Elliptic Curves and 2-Selmer Ranks

Lindsay Cadwallader

B.S., Mathematics

An Undergraduate Honors Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor of Science

at the

University of Connecticut

May 2017

APPROVAL PAGE

Bachelor of Science Honors Thesis

Elliptic Curves and 2-Selmer Ranks

Presented by

Lindsay Cadwallader, B.S. Math

Honors Major Advisor _____
Luke Rogers

Honors Thesis Advisor _____
Álvaro Lozano-Robledo

University of Connecticut

May 2017

ACKNOWLEDGMENTS

I would like to express my appreciation for the guidance of Álvaro Lozano-Robledo and recognize the indispensable role he has played in my data collection and writing of this thesis.

Elliptic Curves and 2-Selmer Ranks

Lindsay Cadwallader, B.S.

University of Connecticut, May 2017

ABSTRACT

This thesis provides background on the theory of elliptic curves and focuses on Selmer ranks and how they can be used to gain information about the rank of an elliptic curve. A conjecture about the distribution of Selmer ranks is discussed and data on the distribution of Selmer ranks within families of elliptic curves that have a fixed torsion subgroup is collected.

Contents

Introduction

The set of rational points on an elliptic curve, $E(\mathbb{Q})$, turns out to have a group structure. By the Mordell-Weil Theorem, discussed in more depth later in this thesis, $E(\mathbb{Q})$ is finitely generated. Using this result, we get the isomorphism

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}, \text{ for some integer } R_E \geq 0.$$

While much is known about the torsion subgroup of $E(\mathbb{Q})$ and the possibilities for its structure, little is known about the rank, R_E, of $E(\mathbb{Q})$ and there is no reliable algorithm to compute it. In particular, it is not known whether there is a bound on how large the rank can be or what the distribution of the ranks of elliptic curves is. There are, however, conjectures on what this distribution is like. Moreover, although the rank cannot always be computed, the Selmer rank, discussed in Chapter 2, can always be computed and bounds the rank. There is a conjecture by Poonen and Rains on the distribution of Selmer ranks, but this conjecture may not hold for families of elliptic curves with a fixed torsion subgroup. This thesis presents data on the distribution of Selmer ranks of elliptic curves with fixed torsion subgroups.

Chapter 1 provides background on elliptic curves, discussing basic definitions, the group structure on $E(\mathbb{Q})$, and defines the Selmer rank and discusses how it can be used to bound the rank of an elliptic curve. Chapter 2 states a conjecture on the distribution of Selmer ranks and includes data collected on the distribution of Selmer ranks within families of elliptic curves that have a fixed torsion subgroup. The code used to compute this data is included in Chapter 3.

Chapter 1

Introduction and Background

1.1 Basic Definitions

In this chapter, we review the theory of elliptic curves, including basic definitions and their group structure. We have followed several references including [5] and [2], following sections 2.2-2.5 and 2.7 in [2] and drawing from Appendix A.

Definition 1.1.1. An *elliptic curve* E over $\mathbb{Q}$ is a smooth cubic projective curve defined over $\mathbb{Q}$ with at least one rational point, $\mathcal{O}$, called the origin.

If the coefficients of the cubic polynomial that defines E are in a field K, we say E is defined over K, written as E/K. If the characteristic of K is not 2 or 3, with a change of variables, E can be written as $y^2 = x^3 + Ax + B$ (see [5], Ch. III). This is called a *(short) Weierstrass equation*. A curve defined by a Weierstrass equation is non-singular if and only if $4A^3 + 27B^2 \neq 0$. We will also define elliptic curves using

a more general Weierstrass equation

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

where the a_i are in $\mathbb{Q}$.

In Sage, elliptic curves can be defined by using the command

```
E = EllipticCurve([a1, a2, a3, a4, a6])
```

if the curve is defined by a general Weierstrass equation, or by using the command

```
E = EllipticCurve([A, B])
```

if the curve is defined by a Weierstrass equation. Sage can convert a general Weierstrass equation defining an elliptic curve into a model of the form $y^2 = x^3 + Ax + B$ using the command

```
E.integral_short_weierstrass_model()
```

Example 1.1.2. To define an elliptic curve with the equation

$$y^2 + xy = x^3 - 49423080x + 130545230400$$

in Sage, the following command is used: `E = EllipticCurve([1, 0, 0, -49423080, 130545230400])`. To find the Weierstrass equation of this curve, the command `E.integral_short_weierstrass_model()` is used and Sage outputs the equation $y^2 = x^3 - 64052311707x + 6090910426477494$.

1.2 Group Structure on $E(\mathbb{Q})$

An addition operation can be defined on $E(\mathbb{Q})$ in such a way that $(E, +)$ is an abelian group. Let E be defined by the equation $y^2 = x^3 + Ax + B$ with A and $B \in \mathbb{Q}$. Let P and Q be two rational points on E and denote the line passing through P and Q, $\overline{PQ}$, as L. In the case that $P = Q$, define L as the tangent line to E at P. Since the elliptic curve E is cubic and already intersects L at two rational points, L must intersect E at a third rational point, call it R. The sum of P and Q is defined as the second intersection of the vertical line passing through R and E.

Example 1.2.1. Consider the curve E given by the general Weierstrass equation $y^2 + xy = x^3 - 1070x + 7812$. The torsion subgroup of this curve can be found using the Sage command `T = E.torsion_subgroup()`. The generators of the torsion subgroup, found using the commands `T.0` and `T.1`, are the points $P = (4, 58)$ and $Q = (-36, 18)$. To calculate $P + Q$, we begin by finding the slope of the line passing through P and Q. It is $m = \frac{58-18}{4-(-36)} = \frac{40}{40} = 1$. So the equation of the line passing through P and Q is $L : y = x + 54$. To find the third point of intersection of L and E, we must solve the following system of equations

$$\begin{cases} y^2 + xy = x^3 - 1070x + 7812 \\ y = x + 54. \end{cases}$$

We substitute the second equation into the first to get $-x^3 + 2x^2 + 1232x - 4896 = 0$. Factoring this equation, we get $-(x-4)(x-34)(x+36) = 0$. We already know that $P = (4, 58)$ and $Q = (-36, 18)$ are points of intersection of E and L. The third point of intersection must have $x = 34$ and $y = 34 + 54 = 88$, so we get $R = (34, 88)$. To

calculate $P+Q$ we must find the second point of intersection of E and the vertical line passing through R, $x = 34$. Substituting 34 for x into $y^2+xy = x^3-1070x+7812$ gives the solutions $y = 88$ and $y = -122$, so $P+Q = (34, -122)$. The sum $P+Q$ can be calculated in Sage by defining the points P and Q and entering `P+Q`.

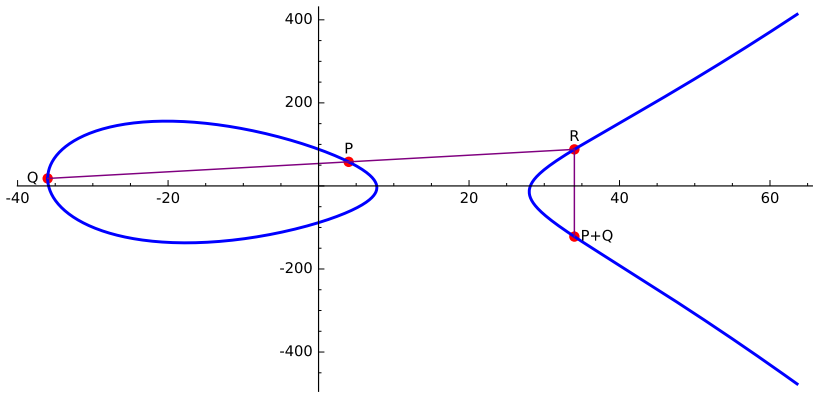

FIGURE 1.2.1: Addition of points on an elliptic curve

Example 1.2.2. We can also find multiples of the point $P = (4, 58)$ on this curve. To calculate $2P$, we must first find the tangent line to $y^2 + xy = x^3 - 1070x + 7812$ at P. Implicit differentiation can be used to find $y' = \frac{3x^2-1070-y}{2y+x}$. We substitute the coordinates of P into this equation to find that the slope of the tangent line at the point P is -9, so the equation for the line tangent to E at P is $y - 58 = -9(x - 4)$. Next, we solve the system of equations

$$\begin{cases} y^2 + xy = x^3 - 1070x + 7812 \\ y - 58 = -9(x - 4) \end{cases}$$

to find the second point of intersection of $y-58 = -9(x-4)$ with E. Doing this gives $R = (64, -482)$. Finally, to find the point $2P$, we find the second point of intersection of the vertical line passing through R and E and get that $2P = (64, 418)$. We can

calculate $3P$ by adding P to $2P$ using the same procedure as in the previous example. $4P$, $5P$, $6P$, and $7P$ can be found in the same way. Note that $7P = (4, -62) = -P$, so $7P + P = \mathcal{O}$, the point at infinity. Thus, P has order 8.

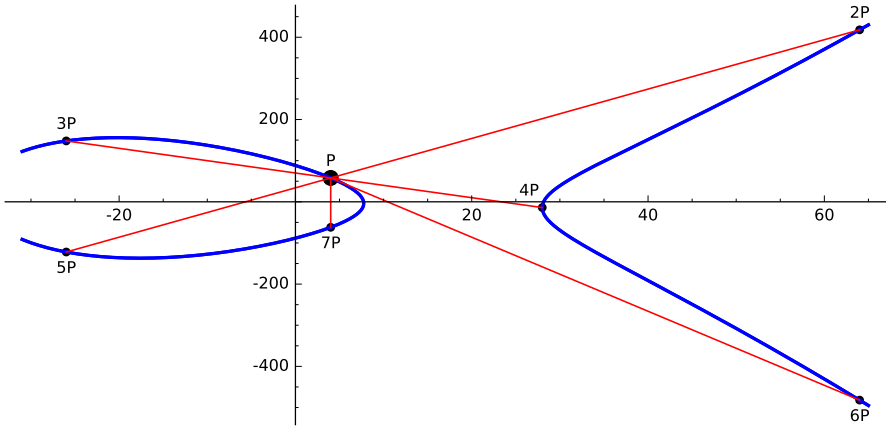

FIGURE 1.2.2: Calculating multiples of a point on an elliptic curve

The following theorem, first conjectured by Henri Poincare in 1908, provides additional information about the structure of $E(\mathbb{Q})$. It is named the Mordell-Weil theorem after Louis Mordell, who proved the theorem in 1922, and Andre Weil, who generalized it in 1928.

Theorem 1.2.3 (Mordell-Weil, [2], Theorem 2.4.3)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group.*

This means that there are points P_1, P_2,...,P_n such that any point Q in $E(\mathbb{Q})$ can be expressed as a linear combination of the P_i, so we have $Q = a_1P_1 + a_2P_2 + \ldots + a_nP_n$, for some $a_i \in \mathbb{Z}$. We call $E(\mathbb{Q})$ the Mordell-Weil group of E.

The weak Mordell-Weil theorem, stated below, is usually used in the proof of the Mordell-Weil theorem.

Theorem 1.2.4 (weak Mordell-Weil, [2], Theorem 2.4.5)**.** $E(\mathbb{Q})/mE(\mathbb{Q})$ *is a finite group for all* $m \geq 2$.

From the Mordell-Weil theorem and the structure of finitely generated abelian groups (see [1], Section 5.2, Theorem 3), we get that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}, \text{ for some integer } R_E \geq 0.$$

The group $E(\mathbb{Q})_{\text{torsion}}$ is the torsion subgroup of $E(\mathbb{Q})$, defined formally as

$$E(\mathbb{Q})_{\text{torsion}} = \{P \in E(\mathbb{Q}) : \text{there is } n \in \mathbb{N} \text{ such that } nP = \mathcal{O}\}.$$

By Mordell-Weil, $E(\mathbb{Q})_{\text{torsion}}$ is finite. The following theorem lists the possibilities for the structure of $E(\mathbb{Q})_{\text{torsion}}$.

Theorem 1.2.5 (Ogg's conjecture; Mazur, [2], Theorem 2.5.2)**.** $E(\mathbb{Q})_{torsion}$ *is isomorphic to one of the following groups:*

$\mathbb{Z}/N\mathbb{Z}$ *with* $1 \leq N \leq 10$ *or* $N = 12$*, or*

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z}$ *with* $1 \leq M \leq 4$.

The structure of the torsion subgroup of an elliptic curve E can be found using the Sage command

```
T = E.torsion_subgroup()
```

As described in Example 1.2.1, the generators of the torsion subgroup can be found by entering the commands `T = E.torsion_subgroup()`, `T.0`, and `T.1`.

The summand $\mathbb{Z}^{R_E}$ is called the *free part* of $E(\mathbb{Q})$. It is R_E copies of $\mathbb{Z}$ with $R_E \geq 0$. The free part of $E(\mathbb{Q})$ is generated by R_E points of infinite order. A point

P is said to have infinite order if there is no $n \in \mathbb{Z}$, $n \neq 0$, such that $nP = \mathcal{O}$. We call the number R_E the *rank* of $E/\mathbb{Q}$.

The rank of an elliptic curve E can be found in Sage by using the command

```
E.rank()
```

and the points of infinite order that generate the free part of $E(\mathbb{Q})$ can be found using the command

```
E.gens()
```

.

It is important to note that these commands may not always work since there is no proven algorithm that gives the rank and generators of the free part of any elliptic curve.

Example 1.2.6. Consider the curve E given by the general Weierstrass equation $y^2 + xy = x^3 - 1070x + 7812$. Recall from Example 1.2.1 that the generators of the torsion subgroup of E are $(4, 58)$ and $(-36, 18)$. Recall also that in Example 1.2.2 the point $(4, 58)$ was shown to have order 8. The point $(-36, 18)$ can be shown to have order 2. Combining this information, we get that the torsion subgroup of E is isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Entering the command `E.gens()` into Sage returns []. This tells us that the rank of this curve, which can also be found using the command `E.rank()`, is 0. So we have $E(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Example 1.2.7. Now consider the curve $E_1/\mathbb{Q} : y^2+xy+y = x^3+x^2-2365x+43251$. This curve has torsion subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$, generated by the point $(29, -4)$, which has order 5. The free part of $E_1(\mathbb{Q})$ is generated by the points $(-37, 304)$ and $(9, 146)$, which have infinite order, so the rank of E_1 is 2. We combine this information to get that $E_1(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}^2$.

Unlike the free part and rank, the torsion subgroup of $E(\mathbb{Q})$ for a given elliptic curve E can always be computed using the algorithm provided by the Nagell-Lutz theorem, that will give the torsion subgroup of $E(\mathbb{Q})$ for a given elliptic curve E, there is no proven algorithm that yields the rank of an elliptic curve.

Theorem 1.2.8 (Nagell-Lutz, [5], Ch. VIII, §7, Cor. 7.2)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of the form*

$$E : y^2 = x^3 + Ax + B, \text{ with } A, B \in \mathbb{Z}.$$

Then every torsion point $P \neq \mathcal{O}$ of E satisfies:

(1) The coordinates of P are integers.

(2) If P is a point of order $n \geq 3$, then $4A^3 + 27B^2$ is divisible by $y(P)^2$.

(3) If P is of order 2, then $y(P) = 0$ and $x(P)^3 + Ax(P) + B = 0$.

Although we may not be able to compute it directly in all cases, we can sometimes get an upper bound for the rank of an elliptic curve as in the following theorem.

Theorem 1.2.9 ([2], Theorem 2.7.4)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of the form*

$$E : y^2 = x^3 + Ax^2 + Bx, \text{ with } A, B \in \mathbb{Z}.$$

For an integer $N \geq 1$, let $\nu(N)$ be the number of distinct positive prime divisors of N. Then

$$R_E \leq \nu(A^2 - 4B) + \nu(B) - 1.$$

1.3 2-Selmer Groups and Selmer Ranks

Computing the 2-Selmer group is another way of bounding the rank of an elliptic curve. In broad terms, a Selmer group is a group of "local" points on $E \mod p^n$, for all p prime and $n \in \mathbb{N}$ and over $\mathbb{R}$, that form a "compatible system". Expanding upon what is meant by "local" or "compatible system" or providing a more exact definition for Selmer groups is beyond the scope of this thesis. For further reading, you may refer to section 2.11 in [2].

One problem mathematicians have studied is whether, for a given equation, having everywhere local solutions, defined as having solutions $\mod p^n$ and over $\mathbb{R}$, for all p prime, $n \in \mathbb{N}$ implies that it has rational solutions. This turns out to be the case, as proven by Hasse and Minkowski, for quadratic equations. However, this implication does not hold for curves of degree three or more.

Example 1.3.1 (Selmer)**.** The curve $3x^3 + 4y^3 = 5$ has solutions $\mod p^n$ and over $\mathbb{R}$, for all p prime, $n \in \mathbb{N}$, but has no rational solutions.

To see how the Selmer group can be used to provide an upper bound on the rank of an elliptic curve, we first define the weak Mordell-Weil group as $E(\mathbb{Q})/2E(\mathbb{Q})$. Recall that this group is finite by Mazur's theorem. The following proposition relates the weak Mordell-Weil group an elliptic curve to its rank.

Proposition 1.3.2. *$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{R_{E/\mathbb{Q}}+d}$, where $d = dim_{\mathbb{Z}/2\mathbb{Z}}E(\mathbb{Q})[2]$. $E(\mathbb{Q})[2]$ is the two-torsion defined over $\mathbb{Q}$.*

In order to prove this proposition, we will need the following results.

Lemma 1.3.3. *If G is a finite abelian group of odd order, then $G/2G$ is trivial.*

Proof. Proving this lemma is equivalent to showing that if G has odd order, then $G = 2G$. Clearly $2G$ is a subgroup of G. We will now show the other inclusion. Let g be an element in G. Then by Lagrange's theorem, the order of g divides the order of G. Since G has odd order, this implies that the order of g, call it n, is also odd (since an odd number cannot have even divisors). By definition, we have that $ng = 0$ in G. This then implies that $(n+1)g = g$ and $2((\frac{n+1}{2})g) = g$ in G. Note that $\frac{n+1}{2} \in \mathbb{Z}$ since n is odd. Thus we have $g = 2h \in 2G$, where $h = (\frac{n+1}{2})g \in G$. □

Theorem 1.3.4 ([1], Section 5.2)**.** *If G is a finite abelian group, then G is a direct product of cyclic groups of order p^n where p is prime.*

Corollary 1.3.5. *If G is a finite abelian group then $G \cong G_{even} \times G_{odd}$, where G_{even} has order that is a power of 2 and G_{odd} has odd order.*

We will use these results to prove Proposition 1.3.2.

Proof of Proposition 1.3.2. We know that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E}$. Dividing both sides of this congruence by their double, we get

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) &\cong (E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E})/(2E(\mathbb{Q})_{\text{tors}} \oplus (2\mathbb{Z})^{R_E}) \\ &\cong E(\mathbb{Q})_{\text{tors}}/2E(\mathbb{Q})_{\text{tors}} \oplus (\mathbb{Z}/2\mathbb{Z})^{R_E}. \end{aligned}$$

By Corollary 1.3.5, we have that if G is a finte abelian group, then

$$\begin{aligned} G/2G &\cong G_{\text{even}} \times G_{\text{odd}}/(2G_{\text{even}} \times 2G_{\text{odd}}) \\ &\cong G_{\text{even}}/2G_{\text{even}} \times G_{\text{odd}}/2G_{\text{odd}} \\ &\cong G_{\text{even}}/2G_{\text{even}}, \end{aligned}$$

since $G_{\text{odd}}/2G_{\text{odd}}$ is trivial by Lemma 1.3.3. By the isomorphism theorem, we have that $(\mathbb{Z}/2^n\mathbb{Z})/(2\mathbb{Z}/2^n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Therefore, if $G = \mathbb{Z}/2^{n_1}\mathbb{Z} \times \mathbb{Z}/2^{n_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/2^{n_d}\mathbb{Z}$ with n_1, n_2, $\ldots n_d \geq 1$, then $G/2G \cong (\mathbb{Z}/2\mathbb{Z})^d$. So $E(\mathbb{Q})_{\text{tors}}/2E(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^d$, and thus $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{R_{E/\mathbb{Q}}+d}$. □

This next "theorem" collects some results about the 2-Selmer group and shows how it can be used to bound the rank of an elliptic curve. For a more in-depth explanation of the 2-Selmer group, refer to [2].

Theorem 1.3.6. *There is a group* $\text{Sel}_2(E/\mathbb{Q})$ *and an injection* $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \text{Sel}_2 E(/\mathbb{Q})$ *such that*

- $\text{Sel}_2(E/\mathbb{Q})$ *is finite and isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^{rank_{\mathbb{Z}/2\mathbb{Z}}Sel_2(E/\mathbb{Q})}$.
- $\text{Sel}_2(E/\mathbb{Q})$ *is explicitly computable.*
- $\text{Sel}_2(E/\mathbb{Q})$ *captures all the compatible families of everywhere local points on* E.

Definition 1.3.7. The *Shafarevich-Tate group*, or the *Sha group* (Ш) is defined by the quotient $Ш(E/\mathbb{Q})[2] := \text{Sel}_2(E/\mathbb{Q})/(E(\mathbb{Q})/2E(\mathbb{Q}))$. If the Sha is trivial, all everywhere local solutions correspond to rational points on the curve.

The weak Mordell-Weil, 2-Selmer, and Sha groups form the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \text{Sel}_2(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[2] \to 0.$$

The Sha group is a measure of the failure of the everywhere local solutions to generate global solutions. Unfortunately, just as with the rank, in most cases we are unable to compute Ш.

Define $s = \text{rank}_{\mathbb{Z}/2\mathbb{Z}} \text{Sel}_2(E/\mathbb{Q})$. We are able to compute s since $\text{Sel}_2(E/\mathbb{Q})$ is computable. The value of s bounds the rank of the elliptic curve since $R_{E/\mathbb{Q}} + d \leq s$.

Note that the value of s is at least the value of d. The 2-Selmer rank of an elliptic curve can be computed in Sage using the command

`E.selmer_rank()`.

Example 1.3.8. Recall the curve $y^2 + xy = x^3 - 1070x + 7812$ from Example 1.2.1 and Example 1.2.6. Using the command `E.selmer_rank()` in Sage, we get that the 2-Selmer rank of this elliptic curve is 2. In Example 1.2.6, we found that the torsion subgroup of this elliptic curve is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. We use this result to compute $E(\mathbb{Q})_{\text{tors}}/2E(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z})/(2(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z})) \cong (\mathbb{Z}/2\mathbb{Z})^2$, so we get $d = 2$. Using the fact that $r + d \leq s$, we can deduce that $r = 0$ since s and d are both 2. This agrees with the value we computed the rank of this curve to be in Example 1.2.6. We can then use this information to get that

$$Ш(E/\mathbb{Q})[2] := \text{Sel}_2(E/\mathbb{Q})/(E(\mathbb{Q})/2E(\mathbb{Q})) \cong (\mathbb{Z}/2\mathbb{Z})^2/(\mathbb{Z}/2\mathbb{Z})^2 \cong \{0\}.$$

In this case, we have the short exact sequence

$$0 \to (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \to 0 \to 0.$$

Example 1.3.9. In Example 1.2.7, we found that the torsion subgroup of the curve $E_1/\mathbb{Q} : y^2 + xy + y = x^3 + x^2 - 2365x + 43251$ is trivial. Using Sage, we find that the 2-Selmer rank of E_1 is 2. We can deduce that $0 \leq r \leq 2$ since we have $d = 0$ and $s = 2$. Using Sage, we compute that the rank of this elliptic curve is 2. As in

Example 1.3.8, since $r+d=s$, Ш is trivial. Again, we have the short exact sequence

$$0 \to (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \to 0 \to 0.$$

Example 1.3.10. Now consider the elliptic curve $E_2/\mathbb{Q} : y^2 = x^3 + 5x$. Using Sage, we compute that E_2 has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and that the 2-Selmer rank of E_2 is 2. From this information, we can deduce that $0 \leq r \leq 1$. It turns out that the rank of this curve is 1. We compute the Sha to be

$$Ш(E/\mathbb{Q})[2] := \text{ Sel}_2(E/\mathbb{Q})/(E(\mathbb{Q})/2E(\mathbb{Q})) \cong (\mathbb{Z}/2\mathbb{Z})^2/\{0\} \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

which gives us the short exact sequence

$$0 \to 0 \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \to (\mathbb{Z}/2\mathbb{Z})^2 \to 0.$$

In each of the three examples discussed above, the Selmer rank has been 2, but each example has had different r and d values. Note that although the curves in Examples 1.3.8 and 1.3.9 have the same short exact sequence, the power of 2 that $\mathbb{Z}/2\mathbb{Z}$ is raised to in the first component of this short exact sequence comes from the 2-torsion of the curve in Example 1.3.8 and from the rank of the curve in Example 1.3.9. The short exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

cannot occur for a curve with a Selmer rank of 2 because of a conjecture about Sha.

Conjecture 1.3.11. *The group* $Ш(E/\mathbb{Q})$ *is finite.*

A consequence of this conjecture, due to Cassels and stated here without proof, is that $|Ш(E/\mathbb{Q})[2]|$ is a square. This result then implies that if a curve has $s = 2$ and $d = 1$, as in Example 1.3.10, it must have $r = 1$. Otherwise, if it were to have $r = 0$, it would have $|Ш(E/\mathbb{Q})[2]| = 2 \neq \square$.

Chapter 2

Distribution of Selmer Ranks

In this chapter, we will discuss conjectures and results on the distribution of Selmer ranks. It would be nice to know what the possible values for $R_{E/\mathbb{Q}}$ are and how frequently each rank occurs. However, as mentioned in the previous chapter, the rank of an elliptic curve cannot always be computed and little is known about the ranks of elliptic curves. Assuming the generalized Riemann hypothesis, the largest known rank is 28.

One approach to obtaining information about the distribution of ranks is to use probabilistic arguments. We will begin by setting up some definitions and notation. Define the set of elliptic curves $\mathcal{E}$ as

$$\mathcal{E} = \{E_{A,B} : y^2 = x^3 + Ax + B, 4A^3 + 27B^2 \neq 0, \text{ if } d^4|A \text{ and } d^6|B, \text{ then } d = \pm 1\}.$$

Definition 2.0.1. The *height* of an elliptic curve $E_{A,B}$ is defined as

$$\mathrm{ht}(E_{A,B} = \max\{4|A|^3, 27B^2\}.$$

Next, we define the set $\mathcal{E}(x) = \{E \in \mathcal{E} : \mathrm{ht}(E) \leq x\}$ to denote the set of all elliptic curves of height less than or equal to x. For $d \geq 0$, we write $R_d(x) = \{E \in \mathcal{E}(x) : \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = d\}$ to represent the set of all elliptic curves of height less that or equal to x that are of rank d. Similarly, we write $S_d(x) = \{E \in \mathcal{E}(x) : \mathrm{Selrank}_{\mathbb{Z}/2\mathbb{Z}} E(\mathbb{Q}) = d\}$, where

$$\mathrm{Selrank}_{\mathbb{Z}/2\mathbb{Z}} E(\mathbb{Q}) = \dim_{\mathbb{Z}/2\mathbb{Z}} \mathrm{Sel}_2(E/\mathbb{Q}) - \dim_{\mathbb{Z}/2\mathbb{Z}} E(\mathbb{Q})[2],$$

to denote the set of elliptic curves of height less than or equal to x that have Selmer rank equal to d.

We would like to be able to compute, for any d, $\frac{\#R_d(x)}{\#\mathcal{E}(x)}$. This quantity represents the probability that an elliptic curve of height less than or equal to x has a rank of d. However, because the rank of an elliptic curve can often not be computed, we will instead work with $\frac{\#S_d(x)}{\#\mathcal{E}(x)}$. A conjecture by Poonen and Rains provides information on this value.

Conjecture 2.0.2 (Poonen, Rains, [4])**.** *The limit* $\lim_{x\to\infty} \frac{\#S_d(x)}{\#\mathcal{E}(x)}$ *exists and it equals* S_d*, where*

$$S_d = \left(\prod_{j\geq 0} \frac{1}{1+2^{-j}}\right) \cdot \left(\prod_{k=1}^{d} \frac{2}{2^k - 1}\right).$$

Approximations of the value of S_d for $d = 0 \ldots 6$ are listed in Table 2.0.1. These approximations appear in [3]. Since the conjecture by Poonen and Rains considers elliptic curves with any torsion subgroup, it is interesting to look at the distribution of Selmer ranks within families of elliptic curves that have a fixed torsion subgroup.

	Poonen and Rains	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$
S_0	0.20971122	0.147489302	0.237189597	0.250529683
S_1	0.41942244	0.34834435	0.441590611	0.452295676
S_2	0.27961496	0.310965151	0.257648765	0.246951345
S_3	0.07988998	0.145491394	0.05837446	0.04737805
S_4	0.01065199	0.039889117	0.005047811	0.002802511
S_5	0.00068722	0.006990622	0.000147933	0.0000427
S_6	0.00002181	0.000788972	0.000000822	0

TABLE 2.0.1: Percentage of Curves with a Fixed Selmer Rank by Family

Data on the distribution of Selmer ranks within a few families of elliptic curves is also displayed in Table 2.0.1. This data was collected using Magma and uses the tables in Appendix E of [2] to generate curves with specified torsion subgroups. The equation used to generate curves with torsion subgroups $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/5\mathbb{Z}$ is

$$E_{a,b} : y^2 + (1-a)xy - by = x^3 - bx^2.$$

The form of the parameters a and b for each family is displayed below, where c is a rational number.

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} : a = \frac{(2c+1)(8c^2+4c+1)}{2(4c+1)(8c^2-1)c},\ b = \frac{(2c+1)(8c^2+4c+1)}{(8c^2-1)^2}$$

$$\mathbb{Z}/4\mathbb{Z} : a = 0,\ b = c$$

$$\mathbb{Z}/5\mathbb{Z} : a = c,\ b = c$$

The code used to compute the data, included in Chapter 3, sets c equal to all rational numbers of the form $\frac{s}{t}$, where s ranges from $-x$ to x and t ranges from 1 to x. The variable x starts at 10 and is increased by 10 for each iteration of the program, up to 1000, increasing the size of the "box" of rational values being used as parameters. The

values s and t are checked to make sure that their GCD is 1 (so duplicate curves are not included twice) and c is checked to make sure its value does not cause the denominator of a or b to be zero or cause the value $4A^3 + 27B^2$ to be zero, if the curve is written in short Weierstrass form. A curve of the form $y^2 + (1-a)xy - by = x^3 - bx^2$ is then created and the minimal model of this curve is found. The program only computes the size of the Selmer group for the additional curves in each iteration. The value of $\dim_{\mathbb{Z}/2\mathbb{Z}}\mathrm{Sel}_2(E/\mathbb{Q})$ is found by taking the log base 2 of the size of the Selmer group. The program outputs the number of curves that have $\dim_{\mathbb{Z}/2\mathbb{Z}}\mathrm{Sel}_2(E/\mathbb{Q})$ equal to 0, 1, 2, . . . , 11+ in the form of a vector after each iteration of the program.

A cumulative account of the number of curves with each value of $\dim_{\mathbb{Z}/2\mathbb{Z}}\mathrm{Sel}_2(E/\mathbb{Q})$ is created by adding up the number of curves with that value in every iteration in the box with the absolute value of s and t less than or equal to x for each value of x. The number of two-torsion points is subtracted from the value $\dim_{\mathbb{Z}/2\mathbb{Z}}\mathrm{Sel}_2(E/\mathbb{Q})$ that the program outputs in order to obtain the number of curves with each Selmer rank within each window of rational parameters. The probablilty that a curve in a particular box will have a certain Selmer rank is then computed by dividing the number of curves with that rank that are in that box by the total number of curves in that box. The way these probabilities change as x increases is depicted in the graphs included below.

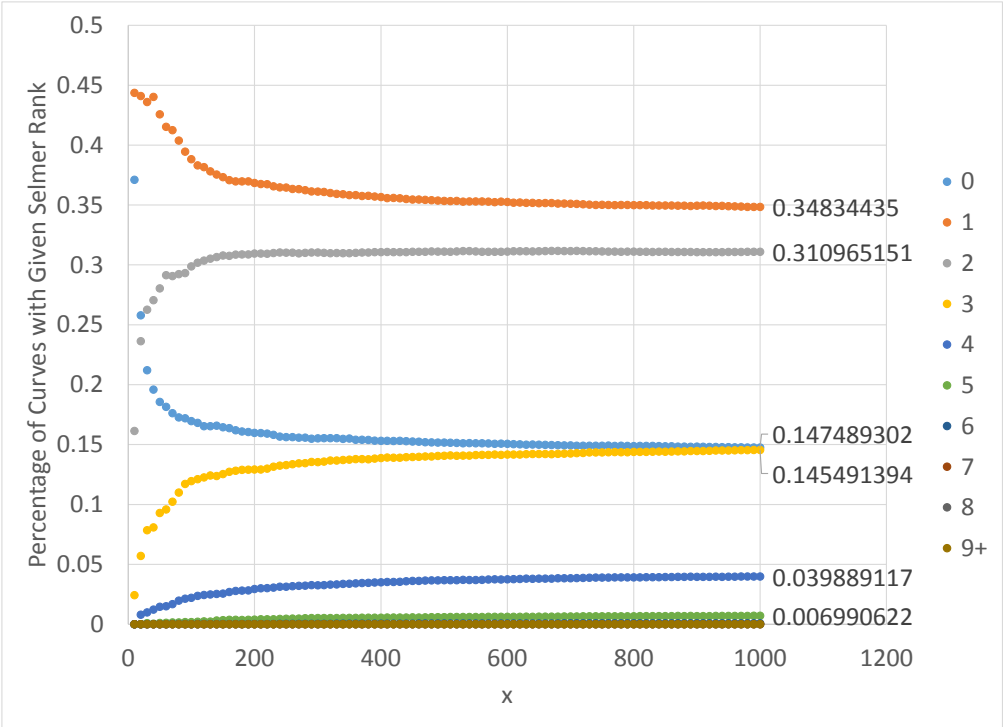

FIGURE 2.0.1: Elliptic Curves with Torsion Subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

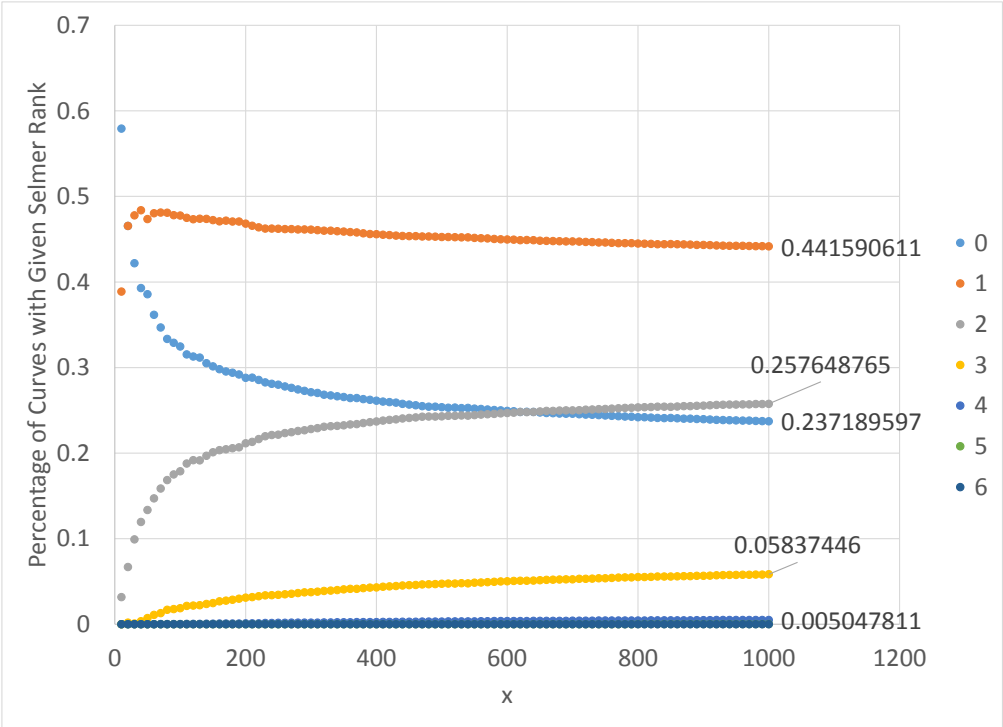

FIGURE 2.0.2: Elliptic Curves with Torsion Subgroup $\mathbb{Z}/4\mathbb{Z}$

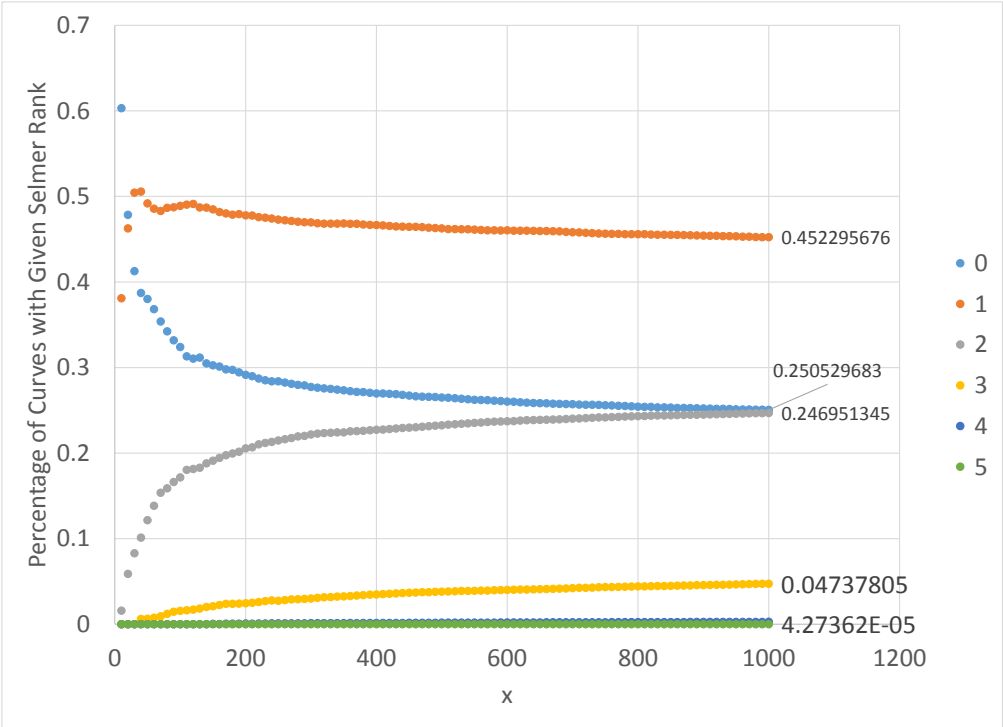

FIGURE 2.0.3: Elliptic Curves with Torsion Subgroup $\mathbb{Z}/5\mathbb{Z}$

Chapter 3

Magma Code

```
CompSize := function(t, s)
    if GCD (t,s) eq 1 then
        c:=t/s;
        if ((c ne -1/4) and (c ne -1/2)) then
            a := (2*c+1)*(8*c^2+4*c+1)/(2*(4*c+1)*(8*(c)^2-1)*(c));
            b := (2*c+1)*(8*(c)^2+4*c+1)/((8*(c)^2-1)^2);
            E := EllipticCurve([1-a,-b,-b,0,0]);
            E:= MinimalModel(E);
            S:=TwoSelmerGroup(E);
            return #S;
        else
            return 0;
        end if;
    else
```

```
            return 0;
        end if;
    end function;
    UpdateRanks := procedure( Ranks, SizeS)
        if SizeS gt 0 then
            if SizeS lt 1025 then
                Bool, a := IsCoercible(Integers(), Log(2, SizeS));
                Ranks[a+1] := Ranks[a+1] + 1;
            else
                Ranks[12] := Ranks[12] + 1;
            end if;
        end if;
    end procedure;
    ringRanks := procedure(x)
        Ranks := [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0];
        for s in [1..(x-10)] do
            for t in [(x-9)..x] do
                UpdateRanks( Ranks, CompSize(t, s));
            end for;
            for t in [(-x)..(-(x-9))] do
                UpdateRanks( Ranks, CompSize(t, s));
            end for;
        end for;
        for s in [(x-9)..x] do
            for t in [(-x)..(-1)] do
```

```
            UpdateRanks( Ranks, CompSize(t, s));
        end for;
        for t in [1..x] do
            UpdateRanks( Ranks, CompSize(t, s));
        end for;
    end for;
    print Ranks;
end procedure;
for m in [1..100] do
    print m;
    ringRanks(10*m);
end for;
```

Bibliography

[1] D. S. Dummit and R. M. Foote, "Abstract Algebra," Prentice Hall, Englewood Cliffs, N.J., 1991.

[2] Á. Lozano-Robledo. "Elliptic Curves, Modular Forms, and Their L-Functions," American Mathematical Society, 2011.

[3] Á. Lozano-Robledo, *A probabilistic model for the distribution of ranks of elliptic curves over* $\mathbb{Q}$, preprint, arXiv:1611.01999.

[4] B. Poonen, E. Rains, "Random maximal isotropic subspaces and Selmer groups", J. Amer. Math. Soc. 25 (2012), 245-269.

[5] J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.