MORDELL-WEIL AND BILLING-MAHLER THEOREMS

AGNIV SARKAR

Abstract. The goal of this expository paper is to provide exposition and an understanding of two beautiful theorems to describe elliptic curves, specifically the Mordell-Weil Theorem and the Billing-Mahler theorem. This paper assumes a strong understanding of group theory, a basic understanding of number theory, modular arithmetic, and geometry, and a very light understanding of linear algebra.

Contents

Date: Summer 2022.

1. Introduction

The solutions to polynomial equations, especially those of the rational form, have been under great interest for over 1800 years, starting with Diophantine equations. Rational solutions are generally of the form $(x_1, x_2, \ldots, x_n) \in \mathbb{Q}$. In order to find rational solutions for linear equations, one can utilize linear algebra to solve them incredibly fast (with a time of $O(n^{2.332})$ [1], where n is the number of unknown variables). Quadratic equations with two variables are also well understood, as they can be solved with quadratic reciprocity and Hensel's Lemma [2].

However, there is some complexity that appears when one aims to find rational solutions for cubics defined in three variables. (Note: this type of increasing dimensions adding a larger amount of complexity is very common within math!). This paper will focus specifically on elliptic curves, as they have an addition law and group structure that leads to interesting results. It is interesting to look at how elliptic curves are related to ellipses.

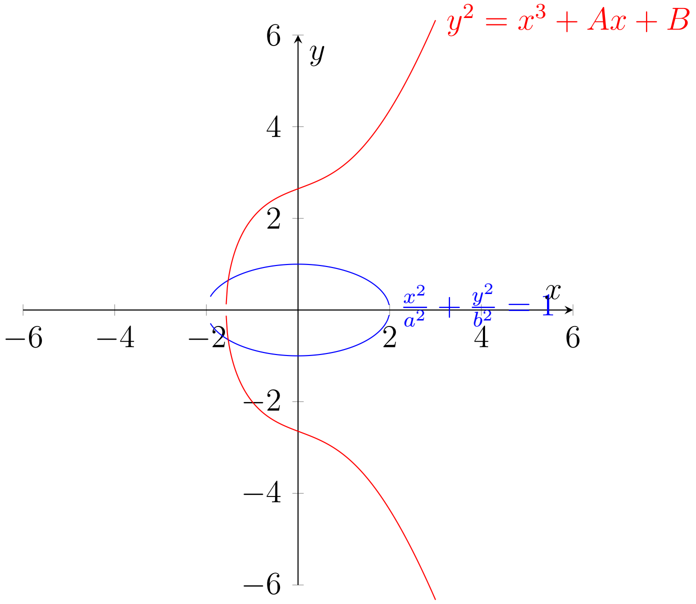

Figure 1. Example of Ellipse and Elliptic Curve

Ellipses are conic sections, and are given by quadratic equations instead of the cubics that we aim to study. The reason that these curves carry on the name is due to how these curves appeared when mathematicians wanted to compute the circumference of an ellipse [3].

An example would be starting with the equation for an ellipse (such that $b < a$).

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

In order to find the circumference, we have to integrate and use the arc length formula.

$$y = f(x) = \pm b\sqrt{1 - \frac{x^2}{a^2}}$$

$$f'(x) = \mp \frac{bx}{a^2\sqrt{1 - \frac{x^2}{a^2}}} = \mp \frac{rx}{\sqrt{a^2 - x^2}} \text{ where } r = \frac{b}{a} < 1$$

$$4\int_0^a \sqrt{1 + f'(x)^2} dx = 4\int_0^a \sqrt{1 + \frac{r^2x^2}{a^2 - x^2}} dx$$

Substitute $x = at$ and $e = \sqrt{1 - r^2}$ to get

$$4a\int_0^1 \sqrt{\frac{1 - e^2t^2}{1 - t^2}} dx.$$

This is an elliptic integral. The integrand $u(t)$ satisfies

$$u^2(1 - t^2) = 1 - e^2t^2$$

This equation defines an elliptic curve. This is how the two different equations share the same name.

2. Group Structure

An elliptic curve is a cubic curve that can be defined over any field K, such as $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$. This curve naturally forms a group structure through a geometrical definition. Over a finite field, the group is similarly finite.

Definition. An elliptic curve E is a nonsingular curve over a field K given by the set

$$E = \{(x, y) : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathbb{O}\}$$

for some constants a, b, c in K such that the discriminant is nonzero, and the point $\mathbb{O}$ is the point at infinity.

The requirements for an elliptic curve are simple to understand. For the curve to be nonsingular, E has distinct roots. Now we will understand the group structure. In order for elliptic curves to form a group, they must have an addition function and an identity element. We shall define both.

Definition. On a curve, we define the addition of any two given points, P and Q to be $P+Q$ such that it is the negative of the third intersection of the line drawn through P and Q and the cubic. The composition of P upon P, or $P + P = 2P$, is the negative of the intersection of the tangent line to the curve at P to the curve.

Why the third intersection? This turns out to be a special case of Bezout's Theorem, which states that the intersections of two different curves of degree m and n contain mn points. So, the line and the curve should have 3 points.

Side note, the negative of a point $P = (x, y)$ is simply $-P = (x, -y)$. Now that we have an addition function, we need an identity element. We should then consider the question, what does $P + (-P)$ give us if $P = (a, 0)$ and $P \in E$?

Clearly, it does not intersect the line at a third point. Since there is no point in the plane that corresponds to it, we shall define it to be the point at infinity, $\mathbb{O}$. In other words, $\mathbb{O}$ is a point on every vertical line.

So, let us write out the abelian group structure so far.

(1) $P + \mathbb{O} = \mathbb{O} + P = P$
(2) $P + (-P) = \mathbb{O}$
(3) $P + (Q + R) = (P + Q) + R$
(4) $P + Q = Q + P$

Another thing that is caused by our group law is that for points $P, Q, R \in E$, they are collinear if and only if $P + Q + R = \mathbb{O}$. These can all be proven with algebra relatively simply (except for (3)) but the geometrical understanding is key. The proof of (3) however is a very long computation with explicit formula. A proof can be found within [4].

2.1. Addition Law.

Let us get a closed formula for the addition law. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and both are on some elliptic curve E, then we must first find the line intersecting them. This would be

$$y = mx + b,$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + 2ax + b}{2y_1} & \text{if } P_1 = P_2 \end{cases} \text{ and } b = y_1 - mx_1$$

Now, we must find the third intersection of E with this line. This now becomes

$$(mx + b)^2 = x^3 + ax^2 + bx + c.$$

As we know some roots, we can write

$$x^3 + ax^2 + bx + c - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3)$$

and solve for x_3. This simplifies nicely into

$$x_3 = m^2 - x_1 - x_2 \text{ and } y_3 = mx_3 + b$$

so that we get that

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = (m^2 - x_1 - x_2, -mx_3 - b) = (x_3, -y_3).$$

We now have an algebraic form of the addition rule. Let us define one more thing.

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

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

which we will denote as $E(K)$.

The set of $\mathbb{Q}$-rational points on E is equivalent to saying the set of rational points on E. If we already have points belonging to $E(\mathbb{Q})$, then we need to figure out a procedure to find other ones. We have already seen the algebraic expansion of the addition law, meaning that if we have points $P, Q \in E(\mathbb{Q})$, then we know $-P, -Q, P + Q, -(P + Q), (-P) + Q, P + (-Q)$ are also in $E(\mathbb{Q})$.

It is pretty elegant how this geometrical definition translated into an algebraic one, meaning we can carry the + function to other fields. I will introduce one other way to define curves.

2.2. **Projective Plane.**

Definition. A projective curve is the set of zeros of a homogeneous polynomial of three variables: $F(x, y, z) = 0$. We will assume that F has coefficients in $\mathbb{Z}$. We recall that $F(x, y, z)$ is homogeneous of degree d if $F(kx, ky, kz) = k^d F(x, y, z)$ for all constants k.

This is a curve in three variables, although it is easy to translate a two variable curve into this. Let $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, which lets $f(\frac{X}{Z}, \frac{Y}{Z}) = 0$ be equal to saying $f(X, Y, Z) = 0$. In other words, $F(X, Y, Z) = Z^d f(x, y)$. The reason we need this definition is to make use of the projective plane. We will not touch heavily on this.

Consider the set of all triples $(X, Y, Z) \in \mathbb{C}^3$ excluding the origin point. Then, let's consider the equivalence relation, where a triple (X, Y, Z) is equivalent to $(\lambda X, \lambda Y, \lambda Z)$, or in other words, all lines passing through where the origin would contain equivalent points.

The projective plane, $\mathbb{P}^2$ is the set of equivalence classes of this equivalence relation. This would be written as,

$$\mathbb{P}^2(\mathbb{C}) = \{(X,Y,Z)|X,Y,Z \in \mathbb{C}\}/ = \{[X:Y:Z]\}.$$

In other words, $[1:2:3]$ is the same point as $[-0.5,-1,-1.5]$.

Why is this relevant? Because of the equivalence relation we have, we can always make $[X,Y,Z] = [\frac{X}{Z},\frac{Y}{Z},1]$ given a nonzero Z. So, if $F(X,Y,Z) = 0$ for some nonzero Z, then $(x,y) = (\frac{X}{Z},\frac{Y}{Z})$ is the same as the original curve $f(x,y)$. When $Z = 0$, however, the curve contains points at infinity.

Now let's write what an elliptic curve looks like in the projective plane,

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

We can see now what it means for $Z = 0$. This would leave the equation $0 = X^3$, meaning that the only points on this line are $[0:1:0]$. This is the intersection of the curve with the line at infinity $Z = 0$. This is the point at infinity $\mathbb{O} = [0:1:0]$!

We will now think about how to find rational solutions to this. Elliptic curves are unique due to not having a really clear way of finding rational solutions. The rational root theorem can find solutions for polynomials in one variable, linear equations in two variables always have infinite rational solutions, and quadratics are relatively well-understood by the use of conics. In order to find rational solutions to this, we have to utilize the geometric and algebraic definitions of the group structure.

3. Mordell-Weil Theorem

3.1. **Setup.**

Theorem 1. (Mordell-Weil) For elliptic curves over the rationals $\mathbb{Q}$, the group of rational points is always finitely generated.

Proof. Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $\mathbb{Q}$ with integer coefficients. First, we need to define a height function. Let us define it for a rational point.

Definition. For a rational number $x = \frac{a}{b}$, the height of x is given by

$$\mathcal{H}(x) = \max(|a|,|b|).$$

So, we can see that the set of all rational points who have a height less than a given x is finite. Now, can extend this to an elliptic curve.

Definition. For an elliptic curve E over $\mathbb{Q}$, the height of a rational point $P = (x, y)$ on E is

$$\mathcal{H}(P) = \mathcal{H}(x), \mathcal{H}(\mathbb{O}) = 1.$$

The small height of a point is simply

$$h(P) = \log \mathcal{H}(P),$$

or it is 0 if $\mathcal{H}(P) = 0$, and it is a nonnegative function.

In order to prove Mordell-Weil, we need to prove 4 different things.

- Finiteness Property of $\mathcal{H}$ on $E(\mathbb{Q})$
- Height of P and P_0 where P_0 is some given point on E satisfies $h(P + P_0) \leq 2h(P) + \kappa_0$ where κ_0 depends on a, b, c, P_0.
- Doubling the point increases the height, or $h(2P) \geq 4h(P) - \kappa$ where κ is dependent on a, b, and c.
- Denote $2E(\mathbb{Q})$ to be the subgroup of $E(\mathbb{Q})$ which contains only points of the form $2P$ where $P \in E(\mathbb{Q})$. Then, $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group.

The first says that the set $\{P \in E(\mathbb{Q}) | \mathcal{H}(P) < C\}$, for some given number C is a finite set. This is true simply because of the finiteness property on the rationals, and this is a subset of those numbers. A subset of a finite set is finite.

3.2. Height of $P + P_0$.

Lemma 1. Let P_0 be a fixed rational point of E. There is a constant κ_0 that depends on P_0 and on a, b, and c, so that

$$h(P + P_0) \leq 2h(P) + \kappa_0, \forall P \in E(\mathbb{Q})$$

Proof. First, we must notice that if $(x, y) \in E(\mathbb{Q})$, then we can write x and y in the form

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

where $m, n, e \in \mathbb{Z}$ such that $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$. This is because if we write

$$x = \frac{m}{M} \text{ and } y = \frac{n}{M}$$

in lowest terms with positive denominators, and then we substitute these into E, we get

$$\frac{n^2}{M^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M}$$

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.$$

This shows that $N^2|M^3n^2$, and as $\gcd(n, N) = 1$, $N^2|M^3$. Now we have to prove the converse. Similarly, we see that $M|N^2m^3$, and because $\gcd(m, M) = 1$, then $M|N^2$. If we refer back to the equation, we see that this would mean $M^3|N^2m^3$, so $M^3|N^2$, meaning $M^3 = N^2$. So, let $e = \frac{N}{M}$, which means

$$\begin{aligned} x &= \frac{m}{M} = \frac{m}{\frac{M^3}{M^2}} = \frac{m}{\frac{N^2}{M^2}} = \frac{m}{e^2} \\ y &= \frac{n}{N} = \frac{n}{\frac{N^3}{N^2}} = \frac{n}{\frac{N^3}{M^3}} = \frac{m}{e^3}. \end{aligned}$$

So we can write the rational points on the curve in the given form.

So, given a point $P = (\frac{m}{e^2}, \frac{n}{e^3}) \in E(\mathbb{Q})$, then we can see that

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

We can get better bounds. We want to show that for some constant $K > 0$,

$$|n| \leq K\mathcal{H}(P)^{\frac{3}{2}}, \forall P \in E(\mathbb{Q}).$$

This is relatively simple. Because we know P satisfies the equation defining E, by multiplying that equation by e^6 gives us

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

By taking absolute values and using the triangle inequality, it follows

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq \mathcal{H}(P)^3 + |a|\mathcal{H}(P)^3 + |b|\mathcal{H}(P)^3 + |c|\mathcal{H}(P)^3 \\ &= \mathcal{H}(P)^3(1 + |a| + |b| + |c|). \end{aligned}$$

So, $K = \sqrt{1 + |a| + |b| + |c|}$, meaning we now have a lower and upper bound for $\mathcal{H}(P)$ given a point P.

The rest of the proof, albeit long, is just expansions of formulas and the triangle inequality.

Note that if $P_0 = \mathbb{O}$, then the lemma is trivial, so let us assume that P_0 is not the point at infinity, rather it has the form (x_0, y_0), and similarly, we will only focus on $P \in \{P_0, -P_0, \mathbb{O}\}$. So, let $P = (x, y)$. We write

$$P + P_0 = (\xi, \eta),$$

and so $\mathcal{H}(P) = \mathcal{H}(\xi)$. We need to find the formula for ξ in terms of (x, y) and (x_0, y_0). Through the formula that we derived earlier, we can write

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

Under expansion $y^2 - x^3$ appears in the numerator, and as such we can replace that with $ax2 + bx + c$. Doing this results in

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

where A, B, C, D, E, F, G are rational numbers that simplify the terms of a, b, c, x_0, y_0. We can also say that they are integers by multiplying the numerator and denominator by the least common multiple of A, B, C, D, E, F, G. So, we can assume they are all integers. Because these are independent of x and y, then we can define κ_0 with these variables.

If we substitute x and y into $\frac{m}{e^2}$ and $\frac{n}{e^3}$ respectively, then

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

Now, ξ is represented as an integer over an integer (albeit not necessarily coprime). So,

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

Remember that

$$e \leq \sqrt{\mathcal{H}(P)}, n \leq K\mathcal{H}(P)^{\frac{3}{2}}, \text{ and } m \leq \mathcal{H}(P),$$

where K can be written with terms a, b, and c. We can now use these all and the triangle inequality to show

$$\begin{aligned}|Ane + Bm^2 + Cme^2 + D^e4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq |AK| + |B| + |C| + |D|\mathcal{H}(P)^2 \\ |Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\ &\leq |E| + |F| + |G|\mathcal{H}(P)^2.\end{aligned}$$

This tells us that

$$\mathcal{H}(P+P_0) = \mathcal{H}(\xi) \leq \max(|AK|+|B|+|C|+|D|, |E|+|F|+|G|)\mathcal{H}(P)^2.$$

By taking the logarithm,

$$h(P+P_0) \leq 2h(P) + \log\max(|AK| + |B| + |C| + |D|, |E| + |F| + |G|).$$

Then, $\kappa_0 = \max(|AK| + |B| + |C| + |D|, |E| + |F| + |G|)$ and we have found a constant that only depends on a, b, c and x_0, y_0, independent of x, y.

□

3.3. **Height of $2P$.**

Lemma 2. There is a constant κ, depending on a, b, and c, so that

$$h(2P) \geq 4h(P) - \kappa, \forall P \in E(\mathbb{Q}).$$

Proof. Again, let $P = (x, y)$ and then let $2P = (\xi, \eta)$. Because the set of 2-torsion points is finite, we don't have to consider it (we simply find the maximum possible κ). So, let $2p \neq \mathbb{O}$. Again, we can use our duplication formula to see

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)},$$

and note that $f(x) \neq 0$. This means that ξ is a polynomial over a polynomial, both with integer coefficients, and also these polynomials have no common complex roots. What we now want to show is

$$h(\xi) \geq 4h(x) - \kappa.$$

So now we want to think about the height of a polynomial.

Lemma 3. Let $\Phi(X)$ and $\tau(X)$ be polynomials with integer coefficients and no common complex roots, with the maximum of the degree's being d. Then, there is an integer $R \geq 1$, depending on Φ and τ such that

$$\gcd(n^d \Phi\left(\frac{m}{n}\right), n^d \tau\left(\frac{m}{n}\right))|R.$$

Also, there are constants κ_1 and κ_2 dependent on the polynomials so that for all rational numbers $\frac{m}{n}$ that are not roots of τ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\Phi\left(\frac{m}{n}\right)}{\tau\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Proof. First, note that $n^d\Phi\left(\frac{m}{n}\right), n^d\tau\left(\frac{m}{n}\right) \in \mathbb{Z}$ as the degree of the polynomials are at most d, which makes sense for the greatest common denominator. Without loss of generality, let $\deg(\Phi) = d$ and $\deg(\tau) = e \leq d$. Let $\phi(m, n) = n^d\Phi\left(\frac{m}{n}\right)$ and $\Psi(n, m) = n^d\tau\left(\frac{m}{n}\right)$. Because $\phi(X)$ and $\tau(X)$ have no common roots, they are coprime in the ring $\mathbb{Q}[X]$, which means that we can find two other polynomials $F(X)$ and $G(X)$ such that

$$F(X)\phi(X) + G(X)\psi(X) = 1.$$

Let A be the least common multiple of the denominators of the coefficients of terms within $F(X)$ and $G(X)$, and let D be the maximum degree of F and G. Then, by plugging in $X = \frac{m}{n}$ and multiplying both sides by An^{D+d} we get

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

Let polynomial $\gamma(m,n)$ be the greatest common divisor of $\phi(m,n)$ and $\Psi(m,n)$. Then, we can see that $\gamma | An^{D+d}$. We can also see that since $\gamma | \phi(m,n)$, it also divides

$$An^{D+d-1}\phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + \ldots + Aa_d n^{D+2d-1}.$$

where a_i is the coefficient of the term X^{d-i} in $\Phi(X)$'s expansion. What this then tells us is that $\gamma | Aa_0 m^d n^{D+d-1}$, as all the other terms are divisible by An^{D+d}. So,

$$\gamma | \gcd(An^{D+d}, Aa_0 m^d n^{D+d-1}),$$

and as $\gcd(m,n) = 1$, we can see that $\gamma | Aa_0 n^{D+d-1}$. Notice that we have decrease the exponent of n in that term. Our end goal is to get rid of it. So, we can repeat this process. We can see $\gamma | Aa_0 n^{D+d-2}\phi(m,n)$, and with the argument outlined above, $\gamma | Aa_0^2 n^{D+d-2}$. We can do this until $\gamma | Aa_0^{D+d}$. So, this means that

$$\gcd(n^d \Phi\left(\frac{m}{n}\right), n^d \tau\left(\frac{m}{n}\right)) | Aa_0^{D+d},$$

or there is a value that the greatest common denominator divides that is only dependent on the polynomials themselves.

So, now we have to prove the second part, which is two inequalities. The proof of the upper bound follows similarly to the proof of the previous property of $h(x)$. The lower bound is much more interesting. First, assume $\frac{m}{n}$ is not a root of Φ, as otherwise the problem would be reduced to a finite set of rationals inputted into the equation, meaning we could just choose the maximum possible κ_1.

If r is any non-zero rational number, then $h(r) = h(\frac{1}{r})$, as the function returns the maximum of the numerator and denominator. Again, we will force the degree of the polynomials with the same numbers as before. So, we want to calculate the height of

$$\xi = \frac{\Phi\left(\frac{m}{n}\right)}{\tau\left(\frac{m}{n}\right)} = \frac{\phi(m,n)}{\Psi(m,n)},$$

and these are integers, which means that $H(\xi) | \max(|\phi(m,n)|, |\Psi(m,n)|)$. We know that for some R,

$$\begin{aligned} H(\xi) &\geq \frac{1}{R}\max(|\phi(m,n)|, |\Psi(m,n)|) \\ &\geq \frac{1}{2R}\left(\left|n^d\Phi\left(\frac{m}{n}\right)\right| + \left|n^d\tau\left(\frac{m}{n}\right)\right|\right). \end{aligned}$$

This works because $\max(a,b) \geq \frac{1}{2}(a+b)$. Also,

$$H(\frac{m}{n})^d = \max(|m|^d, |n|^d).$$

Then,

$$\begin{aligned} \frac{H(\xi)}{H\left(\frac{m}{n}\right)^d} &\geq \frac{1}{2R}\cdot\frac{\left|n^d\Phi\left(\frac{m}{n}\right)\right| + \left|n^d\tau\left(\frac{m}{n}\right)\right|}{\max(|m|^d, |n|^d)} \\ &= \frac{1}{2R}\cdot\frac{\left|\Phi\left(\frac{m}{n}\right)\right| + \left|\tau\left(\frac{m}{n}\right)\right|}{\max(\left|\frac{m}{n}\right|^d, 1)}. \end{aligned}$$

So, we want to look at the function

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

We can first notice that

$$\lim_{|t|\longrightarrow\infty} p(t) \neq 0,$$

as the degree of $\Phi(X)$ is d. So, this limit is either $|a_0|$ or $|a_0| + |b_0|$ (if $\deg(\tau) = d$) where a_0 and b_0 are the leading coefficients of the terms in Φ and τ. However, within some closed interval, we can say that $p(t)$ is continuous, as the polynomials have no common roots. Also, as this function is never 0, we know that it is a positive function that is bounded away from 0 everywhere. So, there is some minimum value that such that $C_1 \leq p(t)$.

We can then write

$$\begin{aligned} \frac{H(\xi)}{H\left(\frac{m}{n}\right)^d} &\geq \frac{1}{2R}\cdot p\left(\frac{m}{n}\right) \\ &\geq \frac{C_1}{2R}. \end{aligned}$$

So,

$$H(\xi) \geq \frac{C_1}{2R} \cdot H\left(\frac{m}{n}\right)^d$$
$$h(\xi) \geq dh(\frac{m}{n}) - \log\left(\frac{2R}{C_1}\right),$$

and that means that $\kappa_1 = \log\left(\frac{2R}{C_1}\right)$ and we have found a lower bound. This concludes the proof of that lemma. □

Because the original ξ we were looking at looked like two polynomials over each other, specifically

$$\xi = \frac{3a^2x^2 + 3abx - ac + 3ax^3 + b^2 - 2bx^2 - 8cx + x^4}{4(ax^2 + bx + c + x^3)},$$

we can use the lemma that we just proved to finish the proof. We see that

$$h(\xi) \geq 4h(x) - \kappa,$$

which means that we have found some constant κ, completing the proof. □

3.4. **Finiteness of** $E(\mathbb{Q})/2E(\mathbb{Q})$.

Lemma 4. The index of $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Proof. This is the hardest lemma. To ease the difficulty, we will assume that the function $f(x)$ defining E has a root in the rational numbers, say x_0, which is the same as saying $x_0 \in \mathbb{Q} \cap E[2]_{tors}$. It is possible to prove it without this, but that dives into algebraic number theory. While that will show up with the Billing-Mahler Theorem, I would rather not bring it up here to keep this section of the paper more approachable.

As x_0 is a root and the coefficients of the function are integers, x_0 is also an integer. This means that we can shift $f(x)$ such that $(x_0, 0)$ is the origin. This means in our new coordinates the curve has the equation

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

This means that the point $P = (0, 0) \in E$ such that $2P = \mathbb{O}$. We can then take the discriminant to be $D = b^2(a^2 - 4b)$, and we will assume $D \neq 0$, which means that $b \neq 0$ and $a^2 - 4b \neq 0$.

Let us look at how the point $P \in E$ is transformed to $2P$. By looking at the x-coordinate of these points, we can say that this transformation is of degree 4. So, we can split this into two different functions of degree two, sending $E \longrightarrow \overline{E} \longrightarrow E$, where $\overline{E}$ is the range of the first function and the domain of the second. This curve is defined with $\overline{E} : y^2 = x^3 - 2ax + (a^2 - 4b)x$. What happens if we apply this procedure (changing a to $-2a$ and b to $(a^2 - 4b)$)?

The resulting curve is $\overline{\overline{E}} : y^2 = x^3 + 4a + 16bx$. This is just a scaled version of E, as we can replace x with $4x$ and y with $8y$ to return to E. Then, $E(\mathbb{Q})$ is isomorphic (there is a bijection between the elements) to $\overline{\overline{E}}(\mathbb{Q})$.

So, let us define the group homomorphisms (transformations that preserve the relationship between elements) $\Phi : E \longrightarrow \overline{E}$, and similarly, $\overline{\Phi} : \overline{E} \longrightarrow \overline{\overline{E}}$. Then, because $\overline{\overline{E}} \cong E$, $\overline{\Phi} \circ \Phi$ is a homomorphism that sends C to itself, which is the multiplication by 2 mapping of points.

So, we need to look at Φ. If $P = (x, y) \in E$ with nonnegative x, then $\Phi(x, y) = (\frac{y^2}{x^2}, \left(\frac{x^2-b}{x^2}\right))$. To verify this, one can plug this into the equation for $\overline{E}$, and it is left up to the reader if they want to prove it for themselves.

So, we need to consider the points $(0, 0)$ and $\mathbb{O}$. We can simply put $\Phi(0, 0) = \overline{\mathbb{O}}$ and $\Phi(\mathbb{O}) = \overline{\mathbb{O}}$. This may seem all arbitrary, but this mapping is actually simple algebra and arithmetic. It is possible to describe this mapping analytically, which does deliver a stronger understanding of this function, but is not necessary.

What is the kernel of Φ, or the elements in E sent to $\overline{\mathbb{O}}$ under Φ? With the algebraic formula for Φ that we gave earlier, we can see that $\mathbb{O}$ and $(0, 0)$ are the only two elements within the kernel. With the explicit formula, it can be shown that Φ is a homomorphism. It can also be shown that with the mapping

$$\overline{\Phi}(\overline{P}) = \begin{cases} \left(\frac{\overline{y^2}}{\overline{x^2}}, \frac{\overline{y}(\overline{x}^2-(a^2-4b))}{\overline{x}^2}\right) & \text{if } \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathbb{O}}, (0, 0) \\ \mathbb{O} & \text{if } \overline{P} = \overline{\mathbb{O}} \text{ or } \overline{P} = (0, 0) \end{cases}$$

we can then get that

$$\overline{\Phi} \circ \Phi(P) = 2P$$

with the explicit formulas.

Now, we can finish up the proof of Mordell's Theorem. Just to recap, we have elliptic curves

$$E : y^2 = x^3 + ax^2 + b \text{ and } \overline{E} : y^2 - 2ax + (a^2 - 4b)x,$$

and the homomorphisms

$$\Phi : E \longrightarrow \overline{E} \text{ and } \overline{\Phi} : \overline{E} \longrightarrow E,$$

such that the compositions

$$\Phi \circ \overline{\Phi} : \overline{E} \longrightarrow \overline{E} \text{ and } \overline{\Phi} \circ \Phi : E \longrightarrow E$$

both describe the multiplication of points by 2, with the kernels of Φ containing $\mathbb{O}, (0,0)$ and of $\overline{\Phi}$ containing $\overline{\mathbb{O}}, (0,0)$ respectively. Let us define the image of $\overline{E}(\mathbb{Q})$ by Φ as the subgroup of rational points that are mapped by Φ into $\overline{E}(\mathbb{Q})$. We claim that for the image of Φ that

- $\overline{\mathbb{O}} \in \Phi(E(\mathbb{Q}))$
- $(0,0) \in \Phi(E(\mathbb{Q})$ if and only if $a^2 - 4b$ is a perfect square
- 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.

The first statement follows instantly, as $\Phi(\mathbb{O}) = \overline{\mathbb{O}}$. The second statement follows from the formula. We can see that a point P satisfies $\overline{P} \in \Phi(P)$ if and only if $P = (x, y)$ such that $\frac{y^2}{x^2} = 0$. Because the precondition of $x \neq 0$, as otherwise it would be the same as the first statement. So, in order for this to be true, $y = 0$. So, for a point $\overline{P} \neq \mathbb{O}$ to be in the image of Φ on $E(\mathbb{Q})$, then if the original point in $E(\mathbb{Q})$ has $x \neq 0$ and $y = 0$. Plugging in $y = 0$ for the equation of $E(\mathbb{Q})$, we get

$$0 = x(x^2 + ax + b).$$

This has a nonzero rational root if and only if the discriminant of this equation is not irrational, or if $a^2 - 4b$ is a square.

Now, let's look at the third statement. If $(\overline{x}, \overline{y}) \in \Phi(E(\mathbb{Q}))$ is a point such that $\overline{x} \neq 0$, then the formula for Φ shows that $\frac{y^2}{x^2} = \overline{x}$ is the square of some rational number. Conversely, assume that $\overline{x} = w^2$, for some rational w. Then, let us try to find a point in $E(\mathbb{Q})$ such that it maps to $\overline{x}$.

Because Φ has two elements in its kernel, then two points map to $(\overline{x}, \overline{y})$, specifically

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

We claim that $P_i = (x_i, y_i) \in E(\mathbb{Q})$ and that $\Phi(P_i) = (\overline{x}, \overline{y})$ for $i = 1, 2$. Since these are rational points, this would prove that $(\overline{x}, \overline{y})$ is in the image of Φ.

We can write out the equations for the points together

$$\begin{aligned} x_1x_2 &= \frac{1}{4}\left((w^2-a)^2 - \frac{\overline{y}^2}{\overline{w}^2}\right) \\ &= \frac{1}{4}\left((\overline{x}-a)^2 - \frac{\overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \\ &= b. \end{aligned}$$

So, to show that P_i lies within $E(\mathbb{Q})$, we need to show that

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}.$$

Because we just showed that $b = x_1x_2$, and since we have $\frac{y_i}{x_i} = \pm w$, this is the same as showing

$$w^2 = x_1 + a + x_2.$$

This follows instantly from expanding x_1 and x_2. So, we need to check that $\Phi(P_i) = (\overline{x}, \overline{y})$, which can be done through explicit formula. So, the third statement is proven.

What we want to prove is that $2E(\mathbb{Q})$ has finite index within $E(\mathbb{Q})$. This would follow if we showed that $(E(\mathbb{Q}) : \overline{\Phi}(\overline{E}(\mathbb{Q})))$ has finite index, or if the index is bounded. From the previous three statements we know that $\overline{\Phi}(\overline{E}(\mathbb{Q}))$ is the set of points within $E(\mathbb{Q})$ such that x is a nonzero rational square, $\mathbb{O}$, or $(0,0)$ if b is a square number. In order to prove that this is a finite group, we want to find a homomorphism from the quotient group $E(\mathbb{Q})/\overline{\Phi}(\overline{E}(\mathbb{Q})$ to a finite group.

Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers, and let $\mathbb{Q}^{*2}$ be the subgroup of $\mathbb{Q}^*$ containing squares of rational numbers. Then, we can introduce the map $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ by defining it to be

$$\begin{aligned} \alpha(\mathbb{O}) &= 1 \pmod{\mathbb{Q}^{*2}}, \\ \alpha((0,0)) &= b \pmod{\mathbb{Q}^{*2}}, \\ \alpha((x,y)) &= x \pmod{\mathbb{Q}^{*2}} \text{ if } x \neq 0. \end{aligned}$$

Now we want to show that α is a homomorphism and that the kernel of this mapping is the image of $\overline{\Phi}$. So let us look at a proposition for this mapping.

Proposition 1. This describes the mapping α, as defined before.

- The map $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ is a homomorphism.

- The kernel of α is the image $\overline{\Phi}(\overline{E}(\mathbb{Q}))$. Then, α is an injective homomorphism
$$E(\mathbb{Q})/\overline{\Phi}(\overline{E}(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$
- 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
$$\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} \ldots p_t^{\epsilon_t} : \text{each } \epsilon_i \text{ equals 0 or 1.}\}$$
- The index $\big(E(\mathbb{Q}) : \overline{\Phi}(\overline{E}(\mathbb{Q}))\big)$ is at most 2^{t+1}.

Proof. Each item corresponds to the one in the proposition.

- First, we can observe that α sends inverses to inverses, because
$$\alpha(-P) = \alpha((x,-y)) = x = \frac{1}{x} \cdot x^2,$$
so,
$$\alpha(-P) \equiv \frac{1}{x} = \frac{1}{\alpha((a,y))} = \alpha(P)^{-1} \pmod{\mathbb{Q}^{*2}}.$$
So, to prove that it is a homomorphism, or that the relations between points hold, we need to show that whenever $P_1 + P_2 + P_3 = \mathbb{O}$, then $\alpha(P_1) + \alpha(P_2) + \alpha(P_2) \equiv 1 \pmod{\mathbb{Q}^{*2}}$.

  So, the triples of points that add to the point at infinity are all collinear, meaning that there exists a line $y = \lambda x + v$ coinciding with these points on x-coordinates x_1, x_2, x_3 correspondingly. We saw that this means that these are the roots of the equation
$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2) = 0,$$
for the cubic $y^2 = x^3 + ax^2 + bx + c$. Then by Vieta's,
$$x_1 + x_2 + x_3 = \lambda^2 - a,$$
$$x_1x_2 + x_1x_3 + x_2x_3 = b - 2$$
$$x_1x_2x_3 = v^2 - c\lambda v.$$
Using the last equation, because c for us is 0, we see that $x_1x_2x_3 = v^2 \in \mathbb{Q}^2$. So,
$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = v^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$
This shows that these points are distinct from $\mathbb{O}$ and $(0,0)$. The other two cases follow as well, due to how we defined α.
- With the definition of α and the description of $\overline{\Phi}(\overline{E}(\mathbb{Q}))$ with the three statements before, it follows that the kernel of α is $\overline{\Phi}(\overline{E}(\mathbb{Q}))$

- Now we want to figure out which rational numbers can be x coordinates in $E(\mathbb{Q})$. We know that those points have the form $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ for integer n, m, e, such that x is in the lowest form. Through substitution and clearing denominators,
$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4).$$
So, the square of n is the product of two integers. If the two terms in the right were relatively prime, they would have to be plus or minus a square, so $x = \frac{m}{e^2}$ would be plus or minus the square of some rational number. Generally, let
$$d = \gcd(m, m^2 + ame^2 + be^4).$$
This means that $d|m, be^4$. However, those are relatively prime, because we assumed that x was written in the lowest terms. This means that $d|b$.

  Then, the greatest common divisor of m and $m^2+ame^2+be^4$ divides b. Since n^2 is the product of those two, every prime dividing m appears to an even power except maybe sometimes for primes dividing b. Therefore,
$$m = \pm(\text{integer})^2 \cdot p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_t^{\epsilon_t},$$
where $\epsilon_i \in \{0, 1\}$, and $p_1 \dots p_t$ are the distinct primes dividing b. This would prove
$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_t^{\epsilon_t} \pmod{\mathbb{Q}^{*2}},$$
and then the image of α is within the group $\mathbb{Q}^*/\mathbb{Q}^{*2}$. If $x = 0$, then $a((0,0)) = b \pmod{\mathbb{Q}^{*2}}$ shows the third part of the proposition.
- The subgroup described before has exactly 2^{t+1} elements. The second part of the proposition says that there is a one to one mapping to this subgroup from $E(\mathbb{Q})/\overline{\Phi}(\overline{E}(\mathbb{Q}))$, meaning that the index of $\overline{\Phi}(\overline{E}(\mathbb{Q}))$ inside $E(\mathbb{Q})$ has at most 2^{t+1}.

□

Now, we can finally begin to fully prove this. There is one final lemma. We have shown that $\left(\overline{E}(\mathbb{Q}) : \Phi(E(\mathbb{Q}))\right)$ and $\left(E(\mathbb{Q}) : \overline{\Phi}(\overline{E}(\mathbb{Q}))\right)$ are finite. Then, we want to prove that $2E(\mathbb{Q})$ has finite index in $E(\mathbb{Q})$.

Because $\overline{\Phi}(\overline{E}(\mathbb{Q}))$ has finite index in $E(\mathbb{Q})$, we can find coset representatives $a_1, a_2, a_3, \dots, a_n$. Similarly, denote $b_1, b_2, \dots, b_m$ as the coset representatives of $\Phi(E(\mathbb{Q}))$ in $\overline{E}(\mathbb{Q})$. We can claim that
$$\{a_i + \overline{\Phi}(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$$
includes a complete set of coset representatives of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$.

In order to show this, let $P \in E(\mathbb{Q})$. To prove the claim, we need to show that P can be written as the sum of an element of this set and an element of $2E(\mathbb{Q})$. Because of coset representatives, we can find some a_i such that $P - a_i \in \overline{Phi}(\overline{E}(\mathbb{Q}))$, say that $a - a_i = \overline{\Phi}(\overline{P})$. Also, we can find some b_j such that $b - b_j = \Phi(P')$. Then,

$$\begin{aligned} P = a_i + \overline{\Phi}(\overline{P}) &= a_i + \overline{\Phi}(b_k + \Phi(P')) \\ &= a_i + \overline{\Phi}(b_j) + \overline{\Phi}(\Phi(P')) \\ &= a_i + \overline{b_j} + 2P'. \end{aligned}$$

This proves that $2E(\mathbb{Q})$ has finite index in $E(\mathbb{Q})$.

So, with all of this, we have proven that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

□

With all of these, we can finally prove the Mordell-Weil Theorem.

3.5. **Proof.** Let

$$h : E(\mathbb{Q}) \longrightarrow [0, \infty)$$

with the following four properties

- The set $\{P \in E(\mathbb{Q}) : h(P) \leq C\}$ for some given C is finite.
- $h(2P) \geq 4h(P) - \kappa, \forall P \in E(\mathbb{Q})$
- $h(P + Q) \leq 2h(P) + \kappa_0, \forall P \in E(\mathbb{Q})$
- $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite

Note that this function is the height function from before, and we have proved that it exists. So, let $E(\mathbb{Q})/2E(\mathbb{Q}) = n$, and let $Q_1, Q_2, Q_3, \ldots Q_n$ be a finite number of coset representatives. So, we can say that for any $P \in E(\mathbb{Q})$, P is within some coset as well. So, there is some index $1 \leq i_1 \leq n$ dependent on P such that $P - Q_{i_1} \in 2E(\mathbb{Q})$ or $P - Q_{i_1} = 2P_1, P_1 \in E(\mathbb{Q})$.

Let's go back to the first equation, $P = Q_{i_1} + 2P_1$. If we substitute P_1 into it, we get

$$P = Q_{i_1} + 2Q_{i_2} + 4P_2,$$

and we can again replace P_2 to get something else. Recursively, this looks like

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m$$

Set $P = -Q_i$. Then by the second property, we get

$$h(P - Q_i) \leq 2h(P) + \kappa_i, \forall P \in E(\mathbb{Q}).$$

We can set up n equations for each coset $Q_1, Q_2, \ldots, Q_n$, which would give us n different κ's. So, let $\kappa' = \max(\kappa_1, \kappa_2, \ldots, \kappa_n)$. Then,

$$\begin{aligned}
h(P - Q_i) &\leq 2h(P) + \kappa', (\forall P \in E(\mathbb{Q}), 1 \leq i \leq n) \\
4h(P_j) &\leq h(2P_j) + \kappa \\
&= h(P_{j-1} - Q_{i_j}) + \kappa \\
&\leq 2h(P_{j-1}) + \kappa' + \kappa \\
h(P_j) &\leq \frac{h(P_{j-1})}{2} + \frac{\kappa' + \kappa}{4} \\
&= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)) \\
&\leq \frac{3}{4}h(P_{j-1}) \\
&\vdots \\
h(P_m) &\leq \kappa' + \kappa
\end{aligned}$$

So, starting with $h(P_{j-1}) \geq \kappa' + \kappa$, as $h(P_j) \leq \frac{3}{4}h(P_{i-1})$. As j gets larger, $h(P_j)$ trends to 0. As such, there must be an m such that $h(P_m) \leq \kappa' + \kappa$. Remember that any point P can be written out as

$$P = Q_1 + 2Q_2 + 4Q_3 + \ldots 2^{n-1}Q_n + 2^n P_m.$$

Since $h(P_m) \leq \kappa' + \kappa$, there are a finite number of possible P_m. So,

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{P_m \in E(\mathbb{Q}) : h(P_m) \leq \kappa' + \kappa\}$$

finitely generate $E(\mathbb{Q})$. We can finitely generate $E(\mathbb{Q})$. □

4. Billing-Mahler Theorem

4.1. **Torsion Points.** This subsection will go over the (not necessarily rational) points of finite order. A point $P \in E : y^2 = f(x) = x^3 + ax^2 + bx + c$ with finite order means that there exists a positive integer m such that

$$mP = P + P + \ldots + P = \mathbb{O}.$$

For the point to have order m, m has to be the smallest element such that $mP = \mathbb{O}$. For some elliptic curve over $\mathbb{Q}$, we will denote the set $E[m]$ to be the set of m-torsion points, meaning

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

Let us focus on $E[2]$. What this means is for some point $P \in E$, $P + P = \mathbb{O}$. More simply put, a point P has order 2 if $P = -P$, so if

$P = (x, y)$, $(x, y) = (x, -y)$. This means that the only points of order two are the roots of E (the points where $y = 0$). So, we know that

$$E[2] = \{\mathbb{O}, P_1, P_2, P_3\}$$

where P_1, P_2, P_3 are the (complex) roots of E. Because these points are of order two, $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (a direct product of two groups of order two).

Let's look at $E[3]$ for more of a challenge. Last time we could write $P = -P$ to simplify finding the points that are not simply the point at infinity. This time we will write a point P having order 3 as $2P = -P$. We can then write $x(2P) = x(-P) = x(P)$ where $x(P)$ is the x-coordinate of P. In order to find the points that satisfy this, we can use the algebraic expansion of the addition function. We can see that P has order 3 if and only if

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

Let us simplify this with cross multiplication and subtraction. We would get

$$4x^4 + 4ax^3 + 4bx^2 + 4cx = x^4 - 2bx^2 - 8c + b^2 - 4ac$$

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

Denote this function as $\psi_3(x)$. Then,

$$\psi_3(x) = 2f(x)f''(x) - f(x)'^2.$$

So, P is a point of order three if and only if it's x coordinate is a root of $\psi_3(x)$. We will prove that $\psi_3(x)$ has 4 distinct roots by showing $\psi_3(x)$ and $\psi_3'(x)$ have different roots. This would mean that $\psi_3(x)$ is a separable function, meaning that no roots repeat.

We can calculate $\psi_3'(x)$ to be

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x).$$

If something is a root of $\psi_3'(x)$, then it is a root of $f(x)$. So, if something is a common root between $\psi_3(x)$ and it's derivative, it's the root of both $f(x)$ and $f'(x)$. However, this is a contradiction to the definition of an elliptic curve. They are nonsingular, meaning that they have different roots. So, we know that $\psi_3(x)$ is a separable function with 4 distinct roots.

We now know the points of order 3. Let x_1, x_2, x_3, x_4 be the roots of $\psi_3(x)$, and let y_i be $\sqrt{f(x_i)}$. Then,

$$\begin{aligned} E[3] = \{ \quad & \mathbb{O}, (x_1, y_1), (x_1, -y_1), (x_2, y_2), (x_2, -y_2), \\ & (x_3, y_3), (x_3, -y_3), (x_4, y_4), (x_4, -y_4)\}, \end{aligned}$$

where each element is distinct and of order 3 or 1. It is interesting to note that these are the inflection points of E as well. The set $E[3]$ becomes an abelian group of order 9, meaning $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

So, if we have a way to translate the statement $mP = 0$ into something else, we can write a $\psi_m(x)$ function (called a division polynomial within the literature) to find the x coordinates of the m-torsion points. Also, it should hopefully look like $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$, which is true. A further proof of this is within [5].

4.2. **Setup.** We can now start looking at the Billing-Mahler Theorem.

Theorem 2. (Billing-Mahler) An elliptic curve defined over $\mathbb{Q}$ does not have a rational torsion point of order 11.

Proof. Let us quickly revisit the projective plane. Remember, if a triple of points in the projective plane is thought of as a vector (X, Y, Z) in $\mathbb{R}^3$, then the all of scalar multiples of that vector can be thought of as the same as the original vector. The projective plane can then be thought of as the set of all directions in $\mathbb{R}^3$.

Let E be an elliptic curve over $\mathbb{Q}$ as a subvariety of $\mathbb{P}^2$ (we will be looking at points on E as they are on the projective plane). Assume towards a contradiction that there exists a rational point $P \in E[11]$. Denote P_i to be iP, or P added to itself i times. This would mean that if $P_i = P_j$, then $i \equiv j \pmod{11}$, and if P_i, P_j, and P_k are collinear, then because that would mean $P_i + P_j + P_k = \mathbb{O}$, we can see that $i + j + k \equiv 0 \pmod{11}$. It will be important to see that

$$P_i, P_j, P_k \text{ are collinear if and only if } i + j + k \equiv 0 \pmod{11}.$$

Let us introduce a lemma.

Lemma 5. Let K be a field and let $(a, b, c), (\alpha, \beta, \gamma) \in \mathbb{P}^2(K)$ be points such that they are distinct. Then, there exists a unique line through these points, given by the equation

$$\begin{vmatrix} x & y & z \\ a & b & c \\ \alpha & \beta & \gamma \end{vmatrix} = -\gamma ay + \alpha\beta z + \gamma bx - \alpha bz - \beta cx + \alpha cy = 0.$$

Two lines given by equations $ux + vy + wz = 0$ and $u'x + v'y + w'z = 0$ coincide if and only if the points (u, v, w) and (u, v, w) coincide as points in $\mathbb{P}^2(K)$. Two distinct lines in $\mathbb{P}^2(K)$ intersect at exactly one point.

Proof. We can write out the statement in matrix form. Let (a, b, c) and $(\alpha, \beta, \gamma) \in \mathbb{P}^2(K)$. Then, we want to find a unique solution to

$$\begin{bmatrix} a & b & c \\ \alpha & \beta & \gamma \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since these are two distinct points, the rows of the left matrix are linearly independent, meaning there exists a unique solution to this equation. This equation turns out to be the stated determinant of a matrix. □

4.3. **Remapping of Coordinates.** So, what would the implications of this point be? Consider the three points $P_0 = (0, 1, 0), P_1 = (a, b, c)$, and $P_2 = (\alpha, \beta, \gamma)$. Because $0 + 1 + 2$ are not equivalent to 0 mod 11, we know that these do not lie on a line. The previous lemma would also tell us that these are linearly independent, meaning that there is a linear map ϕ that maps the points to

$$P_0' := (0, 1, 0), P_1' := (1, 0, 0), P_2' := (0, 0, 1).$$

This preserves lines and the torsion points, so P_1' has order 11 and these points are still not collinear.

Now, let's consider the point $P_3' = (u, v, w)$. Again, P_3', P_0', and P_1' are all noncollinear. As P_0' and P_1' have z-coordinates 0, we can then say $w \neq 0$. So, we can define another mapping ρ that sends (x, y, z) to $(\frac{x}{u}, \frac{y}{v}, \frac{z}{w})$. This is a bijective mapping that doesn't actually change the points P_0', P_1', and P_2' due to the equivalence relation in the projective plane. What this does allow us to do, is now write

$$P_0 = (0, 1, 0), P_1 = (1, 0, 0), P_2 = (0, 0, 1), P_3 = (1, 1, 1).$$

So, let us denote $P_4 = (x_1, x_2, x_3)$.

Proposition 2. With the construction labeled before, $P_{-3} = (1, 0, 1)$, and

$$x_1^2 x_2 - x_1^2 x_3 + x_1 x_3^2 - x_2^2 x_3 = 0$$

Proof. We can define the line between two distinct points using the lemma outlined above. Let the line $L_{i,j}$ be the line between two distinct points P_i and P_j. Also, if $k + m + n \equiv k + i + j \equiv 0 \pmod{11}$, then we know that P_k is the intersection of $L_{i,j}$ and $L_{m,n}$. So, using the lemma, we can get some lines:

$$L_{0,1} : z = 0$$
$$L_{0,2} : x = 0$$

$$L_{0,3} : x - z = 0$$

$$L_{1,2} : y = 0$$

$$L_{1,4} : x_3y - x_2z = 0$$

$$L_{2,3} : x - y = 0$$

Using the previous observation about collinearity, we can see that because $-3 + 0 + 3 \equiv -3 + 1 + 2 \equiv 0 \pmod{11}$, then the intersection of $L_{0,3}$ and $L_{1,2}$ is $P_{-3} = (1, 0, 1)$.

Because of this, $L_{-3,4} : -x_2x + (x_1 - x_3)y + x_2z = 0$. We can find P_{-1} similarly to how we found P_{-3} and find that $P_{-1} = (x_1 - x_3, x_2, 0)$. Then,

$$L_{-1,3} : x_2x - (x_1 - x_3)y + (x_1 - x_2 - x_3)z = 0.$$

We can find $P_{-2} = (0, x_1 - x_2 - x_3, x_1 - x_3)$, and write

$$L_{-2,-3} = (x_1 - x_2 - x_3)x + (x_1 - x_3)y - (x_1 - x_2 - x_3)z = 0.$$

Then we find $P_{-5} = (x_2, x_2, x_3)$, and write

$$L_{0,-5} : x_3x - x_2x = 0.$$

Then we can find

$$P_5 = ((x_1 - x_3)x_2, -x_1x_2 + x_1x_3 + x_2^2 - x_3^2, (x_1 - x_3)x_3).$$

This would mean $x_1 \neq x_3$ as otherwise $P_{-2} = P_0$, a contradiction. So, $P_5 \in \mathbb{P}^2(\mathbb{Q})$ with nonzero x and z coordinates.

Now, we can see that P_2, P_4, and P_5 lie on a line. We can use the lemma and take the determinant to show

$$x_1^2x_2 - x_1^2x_3 + x_1x_3^2 - x_2^2x_3 = 0.$$

□

Now, we can set up a corollary.

Corollary 1. If there exists an elliptic curve defined over $\mathbb{Q}$ that has a rational point of order 11, then the cubic curve C given by the equation:

$$u^2v - u^2w + uw^2 - v^2w = 0$$

has more than 5 rational points.

Proof. The curve would have rational points at $P_0, P_1, P_2, P_3, P_{-3}$, and if we assume the existence of the rational point of order eleven, then P_4 would be a sixth rational point on C. □

So, to disprove that there are any 11 torsion points, we have to show this corollary as false.

4.4. Curve C and Elliptic Curve E.

Proposition 3. The cubic C given by the equation

$$u^2v - u^2w + uw^2 - v^2w = 0$$

has exactly 5 rational points, which are $(0, 1, 0)$, $(1, 0, 0)$, $(0, 0, 1)$, $(1, 1, 1)$, and $(1, 0, 1)$.

Proof. First, notice that C is an elliptic curve, although it is not in the nicer form. We can use an algorithm from T. Nagel [6] that translates C to a Weierstrass form (the form that we are using). This turns out to mean that C is equivalent to $E : y^2 = x^3 - 4x^2 + 16$. This becomes instantly much easier to solve, as we now only have to show that there are only 5 rational points on this curve.

We will have to use the Nagell-Lutz theorem, where a proof of which is outlined in [7]. With this theorem, it becomes clear that $E(\mathbb{Q})_{tors}$ has order 5, containing $\{\mathbb{O}, (0, 4), (0, -4), (4, 4), (4, -4)\}$. Now, we have to show that the rank of $E(\mathbb{Q})$ is 0, or $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \cdot \mathbb{Z}^0$. This is the hardest bit of the proof, and it assumes some algebraic number theory understanding.

The polynomial $f(x) := x^3-4x^2+16$ is irreducible with discriminant $-2^8 \cdot 11$. Let $\theta = \theta_1, \theta_2, \theta_3$ be the roots of f, with θ as the real root. Then, let the cubic number field K be $K := \mathbb{Q}(\theta)$. The discriminant of K is $-44 = -2^2 \cdot 11$, and the ring of integers of K is $O_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2$. This means that the unit rank of K is 1, and the fundamental unit is $\eta := 1 - \frac{1}{2}\theta$. This makes the units of O_K into $O_K^\times = \langle -1 \rangle \times \langle \eta \rangle$. The class number of K is then $h_K = 1$.

With the homomorphism that is defined within the proof of Mordell's Theorem,

$$\mu : E(\mathbb{Q}) \longrightarrow K^\times/(K^\times)^2,$$

we can look at its kernel, which is $2E(\mathbb{Q})$. Because of this and the fact that

$$E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r, (r \geq 0),$$

we can say

$$\Im(\mu) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^e,$$

meaning that we have to prove that μ has a trivial image instead.

What this means is that there is no rational point on E that is trivial under μ. So, assume to the contrary that there is a rational point $(x, y) \in E(\mathbb{Q})$ such that $x - \theta$ is not a square in K.

Let's use the fact that we can write

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

for integers n, m, e such that $\gcd(n, e) = \gcd(m, e) = 1$. Then, we get

$$\mu(x, y) = (x - \theta) \pmod{K^\times)^2} = (n - e^2\theta) \pmod{K^\times)^2}.$$

So, $n - e^2\theta \notin (K^\times)^2$.

Now we consider the integral ideal $(n - e^2\theta)$ of O_K. Also following from Mordell's theorem,

$$n^2 - e^2\theta = \left(\Pi_i \text{ı}_i^{\text{Ə}_i}\right) \cdot \mathbb{A}^2,$$

where $\mathbb{A}$ is some integral ideal, $\text{Ə}_i \in \{0, 1\}$, and ı_i are distinct prime ideals of O_K such that each ı_i divides the discriminant $-2^8 \cdot 11$, meaning that they divide either 2 or 11.

We want to show that all Ə_i are equal to 0. We need to note that the prime decomposition of 2 and 11 in K are

$$(2) = \text{ı}^3, (11) = \text{ıı}^2 \cdot \text{ıı}'^2 \text{ with } \text{ıı} \neq \text{ıı}'.$$

So then we have

$$N_{K/\mathbb{Q}}(\text{ı}) = 2, N_{K/\mathbb{Q}}(\text{ıı}) = N_{K/\mathbb{Q}}(\text{ıı}') = 11.$$

So, the previous product can be written out into

$$\Pi_i \text{ı}_i^{\text{Ə}_i} = \text{ı}^{a_1} \text{ıı}^{a_2} (\text{ıı}')^{a_3},$$

where $a_1, a_2, a_3 \in \{0, 1\}$ and

$$\Pi_i N_{K/\mathbb{Q}}(\text{ı}_i)^{\text{Ə}_i} = 2^{a_1} \cdot 11^{a_2 + a_3}.$$

On the other hand,

$$\begin{aligned}
\Pi_i N_{K/\mathbb{Q}}(\text{ı}_i)^{\text{Ə}_i} \cdot N_{K/\mathbb{Q}}(\mathbb{A})^2 &= N_{K/\mathbb{Q}}(n - e^2\theta) \\
&= ((n - e^2\theta_1)(n - e^2\theta_2)(n - e^2\theta_3)) \\
&= (e^2(x - \theta_1)(x - \theta_2)(x - \theta_3)) \\
&= (e^6 y^2) \\
&= (m)^2,
\end{aligned}$$

meaning that the original product is a square. This would mean that $\text{Ə}_1 = 0$ and $\text{Ə}_2 = \text{Ə}_3$.

If $\text{Ə}_2 = 1$, then, $\text{ıııı}'|(n - e^2\theta)$, meaning

$$11 | \text{ıı}^2 (\text{ıı}')^2 | (n - e^2\theta)^2 = n^2 - 2ne^2\theta + e^4\theta^2,$$

and the number

$$\frac{n^2 - 2ne^2\theta + e^4\theta^2}{11}$$

is the ring of integers $O_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2$. However, this is a contradiction, as it would imply $11 | \gcd(n, e)$, when we have assumed that they are coprime.

So, $a_1 = a_2 = a_3 = 0$. This means that $n - e^2\theta = \mathbb{A}^2$ for some integral ideal $\mathbb{A}$. Since K has class number 1, it follows that $\mathbb{A} = (\alpha)$ for some $\alpha \in O_K$. Then,

$$n - e^2\theta = u \cdot a^2,$$

where u is a unit that is non-square in K, because we have just shown that $n - e^2\theta$ is not a square in K. We can assume that $u \in \{-1, \eta, -\eta\}$, where $\eta := 1 - \frac{1}{2}\theta$, given that we choose an appropriate α. Now,

$$N_{K/\mathbb{Q}(u)} \cdot N_{K/\mathbb{Q}} = N_{K/\mathbb{Q}}(n - e^2\theta) = m^2,$$

where $N_{K/\mathbb{Q}}(u) > 0$ as the right-hand side is a square. Once we consider that $N_{K/\mathbb{Q}}(-1) = -1$, $N_{K/\mathbb{Q}}(\eta) = 1$, implying that $N_{K/\mathbb{Q}(-\eta)} = -1$, we are restricted to

$$n - e^2\theta = \eta \cdot \alpha^2,$$

for some $\alpha \in O_K$.

Let $\beta := \eta\alpha$, and say that $\beta = a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta$, with $a, b, c \in \mathbb{Z}$. We find that a, b, c satisfy

$$\eta \cdot (n - e^2\theta) = (1 - \frac{1}{2}\theta)(n - e^2\theta) = \beta^2 = (a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta^2)^2.$$

Using the fact that $\theta^3 = 4\theta^2 - 16, \theta^4 = 4\theta^3 - 16\theta = 16\theta^2 - 16\theta - 64$, we see that the previous equation is equivalent to

$$n - \left(\tfrac{n}{2} + e^2\right)\theta + \tfrac{e^2}{2}\theta = (a^2 - 4c^2 - 4bc) + (ab - c^2)\theta + \left(\tfrac{b^2}{4} + \tfrac{ac}{2} + bc + c^2\right)\theta^2.$$

As these are two polynomials of θ with degree 2 it follows that their coefficients must be equal. Specifically

$$\begin{aligned} n &= a^2 - 4c^2 - 4bc \\ -n - 2e^2 &= 2ab - 2c^2 \\ 2e^2 &= b^2 + 2ac + 4bc + 4c^2 \end{aligned}$$

The last equality implies that b is even, and the second one implies that n is even, implying that a is even in the first one. Since $2|\gcd(a, b)$, the right-hand side of the final equation is divisible by 4. This directly implies that e is an even number, contradicting the fact that n and e are coprime.

This would mean that the map μ is a trivial map, implying that the rank of $E(\mathbb{Q})$ is of rank 1, so there are only 5 rational points on the elliptic curve, E. This completes the proof of Proposition 3. □

Because Proposition 3 is true, we have now disproved Corollary 1. This means that we have contradicted our original assumption that there exists a rational 11 torsion point.

As such, no elliptic curve forms a group of rational 11-torsion points.

□

5. Extensions of Elliptic Curves

Now the question before I end this paper is, what is the point? Why are we interested in these equations?

There are many answers to this question. Just like how linear systems can represent stochastic models and how quadratic equations can describe velocity, elliptic curve's have their use. They are used in quantum security, pairing based cryptography, Diffie-Hellman cryptography, primality tests, factoring numbers, and a lot more. It is interesting to see how it is used in cryptography.

5.1. **Cryptography.** ECC, or Elliptic Curve Cryptography, is an extremely powerful form of cryptography used today. RSA is the precursor to this. RSA relies on modular arithmetic to start with a given number that represents a message, and raises it to a power and takes the modulo consecutively. This is relatively secure, as if you choose a large enough modulo, you can create an extremely hard factoring problem. The recipient has the method to decipher it, however.

What ECC does is it instead uses the group law on the curve to take the starting message and find a resulting end point. This is a lot more secure than RSA, because elliptic curves on their own are much harder to understand. The recipient of the message also can decipher the original.

ECC is used within finite fields, modulo some large prime, similar to RSA. The group law still holds within finite fields, so this makes sense, and it creates the doubly hard problem of factoring and elliptic curves. A simple explanation can be found here.

The reason torsion points are interesting is because of how ECC determines what secret code to send. It takes the secret message, a, and some original point P, and sends the message aP. If this goes to the point at infinity, then we are out of luck, and there isn't really a way to decipher the message.

This is why we want to study torsion points, in order to better understand when a rational point (as computers cannot handle anything else) goes to the point at infinity before we send the message.

I hope that gives a healthy synopsis on elliptic curves and at least one of their uses.

Acknowledgement

The author is grateful to his advisor Rajiv Nelakanti as well as the professor Prof. Simon Rubinstein-Salzedo who gave this topic.

References

[1] Richard Peng and Santosh S. Vempala. Solving sparse linear systems faster than matrix multiplication. *CoRR*, abs/2007.10254, 2020.

[2] Keith Conrad. A multivariable hensel's lemma. *Lecture note available at http://kconrad. math. uconn. edu/blurbs*, 2020.

[3] Joseph H Silverman and John Torrence Tate. *Rational Points on Elliptic Curves.* Springer, 2nd edition, 2015.

[4] Stefan Friedl. An elementary proof of the group law for elliptic curves. *Groups Complexity Cryptology*, 9(2):117–123, 2017.

[5] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[6] Trygve Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta mathematica*, 52:93–126, 1929.

[7] Michael Galperin. Torsion points of elliptic curves. 2013.

Euler Circle
Email address: agnivsarkar@proofschool.org