Spring 4-30-2012

Elliptic Curves of High Rank

Cecylia Bocovich
Macalester College, cecylia.bocovich@gmail.com

Elliptic Curves of High Rank

Cecylia Bocovich

Mathematics Department

27 April 2012

Advisor: David Bressoud
Reader: James Doyle
Reader: Daniel Flath

Abstract

The study of elliptic curves grows out of the study of elliptic functions which dates back to work done by mathematicians such as Weierstrass, Abel, and Jacobi. Elliptic curves continue to play a prominent role in mathematics today. An elliptic curve E is defined by the equation, $y^2 = x^3 + ax + b$, where a and b are coefficients that satisfy the property $4a^3 + 27b^2 \neq 0$. The rational solutions of this curve form a group. This group, denoted $E(\mathbb{Q})$, is known as the Mordell-Weil group and was proved by Mordell to be isomorphic to $\mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$ where the group of rational torsion points consists of all points of finite order. The rank r is difficult to compute and the main goal of this research is to explore the relationship between ranks of elliptic curves and values of a and b. Specifically, we have put a lower bound on the ranks of equations of the form $C_m : y^2 = x^3 - m^2x + 1$ and $K_m : y^2 = x^3 + m^3x - m^3$

Contents

Chapter 1

Introduction

Elliptic curves play an important role in mathematics. Making their first appearance in Diophantus's *Arithmetica*, the concept of elliptic curves dates back 1800 years. Diopantus studied them in the context of finding two numbers whose product is a cube minus its side [2]. This results in the equation

$$y(y-a) = x^3 - x$$

With a simple expansion, this begins to look like the general equation for elliptic curves we use today:

$$y^2 = x^3 + ax + b$$

Motivated by intractable integrals, the study of elliptic curves has spread to almost all areas of mathematics. From the finite group of solutions in a field $\mathbb{F}_p$ to the complex tori they form in $\mathbb{C}$, the study of elliptic curves involves a combination of number theory, geometry, algebra, and analysis. The innovations of Weierstrass, Jacobi, and Mordell have set the stage for modern mathematicians who continue to explore and discover new patterns in elliptic curves. Despite their long history, there is still much to be learned about elliptic curves and how they behave over various fields.

Of particular current interest, is the size of the rational solutions, or rank, of elliptic curves. Computing the rank of a given curve is still a computationally difficult problem. There have been many explorations into ranks of elliptic curves over the last couple years. Notably, recent work has been done by Barghava [1] in putting bounds on the ranks of elliptic curves. The results indicate that the majority of elliptic curves have relatively low ranks, with over half of all curves having a rank of 0. The Birch and Swinnerton-

Dyer conjecture, one of the most famous unsolved problems in mathematics, is also related to the ranks of elliptic curves.

In this paper, we present two infinite families of curves, all with rank greater than or equal to 2. We extend the results of a paper by Brown and Meyers [2] which examines families of curves of high rank. Through computational exploration, we were able to find evidence of two such families of curves that exhibited this pattern. By combining the geometric, algebraic, and analytic properties of these curves, we were able to find and prove the existence of a lower bound on the ranks of these curves.

The methods set forth by Brown and Meyers, and explained in this paper, may be used to find and bound additional families of curves. Studying the behavior of elliptic curves from multiple viewpoints provides insights into their structure and gives us the tools we need to piece together the puzzle that has been forming for over 18 centuries.

Chapter 2

Background

Elliptic curves have roots in many major areas of mathematics. From their first apperance in Diophantus's *Arithmetica* [10] to their growth out of elliptic integrals, the study of elliptic curves spans the fields of number theory, complex analysis, alegbra, and geometry. This section provides an overview of the general terms and structure of elliptic curves over the rational numbers as well as a glimpse into their beginnings and their properties in other fields.

2.1 Elliptic Curves

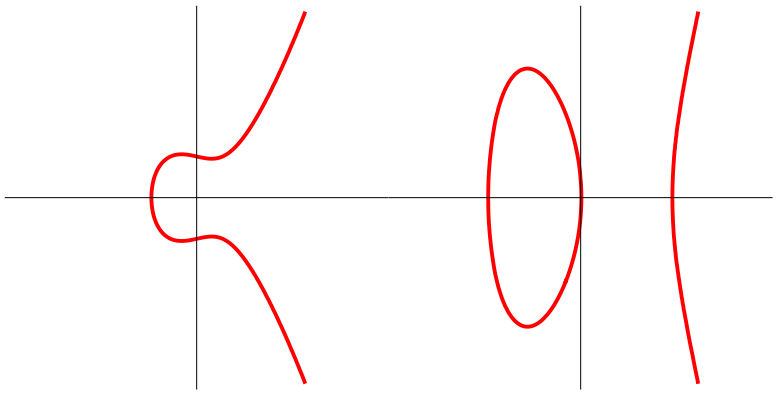
An elliptic curve is most commonly defined as a non-singular equation of the form

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

where the discriminant $\Delta(f) = -4a^3 - 27b^2 \neq 0$. Generally, any nonsingular equation $y^2 = f(x)$ where $f(x)$ is a cubic or quartic polynomial is an elliptic curve and is reducible to this Weierstrass normal form.

In this paper, we are primarily concerned with the solutions to an elliptic curve over the field of rationals, $E(\mathbb{Q})$, but a curve takes on many different properties when viewed over other fields. These properties provide a complete picture and come in useful when proving their behavior over the rationals.

Elliptic curves get their name from a class of functions in the complex plane, where the qualifier "elliptic" comes from, the solutions to an elliptic curve form a torus, uniquely defined by a corresponding doubly periodic elliptic function in $\mathbb{C}$. The curve has 3 complex roots, and when viewed over



(a) A curve with one real root (b) A curve with two real roots

Figure 2.1: Examples of Elliptic Curves over $\mathbb{R}$

the reals, forms a curve with either 1 or 3 real roots that is symmetric across the x-axis.

Another common field over which elliptic curves are studied is the field $\mathbb{F}_p$ of integers modulo a prime p. These solutions form a group that is the basis of elliptic curve cryptography [4].

Despite their name, ellipses are not elliptic curves. The origin of this association stems back to the beginnings of serious study into a class of intractable integrals that would lead to and motivate the development of elliptic functions and their corresponding elliptic curves.

2.1.1 How Elliptic Curves Arose

Although ellipses and elliptic curves occupy completely different classes of functions, the similarities in their names are not a coincidence. Consider the problem of finding the arc length of an ellipse.

Given an ellipse with the general equation

$$\left(\frac{x^2}{a^2}\right) + \left(\frac{y^2}{b^2}\right) = 1$$

The arc length is computed using the formula

$$s = \int \sqrt{1 + f'(x)^2} dx$$

resulting in the integral

$$s = \int_0^a \sqrt{1 + \left(\frac{-bx}{a^2\sqrt{1 - x^2/a^2}}\right)^2} = \int_0^a \sqrt{1 + \frac{b^2x^2}{a^2(1-x^2)}}$$

$$= \int_0^a \sqrt{\frac{(1-x^2) + b^2/a^2x^2}{(1-x^2)}} = \int_0^a \sqrt{\frac{1 - (1 - b^2/a^2)x^2}{(1-x^2)}}$$

$$= a\int_0^1 \sqrt{\frac{1 - k^2x^2}{1-x^2}}dx, \qquad k^2 = 1 - \frac{b^2}{a^2}$$

An integral of this form is defined as Jacobi's complete elliptic integral of the second kind [6].

In fact, these integrals make up a subset of the class of elliptic integrals defined generally as follows,

Definition 2.1.1. An elliptic integral is the integral of a rational function of x and y in which y^2 is a polynomial in x of degree three or four with simple roots [6].

Mathematicians would continue to struggle with the evaluation of these integrals into the early 1800s. Around this time Gauss, Abel, and Jacobi came up with an alternative method for studying these integrals. They looked not at the integral itself, but at the inverse of the integral. This opened up an entirely new class of functions known as elliptic functions [10] [6].

Definition 2.1.2. An elliptic function is a meromorphic function that is doubly-periodic in $\mathbb{C}$, this being a function that is analytic everywhere in the complex plane except at its poles with two independent periods ω_1, ω_2 such that $f(z) = f(z + \omega_1) = f(z + \omega_2)$ and ω_1/ω_2 has positive imaginary part.

Note that the periods of f form a lattice $\mathbb{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ such that for every $\omega \in \mathbb{L}$, $f(z) = f(z + \omega)$. The complex plane is then tesselated by f, repeating itself every period. The quotient space of $\mathbb{C}/\mathbb{L}$ then forms a torus, commonly denoted $\mathbf{X}$. This torus is the elliptic curve uniquely determined by the field of elliptic functions defined on it.

Definition 2.1.3. The fundamental cell of the torus $\mathbf{X}$ obtained from the lattice $\mathbb{L}$ with periods ω_1 and ω_2 is the set

$$\mathcal{F} = \{x = \alpha\omega_1 + \beta\omega_2 \ \mid \ 0 \leq \alpha \leq 1, \ 0 \leq \beta \leq 1\}$$

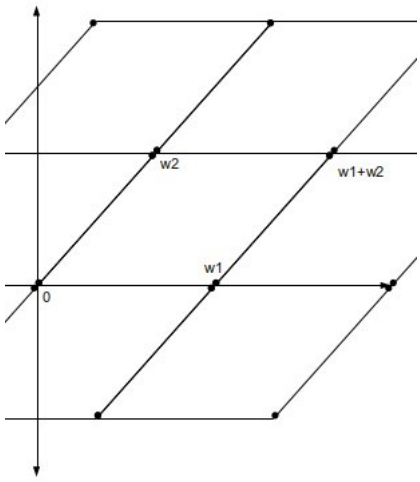


Figure 2.2: The tesselation and period lattice of an elliptic function f in $\mathbb{C}$

Given a period lattice $\mathbb{L}$, we want to be able to find an elliptic function f in the complex torus formed by the lattice. The laws of complex integration require f to have at least 2 poles and 2 corresponding roots in the fundamental cell. In 1850, taking advantage of the simplest of these cases, Weierstrass constructed such a function by placing a double pole at the origin. The function,

$$\wp(x) = \frac{1}{x^2} + \sum_{\omega \in \mathbb{L}^2 - 0} \left[\frac{1}{(x-\omega)^2} - \frac{1}{\omega^2} \right]$$

sums over all periods ω in the lattice and has a double pole at the origin, and therefore at every point $\omega \in \mathbb{L}$. Note that these are also the only points at which $\wp$ has a pole. [6]

The following lemma will prove useful when studying the derivative of $\wp$.

Lemma 2.1.1. *The function $\wp$ is an even function.*

Proof. Note that

$$\wp(-x) = \frac{1}{(-x)^2} + \sum_{\omega \in \mathbb{L}^2 - 0} \left[\frac{1}{(-x-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{(-x)^2} + \sum_{\omega \in \mathbb{L}^2 - 0} \left[\frac{1}{(-1(x-(-\omega))^2} - \frac{1}{(-\omega)^2} \right]$$

$$= \frac{1}{(x)^2} + \sum_{-\omega \in \mathbb{L}^2 - 0} \left[\frac{1}{(x-\omega)^2} - \frac{1}{\omega^2} \right] = \wp(x)$$

The last equality follows from the fact that $\mathbb{L} = -\mathbb{L}$. $\square$

Now consider the derivative of $\wp$.

$$\wp'(x) = \frac{-1}{\omega^3} + -2\sum_{\mathbb{L}}\left[\frac{1}{(x-\omega)^3}\right]$$

This function has a triple pole at the origin, is odd by Lemma 3.1, and has three roots, one at each half-period in the lattice. Using that fact that $\wp'$ is odd, note that

$$\wp'(\omega/2) = \wp'(\omega/2 - \omega) = \wp'(-\omega/2) = -\wp'(\omega/2)$$

Thus, $\wp'(\omega/2) = 0$. Given the fundamental periods ω_1 and ω_2, there are three half periods in the cell. Define the values of $\wp$ at these points to be

$$e_1 = \wp(\omega_1/2) \qquad e_2 = \wp(\omega_1/2 + \omega_2/2) \qquad e_3 = \wp(\omega_2/2)$$

We can now express $\wp'$ a cubic function of $\wp$ in the differential equation

$$(\wp')^2 = 4(\wp - e_1)(\wp - e_2)(\wp - e_3)$$

When evaluated at the half periods, both sides of the equation are zero,

$$(\wp'(\omega_1/2))^2 = 4(e_1 - e_1)(\wp - e_2)(\wp - e_3) = 0$$

and both sides of the equation have a pole of order 6 at 0.

To tie this idea back into the idea that these functions are the inverse of elliptic integrals, note that

$$\wp' = \frac{d\wp}{dx} \Rightarrow dx = \frac{d\wp}{\wp'} = \frac{1}{2}\sqrt{\frac{1}{(\wp - e_1)(\wp - e_2)(\wp - e_3)}}d\wp$$

The Weierstrass $\wp$ function leads directly into the study of elliptic curves. Recall that an elliptic curve is the torus $\mathbf{X} = \mathbb{C}/\mathbb{L}$. This torus has the same structure as the cubic

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3)$$

and begins to look like the familiar format of elliptic curves with which we will be dealing in the remainder of this paper.

2.1.2 Terms and Definitions

For this project, we will mostly be considering rational solutions of an elliptic curve E and also the group of integer points modulo a prime p, denoted $E(\mathbb{Q})$ and $E(\mathbb{F}_p)$, respectively. The solutions form a group under the following additive law:

Definition 2.1.4. The rule for adding two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ to get the point $P + Q = (x_3, y_3)$, on an elliptic curve $E : y^2 = x^3 + ax + b$ is as follows:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y} & \text{if } x_1 = x_2 \end{cases}$$

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

$$y_3 = -(y_1 + \lambda(x_3 - x_1))$$

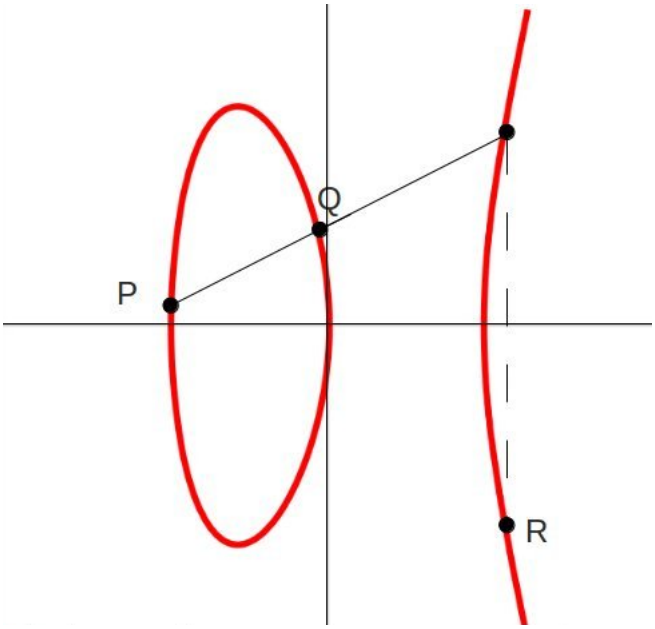


Figure 2.3: Adding two points on a curve

Conceptually, the process of adding two points involves finding the third point of intersection with the line through P and Q and reflecting it across the x-axis. Consider the value of λ as being the slope of the line defined by

the two points on the curve P and Q. If these points have different x-values, the slope takes on the familiar form

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

If however, these two points are the same, the line between them is taken to be the tangent of the curve at that point. In this case, the slope of a tangent is the derivative $\partial y/\partial x$ of the equation $y^2 = x^3 + ax + b$, so $2yy' = 3x^2 + a$ and

$$\lambda = \frac{3x^2 + a}{2y}$$

We now have the line $y = \lambda x + \nu$ where ν is the intercept of the line $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$ representing the line between the two known points. To find the third point of intersection, we substitute this into the equation for the elliptic curve:

$$(\lambda x + \nu)^2 = x^3 + ax + b = \lambda^2 x^2 + 2\lambda\nu x + \nu^2$$

$$x^3 + ax + b - \lambda^2 x^2 - 2\lambda\nu x - \nu^2 = 0$$

The solutions to this cubic equation give the three points x_1, x_2, and x_3 at which the line intercepts the curve [8].

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

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = x^3 + (-x_1 - x_2 - x_3)x^2 + (x_1x_2 + x_2x_3 + x_1x_3)x - x_1x_2x_3$$

The coefficients for each term must be equal, so by looking at the x^2 term,

$$\lambda^2 = x_1 + x_2 + x_3$$

and so the formula for the x-value of the third point of intersection is $x_3 = \lambda^2 - x_1 - x_2$.

To derive the y-value, we simply take the y-value of the third point of intersection, $y_3 = \lambda x_3 + \nu$ and reflect it across the x-axis.

$$y_3 = -(\lambda x_3 + y_1 - \lambda x_1) = -(y_1 + \lambda(x_3 - x_1))$$

From this addition rule, we can define a closed formula for the double of a rational point.

Definition 2.1.5. Given a point $P = (x, y)$ on an elliptic curve $E : y^2 = x^3 + ax + b$, the value of the x-coordinate for the double of a rational point $2P = (x', y')$ is

$$x' = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$$

This is derived from the additive law as follows:

$$x' = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x = \frac{9x^4 + 6x^2a + a^2}{4y^2} - 2x$$

$$= \frac{9x^4 + 6x^2a + a^2 - 8xy^2}{4y^2} = \frac{9x^4 + 6x^2a + a^2 - 8x(x^3 + ax + b)}{4(x^3 + ax + b)}$$

$$x' = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$$

The trouble of finding a third point of intersection arises only when summing two points on the curve with the same x-coordinate. The line intersecting these points is then a vertical line. In this case, we denote the third point of intersection to be the point at infinity. This also serves as the identity of the group.

Definition 2.1.6. The identity of the group of solutions on an elliptic curve E is the point at infinity, denoted $\mathbf{O}$. From this, we also define the inverse, P^{-1} of any point $P = (x, y)$ to be the point $P^{-1} = (x, -y)$.

Two points add up to the identity if and only if they are independent and have the same x-value. Therefore, since the curve is symmetric about the x-axis, the y-coordinates must have opposite signs. From this, we can define the inverse of any point P to be the point that when added to P produces the identity.

By adding a point to itself multiple times, sometimes we arrive back at the identity, $\mathbf{O}$. The number of times a point must be added to itself to reach infinity is the order of that point.

Definition 2.1.7. We denote the order of a point P on an elliptic curve to be the smallest positive integer n, if it exists, such that $nP = \mathbf{O}$. By adding P together n times, we will reach the identity. If no such integer exists, we say P has infinite order.

Solutions to an elliptic curve can be separated into two groups: those of finite order and those of infinite order. Points of infinite order will never

reach the identity. The rank of an elliptic curve is tied in with the structure of the solutions of infinite order. But first, we must consider the structure of the points of finite order and their relationship with the solutions of an elliptic curve in a finite field.

2.2 Elliptic Curves Over Finite Fields

An important group in the study of elliptic curves over rational fields are the solutions over a finite field modulo a prime p. These solutions form a group under the same additive law described above and prove to have important connections to the rational solutions. The group $E(\mathbb{F}_p)$ is also the basis of elliptic curve cryptography.

Given an elliptic curve E, the solutions to the curve in a field $\mathbb{F}_p$ form a group under the same addition, identity and inverse rule as described above. Consider the following example.

Example 2.2.1. Let $E : y^2 = x^3 - 4x + 2$ be an elliptic curve and consider $E(\mathbb{F}_5)$, the set of solutions to the curve modulo 5. Two solutions to this curve are the points $P = (1, 2)$ and $Q = (4, 0)$.

$$4 = 2^2 = 1^3 - 4(1) + 2 = -1 \pmod 5$$

To add these points, we follow the same procedure above:

$$\lambda = \frac{0-2}{4-1} \pmod 5 = 2 \times 3^{-1} \pmod 5 = 2 \times 2 \pmod 5 = 4$$

$$x_3 = 4^2 - 1 - 4 \pmod 5 = 1$$

$$y_3 = -(2 + 4(1 - 1)) = -2$$

Therefore $P + Q = (1, -2)$

Another important piece of information about an elliptic curve is the order of the group of solutions modulo a prime p. As we will see later, this will aid in determining the configuration of the group of rational solutions. Given an elliptic curve $E : y^2 = x^3 + ax + b$, the order of the group of solutions to this curve in $\mathbb{F}_p$ can be found using the calculation

$$|E(\mathbb{F}_p)| = \sum_{x=0}^{p-1} \left[\left(\frac{x^3 + ax + b}{p} \right) + 1 \right]$$

which calculates the Legendre symbol for every possible value of x. The Legendre symbol determines whether or not x^3+ax+b is a quadratic residue modulo p. If it is, the square root exists and there is a solution (x, y) to the curve $y^2 = x^3 + ax + b$. In fact, there are two solutions since both y and $-y$ square to the same value. If the Legendre symbol is 0, there is one solution, and if -1, there are none. $|E(\mathbb{F}_p)|$ can then be found by summing up one more than the Legendre sumbol for every value of $x \in \mathbb{F}_p$.

2.3 Rational Solutions to Elliptic Curves

From here on in, we will assume an elliptic curve E to have rational coefficients. Then, the group of rational solutions to an elliptic curve can be broken into two main parts: the set of points of finite order and the set of points of infinite order. Points of finite order are known as the torsion points of a curve.

Definition 2.3.1. The torsion points of an elliptic curve over the rational numbers $E(\mathbb{Q})$ are defined as all points with finite order.

This leads into an important theorem by Mordell that breaks the group structure of an elliptic curve into torsion points and copies of the integers while also introducing the concept of rank.

Theorem 2.3.1. *(Mordell) The group of rational points on an elliptic curve $E(\mathbb{Q})$ is isomophic to*

$$\mathbb{Z}^r \oplus E(\mathbb{Q})_{TORS}$$

where r is the **rank** *of the curve.*

Computing the ranks of elliptic curves is a computationally complicated problem. It has recently been shown by Bhargava [1] that more than half of all elliptic curves have rank 0. We have managed to find two infinite families of elliptic curves for which the rank is greater than or equal to 2.

Due to the structure of an elliptic curve, a rational solution $P = (x, y)$ has the following property:

Theorem 2.3.2. *Let $P = (x, y)$ be a rational point on the elliptic curve $E : y^2 = x^3 + ax + b$. Then,*

$$x = \frac{u}{r^2}, \qquad y = \frac{v}{r^3}$$

for integers u, r, and v with $gcd(u, r) = gcd(v, r) = 1$.

Proof. Since x and y are rational numbers, we can represent them in reduced form as

$$x = \frac{u}{m}, \qquad y = \frac{v}{n}$$

with $u, m, n, v \in \mathbb{Z}$. Now let p be a prime that divides the denominator of x, $p \mid m$. Then there exist integers s and t such that

$$x = \frac{u}{sp^{\mu}}, \qquad y = \frac{v}{tp^{\nu}}$$

where $\mu > 0$ and $\nu \geq 0$ and $\gcd(u, p) = \gcd(v, p) = \gcd(s, p) = \gcd(t, p) = 1$. By plugging this into the equation for the curve,

$$\left(\frac{v}{tp^{\nu}}\right)^2 = \left(\frac{u}{sp^{\mu}}\right)^3 + a\left(\frac{u}{sp^{\mu}}\right) + b$$

$$\frac{v^2}{t^2p^{2\nu}} = \frac{u^3 + aus^2p^{2\mu} + bs^3p^{3\mu}}{s^3p^{3\mu}}$$

Note that since $\gcd(u, p) = 1$, then $p \not| (u^3 + aus^2p^{2\mu} + bs^3p^{3\mu})$ and since $\gcd(v, p) = 1$ that $p \not| v^2$. Therefore,

$$p^{2\nu} = p^{3\mu} \Rightarrow 2\nu = 3\mu$$

It follows that $3 \mid \nu$ and $2 \mid \mu$ and so $\nu = 3\sigma$ and $\mu = 2\sigma$ for some $\sigma > 0$. Since this works for all prime divisors of m and n, it follows that $m = r^2$ and $n = r^3$ for some $r \in \mathbb{Z}$. □

This fact is used in the proof of the Lutz-Nagell Theorem as well as our theorems that certain points on a curve cannot be doubles of other rational points.

Elliptic curves behave uniquely in each of these contexts. In the complex plane, they are tori, in the reals they are symmetric curves about the x-axis, and finite groups in prime fields. Each of these views provides insight into the structure of the solutions over the rationals examined in this paper.

Chapter 3

Methods

The methods used in this paper for bounding the ranks of entire families of elliptic curves are modeled after those used by Brown and Meyers in their paper "Elliptic Curves from Mordell to Diophantus and Back" [2]. In this paper they prove that elliptic curves of the form $E_m : y^2 = x^3 - x + m^2$ for all integers $m > 1$ have rank at least 2. In doing this, they outline a method that can be modified and extended to put lower bounds on ranks of different families of elliptic curves.

The method consisted of three main parts. The first being finding a family of curves that displays a pattern of having both trivial rational torsion and a rank of 2 or greater. The next step involved proving trivial torsion for these curves, and finally, putting a lower bound on the rank by finding distinct solutions that are not the doubles of other rational points.

3.1 Finding Curves of High Rank

The first step of the process is to find a family of curves that fit the criteria outline above. To accomplish this, we ran tests using Sage [9], a computer algebra package with methods for determining the rank of a given elliptic curve. Brown and Meyers [2] identified the family of curves $E_m : y^2 = x^3 - m^2x + 1$ at the end of their paper as also exhibiting the pattern of having high rank and trivial rational torsion. By trial and error, we were able to discover another family of curves with trivial torsion and rank greater than or equal to 2. This behavior was verified for high values of m.

Once this was verified for values of m into the 100's, we made a conjecture that this pattern would follow for all natural numbers m. The next two steps involved proving that the data we had collected up to this point held for the

entire family of curves.

3.2 Proving Trivial Torsion

After a family of elliptic curves shows promise of having high ranks through rigorous data collection, the next step of the process is to prove that the torsion group of these curves is trivial, that is to say, that the only solution with finite order is the identity at infinity, **O**.

Proving trivial torsion for an entire family of curves can be made easier with the help of the several theorems [8].

Theorem 3.2.1. *(Nagell-Lutz) Let*

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

be a non-singular cubic curve with integer coefficients a,b; and let D be the discriminant of the cubic polynomial f(x),

$$D = -4a^3 - 27b^2.$$

Let $P = (x, y)$ be a point of finite order. Then x and y are integers, and either $y = 0$, in which case P has order 2, or y divides D.

The Nagell-Lutz theorem states that every point of finite order must have integer coordinates. We used this to prove trivial rational torsion by ruling out possible points of finite order by showing they were not integers and thus of infinite order.

The next theorem uses the number of solutions to a curve in a finite field to deduce information about the size and structure of the torsion group. A proof of this result can be found in [7].

Theorem 3.2.2. *Let C be a non-singular elliptic curve*

$$C : y^2 = x^3 + ax + b$$

with discriminant

$$D = -4a^3 - 27b$$

with integer coefficients a and b. For any prime p, as long as p does not divide $2D$, the reduction modulo p of the curve C is an isomorphism of $C(\mathbb{Q})_{TORS}$ onto a subgroup of $C(\mathbb{F}_p)$.

By examining a curve over multiple fields, we can rule out certian structures of the torsion group. As the next theorem tells us, there are only a finite number of structures a torsion group can have.

Theorem 3.2.3. *(Mazur) Let E be an elliptic curve over $\mathbb{Q}$ and suppose that the Mordell-Weil group $E(\mathbb{Q})$ contains a point of finite order N, Then either $1 \leq N \leq 10$ or $N = 12$. More precisely, the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following 15 groups:*

$$\mathbb{Z}/m\mathbb{Z} \text{ for } m \leq 10 \text{ or } m = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2v\mathbb{Z} \text{ for } v \leq 4$$

This discovery was made by mathematician Barry Mazur, and a proof of it can be found in [5]. These proofs provide the tools necessary to prove trivial torsion for the curves in this paper. By collecting information on the orders of the curves over finite fields, the roots of the curves in $\mathbb{R}$, and the inflection points of the curve we have everything we need for our proofs.

3.3 Putting a Lower Bound on the Rank

The next step in the process of proving that a family of elliptic curves has a high rank was to put a lower bound on what the rank could possibly be. To do this, we drew on an important theorem that relates the rank of elliptic curves to doubles of rational points and requires trivial rational torsion as a condition [3].

Theorem 3.3.1. *Let $E(\mathbb{Q})$ be the group of rational points on an elliptic curve E and $2E(\mathbb{Q})$ be the doubles of rational points on the elliptic curve. Suppose also that E has trivial rational torsion. Then the quotient group $E(\mathbb{Q})/2E(\mathbb{Q})$ is an elementary abelian 2-group of order 2^r where r is the rank of $E(\mathbb{Q})$.*

As a result of this theorem, if we can find a collection of n points that are not the doubles of rational points and are independent of each other (i.e. are elements of different cosets of $2E(\mathbb{Q})$), we know that the quotient group has order at least n and that the rank of the curve must be at least $\lceil \log_2(n) \rceil$. The goal of this step in the process is then to find points in the desired family of curves that are not doubles of other rational points. The proof of this is aided by the double point formula derived earlier. Recall that the x-coordinate of the double of a rational point $P = (x, y)$ is

$$x' = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}$$

This, along with the theorem that on an elliptic curve $y^2 = x^3 + ax + b$, the rational solutions x and y must be of the form $x = u/s^2$ $y = v/s^3$ were used to prove, by contradiction that these independent points cannot be the doubles of rational points on the curve.

After finding points P, Q, and $P + Q$ that are not doubles of other rational points, we then proved that the cosets $[P], [Q], [P + Q]$ are indeed distinct and form a subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$. In fact, the following lemma shows that if we have already proven they are not doubles of rational points, it follows immediately that they form distinct cosets. [2]

Lemma 3.3.1. *Let P, Q, and $P+Q$ be solutions to an elliptic curve $E(\mathbb{Q})$ that are not doubles of rational points. Then, the cosets $[P], [Q], [P + Q] \in E(\mathbb{Q})/2E(\mathbb{Q})$ are distinct.*

Proof. We know $[P] \neq [\mathbf{O}]$, $[Q] \neq [\mathbf{O}]$, and $[P + Q] \neq [\mathbf{O}]$. If we assume for the sake of contradiction that $[P] = [Q]$, it follows that

$$[P + Q] = [P] + [Q] = [P] + [P] = [2P] = [\mathbf{O}]$$

which is a contradiction. Similarly, if $[P] = [P + Q]$,

$$[P] + [Q] = [P + Q] = [P] + [\mathbf{O}]$$

and if $[Q] = [P + Q]$, then

$$[P] + [Q] = [P + Q] = [\mathbf{O}] + [Q]$$

Therefore, these cosets are all distinct. □

This result can be extended for larger groups of points as well and is the last piece in the puzzle to putting a lower bound on the rank of an elliptic curve.

Chapter 4

Data

By collecting data on rank and torsion groups of different families of elliptic curves, we were able to confirm the pattern seen by Brown and Meyers on the family of curves $C_m : y^2 = x^3 - m^2 + 1$ as well as discover another family of curves with high rank. This family, which we will denote K_m, has the form

$$K_m : y^2 = x^3 + m^3x - m^3$$

These curves all appear to have trivial torsion groups and rank at least 2 for all $m \geq 4$.

4.1 Curves of the form $C_m : y^2 = x^3 - m^2x + 1$

The first family of curves we are considering are the set of curves $C_m : y^2 = x^3 - m^2x + 1$ for all $m \in \mathbb{N}$. To collect data on the ranks of the curves, we used the following Sage script:

```
for m in range(2,5):
    a = -m*m
    b = 1
    if(4*a^3+27*b^2 != 0):
        R = EllipticCurve([0,0,0,a,b]).rank()
        print R
        T = EllipticCurve([0,0,0,a,b]).torsion()
        print T
```

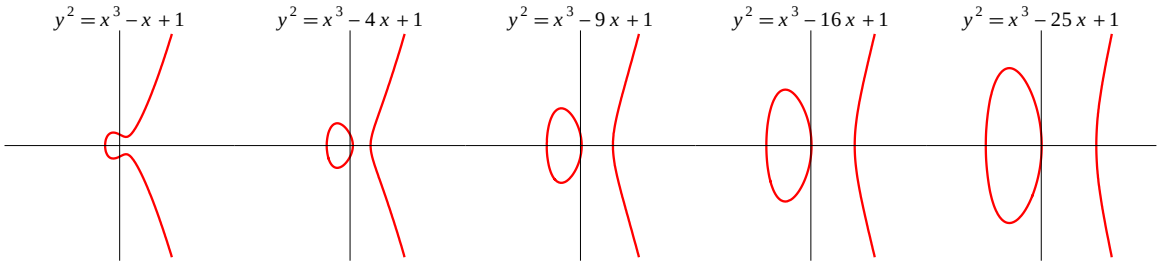
These commands print out the rank and the torsion group for all curves of the form C_m with values of m from x to y.

The following table contains ranks of elliptic curves for values of m.

r	m such that the rank of $C_m = r$
2	2, 3,
3	4, 5, 6, 7, 9, 10, 11, 12, 15, 18, 21
4	8, 13, 14, 16, 19, 20, 22, 23, 26, 27
5	17, 25, 36, 41, 42, 46, 53, 59, 70
6	61, 107, 124, 128, 146, 148, 199

Table 4.1: Ranks of the curves in the family C_m.

The Mathematica plots of these curves over the reals ($C_m(\mathbb{R})$) produced the following output for the first few values of m, $1 \leq m \leq 5$.



(a) $m = 1$ (b) $m = 2$ (c) $m = 3$ (d) $m = 4$ (e) $m = 5$

Figure 4.1: Plots of Elliptic Curves C_m over the reals.

These results allow us to state

Theorem 4.1.1. *Let m be a nonnegative integer, and let C_m be the elliptic curve with equation $y^2 = x^3 - m^2x + 1$. Then C_m has rank at least 3 for all $m \geq 4$.*

4.2 Curves of the form $K_m : y^2 = x^3 + m^3x - m^3$

The next family of curves was discovered by running Sage scripts for various values of a and b in the equation $y^2 = x^3 + ax + b$.

To collect data on the ranks of the curves, we used the following Sage script:

```
for m in range(2,5):
    a = m*m*m
    b = -m*m*m
    if(4*a^3+27*b^2 != 0):
```

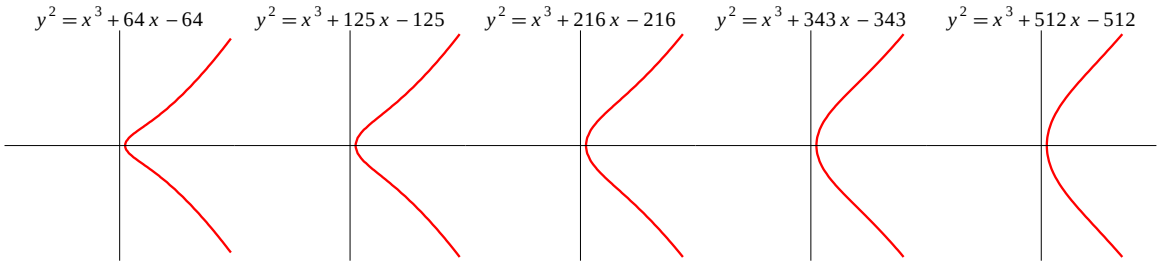
r	m such that the rank of $K_m = r$
1	1, 3
2	2, 4-12, 14-18, 20, 21, 22, 24, 25, 27, 36, 42, 44
3	13, 19, 23, 26, 28, 29, 30, 32, 33, 35, 37, 39, 40, 41, 43, 45, 46
4	31, 38

Table 4.2: Ranks of the curves in the family K_m.

```
R = EllipticCurve([0,0,0,a,b]).rank()
print R
T = EllipticCurve([0,0,0,a,b]).torsion()
print T
```

These commands print out the rank and the torsion group for all curves of the form K_m with values of m from x to y. Table 4.2 contains data on ranks with respect to values of m for elliptic curves of the form $K_m : y^2 = x^3 + m^3x - m^3$.

The Mathematica plots of these curves over the reals ($K_m(\mathbb{R})$) produced the following output for the first few values of m, $4 \leq m \leq 8$.



(a) $m = 4$ (b) $m = 5$ (c) $m = 6$ (d) $m = 7$ (e) $m = 8$

Figure 4.2: Plots of Elliptic Curves K_m over the reals.

These results allow us to state and eventually prove the theorem

Theorem 4.2.1. *Let m be a nonnegative integer, and let K_m be the elliptic curve with equation $y^2 = x^3 + m^3x - m^3$. Then C_m has rank at least 2 for all $m > 3$.*

Chapter 5

Proving Results

After collecting data that strongly suggests high ranks for curves in the two families C_m and K_m, we proved this to be true for all values of $m \in \mathbb{N}$. This is done in two parts. First we showed that each family has a trivial torsion group. We then found points that are not the doubles of other rational points and proved their independence from each other to put a lower bound on the ranks of the curves.

To accomplish the first task, we used a combination of theorems, such as the Nagell-Lutz theorem coupled with the size of each family of curves over finite fields of prime order. These proofs combine the algebraic and geometric properties of elliptic curves over rational, real, and finite fields.

5.1 Curves of the form $C_m : y^2 = x^3 - m^2x + 1$

As the data suggests, these curves all have a trivial torsion group and rank at least 2 for values of m greater than or equal to 2 and a rank of 3 or greater for values of m greater than 3. A proof for the former statement follows and a start on the latter is in the appendix at the end of the paper.

5.1.1 Proving Trivial Torsion

We have determined computationally that curves in this family generally have trivial torsion groups, and now prove it to be true for all integers $m > 1$.

Theorem 5.1.1. *If $m > 1$, then $C_m(\mathbb{Q})_{TORS} = \mathbf{O}$.*

Proof. The discriminant $\Delta(C_m) = -16(27-4m^6)$ is never divisible by 5 or 7 so there is good reduction at 5 and 7. For a proof of this, first assume for the

sake of contradiction that $\Delta(C_m)$ is divisible by 5. It follows that $5 \mid (27 - 4m^6) \Rightarrow 27 \equiv 4m^6 \pmod 5 \Rightarrow 3 \equiv m^6 \pmod 5$. This is a contradiction since 3 is not a quadratic residue modulo 5 and therefore, the 6th root of 3 does not exist. The same method holds for modulo 7.

If $5|m$, then the curve C_m reduces to $y^2 = x^3 + 1$ in $\mathbb{F}_5$. Note that $|C_m(\mathbb{F}_5)| = 6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. $C_m(\mathbb{Q})_{\text{TORS}}$ is isomorphic to a subgroup of $C_m(\mathbb{F}_5)$. So, $C_m(\mathbb{Q})_{\text{TORS}} \cong \{\mathbf{O}\}, \mathbb{Z}_2, \mathbb{Z}_3,$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Consider first the groups $\mathbb{Z}_2$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Both of these groups have elements of order 2. In elliptic curves, an element of order 2 implies $(x, y) = (x, -y)$ for some $(x, y) \in C_m$. Thus, $y = 0$ and $y^2 = 0 = x^3 - m^2x + 1$. These are roots of the curve C_m and by the Nagell-Lutz theorem, a root x of C_m is rational if and only if x is an integer. Now let $C_m = f(x) = x^3 - m^2x + 1$ and consider the following values of $f(x)$ for all values of $m > 1$.:

$$f(0) = (0)^3 - m^2(0) + 1 = 1 > 0$$
$$f(1) = (1)^3 - m^2(1) + 1 = 2 - m^2 < 0$$

This implies there is a root between 0 and 1. Since the root must have finite order and is not an integer, by the Nagell-Lutz Theorem, it is not rational. The same goes for the following values:

$$f(-(m+1)) = -(m+1)^3 + m^2(m+1) + 1 = -2m^2 - 3m < 0$$
$$f(-m) = -(m)^3 + m^2(m) + 1 = -m^3 + m^3 + 1 = 1 > 0$$
$$f(m-1) = (m-1)^3 - m^2(m-1) + 1 = -2m^2 + 3m < 0$$
$$f(m) = m^3 - m^2(m) + 1 = m^3 - m^3 + 1 = 1 > 0$$

These values show there are roots between $-(m+1)$ and $-m$ and between $m-1$ and m respectively.

By the previous argument, these cannot be rational roots. Since all points of order 2 must be roots, it follows there are no elements of order 2 in $C_m(\mathbb{Q})_{\text{TORS}}$. This leaves $C_m(\mathbb{Q})_{\text{TORS}} \cong \{\mathbf{O}\}$ or $\mathbb{Z}_3$. Note all elements in $\mathbb{Z}_3$ are inflection points of the curve. All inflection points P satisfy $3P = \mathbf{O}$ and therefore $2P = -P$. The x coordinate of $2P$ must then equal the x coordinate of P [8]. A point on C_m as order 3 if and only if it is a root of the polynomial equation

$$3x^4 - 6m^2x^2 + 12x + m^4$$

Using Mathematica, we can deduce that these roots cannot take on rational values. The output of the function

$$\text{FullSimplify[NSolve}[3x\text{\^{}}4 - 6m\text{\^{}}2x\text{\^{}}2 + 12x + m\text{\^{}}4 == 0, x]]$$

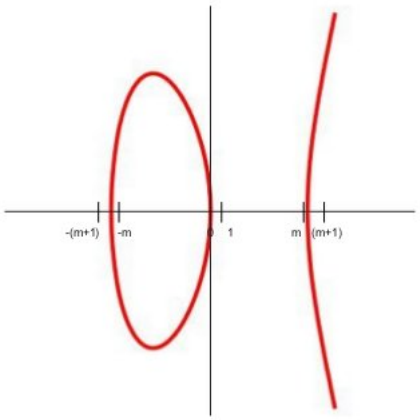


Figure 5.1: Where curves of this family cross the y-axis

cannot be a rational number, much less an integer.

Now consider the case where $5 \not| m$. Then, $m \equiv \pm 1$ or $\pm 2 \pmod 5$. Thus C_m reduces in $\mathbb{F}_5$ to $y^2 = x^3 - x + 1$ or $y^2 = x^3 + x + 1$.

- $y^2 = x^3 - x + 1$
  $|C_m(\mathbb{F}_5)| = 8$. The number of rational torsion points $|C_m(\mathbb{Q})_{\text{TORS}}| = 1, 2, 4,$ or 8. By [Silverman pg 123], $C_m(\mathbb{Q})_{\text{TORS}}$ is isomorphic to a subgroup of $C_m(\mathbb{F}_5)$. Note that $C_m(\mathbb{F}_5) \cong \mathbb{Z}_8$, The generating element being the point $(1, 1)$. This means $C_m(\mathbb{Q})_{\text{TORS}}$ is isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, or $\{O\}$. All of these groups, excluding the trivial group have elements of order 2. We just proved above that C_m has no points of order 2. Therefore, $C_m(\mathbb{Q})_{\text{TORS}} = \{\mathbf{O}\}$.

- $y^2 = x^3 + x + 1$
  $|C_m(\mathbb{F}_5)| = 9$. The number of rational torsion points $|C_m(\mathbb{Q})_{\text{TORS}}| = 1, 3,$ or 9. As shown above, C_m has no rational inflection points. Therefore, $C_m(\mathbb{Q})_{\text{TORS}} = \{\mathbf{O}\}$.

□

5.1.2 Bounding the Ranks

The next theorem proves that the points P,Q,and P+Q are not doubles of rational points on C_m. The data collected suggests that the rank of these curves have a lower bound of 3. We have identified the possible third point and the cosets associated with it, however partial proofs for these points are

left to the appendix at the end of the paper. A complete proof for these points does not yet exist, however we do have complete proofs for the points P, Q, and P+Q.

Theorem 5.1.2. *Let $A = (u/s^2, v/s^3)$ and $B = (w/t^2, z/t^3)$ be points on C_m with $gcd(uv, s) = 1$ and $gcd(wz, t) = 1$. $A \neq 2B$ if:*

(a) $A = P = (0, 1)$

(b) $A = Q = (-1, m)$

(c) $A = P + Q = (1 - m, -m^3 + 3m^2 - 4m + 3)$

(e) $A = R = (m, 1)$

(d) $A = P + R = (-m, -1)$

(f) $A = Q + R = \left(-\frac{(-1+m)\left(2+m+m^2\right)}{(1+m)^2}, -\frac{3-m+3m^2+m^3+2m^4}{(1+m)^3}\right)$

(g) $A = P + Q + R = \left(\frac{2+m+m^3}{(-1+m)^2}, -\frac{3+m+3m^2-m^3+2m^4}{(-1+m)^3}\right)$

Proof. Let $B = (x, y)$ and $A = (x_0, y_0) = 2B$. From the rules for adding points on elliptic curves,

$$x_0 = \left(\frac{3x^2 + (-m^2)}{2y}\right)^2 - 2x = \frac{9x^4 - 6m^2x^2 + m^4 - 8xy^2}{4y^2}$$

By substituting our equation for $C_m : y^2 = x^3 - m^2x + 1$ into the equation we get

$$x_0 = \frac{9x^4 - 6m^2x^2 + m^4 - 8x(x^3 - m^2x + 1)}{4(x^3 - m^2x + 1)} = \frac{x^4 + 2m^2x^2 - 8x + m^4}{4(x^3 - m^2x + 1)}$$

We can now substitute $x_0 = u/s^2$ and $x = w/t^2$ to get the equation

$$4ut^2(w^3 - m^2wt^4 + t^6) = s^2((w^2 + m^2t^4)^2 - 8wt^6) \tag{5.1}$$

(a) In this case, $u = 0$ and $s = 1$. Then equation (5.1) is

$$(w^2 + m^2t^4)^2 - 8wt^6 = 0$$

$$(w^2 + m^2t^4)^2 = 8wt^6$$

$$w^4 + 2w^2m^2t^4 + m^4t^8 = 8wt^6$$

$$w^4 = 8wt^6 - 2w^2m^2t^4 - m^4t^8$$

Since t must divide both sides, this implies $t \mid w$, but since $\gcd(t, w = 1)$, then $t = 1$.

$$w^4 = 8w - 2w^2m^2 - m^4$$

$$w^4 + 2m^2w^2 + m^4 = 8w$$

$$(w^2 + m^2)^2 = 8w$$

Since w^2+m^2 is an integer, this implies $\sqrt{8w}$ is an integer which implies $w = 2l^2$ for some integer l. Then, $w^2 + m^2 = 4l$ and $2l^2 + m^2 = 4l$. Since l is an integer, it follows that $l^2 > l$ making the left hand side larger than the right hand side of the equation which is a contradiction. Therefore, $P = (0, 1)$ cannot be the double of a rational point.

(b) In this case, let $u = -1$ and $s = 1$. Then equation (5.1) is

$$-4t^2(w^3 - m^2wt^4 + t^6) = ((w^2 + m^2t^4)^2 - 8wt^6$$

Now consider this equation modulo 8.

$$4t^2(w^3 - m^2wt^4 + t^6) \equiv (w^2 + m^2t^4)^2 \pmod 8$$

There are three possible cases, if w is even and t is odd, if w is odd and t is even, or if both w and t are odd.

- Let w be even.

$$4t^6m^2w + 4t^8 \equiv m^4t^8 \pmod 8$$

$$4(m^2w + t^2) \equiv m^4t^2 \pmod 8$$

It follows that m is even since the left hand side is even and t cannot be. Then $4t^2 \equiv 0 \pmod 8$. This implies that t is even which is a contradiction.

- Let t be even.

$$(w^2 + m^2t^4)^2 \equiv 0 \pmod 8$$

$$w^4 \equiv 0 \pmod 8$$

This implies w is even which is a contradiction.

– Let w and t be odd. Note that for any odd integer k, $k^2 \equiv 1 \pmod 8$.

$$4(1 - m^2 w + 1) \equiv (1 + m^2)^2 \pmod 8$$

$$4m^2 w \equiv 1 + 2m^2 m^4 \pmod 8$$

if m is even, it follows that $0 \equiv 1 \pmod 8$ which is a contradiction. If m is odd, $4w \equiv 2 \pmod 8$ which is again a contradiction. Therefore, $Q = (-1, m)$ cannot be the double of a rational point.

(c) In this case, let $u = 1 - m$ and $s = 1$. Then,

$$4(1 - m)t^2(w^3 - m^2 w t^4 + t^6) = (w^2 + m^2 t^4)^2 - 8wt^6$$

This implies $t \mid w$ and so $t = 1$ since $\gcd(w, t) = 1$.

$$4(1 - m)(w^3 - m^2 w + 1) = (w^2 + m^2)^2 - 8w$$

Now consider this equation modulo 8.

$$4(1 - m)(w^3 - m^2 w + 1) \equiv (w^2 + m^2)^2 \pmod 8$$

There are 4 cases here

– w is even and m is odd

$$0 \equiv (w^2 + 1)^2 \pmod 8 \Rightarrow 0 \equiv 1 \pmod 8$$

This is a contradiction.

– w is even and m is even

$$4(1 - m)(w^2 - m^2 w + 1) \equiv 0 \pmod 8$$

$$4(\text{odd})(\text{odd}) \equiv 0 \pmod 8$$

This is a contradiction.

– w is odd and m is even

$$4(1 - m)(1 - m^2 + 1) \equiv (1 + m^2)^2 \pmod 8$$

$$0 \equiv 1 \pmod 8$$

This is a contradiction.

– w is odd and m is odd

$$4(1-m)(1-m^2+1) \equiv (1+m^2)^2 \pmod 8$$

$$0 \equiv 4 \pmod 8$$

This is a contradiction.

Therefore the point $P+Q = (1-m, -m^3+3m^2-4m+3)$ cannot be the double of a rational point.

(d) See Appendix

(e) See Appendix

(f) See Appendix

(g) See Appendix

□

Now that we have established these points are not doubles of rationals, we must establish their independence and existence as elements of the group $E(\mathbb{Q})/2E(\mathbb{Q})$.

Theorem 5.1.3. *Let $P = (0,1)$, $Q = (m,1)$ and $R = (-1,m)$. Then*

$$H = \{[\mathbf{O}], [P], [Q], [R], [P+Q], [P+R], [Q+R], [P+Q+R]\}$$

is an 8 element subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ and the points P, Q, and R are independent points in $E(\mathbb{Q})$.

Proof. By Lemma 3.31, this has already been proved. □

This concludes the argument that the rank of $E(\mathbb{Q})$ is at least 3.

5.2 Curves of the form $K_m : y^2 = x^3 + m^3x - m^3$

The following theorems are for all elliptic curves of the form $K_m : y^2 = x^3 + m^3x - m^3$ where m is a positive integer.

5.2.1 Proving Trivial Torsion

Theorem 5.2.1. *If $m > 3$, then $E(\mathbb{Q})_{TORS} = \mathbf{O}$.*

Proof. The discriminant $\Delta(K_m) = -16(4m^9 + 27m^6)$. Since m always divides the discriminant, there is no prime p for which every curve of this form has good reduction in $\mathbb{F}_p$. This proof must then be dealt with on a case-by-case basis dependent on m. The curve E has good reduction in $\mathbb{F}_p$ if and only if $p \not| m$. The following table contains possible reductions of E in fields $\mathbb{F}_p$.

p	$m \pmod p$	$K_m(\mathbb{F}_p)$	$\lvert K_m \rvert$
$E(\mathbb{F}_3)$	1	$y^2 = x^3 + x - 1$	4
	-1	$y^2 = x^3 - x + 1$	7
$E(\mathbb{F}_5)$	1	$y^2 = x^3 + x - 1$	9
	-1	$y^2 = x^3 - x + 1$	8
	2	$y^2 = x^3 - 2x + 2$	5
	-2	$y^2 = x^3 + 2x - 2$	7
$E(\mathbb{F}_7)$	1	$y^2 = x^3 + x - 1$	11
	-1	$y^2 = x^3 - x + 1$	12
	2	$y^2 = x^3 + x - 1$	11
	-2	$y^2 = x^3 - x + 1$	12
	3	$y^2 = x^3 - x + 1$	12
	-3	$y^2 = x^3 + x - 1$	11
$E(\mathbb{F}_{11})$	1	$y^2 = x^3 + x - 1$	10
	-1	$y^2 = x^3 - x + 1$	10
	2	$y^2 = x^3 - 3x + 3$	16
	-2	$y^2 = x^3 + 3x - 3$	16
	3	$y^2 = x^3 + 5x - 5$	6
	-3	$y^2 = x^3 - 5x + 5$	17
	4	$y^2 = x^3 - 2x + 2$	15
	-4	$y^2 = x^3 + 2x - 2$	15
	5	$y^2 = x^3 + 4x - 4$	13
	-5	$y^2 = x^3 - 4x + 4$	13

After looking at this table, we can easily prove trivial torsion for a subset of the family of curves - namely, all curves $y^2 = x^3 + m^3x - m^3$ with $7 \not| m$ and $11 \not| m$. The only factors in common between reduction modulo 7 and reduction modulo 11 are 2 and 3. Similar to the previous family, we have only to show that there exist no integer solutions of order 2 or 3. This

involves showing the roots of the curve and the inflection points are non-integer numbers.

To begin ruling out solutions of order 2, note that all curves in this family contain the points $(1, 1)$ and $(0, \sqrt{-m^3})$. By the intermediate value theorem, these curves must cross the x-axis between in the interval $(0, 1)$. Therefore, the point of intersection is not an integer value and by the Nagell-Lutz theorem, not a rational point.

This is, in fact, the only time these curves cross the x-axis since for all values of m, the discrimant is negative and therefore the cubic curve has only one real root.

Now consider points of order 3, the inflection points of the curve. A point (x, y) has order 3 if and only if x is a root of the polynomial

$$\psi_3(x) = 3x^4 + 6m^3x^2 - 12m^3x - m^6$$

Now we can focus just on those curves with $11|m$ or $7|m$. Another important consquence of the Nagell-Lutz theorem is that if (x, y) is a rational point of finite order, it must not only be an integer point but also $y|D$ where D is the discriminant of the curve. Recall that the discriminant for this family is

$$D = -16(4m^9 + 27m^6)$$

We have proved trivial torsion for all m except those m divisible by 7 or 11. □

5.2.2 Bounding the Ranks

To put a lower bound on the ranks of these curves, we must first show that there exist two independent points that are not doubles of rational points.

Theorem 5.2.2. *Let $A = (u/s^2, v/s^3)$ and $B = (w/t^2, z/t^3)$ be points on C_m with gcd$(uv, s) = 1$ and gcd$(wz, t) = 1$. $A \neq 2B$ if:*

(a) $A = P = (1, 1)$

(b) $A = Q = (m, m^2)$

(c) $A = P + Q = (m^2 + m, -m^2(2 + m))$

Proof. Let $B = (x, y)$ and $A = (x_0, y_0) = 2B$. From the rules for adding points on elliptic curves,

$$x_0 = \left(\frac{3x^2 + m^3}{2y}\right)^2 - 2x = \frac{9x^4 + 6m^3x^2 + m^6 - 8xy^2}{4y^2}$$

By substituting our equation for $E : y^2 = x^3 + m^3x - m^3$ into the relation, we get

$$x_0 = \frac{9x^4 + 6m^3x^2 + m^6 - 8x(x^3 + m^3x - m^3)^2}{4(x^3 + m^3x - m^3)}$$

Now, by substituting in values for $x_0 = u/s^2$ and $x = w/t^2$ we get,

$$4ut^2(w^3 + m^3wt^4 - m^3t^6) = s^2(w^4 - 2m^3w^2t^4 + 8wm^3t^6 + m^6t^8)$$

(a) Let $u = 1$ and $s = 1$. Then,

$$4t^2(w^3 + m^3wt^4 - m^3t^6) = w^4 - 2m^3w^2t^4 + 8wm^3t^6 + m^6t^8$$

This implies that $t^2 \mid w^4$, but since $\gcd(t, w) = 1$, then $t = 1$.

$$4(w^3 + m^3w - m^3) = w^4 - 2m^3w^2 + 8wm^3 + m^6$$

$$4(w^3 - m^3w - m^3) = w^4 - 2m^3w^2 + m^6$$

This, however, implies that

$$(w^2 - m^3) \mid (w^3 - m^3w - m^3)$$

Which is a contradiction. Therefore, $(1, 1)$ cannot be the double of a rational point.

(b) Let $u = m$ and $s = 1$. Then,

$$4mt^2(w^3 + m^3wt^4 - m^3t^6) = (w^4 - 2m^3w^2t^4 + 8wm^3t^6 + m^6t^8)$$

This implies $t^2 \mid w^4$ and therefore $t = 1$.

$$4m(w^3 + m^3w - m^3) = (w^4 - 2m^3w^2 + 8wm^3 + m^6)$$

$$4m(w^3 + -2m^2w + m^3w - m^3) = (w^2 - m^3)^2$$

This implies $(w^2 - m^3) \mid (w^3 + -2m^2w + m^3w - m^3)$, which is a contradiction. therefore, (m, m^2) is not the double of a rational point.

(c) Let $u = m^2 + m$ and $s = 1$.

$$4(m^2 + m)t^2(w^3 + m^3wt^4 - m^3t^6) = (w^4 - 2m^3w^2t^4 + 8wm^3t^6 + m^6t^8)$$

This implies that $t^2 \mid w^4$, but since $\gcd(t, w) = 1$, then $t = 1$.

$$4(m^2 + m)(w^3 + m^3w - m^3) = (w^4 - 2m^3w^2 + 8wm^3 + m^6)$$

$m \mid w$, so we can rewrite w as $w = lm$ for some integer l.

$$4m(m+1)(l^3m^3 + m^4l - m^3) = (m^4l^4 - 2m^5l^2 + 8lm^4 + m^6)$$

$$4(m+1)(l^3 + ml - 1) = l^4 - 2ml^2 + 8l + m^2$$

Consider the case where m is even.

$$4m(l^3 + ml - 1) + 4(l^3 + ml - 1) \equiv l^4 - 2ml^2 + m^2 \pmod 8$$

$$4l^3 - 1 \equiv l^4 - 2ml^2 + m^2 \pmod 8$$

if l is even, we have $-1 \equiv m^2 \pmod 8$ which is a contradiction since m is even. If l is odd, we have $3 \equiv (m - l^2)^2 \pmod 8$ which is a contradiction since 3 is not a quadtric residue of 8.

Now consider the case where m is odd.

$$4(m+1)(l^3 + ml - 1) \equiv l^4 - 2ml^2 + 8l + m^2 \pmod 1)6$$

If l is even,

$$4(m+1)(ml - 1) \equiv -2ml^2 + m^2 \pmod 1)6$$

This is a contradiction since the right hand side will be even, while the left-hand side must be odd. If l is odd,

$$4(m+1)(l^3 + ml - 1) \equiv 1 - 2ml^2 + 8l + m^2 \pmod 1)6$$

$$2(m+1)(l^3 + ml - 1) \equiv 1 - ml^2 + 4l + m^2 \pmod 1)6$$

This makes the left-hand side odd and the right-hand side even which is a contradiction. Therefore, $P+Q$ cannot be the double of a rational point.

□

Now that we have established these points are not the doubles of rationals, we must establish their independence and existence as elements of the group $E(\mathbb{Q})/2E(\mathbb{Q})$.

Theorem 5.2.3. *Let $P = (0, 1)$ and $Q = (m, 1)$. Then*

$$H = \{[\mathbf{O}], [P], [Q], [P + Q]\}$$

is an 8 element subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ and the points P, Q, and $P + Q$ are independent points in $E(\mathbb{Q})$.

Proof. By Lemma 3.31, this has already been proved. □

Chapter 6

Conclusion

Through computational experimentation and data collection on the properties of elliptic curves over multiple fields, we were able to find and prove two infinite families of elliptic curves with high ranks. These curves,

$$C_m : y^2 = x^3 - m^2x + 1 \qquad K_m : y^2 = x^3 + m^3x - m^3$$

have trivial rational torsion groups, and at least three independent points that are not the doubles of other rational solutions to the curve. Tools from geometry, real analysis, and algebra were used in the proofs presented in this paper.

Elliptic curves continue to be of great importance to the mathematical community. By computational exploration, we will continue to find patterns in the behavior of elliptic curves in their many forms.

6.1 Future Work

Still more families of curves that exhibit this behavior likely exist. The methods laid out by Brown *et al* may be used to discover more curves with ranks that can be bounded below. Possibly even all curves that exhibit trivial torsion and high ranks could be identified through this method. Another possible application of these methods could be to bound ranks above as well. By proving that there exist no more independent points that are not doubles of rationals, an upper bound could be put on the ranks of curves in these families.

Appendix A

Unfinished Proofs

While the proofs presented in this paper are sufficient to put a lower bound on the ranks of both curves, the data suggests we can prove an even higher bound for the curves C_m and include more values m for the curves K_m.

A.1 Lower bound on ranks for C_m

There remain 4 possible independent points for curves of the form C_m. These are

$$R = (m, 1), \quad P + R, \quad Q + R, \quad P + Q + R$$

The data collected suggests that for all $m \geq 4$, these curves have rank 3 or greater. Using the same methods employed earlier, proofs for these points are likely to be possible. Brown and Meyers mentioned a difficulty for the point $(m, 1)$ at the end of their paper, suggesting that additional work may need to be employed to complete these proofs [2].

A.2 Trivial Torsion for K_m

While we have already proved trivial rational torsion for curves of the form K_m, $7 \not| m$ and $11 \not| m$, the data suggests that this holds true for all $m \in \mathbb{N}$. The difficulty with proving this stems from the nature of the discriminant. Recall that

$$\Delta(K_m) = -16(4m^9 + 27m^6)$$

In order to reduce the curve to a finite field, we must find a prime p that does not divide $\Delta(K_m)$. This is equivalent to finding a prime p that does

not divide m which is impossible to do for all $m \in \mathbb{N}$.

By using the same methods as before, we can continue to rule out more and more values of m, but will never quite get them all in this manner. An alternative proof might draw on Theorem 3.2.3 which enumerates the 15 possible structures for torsion groups. Using Mathematica, we can rule out points of order 5 and 7 in a similar manner to that done for points of order 3 - by proving they cannot be integers. This will be sufficient, as all 15 possible groups must be either the torsion group, or contain points of order 2,3,5, or 7.

Bibliography

[1] Manjul Barghava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. 2010.

[2] Ezra Brown and Bruce T. Meyers. Elliptic curves from mordell to diophantus and back. *The American Mathematical Monthly*, 109(7), 2002.

[3] J.E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1997.

[4] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, New York, NY, 2010.

[5] Barry Mazur. Modular curves and the eisenstein ideal. *Publications mathmatiques de lI.H..S.*, 47, 1977.

[6] Henry McKean and Victor Moll. *Elliptic Curves*. Cambridge University Press, New York, NY, 1997.

[7] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, NY, 1986.

[8] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer, New York, NY, 1992.

[9] Sage Computer Algebra Software. `http://www.sagemath.org/`.

[10] John Stillwell. Elliptic curves. *The American Mathematical Monthly*, 102(9), 1995.