2013

Factoring the Duplication Map on Elliptic Curves for use in Rank Computations

Tracy Layden
Scripps College

Factoring the Duplication Map on Elliptic Curves for Use in Rank Computations

Tracy Layden

Christopher Towse, Advisor
Dagan Karp, Reader

Submitted to Scripps College in Partial Fulfillment
of the Degree of Bachelor of Arts

April 17, 2013

Department of Mathematics

Abstract

This thesis examines the rank of elliptic curves. We first examine the correspondences between projective space and affine space, and use the projective point at infinity to establish the group law on elliptic curves. We prove a section of Mordell's Theorem to establish that the abelian group of rational points on an elliptic curve is finitely generated. We then use homomorphisms established in our proof to find a formula for the rank, and then provide examples of computations.

Contents

Abstract **iii**

Acknowledgments **vii**

1 Projective Geometry **1**
1.1 Correspondences Between Projective and Affine Space . . . 2

2 Elliptic Curves **5**
2.1 The Group Law on Elliptic Curves 7
2.2 Mordell's Theorem 8
2.3 The Rank of an Elliptic Curve 16
2.4 Finding a Formula for the Rank 17

3 Computing the Rank of Elliptic Curves **21**
3.1 Determining the Order of $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$ 21
3.2 Computational Examples 23

4 Current Information About Elliptic Curves **31**
4.1 Record and Average Ranks 31
4.2 Applications of Elliptic Curves 32

Bibliography **35**

Acknowledgments

I would like to thank Professor Towse for all of his guidance and support. I would also like to thank my family and friends for their love and support as I wrote this thesis.

Chapter 1

Projective Geometry

Most people are familiar with Euclidean geometry, with its two axes and rectangular coordinates that are effective in describing our everyday world. As the name implies, this geometry is based upon the work of Euclid. In his book *The Elements*, Euclid assumes a set of self-evident postulates and axioms, and builds his geometry based upon only these [5]. It is difficult to disagree with the postulates and axioms because they are designed to be brief, self-evident, and assuming no prior knowledge. However, the fifth postulate is perhaps not quite so self-evident. It states that if a straight line intersecting two straight lines makes the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which the angles are less than two right angles [6: 42]. The fifth postulate is known as the parallel postulate because it essentially states that two parallel lines never intersect. Mathematicians have long disagreed that the parallel postulate is self-evident. Most of us have grown up with Euclidean geometry, so it seems perfectly reasonable and obvious that parallel lines do not intersect. However, this does not have to be the case. By supposing that the parallel postulate is false, one can create what are known as non-Euclidean geometries. These geometries fulfill all of Euclid's other postulates and axioms and are legitimate geometries in their own right.

Projective geometry is one such non-Euclidean geometry. In fact, Euclidean geometry is a subset of projective geometry in which one assumes the parallel postulate. Euclidean geometry tells us that all lines intersect at exactly one point, except for parallel lines, which do not intersect. Projective geometry does not have this last condition, and tells us all lines intersect at exactly one point, including parallel lines. We say that parallel

lines intersect *at infinity*. This is an extra point in addition to the points already in Euclidean, also known as affine, space. This point at infinity cannot be graphed in $\mathbb{R}^2$, but we can imagine it if we think about the effects of visual perspective in everyday life. For example, a set of parallel train tracks intersect at the horizon at what is known as the *vanishing point*. The vanishing point is our point at infinity. We can deal with this point at infinity algebraically, and indeed it is necessary to complete some of the group structures we will be examining. Points at infinity are not in the affine plane, but are what distinguish affine space and projective space.

In Euclidean geometry, properties of objects are unchanged by rigid motions. Rigid motions include distances, ratios of distances, angles, and parallelisms. Projective geometry does not preserve these traits, but projective transformations do preserve the type of object, incidence (whether a point lies on a line), and ratios between points. Projective geometry has a notion of dimension, and like Euclidean geometry, exists in any number of dimensions. We denote $\mathbb{P}^1$ as the projective line, $\mathbb{P}^2$ as the projective plane, and so on.

1.1 Correspondences Between Projective and Affine Space

Points in Euclidean space and points in projective space have an algebraic correspondence. We can change points from affine space to projective space and back. Recall that projective space does not preserve lengths; thus scaling is unimportant. To take this into account, we define an equivalence relation so that $[A, B, C] \sim [\lambda A, \lambda B, \lambda C]$ for any $\lambda \neq 0$. Note that $[A, B, C]$ exists in some field. Recall that projective space preserves ratios. The ratios between A, B, and C are what distinguish distinct points. Thus our notation is to write points in the projective plane as $[A : B : C]$.

A point in the projective plane $[A : B : C]$ is sent to $(A/C, B/C)$ in the Euclidean plane. This means we must deal with rational numbers. Note that we do not have to divide through by C, but can choose to divide through by either A or B to perform the transformation; each will result in a different point in affine space. Thus any object in projective space can be transformed into affine space in multiple ways. We cannot allow $[0 : 0 : 0]$ to be a point, because if we did, the transformation to $\mathbb{R}^2$ would involve dividing by 0. A point (x, y) in the Euclidean plane is sent to $[X : Y : 1]$ in the projective plane. We define points $[A : B : 0]$ to be the points at infinity. We can think of the projective plane as $\mathbb{P}^2 = \mathbb{R}^2 \cup \{\infty\}$. The points at infinity

are actually $\mathbb{P}^1$, so we can also write $\mathbb{P}^2 = \mathbb{R}^2 \cup \mathbb{P}^1$. In our later work with elliptic curves, we will be working in projective space because we will be incorporating points at infinity.

Now let us turn our attention to polynomials and curves. An algebraic curve is defined to be the set of solutions to a polynomial equation in two variables [10: 225]. The study of algebraic curves falls under the study of *algebraic geometry*, which uses techniques in geometry and abstract algebra to study systems of algebraic equations and the sets of solutions to those equations. We talk about these solutions as being *zeros* of a polynomial. The fundamental objects that algebraic geometry deals with are called *varieties*. A variety is an irreducible nonempty set that cannot be written as a union of two proper sets. Single points are affine varieties with a dimension of zero, and dimension one varieties are curves.

We homogenize polynomials so we that can talk about an equivalence class of polynomials. A polynomial is *homogeneous of degree* n if the exponents of the variables in each term sum to n. That is, if each term is $ax^iy^jz^k$ with a being a constant, then $i + j + k = n$. For example, $F(x, y, z) = 4y^3 + 5x^2y - 3xz^2$ is homogeneous of degree three. If we have a polynomial $f(x, y)$, we can homogenize it by inserting powers of z to make the polynomial homogeneous. For example, $y^2z = x^3 - 82xz^2$ is the homogenized degree three version of $y^2 = x^3 - 82x$. One can dehomogenize a polynomial by setting z equal to one. If F is homogeneous of degree n, then $F(x, y, z) = z^n f(x/z, y/z)$ and $f(x, y) = F(x, y, 1)$. Homogenizing polynomials is very similar to transforming points to and from affine and projective space; if one homogenizes an affine polynomial, we get the corresponding projective polynomial.

We are interested in finding points on curves, and we will later develop a geometric approach to do so. This requires that we understand at which points curves and lines intersect. Let us examine the intersection of a line and a cubic. Since a line is a degree one curve and a cubic is a degree three curve, we know that they should intersect at three points.

In most cases the three points of intersection are visually apparent. If the line is vertical, we have two special cases: either the line intersects two points on the curve, or it is tangent to the curve and only intersects it at one point. In order for our method of finding points to hold in both of these cases, we need our point at infinity. When the vertical line intersects the curve in two points, the third point of intersection is the point at infinity. When the vertical line is tangent to the curve, we take into account multiplicity of roots. There is a double root at the point of tangency, so the intersection is counted twice. A double root plus the point at infinity

brings us to the required three intersection points. Note that every vertical line intersects the point at infinity.

If the line and the cubic do not appear to intersect at all in $\mathbb{R}^2$, we can algebraically find that they intersect in the complex plane. This tells us that in order to find all of the intersections between the line and the curve, we must allow complex coordinates. However, we are interested in the rational points on curves, not complex points. In our approach to finding intersection points, we will begin with two rational roots. Complex numbers come in pairs, so our single remaining root cannot be complex and must be rational. Thus we will not be working with complex numbers.

We have now shown that in every case our line intersects the curve at three points, as it should algebraically. Note that we draw our curves in $\mathbb{R}^2$, but are dealing with them in $\mathbb{Q}$.

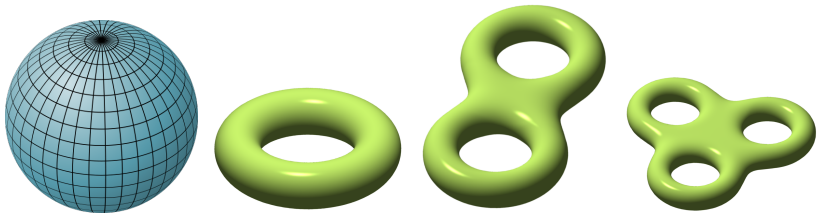
Chapter 2

Elliptic Curves

If we have a connected non-singular projective curve of genus one described by a cubic equation, we have what is known as an *elliptic curve*. Let us look at the components of this definition. A *connected* space is a space which we cannot represent as a union of two or more disjoint nonempty subsets. The *genus* of an object can be thought of as how many 'holes' an object has topologically.

A sphere, with no holes, is of genus zero. A torus, with one hole, is of genus one. Since an elliptic curve is of genus one, it is isomorphic to a torus which, over the complex numbers, is a Riemann surface [11: 260-262]. We can look at elliptic curves over the complex numbers and other fields, including the real numbers and the rational numbers. We are interested in elliptic curves over the rationals.

There exist both singular and non-singular projective curves. A cubic is



(a) Genus 0 (b) Genus 1 (c) Genus 2 (d) Genus 3

singular at a point (a, b) if

$$\frac{\partial P}{\partial x}(a, b) = 0, \frac{\partial P}{\partial y}(a, b) = 0.$$

We say a cubic is *non-singular* if it has no points of singularity. When looking at their graphs, singular curves can be identified if it has a *cusp*, a 'sharp' point, or a *node*, where it intersects itself. Singular curves behave in a dif-

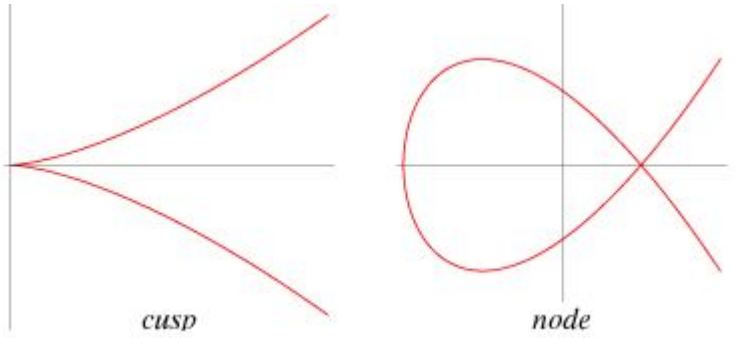


Figure 2.1: Examples of a cusp and a node

ferent fashion than non-singular curves, and in fact behave like conics. We will restrict ourselves to non-singular curves.

Algebraically, an elliptic curve is a Diophantine equation of degree three of the form

$$y^2 = x^3 + ax^2 + bx + c$$

where a, b and c are constants. This form of the equation is called the *Weierstrass normal form*, and it is simpler than the general form of an elliptic curve which is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^4 + a_6.$$

Since elliptic curves are projective curves, we can choose X, Y and Z axes in the projective plane so that the equation for our curve is in Weierstrass form. We will always assume our curves have already undergone the projective transformation necessary to obtain this simpler form, because it is well known that any elliptic curve can be written in Weierstrass form [10: 22-25].

We are interested in finding rational points on elliptic curves, and thus we are interested in finding the roots of their associated cubic equations. Points on an algebraic curve consist of coordinates which are the zeros of

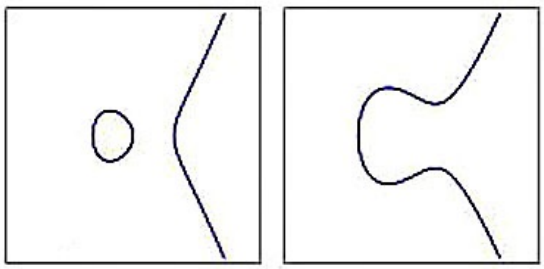


Figure 2.2: Examples of the forms in which elliptic curves can appear.

some polynomial. It has been shown that a cubic equation has only a finite number of integer solutions, but there could be infinitely many rational solutions, or possibly none at all [10: 6]. We are interested in discovering which elliptic curves have rational points and how many such points exist.

2.1 The Group Law on Elliptic Curves

We will now examine how the rational points on an elliptic curve form a group. If one begins with a finite set of solutions to the cubic equation, there is a procedure to find more solutions, which we call adding points on the curve. This group operation is denoted by $+$, since we are dealing with an abelian group.

To add two points, P_1 and P_2, on an elliptic curve, we draw a line through them. When we add a point to itself, we draw a line tangent to the curve at that point. Out line will intersect the curve at our third point, $-P_3$. Note that elliptic curves are symmetric, so we can reflect $-P_3$ over the x-axis to obtain P_3, a fourth point.

Recall our discussion of the intersections of a line and a curve. If our line is vertical we need to take into account the point at infinity, which we will call $\mathcal{O}$, in addition to the visible points on our curve. We need $\mathcal{O}$ not only to take into account all of the points of intersection, but also to complete our group structure. We define the point at infinity as the additive identity in our group so that $P + \mathcal{O} = P$ for any point P on our curve. We can see geometrically that the operation of adding points is commutative, because the line through P_1 and P_2 is the same as the line between P_2 and P_1. If we have a point P_3 and reflect it over the x-axis, we create its inverse, $-P_3$, and $P + P' = \mathcal{O}$. We will not prove associativity here (see Silverman and Tate [10: 19-20]), but our operation is indeed associative. Thus the rational

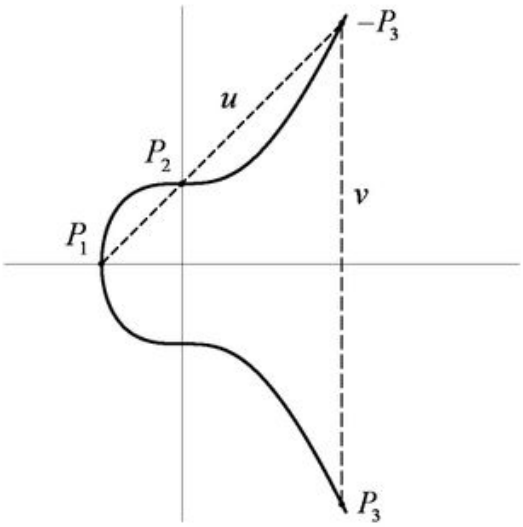


Figure 2.3: Adding points on elliptic curves.

points on an elliptic curve satisfy the requirements to be a group. Note that the point at infinity was necessary to complete our group, so we are looking at elliptic curves in the projective plane.

2.2 Mordell's Theorem

Now that we know our points form a group, we can examine its structure. In 1922, Louis Mordell proved that the group of rational points on a non-singular elliptic curve is a finitely generated abelian group. In other words, there is a finite set of points which we can draw our lines through to create new points which will give us all of the rational points on the elliptic curve. Let $C(\mathbb{Q})$ be the group of rational points on C.

Theorem 2.2.1 (Mordell's Theorem)**.** *If C is an elliptic curve over $\mathbb{Q}$, then the abelian group $C(\mathbb{Q})$ is finitely generated.*

The proof of Mordell's theorem uses Fermat's method of descent. Proofs using methods of descent require the notion of size, so we will need the idea of the *height* of a rational point on an elliptic curve [10: 63].

Definition 1. *Let $x = \frac{m}{n}$ be a rational number written in lowest terms. Then we define the height $H(x)$ to be the maximum of the absolute values of the numerator*

and the denominator:

$$H(x) = \left(\frac{m}{n}\right) = max\{|m|, |n|\}.$$

The height of a rational number is a positive integer.

We will define the height of a rational point $P = (x, y)$ on a curve as the height of its x coordinate, so that $H(P) = H(x)$ [10: 63].

The proof also requires an additive function, so we will define

$$h(P) = logH(P)$$

so that h is a non-negative real number. We will now state the four lemmas that the proof of Mordell's Theorem requires [10: 64-65].

Lemma 2.2.2. *For every real number M, the set*

$$\{P \in C(\mathbb{Q}) : h(p) \leq M\}$$

is finite.

Lemma 2.2.3. *Let P_0 be a fixed rational point on C. There is a constant κ_0 depending on P_0 and on a, b, c, so that*

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

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

Lemma 2.2.4. *There is a constant κ, depending on a, b, c so that*
$h(2P) \geq 4h(P) - \kappa$.

Lemma 2.2.5. *The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite.*

The first three lemmas set up the descent method, and the fourth lemma allows the proof to be completed. For the proof of the first three lemmas see Silverman and Tate [10: 65-75]. We are interested in the fourth lemma because it will set the foundation for our later work computing the size of the set of rational points on elliptic curves, which is known as the *rank*.

Let us now begin our proof of Lemma 2.2.5. First, to ease notation, we will rename our group of rational points on the elliptic curve $C(\mathbb{Q})$ as Γ so that $(C(\mathbb{Q}) : 2C(\mathbb{Q})) = (\Gamma : 2\Gamma)$. Let P be a point on an elliptic curve. Since we are interested in Γ and 2Γ, we want to examine the points P and $2P$. The map $P \to 2P$ is known as the *duplication map*.

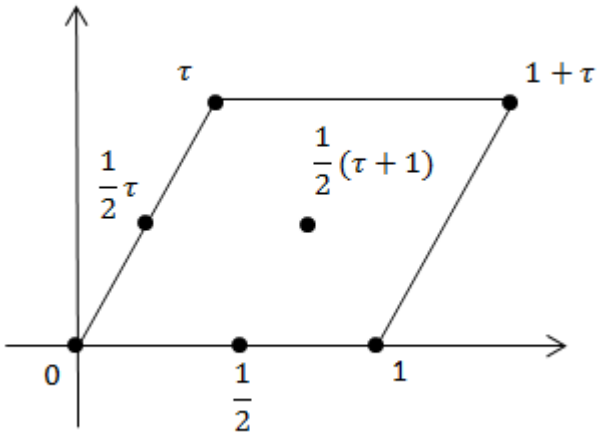


Figure 2.4: Points of order two on C/Λ

Let us examine the duplication map geometrically. Recall that an elliptic curve is isomorphic to a torus. We can examine the torus on the complex projective plane as a lattice over the complex numbers. We call the lattice Λ, and if C is our elliptic curve and R is our torus, then $R = C/\Lambda$.

To better understand how this lattice is a torus, one can imagine the video arcade game "Asteroids." When the spaceship goes off the screen, it comes back on the screen from the opposite side. In our lattice as in the video game, the top and bottom edges are connected, and so are the left and right edges. If we stretch our lattice to connect the top and bottom edges, we have a tube. If we then stretch our tube to connect the remaining two edges to each other, we form a torus. Note that $0 = \tau = 1 + \tau = 1$.

Recall from basic abstract algebra that if we know how many points our map sends to the kernel, we know that the map sends that same number of points to any other point. On our lattice, $(0, 0), 1/2\tau, 1/2$, and $1/2(1+\tau)$ are points of order two. Since four points are in the kernel, we say that $P \to 2P$ is a four-to-one map, or a map of degree four. To make things easier, we can break our duplication map into two simpler pieces by composing two maps of degree two. We will create our two maps so that they go from our curve C to another, related, curve $\bar{C}$, and then back again to C.

If we have at least one rational point of order two, we can always perform a change of coordinates to make that point $(0, 0)$. From this point on, we will be looking at the class of curves that go through the point $(0, 0)$; such curves have $C = 0$ and no constant term.

We have that $C : y^2 = x^3 + ax^2 + bx$. When define our new curve so that

$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. Note that we can create $\bar{\bar{C}}$, and when we do we get

$$\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx.$$

If we set $y = 8y$ and $x = 4x$ and divide the equation by 64, we get C. Since C and $\bar{\bar{C}}$ only differ by scaling, they are isomorphic.

We will define our map between C and $\bar{C}$ so that we can relate the points in Γ to the points in $\bar{\Gamma}$ [10: 71-79].

Proposition 2.2.6. *Let C and $\bar{C}$ be the elliptic curves given by the equations*

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

and

$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$.

Let $T = (0, 0) \in C$.

(a) There is a homomorphism $\phi : C \to \bar{C}$ defined by

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } P = (x, y) \neq \mathcal{O}, T \\ \bar{\mathcal{O}} & \text{if } P = \mathcal{O} \text{ or } P = T. \end{cases}$$

The kernel of ϕ is $\{\mathcal{O}, T\}$.

(b) There is a homomorphism $\psi : \bar{C} \to C$ defined by

$$\psi(\bar{P}) = \begin{cases} \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}\right) & if \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}, \bar{T} \\ \mathcal{O} & if \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T}. \end{cases}$$

The composition $\psi \circ \phi : C \to C$ is multiplication by two: $\psi \circ \phi(P) = 2P$.

For the proof of this proposition, see Silverman and Tate [10: 80-82]. Now that we have our homomorphisms, we want to find out to where our rational points are mapped. Let us examine the relationships between the images of ψ and ϕ in regards to rational points.

Claim 1. *The point $\bar{\mathcal{O}} \in \phi(\Gamma)$.*

We have that $\bar{\mathcal{O}} \in \phi(\Gamma)$ since our homomorphism defines $\bar{\mathcal{O}} = \phi(\mathcal{O})$.

Now let us examine which rational points (x, y) in Γ are sent to $\bar{T} = (0, 0)$.

Claim 2. *The point $\bar{T} = (0,0) \in \phi(\Gamma)$ if and only if $\bar{b} = a^2 - 4b$ is a perfect square.*

Proposition 2.2.6 tells us that

$$\phi(\bar{T}) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right).$$

We know that $(x,y) \neq 0$ since $(0,0) \to \mathcal{O}$. So $\phi(\bar{T}) = (0,0)$ if and only if $x \neq 0$ and $y = 0$. Now let us examine what is necessary for x to be rational under these conditions. We plug $y = 0$ into our equation for C and get that $0 = x^3 + ax^2 + bx = x(x^2 + ax + b)$. We need this to be nonzero and rational, so we need $x^2 + ax + b$ to have a rational root. We solve for x using the quadratic formula to find the roots and note that x is rational if and only if $x^2 - 4b$ is a perfect square. Thus $\bar{T} \in C$ if and only if $a^2 - 4b$. Recall that $a^2 - 4b = \bar{b}$.

Now that we have dealt with $\mathcal{O}$ and T, let us examine which points $\bar{P} = (\bar{x}, \bar{y})$ with $x \neq 0$ are in the image of $\phi(\Gamma)$. That is, we want to know which rational points on C map to $(\bar{x}, \bar{y})$.

Claim 3. *Let $\bar{P} = (\bar{x}, \bar{y}) \in \bar{\Gamma}$ with $\bar{x} \neq 0$. Then $\bar{P} \in \phi(\Gamma)$ if and only if $\bar{x}$ is the square of a rational number.*

First suppose that $\bar{P} \in \phi(\Gamma)$. Our definition of ϕ tells us that $\bar{x} = y^2/x^2 = (y/x)^2$, so $\bar{x}$ is a square. Now suppose that $\bar{x}$ is the square of a rational number. We are working with $(\bar{x}, \bar{y}) \in \bar{\Gamma}$ which satisfies

$$\bar{y}^2 = \bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - 4b\bar{x}.$$

Solving this for b, recalling that $\bar{x} \neq 0$, we get

$$\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{4\bar{x}} = b.$$

We can further write this as

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

Our supposition is that $\bar{x}$ is square of a rational number, so let $\bar{x} = w^2$ with $w \in \mathbb{Q}$. Written like this, we see that we have a difference of squares:

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

Let $x_1 = (\bar{x} - a - \bar{y}/w) \in \mathbb{Q}$ and $x_2 = (\bar{x} - a + \bar{y}/w) \in \mathbb{Q}$.

We now claim that $(x_1, y_1) \in \Gamma$ where $y_1 = x_1 w$, and to prove this we want to show that $y_1 = (x_1 w)^2 = x_1^3 + a x_1^2 + b x_1$. First we deal with the right hand side, and we begin by dividing it by x_1^2 so that we have

$$\begin{aligned} \frac{x_1^3 + a x_1^2 + b x_1}{x_1^2} &= x_1 + a + b/x_1 \\ &= x_1 + a + x_2 \\ &= \bar{x}. \end{aligned}$$

Now we divide right hand side by x_1^2 to get

$$\begin{aligned} \frac{y_1}{x_1^2} &= \frac{(x_1 w)^2}{x_1^2} \\ &= w^2 \\ &= \bar{x}. \end{aligned}$$

Thus we have proved Claim 3.

We now know that $\phi : \Gamma \to \bar{\Gamma}$ such that $\phi(\bar{x}, \bar{y}) = (w^2, \bar{y})$. Now we need to show that $\phi((x, y)) = (\bar{x}, \bar{y})$ such that

$$(x_1, y_1) \to \left(\frac{y_1^2}{x_1^2}, \frac{y_1(x_1^2 - b)}{x_1^2} \right).$$

We already have that

$$\left(\frac{y}{x}\right)^2 = w^2 = \bar{x},$$

which takes care of the first component. For the second component we need to show that

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \bar{y}.$$

We have

$$\begin{aligned} \frac{y_1(x_1^2 - b)}{x_1^2} &= \frac{x_1 w(x_1^2 - x_1 - x_1 x_2)}{x_1^2} \\ &= w(x_1 - x_2) \\ &= w\left(\frac{1}{2}\frac{\bar{y}}{w} + \frac{1}{2}\frac{\bar{y}}{w} \right) \\ &= w\left(\frac{\bar{y}}{w} \right) \\ &= \bar{y}. \end{aligned}$$

Thus we have shown that $\phi((x_1, y_1)) = (\bar{x}, \bar{y})$. A similar proof shows that $(x_2, y_2) \to (\bar{x}, \bar{y})$, where $y_2 = -wx_2$ (see Silverman and Tate [10: 84-85]). This is a two-to-one map, which results from the fact that rational points on elliptic curves can be reflected over the x-axis.

We want to create a one-to-one homomorphism from this two-to-one map. Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers, and let $\mathbb{Q}^{*2}$ be the subgroup of squares of elements of $\mathbb{Q}^*$ such that

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

We will create a map α from Γ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ where

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

We will now state the information about α, which maps points on our curve to those points modulo squares [10: 85-86].

Proposition 2.2.7. *(a) The map $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ is a homomorphism.*

(b) The kernel of α is the image $\psi(\bar{\Gamma})$, and thus α induces a one-to-one homomorphism

$$\frac{\Gamma}{\psi(\bar{\Gamma})} \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

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

$$\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t} : \text{ each } \epsilon_i \text{ equals } 0 \text{ or } 1\}.$$

(d) The index $(\Gamma : \psi(\bar{\Gamma}))$ is at most 2^{t+1}.

For the proof of (a) see Silverman and Tate [10: 86]. For part (b), recall that the image of $\psi(\bar{\Gamma})$ consists of squares. Since α takes points in Γ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$, we can see that $\psi(\bar{\Gamma})$ is the kernel of α. By taking Γ modulo the kernel, $\psi(\bar{\Gamma})$, we make the map injective.

To prove part (c), let us examine the image of α. As we have done before, we begin by finding which rational numbers can occur as the x coordinate of points in Γ. According to Silverman and Tate, such points have coordinates $x = m/e^2$ and $y = n/e^3$ for integers m, n, and e with

$\gcd(m,e) = \gcd(n,e) = 1$. We substitute this information into our equation for an elliptic curve to obtain

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx \\ (n/e^3)^2 &= (m/e^2)^3 + a(m/e^2)^2 + b(m/e^2) \\ n^2/e^6 &= m^5/e^6 + am^2/e^4 + bm/e^2 \\ n^2 &= m^3 + am^2e^2 + bme^4 \\ n^2 &= m(m^2 + ame^2 + be^4). \end{aligned}$$

Let $d = \gcd(m, m^2 + ame^2 + be^4)$. Since d divides m, it must also divide be^4 since every other term in $m^2 + ame^2 + be^4$ has m in it. But since m and e are relatively prime, d must divide b. We can write d as a product of its prime factors, and those factors must divide either m, b or both.

We claim that every prime dividing m is to an even power, except for possibly the primes that divide b. Suppose p_1 is a prime factor of d that does not divide b. Then p_1 does not divide $(m^2 + ame^2 + be^4)$ and must divide m. Since $m(m^2 + ame^2 + be^4)$ equals a square, p_1 must be to an even power.

Now we can write $m = \pm q^2 p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t}$ where q is a rational number, each ϵ_i is either zero or one, and $p_1, \ldots, p_t$ are the distinct primes dividing b. Recall that α takes a point P on our curve and maps it to the x-coordinate modulo squares. We can now write

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t} \pmod{\mathbb{Q}^{*2}}.$$

Thus we have proved part (c) of Proposition 2.2.7.

Proving part (d) amounts to counting elements. The subgroup of part (c) contains 2^{t+1} elements. From part (b), we know that our homomorphism, which maps $\Gamma/\psi(\bar{\Gamma})$ to this subgroup, is injective. Thus the index of $\psi(\bar{\Gamma})$ inside Γ is finite and at most 2^{t+1}.

The last piece of the proof of Lemma 2.2.5 is the following lemma [10: 87].

Lemma 2.2.8. *Let A and B be abelian groups, and consider two homomorphisms $\phi : A \to B$ and $\psi : B \to A$. Suppose that*

$$\psi \circ \phi(a) = 2a \text{ for all } a \in A \text{ and } \phi \circ \psi(b) = 2b \text{ for all } b \in B.$$

Suppose further that $\phi(A)$ has a finite index in B, and $\psi(B)$ has finite index in A. Then $2A$ has finite index in A. More precisely, the index satisfies:

$$(A : 2A) \leq (a : \psi(B))(B : \phi(A)).$$

Part (d) of Proposition 2.2.7 tells us that $(\Gamma : \psi(\bar{\Gamma}))$ has a finite index. This allows us to use Lemma 2.2.8 to state Lemma 2.2.5, that the index of $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite. Lemma 2.2.5 then completes the proof of Mordell's Theorem, that the abelian group of rational points on an elliptic curve is finitely generated.

2.3 The Rank of an Elliptic Curve

Mordell's theorem tells us we can find all of the rational points on an elliptic curve from some finite set using our group law from Section 2.1.

A point in a group is called a *torsion point* if it has finite order. If all points in a group are torsion points, that group is called a *torsion group*. According to the Nagell-Lutz Theorem, rational points on elliptic curves that are torsion points have integer coordinates [9: 391]. Mazur's Theorem tells us that a torsion group can contain at most sixteen points including $\mathcal{O}$ [9: 391]. Torsion groups are completely understood, especially by Mazur's Theorem.

A group is said to be *torsion-free* when it contains no non-trivial torsion elements, other than, of course, the identity. We call torsion-free groups finitely generated *free groups*. A free group is a group in which every element can be written as a finite *unique* linear combination of elements of a generating set. That is, if $P_1, \dots P_r$ form a generating set for a free group G, then every $P \in G$ can be written as

$$P = n_1 P_1 + \cdots + n_r P_r$$

where the integers n_i are uniquely determined by P. This gives us a group isomorphism $G \cong \mathbb{Z}^r$ with r an integer that is greater than or equal to zero.

If S is the torsion subgroup of Γ, then Γ/S is the unique maximal torsion-free quotient of Γ. Recall that Γ is a finitely generated abelian group; because of this, we can write Γ as the direct sum of its torsion subgroup and a torsion-free subgroup so that $\Gamma = S \oplus G$. Note that the torsion part is finite, since each element is of finite order and it consists of a finite number of generators. Thus we can write

$$S \cong C_{p_1^{\nu_1}} \oplus \cdots \oplus C_{p_s^{\nu_s}}$$

where C_{p^k} is the cyclic group $\mathbb{Z}/p^k\mathbb{Z}$. This gives us what is known as the Structure Theorem for Finitely Generated Abelian Groups [11: 405].

Proposition 2.3.1 (Structure Theorem)**.** *We can write any finitely generated abelian group* Γ *as a direct sum of the form*

$$\Gamma \cong C_{p_1^{\nu_1}} \oplus \cdots \oplus C_{p_s^{\nu_s}} \oplus \mathbb{Z}^r.$$

We call the size of the smallest torsion-free generating set, r, the *rank* of the curve. As opposed to the torsion group, the rank is not well understood. Among many other questions, it is not known if the set of ranks of elliptic curves over the rationals is bounded. Even though we will find a formula for the rank, it can be very difficult to obtain the information necessary to use the formula. We will examine various methods one can employ in the computations, but there is no method that guarantees that we can find the necessary information to compute the rank.

2.4 Finding a Formula for the Rank

We will begin our quest to find a formula for the rank with what we know from Mordell's Theorem, that we have a finite set of generators. Since every rational point on our curve can be written as a linear combination of these generators, for any point P belonging to Γ,

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 \cdots m_s Q_s$$

where $P_1, \ldots, P_r$ is a generating set for G, the free part of Γ, and $Q_1, \ldots, Q_s$ is a generating set for S, the torsion part of Γ, and n_r and m_s are integers. The n_i are uniquely determined by P, while the m_s are determined modulo the order of the generators.

Recall that in the proof of Mordell's Theorem we dealt with the quotient group $\Gamma/2\Gamma$. The subgroup 2Γ, written as the direct sum of its torsion parts and free parts, looks like

$$2\Gamma \cong 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z} \oplus 2C_{p_1^{\nu_1}} \oplus 2C_{p_s^{\nu_s}}$$

with each $C_{p_s^{\nu_s}}$ having finite order $p_s^{\nu_s}$. So our quotient group looks like

$$\frac{\Gamma}{2\Gamma} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{C_{p_1^{\nu_1}}}{2C_{p_1^{\nu_1}}} \oplus \cdots \oplus \frac{C_{p_s^{\nu_s}}}{2C_{p_s^{\nu_s}}}.$$

We note that

$$\frac{C_{p_i^{\nu_i}}}{2C_{p_i^{\nu_i}}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong C_2$$

is cyclic of order two. We also can see that

$$\frac{C_{p_i^{\nu_i}}}{2C_{p_i^{\nu_i}}} \cong \begin{cases} C_2 & \text{if } p_i = 2 \\ 0 & \text{if } p_i \neq 2. \end{cases}$$

Let w be the number of j with $p_j = 2$. We can write

$$(\Gamma : 2\Gamma) = 2^{r+w}.$$

Now let us look at $\Gamma[2]$, the subgroup of points belonging to Γ such that $2Q = \mathcal{O}$. Since we are dealing with a subgroup of Γ, we can write each element of this subgroup as a linear combination of the generators. Thus we can write $2Q = \mathcal{O}$ as

$$2(n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s) = \mathcal{O}.$$

This equation has solutions only if $n_i = 0$ for each i and $2m_j \equiv 0 \pmod{p_j^{\nu_j}}$. We have two cases: either p is odd or even. If p is odd and $2m \equiv 0 \pmod{p^\nu}$, then we must have that $m \equiv 0 \pmod{p^\nu}$. If p is even and $2m \equiv 0 \pmod{2^\nu}$, then $m \equiv 0 \pmod{p^{\nu-1}}$. Thus if w is the number of j with $p_j = 2$, then

$$\#\Gamma[2] = 2^w.$$

Recall that $(\Gamma : 2\Gamma) = 2^{r+w}$. With our new information, we can write

$$(\Gamma : 2\Gamma) = 2^{r+w} = 2^r \cdot \#\Gamma[2].$$

Since we have done this work in general, our new result holds for any finitely generated abelian group of rank r.

Recall our homomorphisms ϕ and ψ, and recall that $\phi \circ \psi$ is multiplication by two. We can write

$$(\Gamma : 2\Gamma) = (\Gamma : \psi \circ \phi(\Gamma)).$$

Note that $\Gamma \leq \psi(\bar{\Gamma}) \leq 2\Gamma$. From abstract algebra, we have the fact that if G is a group and $A \leq B \leq G$, then $(G : A) = (G : B)(B : A)$. Using this, we can write

$$(\Gamma : 2\Gamma) = (\Gamma : \psi(\bar{\Gamma}))(\psi(\bar{\Gamma}) : \psi \circ \phi(\Gamma)).$$

We are interested in the rightmost index because it will help us obtain our formula for the rank.

Suppose $\psi : A \to A'$ and B is a subgroup of A to ease notation. Now let us examine $(\psi(A) : \psi(B))$. Recall from abstract algebra the Second Isomorphism Theorem. [4: 97]

Theorem 2.4.1 (The Second Isomorphism Theorem)**.** *Let G be a group, and let A and B be subgroups of G. Then $AB/B \cong A/A \cup B$.*

We can apply this theorem to get

$$\begin{aligned}(\psi(A) : \psi(B) &\cong \frac{A}{B + \ker(\psi)} \\ &\cong \frac{A/B}{(B + \ker(\psi))/B} \\ &\cong \frac{A/B}{\ker(\psi)/(\ker(\psi) \cup B)} \\ &\cong \frac{(A : B)}{(\ker(\psi) : \ker(\psi)) \cap B}.\end{aligned}$$

Let us use this new formula in conjunction with our formula for $(\Gamma : 2\Gamma)$. Let $A = \bar{\Gamma}$ and $B = \phi(\Gamma)$. Then

$$\begin{aligned}(\Gamma : 2\Gamma) &= (\Gamma : \psi(\bar{\Gamma})(\psi(\bar{\Gamma}) : \psi \circ \phi(\Gamma) \\ &= (\Gamma : \psi(A))(\psi(A) : \psi(B)) \\ &= \frac{(\Gamma : \psi(A))(A : B)}{(\ker(\psi) : \ker(\psi) \cap B)} \\ &= \frac{(\Gamma : \psi(\bar{\Gamma}))(\bar{\Gamma} : \phi(B))}{(\ker(\psi) : \ker(\psi) \cap B)}.\end{aligned}$$

Recall that $\bar{T} \in \phi(\Gamma)$ where $\bar{T} = (0, 0)$ if and only if $\bar{b} = a^2 - 4b$ is a square. Thus

$$(\ker(\psi) : \ker(\psi) \cap \phi(\Gamma)) = \begin{cases} 2 & \text{if } \bar{b} \text{ is not a square} \\ 1 & \text{if } \bar{b} \text{ is a square.} \end{cases}$$

Recall that $(\Gamma : 2\Gamma) = 2^r \cdot \#\Gamma[2]$. Recall that in Section 2.2 we found that there are four complex points of order two. Recall that such points have $y = 0$, so our equation becomes $0 = x(x^2 + ax + b)$. Then if $a^2 - 4b$ from the quadratic formula is a square, x is rational, giving us that all four points of order two are rational. If $a^2 - 4b$ is not a square, then we have only two rational points of order two: $\mathcal{O}$ and $(0, 0)$. We can write this conclusion as

$$\#\Gamma[2] = \begin{cases} 2 & \text{if } a^2 - 4b \text{ is not a square} \\ 4 & \text{if } a^2 - 4b \text{ is a square.} \end{cases}$$

We note that

$$\#\Gamma[2] \cdot (\ker(\psi) : \ker(\psi) \cap \phi(\Gamma)) = \begin{cases} 4 & \text{if } a^2 - 4b \text{ is not a square} \\ 4 & \text{if } a^2 - 4b \text{ is a square.} \end{cases}$$

Thus we have

$$2^r = \frac{(\Gamma : 2\Gamma)}{\#\Gamma[2]} = \frac{(\Gamma : \psi(\bar{\Gamma})) \cdot (\bar{\Gamma} : \phi(\Gamma))}{(\ker(\psi) : \ker(\psi) \cap \phi(\Gamma))}.$$

The indices in the numerator will be each a power of two, so we will be dealing with integers. We do not want to have to find the indices in our future computations, so our next task is to change them to an easier to use form. Recall our homomorphism $\bar{\alpha} : \bar{\Gamma} \to Q* /Q^{*2}$ [10: 91]. We showed that $\ker(\alpha) = \psi(\bar{\Gamma})$. So we can write

$$\alpha(\Gamma) \cong \frac{\Gamma}{\ker(\alpha)} \cong \frac{\Gamma}{\psi(\bar{\Gamma})}.$$

Thus

$$(\Gamma : \psi(\bar{\Gamma})) = \#\alpha(\Gamma).$$

Using this same concept on $\bar{\alpha}$, we get that

$$(\bar{\Gamma} : \phi(\Gamma)) = \#\alpha(\Gamma).$$

So we can now write our formula as

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4}.$$

This is the final version of the formula we will use to calculate the rank of an elliptic curve. Note that we need to know the number of points in $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$ in order to use this formula. We can usually find lower bounds on these sets and thus on the rank, but it can be extremely difficult to prove that we have found every point in the sets, which we would need in order to know the rank exactly.

Chapter 3

Computing the Rank of Elliptic Curves

3.1 Determining the Order of $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$

Using our formula for the rank,

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4},$$

involves knowing how many points belong to $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$. We will determine an equation to tell us which rational numbers modulo squares can occur as points on Γ. Our work can then be applied to $\bar{\alpha}(\bar{\Gamma})$ in exactly the same way.

According to Silverman and Tate, points on our curve have coordinates of the form $x = m/e^2$ and $y = n/e^3$ [10: 92]. First suppose that $m = 0$. Then $(x, y) = (0, 0)$ and $\alpha((0, 0)) = b$ by how we defined our homomorphism. This tells us that b modulo squares is always in $\alpha(\Gamma)$. If b is a square, then we know automatically two points on Γ. Let $a^2 - 4b = d^2$ so that $b = (d^2 - a^2)/(-4)$. Then modulo squares, we have the points

$$\left(\frac{-a+d}{2}, 0\right) \text{ and } \left(\frac{-a-d}{2}, 0\right).$$

Thus if $m = 0$, we know that $b \in \alpha(\Gamma)$, and if it is a square, we further know that $(-a \pm d)/2 \in \alpha(\Gamma)$.

Now suppose that $m, n \neq 0$. Recall from Section 2.2 that such points satisfy

$$n^2 = m(m^2 + ame^2 + be^4).$$

Let $b_1 = \pm \gcd(m, b)$, and let us choose the sign that makes it so $mb_1 \geq 0$. We can then write $m = b_1 m_1$ and $b = b_1 b_2$ with $\gcd(m_1, b_1) = 1$ and $m_1 \geq 0$. When we substitute this information into the equation for our curve, we get

$$n^2 = b_1 m_1 (b_1^2 m_1^2 + a b_1 m_1 e^2 + b_1 b_2 e^4) = b_1^2 m_1 (b_1 m_1^2 + a m_1 e^2 + b_2 e^4).$$

We want to simplify this further, so we note that since b_1^2 divides n^2, b_1 divides n. Let $n = b_1 n_1$. Then

$$n_1^2 = m_1 (b_1 m_1^2 + a m_1 e^2 + b_2 e^4).$$

Recall that when $m_1 \geq 0$, we have $\gcd(b_2, m_1) = 1$ and $\gcd(e, m) = 1$. Since m_1 divides m, we also note that $\gcd(e, m_1) = 1$. From this information we can see that m_1 and $b_1 m_1^2 + a m_1 e^2 + b_2 e^4$ are relatively prime. If the product of two relatively prime numbers is a square, then each of those two numbers must also be a square. To represent this, we say that $n_1 = MN$ where

$$M^2 = m_1 \text{ and } N^2 = b_1 m_1^2 + a m_1 e^2 + b_2 e^4.$$

These two equations can be combined to write

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4.$$

This is the version of our equation that we will use to compute the rank. Using this equation, we know that if we begin with a point $(x, y) \in \Gamma$ with $y \neq 0$, then we can write

$$x = \frac{m}{e^2} = \frac{b_1 m_1}{e^2} = \frac{b_1 M^2}{e^2}$$

and

$$y = \frac{n}{e^3} = \frac{b_1 n_1}{e^3} = \frac{b_1 MN}{e^3}.$$

From our assumption that $\gcd(b_2, m_1) = 1$ and the fact that x and y are in lowest terms, we obtain the side conditions that

$$\gcd(M, e) = \gcd(n, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1.$$

Thus we know what the image of $\alpha(\Gamma)$ looks like.

In order to compute the rank, we will need to find $\#\alpha(\Gamma)$ and $\#\bar{\alpha}(\bar{\Gamma})$. We do this by first dealing with C and then working with $\bar{C}$ in the same way. For each possible factorization of $b = b_1 b_2$, we write $N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$. We will then attempt to determine if each equation has a

solution or not. Recall that b is always in $\alpha(\Gamma)$, and that we are looking for points with $m, n \neq 0$ with

$$\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1.$$

For the most part, this will involve crunching numbers, but we will develop techniques to allow us to obtain multiple results at once.

3.2 Computational Examples

We will go through three computational examples to demonstrate methods that are used to find the rank. We will look at the curves $y^2 = x^3 - 82, y^2 = x^3 + 3x$, and $y^2 = x^3 + 73x$. These are carefully chosen examples intended to allow the demonstration of various ad hoc methods that we can use to compute the rank.

Example 1. Our first example will be to find the rank of $C : y^2 = x^3 - 82x$.

Recall that the formula we use to find the rank is

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4}.$$

We will now explicitly find $\#\alpha(\Gamma)$ and $\#\bar{\alpha}(\bar{\Gamma})$.

To begin finding points, we first examine C. We have that $a = 0$ and $b = -82$. We now factor b into $b = b_1 b_2$ modulo squares, and list the different factorizations as the ordered pairs

$$(b_1, b_2) : (1, -82), (-1, 82), (2, -41), (-2, 41), (41, -2), \\ (-41, 2), (82, -1), (-82, 1).$$

For each factorization, we plug b_1, b_2 into $N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$ to get a list of equations:

$$N^2 = M^4 - 82e^4 \tag{3.1}$$
$$N^2 = -M^4 + 82e^4 \tag{3.2}$$
$$N^2 = 2M^4 - 41e^4 \tag{3.3}$$
$$N^2 = -2M^4 + 41e^4 \tag{3.4}$$
$$N^2 = 41M^4 - 2e^4 \tag{3.5}$$
$$N^2 = -41M^4 + 2e^4 \tag{3.6}$$
$$N^2 = 82M^4 - e^4 \tag{3.7}$$
$$N^2 = -82M^4 + e^4. \tag{3.8}$$

We note that equations (3.5) through (3.8) have a corresponding equation in (3.1) through (3.4) where $(b_1, b_2) = (b_2, b_1)$. If we find a solution to one equation, we automatically know the solution to its corresponding equation. Thus we only need to examine the first half of this list. We will put solutions in the form (M, e, N). If an equation has a solution, then $b_1 \in \alpha(\Gamma)$.

First, recall that $b \in \alpha(\Gamma)$ automatically. This tells us without any computations that equation (3.7) as well as its corresponding equation (3.2) both have solutions. Note that $\alpha(\Gamma)$ is a group and thus needs to contain the identity element, so equation (3.1), where $b_1 = 1$, has a solution in addition to its corresponding equation (3.8). So far we have

$$\alpha(\Gamma) \supseteq \{-82, -1, 1, 82\}.$$

Now we need to examine the rest of the equations. First we try plugging in some small numbers to see if there are any easily found solutions. In doing so, we find that equation (3.4) has $(2, 1, 3)$ as a solution, which tells us that equation (3.5) also has a solution, giving us

$$\alpha(\Gamma) \supseteq \{-82, -2-1, 1, 41, 82\}.$$

Upon further examination, there are no more readily apparent solutions. We will next develop a trick using the fact that $\alpha(\Gamma)$ is a group. Examining the group structure of $\alpha(\Gamma)$ so far, we see that it is not yet closed. If we multiply our current elements together, we find that $\alpha(\Gamma)$ must contain 2 and -41 in order to complete the group. With the addition of these two, we have all of the points in $\alpha(\Gamma)$.

We have found that

$$\alpha(\Gamma) = \{-82, -41, -2, -1, 1, 2, 41, 82\}$$

and

$$\#\alpha(\Gamma) = 8.$$

In this case, every equation has a solution.

We next examine $\bar{C} = x^3 + 328x$ using the same technique. We have $\bar{b} = a^2 - 4b = 328$, which is not a square. Listing the factors of $\bar{b}$ modulo squares we have

$$(\bar{b_1}, \bar{b_2}) : (-1, -82), (1, 82), (2, 41), (-2, -41), (41, 2), (-41, -2), \\ (82, 1), (-82, -1).$$

Note that we used the facts that $328 \equiv 82 \pmod{\mathbb{Q}^{*2}}, 8 \equiv 2 \pmod{\mathbb{Q}^{*2}}$, and $164 \equiv 41 \pmod{\mathbb{Q}^{*2}}$. We plug each factorization into $N^2 = \bar{b_1}M^4 + \bar{a}M^2e^2 + \bar{b_2}e^4$ to get:

$$\begin{aligned} N^2 &= -M^4 - 82e^4 && (3.9)\\ N^2 &= M^4 + 82e^4 && (3.10)\\ N^2 &= 2M^4 + 41e^4 && (3.11)\\ N^2 &= -2M^4 - 41e^4 && (3.12)\\ N^2 &= 41M^4 + 2e^4 && (3.13)\\ N^2 &= -41M^4 - 2e^4 && (3.14)\\ N^2 &= 82M^4 + 2e^4 && (3.15)\\ N^2 &= -82M^4 - 2e^4 && (3.16) \end{aligned}$$

First we note our corresponding equations: (3.10) and (3.14), and (3.11) and (3.13). Note that this time there are not any equations we can eliminate with $(\bar{b_1}, \bar{b_2}) = (\bar{b_2}, \bar{b_1})$.

We note that if both $\bar{b_1}$ and $\bar{b_2}$ are negative, N^2 would be negative. Thus any pairs where both $\bar{b_1}$ and $\bar{b_2}$ are negative can be eliminated because they have no solutions. In our case, we can eliminate the equations (3.9), (3.12), (3.14), and (3.16) as not having solutions. The following is our reduced list of equations:

$$\begin{aligned} N^2 &= M^4 + 82e^4 && (3.17)\\ N^2 &= 2M^4 + 41e^4 && (3.18)\\ N^2 &= 41M^4 + 2e^4 && (3.19)\\ N^2 &= 82M^4 + 2e^4. && (3.20) \end{aligned}$$

We have that $\bar{b_1} = 328 \equiv 82 \pmod{\mathbb{Q}^{*2}}$ and $\bar{b_1} = 1$ are automatically in our set, so equations (3.17) and (3.20) have solutions. By trying small numbers, we find that both equation (3.18) and its corresponding equation (3.19) have the solution $(1, 1, 7)$. We have now found solutions to all of our equations and know that

$$\bar{\alpha}(\bar{\Gamma}) = \{82, 1, 2, 41\},$$

and thus

$$\#\bar{\alpha}(\bar{\Gamma}) = 4.$$

Compiling our information, we have found that $\#\alpha(\Gamma) = 8$ and $\#\bar{\alpha}(\bar{\Gamma}) = 4$. We can now plug these numbers into our equation for the rank to get

$$2^r = \frac{8 \cdot 4}{4} = 2^3.$$

Thus the rank of $C : y^2 = x^3 - 82x$ is three.

Example 2. Now let us find the rank of $C : y^2 = x^3 + 3x$.

Note that on C we have $a = 0$, and $b = 3$. We begin by factoring b and writing all of the possible factors as the ordered pairs modulo squares to obtain

$$(b_1, b_2) : (1, 3), (-1, -3), (3, 1), (-3, -1).$$

We plug each factorization into $N^2 = b_1 M^4 + aM^2 e^2 + b_2 e^4$ to get

$$N^2 = M^4 + 3e^4 \tag{3.21}$$
$$N^2 = -M^4 - 3e^4 \tag{3.22}$$
$$N^2 = 3M^4 + e^4 \tag{3.23}$$
$$N^2 = -3M^4 - e^4. \tag{3.24}$$

Immediately we see that equations (3.22) and (3.24) do not have solutions because both b_1 and b_2 are negative. Since the remaining two equations (3.21) and (3.23) are corresponding equations, we only have to see if one of the two equations has a solution on C. By plugging in small numbers, we can find that $(1, 1, 2)$ is a solution to (3.21) and (3.23). However, we could have known that such a solution existed without any computations because in equation (3.21), $b_1 = 1$. We have found that

$$\alpha(\Gamma) = \{1, -1\}$$

and

$$\#\alpha(\Gamma) = 2.$$

Now we examine $\bar{C} = x^3 - 12x$ where $\bar{b} = -12 \equiv -3 \pmod{\mathbb{Q}^{*2}}$. We write the factors of $\bar{b}$ as the ordered pairs modulo squares

$$(\bar{b_1}, \bar{b_2}) : (1, -12), (-1, 12), (2, -6), (-2, 6)(3, -4), (-3, 4), (4, -3), (-4, 3),$$
$$(6, -2), (-6, 2).$$

We plug each factorization into $N^2 = \bar{b_1}M^4 + \bar{a}M^2e^2 + \bar{b_2}e^4$ to get

$$\begin{aligned} N^2 &= M^4 - 3e^4 && (3.25)\\ N^2 &= -M^4 + 3e^4 && (3.26)\\ N^2 &= 2M^4 - 6e^4 && (3.27)\\ N^2 &= -2M^4 + 6e^4 && (3.28)\\ N^2 &= 3M^4 - e^4 && (3.29)\\ N^2 &= -3M^4 + e^4 && (3.30)\\ N^2 &= M^4 - 3e^4 && (3.31)\\ N^2 &= -M^4 + 3e^4 && (3.32)\\ N^2 &= 6M^4 - 2e^4 && (3.33)\\ N^2 &= -6M^4 + 2e^4. && (3.34) \end{aligned}$$

We cannot immediately eliminate any equations as not having solutions. As always, we do know that b_1 and the identity are in $\alpha(\Gamma)$, which tells us that equations (3.26), (3.31) and (3.32) have solutions. By plugging in small numbers we find that $(1, 1, 2)$ is a solution for (3.29) and (3.34), and $(1, 1, 1)$ is a solution for (3.31) and (3.32).

We need to develop new methods in order to check the rest of our equations. First note that if an equation does not have a solution modulo some number, it does not have a solution at all, and that $M^4 \equiv e^4 \equiv 1 \pmod 3$. Let us look at equation (3.29) modulo three, and suppose it has a solution:

$$N^2 \equiv -1 \equiv 2 \pmod 3.$$

This equation does not have a solution because 2 is not a square. Similarly, we can write equation (3.27) as

$$N^2 \equiv -4 \equiv 2 \pmod 3.$$

Once again, this equation does not have a solution. We look at our final equation, (3.26), in the same way to obtain

$$N^2 \equiv 2 \pmod 3,$$

which also has no solutions.

With that, we have eliminated the rest of our equations. We have found that equations (3.25), (3.28), (3.30), and (3.33) have solutions, and have shown that the rest of the equations cannot have solutions. Thus we know that

$$\bar{\alpha}(\bar{\Gamma}) = \{-3, -2, 1, 6\}$$

and

$$\#\bar{\alpha}(\bar{\Gamma}) = 4.$$

We now apply our equation for the rank to find

$$2^r = \frac{2_4}{4} = 4.$$

Thus the rank of $C : y^2 = x^3 + 3x$ is one.

Example 3. Now let us find the rank of $C : y^2 = x^3 + 73x$.

As before, we find the factors of $b = 73$, and we obtain four equations that do not correspond. Two of the equations are subsequently eliminated because b_1 and b_2 are both negative, and we know that the other two equations must have solutions because $b = 1$ and $b = 73$ are automatically in $\alpha(\Gamma)$. So we have

$$\alpha(\Gamma) = \{1, 73\}.$$

Now we look at $\bar{C} : y^2 = x^3 - 292x$. Note that $-292 \equiv -73$. Taking into account that the equations with $\bar{b_1} = 1$ or $\bar{b_1} = \bar{b}$ automatically have solutions, we are left with:

$$N^2 = -M^4 - 292e^4 \tag{3.35}$$
$$N^2 = 2M^4 - 146e^4 \tag{3.36}$$
$$N^2 = -2M^4 + 146e^4 \tag{3.37}$$
$$N^2 = 73M^4 - 4e^4. \tag{3.38}$$

By plugging in small numbers, we find that $(1, 2, 3)$ is a solution to equation (3.38). We add the b_1's in these equations as well as those in their corresponding equations into our set of points in $\bar{\alpha}(\bar{\Gamma})$. Stopping here briefly, we note that so far we have

$$\#\alpha(\Gamma) = 2$$

and

$$\bar{\alpha}(\bar{\Gamma}) \supseteq \{-73, 1, 2, -146\}.$$

Recall that our equation for the rank is

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4}.$$

Once we can prove if some of the equations either have solutions or do not have solutions, we can narrow down what the rank can possibly be. In this case, if we can prove that if at least one equation has no solution, the rank must be one. If we can find one more solution, then the rank must be two, because $\bar{\alpha}(\bar{\Gamma})$ must have four more points in order for the equation to be satisfied. The rank cannot be any higher because we have eight original equations. Thus if we can learn about one more equation we find the rank and do not have to do any more work.

In this case, we next find that $(3, 1, 4)$ is a solution to equation (3.36) so that $b_1 = 73 \in \bar{\alpha}(\bar{\Gamma})$. We do not need to explicitly find any more solutions, because the rank of $C : y^2 = x^3 + 73x$ must be two.

To determine if our equations have solutions, we either have to explicitly find a solution, show that one has to exist, or show that one cannot exist. We have developed several techniques to help us with this task.

First, we noted that if two equations correspond, what we know about one applies to the other. Often this means we only have to check half of our equations. We next noted that if b_1 and b_2 are both negative, the equation does not have a solution in the real numbers and thus does not have a rational solution. If in our equation for C our b is positive, we immediately know that we can use this trick and dramatically reduce the number of equations we have to examine.

When we only have a couple of equations left, it can be useful to check the group structure to see which points must be included in order for the group to be closed. We then looked at equations modulo three to prove that equations did not have solutions. We can also use this trick modulo other numbers. For example, from Fermat's Little Theorem we know that $M^4 \equiv e^4 \equiv 1 \pmod 5$. We then get that $N^2 \equiv c \pmod 5$ where c is an integer. As when working in modulo three, if c is not a square, the equation has no solutions.

One further trick is keeping track of how many equations we have solved. It is possible to find the rank without explicitly finding every solution due to the nature of the rank formula.

Though we have a nice selection of techniques, in practice one will come across many situations in which further ad hoc techniques must be developed. Though computing the rank of some curves is simple, there is no known method for determining the rank that always works in general because of the difficulty of proving that we have found all of the possible points in $\alpha(\Gamma)$ and $\bar{\alpha}(\bar{\Gamma})$.

Chapter 4

Current Information About Elliptic Curves

In closing, we will put elliptic curves and their ranks in context by discussing record ranks and applications of elliptic curves. So far we have concentrated on the proof of Mordell's Theorem and the methods used to compute the rank. Our examples are meant to demonstrate how calculating the rank uses primarily ad hoc methods. Much about the rank is not fully understood.

One of the Clay Mathematics Institute Millennium Prize Problems is the Birch and Swinnerton-Dyer Conjecture [2]. An elliptic curve E has an associated zeta function $\zeta_E(s)$. One version of the conjecture says $s = 1$ is a zero at ζ_E if and only if the rank of E is greater than or equal to one. More generally, the rank of E equals the order of vanishing of ζ at $s = 1$. As of the time of writing, only special cases of this conjecture have been proven correct.

4.1 Record and Average Ranks

The elliptic curves in our examples have low ranks, but it is possible to construct curves with much higher ranks. It is not known what values of the rank are possible for elliptic curves over the rationals, but many mathematicians informally conjecture that the rank can be arbitrarily large. It is easier to figure out within what range the rank falls than to calculate the exact rank. Even curves with record ranks often have a lower bound but are not known exactly.

The current curve of a record rank was found by Elkies in 2006 and is of rank greater than or equal to 28 [3]. If

$$a = 20067762415575526585033208209338542750930230312178956502$$

and

$$b = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9,$$

then the curve is

$$y^2 + xy + y = x^3 - x^2 - ax + b.$$

The current curve with highest rank that is known exactly was found by Elkies in 2009, and has rank 19 [3]. If

$$c = 31368015812338065133318565292206590792820353345$$

and

$$d = 3020388026985660873356431884295434986245220416838744935551860625681598 47$$

then the curve is

$$y^2 + xy + y = x^3 - x^2 + cx + d.$$

The curves with record ranks all contain large numbers, which demonstrates that we would not come across these curves by accident. Indeed, computers are used to compute these high ranks. Though such computer programs use different methods than the one we used, they similarly involve solving linear equations.

While we might not know how high ranks can be, we do have information about how many high-rank curves exist. In 1997, Nagao found that there are infinitely many elliptic curves over $\mathbb{Q}$ with a non-trivial rational 2-torsion point and with rank greater than or equal to six [7]. Though it is possible to construct high-rank curves, the probability of randomly coming across a high-rank curve is very low. In fact, Bhargava and Shankar proved that the average rank of elliptic curves is bounded, and is at most 1.5 [1]. Thus the majority of elliptic curves have small ranks.

4.2 Applications of Elliptic Curves

It is valuable to mention that there are broader applications of elliptic curves beyond calculations of the rank, particularly in the study of cryptography and Fermat's Last Theorem.

4.2.1 Elliptic Curve Cryptography

Cryptography is the study and practice of transmitting data securely. New techniques are constantly being developed in order to continually keep information secure. Elliptic curve cryptography, first presented in 1985, has over time remained resilient in the face of new attacks [8]. In addition, it uses fewer bits and is faster in many situations than other cryptographic systems [11: 159]. The majority of cryptographic systems use the *discrete logarithm problem*. This is the difficulty of finding an integer k such that $a^k \equiv b \pmod{p}$. The integers a and b could belong to any group. If our group is an elliptic curve, then a and b are points on that curve. The curves used in cryptography are chosen so that the discrete logarithm problem is difficult on them. Note that $a^k \equiv b \pmod{p}$ is written multiplicatively, but in the case of elliptic curves we use addition.

4.2.2 Fermat's Last Theorem

A famous mathematical application of elliptic curves is their use in the proof of Fermat's Last Theorem. Fermat's Last Theorem, conjectured by Pierre de Fermat in 1637, says that the equation $a^n + b^n = c^n$ has no solutions in positive integers if $n \geq 3$. Over the years, many mathematicians worked on this problem unsuccessfully, though much of their work built the foundation for the final proof.

In 1986, Gerhard Frey suggested what would be the ultimately successful strategy. We will go into a sketch of the proof. Frey suggested using what is now known as the Frey curve: $y^2 = x(x + A^p)(x - B^p)$ where (A, B, C) is a supposed solution to Fermat's equation and p is a prime. Frey conjectured that a curve such as the Frey curve could not exist. In 1986, Ken Ribet proved that the Frey curve, if it exists, is not *modular*. Andrew Wiles then proved that curves in the special class of elliptic curves we deal with must all be modular. Thus $a^p + b^p = c^p$ has no nonzero integer solutions, and neither does Fermat's equation.

Although Fermat's Last Theorem itself is mostly just a curiosity with no applications, its proof greatly stimulated the study of algebraic number theory. A great number of new techniques were developed to prove the many theorems that lead to the final result.

Bibliography

[1] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *arXiv:1006.1002*, June 2010.

[2] Clay Mathematics Institute. Birch and Swinnerton-Dyer Conjecture. URL `http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture`.

[3] Andrej Dujella. History of elliptic curve rank records. URL `http://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.

[4] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004. ISBN 0-471-43334-9.

[5] Euclid. *Euclid's Elements*. Green Lion Press, Santa Fe, NM, 2002. ISBN 1-888009-18-7; 1-888009-19-5. All thirteen books complete in one volume, The Thomas L. Heath translation, Edited by Dana Densmore.

[6] Victor J. Katz. *A history of mathematics*. HarperCollins College Publishers, New York, 1993. ISBN 0-673-38039-4.

[7] Koh-ichi Nagao. Construction of high-rank elliptic curves with a nontrivial torsion point. *Math. Comp.*, 66(217):411–415, 1997. ISSN 0025-5718. doi: 10.1090/S0025-5718-97-00779-5. URL `http://dx.doi.org/10.1090/S0025-5718-97-00779-5`.

[8] National Security Association. The case for elliptic curve cryptography, January 2009.

[9] Joseph H. Silverman. *A Friendly Introduction to Number Theory*. Pearson Education, Inc., 3rd edition, 2006.

[10] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. ISBN 0-387-97825-9.

[11] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. ISBN 978-1-4200-7146-7; 1-4200-7146-7. doi: 10.1201/9781420071474. URL http://dx.doi.org/10.1201/9781420071474. Number theory and cryptography.