2012

Odd or Even: Uncovering Parity of Rank in a Family of Rational Elliptic Curves

Anika Lindemann
Colby College

ODD OR EVEN: UNCOVERING PARITY OF RANK IN A FAMILY OF RATIONAL ELLIPTIC CURVES

ANIKA LINDEMANN

Date: May 15, 2012.

Preamble

Puzzled by equations in multiple variables for centuries, mathematicians have made relatively few strides in solving these seemingly friendly, but unruly beasts. Currently, there is no systematic method for finding all rational values, that satisfy any equation with degree higher than a quadratic. This is bizarre. Solving these has preoccupied great minds since before the formal notion of an equation existed. Before any sort of mathematical formality, these questions were nested in plucky riddles and folded into folk tales. Because they are so simple to state, these equations are accessible to a very general audience. Yet an astounding amount of mathematical power is needed to even begin to generate universal results. On the one hand, it is easy to see that solutions do or do not exist for certain equations, but finding and proving the exact number of solutions is really hard, maybe impossible in some cases. On the other hand, this makes it a wonderful topic to research. The problems are beautiful and elegant to state, and accessible to anyone with some basic undergraduate knowledge. Yet, to even begin to solve these problems requires sophisticated tools from the far corners of geometry, topology, analysis and algebra.

To get us started, elliptic curves define a subset of these multi-variable equations: cubic equations in two variables.

$$y^2 = x^3 + Ax + B$$

This thesis will set out to explore two families of elliptic curves over the rational field. When proofs are necessary or not too complicated they will be included. However, some of the theorems stated are far too hard, so only references will be provided. While a lot of algebraic techniques will be employed, it is important to remember that these curves are also geometric objects. As we explore the algebraic property of elliptic curves, a question that will always exist is "where does the geometry appear"? Thus, illustrations will be provided in the hopes of providing a more intuitive understanding of the underpinnings of the geometry.

First, we will define elliptic curves more formally, then we will discuss the group structure of the rational points on elliptic curves. Next, we

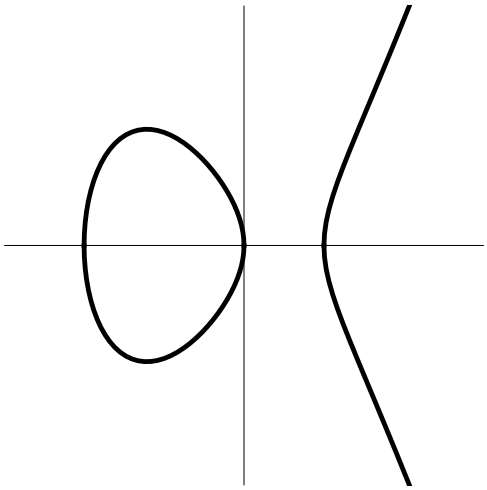

Figure 1. An Elliptic Curve with Three Real Roots

will explore the group structure of a a family of elliptic curves corresponding to a parameterized cyclic cubic over the integers. This will be carried out under the guidance of Larry Washington's paper, *Class Numbers of the Simplest Cubic Fields*. Finally, using experimental methods, we will test the solutions to this family of curves over the rational field culminating in a conjecture that generalizes some of Washington's results.

Contents

1. Diophantine Equations: The Background to Elliptic Curves

In third century Alexandria, math was just coming into its own as an axiomatic art. Diophantus, the first to use symbols in mathematics, was putting the finishing touches on *Arithmetica*, which included 150 problems describing equations with multiple variables. Diophantus always looked for rational solutions to these equations [1]. Today we use the term *Diophantine Equation*, for polynomial equations in several variables with integer (or rational) coefficients:

$$F(x_1, x_2, ..., x_n) = 0 \tag{1}$$

A *rational* solution is any n-tuple $[x^*{}_1, x^*{}_2, ..., x^*_n]$ where $x \in \mathbb{Q}$ such that Eq. 1 is true. An *integer* solution is any n-tuple $[x^*{}_1, x^*{}_2, ..., x^*_n]$ where $x \in \mathbb{Z}$. One can also consider systems of such equations. Finding a solution can sometimes be as easy as plugging in some "obvious" numbers. However, three basic problems continue to arise when these equations are studied, all stemming from the question, "Is it possible to fully solve this equation?"

(1) If the equation is solvable, determining if the number of solutions is finite or infinite.
(2) Specifying each and every solution.
(3) Proving, in the case of an unsolvable equation, that there is no solution.

These problems could be solved if there was indeed a general way to solve Diophantine Equations. In fact, in 1900, David Hilbert, the German mathematician responsible for Hilbert Spaces, asked at the Second International Congress of Mathematics, as the tenth bullet in a list of twenty-three fundamental math questions, whether there was a finite algorithm for determining if any Diophantine Equation is solvable. It took mathematicians seventy years, but Matyasevich, Putnam and Robinson finally proved that that there is no such algorithm to prove if it has integral solutions. However, it is possible to check in a finite number of steps if it has positive rational solutions, although it is unknown whether there exists an algorithm for general rational solutions. [2]

Unfortunately, it can be near impossible to prove that even a specific family of Diophantine Equations has no solutions. Mathematicians were haunted for centuries by Fermat's Last Theorem, that no integer solutions exist for $x^n + y^n = z^n$ when $n > 2$. In 1637, Fermat notoriously wrote in his copy of Arithmetica, next to Diophantus' sum of squares problem, that he had a proof no solutions existed, but that it was too large to fit in the margin. It took over three hundred years until Andrew Wiles finally proved the crucial last step that unlocked the theorem. Interestingly enough, elliptic curves played a major role in his proof. The proof of the theorem, however, spans much farther back than Wiles and depends on an extensive theory developed by several mathematicians over four decades. The final step, which was provided by Wiles, is over over one hundred pages long [3].

1.1. **Polynomial Equations in One Variable.** Fortunately, there exist simpler families of monic polynomials that are much easier to solve. For instance, the solutions of polynomials in one variable with integer coefficients must be comprised of the integer divisors of the constant coefficient, i.e. If $p \in \mathbb{Z}$ is a solution of $x^n + a_1 x^{n-1} + ... + a_n = 0$ where $a_i \in \mathbb{Z}$ for all i then p divides a_n. Therefore, there is a very simple way to check the integer solutions of this polynomial, just factor the constant coefficient, plug the factors into the equation and check if they satisfy the equation. More generally, if the polynomial is not monic then the only rational solutions can be $p/q \in \mathbb{Q}$, where q divides the leading coefficient.

1.2. **Linear Equations in Two Variables.** For more variables, looking at polynomials of higher degree becomes difficult quickly. Therefore, we consider linear equations with two variables first, $ax + by = d$ where a, b and $d \in \mathbb{Z}$. There are infinitely many integer solutions if $\gcd(a, b)$ is a divisor of d, which is easy to check with Euclid's algorithm. Geometrically, the solutions of this equation are all points $[x, y]$ where $x, y \in \mathbb{Z}$ lie on the line $y = \frac{d}{b} - \frac{a}{b}x$. If we want rational solutions, then this equation shows that any $x \in \mathbb{Q}$ corresponds to a $y \in \mathbb{Q}$.

1.3. **Quadratic Equations in Two Variables.** For quadratic polynomials with two variables, $ax^2 + bxy + cy^2 = d$ where a, b, c and $d \in \mathbb{Z}$ finding all rational solutions is more difficult but still possible. By using a p-adic method of checking that there are solutions modulo powers of primes

for all primes (this boils down to looking at powers of certain primes depending on the coefficients) it is possible to decide whether solutions can be found. Then, using stereographic projections, there is a routine way to find all the other solutions [3].

Geometrically, non-singular quadratic polynomials describe conic sections. Any nonsingular quadratic polynomial can be altered by a change of variables into one of these three forms:

$Ax^2 + By^2 = C$ ellipse,
$Ax^2 - By^2 = C$ hyperbola and
$Ax + By^2 = C$ parabola

The solutions to these equations are clearly all rational points that lie on these curves.

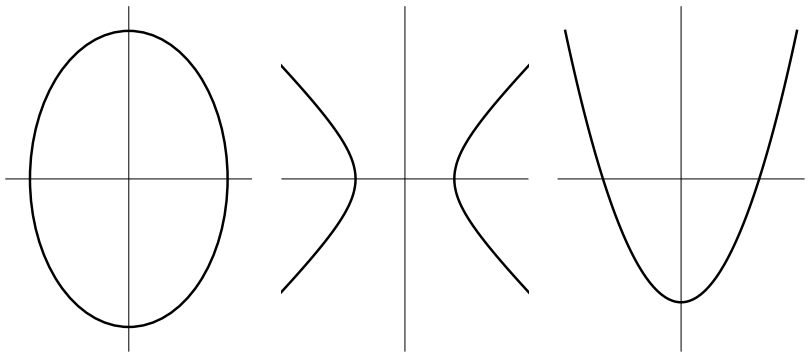

Figure 2. An ellipse, a hyperbola and a parabola in $\mathbb{R}^2$

Both linear and quadratic equations in two variables describe curves of genus zero. However, when we try to explore simple curves of genus one, elliptic curves, we run into trouble. Even though they are described by cubic equations in two variables, no known algorithm for finding rational solutions exists. Yet, if an algorithm were discovered, it would help mathematicians make enormous strides in obtaining insights into conjectures and ideas about curves of higher genus. Thus the study of

elliptic curves is beneficial in many studies of curves of higher complexity.

2. Defining Elliptic Curves

Definition 2.1. *Let K be a field. An* elliptic curve *over K is a nonsingular projective curve of genus one E with one rational point $\mathcal{O}$.*

$$E(K) : F(x, y, z) = ax^3 + bx^2z + cxz^2 + dxyz + ey^2z + fyz^2 + gz^3 \tag{2}$$

where $a, b, c, d, e, f, g \in K$.

Every elliptic curve can be embedded into the projective plane as a nonsingular cubic with at least one rational point $\mathcal{O}$. To explain this, think of the usual affine plane with coordinates (x, y) and reinterpret these coordinates as $[x : y : 1]$, where triples $[a : b : c]$ and $[ta : tb : tc]$ are considered the same. Clearly any triple $[x : y : z]$ with $z \neq 0$ is equal to $[\frac{x}{z} : \frac{y}{z} : 1]$. To obtain the projective plane $\mathbb{P}^2$ we just allow all triples, and think of triples [a : b : o] as forming a "line at infinity".

The Riemann-Roch Theorem [3] allows us to find functions x, y, z on an elliptic curve that together give an embedding,

$$E \hookrightarrow \mathbb{P}^2$$

$$P \mapsto [x(P), y(P), z(P)]$$

The image of E will consist of the points $[x : y : z]$ in $\mathbb{P}^2$ such that $F(x, y, z) = 0$, where F is a homogeneous cubic polynomial [Eq. 2]. We also chose our embedding such that our rational point $\mathcal{O}$ maps to $[0 : 1 : 0]$ which is a point on the "line at infinity" at which all vertical lines in $\mathbb{R}^2$ intersect. Also, as long as K does not have characteristic 2 or 3, we can then modify the embedding to get an equation of the form,

$$zy^2 = x^3 + Ax^2z + Bxz^2 + Cz^3 \tag{3}$$

where the coefficients are in K.
The only point $[x : y : 0]$ satisfying this equation is $\mathcal{O}$, so we will focus on the affine part, setting $z = 1$ to get

$$y^2 = x^3 + Ax + Bx + C \tag{4}$$

We will often write $f(x) = x^3 + Ax^2 + Bx + C$ and use $y^2 = f(x)$ for the equation. It is important to remember that the points on E consist of all pairs (x, y) such that $y^2 = f(x)$ plus the point at infinity $\mathcal{O}$, infinitely far away in the vertical direction.

Recall that our definition of elliptic curve specified that E be non-singular. Once we have an explicit equation, we can check this directly:

Theorem 2.2. *Let E be an elliptic curve given as*

$$g(x, y) = y^2 - x^3 + Ax^2 + Bx + C = 0 \tag{5}$$

Suppose P is a real solution on that curve and P satisfies,

$$\frac{\partial g}{\partial x}\Big|_P = \frac{\partial g}{\partial y}\Big|_P = 0$$

then E is singular. Equivalently, E is singular if and only if for $f(x) = x^3 + Ax^2 + Bx + C$

$$\Delta_f = A^2B^2 - 4B^3 - 4A^3C - 27C^2 + 18ABC = 0$$

where Δ_f is the discriminant of $f(x)$.

Geometrically, a non-singular curve is one with no cusps and no intersections.

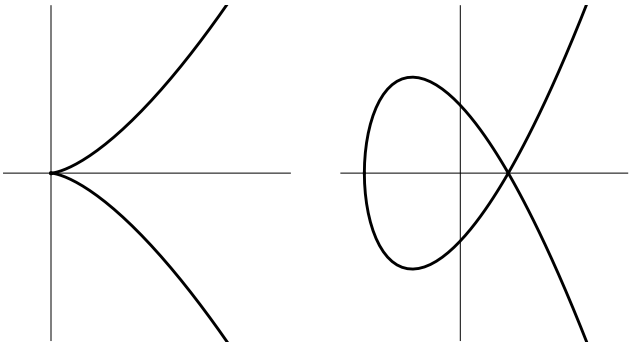

Figure 3. An example of two singular cubic curves. The left one contains a cusp and the right one contains an intersection.

We are interested in rational points, so in general we will assume $A, B, C \in \mathbb{Q}$. In fact, however, we can work with $A, B, C \in \mathbb{Z}$ as well,

since a simple change of variables reduces the general case to integer coefficients [3].

$$y^2 = x^3 + u_2x^2 + u_4x + u_6 \tag{6}$$

with $u_i \in \mathbb{Q}$ for $i = 2, 4, 6$.

The subscripts of the coefficients give a general strategy for transforming an elliptic curve with rational coefficients to an isomorphic curve with integer coordinates [3].

Here is the general method for changing variables . Let $E/\mathbb{Q}$ be of the form $y^2 = x^3 + u_2x^2 + u_4x + u_6$ then with a change of variables $\sigma : (x, y) \to (v^{-2}x, v^{-3}y)$, where v is the common denominator of the rational coefficients, we find,

$\sigma(E) : v^{-6}y^2 = v^{-6}x^3 + u_2v^{-4}x^2 + u_4v^{-2}x + u_6$

Multiply through by v^6.

$\sigma(E) : y^2 = x^3 + u_2v^2x^2 + u_4v^4x + v^6u_6$
and clearly $u_iv^i \in \mathbb{Z}$ for $i = 2, 4, 6$.

We note that this does not mean that rational solutions are transformed into integer solutions. In fact, integer solutions are extremely hard to find when there are integer coefficients. One of the earlier general theorems classifying points on an elliptic curve is about integral solutions.

Theorem 2.3. *Let E be an elliptic curve given by $y^2 = x^3 + Ax^2 + Bx + C$ where $A, B, C \in \mathbb{Z}$. Then E only has a finite number of integral solutions.*

This theorem, proved by Carl Ludwig Siegel in 1929, is a very elegant and easy to state theorem, and yet it still provides no insight into finding how many purely *rational* solutions exist for an elliptic curve. So we turn to looking at rational points to try and identify the group structure of the curves [3].

3. The Group Structure

Now we are ready to build the foundations for finding the rational solutions of an elliptic curve.

Definition 3.1. *The rational solutions over the elliptic curve are defined as,*

$$E(\mathbb{Q}) = \{x, y \in \mathbb{Q} : y^2 = x^3 + Ax^2 + Bx + C\} \cup \{\mathcal{O}\} \tag{7}$$

The only reason that mathematicians think that finding these solutions may one day be possible is that there is an algebraic aspect to the rational points on an elliptic curve; they form an abelian group under addition. This is the most important insight, providing a glimmer of hope to mathematicians that there may be an efficient way to solve for all rational solutions of an elliptic curve.

3.1. Adding Points on an Elliptic Curve.

Suppose, we have found a point P, (x_p, y_p) and a point Q, (x_q, y_q) on our elliptic curve where $Q, P \in E(\mathbb{Q})$. We define addition to be finding where the line defined by points P and Q, $\overline{PQ}$, intersect with a third point on the cubic $-R$, which is then reflected over the x-axis to find R. If $P = Q$ we take the line $\overline{PQ}$ to be the line tangent to E at P.

Theorem 3.2. *Suppose the curve $y^2 = x^3+Ax^2+Bx+C$ where $A, B, C \in \mathbb{Q}$ intersects the line $y = mx + y_0$ in exactly three places. If the line intersects two rational points P and Q, then it will intersect a third point R that is also rational.*

Proof. There are three cases,
i) $x_p \neq x_q$
ii) $P = Q$ except where the tangent line is infinite.
iii) $x_p = x_q$ and $y_p \neq y_q$

i) In the first case, we can determine an explicit formula for the point R. First we find $\overline{PQ}$, we know it is given by $y = mx + y_0$. We can easily compute $m = \frac{y_q - y_p}{x_q - x_p}$ and $y_0 = y_q - mx_q = y_p - mx_p$. (Note m and y_0 are both rational). So by substituting y for $mx + y_0$, the intersections are given by the solutions to

$$(mx + y_o)^2 = x^3 + Ax^2 + Bx + C.$$

Thus,

$$(mx)^2 + 2my_0x + {y_0}^2 = x^3 + Ax^2 + Bx + C$$

and

$$0 = x^3 + (A - m^2)x^2 + B - (2my_0)x + (C - y_0)^2.$$

Yet, this is just a cubic in one variable and we already know two the of the solutions, x_p and x_q, so there must be an x_r such that,

$$(x - x_r)(x - x_p)(x - x_q) = x^3 + (A - m^2)x^2 + B - (2my_0)x + (C - y_0)^2.$$

Thus,

$$x^3 - (x_q + x_p + x_r)x^2 + (x_qx_r + x_px_q + x_rx_p) - (x_qx_px_r) = x^3 + (A - m^2)x^2 + B - (2my_0)x + (C - y_0)^2.$$

Now, look at the x^2 coefficient and the coordinates of R are clear,

$$x_r = m^2 - A - x_q - x_p$$

$$y_r = mx_r + y_0$$

Since the operations performed to find this third point were only addition and multiplication on rational elements, and these operations are closed under $\mathbb{Q}$, then R is rational.

ii) In the second case, if $P = Q$ then we find the tangent line to P. Since $y^2 = f(x)$, by differentiating $2yy' = f'(x)$ then $y' = \frac{f'(x)}{2y}$. Therefore we use $m = \frac{f(x_p)}{2y_p}$. However, once we determine this tangent line equation, we can use the same formula as above to find a second unique point.

iii) In the third case, the equations for x_r still hold, but the slope is infinite. This is because if $x_p = x_q$ then $y_p = \pm y_q$. It would seem at first glance that the vertical line is only intersecting two points of the elliptic curve.Yet, let us perform a thought experiment, in the affine plane, any distinct lines intersect at exactly one point, unless these lines are parallel. However, when we study elliptic curves we look at them on the affine plane, but we add the point out at infinity $\mathcal{O}$ corresponding to the point where all vertical lines intersect. Therefore, the third point on the elliptic curve is $\mathcal{O}$ i.e. $[0, 1, 0]$, which is rational. □

Given the theorem, we can define addition.

Theorem 3.3. *Let $P, Q \in E(\mathbb{Q})$, and let R be the third point of intersection between E and the line $\overline{PQ}$. If $R = \mathcal{O}$, there we let $P + Q = \mathcal{O}$. If not, write $R = (x_r, y_r)$. There we we define,*

$$P + Q = (x_r, -y_r) \tag{8}$$

This illuminates an additive identity and also makes subtraction (inverses) possible, hinting at some sort of group structure inherent in adding points.

Before we delve further into the group structure let us check that addition forms a group. To do this we check that it satisfies the group laws and is abelian. We take the group operation to be addition of points, which we have already shown is closed under the rationals. So we just need to show that it is

i) Associative: since we can write $P+Q$ explicitly in terms of x_p, y_p, x_q, y_q we can check associativity via some long and tedious calculations. Alternatively, we can use The Picard Theorem from algebraic geometry to demonstrate associativity [7].
ii) Contains the identity: We already have an inkling that the identity is the point out at infinity. By adding $\mathcal{O}$ to any other point P, we see that the line $\overline{P\mathcal{O}}$ also passes through the third point $-P = (x_p, -y_p)$. Then reflecting the third point, $-P$ over the x-axis, we get P. Therefore, for any rational point P, $P + \mathcal{O} = P$.

ii) Contains inverses: Similarly, the inverse of P is $-P$, as the third point of intersection will be the identity $\mathcal{O}$.

To show that it is abelian is fairly simple, the line between P and Q, $\overline{PQ}$ is the same as the line between Q and P, $\overline{QP}$. To make all of this more concrete let us consider the following example.

Now that we know that addition of rational points forms a group, the next natural thing is to examine the group structure to help us predict other points and to determine the number of rational points on the curve. The underlying group structure of every $E(\mathbb{Q})$ can be traced back to the Mordell-Weil Theorem.

Theorem 3.4. *$E_{\mathbb{Q}}$ is a finitely generated abelian group. In other words, there are points $P_1, P_2, ...P_n$ such that any other point Q in $E_{\mathbb{Q}}$ can be expressed as a linear combination*

$$Q = a_1P_1 + a_2P_2 + ... + a_nP_n \tag{9}$$

for some $a_i \in \mathbb{Z}$

A consequence of this theorem is that we can now define the group structure.

3.2. **Demonstrating the Group Structure.** The group $E(\mathbb{Q})$ is isomorphic to the direct sum of two Abelian groups,

$$E_{\mathbb{Q}} \cong \text{torsion}(E_{\mathbb{Q}}) \oplus \mathbb{Z}^{r_E} \tag{10}$$

The first summand is the group of all points of finite order, is called the Torsion and will be denoted by torsion$E(\mathbb{Q})$. The second summand is the group of all rational points of infinite order, and is a finitely generated group whose order is denoted by r_E. We will now discuss these groups in further detail.

3.3. **The Torsion.**

Definition 3.5. *A point P has finite order if $mP = \mathcal{O}$ for some $m \in \mathbb{Z}$. We then say that this point is an m-torsion point.*

The points that have finite order make up the torsion, a subgroup of rational solutions, i.e.

$$\text{torsion}(E_{\mathbb{Q}}) = \{P \in E_{\mathbb{Q}} : \exists n \in \mathbb{N} \mid np = \mathcal{O}\} \tag{11}$$

To find points of finite order, E. Lutz and T. Nagell independently proved that if P is a point of order $m > 3$ then $x(P)$ and $y(P)$ are integers and $y(P)^2$ divides the discriminant of the cubic, Δ_f.

To start characterizing torsion points we start by examining points of order 2, denoted by $E[2]$. Clearly, $2\mathcal{O} = \mathcal{O}$. Otherwise, let $Q = (x_q, y_q)$ be a point such that $2Q = \mathcal{O}$, equivalently $Q = -Q$. The negative of a point is the point reflected over the x-axis. So, for a point to be its own

inverse it must actually lie on the x-axis, $y_q = 0$. Therefore x_q must also be a solution to the equation $x^3 + Ax^2 + Bx + C = 0$. So if $f(x)$ is reducible over the rationals the curve will have either one or three points of order two. Therefore we can characterize the set of 2-torsion points, $E[2]$, as forming a subgroup of $E(\mathbb{Q})$, which is either the trivial group if the cubic is irreducible, or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if the cubic has one root and isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if the cubic has three roots.

This prompts the question of what other torsion subgroups might look like. The following theorem describes all possibilities. It was conjectured by Ogg and proven by Mazur [4].

Theorem 3.6. *(Mazur) Let $E(\mathbb{Q})$ be an elliptic curve. Then torsion$(E_{\mathbb{Q}})$ is isomorphic to the following groups:*

$$\mathbb{Z}/N\mathbb{Z} \text{ with } 1 \leq N \leq 10 \text{ or } N = 12, \text{ or}$$
$$\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/M\mathbb{Z} \text{ with } 1 \leq M \leq 4.$$

This is a really beautiful theorem because it allows us to classify any torsion subgroup of an elliptic curve as having one of fifteen completely understood group structures. It is also very difficult to prove.

To fully be able to describe the group structure of the curves (and prove that these are the torsion subgroup structures) we have to look at points of infinite order. Fortunately, Mazur and Ogg's theorem let us see when we have reached points of infinite order. To be absolutely certain that a point has infinite order, we just have to check that it is not a twelve torsion point or less. So, we can start to think about the infinite part of the Mordell-Weil Group isomorphic to $\mathbb{Z}^{r_E}$.

3.4. **The Free Part.** This is where the Mordell-Weil Theorem becomes very useful. Even though there might be an infinite number of points we know that all points are linear combinations of a finite number of "generator" points. These points can be added together and scaled to form the subgroup of points of infinite order, the free part. Before we talk more about the generators, however, let us explore more deeply the the spanning of our group by addition of points. There is an issue of linear dependence.

Definition 3.7. *Let $E(\mathbb{Q})$ be an elliptic curve. The rational points $P_1, P_2, ...P_m \in E_{\mathbb{Q}}$ are* linearly dependent *if there are $n_1, n_2, ...n_m \in \mathbb{Z}$ such that*

$$n_1P_1 + n_2P_2 + ... + n_mP_m = T$$

where T is a torsion point. Otherwise, if there is no such relation we say that points are linearly independent.

The rank of an elliptic curve, r^E is the order of the smallest torsion-free generating set. In other words, it is the order of any set of linearly independent points that span every point of infinite order.

This is where we get to the crux of this thesis, how do we find the r_E, and given r_E how do we find generators of the free part of the Mordell-Weil group? There is no definitive algorithm for finding these generators that works for each curve or there would be no thesis. In fact, there is not even a proven way to efficiently determine r_E.

Even though finding torsion points is relatively easy, finding generating points can be more than difficult. With torsion points, it is safe to assume, from the Lutz-Nagell Theorem, that if the coefficients of the cubic look concise, then the coordinates of the points also look concise [5]. However, this is not the case with generators.

For example, consider the curve given in [3] pp. 42, $E/Q : y^2 = x^3 + 877x$. It is known that the rank of this curve is equal to 1, so there any point of infinite order can be expressed as a multiple of one point P. It turns out that the x-coordinate of the smallest generator P, is

$$x_p = (612776083187947368101/78841535860683900210)^2$$

Given that finding generators is so hard, we will focus only on the rank r_E, the number of generators. That is still very hard so our main question will be simply be whether r_E is odd or even.

4. Cyclic Cubics: The One-Parameter Family

In exploring ways to find the ranks of elliptic curves, two families of curves appeared in my research. It turned out that there is interesting connection between these two families that helps us to understand their

rank and ultimately, their solutions. The first family of curves is $y^2 = f(x)$ where

$$x^3 + mx^2 - (m+3)x + 1 = y^2 = f(x) \tag{12}$$

$m \in \mathbb{Q}$,

This family of one parameter curves appears in Larry Washington's Paper *Class Numbers of the Simplest Cubic Fields*. The other family of curves appeared in a letter from Ezra Brown to Fernando Gouvêa, as a variation on the family of curves as outlined in *Average Root Numbers for a Nonconstant Family of Elliptic Curves* by Ottavio Rizzo. The family of curves as described by Ezra Brown is,

$$y^2 = x^3 + (b+3)x^2 + bx - 1 \tag{13}$$

where $b \in \mathbb{Q}$

4.1. **Comparing Brown and Washington's Curves.** To see how these curves are related, let us first put both curves into the same parameter, i.e. let $b + 3 \mapsto -m$. Then Brown's curve becomes

$$y^2 = x^3 - mx^2 - (m+3)x - 1 = f(x) \tag{14}$$

This family of curves looks very similar to Washington's curve [Eq. 12]. Yet these families of curves are not the same. The variation in curves is due to the fact that one is the twist of the other,

Definition 4.1. *For an elliptic curve E given by $y^2 = f(x)$, we define its* twist by -1 *to be the curve E_{-1} defined by $y^2 = -f(-x)$.*

The curves E and E_{-1} are isomorphic over $\mathbb{C}$. If we have a point (x, y) on E_{-1}, then $y^2 = -f(-x)$ so $-y^2 = f(-x)$ so $(iy)^2 = f(-x)$ and $(-x, iy)$ is a point on E. The function
$(x, y) \mapsto (-x, iy)$ is a bijection between complex points on E_{-1} and complex points on E, so E_{-1}. The bijection, however, cannot be written without using $i = \sqrt{-1}$, so the curves are not isomorphic over $\mathbb{Q}$. In particular, the groups $E(\mathbb{Q})$ and $E_{-1}(\mathbb{Q})$ are not necessarily related.

To see that the family of curves described by Washington is the twist by -1 of Brown's curve [Eq. 13] we send, $(-x, iy) \mapsto (x, y)$, thus $-f(x) \mapsto -y^2$, so we get,

$$-y^2 = -x^3 - mx^2 + (m+3)x - 1$$

which equals,

$$y^2 = x^3 + mx^2 - (m+3)x + 1,$$

This is Washington's curve. As it turns out, both of these families of curves have easy solutions, namely (0,1) for Washington's curve verses (1, -1) for Washington's curve. We will show later that if $f(x)$ is irreducible both of these points have infinite order.

4.2. **Showing the Family of Curves are Cyclic Cubics.** To understand why Washington's family of curves is so special, we first need to first prove that the roots of the polynomial, $f(x)$, are the generators of a cyclic cubic field. However, notice that an immediate solution is $(0, 1)$.

Definition 4.2. *A* cubic field *is a field extension of* $\mathbb{Q}$ *of degree three. Such a field is then isomorphic to a field of the form* $\mathbb{Q}[x]/g(x)$ *where g(x) is an irreducible cubic polynomial.*

Definition 4.3. *A cubic field is said to be* cyclic *if the discriminant of the irreducible polynomial g(x) is a square.*

If K is a cyclic cubic field corresponding to a polynomial $g(x)$ then there are two conditions it must satisfy. All the roots of $g(x)$ are real and if we fix a real root ρ, all the other roots can be expressed as rational functions of ρ. Note that cyclic cubics are what Washington means by the "simplest" cubic fields.

An easy computation shows that the discriminant of our generating polynomial $\Delta_f = (m^2 + 3m + 9)^2$, is clearly a square.

Theorem 4.4. *Let* ρ *be a negative real root of f(x), the remaining roots of* $f(x)$ *are* $\rho' = \frac{1}{1-\rho}$ *and* $\rho'' = 1 - \frac{1}{\rho}$. *Thus,* $\rho, \rho', \rho'' \in \mathbb{R}$.

Proof. Since m is the coefficient of x^2 we know that

$$-m = \rho + \frac{1}{1-\rho} + 1 - \frac{1}{\rho} = \frac{-\rho^3 + 3\rho - 1}{\rho^2 - \rho}$$

Now we try to construct f(x) from the roots.

$$(x-\rho)(x-\frac{1}{1-\rho})(x-(1-\frac{1}{\rho})) = x^3-(\rho+\frac{1}{1-\rho}+\frac{\rho-1}{\rho})x^2+(\frac{\rho}{1-\rho}+\rho-1-\frac{1}{\rho})x+1$$

Note that the x^2 coefficient is $-m$ which we expected from the definition of a cubic polynomial. The coefficient of x is harder to discern as the polynomial

$$(\frac{\rho}{1-\rho} + \rho - 1 - \frac{1}{\rho})$$

$$= \frac{3\rho^2 - \rho^3 - 1}{\rho^2 - \rho}$$

$$= \frac{3\rho^2}{\rho^2 - \rho} + \frac{3\rho}{\rho^2 - \rho} - m$$

$$= \frac{3\rho^2 - 3\rho}{\rho^2 - \rho}$$

$$= -m + 3\frac{\rho - \rho^2}{\rho^2 - \rho} = -m - 3$$

Thus,

$$(x - \rho)(x - \frac{1}{1-\rho})(x - (1 - \frac{1}{\rho}) = x^3 + mx^2 - (m+3)x + 1$$

Thus, the cubic field determined by the irreducible polynomial, over the rationals, is cyclic.

□

We should note that since the polynomial has three real roots, any curve, $y^2 = f(x)$ from Washington's family will always intersect the y-axis at exactly three points as seen in Figure 1. The closed loop is defined by the closed curve constrained by the smallest of the two roots of $f(x)$. The open loop is the component of E that runs through the point at infinity. We define the rational points on the open loop as $E^\circ(\mathbb{Q})$ and the rational points on the closed loop as $E(\mathbb{Q}) - E^\circ(\mathbb{Q})$.

Let us note that an analogous argument can be given for the twisted family. It is not clear that the results we will derive surround Washington's family of curves will be the same for its twist.

5. Understanding the Rank of This Family of Curves

Now that we have established that our polynomial is a cyclic cubic we can ask what implications does this have? Lawrence Washington in

Class Numbers of the Simplest Cubic Fields uses this to show that when $m \in \mathbb{Z}$ the rank of the curve is always odd. We briefly outline his argument which proves this. We start by looking at the field K generated by this cubic and its ideal class group, $\mathcal{C}$, in the loosest of terms measures the extent to which unique factorization fails in our field. The ideal class group, $\mathcal{C}$ is a finite abelian group, so we can look at $\mathcal{C}_2 = \{x \in \mathcal{C} | x^2 = 1\}$. This can be thought of as a vector space over $\mathbb{Z}/2\mathbb{Z}$ and we will be interested in its dimension.

By using the fact that the Galois group of $K/\mathbb{Q}$ acts on $\mathcal{C}_2$ without nontrivial fixed points, one can show that the dimension of $\mathcal{C}_2$ is even [6].

Theorem 5.1. *(Washington) There is an exact sequence*

$$1 \to E^{\circ}(\mathbb{Q})/2E(\mathbb{Q}) \to C_2 \to Ш_2 \to 1.$$

Therefore, by equating $rk(\mathcal{C}_2)$, the generators of the two part of the class group, and $\dim(\mathcal{C}_2)$, the dimension over $\mathbb{Z}/2\mathbb{Z}$,

$$rk(E(\mathbb{Q})) \leq 1 + rk(\mathcal{C}_2) = 1 + dim(\mathcal{C}_2) - dim(Ш_2) \leq 1 + dim(\mathcal{C}_2)$$

This theorem will guide us in trying to determine the parity of rank of our family of elliptic curves. First, however, we return to a geometric picture of our general curve to give us a better understanding of this exact sequence. We note that it seems that the sum of any point $P \in E(\mathbb{Q})$ to itself will give us a point on the open loop, i.e. on $E^{\circ}(\mathbb{Q})$. We can verify this by noting that $E(\mathbb{R})$ is a compact Lie group with two components, the open loop and the closed loop. Therefore we define the curve as,

$$E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Where the closed loop is isomorphic to $\mathbb{R}/\mathbb{Z}$ and the open loop is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ Consider any point P, such that P corresponds to $(\alpha$ mod$\mathbb{Z}$ where $\alpha \in \mathbb{Z}$ and $(\alpha \equiv 0 or 1$ mod$2)$, then $2P$ corresponds to $(2\alpha$ mod $\mathbb{Z}$, 0 mod$2)$. Therefore, $2P$ is clearly on the open loop.

We can also see that the point $(0, 1)$ on each curve in our family is on the closed loop, because $\rho < 0 < \rho'$.

To show that this point has infinite order, we consider that since is

lies on the closed curve, it cannot have order two, because then it would lie on the x-axis, which it does not. If there are no points of order 2, there cannot be points of higher even order either. We also know that it cannot be a point of odd order, because then we would have $(2k-1)P = 0$, which is impossible because $2kP = kP + kP$ is on the open loop, while P is on the closed loop. Thus, no points of odd order can be on the closed loop. So there are no torsion points on the loop and (0,1) is clearly a point of infinite order. Here we have always assumed that the polynomial is irreducible over $\mathbb{Q}$. Otherwise, if the polynomial is reducible over the rationals, there are then 2-torsion points, the points on the x-axis, and thus there might be other points of even order on the closed loop.

This is helpful because if there is no 2-torsion we have $rkE(\mathbb{Q}) = \dim(E(\mathbb{Q})/2E(\mathbb{Q}))$ .Since (0,1) is on the closed loop and it has infinite order, we can take it as one the generators of the generator of the free part. Thus, $rk_2(E(\mathbb{Q})/2(E(\mathbb{Q}) = 1 + rk_2(E^\circ(\mathbb{Q})/2(E(\mathbb{Q}))$, which implies the rank of our curve is equal to the number of infinite order points on the open loop minus the generator on the closed loop. Another major reason that this point is helpful, is that one of the problems of trying to compute the rank of elliptic curves is that many curves have zero rank. When we start to work experimentally with curves and their ranks, it helps to know that they will always at least have rank ≥ 1.

The most mysterious part of the exact sequence is the group $Ш_2$, the 2-torsion part of the Tate-Shafarevich group Ш. Very little is known about this. For our purposes it's enough to note that it is conjectured to be finite and that if it is finite then
$dim Ш_2$ is known to be even. Hence the presence of $Ш_2$ in the exact sequence does not affect our conclusions about the party of the rank.

We are now in a position to outline Washington's main argument, which starts from a standard exact sequence used for conjecturing the rank,

$$1 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathcal{S}_2 \to Ш_2 \to 1 \tag{15}$$

Here $\mathcal{S}$ is the 2-torsion of the "Selmer Group", which can be thought of as parameterizing "good candidates" for points in $E(\mathbb{Q})$. From this point of view, Ш corresponds to good candidates that fail to yield points in $E(\mathbb{Q})$.

Washington then creates a surjective map from $\mathcal{C}_2$ to the Selmer group $\mathcal{S}_2$. Because it is surjective, we can replace the Selmer group with the 2-part of the ideal class group however to preserve the exact sequence requires replacing $E(\mathbb{Q})/2E(\mathbb{Q})$ by $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$.

$$1 \to E^\circ(\mathbb{Q})/2E(\mathbb{Q}) \to \mathcal{C}_2 \to Ш_2 \to 1$$

Furthermore, since we know $\mathcal{C}_2$ has even rank because of its Galois structure and we know $Ш_2$ has even rank, we then know that $E^\circ(\mathbb{Q})/2E(\mathbb{Q})$ also has even rank, and working under the equality in Theorem 5.1, $E(\mathbb{Q})/2E(\mathbb{Q})$ has odd rank. Therefore $E(\mathbb{Q})$ has odd rank.

This is a very powerful result, however, because the proof depends on Washington relating $\mathcal{C}_2$ to $\mathcal{S}_2$, it only holds for $m \in \mathbb{Z}$. Therefore, to understand what is going on for rational values of m becomes much more difficult. To try and figure out what is happening when $m \in \mathbb{Q}$ we move on to experimental testing.

6. Experimental Determination

This section will attempt to outline possible conjectures regarding the parity of the rank of the elliptic curve, $E_m(\mathbb{Q})$ as a function of $m \in \mathbb{Q}$. To do this, countless values of m were plugged into the curve $f_m(x) = y^2 = x^3 + mx^2 - (m+3)x + 1$ when $m \in \mathbb{Q}$ and then the rank was computed using Sage. Unfortunately, since there is no known efficient theorem for computing the rank of an elliptic curve, only certain ranks have been calculated and proved. Thus, for our curves, it is hard to be certain about what is being seen, because eventually SAGE runs out of computing power. Also, note that no cases where $f_m(x) = x^3+mx^2-(m+3)x+1$ is reducible are considered.

Before parity of rank is described, let us first note that m is always in its most reduced form and let us introduce the notation $\sigma m = 0$ if the rank of the elliptic curve is odd and $\sigma m = 1$ if the rank is even. We use

this notation because it neatly summarizes the first proposition derived from our experimental results,

Conjecture 6.1. *If there is an $m \in \mathbb{Q}$ and $x_1 \neq x_2$ and $y_1 \neq y_2$ so that we do not encounter any squares. Then,*
If $\sigma(\frac{x_1}{y_1}) = 1$ and $\sigma(\frac{x_2}{y_2}) = 1$

then $\sigma(m) = \sigma(\frac{x_1}{y_1})\sigma(\frac{x_2}{y_2}) = 1$

If $\sigma(\frac{x_1}{y_1}) = 0$ and $\sigma(\frac{x_2}{y_2}) = 0$

then $\sigma(m) = \sigma(\frac{x_1}{y_1})\sigma(\frac{x_2}{y_2}) = 0$

If $\sigma(\frac{x_1}{y_1}) = 0$ and $\sigma(\frac{x_2}{y_2}) = 1$

then $\sigma(m) = \sigma(\frac{x_1}{y_1})\sigma(\frac{x_2}{y_2}) = 0$

This is almost identical to how parity changes under multiplication, except even multiplied by odd, is odd. However, when there are squares, a new law emerges,

Conjecture 6.2. *Suppose $m = (\frac{x}{y})^2$ in its most reduced form and $f_{\sqrt{m}}(x)$ is irreducible, then the multiplication rule changes,*

If $\sigma(\sqrt{m}) = 1$ then $\sigma(m) = 0$

If $\sigma(\sqrt{m}) = 0$ then $\sigma(m) = 1$

It is much easier to classify an m that does not have an odd square denominator.

Conjecture 6.3. *Let $m = \frac{x}{y}$ such that y is not a square,*

If $y \equiv 1$ mod4 then $\sigma(m) = 0$.

If $y \equiv 3$ mod4 then $\sigma(m) = 1$

Conjecture 6.4. *Let $m = \frac{x}{y}$ such that $y = 2k$,*

If $x \equiv 1$ mod4 then $\sigma(m) = 1$

If $x \equiv 3 mod 4$ *then* $\sigma(m) = 0$

This suggests that the rank of m with an even denominator is odd if and only if m^{-1} is even. Likewise, the rank of m with an even denominator is even if and only if m^{-1} is odd. When we start to look at odd square denominators the problem becomes complicated very quickly because the congruence conditions become very complex.

Proposition 6.5. *Suppose, that* $m = \frac{x}{y^2}$ *such that* y *is square-free, then* 1 *mod*y^2 *is even if* $y \equiv 1 \mathrm{mod} 4$ *and odd if* $y \equiv 3 \mathrm{mod} 4$.

Proposition 6.6. *Suppose, that* $m = \frac{x}{y^2}$ *such that* y *is square-free and odd, then for* $\gcd(x, y) = 1$, $\sigma(m) = x$ *mod* y.

Proposition 6.7. *Suppose, that* $m = \frac{x}{y^2}$ *such that* y *is square-free and odd, then for* $\gcd(x, y) = 1$, $\sigma(m) = \sigma(\frac{\alpha}{y})$ *when* $x \equiv \alpha$ *mod* y. *Furthermore,* $\sigma(\frac{-\alpha}{y}) = (\sigma(\frac{\alpha}{y}))^{-1}$, *i.e. the parity flips when* α *negative.*

Other patterns may yet emerge, but more testing is needed. Sadly, because computing and proving these ranks can so computationally intensive, finding the free part for larger$m$ becomes impossible using open source software. Also, it may be that not all values of m are classifiable because they either make the polynomial reducible or produce a singular discriminant modulo some prime. Washington identified that his argument fails when $m \equiv 3$ mod9, $\Delta \equiv 0$ mod27. With more testing, we hope that there may be some congruence condition for the discriminant that will reveal itself as being too difficult and rare to generally classify.

7. Results and Conclusion

In Washington's paper, the rank for $E_m(\mathbb{Q})$ with $m \in \mathbb{Z}$ and abiding by a few congruence conditions is always odd. We have conjectured that the rank for $E_m(\mathbb{Q})$ with $m \in \mathbb{Q}$ where the denominator is free of square odds, and m is not a square, obeys an extremely regular pattern of being odd or even depending on some congruence conditions modulo 4. So the natural next step, is to try and prove this connection. We know from Washington's paper when m is a rational number that there is a homomorphism from the two part of the class group to the Selmer group. Unlike the integers, when we knew that the map from $\mathcal{S}_2$ to $\mathcal{C}_2$ was surjective, we do not know what happens when m is in the rationals. For

instance, it may be that the map from $\mathcal{S}_2$ to $\mathcal{C}_2$ is no longer surjective, and thus $\mathcal{S}_2$ does not fully describe $\mathcal{C}_2$, so it cannot be included in the exact sequence. Therefore, to further explore this problem I would recommend looking at this map from the Selmer group to the two part of the class group and seeing where it breaks down and why it is not surjective. It also may be worth exploring this family of curves and its twists as described by Bud Brown. We can even raise this family of curves to $C(m)$ where it has rank 2, perhaps there is a way to decompose this to understand the ranks of $E_m(\mathbb{Q})$. There are many different ways that this research can be extended, and this again emphasizes why people fall in love with elliptic curves. They are beautiful, easy to state, and a mathematician can validly choose to approach the problem from almost any field of math.

References

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations: A Problem-Based Approach* Birkhäuser, New York 2010.

[2] Y. Matiyasevich, *Hilbert's Tenth Problem* MIT Press, Cambridge, Massachusetts 1993.

[3] A. Lozano-Robledo, *Elliptic Curves, Modular Forms and Their L-Functions* American Mathematical Society, Providence, Rhode Island 2011.

[4] B. Mazur, *Modular Curves and the Einstein ideal* IHES Publ. Math. 46 (1977), 33-186.

[5] L. Nagell, *Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[6] D. Shanks , *The Simplest Cubic Fields* The Mathematics of Computation **128** Vol. 28 (October, 1974), 1137–1152.

[7] J. Silverman *The Arithmetic of Elliptic Curves* Graduate Texts in Mathematics (October, 1994).