out that for any elliptic curve, if we start with a specially chosen finite set of points, draw all possible lines through them to find new rational points, and keep iterating this process, then we can obtain all rational points on the curve. This theorem is the main subject of this paper.

The proof blends ideas from number theory, geometry and algebra. We have already alluded to the fact that it is useful to consider number theoretic questions from a geometric perspective. By considering the sets of real or complex solutions to a Diophantine equation as a geometric object, it is easier to see how to obtain new rational solutions from known ones. But there is also a key algebraic idea that we have not yet mentioned. We can make the set of rational solutions to $y^2 = x^3 + ax^2 + bx + c$ along with a special "point at infinity" - a notion that will be made precise in the next section - into an abelian group. (Loosely speaking, the sum of two points is obtained by considering the line through them and its intersection with the curve, and then reflecting this intersection point about the x-axis.) We denote this group by $E(\mathbb{Q})$. The main theorem we prove in this paper, known as the Mordell-Weil theorem, states that the group $E(\mathbb{Q})$ is finitely generated.

We begin by formally defining elliptic curves and their group law. Next, we briefly discuss the torsion subgroup and how to compute it. We then prove the Mordell-Weil theorem using a descent argument involving height functions, a tool that translates the geometric information of the group law into number theoretic information about the points on an elliptic curve. In addition to height functions, the proof of the Mordell-Weil theorem requires the fact that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Here $2E(\mathbb{Q})$ refers to the image of the multiplication by 2 map, that is $P \mapsto P + P$, where $+$ is the group operation on $E(\mathbb{Q})$. The remainder of the paper will focus on understanding this deep fact. We begin this investigation by giving part of the proof a more general fact, called the Weak Mordell-Weil theorem, which states the group $E(K)/mE(K)$ is finite for any positive integer m and any number field K. We then return to the case where $m = 2$ and $K = \mathbb{Q}$ and provide a proof relying on the additional assumption that the right hand side of $y^2 = x^3 + ax^2 + bx + c$ has three rational roots. Afterwards, we show $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite for any elliptic curve over $\mathbb{Q}$.

2. The Group Law

Definition 2.1. An *elliptic curve* E over a field K of characteristic different from 2 is a nonsingular projective curve given by the equation

$$F(X, Y, Z) = Y^2Z - (X^3 + aX^2Z + bXZ^2 + cZ^3) = 0, \tag{2.2}$$

where $a, b, c \in K$.

Remark 2.3. If char$K \neq 2$ then any nonsingular projective cubic curve can be reparametrized into this form by a projective transformation. (See [3] for details.)

We can identify the projective plane $\mathbb{P}^2$ with $\mathbb{A}^2 \cup \mathbb{P}^1$, where $\mathbb{A}^2$ denotes the affine plane and $\mathbb{P}^1$ denotes the projective line. The projective line is the set of all directions in the plane, which we call points at infinity. If $Z \neq 0$ then we associate the projective point $(X : Y : Z)$ with the affine point $(X/Z, Y/Z)$. We associate $(X : Y : 0)$ with the projective point $(X : Y) \in \mathbb{P}^1$. (For further details, see [3] Appendix A.)

Viewing the projective plane as $\mathbb{A}^2 \cup \mathbb{P}^1$, our projective curve $F(X, Y, Z) = 0$ consists of a curve in the affine plane together with points at infinity. Setting $Z = 1$ in (2.2) we get the affine curve

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

Note that since we assumed the projective curve $F(X, Y, Z) = 0$ is nonsingular, the above affine curve is nonsingular as well. This means $f(x)$ has distinct roots over the algebraic closure $\overline{K}$. Also note that if (x, y) is a point on the curve, so is $(x, -y)$, so the curve is symmetric about the x-axis.

Now we consider the points at infinity. Setting $Z = 0$ in (2.2) we get $X^3 = 0$, which means $X = 0$. So $(0 : 1 : 0) \in \mathbb{P}^2$ is the only point at infinity. Under our identification $\mathbb{P}^2 \cong \mathbb{A}^2 \cup \mathbb{P}^1$, this projective point corresponds to the vertical direction in the xy-plane, or the point at infinity where all vertical lines meet. So from now on we will think of an elliptic curve as the affine curve $y^2 = f(x) = x^3 + ax^2 + bx + c$ together with a point at infinity in the vertical direction which we will call $\mathcal{O}$.

Definition 2.4. Let $E : y^2 = f(x)$ be an elliptic curve over K. The set of K-*rational points* on E is the set

$$\{(x, y) \in K \times K \mid y^2 = f(x)\}.$$

We denote this set by $E(K)$.

We refer to the $\mathbb{Q}$-rational points $E(\mathbb{Q})$ simply as the rational points on E. If we already know some points in $E(\mathbb{Q})$, we can ask ourselves how to find new ones. If we draw a line through two rational points P and Q and this line happens to intersect the curve again in some point R, then R will be a rational point as well. It turns out that every line intersects an elliptic curve in three points if we include $\mathcal{O}$ as a point and count tangent intersections with multiplicity 2 or 3. (This is a special case of Bezout's Theorem, which states that two curves of degree m and n intersect in mn points. For a proof see [3] Appendix A.)

Using this, we can define a binary operation on $E(\mathbb{Q})$. Given distinct points $P, Q \in E(\mathbb{Q})$, define $P * Q$ to be the third point of intersection between the curve and the line passing through P and Q. Note that $P * Q \in E(\mathbb{Q})$ as well. Define $P + Q$ to be the reflection of $P * Q$ about the x-axis. To define $P * P$, we take the line tangent to E at P (which is well-defined for every P because E is non-singular) and let $P * P$ be the third intersection point of E with the tangent line. As before, we take $P + P$ to be the reflection of $P * P$ about the x-axis.

We claim the commutative binary operation $+$ makes the set $E(\mathbb{Q})$ into a group. Checking associativity is tedious. The main tool is the following algebraic geometry fact.

Theorem 2.5. *Let C_1 and C_2 be two cubic curves. Let C be a curve passing through eight of the nine intersection points of C_1 and C_2. Then C passes through the ninth intersection point as well.*

For further details about associativity, see [3] or [4].

To finish showing $(E(\mathbb{Q}), +)$ is a group, we check the existence of an identity and inverses. We claim $\mathcal{O}$ is the identity element. To see this, note that the line through P and $\mathcal{O}$ is the vertical line passing through P. Then $P * \mathcal{O}$ is the reflection of P about the x-axis and $P + \mathcal{O}$ is obtained by again reflecting about the x-axis. So $P + \mathcal{O} = P$ for all P. Now we claim $-P = P * \mathcal{O}$. Since the line through P and $P * \mathcal{O}$ is the vertical line, we get $P + P * \mathcal{O} = \mathcal{O}$. So given P, we obtain $-P$ by reflecting P about the x-axis. Equivalently, if $P = (x, y)$ then $-P = (x, -y)$. Thus $E(\mathbb{Q})$ is an abelian group.

Remark 2.6. The points $P, Q, R \in E(\mathbb{Q})$ are collinear iff $P + Q + R = \mathcal{O}$. This will come up in later sections.

Next, we discuss explicit formulas for the group law. Let $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\mathbb{Q})$. Write $P + Q = (x_3, y_3)$. Let $y = \lambda x + \nu$ be the line passing through P and Q if P and Q are distinct. If $P = Q$ let $y = \lambda x + \nu$ be the tangent to E at P. Then equating y-coordinates of the elliptic curve and the line we have $f(x) = (\lambda x + \nu)^2$ precisely when $x = x_1, x_2, x_3$. We can rewrite this as

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{2.7}$$

Equating the x^2 coefficients of both sides and rearranging gives

$$x_3 = \lambda^2 - a - x_1 - x_2.$$

When P and Q are distinct, we have $\lambda = (y_2 - y_1)/(x_2 - x_1)$. If $P = Q = (x, y)$, we use implicit differentiation to find $\lambda = f'(x)/2y$. In this case, we can simplify to obtain

$$x_3 = x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)}. \tag{2.8}$$

One can use the relation $-y_3 = \lambda x_3 + \nu$ to derive an explicit formula for the y-coordinates.

These formulas allow us to define a group law on an elliptic curve over any field. For instance, it is difficult to visualize the geometry of the group law over a finite field, but the above formulas still make sense.

3. Torsion Points

The first step in understanding the group of points on an elliptic curve over $\mathbb{Q}$ is understanding the points of finite order. In this section, we examine the group structure of the points of finite order. We also prove a theorem that lets us compute the torsion points over $E(\mathbb{Q})$.

Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\mathbb{Q}$. Let

$$E[m] = \{P \in E(\overline{\mathbb{Q}}) \,|\, mP = \mathcal{O}\},$$

which we refer to as the set of m-torsion points. Note that we can derive an explicit formula for the multiplication by m map from the addition and multiplication formulas in the previous section. The actual formula does not matter, but it is important to keep in mind that if $P = (x, y)$ the x-coordinate of mP will be given

by some rational function of x with coefficients in $\mathbb{Q}$. We want to determine the group structure of $E[m]$.

First we consider points of order 2, that is, points such that $P = -P$. This means $(x, y) = (x, -y)$. Thus $y = 0$. If we let x_1, x_2, x_3 denote the roots of $f(x)$ then $E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$. Since each of the nontrivial points has exact order 2, we have $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Next, we consider $E[3]$. These are points such that $3P = \mathcal{O}$ or equivalently $2P = -P$. Setting $x(2P) = -x$ gives x is a root of

$$g(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

We claim $g(x)$ has four distinct roots. To see this, we show g has no roots in common with g'. We have $g'(x) = 12x^3 + 12ax^2 + 12bx + 12c = 12f(x)$. The reader can check $g(x) = 2f(x)f''(x) - f'(x)^2$. Suppose for contradiction that g and g' share a root α. Then α is a root of g' implies α is a root of f. Looking at the expression for g, we see that α is a root of f'. This contradicts the assumption that f has no repeated roots, so g must have distinct roots.

So there are four possible x-coordinates for points of order 3. For each root x we have $\pm\sqrt{f(x)}$ as possible y-coordinates. These two y-coordinates are distinct whenever $f(x) \neq 0$ which is always the case since x does not have order 2. So $E[3]$ consists of these eight points in addition to the point $\mathcal{O}$. As an abstract group, we have $E[3] = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

In general, we have $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. One proof uses the fact that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ where Λ is a lattice. (See [4] Chapter VI for more details.) To prove $E(\mathbb{Q})$ is finitely generated, we will only need $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Since our main objective is to understand the group $E(\mathbb{Q})$, we now consider the torsion points which have coordinates in $\mathbb{Q}$ and denote this subgroup by $E(\mathbb{Q})_{\text{tors}}$. We have the following surprising fact, which we will not prove.

Theorem 3.1 (Nagell-Lutz)**.** *Let $E : y^2 = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$. If $(x, y) \in E(\mathbb{Q})_{\text{tors}}$ then $x, y \in \mathbb{Z}$.*

For a proof, see [3] Sections 2.4 and 2.5. Also note that after a change of variables, we can assume the equation of any elliptic curve over $\mathbb{Q}$ has integer coefficients.

In light of this result, it makes sense to reduce the coordinates of torsion points mod p. We use the notation $(\tilde{x}, \tilde{y})$ to denote (x, y) reduced mod p. To compute the torsion subgroup, we need to consider elliptic curves over $\mathbb{F}_p$ for $p \geq 3$. Although it is hard to visualize projective space over a finite field, the addition and duplication formulas still make sense. Given an elliptic curve E over $\mathbb{Q}$ given by an equation with integer coefficients, we can sometimes reduce the coefficients mod p to get an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$. We need $y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$ to have distinct roots in $\mathbb{F}_p$. We say E has *good reduction* at p if this is the case, and bad reduction if not. Let Δ denote the discriminant of $f(x) = x^3 + ax^2 + bx + c$. Then E has good reduction at the prime p iff p does not divide Δ. To see this, note that the discriminant of f is a polynomial in the coefficients of f. So taking the discriminant of f commutes with reduction of the coefficients mod p, meaning $\tilde{\Delta}$ is the discriminant of $\tilde{f}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$. So $\tilde{f}$ has distinct roots iff $\tilde{\Delta} \neq 0$ in $\mathbb{F}_p$. Equivalently, p does not divide Δ.

Theorem 3.2. *Let p be a prime so that E has good reduction at p. Let $\phi : E(\mathbb{Q})_{\text{tors}} \to \tilde{E}(\mathbb{F}_p)$ be given by $\mathcal{O} \mapsto \tilde{O}$ and $(x, y) \mapsto (\tilde{x}, \tilde{y})$. Then ϕ is an injective homomorphism, and thus $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\tilde{E}(\mathbb{F}_p)$.*

Proof. First we check ϕ is a homomorphism. Note that

$$\phi(-P) = \phi(x, -y) = (\tilde{x}, -\tilde{y}) = -\phi(P).$$

So to show $\phi(P+Q) = \phi(P) + \phi(Q)$ it suffices to show that if $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = (x_3, y_3)$ sum to $\mathcal{O}$ then

$$\phi(P) + \phi(Q) + \phi(R) = \tilde{P} + \tilde{Q} + \tilde{R} = \tilde{\mathcal{O}}.$$

Since P, Q, R are collinear (see Remark 2.6) we have

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) \tag{3.3}$$

for some $\lambda, \nu \in \mathbb{Q}$. Recall the addition formulas $x_3 = \lambda^2 - a - x_1 - x_1$ and $y_3 = -(\lambda x_3 + \nu)$. The fact that a, x_1, x_2, x_3 are all integers implies λ and ν are integers. So it makes sense to reduce (3.3) mod p. This implies $\tilde{P}$, $\tilde{Q}$ and $\tilde{R}$ are collinear and hence sum to $\tilde{\mathcal{O}}$. So ϕ is a homomorphism. Clearly, $\ker \phi = \mathcal{O}$ so ϕ is injective. □

Corollary 3.4. *The order of the torsion subgroup Φ divides the order of $\tilde{E}(\mathbb{F}_p)$ for every prime p with good reduction.*

This result is very useful for computing the torsion subgroup. We provide an example.

Example 3.5. Let $E : y^2 = x^3 - x$. Then $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Since $y^2 = x^3 - x = x(x-1)(x+1)$ we get $E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}$. Thus $|E(\mathbb{Q})_{\text{tors}}| \geq 4$. To get an upper bound on the size of the torsion subgroup, we use the above corollary. First note $\Delta = 4$. So E has good reduction at $p = 3$. Reducing mod 3, we get the curve $\tilde{E} : y^2 = x^3 - x$ over $\mathbb{F}_3$. For any $x \in \mathbb{F}_3$ we have $x^3 - x = 0$. So $\tilde{E}(\mathbb{F}_p) = \{\mathcal{O}, (0,0), (1,0), (2,0)\}$ and thus $|\tilde{E}(\mathbb{F}_p)| = 4$. By the corollary, $|E(\mathbb{Q})_{\text{tors}}|$ divides 4. Thus $E(\mathbb{Q})_{\text{tors}}$ has order 4. Since $E[2] \subset E(\mathbb{Q})_{\text{tors}}$ we get $E(\mathbb{Q})_{\text{tors}} = E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

4. Mordell-Weil Theorem

In this section, we prove the Mordell-Weil theorem, assuming some lemmas.

Definition 4.1. The *height* H of a rational number m/n in lowest terms is given by

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

The notion of height is useful in establishing finiteness results because the set of rational numbers less than some given height M is finite.

Definition 4.2. Let $P = (x, y) \in E(\mathbb{Q})$. We define the height of a point to be the height of its x-coordinate.

The set of points on an elliptic curve with height less than M is also a finite set. To see this, note that for each of the finitely many x-coordinates of height less than M there are at most two distinct y-coordinates.

It is more convenient to have a function that behaves additively, so we let $h = \log H$. We have the following two lemmas, which tell us how much the operations of addition and duplication increase the height of a point. For proofs, see [3] Sections 3.2 and 3.3.

Lemma 4.3. *Let $Q_0 \in E(\mathbb{Q})$. Then there is a constant κ_0 such that*

$$h(P + Q_0) \leq 2h(P) + \kappa_0$$

for all $P \in E(\mathbb{Q})$.

Lemma 4.4. *There is a constant κ so that*

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

for all $P \in E(\mathbb{Q})$.

And, finally, we require the following fact, which is the most interesting part behind the theorem.

Theorem 4.5. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Using these results, we are ready to prove our main theorem.

Theorem 4.6 (Mordell-Weil)**.** *The group $E(\mathbb{Q})$ is finitely generated.*

Proof. We have $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Let $Q_1, \ldots, Q_n$ be coset representatives for the quotient. Then given any $P \in E(\mathbb{Q})$ we have $P = Q_1 + 2P_1$ for some $P_1 \in E(\mathbb{Q})$ (after relabelling the Q_i). Continuing in this manner, we have $P_1 = Q_2 + 2P_2$ for some $P_2 \in E(\mathbb{Q})$ up to $P_{n-1} = Q_n + 2P_n$. Substituting, we get

$$P = Q_1 + 2P_2 + 4P_2 + \cdots + 2^{n-2}(Q_n + 2P_n).$$

So it suffices to show that no matter what P we choose, the set of possible P_n will be finite. This is where we use heights. We will show that no matter what P is, the set of possible P_n come from a set of points less than a given height. The idea is that the heights of the P_i are decreasing, so for m large enough we get $h(P_m) \leq C$.

Applying Lemma 4.3 with $Q_0 = Q_i$ we get

$$h(2P_i) = h(P_{i-1} - Q_i) \leq h(P_{i-1}) + \kappa_i.$$

By Lemma 4.4 we have

$$4h(P_i) \leq h(2P_i) + \kappa.$$

Combining the above two inequalities we get

$$4h(P_i) \leq 2h(P_{i-1}) + C,$$

where $C = \max_i \kappa_i + \kappa$. So

$$\begin{aligned} h(P_i) &\leq \frac{1}{2}h(P_{i-1}) + C \\ &= \frac{3}{4}h(P_{i-1}) - \frac{1}{4}(h(P_{i-1}) - C). \end{aligned}$$

If $h(P_{i-1}) \geq C$ then we have $h(P_i) \leq \frac{3}{4}h(P_{i-1})$. This means as i gets larger the height of P_i approaches 0. So there is eventually an m large enough with $h(P_m) \leq C$. So for any $P \in E(\mathbb{Q})$ there exists P_n so that

$$P = Q_1 + 2Q_2 + \cdots + 2^{n-2}Q_n + 2^{n-1}P_n,$$

where $h(P_n) \leq C$. But we already noted that $\{P \in E(\mathbb{Q}) : h(P) \leq C\}$ is a finite set. So $E(\mathbb{Q})$ is generated by the Q_i along with elements from this set. This completes the proof that $E(\mathbb{Q})$ is finitely generated. □

5. Weak Mordell-Weil Theorem for General m and K

To complete our proof of the Mordell-Weil theorem, we need to show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. First we note that the following generalization of the theorem holds as well, but the complete proof is beyond the scope of this paper.

Theorem 5.1 (Weak Mordell-Weil)**.** *Let K be a number field. Then the group $E(K)/mE(K)$ is finite.*

Before we set $K = \mathbb{Q}$ and $m = 2$, we use this section to make some remarks that apply to the general case. In particular, we will reduce the finiteness of $E(K)/mE(K)$ to the finiteness of a certain field extension of K. In the subsequent section, we will prove the field extension is finite when $m = 2$, $K = \mathbb{Q}$ and $E[2] \subset E(\mathbb{Q})$. We say more about $E(K)/2E(K)$ for general number fields K at the end of the paper. For general m, it is not feasible to find the field extension explicitly. In order to prove Theorem 5.1, one must resort to algebraic number theory that is beyond the scope of this paper. (See Section VIII.1 of [4].)

It will be helpful to assume $E[m] \subset E(K)$. To see that we can do this, we need the following lemma.

Lemma 5.2. *Let K be a number field and let L/K be a finite Galois extension with Galois group G. If $E(L)/mE(L)$ is finite, then so is $E(K)/mE(K)$.*

Proof. Consider the map $E(K)/mE(K) \to E(L)/mE(L)$ given by $P + mE(K) \mapsto P + mE(L)$ where we now view P as an element of $E(L)$. This is well-defined since $P - P' \in mE(K)$ implies $P - P' \in mE(L)$. Let Φ be the kernel of this map. Then we have an exact sequence

$$0 \longrightarrow \Phi \longrightarrow E(K)/mE(K) \longrightarrow E(L)/mE(L).$$

So it suffices to show Φ is finite. We have

$$\Phi = \frac{E(K) \cap mE(L)}{mE(K)}.$$

To each $P \in \Phi$ we associate a map from G to $E(\overline{K})$ as follows. For each $P \in \Phi$ there is $Q \in E(L)$ so that $mQ = P$. Let $\lambda_P(\sigma) = Q^\sigma - Q$ for $\sigma \in G$. We claim the image of λ_P is in $E[m]$. Indeed,

$$m(Q^\sigma - Q) = m(Q^\sigma) - mQ = P^\sigma - P = \mathcal{O},$$

where the last equality is due to the fact that $P \in E(K)$ and is thus fixed by every element of G.

Next, we claim $P \mapsto \lambda_P$ is injective. If $P - P' \in mE(K)$ then

$$\lambda_P(\sigma) - \lambda_{P'}(\sigma) = (Q^\sigma - Q) - (Q' - Q'^\sigma) = (Q - Q')^\sigma - (Q - Q').$$

But $P - P' = m(Q - Q') \in mE(K)$ so $Q - Q' \in E(K)$. Thus $Q - Q'$ is fixed by every element in G, and so $(Q - Q')^\sigma - (Q - Q') = \mathcal{O}$.

So Φ injects into the set of maps between G and $E[m]$. Since both G and $E[m]$ are finite sets, we see that Φ is also finite which completes the proof. □

Remark 5.3. For the reader familiar with group cohomology, the map λ_P is a 1-cocycle and we have realized Φ as a subgroup of $H^1(G, E[m])$.

Corollary 5.4. *It suffices to prove $E(K)/mE(K)$ finite for K satisfying $E[m] \subset E(K)$.*

Proof. Given an elliptic curve E over K, let L/K be the field extension given by adjoining to K the coordinates of all the points in $E[m]$. This is obviously a finite extension; we claim it is also a Galois extension. Using the addition and duplication formulas given in Section 2, we can derive an explicit formula for the multiplication by m map. For $P = (x_1, y_1)$, the x-coordinate of a point mP will be given by a rational function of x_1 with coefficients in K. We have $mP = \mathcal{O}$ iff this rational function is infinite, that is when the denominator vanishes. So x_1 is the x-coordinate of an m-torsion point precisely when it is a root of the polynomial in the denominator. So the field extension of K given by adjoining the x-coordinates of all the m-torsion points is equal to the splitting field of this polynomial, so it is a Galois extension. Similarly, we find a formula for the y-coordinate and use the same argument to show adjoining all the y coordinates gives a splitting field, and hence a Galois extension. Since L is the compositum of these two extensions, we see L is also a Galois extension.

Since L/K is a finite Galois extension, the previous lemma tells us $E(L)/mE(L)$ finite implies $E(K)/mE(K)$ finite. So we only have to show $E(L)/mE(L)$ is finite for L with $E[m] \subset E(L)$. □

In light of this result, we will assume from now on that $E[m] \subset E(K)$ and use this to show $E(K)/mE(K)$ is finite. Intuitively, we can think of the size of $E(K)/mE(K)$ as a measure of how large $E(K)$ is compared to $mE(K)$. This is a question of how hard it is to invert the multiplication by m map in $E(K)$. Given $P \in E(K)$ we can always find $Q \in E(\overline{K})$ so that $mQ = P$. To see this, note that we can derive an explicit formula for the multiplication by m map using the addition and duplication formulas from Section 2. Given $Q = (x, y)$, the x-coordinate of a point mQ is given by a rational function of x with coefficients in K. Setting this equal to the x-coordinate of $P \in E(K)$, we get that x is the root of a polynomial with coefficients in K. So x is in the algebraic closure $\overline{K}$. Thus the multiplication by m map is surjective on $E(\overline{K})$ and we have the following short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{m} E(\overline{K}) \longrightarrow 0. \tag{5.5}$$

However, we do not necessarily have $Q \in E(K)$. In other words, the multiplication by m map is not always surjective when restricted to $E(K)$. So we instead get the following exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(K) \xrightarrow{m} E(K). \tag{5.6}$$

Let $G = \mathrm{Gal}(\overline{K}/K)$. For $Q = (x, y)$ and $\sigma \in G$, let Q^σ denote $(\sigma(x), \sigma(y))$. We can measure the failure of the multiplication by m map on $E(K)$ to be surjective by considering the quantities $Q^\sigma - Q$ for $\sigma \in G$. Indeed, if $Q \in E(K)$ then $Q^\sigma - Q = \mathcal{O}$ for every $\sigma \in G$, so this is measuring the failure of Q to be in $E(K)$. Now given $P \in E(K)$ and Q so that $mQ = P$, we define

$$\phi_Q(\sigma) = Q^\sigma - Q$$

for all $\sigma \in G$. We claim ϕ_Q depends only on P. To see this, suppose we have $mQ' = P$. Then $(\phi_{Q'} - \phi_Q)(\sigma) = (Q - Q')^\sigma - (Q - Q')$. But $m(Q - Q') = P - P = \mathcal{O}$. So $Q - Q' \in E[m] \subset E(K)$. Since the action of G on K is trivial, we see that $(Q - Q')^\sigma - (Q - Q') = \mathcal{O}$ and hence $\phi_{Q'} = \phi_Q$. This shows ϕ_Q only depends on P, so we will denote it by ϕ_P from now on. We claim ϕ_P is a homomorphism. We will use the fact that $(mQ)^\sigma = m(Q^\sigma)$. This holds because the multiplication by

m map is given by a rational function with coefficients in K so it commutes with any automorphism σ of $\overline{K}$ fixing K. We have

$$\begin{aligned}\phi_P(\sigma\tau) = Q^{\sigma\tau} - Q &= Q^{\sigma\tau} - Q^\sigma + Q^\sigma - Q \\ &= Q^{\sigma\tau} - Q^\sigma + \phi_P(\sigma) \\ &= \phi_{(mQ)^\sigma}(\tau) + \phi_P(\sigma) \\ &= \phi_{m(Q^\sigma)}(\tau) + \phi_P(\sigma) \\ &= \phi_{P^\sigma}(\tau) + \phi_P(\sigma) \\ &= \phi_P(\tau) + \phi_P(\sigma),\end{aligned}$$

where the last equality is due to the fact that the action of G on K is trivial. Next, note that the image of ϕ_P is contained in $E[m]$. We have

$$m(Q^\sigma - Q) = (mQ)^\sigma - mQ = P^\sigma - P = \mathcal{O},$$

where the last equality uses $P \in E(K)$. To summarize, we have defined a map from $E(K)$ to $\mathrm{Hom}(G, E[m])$ given by $P \mapsto \phi_P$. Call this map δ.

We claim δ is a homomorphism. Given $P_1, P_2 \in E(K)$ take $Q_1, Q_2 \in E(\overline{K})$ with $mQ_i = P_i$ for $i = 1, 2$. Then $m(Q_1 + Q_2) = P_1 + P_2$. So for all $\sigma \in G$ we get

$$\begin{aligned}\phi_{P_1+P_2}(\sigma) &= (Q_1 + Q_2)^\sigma - (Q_1 + Q_2) \\ &= Q_1^\sigma - Q_1 + Q_2^\sigma - Q_2 \\ &= (\phi_{P_1} + \phi_{P_2})(\sigma),\end{aligned}$$

which proves the claim. Now we consider $\ker\delta$. Suppose P is such that ϕ_P is the identity. Then $Q^\sigma = Q$ for all $\sigma \in G$ and so $Q \in E(K)$. This means $P \in mE(K)$. Conversely, if $P \in mE(K)$ then there is $Q \in E(K)$ with $mQ = P$. Then Q is fixed by every element of G, that is $Q^\sigma - Q = \mathcal{O}$ for all $\sigma \in G$. So $\ker\delta = mE(K)$. This means we have an injection

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G, E[m]).$$

To summarize, we have proved the following.

Proposition 5.7. *Let E be an elliptic curve and K be a number field such that $E[m] \subset E(K)$. Then $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G, E[m])$.*

Remark 5.8. To the reader familiar with group cohomology, the map δ is the connecting homomorphism in the long exact sequence for cohomology. To see this, consider again the short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{m} E(\overline{K}) \longrightarrow 0.$$

Taking G-cohomology we get the long exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(K) \xrightarrow{m} E(K) \xrightarrow{\delta} H^1(G, E[m]) \longrightarrow H^1(G, E(\overline{K}) \longrightarrow \cdots.$$

Since we are assuming $E[m] \subset E(K)$, the action of G on $E[m]$ is trivial. Therefore $H^1(G, E[m]) \cong \mathrm{Hom}(G, E[m])$. So we get a homomorphism $\delta : E(K) \to \mathrm{Hom}(G, E[m])$ as before. Exactness of the sequence at the second $E(K)$ gives $mE(K) = \ker\delta$. So we get $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(G, E[m])$ as before.

Our first proof of this fact was just showing how we can get from the short exact sequence of G-modules to the long exact sequence of cohomology in this specific case, and the arguments generalize to any short exact sequence of G-modules. When we showed ϕ_P is a homomorphism, we had $\phi_P(\sigma\tau) = \phi_{P^\sigma}(\tau) + \phi_P(\sigma)$. This shows

ϕ_P is a 1-cocycle. We then used $P \in E(K)$ to conclude that ϕ_P is a homomorphism. Before this, we showed $\phi_P(\sigma) = Q^\sigma - Q$ for Q with $mQ = P$ does not depend on Q. To do this, we first wrote $\phi_Q(\sigma) - \phi_{Q'}(\sigma) = (Q - Q')^\sigma - (Q - Q')$ and showed $Q - Q' \in E[m]$. In the language of group cohomology, this means ϕ_Q and $\phi_{Q'}$ differ by a coboundary. We then showed the only coboundary is the trivial coboundary using $E[m] \subset E(K)$. So our argument showed $\phi_P \in H^1(G, E[m])$, the group of cocycles modulo coboundaries, and used $E[m] \subset E(K)$ to get $H^1(G, E[m]) = \mathrm{Hom}(G, E[m])$.

Remark 5.9. The exact sequences (5.5) and (5.6) are analogous to the exact sequences one encounters in the study of Kummer theory of fields. Instead of $E(K)$ containing $E[m]$ we consider the abelian multiplicative group $K^\times$ containing the mth roots of unity μ_m. Then we have a short exact sequence

$$0 \longrightarrow \mu_m \longrightarrow \overline{K}^\times \xrightarrow{m} \overline{K}^\times \longrightarrow 0, \tag{5.10}$$

where instead of the multiplication by m map, we are considering the mth power map. Taking G-cohomology, we get the long exact sequence

$$1 \longrightarrow \mu_m \longrightarrow K^\times \xrightarrow{m} K^\times \xrightarrow{\delta} H^1(G, \mu_m) \longrightarrow H^1(G, \overline{K}^\times) \longrightarrow \dots. \tag{5.11}$$

Since the action of G on μ_m is trivial, we have $H^1(G, \mu_m) \cong \mathrm{Hom}(G, \mu_m)$. By the famous Hilbert's Theorem 90 (for a proof see [1], Section 17.3), the group $H^1(G, \overline{K}^\times)$ is trivial, so we immediately obtain $K^\times/(K^\times)^m \cong \mathrm{Hom}(G, \mu_m)$. For elliptic curves, we do not have an analogue of Hilbert's Theorem 90, so the connecting homomorphism δ need not be an isomorphism. So we have to do more work to determine $E(K)/mE(K)$, which is what we do next.

We want to show the image of $E(K)/mE(K)$ in $\mathrm{Hom}(G, E[m])$ is finite. We begin by interpreting $\mathrm{Hom}(G, E[m])$ in a more useful way. Given $f \in \mathrm{Hom}(G, E[m])$ let $H = \ker f$ and let $L = \overline{K}^H$ be the corresponding fixed field. We have $H \trianglelefteq G$. Also, H is closed in the profinite topology since it has finite index. So Galois theory tells us L/K is a Galois extension with Galois group G/H. By the first isomorphism theorem, we have $G/H \cong \mathrm{im} f \subset E[m]$. Recall $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (see Section 3). So we can associate $\mathrm{Hom}(G, E[m])$ with Galois extensions of K having Galois group contained in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Now we consider the image of $E(K)/mE(K)$, which is the set of homomorphisms ϕ_P. As in the previous paragraph, we associate these to fields $L_P = \overline{K}^{\ker \phi_P}$. We claim $L_P = K(Q)$, where $K(Q)$ means $K(x, y)$ and $Q = (x, y)$. We have L_P is the fixed field of $\ker \phi_P = \{\sigma \in G \,|\, Q^\sigma = Q\}$. We also have $K(Q)$ is the fixed field of the subgroup $\{\sigma \in G \,|\, \sigma(x) = x, \sigma(y) = y\}$. But this is precisely $\ker \phi_P$. So $L_P = K(Q)$.

Remark 5.12. If $Q' = (x', y')$ is any point in $E(\overline{K})$ such that $mQ' = P$, then $x', y' \in K(Q) = L_P$. To see this, note that $m(Q' - Q) = P - P = \mathcal{O}$. So $Q' - Q \in E[m] \subset E(K) \subset E(L_P)$. Since $Q' = Q + (Q' - Q)$, we have x' is given by a rational function of the coordinates of Q and $Q - Q'$. Since both these points are in $E(L_P)$, we see $x' \in L_P$. A similar argument shows $y' \in L_P$.

Let L be the compositum of all the L_P as P ranges through $E(K)$. Recall that at the beginning of this section, we said we could think about the putative finiteness of $E(K)/mE(K)$ as a question of how hard it is to invert the multiplication by m

map in $E(K)$. We now know that given any $P \in E(K)$ we have $Q \in E(L)$ with $mQ = P$. So the size of L should have some relation to the size of $E(K)/mE(K)$. We make this precise below.

Proposition 5.13. *Suppose* $\mathrm{Gal}(L/K)$ *is finite. Then* $E(K)/mE(K)$ *is also finite.*

Proof. In light of the injection given by Proposition 5.7, showing $E(K)/mE(K)$ is finite amounts to showing the set $\{\phi_P \mid P \in E(K)\} \subset \mathrm{Hom}(G, E[m])$ is finite. Each ϕ_P is trivial on $\mathrm{Gal}(\overline{K}/L)$ since $Q^\sigma = Q$ for all $Q \in E(L)$. The maps in $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K, E[m])$ that are trivial on $\mathrm{Gal}(\overline{K}/L)$ can be identified with maps out of the quotient group $\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L)$. From Galois theory, we know this quotient group is isomorphic to $\mathrm{Gal}(L/K)$. So

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E[m]).$$

Since $\mathrm{Gal}(L/K)$ and $E[m]$ are both finite, so is $\mathrm{Hom}(\mathrm{Gal}(L/K), E[m])$. Thus, $E(K)/mE(K)$ is finite. □

6. Weak Mordell-Weil for $E[2] \subset E(\mathbb{Q})$

With this reformulation in mind, we consider the following special case of the weak Mordell-Weil theorem.

Theorem 6.1. *Let* E *be such that* $E[2] \subset \mathbb{Q}$. *Then* $E(\mathbb{Q})/2E(\mathbb{Q})$ *is finite.*

We want to show the field L defined in the previous section is a finite extension of $\mathbb{Q}$. Setting $K = \mathbb{Q}$ and $m = 2$ in the discussion preceding Remark 5.12 we get that each L_P is contained in a biquadratic extension of $\mathbb{Q}$. We explicitly compute L_P from the duplication formula and use the result to show the compositum L is finite.

Since we are assuming $E[2] \subset \mathbb{Q}$, after a change of coordinates we can assume one of the 2-torsion points is the origin. So we have $E : y^2 = x(x-e_1)(x-e_2)$ with $e_1, e_2 \in \mathbb{Q}$. In this case, the duplication formula simplifies to

$$x(2Q) = \frac{x^4 - 2e_1e_2x + (e_1e_1)^2}{4y^2}. \tag{6.2}$$

Fix $P = (\alpha, \beta) \in E(\mathbb{Q})$. We want $Q = (x_1, y_1)$ so that $2Q = P$. Substituting for y^2 and rearranging, we get x_1 is a root of

$$g(x) := x^4 - 4\alpha x^3 + (4e_1\alpha - 2e_1e_2)x^2 - 4e_1e_2\alpha x + e_1^2e_2^2. \tag{6.3}$$

This polynomial has 4 roots. This makes sense because there are four points Q which double to P. This is because any two of them differ by a nontrivial 2-torsion point (see Remark 5.12), and there are three nontrivial 2-torsion points.

We are interested in the splitting field of the polynomial g, which we know from the theoretical argument should be given by adjoining two square roots to $\mathbb{Q}$. Replacing x with $x+\alpha$ does not change the splitting field, but this allows us to get rid of the x^3 term. We obtain the polynomial

$$\begin{aligned} x^4 &+ (4e_1\alpha + 4e_2\alpha - 2e_1e_2 - 6\alpha^2)x^2 + (8e_1\alpha^2 + 8e_2\alpha^2 - 8\alpha^3 - 8e_1e_2\alpha)x \\ &+ (e_1^2e_2^2 - 6e_1e_2\alpha^2 + 4e_1\alpha^3 + 4e_2\alpha^3 - 3\alpha^4). \end{aligned}$$

The four roots are

$$\pm\sqrt{(\alpha-e_1)(\alpha-e_2)} \pm \sqrt{2\alpha^2 - e_1\alpha - e_2\alpha - 2\alpha\sqrt{(\alpha-e_1)(\alpha-e_2)}}.$$

Proposition 6.4. *The splitting field of $g(x)$ is $L_P = \mathbb{Q}(\sqrt{\alpha - e_1}, \sqrt{\alpha - e_2})$. Furthermore, there exists $Q \in E(L_P)$ so that $2Q = (\alpha, \beta)$.*

Proof. To show the roots of $g(x+\alpha)$ are in L_P it suffices to show that $2\alpha^2 - e_1\alpha - e_2\alpha - 2\alpha\sqrt{(\alpha - e_1)(\alpha - e_2)}$ is a square in L_P. We have

$$\begin{aligned} 2\alpha^2 - e_1\alpha - e_2\alpha - 2\alpha\sqrt{(\alpha - e_1)(\alpha - e_2)} &= (\alpha^2 - e_1\alpha) + (\alpha^2 - e_2\alpha) - 2\alpha\sqrt{(\alpha - e_1)(\alpha - e_2)} \\ &= \left(\sqrt{\alpha(\alpha - e_1)} - \sqrt{\alpha(\alpha - e_2)}\right)^2. \end{aligned}$$

So it suffices to show $\sqrt{\alpha} \in L_P$. Indeed, $\alpha(\alpha - e_1)(\alpha - e_2) = \beta^2$, so

$$\sqrt{\alpha(\alpha - e_1)(\alpha - e_2)} = \pm\beta \in \mathbb{Q}.$$

Dividing by $\sqrt{(\alpha - e_1)(\alpha - e_2)} \in L_P$, we see $\sqrt{\alpha} \in L_P$.

The above calculation shows we can write the roots of $g(x + \alpha)$ as

$$\pm\sqrt{(\alpha - e_1)(\alpha - e_2)} \pm \left(\sqrt{\alpha(\alpha - e_1)} - \sqrt{\alpha(\alpha - e_2)}\right).$$

From here, it is easy to see that $\sqrt{\alpha - e_1}$ and $\sqrt{\alpha - e_2}$ are in the splitting field of g, so the splitting field of g contains L_P. This proves the first part of the claim.

Now let $Q = (x, y) \in E(\overline{\mathbb{Q}})$ be a point such that $2Q = P = (\alpha, \beta)$. We have shown $x \in L_P$. To prove the second part of the claim, we need to show $y \in L_P$. We will show $y \in \mathbb{Q}(x)$. We know $\mathbb{Q}(x)$ is the fixed field of the subgroup $\{\sigma \in G \mid \sigma(x) = x\}$. We want to show that if $\sigma(x) = x$ then $\sigma(y) = y$. Since $y^2 = x(x - e_1)(x - e_2)$ we have $\sigma(y)^2 = y^2$. So $\sigma(y) = \pm y$. Suppose for contradiction $\sigma(y) = -y$. This means $Q^\sigma = -Q$. Since the multiplication by 2 map is given by a rational function with coefficients in $\mathbb{Q}$, it commutes with σ. So we have

$$P = P^\sigma = (2Q)^\sigma = 2(Q^\sigma) = -2Q = -P.$$

If P does not have order 2, we have reached a contradiction.

If P has order 2, we have α is either 0, e_1 or e_2. If $\alpha = 0$, the roots of $g(x)$ are $\pm\sqrt{e_1e_2}$ (each occurring with multiplicity 2). We have $L_P = \mathbb{Q}(\sqrt{-e_1}, \sqrt{-e_2})$. Plugging $x = \sqrt{e_1e_2}$ into $y^2 = x(x - e_1)(x - e_2)$ we get

$$y^2 = 2e_1e_2\sqrt{e_1e_2} - (e_1 + e_2)e_1e_2 = (e_1\sqrt{-e_2} + e_2\sqrt{-e_1})^2.$$

So $y \in L_P$. Similarly, for $x = -\sqrt{e_1e_2}$ we get

$$y^2 = (e_1\sqrt{-e_2} - e_2\sqrt{-e_1})^2,$$

so again $y \in L_P$. The cases $\alpha = e_1$ and $\alpha = e_2$ are similar and are left as exercises for the reader. □

Before we show the compositum of all the L_P is a finite extension of $\mathbb{Q}$ we use this proposition to compute the torsion subgroup for an example.

Example 6.5. Let $E : y^2 = f(x) = x(x - 16)(x - 25) = x^3 - 41x^2 + 400$. Then $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Proof. First note that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = E[2] \subset E(\mathbb{Q})_{\text{tors}}$ because all the roots of f are rational. We find $\Delta = 2^8 3^4 5^4$. So E has good reduction at 7. Reducing mod 7 we obtain the curve $y^2 = \tilde{f}(x) = x^3 + x^2 + x$ over $\mathbb{F}_7$. The squares in $\mathbb{F}_7$ are $0, 1, 2, 4$. We compute the values $f(x)$ for all $x \in \mathbb{F}_7$ and see which ones are squares. We obtain

$$\tilde{E}(\mathbb{F}_7) \cong \{\mathcal{O},\ (0,0),\ (2,0),\ (4,0),\ (3,\pm 2),\ (5,\pm 1)\}.$$

So $|\tilde{E}(\mathbb{F}_7)| = 8$. This means $E(\mathbb{Q})_{\text{tors}}$ is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or a group of order 8. We claim $E(\mathbb{Q})_{\text{tors}}$ has order 8, which we show by finding a point of order 4. Given a point $(\alpha, 0) \in E(\mathbb{Q})$ of order 2, it suffices to find $Q = (x, y)$ so that $2Q = (\alpha, 0)$. We know from the previous proposition that $Q \in E(L_P)$ where $L_P = \mathbb{Q}(\sqrt{\alpha - 16}, \sqrt{\alpha - 25})$. Taking $\alpha = 25$ we get $L_P = \mathbb{Q}$. So $E(\mathbb{Q})_{\text{tors}}$ contains a point of order 4 and has $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ as a subgroup. We get $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. □

Now we show the compositum of all the L_P is a finite extension. Note that since $\alpha(\alpha - e_1)(\alpha - e_2)$ is a square in $\mathbb{Q}$ we can write

$$L_P = \mathbb{Q}(\sqrt{\alpha - e_1}, \sqrt{\alpha - e_2}) = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\alpha - e_1}).$$

We want to show L is given by adjoining finitely many square roots to $\mathbb{Q}$. To prove this, we need a preliminary lemma.

Lemma 6.6. *Let $(x, y) \in E(\mathbb{Q})$. Then $x = m/e^2$ and $y = n/e^3$ for some $m, n, e \in \mathbb{Z}$ with m and n both prime to e.*

Proof. To start, write $x = m/M$ and $y = n/N$ in lowest terms. Plugging these into $y^2 = x^3 + ax^2 + bx + c$ and clearing denominators, we obtain

$$n^2M^3 = N^2(m^3 + am^2M + bmM^2 + cM^3). \tag{6.7}$$

So $N^2 \mid n^2M^3 \implies N^2 \mid M^3$ since n is prime to N.

Next, we claim $M^3 \mid N^2$. Note that M divides both sides of (6.10) but M cannot divide the second term on the right, since this would imply $M|m^3$ but $\gcd(m, M) = 1$. So $M|N^2$. Now note that

$$N^2m^3 = n^2M^3 - N^2M(am^2 + bmM + cM^2). \tag{6.8}$$

So since $M \mid N^2$ we see that M^2 divides both terms on the right and thus $M^2|N^2m^3$. Since M and m are coprime we get $M^2 \mid N^2$ and consequently $M \mid N$. By (6.8) we see that M^3 divides both terms on the left and so $M^3|N^2m^3 \implies M^3 \mid N^2$. So we have shown $M^3 = N^2$ and $M \mid N$. Let $e = N/M$. Then

$$e^2 = N^2/M^2 = M^3/M^2 = M \quad \text{and} \quad e^3 = N^3/M^3 = N^3/N^2 = N.$$

So we see that $x = m/e^2$ and $y = n/e^3$ as desired. □

We use this to prove the following key result.

Lemma 6.9. *Let $E : y^2 = x^3 + ax^2 + bx$. Let $(x, y) \in E(\mathbb{Q})$. Then modulo squares there are only finitely many possibilities for the value of x.*

Proof. By the previous lemma, $x = m/e^2$ and $y = n/e^3$ for some $m, n, e \in \mathbb{Z}$. We are interested in the squarefree part of m. Plugging into the equation for E and clearing denominators, we get

$$n^2 = m(m^2 + ame^2 + be^4). \tag{6.10}$$

So the right hand side is a square. Let $d = \gcd(m, m^2 + ame^2 + be^4)$. Then d is precisely the squarefree part of m. Since $d \mid (m^2 + ame^2 + be^4)$ and $d \mid m$ we get $d \mid be^4$. Since $\gcd(m, e) = 1$ we get $d|b$. So the primes dividing x when viewed as an element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ must be among the finitely many primes that divide b. □

This tells us that $\mathbb{Q}(\sqrt{\alpha})$ is contained in the extension of $\mathbb{Q}$ obtained by adjoining $i = \sqrt{-1}$ and the square roots of the finitely many primes dividing e_1e_2. (We are working with the curve $E : y^2 = x(x - e_1)(x - e_1) = x^3 - (e_1 + e_2)x^2 + e_1e_2x$

and the previous lemma refers to primes dividing the coefficient of x.) But since $L_P = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\alpha - e_1})$ we also need to deal with $\mathbb{Q}(\sqrt{\alpha - e_1})$. Consider the elliptic curve $E' : y^2 = x(x + e_1)(x + e_1 - e_2)$. If α is the x-coordinate of a point on E then $\alpha - e_1$ is a point on the curve E'. By Lemma 6.9, there are only finitely many primes dividing the squarefree part of $\alpha - e_1$. More precisely, they are among the finitely many primes dividing $e_1^2 - e_1e_2$, which is the coefficient of x in the equation for E'. So L is a finite extension, which completes the proof that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite when $E[2] \subset E(\mathbb{Q})$.

Before we generalize this to the case where $E[2] \not\subset E(\mathbb{Q})$, we can use the above argument to get a bound on the rank of the finitely generated abelian group $E(\mathbb{Q})$.

Proposition 6.11. *Let E be given by $y^2 = x(x - e_1)(x - e_2)$ for $e_1, e_2 \in \mathbb{Q}$ and let r be the rank of $E(\mathbb{Q})$. Then $r \leq 2M$, where M is the number of distinct prime factors of $e_1e_2(e_1^2 - e_1e_2)$.*

Proof. By the classification theorem of finitely generated abelian groups, we have $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where r is the rank of $E(\mathbb{Q})$. But we assumed $E[2] \subset E(\mathbb{Q})$ so we have

$$E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \bigoplus_{i=1}^{n} (\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}) \oplus \mathbb{Z}^r,$$

where each $p_i \geq 3$. Thus,

$$2E(\mathbb{Q}) \cong (2\mathbb{Z}/2\mathbb{Z})^2 \oplus \bigoplus_{i=1}^{n} (2\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}) \oplus 2\mathbb{Z}^r.$$

Taking the quotient, we get

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^r. \tag{6.12}$$

From the proof of Proposition 5.13, we know $E(\mathbb{Q})/2E(\mathbb{Q})$ is isomorphic to a subgroup of $\text{Hom}(\text{Gal}(L/\mathbb{Q}), E[2])$. Since $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ this can be identified with

$$\text{Hom}(\text{Gal}(L/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \text{Hom}(\text{Gal}(L/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}) \times \text{Hom}(\text{Gal}(L/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z}).$$

We claim $|\text{Hom}(\text{Gal}(L/\mathbb{Q}), \mathbb{Z}/2\mathbb{Z})| = 2^N$ for some N. We know $\text{Gal}(L/\mathbb{Q})$ is given by adjoining finitely many square roots to $\mathbb{Q}$, so we have $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^N$ for some N. We have $|\text{Hom}((\mathbb{Z}/2\mathbb{Z})^N, \mathbb{Z}/2\mathbb{Z})| = 2^N$ because a homomorphism is determined by where it sends the N generators of $(\mathbb{Z}/2\mathbb{Z})^N$ and each generator can go to two possible places. So $|\text{Hom}(\text{Gal}(L/K), E[2])| = 2^{2N}$. By (6.12) we have $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2}$. So $r \leq 2(N - 1)$.

By the proof of Lemma 6.9, we have that $N - 1$ is bounded by the number of primes dividing e_1e_2 and $e_1^2 - e_1e_2$. The reason we have $N - 1$ instead of N is that L might contain $i = \sqrt{-1}$ in addition to the square roots of the primes dividing $e_1e_2(e_1^2 - e_1e_2)$. Thus $N - 1 \leq M$, which completes the proof. □

7. Weak Mordell-Weil for $m = 2$ and $K = \mathbb{Q}$

Next we present an argument for why the theorem is true even if we do not make the assumption that the 2-torsion is contained in $E(\mathbb{Q})$. As usual, we have $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ with a, b, $c \in \mathbb{Q}$.

For now, we view E as an elliptic curve over an arbitrary number field K. We consider the ring $R = K[\xi] = K[x]/(f(x))$. We also consider its group of units $R^\times$,

which consists of the cosets whose representatives are relatively prime to $f(x)$. By the Chinese Remainder Theorem we have

$$R \cong \bigoplus_{i=1}^{n} K[x]/(f_i(x)),$$

where each f_i is irreducible over K and n is either 1, 2 or 3. Furthermore, the units of R are just the units of the individual factors on the right.

We construct a homomorphism $\phi : E(K) \to R^\times/(R^\times)^2$ with kernel $2E(K)$. If $P = (\alpha, \beta)$ does not have order 2 (meaning $\beta \neq 0$) then we let

$$\phi(P) = \alpha - x \mod f(x),$$

viewed of course as an element of $R^\times/(R^\times)^2$. Since α is not a root of f this is indeed a unit. Now if $P = (\alpha, 0) \in E(K)$ then write $f(x) = (x - \alpha)g(x)$. So

$$R \cong K[x]/(x - \alpha) \oplus K[x]/(g(x)),$$

where the first component is isomorphic to K. We let

$$\phi(P) = (f'(\alpha), \alpha - x \mod g(x)),$$

again modulo squares. Since f is separable, we must have $f'(\alpha) \neq 0$, so $\phi(P)$ is indeed a unit.

Proposition 7.1. *The map ϕ is a homomorphism.*

Proof. First we show ϕ sends inverses to inverses. Note that $\phi(P) = \phi(-P)$ since the definition of ϕ only depends on the x-coordinate of P. So $\phi(P)\phi(-P) = 1$ in $R^\times/(R^\times)^2$. Thus, it suffices to show that if $A = (x_1, y_1), B = (x_2, y_2), C = (x_3, y_3)$ are collinear then $\phi(A)\phi(B)\phi(C) = 1$. First note that if $x_1 = x_2$ then the collinearity condition forces $B = -A$ and $C = \mathcal{O}$. We then have $\phi(A)\phi(-A)\phi(\mathcal{O}) = 1$ modulo squares. So now take A, B, C to be distinct. If none of them have order 2 then we have

$$\phi(A)\phi(B)\phi(C) = (x_1 - x)(x_2 - x)(x_3 - x) \mod f(x).$$

As in (2.7), the collinearity condition means there are $\lambda, \nu \in K$ with

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{7.2}$$

Reducing the equation mod $f(x)$ shows $\phi(A)\phi(B)\phi(C) = 1$.

Now say $y_1 = 0$ and $y_2, y_3 \neq 0$. Then we need to look at $\phi(A)\phi(B)\phi(C)$ one factor at a time. In the first factor, we have

$$\phi(A)\phi(B)\phi(C) = f'(\alpha)(x_2 - x)(x_3 - x) = (x_2 - x)^2(x_3 - x)^2.$$

For the second factor, we have $\phi(A) = \alpha - x \mod g(x)$. Reducing (7.2) mod $g(x)$ we get the desired result.

The final case is when A, B, C all have order 2. (If f has two rational roots, it must have three.) Then $R \cong K \oplus K \oplus K$. Using a similar argument to the one above, it is easy to see that $\phi(A)\phi(B)\phi(C) = (f'(x_1)^2, f'(x_2)^2, f'(x_3)^2)$. □

Proposition 7.3. *The kernel of ϕ is $2E(K)$.*

Proof. For this proof we will assume E is given by $y^2 = x^3 + ax + b$, which we can always do after applying a change of variables. From the previous proposition, we have $\phi(2P) = \phi(P)^2 = 1$ for all P. So $2E(K) \subset \ker \phi$. Conversely, suppose P is such that $\phi(P) = 1$. We want to find $Q = (h, t)$ so that $2Q = P$. Geometrically,

this means we have some line $y = \lambda x + \nu$ that intersects the curve E transversally at $P = (\alpha, \beta)$ and tangentially at $Q = (h, t)$. So we want

$$f(x) - (\lambda x + \nu)^2 = (x - \alpha)(x - h)^2. \tag{7.4}$$

But we need to work in the ring $K[\xi] = K[x]/(f(x))$ since that is where the image of ϕ lies. So we show

$$(\lambda\xi + \nu)^2 = (\alpha - \xi)(\xi - h)^2. \tag{7.5}$$

Now $\alpha - \xi = \phi(P) = 1$. This means $\alpha - \xi$ is a square in $K[\xi]$. The elements in this quotient ring are represented by polynomials of degree less than 2. So we have

$$\xi - \alpha = (\alpha_2\xi^2 + \alpha\xi + \alpha_0)^2$$

for some $\alpha_i \in K$. Note that $\alpha_2 \neq 0$. (If not, the linear independence of $1, \xi, \xi^2$ gives a contradiction.) We also have

$$(\alpha_2\xi^2 + \alpha_1\xi + \alpha_0)(-\alpha_2\xi + \alpha_1) = e\xi + f,$$

for some $e, f \in K$, where we use $\xi^3 = -a\xi - b$ or $f(\xi) = 0$ in $K[\xi]$. Now squaring, we get

$$(e\xi + f)^2 = (\alpha - \xi)(-\alpha_2\xi + \alpha_1)^2.$$

Dividing by α_2^2 we get

$$(\lambda\xi + \nu)^2 = (\alpha - \xi)(h - \xi)^2$$

for some h, λ, $\nu \in K$. This means $(\lambda x + \nu)^2 - (\alpha - x)(h - x)^2$ is a multiple of $f(x)$. We actually have $(\lambda x + \nu)^2 - (\alpha - x)(h - x)^2 = f(x)$ since both sides are monic cubic polynomials. So the line $y = \lambda x + \nu$ intersects the elliptic curve E at (α, β) or $(\alpha, -\beta)$ and is tangent to the curve at (h, t) for some t. We get $(\alpha, \pm\beta) + 2(h, t) = \mathcal{O}$. So $P = 2Q$ where $Q = (h, \pm t)$. So $\ker\phi \subset 2E(K)$. □

By the first isomorphism theorem, we are left to show $\phi(E(K)) \subset R^\times/(R^\times)^2$ is finite. We consider the following special case first.

Theorem 7.6. *Let $E : y^2 = f(x)$ be an elliptic curve such that $f(x)$ has three rational roots, i.e. $E[2] \subset E(\mathbb{Q})$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. We need to show that $\phi(E) \subset R^\times/(R^\times)^2$ is finite. Since $E[2] \subset E(\mathbb{Q})$ we have

$$R = \mathbb{Q}[x]/(f(x)) \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}.$$

So we think of the image of ϕ as living in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Since there are finitely many points of order 2, we do not need to consider their image. If $P = (\alpha, \beta)$ is not a point of order 2, then $\phi(P)$ is simply α viewed as an element of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. By Lemma 6.9, we know there are only finitely many possible values for α modulo squares, and this completes the proof. □

To relate this back to the proof given in the previous section, we consider the question of when it is possible to divide a point P by 2, that is find $Q \in E(\mathbb{Q})$ such that $2Q = P$. We consider ϕ acting on the points of the form (α, β) where $\beta \neq 0$. We know that a point is divisible by 2 precisely when it's in the kernel of ϕ by Proposition 7.3. Note that

$$\phi(P) = (\alpha - x,\, \alpha - x,\, \alpha - x) \subset \mathbb{Q}[x]/(x - e_1) \oplus \mathbb{Q}[x]/(x - e_2) \oplus \mathbb{Q}[x]/(x - e_3).$$

Identifying each of these factors with $\mathbb{Q}$ via the maps $x \mapsto e_i$ we get

$$\phi(P) = (\alpha - e_1,\, \alpha - e_2,\, \alpha - e_3).$$

So P is divisible by 2 precisely when each of these coordinates is a square in $\mathbb{Q}$. Now let $L = \mathbb{Q}(\sqrt{\alpha - e_1}, \sqrt{\alpha - e_2}, \sqrt{\alpha - e_3})$. Since $(x - e_1)(x - e_2)(x - e_3)$ is a square in $\mathbb{Q}$, we get L by adjoining only two of the three square roots. Then L is the field extension in which the coordinates of Q lie, and this is precisely what we saw in the previous section.

There is still more to be said about why we first considered the injection

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathrm{Hom}(G, E[2])$$

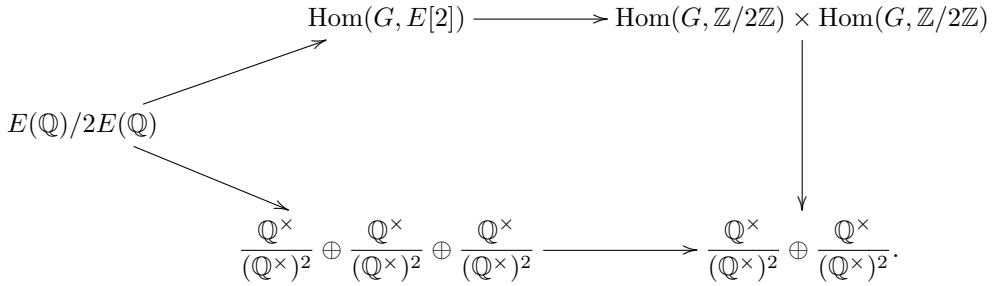
in Sections 5 and 6 and then

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow R^\times/(R^\times)^2$$

in this section. Recall that elements of $\mathrm{Hom}(G, E[2])$ correspond to extensions of $\mathbb{Q}$ contained in biquadratic extensions. In Section 5, we noted more generally $\mathrm{Hom}(G, E[m])$ corresponds to extensions L/K with $\mathrm{Gal}(L/K) \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. The key fact used was $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Setting $m = 2$ and $K = \mathbb{Q}$ gives the desired result. In this special case, the relation between $\mathrm{Hom}(G, E[2])$ and biquadratic extensions of $\mathbb{Q}$ stems from $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. These groups are not canonically isomorphic; choosing an isomorphism amounts to choosing two generators of $E[2]$, where any two nontrivial elements of $E[2]$ will do. This isomorphism induces an isomorphism $\mathrm{Hom}(G, E[2]) \cong \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$.

In the argument given in this section, we instead have an injection of $E(\mathbb{Q})/2E(\mathbb{Q})$ into $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Each of the three factors corresponds to the three points of order 2. We can choose two of them and get a map into $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This is analogous to choosing generators for $E[2]$ as we did in the previous paragraph.

From Kummer theory (see Remark 5.9), we have $\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Now choose two generators of $E[2]$. As mentioned before, this choice induces a map $\mathrm{Hom}(G, E[2]) \to (\mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}))^2$ and a map $(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3 \to (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^2$. Then the following diagram commutes



When the 2-torsion is not entirely contained in $E(\mathbb{Q})$, we need to do more work to see that $\phi(E)$ is finite. We use two standard finiteness theorems from algebraic number theory: the finiteness of the class number and Dirichlet's unit theorem.

We want to show $\phi(E)$ is finite. We don't need to worry about the image of the 2-torsion, since it is a finite set. So suppose $P = (\alpha, \beta) \in E(\mathbb{Q})$ with $\beta \neq 0$. By Lemma 6.6, we have $\alpha = m/e^2$ in lowest terms. Let θ be a fixed root of $f(x)$. Write $f(x) = (x - \theta)g(x)$. We will consider the image of ϕ in the component of $\mathbb{Q}[x]/(f(x))$ corresponding to $K := \mathbb{Q}(\theta)$. In this component, we have $\phi(P) = m/e^2 - \theta$. We

need an analogue of Lemma 6.9, where we show that there are only finitely many coset representatives for such elements when viewed as elements of $K^\times/(K^\times)^2$.

Lemma 7.7. *We have $m/e^2-\theta = u\gamma\tau^2$, where u is a unit, γ is an algebraic integer from some finite set and $\tau \in K$.*

It suffices to show $m - e^2\theta = u\gamma\tau^2$, where γ is an algebraic integer from some finite set and $\tau \in K$. This formulation has the advantage that $m - e^2\theta$ is an algebraic integer. We know

$$\left(\frac{m}{e^2} - \theta\right) g\left(\frac{m}{e^2}\right) = f\left(\frac{m}{e^2}\right) = \left(\frac{r}{s}\right)^2$$

where $\beta = r/s$ in lowest terms. As in the proof of Lemma 6.9, our next step is to clear denominators. We multiply both sides by s^2. We also multiply both sides by e^4 because $g(m/e^2)$ is not necessarily an algebraic integer but $e^4 g(m/e^2)$ is. So we get

$$e^6 r^2 = s^2(m - e^2\theta)g(m/e^2)e^4. \tag{7.8}$$

This is the analogue of (6.10) in Lemma 6.9. Since the left hand side is a square, so is the right hand side. Our next step in Lemma 6.9 was to take the gcd d of the two non-square factors. This motivates us to define the ideal

$$I(P) = (m - e^2\theta, g(m/e^2)e^4).$$

In Lemma 6.9 we showed that $d|b$, hence there were only finitely many possibilities for d. We do something analogous now.

Proposition 7.9. *We have $I(P) \supset (g(\theta))$.*

Proof. We have $g(x) - g(\theta) = (x - \theta)t(x)$ where $t(x)$ is a linear polynomial with coefficients in $\mathbb{Z}[\theta]$. Setting $x = m/e^2$ and multiplying by e^4 gives

$$e^4 g(m/e^2) - e^4 g(\theta) = e^2(m - e^2\theta)t(m/e^2).$$

So $e^4 g(\theta) \in I(P)$. Next, we have

$$\begin{aligned} g(\theta)x^2 - g(x)\theta^2 &= g(\theta)(x^2 - \theta^2) + \theta^2(g(\theta) - g(x)) \\ &= (x - \theta)t(x) \end{aligned}$$

for some polynomial t. Setting $x = m/e^2$ and multiplying by e^4, we get

$$m^2 g(\theta) - \theta^2 e^4 g(m/e^2) = e^2(m - e^2\theta)t(m/e^2).$$

This means $m^2 g(\theta) \in I(P)$. So $I(P) \supset (m^2 g(\theta), e^4 g(\theta)) \supset (g(\theta))$, where the latter inclusion is due to the fact that m and e^2 are coprime. □

Proof of Lemma 7.7. Recall our goal is to show $m - e^2\theta = u\gamma\tau^2$ where u is a unit, γ is an algebraic integer from some finite set and $\tau \in K$. We do this by showing $(m - e^2\theta) = (\gamma\tau^2)$.

First we relate $(m-e^2\theta)$ to $I(P)$. We write $(m-e^2\theta) = I(P)A$ and $(e^4 g(m/e^2) = I(P)B$ for some coprime ideals A and B. From (7.8) we get $s^2 I(P)AI(P)B$ is a square. Since A and B are coprime, we get A is a square. So we can write $(m - e^2\theta) = I(P)C^2$ for some ideal C.

Now we need to show $I(P)C^2 = (\gamma\tau^2)$ where γ is an algebraic integer from some finite set and $\tau \in K$. By the previous proposition, we know $\{I(P) \mid P \in E(\mathbb{Q})\}$ is a finite set. We also need to consider how C changes as P ranges through $E(\mathbb{Q})$. We use the finiteness of the class number. Let $C_1, \ldots, C_n$ be a set of representatives for

the ideal classes of $\mathcal{O}_K$, the ring of integers of the number field K. Then $C \sim C_i$ for some i. By definition, this means we have $\rho_1, \rho_2 \in \mathcal{O}_K$ with $(\rho_1)C = (\rho_2)C_i$. Setting $\tau = \rho_2/\rho_1$ we get $C = (\tau)C_i$. Then we get

$$(m - e^2\theta) = I(P)C^2 = I(P)(\tau^2)C_i^2.$$

This means the ideal $I(P)C_i^2$ is principal. We write $I(P)C_i^2 = (\gamma)$ where $\gamma \in \mathcal{O}_K$. Since there are finitely many $I(P)$ and finitely many C_i there are only finitely many possibilities for γ. Writing $(m - e^2\theta) = (\gamma\tau^2)$ finishes the proof. □

Theorem 7.10. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

Proof. From Propositions 7.1 and 7.3 we have a homomorphism $\phi : E(\mathbb{Q}) \to R^\times/(R^\times)^2$ with kernel $2E(\mathbb{Q})$. By the first isomorphism theorem, it suffices to show $\phi(E(\mathbb{Q}))$ is finite. If $P = (m/e^2, \beta)$ does not have order dividing 2, we have $\phi(P)$ is the coset $m/e^2 - x$ modulo $(R^\times)^2$. Let θ be a root of f and let $K = \mathbb{Q}(\theta)$ be a component of the ring $\mathbb{Q}[x]/(f(x))$. By the previous lemma, $m/e^2 - x$ has coset representative $u\gamma$ for some unit u. By Dirichlet's unit theorem, the group of units is finitely generated, so $u = u_1^{m_1} \dots u_n^{m_n}$ for some units u_i and integers m_i. We can assume each m_i is either 0 or 1 since we are working modulo squares. Since γ is from a finite set of algebraic integers, this shows $m/e^2 - x$ has finitely many coset representatives in $R^\times/(R^\times)^2$, which proves the theorem. □

To conclude, we briefly discuss the ideas behind generalizing this argument to elliptic curves over any number field K. The later proofs in this section heavily rely on the fact that rational points on E have x-coordinates of the form m/e^2 for $m, e \in \mathbb{Z}$. However, if E is an elliptic curve over a number field K whose ring of integers $\mathcal{O}_K$ is a unique factorization domain, we can copy the proof of Lemma 6.6 to get that x-coordinates of points in $E(K)$ have the form m/e^2 for $m, e \in \mathcal{O}_K$. Then we can repeat the arguments given above to show $E(K)/2E(K)$ is finite. In the general case, we can invert finitely many ideals in $\mathcal{O}_K$ to make it into a principal ideal domain, and hence a UFD. Generalizing the above argument then requires the S-unit theorem. We also mention that it is possible to deduce $E(K)$ is finitely generated from the finiteness of $E(K)/2E(K)$ using methods similar to those in Section 5. However, there is the additional difficulty of developing a general theory of height functions on number fields, since the definitions in the previous section do not make sense when $\mathcal{O}_K$ is not a UFD. This is done in Chapter VIII of [4].

Acknowledgments. I would like to thank my mentor, Karl Schaefer, for teaching me about elliptic curves and for helping me extensively with this paper. I would like to thank Matt Emerton for teaching me about elliptic curves and suggesting topics to study and write about. I would also like to thank Peter May for organizing the REU and reviewing this paper.

References

[1] David S. Dummit, Richard M. Foote. *Abstract Algebra.* John Wiley and Sons. 2004.
[2] Kenneth Ireland, Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer. 1990.
[3] Joseph H. Silverman, John T. Tate. *Rational Points on Elliptic Curves, Second Edition.* Springer. 2015.
[4] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, Second Edition.* Springer. 2008.