Variations of the Taxicab Problem

Laura Mensh

B.A., Mathematics

An Undergraduate Honors Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Bachelor of Arts

at the

University of Connecticut

May 2024

APPROVAL PAGE

Variations of the Taxicab Problem

Presented by

Laura Mensh, B.A. Math

Honors Major Advisor _____
Thomas Roby

Honors Thesis Advisor _____
Álvaro Lozano-Robledo

University of Connecticut

May 2024

ACKNOWLEDGMENTS

I would like to thank all of my math professors during my time at Uconn. I learned so much from them and would not be where I am today mathematically if not for them. Specifically, I would like to thank Álvaro Lozano-Robledo, who I was lucky enough to work with throughout the entirety of writing this paper. His help was indispensable and this paper would not exist without him.

Variations of the Taxicab Problem

Laura Mensh, B.A.

University of Connecticut, May 2024

ABSTRACT

This thesis provides some background on the theory of elliptic curves in order to be able to define the rank of a curve. Chapter one focuses on providing background so that the reader can understand the results that were found about three different elliptic curves. These results include a list of ranks for each curve as well as some integer solutions. We will look more closely at a few interesting curves that have multiple solutions.

Contents

Chapter 1

Preliminaries

1.1 Introduction

Srinivasa Ramanujan was born in India in 1887. He grew up in poverty and had almost no formal training in pure mathematics. However, he was still able to make incredible contributions to the field. He died at the age of 32, and in this short time he had come up with nearly 3900 results. Ramanujan sent many of these results to other mathematicians who did not take his work seriously because they believed it to be too abstract and too novel. This led him to reach out to G. H. Hardy, a mathematician located at the University of Cambridge. Hardy convinced Ramanujan to move to Cambridge where they collaborated closely and Hardy became a mentor to Ramanujan. Hardy gave high praise to Ramanujan, he compared Ramanujan to mathematicians like Euler and Jacobi [OR98].

These two mathematicians also have a well-known anecdote about them which is where the Hardy–Ramanujan number arose. Hardy was visiting Ramanujan in the

hospital and had taken a taxicab to see him, which was numbered 1729. He mentioned that it was a boring number and therefore could be a bad omen. Ramanujan told him that it was not a boring number because it was the first integer that could be represented by two sets of two cubes.

$$x_1^3 + y_1^3 = x_2^3 + x_2^3 = 1729,$$

where $(x_1, y_1) = (1, 12)$ and $(x_2, y_2) = (9, 10)$. This kind of number is known as a *taxicab number*.

Definition 1.1.1. The n-th taxicab number $\mathrm{Ta}(n)$ is the smallest number that can be represented in n ways as a sum of positive cubes

Ramanujan and Hardy were not the first people to come up with this, but referring to these types of numbers as taxicab numbers does come from the previous anecdote. This property was known as early as 1657, F. de Bessy found the third taxicab number:

$$\begin{aligned} \mathrm{Ta}(3) &= 87539319 \\ &= 167^3 + 436^3 \\ &= 228^3 + 423^3 \\ &= 255^3 + 414^3. \end{aligned}$$

The equation that we are plugging solutions into is $x^3 + y^3 = d$. We are discussing this example because it satisfies the criteria to be an elliptic curve. This equation can be put into the projective space and then with a change of variables we get an equation of an elliptic curve in what we call Weierstrass form. We will talk more

about projective space and Weierstrass form in the following sections. Then you can find the rank of each curve in this form which tells you how many generators that elliptic curve has. You can sometimes find the integral solutions of the curves as well which are the points on the curve that are integers. Finding integral solutions of an elliptic curve is difficult even when using a program, so it is also interesting to look at the ranks to see how many generators a number has within that elliptic curve. In this paper we will also look at variations of the taxicab problem. I have taken the following variations and made a list of ranks for the rational and integer solutions of these curves:

$$y^2 - x^3 = d,$$

$$x^3 + y^3 + x^2 + y^2 = d.$$

Putting these into projective space allows us to find the rank of the rational and the number of integer solutions. It also allows us to find the values of x and y that are integers for a curve $y^2 - x^3 = d$.

1.2 Elliptic curves

Definition 1.2.1. An elliptic curve over $\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$ with at least one rational point $\mathcal{O} \in E(\mathbb{Q})$ that we call the origin.

In particular an elliptic curve can be written as the curve E in the projective plane as $F(X, Y, Z) = 0$, where F is given by

$$F(X,Y,Z) = aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+jYZ^2+kZ^3.$$

Let us go through the terms in this definition one by one starting with the projective plane. The simple way to think of the projective plane is like an ordinary plane with additional points at infinity. At these points parallel lines intersect. In order to formally define the projective plane we must first define the real projective line.

1.3 Projective Space

Definition 1.3.1. The real projective line is defined by

$$\mathbb{P}^1(\mathbb{R}) = \{[x, y] : x, y \in \mathbb{R} \text{ when } (x, y) \neq (0, 0)\}.$$

The real projective line is the set of all lines that go through the origin. We can do a decomposition of $\mathbb{P}^1(\mathbb{R})$ to get

$$\mathbb{P}^1(\mathbb{R}) = \{[x, 1] : x \in \mathbb{R}\} \cup \{[1, 0]\}.$$

We can do this because when we have the point $[x, y]$ when $y \neq 0$, we have $[\frac{x}{y}, 1]$. This means that the class of [x,y] has a unique representative of the form $[a, 1]$ for some $a = \frac{x}{y} \in \mathbb{R}$. This allows for the previous decomposition. This decomposition is important to understanding projective lines because the point $[1, 0]$ is the point on the line at infinity. As x gets larger in the point $[x, 1]$ the line that it corresponds to which goes through the origin gets closer to the point $[0, 1]$, which is the point at infinity.

We can now define the projective plane in a similar way. First let $a, b, c, x, y, z \in \mathbb{R}$ such that neither (x, y, z) or (a, b, c) are the zero vector. We define classes of similar

vectors by

$$[x, y, z] = \{(a, b, c) : a, b, c \in \mathbb{R} \text{ such that } (a, b, c) \neq \vec{0} \text{ and } (x, y, z) \sim (a, b, c)$$

So we see that $[x, y, z]$ contains all of the points in the line in $\mathbb{R}^3$ that go through the (x, y, z) and $(0, 0, 0)$ except for the origin. The projective plane is the collection of all such lines:

$$\mathbb{P}^2(\mathbb{R}) = \{[x, y, z] : x, y, x \in \mathbb{R} \text{ such that } (x, y, z) \neq (0, 0, 0)\}$$

when $z \neq 0$, $(x, y, z) \sim (\frac{x}{z}, \frac{y}{z}, 1)$. Now we can decompose $\mathbb{P}^2(\mathbb{R})$ in the same way we did it for the line and get:

$$\mathbb{P}^2(\mathbb{R}) = \{(x, y, 1) : x, y \in \mathbb{R}\} \cup \{[a, b, 0] : a, b \in \mathbb{R}\}.$$

This decomposition shows us the that projective plane is the union of the real plane $\mathbb{R}^2$, also known as the affine plane, and that the points at infinity form a projective line [L-R19, P. 415].

We will now move onto why the projective plane is important to the study of elliptic curves. In order to find points on the elliptic curve we must find a projectivization of the curve. This means putting the curve into the projective plane. We will show how to put a curve into projective space using the following curve: $ax^3 + bx^2y + cxy^2 + dy^3 + fxy + gy^2 + hx + jy + k = 0$.

Example 1.3.2. Take the curve: $ax^3+bx^2y+cxy^2+dy^3+fxy+gy^2+hx+jy+k = 0$. In order to put it into the projective plane we must find $F(X, Y, Z)$. To do this we

have to make every term have the same degree. The highest degree of this curve is 3. Therefore, the first four terms in the expression do not get multiplied by Z because they also have a degree of 3. Every other term gets multiplied by a power of Z that will make it degree 3. When we do this we get:

$$aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + jYZ^2 + kZ^3 = 0.$$

This is how we defined an elliptic curve earlier in the section.

Example 1.3.3. Let us put $x^3 + y^3 = d$ into projective space. The highest degree here is 3 and both x and y are to the power 3. So we do not add a Z to either of them. The only term that needs to be multiplied by Z is d. By doing this we get that the projectivization of the curve is

$$X^3 + Y^3 - dZ^3 = 0.$$

Let us do this for the variations of the taxicab problem.

Example 1.3.4. Take the curve $y^2 - x^3 = d$. Once again we must have every term have the same degree. So we multiply y^2 by Z, we leave x^3 and then we multiply d by Z^3 because d is a constant. This gives us:

$$Y^2Z - X^3 - dZ^3 = 0.$$

This would be the projectivization of $y^2 - x^3 = d$ curve.

Example 1.3.5. Take the curve $x^3 + y^3 + x^2 + y^2 = d$. The projectivization of this

would be:

$$X^3 + Y^3 + X^2Z + Y^2Z - dZ^3 = 0.$$

Example 1.3.6. Consider $x^2 + y^3 = d$. The projectivization of this would be

$$X^2Z + Y^3 - dZ^3 = 0.$$

1.4 Smoothness

When choosing which cubic equations to use we had to make sure that the curves were non singular, otherwise they would not be considered elliptic curves. When a curve is non-singular it is called a smooth curve. Let us define what a smooth curve is.

Definition 1.4.1. First we will define what it means for a curve to be singular. A projective curve C is singular at a point P if and only if: $\frac{\delta F}{\delta x}(P) = \frac{\delta F}{\delta y}(P) = \frac{\delta F}{\delta z}(P) = 0$. If this is not true for a point then that point is non-singular. If every point on the curve is non-singular then the curve is smooth. This definition is found as definition 15.1.7 in [L-R19].

In other words, the only point on the curve that can have the result:

$$\frac{\delta F}{\delta x}(P) = \frac{\delta F}{\delta y}(P) = \frac{\delta F}{\delta z}(P) = 0$$

is [0,0,0] for [X,Y,Z]. Let us look at an example of a curve that would not be considered smooth.

Example 1.4.2. Consider the curve $ZY^2 + Y^3 + X^3 = 0$. The partial derivatives of

the function are:

$$\frac{\delta F}{\delta X} = 3X^2, \quad \frac{\delta F}{\delta y} = 2ZY + 2Y^3, \quad \frac{\delta F}{\delta z} = Y^2.$$

For $\frac{\delta F}{\delta X}$ to equal 0, X has to equal 0. For $\frac{\delta F}{\delta z}$ to equal 0 then Y has to equal 0. When $Y = 0$ then we can plug that value into $\frac{\delta F}{\delta y} = 2ZY + 2Y^3$ to get $2Z \cdot 0 + 2 \cdot 0^3$ which gives us that $\frac{\delta F}{\delta y} = 0$ even if Z does not equal 0, this means Z can equal any number. So the point $[0, 0, 1]$ is a point where the curve is singular and therefore, the curve is not smooth and not an elliptic curve.

Let us show that the taxicab problem is a smooth curve.

Example 1.4.3. Take $X^3 + Y^3 - dZ^3 = 0$ and find the partial derivatives of the function:

$$\frac{\delta F}{\delta X} = 3X^2, \quad \frac{\delta F}{\delta Y} = 3Y^2, \quad \frac{\delta F}{\delta Z} = 3Z^2 d.$$

The only way to have each partial derivative equal 0 we have to have $X = 0, Y = 0, Z = 0$. So the point $[0, 0, 0]$ is the only singular point on the curve which implies that it is smooth since the point $[0, 0, 0]$ does not belong to the projective plane.

Now we will show that the variations of the taxicab problem are singular curves and therefore elliptic curves.

Example 1.4.4. Take the curve $Y^2Z - X^3 - dZ^3$. Now we will find the partial derivatives of X, Y, and Z:

$$\frac{\delta F}{\delta X} = 3X^2, \quad \frac{\delta F}{\delta Y} = 2YZ, \quad \frac{\delta F}{\delta Z} = Y^2 - 3dZ^2.$$

From this we can see that X has to equal 0. In order for $\frac{\delta F}{\delta Y} = 0$, Y or Z has to equal

0. Let us first say that $Y = 0$. Then we have $0^2 - 3dZ^2 = 0$ To make this true Z has to equal 0. Now let us take the other case where $Z = 0$, we have $Y^2 - 0 = 0$ then Y has to be 0 in order to get $\frac{\delta F}{\delta Z} = 0$. So we have shown that the curve is non-singular at every point.

Now we will show that the following example is also smooth.

Example 1.4.5. Take $X^3 + Y^3 + X^2Z + Y^2Z - dZ^3$ and find the partial derivatives:

$$\frac{\delta F}{\delta X} = 3X^2 + 2XZ, \quad \frac{\delta F}{\delta Y} = 3Y^2 + 2YZ, \quad \frac{\delta F}{\delta Z} = X^2 + Y^2 - 3dZ^2.$$

Using a system of equations, you can see that the only point that has

$$\frac{\delta F}{\delta X}(P) = \frac{\delta F}{\delta Y}(P) = \frac{\delta F}{\delta Z}(P) = 0$$

is [0,0,0] and therefore the curve is smooth.

Example 1.4.6. Now let us look at $X^2Z + Y^3 - dZ^3$. We will take the partial derivatives:

$$\frac{\delta F}{\delta X} = 2XZ, \quad \frac{\delta F}{\delta Y} = 3Y^2, \quad \frac{\delta F}{\delta Z} = X^2 - 3dZ^2.$$

For $\frac{\delta F}{\delta Y} = 0, Y$ has to equal 0. For $\frac{\delta F}{\delta X}, X$ or Z equals 0. When doing both of these cases for $\frac{\delta F}{\delta Z}$ the other value will also be 0. So $[0, 0, 0]$ is the only point where each partial derivative is 0 and therefore the curve is smooth.

So the variations of the taxicab that we focused on are all smooth and therefore, they are also elliptic curves. Another way to test if a curve E is smooth is when it is in the form $E : y^2 = x^3 + Ax + B$, we know that it is non-singular when $4A^3 + 27B^2 \neq 0$. In projective coordinates the curve would be given by $E : ZY^2 = X^3 + AXZ^2 + BZ^3$.

So when the curve is in this form it is simpler to check if the curve is smooth this way. The value of $4A^3+27B^2$ is related to the discriminant of E which is $-16\cdot(4A^3+27B^2)$. When the curve is in the form that E is in, it is known as the Weierstrass form. The curve being in this form makes it easier to check if it is non-singular. It is also easier to find the points on the curve. We will talk about Weierstrass form in the next section, but let us first show that one of the previous curves we discussed is non-singular using this new test.

Example 1.4.7. Take $y^2 - x^3 = d$ which we can rearrange to get $y^2 = x^3 + d$ which is now in Weirestrass form. In this case $A = 0, B = 1$. So we have

$$4 \cdot 0^3 + 27 \cdot 1^2$$

which equals 27, so it is non-zero and therefore the curve is smooth.

Now we will discuss Weierstrass equations and how to put elliptic curves into this form.

1.5 Weierstrass Equations

Let us begin with the definition.

Definition 1.5.1. An equation of the form

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

for some constants $a_i \in \mathbb{Q}$ is called a Weierstrass equation. We can reduce it to the

form

$$y^2 = x^3 + a_4x + a_6$$

when $a_1 = a_2 = a_3 = 0$ and this form is called a short Weierstrass equation (this can be done because the field of definition, $\mathbb{Q}$, is of characteristic 0).

Remark 1.5.2. We can show that any long Weierstrass equation can be reduced to a short one. This can be found in [L-R19, P. 425]. Let us start with the long form and call it C given by

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

for some constants $A_i \in \mathbb{Q}$. First we will complete the square in the variable y by adding $(\frac{a_1x+a_3}{2})^2$ on both sides:

$$\left(y + \frac{a_1x + a_3}{2}\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \left(\frac{a_1x + a_3}{2}\right).$$

Now we will do a change of variables where $u = x$ and $v = y + \frac{a_1x+a_3}{2}$. This change of variables leaves us with

$$v^2 = u^3 + au^2 + bu + c$$

for some $a, b, c \in \mathbb{Q}$. We will now do a second change of variables where $s = u + \frac{a}{3}$ and $t = v$ which brings the equation to the form:

$$t^2 = s^3 + As + B$$

for some $A, B \in \mathbb{Q}$. This is the short Weierstrass form which is what we wanted to

show.

There are a few methods that can be used to put a curve into Weierstrass form. We will use the method for smooth curves. Let us first take the taxicab problem itself.

Example 1.5.3. Take $\hat{C} : X^3 + Y^3 - dZ^3 = 0$. We know that there is a point $P = [\sqrt[3]{d}, 0, 1]$ on $\hat{C}$. The tangent line to this point would be

$$L : \sqrt[3]{d^2}X - dZ = 0$$

which is equal to $L : X - \sqrt[3]{d}Z = 0$. We can see that P is a point of triple intersection between L and $\hat{C}$ because we have the following system of equations:

$$L \cap \hat{C} = \begin{cases} X^3 + Y^3 = dZ^3 = 0 \\ X - \sqrt[3]{d}Z = 0 \end{cases}$$

and this system implies that $Y^3 = 0$. Therefore the only solution is $P = [\sqrt[3]{d}, 0, 1]$. Now we need to build an invertible matrix for a change of variables with $W = X - \sqrt[3]{d}Z$. We choose $U = X, V = Y, W = X - \sqrt[3]{d}Z$ Which makes the following matrix:

$$\begin{pmatrix} r_1 & s_1 & t_1 \\ r_2 & s_2 & t_2 \\ r & s & t \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -\sqrt[3]{d} \end{pmatrix}$$

and this matrix is invertible. The equation for $\hat{C}$ becomes:

$$\hat{C} : U^3 + V3 - d\left(\frac{1}{\sqrt[3]{d}}(U - W)\right)^3 = 0,$$

which we can simplify to get:

$$\hat{C} : U^3 + V^3 - (U - W)^3 = V^3 + 3U^2W - 3UW^2 + W^3 = 0.$$

We can take the affine chart $\{[y, -x, 1] : x, y \in \mathbb{R}\}$. So the affine equation is given by

$$3y^2 - 3y - x^3 + 1 = 0$$

which is equal to $3y^2 - 3y = x^3 - 1$. We now need to do another change of variables: $(s, t) = (x/3, y/3)$. When we do this change we get:

$$3(3t)^2 - 3(3t) = (3s)^3 - 1$$

and this simplifies to $27t^2 - 9t = 27^3 - 1$. We can divide by 27 to get $t^2 - t/s = s^3 - 1/27$ which is Weierstrass form. This can also be simplified even further to get $y^2 = x^3 - 432d^2$. This example comes from example 15.3.6 in [L-R19].

Now we will put the variations of the taxicab problem into short Weierstrass form.

Example 1.5.4. We will start with $y^2 - x^3 = d$ which is very simple. We just need to subtract x^3 from both sides to get $y^2 = x^3 + d$ which is now in short Weierstrass form.

Example 1.5.5. Now we will put $x^2 + y^3 = d$ into Weierstrass form. With this curve we can do a change of variables where $(X, Y) = (-y, x)$. This will give us $Y^2 = X^3 + d$ and this is now in Weierstrass form.

The last variation is much more difficult to transform so I used Magma [BCP97].

Example 1.5.6. For $x^3 + y^3 + x^2 + y^2 = d$, I used the following code:

```
Q<d>:=FunctionField(Rationals());

P<x,y,z>:=ProjectiveSpace(Q,2);

f:=x^3+y^3+x^2\cdot z+y^2\cdot z-d\cdot z^3;

C:=Curve(P,f);

E:=EllipticCurve(C,C![1,-1,0]);

E;

MinimalModel(E);
```

This code gives us the following Weierstrass equation:

$y^2 + 16/27 \cdot x \cdot y = x^3 + (32/27 \cdot d - 128/243) \cdot x^2 + (1024/2187 \cdot d^2 - 20480/59049 \cdot d + 32768/531441) \cdot x + (32768/531441 \cdot d^3 - 1048576/14348907 \cdot d^2 + 9961472/387420489 \cdot d - 29360128/10460353203)$.

This would have been tedious to do by hand however, Magma was able to do it very quickly.

Now that we have shown what an elliptic curve is we can begin to look at its properties.

1.6 Group Structure

As it turns out the points on elliptic curves form groups and have group structure. Let us define the addition law on points on the elliptic curve. Let E be an elliptic curve in the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. Then let P and Q be two rational points in $E(\mathbb{Q})$ and let $\lambda = \overline{PQ}$ be the line that goes through both points. If $P = Q$ then λ is the tangent line to that point. One can show that there is also

a third point of intersection R in $\lambda \cap E$ which is also defined over $\mathbb{Q}$. We can get this third point by adding P and Q because group structure guarantees that adding these two points will get a third point that is also on the curve. When we add the points P and Q we get the line that intersects the vertical line that goes through R. So we need to reflect this new point across the x-axis to get R. Knowing this we can say that $(E, +)$ is an abelian group since addition is commutative. We know that $\overline{PQ} = \overline{QP}$ because the line through these points is the same no matter which direction you go in. The identity element that is necessary for group structure is the origin. For every $P \in E(\mathbb{Q})$ there exists a point $-P$ such that $P + (-P) = \mathcal{O}$ which means every point has an inverse in the group. The addition of points is also associative, which means that we have fulfilled all of the elements needed to show that $(E, +)$ has group structure. Now that we have shown this we know that if you find one point on the curve you can use addition to find other points on the curve. There is an algorithm for the addition of points on an elliptic curve, which we will describe next. This algorithm can be found in [ST92, P. 118].

Let $E : y^2 = x^3 + AX + B$ and $P, Q \in E$.

a) if P=$\mathcal{O}$ then $P + Q = Q$,

b) if $Q = \mathcal{O}$ then $P + Q = P$,

c) if $P = (x_1, y_1), Q = (x_2, y_2)$ and if $x_1 = x_2, y_1 = -y_2$, then $P + Q = 0$. Otherwise we define $\lambda = \begin{cases} \frac{y_2 - y}{x_2 - x_1} \text{ if } P \neq Q \\ \frac{3x_1^2 + A}{2y_1} \text{ if } P = Q \end{cases}$ And let $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$. Then $P + Q = (x_3, y_3)$. Let us look at some examples

Example 1.6.1. Let $E : y^2 = x^3 + 1$. We know that the point $P = (-1, 0)$ and $Q = (0, 1)$. Now we want to find P+Q. Since these two points are different, we can

find the slope of the line that goes through them. $\lambda = \frac{1-0}{0-1} = 1$. We get

$$x_3 = 1^2 - (-1 - 0) = 2$$

and

$$y_3 = 1(-1 - 2) - 0 = -3.$$

So we have that $P + Q = (2, -3)$. We can also find 2Q for this curve. Since both points are equal to each other we use the second equation in the system. We get $\lambda = \frac{3 \cdot 0 + 0}{2 \cdot 1} = 0$ So

$$x_3 = 0 - 0 - 0 = 0$$

and

$$y_3 = 0(-1 - 0) - 1 = -1.$$

Thus, $2Q = (0, -1)$. We should also note that the point $R = (2, 3)$ is on this curve. This means that we can find $2R$, $3R$, $4R$, $5R$, $6R$ in the same way shown above. We get that $2R = (0, 1)$, $3R = (-1, 0)$, $4R = (0, -1)$, $5R = (2, -3)$, $6R = \mathcal{O}$. The reason that $6R = \mathcal{O}$ is because $6R = 5R + R$ and $5R = -R$, so we have $R - R = \mathcal{O}$. This means that R has finite order 6. Not every point on the curve has a finite order however for this curve R does.

This is an example that helps show why the Mordell–Weil theorem is true. We can see that there is a point on the curve that has finite order meaning that the group is finitely generated. The Mordell-Weil theorem states that this is true for all elliptic curves. We will now define this theorem.

Theorem 1.6.2 (The Mordell–Weil Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then,*

$E(\mathbb{Q})$ is a finitely generated abelian group. Meaning there are points $P_1, ..., P_n$ such that any point Q in $E(\mathbb{Q})$ can be expressed as a linear combination

$$Q = a_1P_1 + a_2P_2 + \cdots + a_nP_n$$

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

Using this theorem as well as the general structure theory of finitely generated abelian groups we can say that:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^{R_E}$$

where R_E is the rank of the curve. This means that $E(\mathbb{Q})$ is isomorphic to the direct sum of two abelian groups. Let us break down the right side of the equation and talk about each term. The first term is the torsion subgroup. A *torsion point* is a point such that when you multiply it by a constant you get the origin point. The torsion subgroup is the set of all the points on the curve E that have finite order. If we were looking at the curve from Example 1.6.1, one of those points would be R. The formal definition of the torsion subgroup is:

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

The second term of the sum, $\mathbb{Z}^{R_E}$, is called the free part. There are R_E copies of $\mathbb{Z}$ for some integer R_E where E is generated by R_E points of $E(\mathbb{Q})$ of infinite order. This means it is the opposite of the first summand. The number R_E will be the number of points such that $P \in E(\mathbb{Q})$ but $nP \neq \mathcal{O}$ for all non-zero $n \in \mathbb{Z}$ [L-R19, P. 445]. This

brings us to ranks.

1.7 Ranks

The rank is the amount of generators that a cubic equation has. There is no known algorithm for finding this value. However, the height of an equation can be helpful in understanding how complex the generators are. This method will not give you what the generators are specifically. Let us first define the height of a rational number.

Definition 1.7.1. Let $x = m/n$ be a rational number written in lowest terms. Then we can define the height of x to be

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

This definition is in [ST92, P. 65].

This can be used to find the height of a point $P = (x, y)$ on a curve. We define the (naive) height of a point P by $H(P) = H(x(P))$, where $H(x(P))$ is the height of the x-coordinate of P. Now we can define the canonical height of $P \in E(\mathbb{Q})$ by

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} \frac{H(2^N P)}{4^N}.$$

Serge Lang then used the idea of canonical height to conjecture that it could be used to show that there is an upper bound to what the rank could be. It is important to note that the set of all rational numbers whose height is less than some fixed number is a finite set [ST92, P. 66].

Conjecture 1.7.2. *For all $\epsilon > 0$ there is a constant C_ϵ such that there is a system of generators $\{P_i : i = 1, ..., R_E\}$ of $E(\mathbb{Q})$ whose canonical height was as follows:*

$$\hat{h}(P_i) \leq C_\epsilon \cdot |\Delta_E|^{1/2+\epsilon}$$

This previous conjecture can be found in [L-R19, P.455]. There is also a theorem for determining the upper bounds of the rank of an elliptic curve. The following theorem can be found as a proposition 1.1 in [AL-RP08].

Theorem 1.7.3. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation of the form*

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

Let R_E be the rank of $E(\mathbb{Q})$. For an integer $N \geq 1$ let $v(N)$ be the number of distinct positive prime divisors of N Then

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

More generally let $E/\mathbb{Q}$ be any elliptic curve with a non-trivial 2-torsion point and let a be the number of prime of additive bad reduction of $E/\mathbb{Q}$. Then

$$R_E \leq m + 2a - 1.$$

This is an important tool for finding out the maximum amount of generators that a curve can have. Another method that is used to find generators is descent.

1.7.1 Descent

The following theorem comes from [ST92] and is listed as theorem 3.5.

Theorem 1.7.4. *Let Γ be a commutative group, ands suppose there is a function*

$$h : \Gamma \to [0, \infty)$$

With the following three properties:

(a) For every real number M, the set $\{P \in \Gamma : h(P) \leq M\}$,

(b) for every $P_0 \in \Gamma$ there is a constant k_0 so that

$$h(P + P_0) \leq 2h(P) + k_0 \text{ for all } P \in \Gamma,$$

(c) there is a constant k so that

$$h(2P) \geq 4h(P) - k \text{ for all } P \in \Gamma.$$

Suppose further that (d) The subgroup 2Γ has finite index in Γ.

Then, Γ is finitely generated.

This theorem allows us to start with an arbitrary point on the curve and then manipulate it to descend to a smaller point. The height can be used to measure the size of the point. The repeated application of this leads to either a finite set of generating point which is what we are looking for. Or it leads to a contradiction which would mean that there are no solutions. You can use this theorem to prove

that there are a number of additional curves such that if there is a point on the curve, it comes from one of these curves. This allows you to create bounds for your specific curve by only counting the curves that are above your curve. Then you can find curves on those points. Then you "descend" from those points to find the generators of the curve that you are looking at. Magma is able to run these calculations much quicker than a person could so we used that in order to find the ranks of the different curves.

Chapter 2

Results

Now that we have explained what an elliptic curve is and how to find its rank, we can now discuss the specific variations of the taxicab problem and their ranks.

First we will start by looking at the original taxicab problem $x^3 + y^3 = d$. I was looking for two different things with this elliptic curve. There is more known about this curve when d is equal to an integer, so I looked at rational values of d. I knew that in order to see the rank of every elliptic curve. I would have to test the numbers in a box. I started with rational values of d that have a denominator $(1, 20)$ where each number is a natural number. I also chose numerators in the range $(1, 20)$ where the greatest common factor of the numerator and denominator was 1. This guaranteed that I would not test the same elliptic curve more than once. This range continued to expand until I had tested all of the numbers between 1 and 130 for both the numerator and the denominator. The following table shows the comparison between the amount of curves with rank two and rank three.

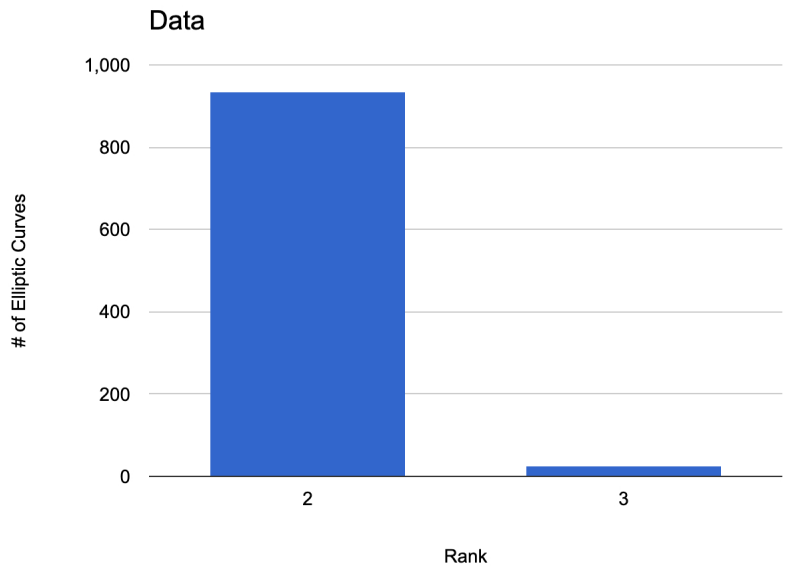

FIGURE 2.0.1: These are the results for $x^3 + y^3 = d$ where d was the set of all rational points with the numerator and denominator between 1 and 130. The graph shows that there were 936 elliptic curves with rank two and 26 curves with rank three

There were 936 elliptic curves of the form $x^3+y^3 = d$ with rank two and 26 curves with rank three. Within this range there were zero curves with rank four or higher. The rational number with the smallest height of rank two was 10/9 We can see two of these generators are $(107/171, 163/171)$ and $(289/279, -19/279)$. You can see that both of these sets of points equal 10/9 when plugged into the elliptic curve.

$$\left(\frac{107}{171}\right)^3 + \left(\frac{163}{171}\right)^3 = \left(\frac{289}{279}\right)^3 + \left(\frac{-19}{279}\right)^3 = \frac{10}{9}.$$

The smallest rational number with rank three was 51/50. This means that there are at least three solutions to the elliptic curve where $d = 51/50$. We can see that three of these generators are $(10547/10470, -1367/10470), (6823/6870, 2357/6870)$

and $(34417/46140, 39023/46140)$. When you cube each value and add the sets together you will get that they are all equal to $51/50$.

$$\left(\frac{10547}{10470}\right)^3 + \left(\frac{-1367}{10470}\right)^3 = \left(\frac{6823}{6870}\right)^3 + \left(\frac{2357}{6870}\right)^3 = \left(\frac{34417}{46140}\right)^3 + \left(\frac{39023}{46140}\right)^3 = \frac{51}{50}.$$

Another interesting result that we saw was that 1729 was not the first integer that has two generators. We discussed in the introduction that 1729 is the n-th taxicab number when $n = 2$ so finding another integer that has a similar property is interesting. The value $d = 19$ also has two generators meaning that it has at least two sets of points that both result in $d = 19$. These generators are not integers so 1729 is still the first integer solution that has two sets of points that are also integers. However, we can see that $(3, -2)$ and $(5/2, 3/2)$ are both generators of this curve and are therefore both solutions for $d = 19$. We can show this as well by plugging the points back into the equation, the first set of points is:

$$3^3 + (-2)^3 = 27 - 8 = 19.$$

The second set is:

$$\left(\frac{5}{2}\right)^3 + \left(\frac{3}{2}\right)^3 = \frac{125}{8} + \frac{27}{8} = \frac{152}{8} = 19.$$

So both rational points work for $d = 19$. The next thing I looked at was this same curve but when d was an integer. I got the following results.

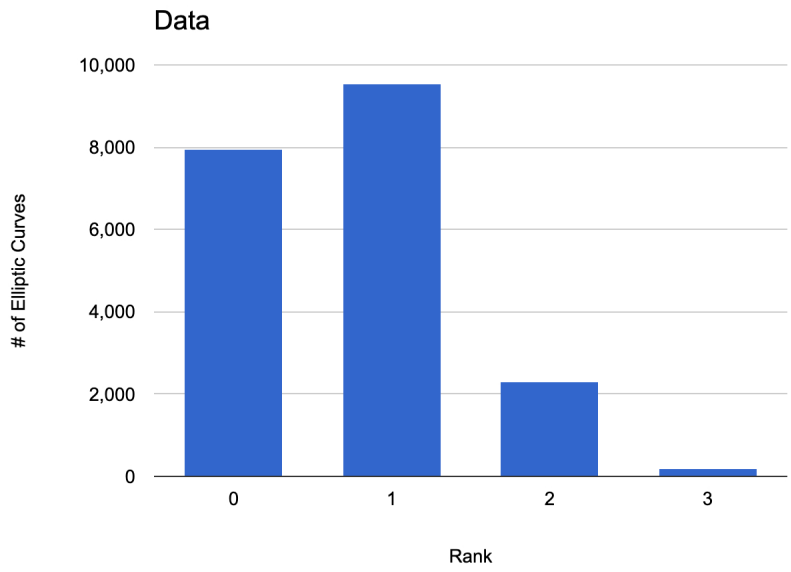

FIGURE 2.0.2: These are the results for $x^3 + y^3 = d$ where d is an integer between 1 and 20000. There were 7954 elliptic curves with rank zero, 9558 curves with rank one, 2292 curves with rank two and 196 with rank three.

I tested all of the curves where d was equal to the integers between 1 and 20000. From these results I found that here were 9558 elliptic curves with rank one, 2292 curves with rank two and 196 with rank three. The first curve that had rank one was when $d = 6$. The generator of this curve was $(17/21, 37/21)$. We can see that this works when plugged back into the curve:

$$\left(\frac{17}{21}\right)^3 + \left(\frac{37}{21}\right)^3 = 6.$$

The first curve that had rank two was when $d = 19$. Which we already showed above. The first curve with rank three was when $d = 657$. The generators of this curve are $(17/2, 7/2), (3017/481, 3574/481), (-7, 10)$. We can see that all of these have the

result $d = 657$:

$$\left(\frac{17}{2}\right)^3 + \left(\frac{7}{2}\right)^3 = \left(\frac{3017}{481}\right)^3 + \left(\frac{3574}{481}\right)^3 = (-7)^3 + (10)^3 = 657.$$

Something interesting to note is that $d = 1729$ is only rank one. This is interesting because that means that curves that are rank one can still have multiple solutions, having rank two just guarantees that there are at least two different solutions. We also saw that there are 197 elliptic curves that have rank two before the curve where $d = 1729$, which means that there are at least 197 other integers that can also be represented in two ways.

Let us move on to the first variation of the taxicab problem: $x^3 + y^3 + x^2 + y^2 = d$.

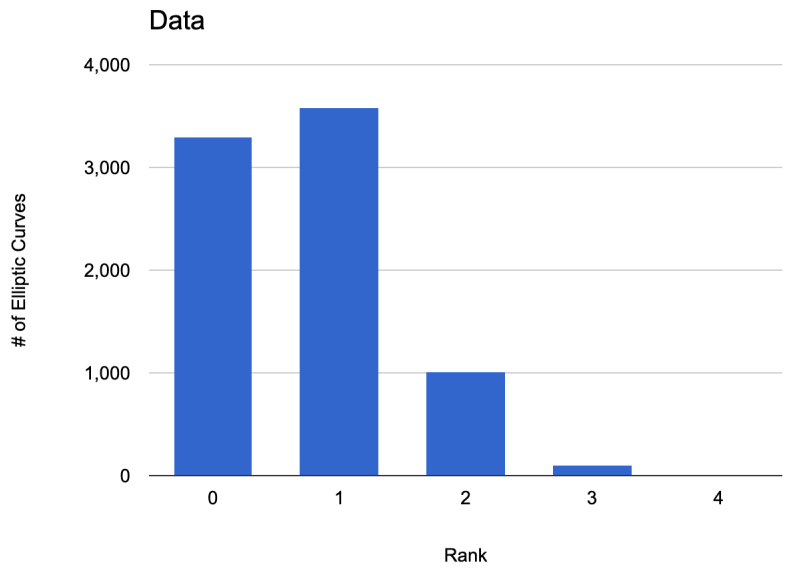

FIGURE 2.0.3: These are the results for the graph $x^3 + y^3 + x^2 + y^2$ when d was equal to the integers in the range $[1, 8000]$. It shows that there were 3297 elliptic curves with rank zero, 3587 curves with rank one, 1014 curves with rank two, 100 curves with rank three, and 2 curves with rank four.

When looking at this curve we tested for the rank for the integer values of d in the range $[1, 8000]$ We found that there were 3587 curves with a rank equal to one, 1014 curves with rank equal to two, 100 curves with rank equal to three, and 2 curves with rank equal to four. Testing this variation took a lot longer than the previous curve which is why less values of d were tested. The first curve that had a rank of 1 was when $d = 2$. The generator of this curve is $(1, 0)$ which is not a very interesting result. When you plug it back into the curve you get:

$$x^3 + y^3 + x^2 + y^2 = 1^3 + 0^3 + 1^2 + 0^2 = 2.$$

The first curve that had rank equal to two was when $d = 14$. The two generators for this curve are $(1, 2)$ and $(-7/9, 19/9)$. We can show that they both result in $d = 14$:

$$1^3 + 2^3 + 1^2 + 2^2 = 14 = \left(\frac{-7}{9}\right)^3 + \left(\frac{19}{9}\right)^3 + \left(\frac{-7}{9}\right)^2 + \left(\frac{19}{9}\right)^2.$$

The first curve that had a rank of three was when $d = 197$. The generators of this curve are $(-252/52, 329/52), (1/2, 11/2), (66119/9422, -58227/9422)$. We can see that these are all equal to each other:

$$\left(\frac{-252}{52}\right)^3 + \left(\frac{329}{52}\right)^3 + \left(\frac{-252}{52}\right)^2 + \left(\frac{329}{52}\right)^2 = \left(\frac{1}{2}\right)^3 + \left(\frac{11}{2}\right)^3 + \left(\frac{1}{2}\right)^2 + \left(\frac{11}{2}\right)^2$$

$$= \left(\frac{66119}{9422}\right)^3 + \left(\frac{-58227}{9422}\right)^3 + \left(\frac{66119}{9422}\right)^2 + \left(\frac{-58227}{9422}\right)^2 = 197.$$

The first curve that had a rank equal to four was when $d = 4282$. The generators of

this curve are

$$(145/9, -52/9), (199/31, 481/31), (3931/247, -434/247), (2320/157, 1429/157).$$

We can show that all of these generators result in $d = 4282$. First take $(145/9, -52/9)$:

$$\left(\frac{145}{9}\right)^3 + \left(\frac{-52}{9}\right)^3 + \left(\frac{145}{9}\right)^2 + \left(\frac{-52}{9}\right)^2 = 4282.$$

Now take $(199/31, 481/31)$:

$$\left(\frac{199}{31}\right)^3 + \left(\frac{481}{31}\right)^3 + \left(\frac{199}{31}\right)^2 + \left(\frac{481}{31}\right)^2 = 4282.$$

Now take $(3931/247, -434/247)$:

$$\left(\frac{3931}{247}\right)^3 + \left(\frac{-434}{247}\right)^3 + \left(\frac{3931}{247}\right)^2 + \left(\frac{-434}{31}\right)^2 = 4282.$$

Lastly take $(2320/157, 1429/157)$:

$$\left(\frac{2320}{157}\right)^3 + \left(\frac{1429}{157}\right)^3 + \left(\frac{2320}{157}\right)^2 + \left(\frac{1429}{157}\right)^2 = 4282.$$

So we have shown that all four generators get a result of 4282. Having four different solutions to one equation is an interesting result especially because two of them are positive solutions. You can find more solutions as well, we just know that there are at least four.

We are now going to move onto the last curve $y^2 - x^3 = d$. For this curve we were able to gather both the ranks of each curve as well as the integer solutions to

each curve. In Magma there is a code that will find the integer solutions on a curve in Weierstrass form. We were able to get the integer solutions to this curve because it is already in Weierstrass form so we did not need to map it to a different curve first. With the other two curves we had to do a change of variables in order to put it into Weierstrass form so when the integer solutions are mapped back to the original equation, it is unlikely that they would still be integers. Now, let us first look at the distribution of ranks on this curve.

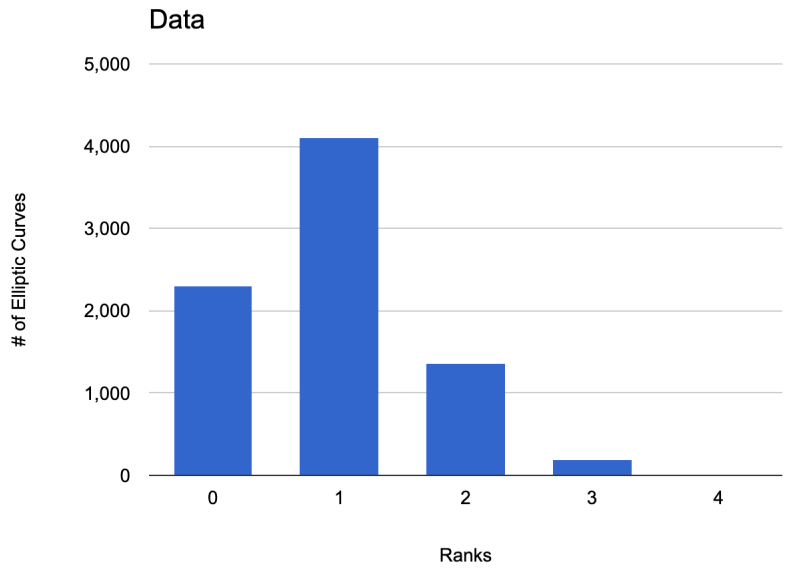

FIGURE 2.0.4: These are the results for the graph $y^2 - x^3 = d$ when d was equal to the integers in the range $[1, 8000]$. It shows that there were 2312 curves with a rank of zero. 4108 elliptic curves with a rank of one, 1365 curves with a rank of two, 192 curves with a rank of three, and 7 curves with a rank of four.

The first curve that has a rank equal to one is when $d = 2$. The generator of this curve is $(-1, 1)$ which we can plug into the elliptic curve to see that this solution works: $1^2 - (-1)^3 = 2$. The first curve that has a rank equal to two is when $d = 15$. This curve has rank two and two integer solutions however they only share one of

these solutions in common. The integer solutions are $(1, 4)$ and $(109, 1138)$ whereas the generators are $(1, 4)$ and $(1/4, 31/8)$. We can see that these solutions work when plugged back in. We have

$$4^2 - 1^3 = 1138^2 - 109^3 = \left(\frac{31}{8}\right)^2 - \left(\frac{31}{8}\right)^3 = 15.$$

The first curve with a rank of three was when $d = 113$. The generators of this curve are $(2, 11), (8, 25),$ and $(11, 38)$. We can see that all of these are equal to 113.

$$11^2 - 2^3 = 25^2 - 8^3 = 38^2 - 11^3 = 113.$$

These are also all integer solutions of the curve. There are an additional three integer solutions to this curve, meaning that the curve has six integer solutions. These are: $(-4, 7), (2, 11), (8, 25), (11, 38), (26, 133)$ and $(422, 8669)$. The first curve with a rank of four was when $d = 2089$. This curve had 14 different integer solutions. The generators of this curve are: $(3, 46), (8, 51), (-4, 45)$, and $(18, 89)$. We can see that these all get a solution of $d = 2089$.

$$46^2 - 3^3 = 51^2 - 8^3 = 45^2 - (-4)^3 = 89^2 - 18^3 = 2089.$$

The 14 integer solutions of this curve are: $(-12, 19), (-10, 33), (-4, 45), (3, 46),$ $(8, 51), (18, 89), (60, 467), (71, 600), (80, 717), (170, 2217), (183, 2476), (698, 18441),$ $(9278, 893679)$ and $(129968, 46854861)$. We can see here that having a higher rank can indicate that there will be more integer solutions. This now moves us onto the amount of integer solutions each curve has. When testing the curves we were only interested in the curves that had two or more integer solutions, so there is no data

for which curves have only one integer solution or none at all.

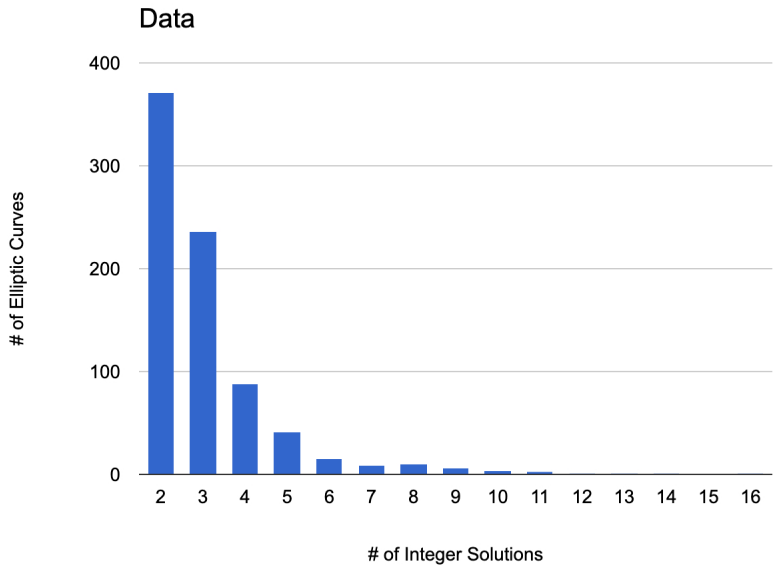

FIGURE 2.0.5: These are the integer results for the curve $y^2 - x^3 = d$ for values of d=[1,8000]. This shows that there were 372 curves with 2 integer solutions, 236 curves with 3 integer solutions, 88 curves with 4 integer solutions, 42 curves with 5 integer solution,. 16 curves with 6 integer solutions, 9 curves with 7 integer solutions, 10 curves with 8 integer solutions, 6 curves with 9 integer solutions, 4 curves with 10 integer solutions, 3 curves with 11 integer solutions, 1 curve with 12 integer solutions, 1 curve with 13 integer solutions, 1 curve with 14 integer solutions, 0 curves with 15 integer solutions, and 1 curve with 16 integer solutions.

This curve was tested for values of d in the range $[1, 8000]$ and it had the following results: 372 curves with 2 integer solutions, 236 curves with 3 integer solutions, 88 curves with 4 integer solutions, 42 curves with 5 integer solution, 16 curves with 6 integer solutions, 9 curves with 7 integer solutions, 10 curves with 8 integer solutions, 6 curves with 9 integer solutions, 4 curves with 10 integer solutions, 3 curves with 11 integer solutions, 1 curve with 12 integer solutions, 1 curve with 13 integer solutions, 1 curve with 14 integer solutions, 0 curves with 15 integer solutions, and 1 curve

with 16 integer solutions. We can now look at the rank of the curves that had 10 or more integer solutions. The curves that had 10 integer solutions were when $d = 2817, 4112, 4312, 5841$. We also found out the rank of each of these curves which can be represented as (I, r) where I is the integer and r is the rank. For the curves with 10 integer solutions we have $(2817, 3), (4112, 3), (4312, 3), (5841, 3)$. The curves that had 11 integer solutions were $d = 1737, 3025, 7057$ and the ranks were as follows: $(1737, 3), (3025, 2), (7057, 4)$. The curve that had 12 integer solutions was $d = 4481$ and it had a rank of four. The curve that had 13 integer solutions was $d = 225$ and it had a rank of two. The curve that had 14 integer solutions was $d = 2089$ and it had a rank of four. Finally the curve that had 16 integer solutions was $d = 1025$ and it had a rank of three. Let us now look more closely at the curve that has 16 integer solutions. This is the curve $y^2 - x^2 = 1025$. The 16 integer solutions of this curve are

$$(-10, 5), (-5, 30), (-4, 31), (-1, 32), (4, 33), (10, 45), (20, -95), (40, 255), (50, 355),$$
$$(64, 513), (155, 1930), (166, 2139), (446, 9419), (920, 27905), (3631, 218796), (3730, 227805).$$

Another interesting aspect to look at is how many integer solutions the curves of rank four had. You would expect them to be high especially because 3 of the curves that had a large amount of integer solutions had a rank of four. However, this is nor necessarily the case. There were 7 curves that had a rank of four. 3 of these curves are the ones listed above, 2089 with 14 integer solutions, 4481 with 12 integer solutions, and 7057 with 11 integer solutions. The 4 other curves with a rank of four were $d = 3391$ which had 3 integer solutions, $d = 4910$ which had 3 integer solutions, $d = 6856$ which had 6 integer solutions, and $d = 7954$ which had 3 integer solutions. That means that a rank cannot necessarily predict how many integer solutions a curve will have. From the data we have it is possible that having a rank of four for this

curve will guarantee that there will be multiple integer solutions. However, 7 curves having this property is not nearly enough to be able to say this. We have now seen curves that have many integer solutions that have a rank of two as well as curves with rank four that do not have that many integer solutions.

In synopsis, we have been able to gather a large list of ranks for each of these curves, we have gathered integer solutions for $y^2 = x^3 + d$, and we have looked closely at interesting curves.

Chapter 3

Appendix

I used the following code in Magma to gather the results listed in this paper. To find the ranks of the rational solutions of $x^3 + y^3 = d$ I use:

```
Rats:=<>;
for n in [1..130] do
   for d in [1..130] do
      if (GCD(d,n) eq 1) and (n ne 0) then
         t:=n/d;
         P<X,Y,Z>:=ProjectiveSpace(Rationals(),2);
         f:=X^3+Y^3-t*Z^3;
         C:=Curve(P,f);
         E,mappy2:=EllipticCurve(C,C![1,-1,0]);
         r:=Rank(E);
         gens:=Generators(E);
```

```
            if r ge 2 then
                Rats:=Append(Rats,<t,r>);
            end if;
        end if;
    end for;
end for;
Rats;
```

To find the ranks of the integer solutions of $x^3 + y^3 = d$ I used:

```
for n in [1..N] do
        t:=n;
        P<X,Y,Z>:=ProjectiveSpace(Rationals(),2);
        f:=X^3+Y^3-t*Z^3;
        C:=Curve(P,f);
        E,mappy2:=EllipticCurve(C,C![1,-1,0]);
        r:=Rank(E);
        if r ge 1 then
            print t;
            print r;
        end if;
end for;
```

To find the ranks of $x^3 + y^3 + x^2 + y^2 = d$ I used the following code:

```
SetClassGroupBounds("GRH");
for n in [1..3000] do
```

```
    t:=n;
    P<X,Y,Z>:=ProjectiveSpace(Rationals(),2);
    f:=X^3+Y^3+Z*(X^2+Y^2)-t*Z^3;
    C:=Curve(P,f);
    E,mappy2:=EllipticCurve(C,C![1,-1,0]);
    r:=Rank(E);
    if r ge 1 then
        print t;
    end if;
end for;
```

To find the ranks of $y^2 = x^3 - d$ I used the code:

```
for d:=1 to N do
    E:=EllipticCurve([0,d]);
    r:=Rank(E);
    if r ge 1 then
        print r;
    end if;
end for;
```

To find the generators of each of these curves I used variations of the following code:

```
P<X,Y,Z>:=ProjectiveSpace(Rationals(),2);
d:=_;
f:=_;
```

```
C:=Curve(P,f);
E,mappy1:=EllipticCurve(C,C![_,_,_]);
E2,mappy2:=MinimalModel(E);
G:=Generators(E2);
P:=G[1]; Q:=G[2]; R:=G[3]; S:=G[4];
Inverse(mappy1)(Inverse(mappy2)(P));
Inverse(mappy1)(Inverse(mappy2)(Q));
Inverse(mappy1)(Inverse(mappy2)(R));
Inverse(mappy1)(Inverse(mappy2)(S));
```

I plugged in the d value that I wanted to find the generators for. Then I put in the equation of the curve on the next line. For `$(C,C![_,_,_])$` I put in a point on the curve. Then depending on the rank of the curve I chose the amount of generators to map back to the curve.

Lastly to find the integer points on the curve $y^2 = x^3 + d$ I used the following code:

```
for d:=1 to 100 do
     E:=EllipticCurve([0,d]);
     I:=IntegralPoints(E);
     if #I gt 1 then
         print d, I;
     end if;
end for;
```

Bibliography

[AL-RP08] J. Aguirre, Á. Lozano-Robledo, and J. C. Peral. *Elliptic Curves of maximal rank,* Proceedings of the "Segundas Jornadas de Teoría de Números", Bibl. Rev. Mat. Iberoamerican, Rev. Mat. Iberoamericana, Madrid, 2008, pp1-28.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.

[L-R19] Á. Lozano-Robledo, *Number Theory and Geometry An Introduction to Arithmetic Geometry*, American Mathematical Society, 2019

[OR98] J. J. O'Connor, E. F. Robertson. "Srinivasa Ramanujan - Biography." Mac Tutor, School of Mathematics and Statistics University of St Andrews, Scotland, June 1998, mathshistory.st-andrews.ac.uk/Biographies/Ramanujan/.

[ST92] J. H. Silverman, J. T. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.