Spring 2011

Elliptic Curves: Minimally Spanning Prime Fields and Supersingularity

Travis McGrath
Bard College, tm996@bard.edu

Elliptic Curves: Minimally Spanning Prime Fields and Supersingularity

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Travis McGrath

Annandale-on-Hudson, New York
May, 2011

Abstract

Elliptic curves are cubic curves that have been studied throughout history. From Diophantus of Alexandria to modern-day cryptography, Elliptic Curves have been a central focus of mathematics. This project explores certain geometric properties of elliptic curves defined over finite fields.

Fix a finite field. This project starts by demonstrating that given enough elliptic curves, their union will contain every point in the affine plane. We then find the fewest curves possible such that their union still contains all these points. Using some of the tools discussed in solving this problem, we then explore what can be said about the number of solutions for a particular class of elliptic curves.

Contents

Dedication

Dedicated affectionally to my "olds," George Jolly and Caroline Seligman, for taking me into their home and bringing me into their family.

Acknowledgments

It would be impossible to list here everyone to who has helped shaped such a wonderful experience at Bard. So keeping this in mind I'd like to give thanks to LJ, Duke, Elieen, Clark, Che, V, Lolo, Josh, Claire, Kye, and Jasper, for their friendship and support.

To Ariana, Akima, Jen, Paul, Susanna, Jim, Janet, Kathy, Mary, Greg, Kate and Priscilla for their seemingly endless advice and willingness to listen.

To John, Greg, Jim & Maria, Sam, Mary, Lauren, Ethan, Bob, Becky, Keith, Amy, Melanie, Liz, Hap, Nicola, Julianne and Susan for being inspirational professors each pushing me to find something more not only in the material but within myself.

And of course to my family back north: George, Caroline, Bob, Elaine, Izzy, Joe, Susan, Rachel, Leonard, Jenny, Chris, Leah, Bear and Tom.

I'd also like to acknowledge Maka Geller who in memory continues to inspire kindness, curiosity and adventure.

1
Introduction

1.1 Mathematical Importance and Practical Application of Elliptic Curves

Though we will soon define an elliptic curve as a solution set to an algebraic equation, elliptic curves can also be seen graphically and in the 19^{th} century were shown to also be able to be made into groups. Because of their inherent group structure, elliptic curves often allow conjectures that seem to be arithmetic in nature to be answered with algebra or number theory. For this reason elliptic curves appear all over various areas of mathematics. Perhaps the most famous example of this is Andrew Wiles' proof of Fermat's Last Theorem in which elliptic curves played a central role. Elliptic curves are also used by mathematicians for Integer factorization, testing primality.

In terms of practical application, elliptic curves are utilized in cryptography. Elliptic Curve Cryptography (ECC) is a public key system and is believed to be as unbreakable as RSA, the current standard for most secure information. The advantage to ECC is that it can be implemented with a small group of curves requiring less storage and transmission.

Elliptic curves also allow for digital signatures and identification. In 2005 the United States National Security Agency moved much of its protection to Elliptic Curve Cryptography.

1.2 Overview of The Project

This project started when John introduced me to elliptic curves. Elliptic curves are defined by two constants a and b and can be viewed over any field. John's suggestion was to graph a fixed elliptic curve for various prime fields. The goal he had in mind was to see if for certain primes, points on this fixed curve clustered in some particular region. Following this advice I started graphing curves for various primes using the computer language SAGE. While looking at graphs I started to be curious about how it might look if different curves were graphed over the same prime field. This lead to an interesting discovery which became the focus of the project.

In Chapter 2 we will give a basic definition and establish several properties of elliptic curves modulo prime fields that will be used throughout the project. Chapter 3 describes the previously mentioned graphic discovery and poses the question that the rest of the project attempts to solve. In Chapter4 we use SAGE to gather data and estimate a solution. Chapter 5 utilizes tools from number theory including quadratic reciprocity to provide an actual solution. From this solution another interesting fact arises with regard to the number of solutions an elliptic curve has. In Chapter 6 this fact is proven using both number theory and traditional calculus for a specific elliptic curve. Chapter 7 attempts to make the same proofs as the previous chapter but generalized to a specific class of curves. Chapter 9 demonstrates data for brute force proofs and 8 provides the SAGE code for earlier estimates.

2
Background

2.1 Definition of Elliptic Curves and Prime Fields

To begin with we must define an elliptic curve. For more details and a less simplified formula, see chapter III of "The Arithmetic of Elliptic Curves" by Joseph H. Silverman. [1]

Definition 2.1.1. Let $\mathbb{F}$ be a field and let $a, b \in \mathbb{F}$ such that $4a^3 + 27b^2 \neq 0$. An elliptic curve $E(\mathbb{F})$ is the set $\{(x, y) \in \mathbb{F} \times \mathbb{F} : y^2 = x^3 + ax + b\}$.

We will refer to $4a^3+27b^2 \neq 0$ as the discriminant test. This test ensures that x^3+ax+b has no repeated roots. Since a, b can be elements of any field we will look specifically at the field $\mathbb{F}_p$, that is, the field $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number. We will use the notation $E(\mathbb{F}_p)$ to denote the solutions to $y^2 = x^3+ax+b$, which also specifies which prime field we are using. We may also use the notation $E_{a,b}$ with the understanding that we are referring to the prime field $\mathbb{F}_p$ because $a, b \in \mathbb{F}_p$.

With this choice of field we must alter our definition slightly for $p = 2$ and $p = 3$. The altered definitions are as follows:

Definition 2.1.2. An elliptic curve $E(\mathbb{F}_2)$ is either the set $\{(x,y) \in \mathbb{F}_2 \times \mathbb{F}_2 : y^2 + xy = x^3 + ax + b \text{ and } b \neq 0\}$ or the set $\{(x,y) \in \mathbb{F}_2 \times \mathbb{F}_2 : y^2 + ay = x^3 + bx + c \text{ and } a \neq 0\}$ for $a, b, c \in \mathbb{F}_2$.

Definition 2.1.3. An elliptic curve $E(\mathbb{F}_3)$ is either the set $\{(x,y) \in \mathbb{F}_3 \times \mathbb{F}_3 : y^2 = x^3 + ax^2 + b \text{ and } ab \neq 0\}$ or the set $\{(x,y) \in \mathbb{F}_3 \times \mathbb{F}_3 : y^2 + ay = x^3 + ax + b \text{ and } a \neq 0\}$ for $a, b \in \mathbb{F}_3$.

The majority of this project will focus on primes greater than three so these altered definitions will only be used in a few instances.

2.2 Properties of Elliptic Curves

2.2.1 Number of Elliptic Curves mod p

This section will demonstrate that for each prime $p \geq 5$ there are $p^2 - p$ elliptic curves defined over $\mathbb{F}_p$. To do this first we define $\mathbb{F}_p^\times$ to be the units of $\mathbb{F}_p$ which are simply $\mathbb{F}_p - \{0\}$. It is a theorem of abstract algebra that $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$.

Lemma 2.2.1. *There are p solutions to the equation $4a^3 + 27b^2 = 0 \mod p$.*

Proof. If one of $a, b = 0$ and $4a^3 + 27b^2 = 0 \mod p$, then both $a, b = 0$. Thus we see that there is one solution at $a = 0$, $b = 0$ and can assume $a, b \neq 0$.

Suppose $a, b \in \mathbb{F}_p^\times$. By simple algebraic manipulation it is clear that $4a^3 + 27b^2 = 0 \mod p$ is equivalent to the statement $b^2 = \frac{-4a^3}{27}$. We can divide by 27 safely because $p \neq 3$. So the number of solutions will be how many times $\frac{-4a^3}{27}$ is a perfect square. But because $b^2 = (-b)^2$ we get two choices of b for each time $\frac{-4a^3}{27}$ is a square. So it will suffice to show that $\frac{-4a^3}{27}$ is a square for $\frac{p-1}{2}$ distinct choices of a, non of which are the additive inverse of each other.

Let $C : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ defined by $C(a) = a^3$. It is easy to see that C is a homomorphism.

Case 1: Suppose $p \equiv 2 \mod 3$. Then $p-1 = 1 \mod 3$. Let α be a generator of $\mathbb{F}_p^\times$. Then $1 = \alpha^{p-1}$. Because $(p-1) \nmid 3$ there is no $n > 0$ such that $\alpha^{n^3} = \alpha^{p-1}$. So $|\ker C| = 1$. So the image of C is $\mathbb{F}_p^\times$. But because the elements of $\mathbb{F}_p^\times$ can be expressed as consecutive powers of α. This can be seen as $\{\alpha, \alpha^2, \alpha^3, \alpha^4 \dots\}$ or equivalently. $\{\alpha, (\alpha)^2, \alpha^3, (\alpha^2)^2 \dots\}$. From this it is easy to see that half of the group are squares. So the number of squares is $\frac{p-1}{2}$.

Case 2: Suppose $p \equiv 1 \mod 3$. Then $p-1 \equiv 0 \mod 3$. Let α be a generator of $\mathbb{F}_p^\times$. Then $1 = \alpha^{p-1}$. Because $p-1 \mid 3$ there exist n such that $\alpha^{n^3} = \alpha^{p-1}$. In fact there are exactly three n which can be written as $0, \frac{p-1}{3}, \frac{2(p-1)}{3}$. So $|\ker C| = 3$. So $|\operatorname{im} C| = \frac{p-1}{3}$. But because the image is a subgroup of $\mathbb{F}_p^\times$, it is cyclic, and can be expressed as consecutive powers of some δ so we know that half of these elements are squares. So the number of squares is $\frac{p-1}{6}$. Each one of these squares can be expressed as δ^n where $n \mid 3$. Then $\frac{n}{3}, \frac{n}{3} + \frac{p-1}{3}, \frac{n}{3} + \frac{2(p-1)}{3}$. all cube to n. So there are three choices of a such that a^3 is a square. Thus the number of squares is $\frac{p-1}{2}$.

It is clear that that if $a \neq b$ then $\frac{-4a^3}{27} \neq \frac{-4b^3}{27}$. Thus $\frac{-4a^3}{27}$ is a square $\frac{p-1}{2}$ times. □

This proof tells us how many curves there can be for a given $\mathbb{F}_p$. This knowledge is essential in order to state main problem of this project.

Theorem 2.2.2. *The number of $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ such that $y^2 = x^3 + ax + b$ is an elliptic curve is $p^2 - p$.*

Proof. There are p choices for a and p choices for b. So there are p^2 choices for (a, b). By Lemma 2.2.1 there are p solutions to the equation $4a^3 + 27b^2 = 0 \mod p$, which means p curves fail the discriminant test. Thus there are $p^2 - p$ choices of (a, b) that produce elliptic curves. □

2.3 Number of Solutions For a Curve mod p

Let E be defined over $\mathbb{F}_p$. Then by Hasse's theorem the number of solutions of $E(\mathbb{F}_p)$ is an integer given by the formula: $|E(\mathbb{F}_p)| = p - a_p$ where a_p is in the range $-2\sqrt{p} < a_p < 2\sqrt{p}$.[2, Chapter V, Page 132]

Lemma 2.3.1. *Let $p > 7$ and let E be an elliptic curve over $\mathbb{F}_p$, then $|E(\mathbb{F}_p)| \geq 2$.*

For this proof we will look at the minimum value of number of solutions $p - 2\sqrt{p}$.

Proof. Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined by $f(x) = x - 2\sqrt{x}$. Taking the derivative $f'(x) = 1 - \frac{1}{\sqrt{x}}$ we see that if $x > 1$ then f is always increasing. Also $f(11) > 3$. So for $x \geq 11, f(x) > 3$. So for every $p \geq 11$ there are more than two solutions. Since every prime greater than 11 is also greater than 7 it is clear that our lemma holds. □

2.4 Equivalence of Elliptic Curves

We will now define what it means for two elliptic curves to be equivalent.

Definition 2.4.1. Let E_1, E_2 defined by the equations $y^2 = x^3 + a_1x + b_1$ and $y^2 = x^3 + a_2x + b_2$, respectively, be elliptic curves. Then E_1 and E_2 are equivalent if they have the same solution set, i.e. $E_1(\mathbb{F}_p) = E_2(\mathbb{F}_p)$ as sets.

We will use the notation $\sim$ to mean equivalence. It is very easy to see that if $a_1 = a_2$ and $b_1 = b_2$ then the curves E_1, E_2 are equivalent. However we will prove that if $a_1 \neq a_2$ or $b_1 \neq b_2$ then $E_1 \nsim E_2$. By contrapositive we can state the theorem as follows.

Theorem 2.4.2. *If $E_1 \sim E_2$ then $a_1 = a_2$ and $b_1 = b_2$.*

Proof. Let $p \geq 3$ and let $E_1 \sim E_2$. Suppose $(x_o, y_o) \in E_1, E_2$ and $(x_\alpha, y_\alpha) \in E_1, E_2$ such that $x_o \neq x_\alpha$. By lemma 2.3.1 we know that two such points must exist for $p \geq 11$. For $p = 5$ or 7 this Theorem is easily proven by brute force as you can see in Section

9.1. Then $y_o^2 = x_o^3 + a_1 x_o + b_1$, $y_o^2 = x_o^3 + a_2 x_o + b_2$ and similarly $y_\alpha^2 = x_\alpha^3 + a_1 x_\alpha + b_1$, $y_\alpha^2 = x_\alpha^3 + a_2 x_\alpha + b_2$. Taking the difference of each pair of equations we see that

$$a_1 = (y_o^2 - y_\alpha^2 - x_o^3 + x_\alpha^3)(x_o - x_\alpha)^{-1} = a_2$$

So it is easy then to see that

$$b_1 = y_o^2 - x_o^3 - a_1 x_o = b_2$$

Thus $a_1 = a_2$ and $b_1 = b_2$. □

This proof reveals more than just equivalence of elliptic curves. From it we see that two elliptic curves with distinct a, b values can have at most two points as common solutions. These shared points will be of the form $(x_o, y_o), (x_o, -y_o)$. This result will be particularly important in Section 3.3.

2.5 Intersection of Elliptic Curves

When two elliptic curves do not have equivalent a's and/or b's, we can show some facts with regard to how many common solutions the two curves have.

Theorem 2.5.1. *If $a_1 = a_2$ and $b_1 \neq b_2$ then E_1, E_2 have no common solutions.*

Proof. Let $a_1 = a_2$ and $b_1 \neq b_2$. Let $(x_o, y_o) \in E_1$ and assume $(x_o, y_o) \in E_2$. Then $y_o^2 = x_o^3 + a_1 x_o + b_1$, and $y_o^2 = x_o^3 + a_2 x_o + b_2$. We can solve for the b_i's and see that $b_1 = y_o^2 - x_o^3 - a_1 x_o = y_o^2 - x_o^3 - a_2 x_o = b_2$. This is a contradiction so we see that no such (x_o, y_o) can exist. □

We can also learn something interesting when $a_1 \neq a_2$ and $b_1 = b_2$. In terms of equivalence, the properties we can prove depend on whether b_1 is a perfect square or not.

Theorem 2.5.2. *Suppose b_1, b_2 are not square modulo p. If $a_1 \neq a_2$ and $b_1 = b_2$ then E_1, E_2 have no solutions in common.*

Proof. Let $a_1 \neq a_2$ and $b_1 = b_2$. Since b_1, b_2 are not perfect squares, $E_1(\mathbb{F}_p), E_2(\mathbb{F}_p)$ can not have any solutions of the form $(0, y_o)$. Assume $(x_o, y_o) \in E_1(\mathbb{F}_p), E_2(\mathbb{F}_p)$. Then $y_o^2 = x_o^3 + a_1 x_o + b_1$, and $y_o^2 = x_o^3 + a_2 x_o + b_2$. We can solve for the a_i's and see that $a_1 = (y_o^2 - x_o^3 - b_1)x_o^{-1} = (y_o^2 - x_o^3 - b_2)x_o^{-1} = a_2$. This is a contradiction so E_1, E_2 have no common solutions. □

Theorem 2.5.3. *Suppose $b_1, b_2 \neq 0$ and are not square modulo p. If $a_1 \neq a_2$ and $b_1 = b_2$ then E_1, E_2 have exactly two points as common solutions.*

Proof. Since b_1, b_2 are perfect squares, E_1, E_2 have the solutions $(0, \sqrt{b_1}), (0, -\sqrt{b_1})$, where $\sqrt{b_1}$ refers to a fixed square root of $b_1 \mod p$. Assume $(x_o, y_o) \in E_1, E_2$ such that $x_o \neq 0$. Then $y_o^2 = x_o^3 + a_1 x_o + b_1$, $y_o^2 = x_o^3 + a_2 x_o + b_2$. We can solve for the a_i's and see that $a_1 = (y_o^2 - x_o^3 - b_1)x_o^{-1} = (y_o^2 - x_o^3 - b_2)x_o^{-1} = a_2$. This is a contradiction so the only common solutions E_1, E_2 have are $(0, \sqrt{b_1}), (0, -\sqrt{b_1})$. □

These facts about overlap will be useful in Chapter 4 while trying to find bounds for the main problem of this project.

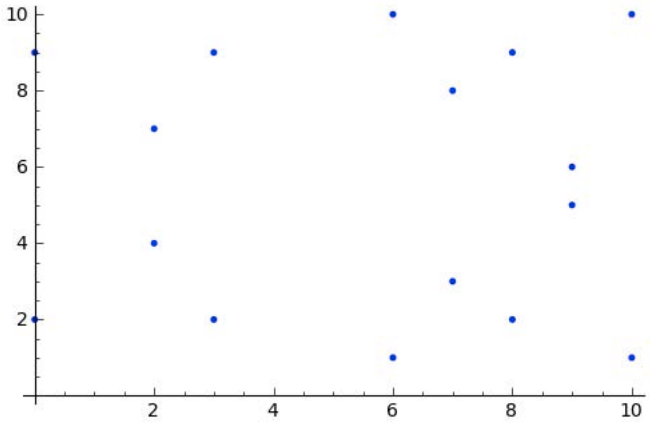
3

The Spanning Property and Minimal Spanning Curves

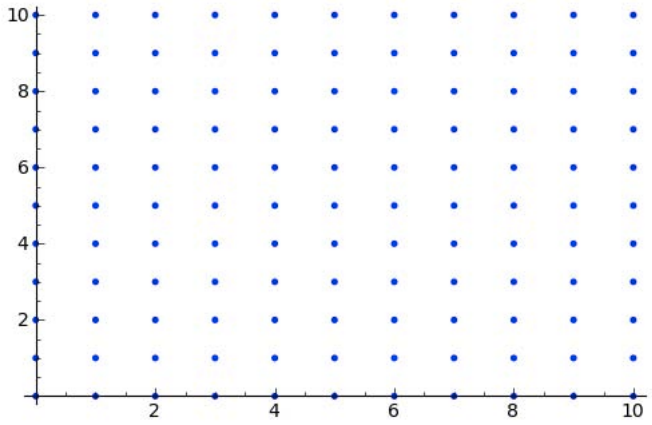
This chapter will describe a property of all the elliptic curves over a fixed prime field that we call the spanning property. The Spanning Property will be the main focus of this project.

3.1 Visualizing the Spanning Property

As well as having an algebraic formula and a group structure [2, Chapter 3, Page 68], elliptic curves can be studied geometrically. To show this we will start by taking the single curve $E(\mathbb{F}_{11})$ defined by the curve $y^2 = x^3 + 2x + 4$. We can plot each solution on an xy axis representing $\mathbb{F}_{11} \times \mathbb{F}_{11}$.



With this example in mind we can ask what happens when all 110 elliptic curves in $\mathbb{F}_{11}$ are plotted on the same graph? Using SAGE we can plot all these graphs together and see the result.



This result is interesting because it means each point in $\mathbb{F}_{11} \times \mathbb{F}_{11}$ is on at least one elliptic curve. It is natural then to try and generalize this and see for which primes p do all the curves together cover $\mathbb{F}_p \times \mathbb{F}_p$. It turns out the answer is that every prime p has this property but to show this we will turn away from geometry and instead use number theory.

3.2 Proof of the Spanning Property

In this section we will prove that for every point (x_o, y_o) in $\mathbb{F}_p \times \mathbb{F}_p$ there is an elliptic curve that has that point as a solution. This means when all the elliptic curves are graphed on the same axes the entire field is covered. Because it is entirely covered we call this the *Spanning Property.*

Theorem 3.2.1. *Let p be a prime. For every $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, there exists an elliptic curve E defined over $\mathbb{F}_p$ such that $(x, y) \in E(\mathbb{F}_p)$.*

Proof. To prove this theorem we use brute force for $p = 2$ and $p = 3$ and then a unified approach for $p > 3$. The following tables show the possible points in each field on the left and elliptic curves for which those points are solutions on the right. Note that each of these curves also pass the appropriate discriminant test for $E(\mathbb{F}_p)$. It is clear that in each table are all possible (x, y) in the respective field are covered.

First suppose $p = 2$.

(x, y)	$E(\mathbb{F}_2)$
(1,0), (1,1)	$y^2 + xy = x^3 + 1$
(0,1)	$y^2 + xy = x^3 + x^2 + 1$
(0,0)	$y^2 + y = x^3$

Now suppose $p = 3$.

(x, y)	$E(\mathbb{F}_3)$
(0,0), (1,0), (2,1)	$y^2 = x^3 + x$
(0,1), (0,2), (2,2)	$y^2 = x^3 + x + 1$
(1,1), (1,2), (2,0)	$y^2 = x^3 + x + 2$

Now suppose $p > 3$. Let $x_o, y_o \in \mathbb{F}_p \times \mathbb{F}_p$. We see that (x_o, y_o) is a solution on an elliptic curve if there exist an $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ such that $y_o^2 = x_o^3 + ax_o + b$ and $4a^3 + 27b^2 \neq 0 \pmod{p}$.

To show that for every $(x_o, y_o) \in \mathbb{F}_p \times \mathbb{F}_p$ there exists E with $(x_o, y_o) \in E(\mathbb{F}_p)$ we have two cases.

Case 1: Suppose $x_o^3 \neq y_o^2$. Choose $a = 0$ and $b = y_o^2 - x_o^3$. With this choice of (a, b) we see that the curve passes the discriminant $4a^3 + 27b^2 \neq 0 \pmod{p}$ and thus is an elliptic curve $E/\mathbb{F}_p$. Then by substitution we see that $X^3 + aX + b = X^3 + 0 \cdot X + (y_o^2 - x_o^3) = x_o^3 + 0 \cdot x_o + (y_o^2 - x_o^3) = y_o^2$. Thus $(x_o, y_o) \in E(\mathbb{F}_p)$

Case 2: Now suppose $x_o^3 = y_o^2$. We see that $0 = ax_o + b$ and subsequently $b = -x_o$. Choose $a = 1$. Then (x_o, y_o) is a solution to the equation $Y^2 = X^3 + X - x_o$ unless $4 + 27x_o^2 = 0 \pmod{p}$.

If $4 + 27x_o^2 = 0 \pmod{p}$ then choose $a = -1$. Then $b = x_o$. Then (x_o, y_o) is a solution to the equation $Y^2 = X^3 - X + x_o$ unless $-4 + 27x_o^2 = 0 \pmod{p}$.

If both $4 + 27x_o^2 = 0 \pmod{p}$ and $-4 + 27x_o^2 = 0 \pmod{p}$ then we can add these two equations. Thus $54x_o = 0 \pmod{p}$. Since $54 = 3^3 \times 2$ this is only possible if $x_o = 0$. Since $x_o^3 = y_o^2$, $y_o^2 = 0$.

For $(x_o, y_o) = (0, 0)$ choose $(a, b) = (1, 0)$. This is true because $y_o^2 = 0 = x_o^3 + x_o$ and $4 \neq 0 \pmod{p}$. Thus $(x_o, y_o) \in E(\mathbb{F}_p)$.

□

3.3 Minimum Number of Curves to Span the Plane $\mathbb{F}_p \times \mathbb{F}_p$

Now we have a proof that with all the curves we can cover the plane made by $\mathbb{F}_p \times \mathbb{F}_p$. It is then natural to ask wether we need all the curves to span the plane. What is the minimum number of curves one can use to span the plane? This problem can be stated precisely as follows.

Problem: Let $\{E_1, E_2, \ldots E_{p^2-p}\}$ the set of all elliptic curves over $\mathbb{F}_p$. From Theorem 3.2.1 we know that $|\bigcup_{i=1}^{p^2-p} E_i(\mathbb{F}_p)| = p^2$. What is the smallest $n \in \mathbb{N}$ such that $|\bigcup_{i=1}^{n} E_i(\mathbb{F}_p)| = p^2$.

4
Computational Bounds

Since there is no immediately obvious way to calculate the minimum number of curves n needed to span the plane, we can computationally look for upper and lower bounds instead. We already know that n is bounded above by $p^2 - p$. However it is very easy to show that this is not the least upper bound. Similarly while 1 must be a lower bound because we would need at least 1 curve, we know that this is not the greatest lower bound. The following subsections will discuss methods for finding upper then lower bounds both theoretically and computationally. It is worth noting that because any combination of the $p^2 - p$ curves may span $\mathbb{F}_p$ it is not feasible to use brute force to find a minimum spanning set.

4.1 Upper Bound

The following three methods produce upper bounds on the minimum number of curves needed. After describing each algorithm I will offer analysis as well as a table of results. Also in Chapter 8 there is the SAGE code for each of these methods.

4.1.1 Proof Method

The proof of the spanning property defines an elliptic curve for each point in the plane. We can simply go through the same checks as the proof and maintain a list of the curves used. This runs as follows. Create a list of the p^2 points in the plane. For each point (x_o, y_o):

1. If $x_o^3 \neq y_o^2$ add the curve $(0, y_o^2 - x_o^3)$ to the list of required curves if it isn't already there.

2. If $x_o^3 = y_o^2$ and $27x_o^2 + 4 = 0 \mod p$ add the curve $(1, -x_o)$ to the list of required curves if it isn't already there.

3. If $x_o^3 = y_o^2$ and $27x_o^2 - 4 = 0 \mod p$ add the curve $(-1, x_o)$ to the list of required curves if it isn't already there.

4. If the point is $(0, 0)$ add the curve $(1, 0)$ to the list of required curves if it isn't already there.

4.1.2 Largest Curve Method

To find a better upper bound we can use SAGE to run a program that works as follows:

1. Create a list of the p^2 points in the plane and all $p^2 - p$ curves that pass the discriminant test.

2. Find the curve that has the most of solutions on the list of points. Add this curve to the list of required curves.

3. Remove the solutions of this curve from the list of points and that curve from the list of unused curves.

4. Repeat steps two and three until there are no points left in the original list.

4.1.3 Random Method

Since the above two methods do not provide a guaranteed lower bound it may be possible for a computer to find a better lower bound using brute force and random selection. So in SAGE one can write a program that runs as follows.

1. Generate a list of all possible (a, b) that pass the discriminant test for p.

2. Pick a random (a, b) from this list and put any solution points that aren't already there into a list of covered points.

3. Remove (a, b) from the list of curves.

4. Repeat steps 2 and 3 until the list of solution points has length p^2. Record the number of curves used.

5. Repeat steps 1 through 4 a large number of times (1,000,000). Find the smallest number recorded.

Running this program a million times for the small primes $5, 7$ gives better solutions than the two other estimates. For primes greater than 9 though the other methods for estimating are both more effective and more efficient.

4.1.4 Results of Computational Upper Bound Methods

This table shows the results of the three algorithms. Because the random algorithm was so inefficient its results are only listed up to $p = 41$.

p	Largets Curve	Proof Technique	Random
5	5	8	4
7	9	11	8
11	11	20	17
13	17	22	25
17	22	29	40
19	28	35	49
23	33	41	63
29	42	50	94
31	46	54	107
37	63	64	135
41	69	71	158
43	64	75	
47	84	84	
53	81	92	
59	109	107	
61	113	106	
67	100	119	
71	137	127	
73	109	127	
79	118	141	
83	165	149	
89	179	155	
97	145	169	
101	150	176	
103	154	183	
107	230	191	
109	176	190	
113	242	197	
127	202	225	
131	294	236	
137	204	239	
139	208	248	
149	236	260	

4.1.5 Worst Case Scenario Method

Using what we know about how curves intersect from Section 2.5 and what we know about the size of curves from Section 2.3 we can try create a theoretical upper bound.

Hasse's theorem tells us that the smallest number of solutions a curve can have is $p - \lfloor 2\sqrt{p} \rfloor$. To see the worst case scenario then, the obvious thing to do then is to divide p^2 by this smallest size. This produces a result of $\lceil \frac{p^2}{p-\lfloor 2\sqrt{p} \rfloor} \rceil$.

Though this is good, it is not necessarily an upper bound as it does not account for points intersecting on various curves. We know that each curve can intersect with each previously chosen curve at most 2 points. Since we are looking at the worst case we can assume each curve intersects with each previous curve at two points. This means when we add the n^{th} curve we get $p - \lfloor 2\sqrt{p} \rfloor - 2(n-1)$ new points. We will define $f(n)$ to be $p - \lfloor 2\sqrt{p} \rfloor - 2(n-1)$. So the upper bound will be n such that $\sum_{i=0}^{n} f(i) \geq p^2$. However we will show that no such n exists. First we will find a polynomial expression for the summation. For clarity let $c = p - \lfloor 2\sqrt{p} \rfloor$

$$\begin{aligned}\sum_{i=0}^{n} f(i) &= \sum_{i=0}^{n} c - 2(i-1) = \sum_{i=0}^{n} c + 2 - 2i \\ &= nc + 2n - 2\sum_{i=0}^{n} i = nc + 2n - 2\frac{n(n+1)}{2} \\ &= nc + 2n - n^2 - n = -n^2 + nc + n = n(-n + c + 1)\end{aligned}$$

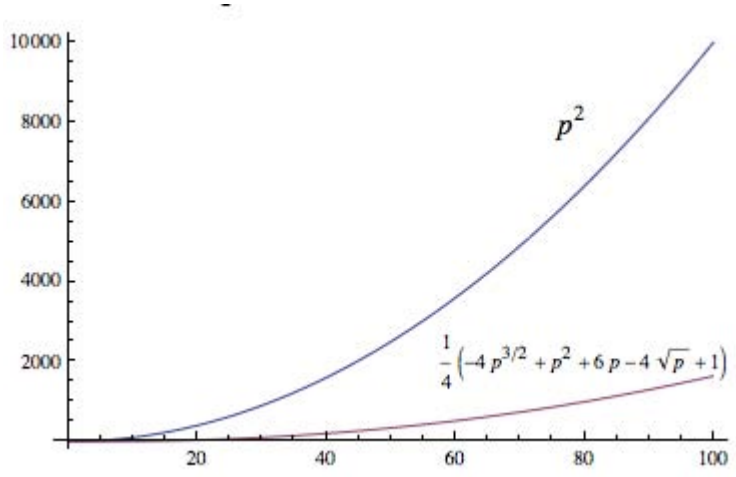
So we see that this is a parabola with negative concavity and roots at $0, c+1$. So we know the maximum must be halfway between the roots at $\frac{c+1}{2}$.We now show that $\sum_{i=0}^{\frac{c+1}{2}} f(i) < p^2$.

$$\begin{aligned}\sum_{i=0}^{\frac{c+1}{2}} f(i) &= \frac{c+1}{2}(\frac{1-c}{2} + 1 + c) \\ &= \frac{-c^2 - 2c - 1}{4} + \frac{2c^2 + 2c}{4} + \frac{2c+2}{4} = \frac{c^2 + 2c + 1}{4} \\ &= \frac{(p - \lfloor 2\sqrt{p} \rfloor)^2 + 2(p - \lfloor 2\sqrt{p} \rfloor) + 1}{4} \\ &= \frac{p^2 - 2p\lfloor 2\sqrt{p} \rfloor + (\lfloor 2\sqrt{p} \rfloor)^2 + 2p - 2\lfloor 2\sqrt{p} \rfloor + 1}{4}\end{aligned}$$

Because we know that $p - \lfloor 2\sqrt{p} \rfloor \leq p - 2\sqrt{p}$ we see that,

$$\begin{aligned} &\leq \frac{p^2 - 2p(2\sqrt{p}) + (2\sqrt{p})^2 + 2p - 2(2\sqrt{p}) + 1}{4} \\ &= \frac{p^2 - 4p\sqrt{p} + 4p + 2p - 4\sqrt{p} + 1}{4} \\ &= \frac{p^2 - 4p\sqrt{p} + 6p - 4\sqrt{p} + 1}{4} \end{aligned}$$

To see that $\frac{p^2-4p\sqrt{p}+6p-4\sqrt{p}+1}{4} < p^2$ we can simply graph the two functions together. We can see that p^2 is always greater.



Thus $\sum_{i=0}^{\frac{c-1}{2}} f(i) \leq \frac{p^2-4p\sqrt{p}+6p-4\sqrt{p}+1}{4} < p^2$.

This means our attempt to make a generalized upper bound does not work because we must account of intersection between curves. However we can do better looking for a theoretic lower bound.

4.2 Lower Bound

We can find a lower bound by finding a set of curves that do not necesarily span the field but are required to span the field or, by using the size curves to estimate a minimum number that would be needed. The following two sections will lay out each of these techniques.

4.2.1 Table Method

One method to look for a lower bound is to make a table. Across the top of the table goes a list of all the points in the plane. The curves that pass the discriminant test are listed down the side. Where a point is a solution to the curve we put a 1 and we put a 0 every where else. If any column has a single 1 then we know the corresponding curve must be in the minimum set in order to cover the point corresponding to that column.

An example of this can be seen for $p = 3$:

Curves/Points	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)	(0,2)	(1,2)	(2,2)
$y^2 = x^3 + x$	1					1			1
$y^2 = x^3 + x + 1$		1		1			1		
$y^2 = x^3 + x + 2$			1		1			1	
$y^2 = x^3 + 2x$	1	1	1						
$y^2 = x^3 + 2x + 1$				1	1	1	1	1	1
$y^2 = x^3 + 2x + 2$									

As one can see there is no column that sums to 1. By testing several primes in SAGE it seems that this in fact never happens. This warrants a proof.

Theorem 4.2.1. *For every $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, if (x, y) is a solution to $E_1(\mathbb{F}_p)$ then (x, y) is a solution to a different elliptic curve $E_2(\mathbb{F}_p)$.*

Proof. Let E_1 be defined by $y^2 = x^3 + a_1x + b_1$ and E_2 be defined by $y^2 = x^3 + a_2x + b_2$ for some $a_1, a_2, b_1, b_2 \in \mathbb{F}_p$ such that $E_1 \nsim E_2$. Let (x_o, y_o) be a solution to E_1. Then $y_o^2 = x_o^3 + a_1x_o + b_1$.

Case 1: Let $x_o = 0$. It follows easily that $y_o^2 = b_1$. Choose an $a_2 \neq a_1$ and $b_2 = b_1$. Then E_2 is $y^2 = x^3 + a_2x + b_1$. We check that (x_o, y_o) is a solution to E_2 by substitution and see that indeed $y_o^2 = b_1$.

Case 2: Let $x_o \neq 0$ and $\frac{b_1}{x_o} \neq a_1$. Choose an $a_2 = \frac{b_1}{x_o}$ and $b_2 = a_1x_o$. Note $a_1 \neq a_2$. Then E_2 is $y^2 = x^3 + \frac{b_1}{x_o}x + a_1x_o$. We check that (x_o, y_o) is a solution to E_2 by substitution and see that indeed $y_o^2 = x_o^3 + a_1x_o + b_1$.

Case 3: Let $x_o \neq 0$, $\frac{b_1}{x_o} = a_1$, and $b_1 \neq 0$. Choose an $a_2 = 0$ and $b_2 = 2b_1$. Note $a_1 \neq a_2$. It follows then that $y_o^2 = x_o^3 + \frac{b_1}{x_o}x_o + b_1 = x_o^3 + 2b_1$. Then E_2 is $y^2 = x^3 + 0x + 2b_1$. We check that (x_o, y_o) is a solution to E_2 by substitution and see that indeed $y_o^2 = x_o^3 + 0x_o + 2b_1 = x_o^3 + 2b_1$.
Case 4: Let $x_o \neq 0$, $\frac{b_1}{x_o} = a_1$, and $b_1 = 0$. Note that this implies that $a_1 = 0$. This means E_1 fails the discriminant test so we need not worry about this case. □

Though this proof does not give a lower bound it does demonstrate an interesting aspect about how elliptic curves intersect. While no two curves can intersect at more than two points, every point is the intersection of at least two distinct elliptic curves.

4.2.2 Best Case Scenario Method

With Hasse's theorem we know that n, the number of solutions to the curve $E(\mathbb{F}_p)$, is in the range $\lfloor -2\sqrt{p} \rfloor + p < n < \lceil 2\sqrt{p} \rceil + p$. Let us assume that each curve has completely distinct solutions. Let us also assume that each curve we choose is as large as possible, that is it has $\lceil 2\sqrt{p} \rceil + p$ solutions. Then to cover p^2 points we need $\lceil \frac{p^2}{p + \lfloor 2\sqrt{p} \rfloor} \rceil$ curves. This gives us a lower bound. Unlike the upper bound we don't have to worry about intersection because we know we can have curves that don't intersect and we are assuming the best case scenario.

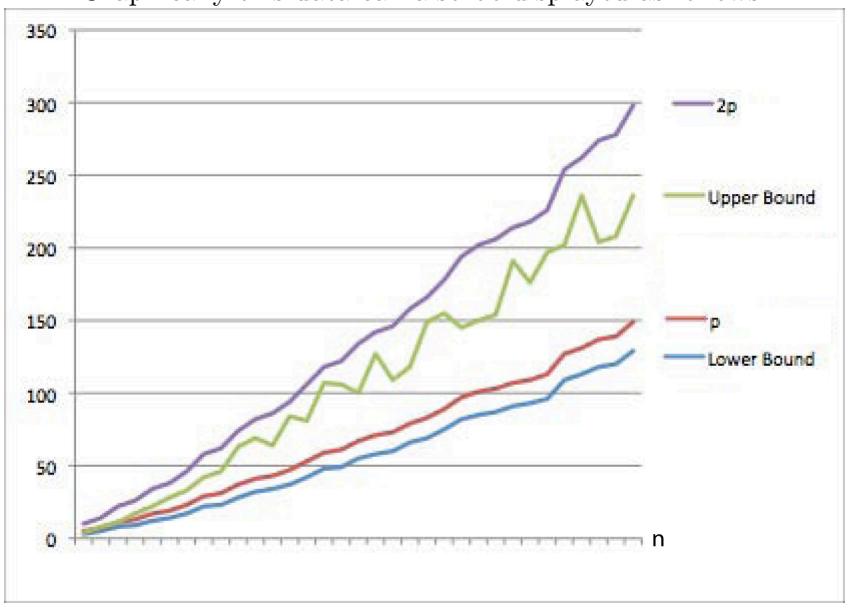
However using a program in SAGE it is easy to see even without worrying about solutions being distinct that for many primes there are not this many curves of size $\lceil 2\sqrt{p} \rceil + p$. The lack of large enough curves means while this is a lower bound but it is not a a solution to the spanning property.

4.3 Summary

We can make a table of the lower bound and the best upper bound we calculated to give an idea of the range for the spanning property. The right most column is $2p$ to give an idea of the size of the upper bound.

p	Lower Bound	Upper Bound	$2p$
5	3	4	10
7	5	8	14
11	8	11	22
13	9	17	26
17	12	22	34
19	14	28	38
23	17	33	46
29	22	42	58
31	23	46	62
37	28	63	74
41	32	69	82
43	34	64	86
47	37	84	94
53	42	81	106
59	48	107	118
61	49	106	122
67	55	100	134
71	58	127	142
73	60	109	146
79	66	118	158
83	69	149	166
89	75	155	178
97	82	145	194
101	85	150	202
103	87	154	206
107	91	191	214
109	93	176	218
113	96	197	226
127	109	202	254
131	113	236	262
137	118	204	274
139	120	208	278
149	129	236	298

Graphically this data can also be displayed as follows:



From the table and graph we see that p is in the range between the upper and lower bounds. This means it is possible that the minimum number of curves to span $\mathbb{F}_p$ is p. The next chapter will investigate and in fact prove that this is the case.

5
Number Theoretic Solution

This chapter will demonstrate two alternate solutions to the spanning problem. The first will use bounds and asymptotes. The second will use number theory to solve the spanning problem for $p \equiv 3 \mod 4$.

5.1 p Curves that Span $\mathbb{F}_p \times \mathbb{F}_p$

From the table in Section 4.3 we get the inkling that the answer may be p. So it seems reasonable to look for an easy way to make sets of p curves. One obvious way to do this is to fix either a and vary b or vice versa. However we know that this cannot work for every a, b because of the discriminant test. Some a's do provide p curves that pass the discriminant test when b varies from 0 to $p-1$. We can demonstrate exactly how many such a's there are.

Lemma 5.1.1. *Let $a_i, b \in \mathbb{F}_p^\times$. There are $\frac{p-1}{2}$ distinct values of a_i such that $4a_i^3 + 27b^2 \not\equiv 0 \mod p$.*

Proof. Recall from Lemma 2.2.1 that there are p solutions to $4a^3 + 27b^2 \equiv 0 \mod p$. In Lemma 2.2.1 we showed that the only solution where $a = 0$ is $a = 0$, $b = 0$. So there are

$p-1$ solutions where $a \neq 0$. Let G be the set of these $p-1$ solutions. Mathematically, $G = \{(a,b) | a \neq 0, 4a^3 + 27b^2 = 0 \mod p\}$. Let $(a_o, b_o) \in G$. Because $x^2 = (-x)^2$, we know then that $(a_o, -b_o) \in G$. We can also see there is no other $b \in \mathbb{F}_p^\times$ such that $(a_o, b) \in G$. This means for each a_o there are exactly two values of b. Because there are $p-1$ solutions and two choices of b for every a then there must be $\frac{p-1}{2}$ a_i such that $(a_i, b) \in G$. So of the p possible a_i, $\frac{p-1}{2} + 1$ fail the discriminant test for some choice of b. Equivalently, there are $p - \frac{p-1}{2} + 1$ or, $\frac{p-1}{2}$ a_i such that $4a_i^3 + 27b^2 \not\equiv 0 \mod p$ for any $b \in \mathbb{F}_p$. □

Now we have $\frac{p-1}{2}$ sets of p curves that are easy to discuss. We can demonstrate that any one of these sets spans $\mathbb{F}_p \times \mathbb{F}_p$.

Theorem 5.1.2. *Let $p \geq 5$. If $a_o \in \mathbb{F}_p^\times$ such that $4a_o^3 + 27b^2 \not\equiv 0 \mod p$ for any $b \in \mathbb{F}_p$, then $|\bigcup_{b=0}^{p-1} E_{a_o,b}| = p^2$.*

Proof. Let $a_o \in \mathbb{F}_p^\times$ such that $4a_o^3 + 27b^2 \not\equiv 0 \mod p$ for any $b \in \mathbb{F}_p$. Note that because a_i is equal for each curve $E_{a_i,b}$ we know from Lemma 2.5.1 that each point will be distinct.

Let $(x_o, y_o) \in \mathbb{F}_p \times \mathbb{F}_p$. We can show that either $(x_o, y_o) \in E_{a_o,0}$ or $(x_o, y_o) \in E_{a_o,b}$ for some $b \in \mathbb{F}_p^\times$. Assume $(x_o, y_o) \notin E_{a_o,0}$. Then $y_o^2 \neq x_o^3 + a_o x_o$ and $y_o^2 - x_o^3 - a_o x_o \neq 0$. So choose $b = y_o^2 - x_o^3 - a_o x_o$. Then $x_o^3 + a_o x_o + b = x_o^3 + a_o x_o + (y_o^2 - x_o^3 - a_o x_o) = y_o^2$. Thus $(x_o, y_o) \in E_{a_o,b}$. □

A careful reader will notice that this is does not guarantee a minimum spanning set but creates an upper bound of p. To demonstrate that this is a minimal solution we can show that the lower bound discussed in Section 4.2.2 is asymptotic to p.

5.2 Asymptotic Bounds

As we established in Section 4.2.2 the lower bound for the minimum number of elliptic curves needed to span the field is $\lceil \frac{p^2}{p+\lfloor 2\sqrt{p} \rfloor} \rceil$. However, using calculus, we can show that as p approaches infinity this bound is asymptoticly close to p.

Theorem 5.2.1. *We have the following limit* $\lim_{p \longrightarrow \infty} \lceil \frac{p^2}{p + \lfloor 2\sqrt{p} \rfloor} \rceil = p.$

Proof. $\lim_{p \longrightarrow \infty} \lceil \frac{p^2}{p + \lfloor 2\sqrt{p} \rfloor} \rceil = \lim_{p \longrightarrow \infty} \lceil \frac{\frac{1}{p}}{\frac{1}{p}} \times \frac{p^2}{p + \lfloor 2\sqrt{p} \rfloor} \rceil = \lim_{p \longrightarrow \infty} \lceil \frac{p}{1 + \frac{\lfloor 2\sqrt{p} \rfloor}{p}} \rceil$

It is clear that as we take this limit $\frac{\lfloor 2\sqrt{p} \rfloor}{p}$ goes to 0. So, $= \lceil \frac{p}{1+0} \rceil = \lceil p \rceil = p.$ □

This proof completes the problem of finding a minimal number of elliptic curves to span $\mathbb{F}_p \times \mathbb{F}_p$. We know p is a constant upper bound and that the lower bound approaches p so for large enough primes the minimum number of curves needed will be p.

5.3 Alternate Proof When $p \equiv 3 \mod 4$

In this section we can utilize number theory to demonstrate how the previous proof can be done differently. We must begin with a definition and some explination.

Definition 5.3.1. An element $q \neq 0 \in \mathbb{F}_p$ is a quadratic **residue** if there exists $x \in \mathbb{F}_p$ such that $x^2 \equiv q \mod p$ and a quadratic **nonresidue** if no such x exists.

From the law of quadratic reciprocity we will take it as fact that the product of two nonresidues is a residue and the product of a nonresidue and a residue is a nonresidue. Also from Euler's theorem we know that -1 is a residue when $p \equiv 1 \mod 4$ and a non residue when $p \equiv 3 \mod 4$.[3, Chapter 5, Page 100] From this it follows that if $p \equiv 1 \mod 4$ the negative of a residue is a residue and the negative of a nonresidue is a nonresidue. If $p \equiv 3 \mod 4$ the negative of a residue is a nonresidue and the negative of a nonresidue is a residue.

With this knowledge from number theory we can make very strong statments about the number of solutions for a given curve. We will use the notation $len(a, b)$ to mean the number of solutions to $E_{a,b}$.

Lemma 5.3.2. *If* $(x_o, 0) \in E_{a,b}$ *then* $(-x_o, 0) \in E_{a,-b}$.

Proof. Let $(x_o, 0) \in E_{a,b}$. Then $0 = x_o^3 + ax_o + b$. Multiplying by -1 we see that

$$0 = -x_o^3 - ax_o - b = (-x_o)^3 + a(-x_o) - b.$$

Thus $(-x_o, 0) \in E_{a,-b}$. □

Lemma 5.3.3. *Let* $p \equiv 3 \mod 4$ *and* $y_o \in \mathbb{F}_p^\times$. *If* $(x_o, y_o) \in E_{a,b}$ *then* $(-x_o, Y) \notin E_{a,-b}$ *for any* $Y \in \mathbb{F}_p^\times$.

Proof. Let $y_o \in [1, \ldots p-1]$ and $(x_o, y_o) \in E_{a,b}$. Assume there exists some Y such that $(-x_o, Y) \notin E_{a,-b}$ Then,

$$Y^2 = (-x_o)^3 + a(-x_o) - b$$
$$Y^2 = -1(x_o^3 + ax_o + b)$$
$$Y^2 = -y_o^2.$$

This is a contradiction because we know y_o is a quadratic residue and when $p \equiv 3 \mod 4$ the negative of a residue must be a non residue. Thus $(-x_o, Y) \notin E_{a,-b}$ for any $Y \in [1, \ldots p-1]$. □

Theorem 5.3.4. *If* $p \equiv 3 \mod 4$ *then* $len(a, b) + len(a, -b) = 2p$.

Proof. Let $E_{a,b}, E_{a,-b}$ be elliptic curves. Let z be the number of solutions to $E_{a,b}$ of the form $(x_o, 0)$ and n be the number of solutions to $E_{a,b}$ of the form (x_o, y_o) where $y_o \neq 0$. By lemma 5.3.2 we see that $E_{a,-b}$ must have z solutions of the form $(X, 0)$. Let m represent the number of solutions to $E_{a,-b}$ not of this form. We can see that at most

$m \leq 2(p - z - \frac{1}{2}n)$. We know this is true because $p - z - \frac{1}{2}n$ represent those x that are not already solutions to $E_{a,-b}$ and are not restricted by lemma 5.3.3. At each of these x values $E_{a,-b}$ could have at most 2 solutions. Assuming $m = 2(p - z - \frac{1}{2}n)$ we see that $len(a, b) + len(a, -b) = n + m + z + z = n + 2z + 2(p - z - \frac{1}{2}n) = 2p$. So we must show that at each of these x values $E_{a,-b}$ has two non zero solutions.

Assume $(w, Y) \notin E_{a,-b}$ for some $z, Y \in \mathbb{F}_p^\times$ and $w \neq -x_o$ for any x_o such that $(x_o, Y) \in E_{a,b}$. This means that $w^3 + aw - b$ is a non residue. Since we know that -1 is a non residue we can expect a residue from the product of -1 and $w^3 + aw - b$. So,

$$Y^2 = -w^3 - aw - b$$

$$Y^2 = (-w)^3 + a(-w) + b$$

Thus $(-w, Y) \in E_{a,b}$. This is a contradiction to the definition of w because w can not equal the negative of any x value that provides a solution to $E_{a,b}$. Thus $(w, Y), (w, -Y) \in E_{a,-b}$. This produces the two solutions at each point and shows that m does in fact equal $2(p - w - \frac{1}{2}n)$, so our theorem holds. □

Corollary 5.3.5. *Let $a_o \in \mathbb{F}_p^\times$. If $p \equiv 3 \mod 4$ then $len(a_o, 0) = p$.*

Proof. From Theorem 5.3.4 we know that

$$len(a_o, 0) + len(a_o, -0) = 2len(a_o, 0) = 2p$$

Thus, $len(a_o, 0) = p$. □

Theorem 5.3.6. *If $p \equiv 3 \mod 4$ then there are p distinct elliptic curves such that their union has size p^2.*

Proof. Let $p \equiv 3 \mod 4$.By Corollary 5.3.5 we know that $len(a, 0)$ has p solutions. Let us then fix an $a_o \in \mathbb{F}_p$ such that $E_{a_o,b}$ is an elliptic curve for all $b \in \mathbb{F}_p$. Then,

$$|\bigcup_{b=0}^{p-1} E_{a_o,b}| = (\sum_{b=1}^{p-1} len(a_o, b)) + p$$

We know that $E_{a,b}$ can be paired with $E_{a,-b}$ into $\frac{p-1}{2}$ distinct pairs of curves so,

$$= (\sum_{b=1}^{\frac{p-1}{2}} len(a_o, b) + len(a_o, -b)) + p$$

From Theorem 5.3.4 we know that the union of each of these $\frac{p-1}{2}$ pairs has $2p$ distinct points. Thus,

$$= (\sum_{b=1}^{\frac{p-1}{2}} 2p) + p$$

$$= 2p\frac{p-1}{2} + p = p^2 - p + p = p^2$$

. □

6
Supersingularity

This chapter will demonstrate how some of the number theory from previous chapters can be used to provide facts about elliptic curves. We will start by looking at the specific curve $y^2 = x^3 + x$. For this curve we will show a traditional proof involving calculus and group theory of a property called supersingularity. Then we will demonstrate how the converse can be done easily with number theory. Then we will demonstrate an attempt to generalize these proofs into a very powerful theorem. But first a few quick definitions.

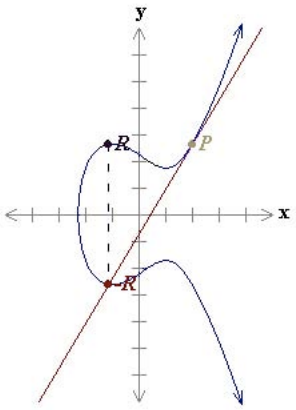
Definition 6.0.7. A prime is *supersingular* for a given elliptic curve if $|E(\mathbb{F}_p)| = p$.

By attaching a point σ to $\mathbb{F}_p \times \mathbb{F}_p$ we can create a set called *Projective Space*. We call σ the point at infinity. We will not go into elaborate detail because we will only need Projective Space for a few proofs.

Using σ as the additive identity it is a fact that the solutions to an elliptic curve form an Abelian group.

To clarify in the previous definition when we say σ is an additive identity we do not mean addition as it is commonly used. Instead we mean elliptic curve addition. To add two points, say P and Q, we draw a line through those points. It is a nontrivial fact that

we will not prove here that this line intersect the elliptic curve in a third place denoted $-R$. If this line is vertical we use σ as $-R$. We then reflect $-R$ across the x axis to get $P+Q=R$. We are assured a value at the reflection of $-R$ because of the y^2 in the formula for E. Adding a point to itself works in exactly the same way except we use a tangent line. The graphic below demonstrates $P+P=R$.



With this understanding of elliptic curve addition we can move forward. [4].

6.1 Traditional Proof of Supersingularity for $y^2 = x^3 + x$

Let E be the curve defined by $y^2 = x^3 + x$. The following theorems will demonstrate which primes are supersingular for E.

Theorem 6.1.1. *In projective space the number of solutions to* $E(\mathbb{F}_p) \equiv 0 \mod 4$.

Proof. Case 1: Let $p \equiv 1 \mod 4$. Also let $y = 0$. Then $0 = x(x^2 + 1)$. Solutions then exist at $(0, 0)$ and $x^2 + 1 = 0$. We have already seen that $x^2 = -1$ has two solutions mod p when $p \equiv 1 \mod 4$, which we denote $\pm\sqrt{1}$. So

$$y^2 = x^3 + x = x(x + \sqrt{-1})(x - \sqrt{-1})$$

This means the points $\{(\sqrt{-1},0),(-\sqrt{-1},0),(0,0),\sigma\}$ are all elements of $E(\mathbb{F}_p \cup \{\sigma\})$. These points form a subgroup using Elliptic curve addition. Because the order of any subgroup divides the order of the group we see that $4|\#E(\mathbb{F}_p \cup \{\sigma\})$.

Because -1 is a quadratic non residue when $p \equiv 3 \mod 4$ we will have to use a different technique for our second case.

Case 2: Let $p \equiv 3 \mod 4$. Unlike the above case we see that there is only one point on E when $y = 0$. Let $y = 0$. Then $0 = x(x^2+1)$. So $(0,0)$ is a solution point but there are no solutions to $x^2+1 = 0 \mod p$. So we must find a point P, on E such that $P+P = (0,0)$. Because $(0,0)$ has order 2 such a P would form a subgroup of order 4.

Let $P = (A,B) \in E$ for $A, B \in \mathbb{F}_p$. As described above to add $P+P$ we must find the tangent line. We can use calculus to see that $2yy' = 3x^2+1$ which simplifies to $y' = \frac{3x^2+1}{2y}$. At P the slope of the tangent line, m, is $\frac{3A^2+1}{2B}$. Using the formula for a line $y = mx+b$ we can calculate $b = B - \frac{3A^2+1}{2B}A$. Also notice that $0 = -B^2 + A^3 + A$. Then

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

$$(mx+b)^2 - x^3 - x = 0$$

$$-x^3 + m^2x^2 + (2mb-1)x + b^2 = 0$$

$$-x^3 + \frac{9A^4+6A^2+1}{4B^2}x^2 + 3A^2x + \frac{9A^4+6A^2+1}{4B^2}x^2Ax + \frac{9A^4+6A^2+1}{4B^2}x^2A^2 - 2A^3 - A^3 - A + B^2 = 0$$

$$-x^3 + \frac{9A^4+6A^2+1}{4B^2}x^2 + 3A^2x + \frac{9A^4+6A^2+1}{4B^2}x^2Ax + \frac{9A^4+6A^2+1}{4B^2}x^2A^2 - 2A^3 = 0$$

Here we can factor out $(x-A)^2$ to find the third point of intersection between the tangent line and E.

$$(x^2 - 2Ax + A^2)(-x + \frac{9A^4+6A^2+1}{4B^2} - 2A)$$

So the x value at the third point of intersection is $\frac{9A^4+6A^2+1}{4B^2} - 2A$.

We can then solve for the y value of this third point by solving $y = mx + b$. Thus,

$$2(A,B) = (\frac{9A^4+6A^2+1}{4B^2} - 2A, B + (\frac{3A^2+1}{2B})^3 - 3A\frac{3A^2+1}{2B})$$

To get a point of order 4 solve we set $y = 0$:

$$B + (\frac{3A^2+1}{2B})^3 - 3A\frac{3A^2+1}{2B} = 0$$

$$B + \frac{27A^6+27A^4+9A^2+1}{8B^3} + \frac{-9A^3+-3A}{2B} = 0$$

$$\frac{8B^4+27A^6+27A^4+9A^2+1+4B^2(-9A^3+-3A)}{8B^3} = 0$$

We know this can only be zero if the numerator is zero. Also notice that $B^2 = A^3 + A$ and $B^4 = (A^3 + A)^2$ So,

$$8(A^6+2A^4+A^2) + (4A^3+4A)(-9A^3+-3A) + 27A^6+27A^4+9A^2+1 = 0$$

$$8A^6+16A^4+8A^2+-36A^6-12A^4-36A^4-12A^2+27A^6+27A^4+9A^2+1 = 0$$

$$-A^6-5A^4+5A^2+1 = 0$$

It is clear that 1 and -1 are solutions to this equation for A. Substituting 1,-1 into $y^2 = x^3 + x$ we get that the points $(1, \sqrt{2})$ and $(-1, \sqrt{-2})$. We know that either 2 or -2 is a residue so one of these two points does exist. Since elliptic curves are Abelian groups, that point generates a subgroup of order four. Thus $4|\#E(\mathbb{F}_p \cup \{\sigma\})$.

□

Corollary 6.1.2. *If p is supersingular for $y^2 = x^3 + x$ then the number of solutions to $E(\mathbb{F}_p)$ is $p \equiv 3 \mod 4$.*

Proof. Since there is no point at infinity as there is in projective space, the number of solutions in $\mathbb{F}_p$ equals the number of solutions in projective space minus one. This means the number of solutions to $\#E(\mathbb{F}_p) \equiv 3 \mod 4$. So if p is supersingular then $p = \#E(\mathbb{F}_p) \equiv 3 \mod 4$. □

This proof does not actually provide primes for which $y^2 = x^3 + x$ is supersingular. It only says that if such a prime exists it must be true that $p \equiv 3 \mod 4$. Though this is certainly non trivial the next theorem will show that we can do much better.

Combining Corollary 5.3.5 and the traditional proof from 6.1 we can show the following theorem.

Theorem 6.1.3. *A prime p is supersingular for $y^2 = x^3 + x$ if and only if $p \equiv 3 \mod 4$.*

Proof. Let p be supersingular for $y^2 = x^3 + x$. Then by theorem 6.1.2 we know that $p \equiv 3 \mod 4$.

Let $p \equiv 3 \mod 4$. By corollary 5.3.5 we see that $len(1, 0) = p$. Thus p is supersingular for $y^2 = x^3 + x$. □

7
Generalizing Chapter 6 and Unsolved Conjectures

In this chapter we will try and generalize Theorem 6.1.3 to all curves of the form $y^2 = x^3 + a_o x$. Most of the cases can be done fairly easily but, the one remaining case will be left as a conjecture. Though left unsolved we will demonstrate data to show its likelihood as well a lemma that if proven would imply our desired result. To be precise about what we are trying to generalize we will write the conjecture as such.

Conjecture 7.0.4. *Let $a_o \in \mathbb{F}_p^\times$. Then p is supersingular for the curve $y^2 = x^3 + a_o x$ if and only if $p \equiv 3 \mod 4$.*

7.1 Solved Cases

7.1.1 $p \equiv 3 \mod 4$

Recall Corollary 5.3.5 tells us that if $p \equiv 3 \mod 4$ then $len(a_o, 0) = p$. So we see that if $p \equiv 3 \mod 4$ then p is supersingular for the curve $y^2 = x^3 + a_o x$. Now it will suffice to show that when $p \equiv 1 \mod 4$, p is not supersingular for any curve $y^2 = x^3 + a_o x$.

7.1.2 $p \equiv 1 \mod 4$ *case* 1

To serve as a reminder that a is a residue we will use the notation $a_\square$.

Lemma 7.1.1. *If $p \equiv 1 \mod 4$ and let $a_\square \in \mathbb{F}_p^\times$ be a quadratic residue modulo p then $len(a_\square, 0) \not\equiv p$.*

Proof. Let $p \equiv 1 \mod 4$ and let $a_\square$ be a quadratic residue modulo p. Because $a_\square$ and -1 are both residues their product $-a_\square$ must also be a residue. This means we know $\sqrt{-a_\square}$ and $-\sqrt{-a_\square}$ exist in $\mathbb{F}_p$. Suppose $y = 0$. Then $0 = x(x^2 + a_\square)$. Solutions then exist at $(0, 0)$ and $x^2 + a_\square = 0$. This means the points $\{(\sqrt{-a_\square}, 0), (-\sqrt{-a_\square}, 0), (0, 0), \sigma\}$ are all elements of $E(\mathbb{F}_p \cup \{\sigma\})$. These points form a subgroup using elliptic curve addition. Because the order of any subgroup divides the order of the group we see that $4 | \#E(\mathbb{F}_p \cup \sigma)$. Thus $\#E(\mathbb{F}_p) = \#E(\mathbb{F}_p \cup \{\sigma\}) - 1 \equiv 3 \not\equiv 1 \mod 4$ so p can not be supersingular for $y^2 = x^3 + a_\square x$. □

7.2 Unsolved Case

Before diving into this case we will show some data to try and demonstrate that no value of a_o will make p be supersingular. Below is a table demonstrating this for $p = 13$. From this table we will make several observations that will help us elaborate on our conjecture.

a_o	residue (y/n)	$len(a_o, 0)$	$len(a_o, 0) \mod 4$
1	y	19	3
2	n	9	1
3	y	19	3
4	y	7	3
5	n	9	1
6	n	9	1
7	n	17	1
8	n	17	1
9	y	19	3
10	y	7	3
11	n	17	1
12	y	7	3

To serve as a reminder that a is a nonresidue we will use the notation $a_\triangle$. Let $p \equiv 1 \mod 4$ and $a_\triangle$ be a quadratic non residue in $\mathbb{F}_p$. Perhaps the first thing to notice is that $len(a_\triangle, 0) \equiv 1 \mod 4$. We can prove this.

Theorem 7.2.1. *If $p \equiv 1 \mod 4$ and $a_\triangle$ is a quadratic non residue then $len(a_\triangle, 0) \equiv 1 \mod 4$.*

Proof. Let $x_o, y_o \in \mathbb{F}_p$ such that $y_o \neq 0$. Suppose $(x_o, y_o) \in E_{a_\triangle,0}$. We know then that $(x_o, -y_o) \in E_{a_\triangle,0}$. We can ask does $E_{a_\triangle,0}$ have any solutions at $-x_o$. We know that $y_o^2 = x_o^3 + x_o$, so $(-x_o)^3 - x_o = -1(x_o^3 + x_o) = -y_o = (\sqrt{-1}y_o)^2$. This means $(-x_o, y_o), (-x_o, -y_o) \in E_{a_\triangle,0}$. Thus the number of points on $E_{a_\triangle,0}$ where $y \neq 0$ is divisible by 4. Let $y = 0$ then $0 = x(x^2 + a_\triangle)$. Because $a_\triangle$ is a non residue we know that there are no possible values of $x \in \mathbb{F}_p$ such that $x^2 = -a_\triangle$.Thus when $y = 0$ there is only a solution at $(0, 0)$. Thus $len(a_\triangle, 0) \equiv 1 \mod 4$. □

This proof leaves open the possibility of supersingularity because $len(a_\triangle, 0) \equiv 1 \mod 4$ and $p \equiv 1 \mod 4$. With our next observation we will demonstrate a theorem and then finish with a unproven conjecture that would in fact prove our desired result. To show this theorem and conjecture we will narrow our focus on the table.

$a_\triangle$	residue (y/n)	$len(a_o, 0)$	$len(a_\triangle, 0) \mod 4$
2	n	9	1
5	n	9	1
6	n	9	1
7	n	17	1
8	n	17	1
11	n	17	1

From this we might conjecture that $len(a_\triangle, 0) + len(-a_\triangle, 0) = 2p$ and $len(a_\triangle, 0) \neq len(-a_\triangle, 0)$ which would provide the result we desire. However for $p = 17$ we see this is not true.

$a_\triangle$	residue (y/n)	$len(a_\triangle, 0)$	$len(a_\triangle, 0) \mod 4$
3	n	25	1
5	n	25	1
6	n	9	1
7	n	9	1
10	n	9	1
11	n	9	1
12	n	25	1
14	n	25	1

It does seem to be the case however that there is a way of pairing curves such that their solutions total $2p$. Using a series of lemmas we can prove that curves can be paired to add to $2p$. We will start by looking at the curves $E_{a_\triangle,0}$ and $E_{a_\triangle^3,0}$ when $y = 0$.

Lemma 7.2.2. *If $y = 0$ then the only solution to $E_{a_\triangle,0}$ and $E_{a_\triangle^3,0}$ is $(0, 0)$.*

Proof. Let $y = 0$. Then $0 = x(x^2 + a_\triangle)$ and $0 = x(x^2 + a_\triangle^3)$. It is clear then that $(0, 0)$ is a solution to $E_{a_\triangle,0}$ and $E(a_\triangle^3, 0)$. Also we see that $0 = x^2 + a_\triangle^3$ and $0 = x^2 + a_\triangle$ have no solutions because $a_\triangle$ is a nonresidue. □

Now we can focus on the $p - 1$ values where $x, y \in \mathbb{F}_p^\times$.

Lemma 7.2.3. *Let $x_o, y_o \in \mathbb{F}_p^\times$. If $(x_o, y_o) \in E_{a_\triangle,0}$ then $(a_\triangle x_o, Y) \notin E_{a_\triangle^3,0}$ for any $Y \in \mathbb{F}_p^\times$.*

Proof. Let $(x_o, y_o) \in E_{a_\triangle,0}$. Then $y_o^2 = x_o^3 + a_\triangle x_o$. Assume $(a_\triangle x_o, Y) \in E_{a_\triangle^3,0}$ for some $Y \in \mathbb{F}_p^\times$. Then $Y^2 = (a_\triangle x_o)^3 + a_\triangle^3(a_\triangle x_o) = a_\triangle^3(x_o^3 + a_\triangle x_o) = a_\triangle^3 y_o^2$ We see though that $a_\triangle^3 y_o^2$ is a non residue since $a_\triangle^3$ is a non residue and y_o^2 is a residue. This is a contradiction so our theorem holds. □

Lemma 7.2.4. *Let $z \in \mathbb{F}_p^\times$. If $z \not\equiv a_\triangle x$ for any x such that $(x, Y) \in E_{a_\triangle,0}$ for any $Y \in \mathbb{F}_p^\times$ then $(z, Y) \in E_{a_\triangle^3,0}$ for some $Y \in \mathbb{F}_p^\times$.*

Proof. Let $z \not\equiv a_\triangle x$ for any x such that $(x, Y) \in E_{a_\triangle,0}$ for any $Y \in \mathbb{F}_p^\times$. Assume $(z, Y) \notin E_{a_\triangle^3,0}$ for any $Y \in \mathbb{F}_p^\times$. Then $z^3 + a_\triangle^3 z$ is a non residue. We know that $a_\triangle^{-1}$ is also a

non residue since $a_\triangle * a_\triangle^{-1} = 1$. So $a_\triangle^{-3}(z^3 + a_\triangle^3 z)$ must be a residue. But we see that, $a_\triangle^{-3}(z^3+a_\triangle^3 z) = a_\triangle^{-3}z^3+z = (a_\triangle^{-1}z)^3+a_\triangle(a_\triangle^{-1})z$ Thus $(a_\triangle^{-1}z, Y) \in E_{a_\triangle,0}$ for some $Y \in \mathbb{F}_p^\times$. This is a contradiction of the definition of z so $(z, Y) \in E_{a_\triangle^3,0}$. □

Now with these three lemmas we can show that the solutions $E_{a_\triangle,0}$ and $E_{a_\triangle^3,0}$ sum to $2p$.

Theorem 7.2.5. *If* $p \equiv 1 \mod 4$ *then* $len(a_\triangle, 0) + len(a_\triangle^3, 0) = 2p$.

Proof. We know from lemma 7.2.2 that $E_{a_\triangle,0}$ and $E_{a_\triangle^3,0}$ have one solution at $(0, 0)$. Let n be the number of solutions to $E_{a_\triangle,0}$ of the form (x_o, y_o) where $x_o \neq 0$. Let m be the number of solutions to $E_{a_\triangle^3,0}$ where $x_o \neq 0$.

We can see that at most $m \leq 2(p - 1 - \frac{1}{2}n)$. We know this is true because $p - 1 - \frac{1}{2}n$ represent all possible x's that are not 0 or restricted by lemma 7.2.3 because $a_\triangle^{-1}x \in E_{a_\triangle,0}$. By lemma 7.2.4 we know that $E_{a_\triangle^3,0}$ has two solutions at each of these x values. So $m = 2(p - 1 - \frac{1}{2}n)$.

Thus $len(a_\triangle, 0) + len(a_\triangle^3, 0) = n + m + 1 + 1 = n + 1 + 2(p - 1 - \frac{1}{2}n) = 2p$. □

This theorem is almost sufficient to prove that $E_{a_\triangle,0}$ is never supersingular for $p \equiv 1 \mod 4$. What's missing and left proven is the following conjecture.

Conjecture 7.2.6. *If* $p \equiv 1 \mod 4$ *then* $len(a_\triangle, 0) \neq len(a_\triangle^3, 0)$.

Assuming this conjecture is true it is easy to show that our generalized conjecture about supersingularity holds.

Let $a_\triangle$ be a non residue and $p \equiv 1 \mod 4$. Assume $len(a_\triangle, 0) = p$. From Theorem 7.2.5 we know that $len(a_\triangle, 0) + len(a_\triangle^3, 0) = 2p$. So, $len(a_\triangle^3, 0) = 2p - p$. This means $len(a_\triangle^3, 0) = p$. This would contradict Conjecture 7.2.6. Thus $len(a_\triangle, 0) \neq p$ which would prove the last case for Conjecture 7.0.4.

8
Appendix: Samples of SAGE Code

We will start with some utility methods that do things like find the solutions to elliptic curves or produce $\mathbb{F}_p \times \mathbb{F}_p$ as a list tuples. These do not warrant much description.

```
def solveCurveForList(a,b,p, list):
    pointsOnCurve = [ ]
    for point in list:
        x,y = point
        if (y^2)%p == ((x^3) + a*x + b)%p:
            pointsOnCurve.append((check(x,p),check(y,p)))
    return pointsOnCurve

def check(z, p):
    r = z
    if (z > (p-1)/2):
        r = - (p-z)
    return r

def generateField(p):
    pointsInField = [ ]
    for x in range(p):
        for y in range(p):
            pointsInField.append((check(x,p),check(y,p)))
    return pointsInField

def generateCurves(p):
    curvesInField = [ ]
    for a in range(p):
        for b in range(p):
            if (4*(a^3) + 27*(b^2)) %p != 0:
                curvesInField.append((a,b))
    return curvesInField
```

```
def isNotIn(element, list):
    for i in list:
        if i == element:
            return False
    return True
```

The following method is used in Section 4.1.1 to create an upper bound based on the proof of the spanning property in Section 3.2.1.

```
def proofTechniqueUpperBound(p):
    pointsInField = generateField(p)
    curvesNeeded = [ ]
    for point in pointsInField:
        x,y = point
        if point == (0,0):
            if isNotIn((1,0), curvesNeeded):
                curvesNeeded.append((1,0))
        elif (x^3)%p != (y^2)%p:
            b = ((y^2)-(x^3))%p
            element = (0,b)
            if isNotIn(element, curvesNeeded):
                curvesNeeded.append((0, b))
        elif (x^3)%p == (y^2)%p:
            if (4 + 27*x^2)%p != 0:
                if isNotIn((1,-x), curvesNeeded):
                    curvesNeeded.append((1,(-x)%p))
            elif (-4 + 27*x^2)%p != 0:
                element = (-1, x)
                if isNotIn(element, curvesNeeded):
                    curvesNeeded.append((-1,(x)%p))
    return curvesNeeded
```

The following method is used in Section 4.1.2 to create an upper bound by the curve with the largest number of solutions to the points left uncovered.

```
def largestCurveUpperBound(p):
    pointsInField = generateField(p)
    curvesNeeded = [ ]
    unusedCurves = generateCurves(p)
    largestCurve = [ ]
    currentCurve = [ ]

    while(len(pointsInField) > 0):
        for curve in unusedCurves:
            a,b = curve
            currentCurve = solveCurveForList(a,b,p, pointsInField)
            if len(currentCurve) len(largestCurve):
                largestCurve = currentCurve
        for point in largestCurve:
            x,y = point
            pointsInField.remove((x,y))
        largestCurve = [ ]
```

```
        curvesNeeded.append((a,b))
        unusedCurves.remove((a,b))

    return curvesNeeded
```

This method and for loop discussed in Section 4.1.3 uses randomly selected curves to try and find an upper bound. It is incredibly inefficient.

```
def randomUpperBound(p):
    pointsInField = generateField(p)
    unusedCurves = generateCurves(p)
    currentCurve = [ ]
    count = 0
    curvesNeeded = 0

    while(count < p^2):
        range = len(unusedCurves)
        curve =  unusedCurves[int(random() * len(unusedCurves))]
        a,b = curve
        currentCurve = solveCurveForList(a,b,p, pointsInField)
        for point in currentCurve:
            x,y = point
            pointsInField.remove((x,y))
            count += 1
        curvesNeeded += 1
        unusedCurves.remove((a,b))
    return curvesNeeded

 for p in prime_list:
    i = 0
    bestGuess = p^2 - p
    while(i < 1000000):
        currentGuess = guessRandom(p)
        if currentGuess < bestGuess:
            bestGuess = currentGuess
        i += 1
    print bestGuess
```

9
Appendix: Brute Force for Small Primes

9.1 Equivalence of elliptic curves for $p = 5, 7$

In this section we will construct and run a SAGE to prove Theorem 2.4.2 for $p = 5, 7$. The program utilizes the methods solveCurve and generateCurves discussed in the previous chapter. The first method areEqual compares two curves and returns True if they are equivalent sets. The second method takes a prime p as input. For this fixed p it makes a list of every elliptic curve. For each curve it compares it with each other curve with a different a's or b's and checks to make sure the two curves are not equal. It prints out any two elliptic curves that have the same solution set but different a's or b's.

```
def areEqual(listOne, listTwo):
    same = True
    for point in listOne:
        if point not in listTwo:
            same = False
    for point in listTwo:
        if point not in listOne:
            same = False
    return same

def test(p):
    eCurves = generateCurves(p)
    for curveOne in eCurves:
        a,b = curveOne
        solOne = solveCurve(a,b,p)
        for curveTwo in eCurves:
            c,d = curveTwo
            if a != c or b != d:
                solTwo = solveCurve(c,d,p)
                if areEqual(solOne, solTwo):
                    print a,b, 'is the same as', c,d
```

```
    print 'Done.'
```

If our Theorem is correct then for $p = 5, 7$ the method will simply print done. Below is a graphic of this program being run in SAGE and as expected our theorem holds for $5, 7$.

```
def test(p):
    eCurves = generateCurves(p)
    for curveOne in eCurves:
        a,b = curveOne
        solOne = solveCurve(a,b,p)
        for curveTwo in eCurves:
            c,d = curveTwo
            if a != c or b != d:
                solTwo = solveCurve(c,d,p)
                if areEqual(solOne, solTwo):
                    print a,b, 'is the same as', c,d
    print 'Done.'
```

```
test(5)
```

evaluate

```
    Done.
```

```
test(7)
```

```
    Done.
```

Bibliography

[1] Joseph H. Silverman, *Rational Points on Elliptic Curves*, Springer, New York, NY, 1992.

[2] ———, *The Arithmetic of Elliptic Curves*, Springer, New York, NY, 1986.

[3] William J. LeVeque, *Fundamentals of Number Theory*, Dover Publications Inc., New York, NY, 1996.

[4] *Tutorial: Doubling the point P*, Certicom Corp, http://www.certicom.com/index.php/213-doubling-the-point-p, 2011.