Elliptic Curves

Undergraduate Thesis

Christian Testa

April 2017

advised by
George McNinch, Robert Lemke Oliver
Department of Mathematics
Tufts University

Contents

List of Figures

Acknowledgements

Working on this thesis with Professors George McNinch and Robert Lemke Oliver has been captivating, not least because of their ability to make mathematics thrilling and fun. I cannot thank them enough for the many valuable hours I have learned from them. I am grateful for many of the Tufts faculty who have helped me along the way, including the Mathematics Department professors who have kindly taught me so many fascinating and humbling subjects, Tufts Technology Services who have allowed me to run computations in SageMath on the University's cluster, and the Tufts Office of Institutional Research and Evaluation where I have worked for four years. Many of my friends have developed an expectation that my messages to them will bring plots of elliptic curves. For their great perspectives and delightful inquisitions into the subject in response, I thank all of them. Without my family's support and guidance, I would not be who I am today. For the countless ways in which I have benefitted from them I am thankful.

1 Introduction

In this thesis I will explain elliptic curves, some common vocabulary surrounding them, some popular relevant theorems and conjectures, and perform an investigation into a subject of my interest. I will begin with a short introductory chapter to the necessary vocabulary and ideas to formally state what an elliptic curve is so that the reader may always have solid grounding as we tour through elliptic curves' history in the second chapter. The third chapter of this thesis is a single page cheat-sheet to the parts of SageMath which I have found the most relevant to elliptic curves through my studies. Last, the fourth chapter is an investigation into how the infinite part of rational elliptic curves and the structure of finite field elliptic curves are interrelated. In writing this thesis, it is my hope that I can make tangible some of the mystery surrounding elliptic curves through data visualization and historical exposition. Finally, I would like to inspire the notion that even through explorative programming and heuristic arguments we may create new scientific discoveries in the world of mathematics.

Prerequisite knowledge assumed includes some familiarity with fields, polynomials, sets, calculus, and cyclic group theory. The integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, finite fields $\mathbb{F}_q$, and an arbitrary field k will make frequent appearances.

All original pictures which appear in this thesis are hosted online along with example code. Professor Drew Sutherland at MIT has kindly allowed me to use the Sato-Tate Distribution image from his website. The Wikimedia Commons is the source for another three images in this thesis, which appear in the Weierstraß Elliptic $\wp$ Function figure.

1.1 What is an Elliptic Curve?

Before we can describe an elliptic curve, we must know something about curves. Curves exist in lots of different contexts: in the cartesian plane, Euclidean space of arbitrary dimension over arbitrary fields, and a whole lot more. Further, for every field k, there are many different ways we could construct space with coordinates in k in which a curve could exist. We will consider two spaces that exist for any field k, the affine and projective spaces, before we consider the elliptic curves which exist within them.

The **affine plane over** k, denoted $\mathbb{A}^2(k)$, is the set of points in $k \times k$ for a given field k. A familiar example of affine space is Euclidean 2 or 3 dimensional space, which are denoted

here $\mathbb{A}^3(\mathbb{R})$ and $\mathbb{A}^3(\mathbb{R})$. This generalizes to affine space over k, $\mathbb{A}^n(k)$, the set of n-tuples in k.

The **projective plane** over k is given by the set of tuples

$$\mathbb{P}^2(k) = \{(x, y, z) \in k^3 | (x, y, z) \neq (0, 0, 0)\}/\sim,$$

where $\sim$ denotes the equivalence relation where $(x, y, z) \sim (x', y', z')$ if and only if there exists some scaling factor $c \neq 0$ such that $(x', y', z') = (cx, cy, cz)$.

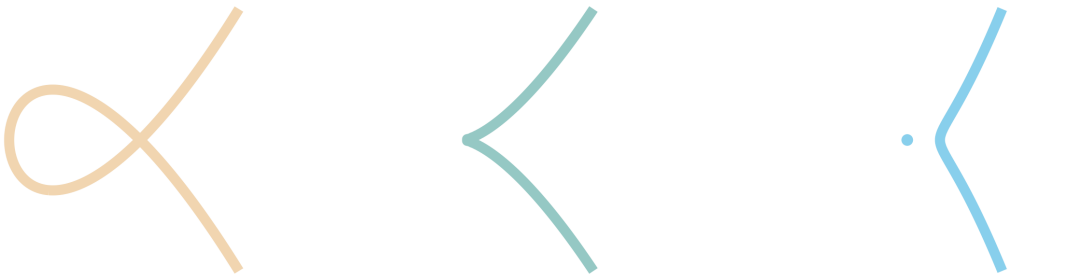
This equivalence relation can be intuitively thought of as stating that two coordinates are considered the same point in projective 2-d space if and only if the same coordinates in affine 3-d space lie on the same line through the origin.

A point on the projective plane is traditionally denoted $(x : y : z)$ since it is only the ratios between among the coordinates that determines the point. That is, the ratios $x : y$, $y : z$, and $z : x$ will remain constant regardless of the coordinate representation of the point in $\mathbb{P}^2(k)$.

An algebraic **affine plane curve** is a nonempty set of points in $\mathbb{A}^2(k)$ which are the solutions of some polynomial in two variables with coefficients in k. That is, if f is a polynomial equation $f(x, y) \colon \mathbb{A}^2(k) \to k$ then a nonempty set of points $\{(x, y) | f(x, y) = 0\}$ is an algebraic affine plane curve.

An algebraic **projective plane curve** is a nonempty set of points in $\mathbb{P}^2(k)$ which are the solutions of some homogeneous polynomial in the projective plane $f(x : y : z) \colon \mathbb{P}^2(k) \to k$ with coefficients in k.

The **degree** of an algebraic plane curve is taken to be the greatest sum of exponents on x and y in any single term of the polynomial for which the points on the curve are the solution set. A polynomial is **homogeneous** if every term of the polynomial has the same degree. This is a necessary condition a polynomial whose solution set is an algebraic curve in the projective plane must satisfy in order to be well defined with respect to the equivalence relation used to construct the projective plane.



Crunode: $y^2 = x^3 + x^2$ Ordinary Cusp: $y^2 = x^3$ Acnode: $y^2 = x^3 - x^2$

Figure 1.1: Different Kinds of Degree Three Singularities.

We say that a point on a curve is **singular** if every partial derivative vanishes. That is, if f is a curve in n dimensional space, either affine or projective, then we say that f is singular at some point if

$$\frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = ... = \frac{\partial f}{\partial x_n} = f(x_1, x_2, ..., x_n) = 0.$$

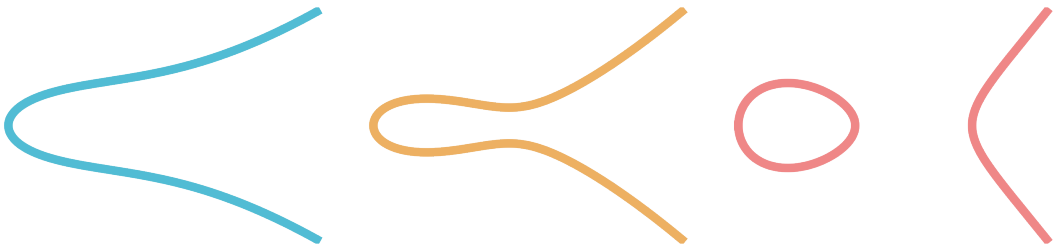
A curve is **singular** if it contains one or more singular points. Naturally, we say a curve is **nonsingular** if it contains no singular points.

Singularities come in two kinds: nodes and cusps. Each of these break down into further subcategories. For double points, the possibilities include acnodes, crunodes, and ordinary cusps, while singularities of higher multiplicity could be tacnodes and rhamphoid cusps. We will only be concerned with the former in the context of elliptic curves.

Finally, we can make the following definition.

Definition. An **elliptic curve** is a degree three nonsingular plane curve, affine or projective, with the point at infinity denoted $\mathcal{O}$.

In the affine case, the point at infinity $\mathcal{O}$ can be thought of as a symbol we pair the curve with, and the point $\mathcal{O}$ itself does not exist in the (x, y) plane over k. In the projective case, the point at infinity is simply the point where the curve intersects the line at $z = 0$. We will need this point at infinity as the identity to realize the group structure of elliptic curves.



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

Figure 1.2: Three Example Elliptic Curves

2 The History of Elliptic Curves

This chapter contains a part of the story of how elliptic curves, a seemingly simple class of equations to define, have found themselves at the forefront of modern mathematical research. The story is winding, and has roots in the very origins of algebra: Diophantus' *Arithmetica*. Progress in the 19th century on elliptic functions yielded both parametrization and geometric intuition for complex elliptic curves. The finitely generated abelian group structure for the rational points of an elliptic curve was discovered in the early 20th century. Recently, incredible progress has been made over the course of the 20th century to tie elliptic curves and modular forms together. Elliptic curves, though equationally only slightly more complicated than conics, present a rich and fascinating subtlty in their properties and incredible number of mysterious features.

Table 2.1: Timeline of Elliptic Curves.

285 a.d.	Diophantus publishes *Arithmetica*
...	
1637	Fermat states Fermat's Last Theorem
1669	Newton expresses arc-lenghts of ellipses as infinite series
1750	Euler states a group law for Elliptic Integrals
1779	Bezout's Theorem is Stated
...	Gauss, Fagnano, Bernoulli, Legendre, Jacobi, Eisenstein, Abel, and others work on elliptic functions
1862	Weierstraß Parametrizes $\wp$
1916	Ramanujan conjectures τ congruences
1922	Mordell-Weil Theorem
1933	Hasse's Bound
1973	Deligne Proves Weil's Riemann Hypothesis
1977	Mazur's Torsion Theorem
1985	Elliptic Curve Cryptography is born
1987	Lenstra's Integer Factorization Algorithm
1995	Wiles' Modularity Theorem
2006	Elkies' Discovery of a Rank ≥ 28 Curve
2006	Proof of the Sato-Tate Conjecture is Finished

2.1 Discovery and Early Ideas

Elliptic curves' history begins early, but little progress beyond Diophantus' contributions was made until 17th century and the Age of Reason when Fermat studied integer solutions to Diophantine Equations and Newton who classified the shapes of real nonsingular projective cubic curves. Some of the earliest appearances of elliptic curves lie in Diophantus' text *Arithmetica*. A problem Diophantus considered has been reworded artfully in modern language as the following [Bas97].

> To divide a given number into two numbers such that their product is a cube minus its side.

Diophantus, considered by some to be the "Father of Algebra," was principally concerned with what is today called the subject of Diophantine equations, the study of integer solutions to polynomial equations, usually with two or more variables. The elliptic curve Diophantus concieved of was the equation

$$y(a-y) = x^3 - x,$$

for which he sought nontrivial solutions (x, y) when $a = 6$, and solved with

$$(x, y) = (17/9, 26/27).$$

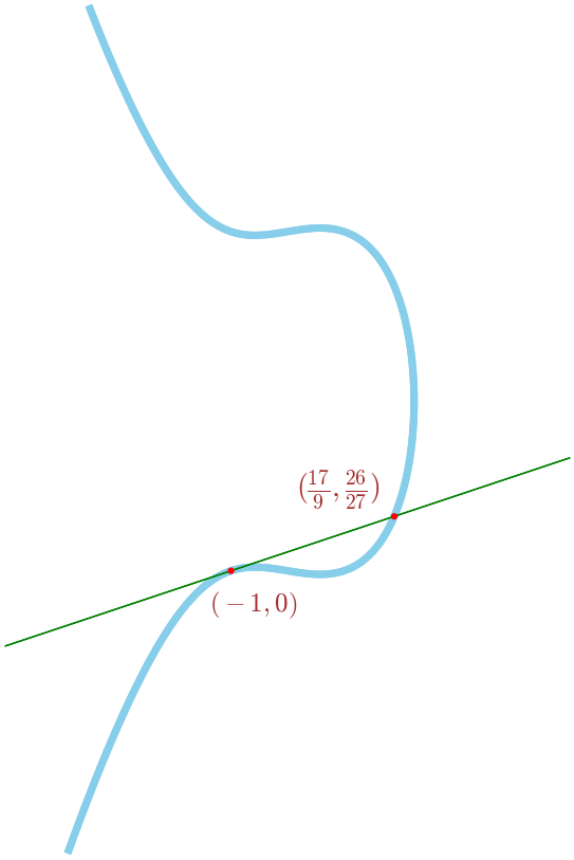


Figure 2.1: $y(6-y) = x^3 - x$

Diophantus was an early character to use the tangent and secant methods to construct points on algebraic curves. To solve this problem, he constructed the tangent line to the elliptic curve given at $(-1, 0)$, which intersected the curve once again at his desired solution.

Given Diophantus' starting point $(-1, 0)$, he constructed a point with both positive x and y which satisfied his desired criterion by using the tangent on an elliptic curve. While his work makes no explicit mention of elliptic curves as a set of curves, his methods and desire to find nontrivial rational solutions to Diophantine equations set the stage for the beginning of the relationship between number theory and elliptic curves.

2.1.1 Point Doubling

In 1621 Bachet discovered that given a rational solution $x, y \in \mathbb{Q}$ to the equation

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

then the following is also a solution

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right).$$

Early relative to other work on elliptic curves, the point doubling formula is one of the first hints of the group structure in the history of elliptic curves. Bachet had shown that given a point on $y^2 - x^3 = c$, it may be used to construct another. However this entirely was outside the modern context of "doubling" and point multiplication on elliptic curves, a much later development.

2.1.2 Newton's Consideration of Curves

In 1667 Newton began to work on classifying generic cubic curves into 72 distinct categories of polynomial structures, overlooking 6 in his study. Newton had formulated ideas beginning the study of projective curves by considering not only the intersection degree counting multiplicity but also counting points at infinity. While his proof technique was criticized by Euler for lacking unifying principle, motivation for his methods and the beginnings of projective geometry can be found in his remarks titled *On the Genesis of Curves by Shadows* where he gave the theory of perspective through rays of light casting shadows of objects onto the infinite plane. Stillwell's *Mathematics and Its History* has a section on Newton's Classification of Cubics which provides a short and very readable introduction to Newton's classification [Sti10].

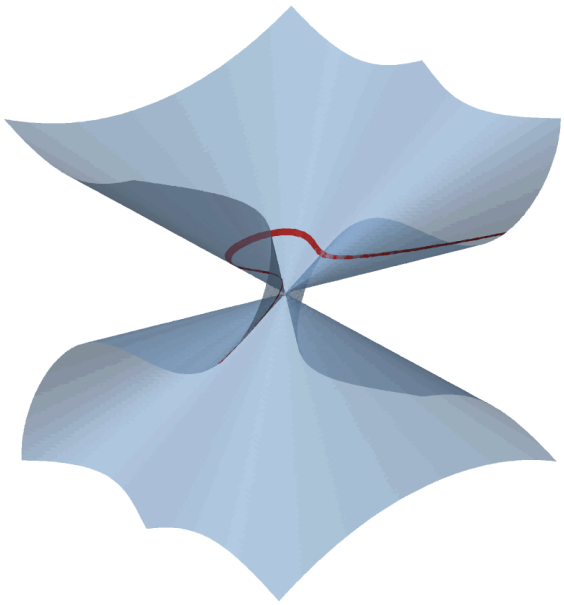


Figure 2.2:
The Cone of a Curve in $\mathbb{P}^2(\mathbb{R})$

2.1.3 Bezout's Theorem

$y^2 = x^3 + x^2 + 1$ and the line $x = 1$ $\quad$ $y^2z = x^3 + x^2z + z^3$ and $x = z$

Figure 2.3: Bezout's Theorem Illustrated

First, note that while there are only two intersections between the elliptic curve and line given in the affine plane, there are three intersections in the projective plane between the corresponding projective elliptic curve and line in the projective plane. This difference in the count of intersection numbers in affine and projective space here exemplifies the difference between the affine and projective versions of Bezout's theorem, and this distinction is a crucial theoretical step on the way to elliptic curve addition.

Theorem. If P and Q are algebraic affine plane curves given as polynomials with a constant greatest common divisor and no common polynomial component, then the number of intersection points between P and Q is bounded by the product of the degrees of the polynomials.

$$|\{(x, y) \text{ such that } P(x, y) = Q(x, y) = 0\}| \leq \deg P \cdot \deg Q$$

In volume one of *Principia*, Newton claims that two curves have a number of intersection given by the product of their degrees. However, the truth is slightly more subtle than this.

Theorem. If $P(x, y, z)$ and $Q(x, y, z)$ are algebraic projective plane curves given as polynomials with a constant greatest common divisor and no common polynomial component, then the number of intersection points between P and Q counting the multiplicity of points and the point at infinity is equal to the product of the degrees of P and Q as polynomials.

$$|\{(x : y : z) \text{ such that } P(x : y : z) = Q(x : y : z) = 0\}| = \deg P \cdot \deg Q$$

Bezout's statement of the theorem is an improvement on Newton's formulation, but it is still somewhat unlike the modern formulation and proof techniques, for which one should look to Hartshorne's Chapter 1 of *Algebraic Geometry* [Har77] or the appendix on *Projective Geometry* in Silverman and Tate's *Rational Points on Elliptic Curves* [ST15]. Proofs vary individually, but often one of the crucial concepts to the proof of Bezout's theorem is that polynomials over any field are a unique factorization domain, and so every polynomial may be uniquely factored into irreducible components.

2.1.4 Addition and Multiplication of Points

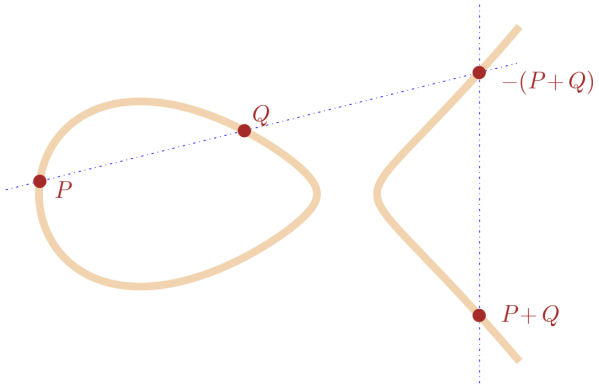


Figure 2.4: Point Addition

With Bezout's Theorem in mind, we know that there will always be three points of intersection between an elliptic curve and a line if we properly count multiplicity and the point at infinity. To make sense of the point at infinity in the affine plane, we say that the line through a point P and infinity is the vertical line through P with infinite slope. In order to ensure the existence of inverses, we construct addition such that three collinear points sum to the identity. To sum P and Q, first we construct the line through P and Q, $\overline{PQ}$. $\overline{PQ}$ intersects our elliptic curve once again by Bezout's Theorem, and we take this point to be $-(P+Q)$. Given $-(P+Q)$ and the requirement three points on a line sum to the identity $\mathcal{O}$, since $\mathcal{O}$ and $-(P+Q)$ are already on a vertical line, we take the guaranteed third point on this vertical line to be $(P+Q)$.

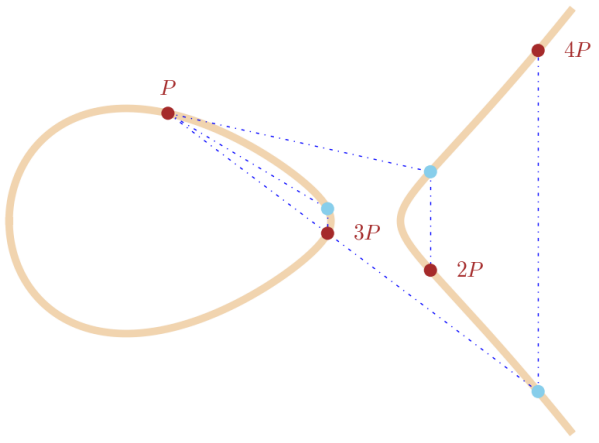


Figure 2.5: Point Multiplication

We handle the case of adding a point to itself by replacing the line through P and Q with the tangent line at P for the first step of addition. Having done so, we can multiply any

point by any integer value, since we can repeatedly add it to itself as well as always add its inverse to itself. To construct the inverse of a point P we take the line through $\mathcal{O}$ and P to find the third point $-P$.

We will later find that elliptic curve point addition defines a group operation. However, in following the historical timeline we will take a short trip through calculus and complex analysis before returning to the group structure of elliptic curves.

2.2 From Integrals to $E/\mathbb{C}$

Elliptic curves arise in diverse situations such as solving pendulum integral equations or considering the topological manifolds with one hole. The seemingly disproportionate number of contexts in which elliptic curves appear is in part what gives rise to their arithmetic's frequent appearance throughout diverse modern subjects including cryptography, integer factorization, string theory, and more. The story of how elliptic curves came to be is rooted, perhaps surprisingly, in complex analysis. We begin this section with a particular set of integrals, the elliptic integrals, and end with the parametrization of the elliptic functions, a family of complex functions through which the correspondence between embeddings of the torus into the complex projective plane and complex elliptic curves is established. The elliptic integrals are integrals with integrands given as particular rational polynomials of an argument t and the square root of another degree three or four polynomial, $\sqrt{P(t)}$. Interest in elliptic integrals comes not from their individual evaluation, but rather from how the evaluation of an elliptic integral at varying upper bounds is governed by an algebraic addition law. Elliptic integrals are then inverted to form the elliptic functions, and through elliptic functions we may begin to understand the origins of the study of complex elliptic curves. Through Weierstraß work on elliptic functions and Riemann's introduction of surfaces to the theory of complex analysis, the connection between elliptic curves and a new subject, algebraic geometry, is born.

2.2.1 Elliptic Integrals

Elliptic integrals, in their modern definition, are taken to be integrals of the form

$$\int_0^x R(t, \sqrt{P(t)}),$$

where $P(t)$ is a degree three or four polynomial which has no repeated roots. Of course, this is a modern definition and does not give an inkling to why these should be connected to elliptic curves. For that, we have to start with the work of Fagnano, Euler, Bernoulli, and others on specific elliptic integrals. After Newton's work on gravity questions like the following were being asked.

> What is the curve with the property that the time taken for a particle to traverse the curve is proportional to the distance from a fixed point. – Fagnano

Bernoulli called the solution of this problem the "paracentric isochrone", which is given by $\int_0^x 1/\sqrt{1-t^4}\,dt$.

It is from questions and integrals like from which the first notions behind elliptic integrals were constructed. Fagnano, Bernoulli, Euler, and others worked on elliptic integrals born from ideas about pendulums, lemniscates, and elasticity. These integrals which appear throughout the calculus of many subjects are in part why it is that elliptic curves have found applications in such a variety of subjects.

It was mathematicians like Euler, Legendre, Abel, and Jacobi who first discovered algebraic integral addition formulas for elliptic integrals in general. Every year, countless students encounter an algebraic integral addition formula without recognizing it.

$$\int_0^{\sin u} \frac{dx}{\sqrt{1-x^2}} + \int_0^{\sin v} \frac{dx}{\sqrt{1-x^2}} = \int_0^{\sin(u+v)} \frac{dx}{\sqrt{1-x^2}}$$

This equation has the delightful property that the upper summands, if taken as variables $y = \sin u$ and $z = \sin v$, sum according to the following algebraic integral addition formula

$$\sin(u+v) = y\sqrt{1-z^2} + z\sqrt{1-y^2}.$$

One might ask themselves what functions, similar to the integral functions of their upper bound used above, satisfy algebraic integral addition formulas? Euler discovered the addition formula for elliptic integrals of the first kind.

$$\int_0^u \frac{dx}{\sqrt{P(x)}} + \int_0^v \frac{dx}{\sqrt{P(x)}} = \int_0^{T(u,v)} \frac{dx}{\sqrt{P(x)}}, \qquad T(u,v) = \frac{u\sqrt{P(v)} + v\sqrt{P(u)}}{1-k^2u^2v^2}$$

where $P(x) = (1-x^2)(1-k^2x^2)$ for a k such that $0 < k < 1$.

Legendre subsequently studied the first, second, and third kinds of elliptic integrals and their addition formulas.

$$\int \frac{dx}{\sqrt{1-x^2}\sqrt{1-l^2x^2}}, \qquad \int \frac{x^2dx}{\sqrt{1-x^2}\sqrt{1-l^2x^2}}, \qquad \int \frac{dx}{(x-a)\sqrt{1-x^2}\sqrt{1-l^2x^2}}.$$

For a light introduction to elliptic integrals, *A Brief History of Elliptic Integral Addition Theorems* [Bar09] and *The Lemniscate and Fagnano's Contributions to Elliptic Integrals* [Ayo84] are wonderful historical and technical narratives of beautiful born out of early integral calculus.

2.2.2 Elliptic Functions

The elliptic functions were discovered to have a unifying feature: double periodicity. Likening the elliptic integrals to trigonometric integrals, the inversion relationship given by

$$\omega(u) = \int_0^u \frac{dx}{\sqrt{1-x^2}}, \qquad \sin(\omega(u)) = u$$

motivated Abel, Jacobi, and others to consider the functions defined by similar relationships

$$\omega(\phi) = \int_0^\phi \frac{dt}{\sqrt{1-k^2\sin^2 t}}, \qquad \operatorname{sn}(\omega(\phi)) = \sin\phi,$$

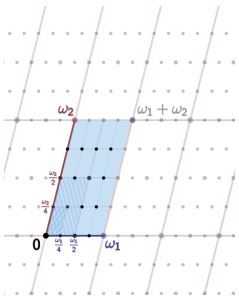
$$\operatorname{cn}(\omega(\phi)) = \cos\phi, \qquad \operatorname{dn}(\omega(\phi)) = \sqrt{1-k^2\sin^2\phi}.$$

These are our first examples of elliptic functions, which are now defined as the inverse functions of elliptic integrals. These functions not only extend to complex functions, but also have algebraic addition formulas such as

$$\operatorname{sn}(\omega+\eta) = \frac{\operatorname{sn}\omega\operatorname{cn}\eta\operatorname{dn}\eta + \operatorname{sn}\eta\operatorname{cn}\omega\operatorname{dn}\omega}{1-k^2\operatorname{sn}^2\omega\operatorname{sn}^2\eta}.$$

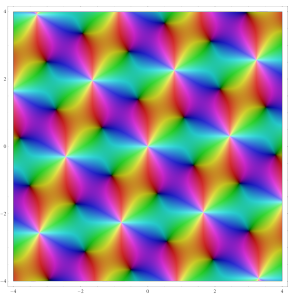
Stillwell also tells the story of elliptic functions in a chapter of his *Mathematics and its History* [Sti10] Lang's book on *Elliptic Functions* is an advanced reference [Lan87].

2.2.3 Weierstraß' $\wp$



Four-torsion points of $\mathbb{C}/\Lambda$

Weierestraß' stylized p



A complex graph of $\wp(z)$

Figure 2.6: Weierstraß' Elliptic $\wp$ Function
images above from Wikimedia Commons.

Before we may begin with Weierstraß' theory, we will need lattices. Here, lattices will be denoted Λ and are all the integer coefficient linear combinations of ω_1 and ω_2 for some ω_1 and ω_2 which cannot be expressed as $\mathbb{R}$-multiples of one another, i.e. $\omega_1 \neq c\omega_2 \forall c \in \mathbb{R}$.

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}.$$

Next, we define two constants associated to a lattice, g_2 and g_3, constructed from the Eisenstein series which Weierstraß used to define his $\wp$ function. Here, lattices will be denoted Λ and are all the integer coefficient linear combinations of ω_1 and ω_2 for some ω_1 and ω_2 which do not divide one another.

$$g_2(\omega_1, \omega_2) = 60 \sum_{(m,n)\neq(0,0)} (m\omega_1+n\omega_2)^{-4} \quad \text{and} \quad g_3(\omega_1, \omega_2) = 140 \sum_{(m,n)\neq(0,0)} (m\omega_1+n\omega_2)^{-6}$$

Often we normalize lattices in the complex plane such that the generating set is $\{1, \omega_2/\omega_1\}$ when ω_1 is not already 1. With the definition for Eisenstein series $G_{2k}(\omega_1, \omega_2)$ as functions of ω_1 and ω_2 already used above in the definitions of g_2 and g_3, here the definition in a single variable τ from the upper half plane is given as a sum over nonzero integer pairs.

$$G_{2k}(\tau) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}^\times} \frac{1}{(m+n\tau)^{2k}}.$$

For Weierstraß' theory, the foundation of elliptic functions comes from the following functions' relationship.

$$\wp^{-1}(z, g_2, g_3) = \int_\infty^z \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}},$$

$$\wp(z, \omega_1, \omega_3) = \frac{1}{z^2} + \sum_{n^2+m^2\neq 0} \frac{1}{(z+m\omega_1+n\omega_2)^2} - \frac{1}{(m\omega_1+n\omega_2)^2},$$

The sum in the definition of $\wp$ is over n and m integers and $\wp$ is defined for $z \in \mathbb{R}$ and $4z^3 - g_2 z - g_3 > 0$. While this inverse relationship holds for $z \in \mathbb{R}$, $\wp$ can be taken as a complex function dependent on $z, \omega_1, \omega_2 \in \mathbb{C}$, where ω_1 and ω_2 are the periods of each of the two distinct directions in the complex plane for which the first integral is periodic.

By construction, $\wp$ and its derivative $\wp'$ are themselves elliptic functions. However, they are very special elliptic functions. Weierstraß showed that all elliptic functions could be expressed as complex rational functions of $\wp$ and its derivative. Further, the $\wp$ function satisfied the following differential equation.

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp - g_3.$$

To exactly classify the elliptic functions, we need to know about meromorphicity, the condition that a function of complex arguments have only removable singularities and otherwise derivatives exist everywhere. Elliptic functions are are in fact equivalent to complex elliptic curves. They were first discovered as the the doubly periodic meromorphic functions, but were then parametrized by the Weierstraß $\wp$ function and its derivative, satisfying the given differential equation. Through this last step, the new equivalence between equations of the form $y^2 = x^3 + ax + b$ and the field of meromorphic functions doubly periodic with respect to a particular lattice is established.

One reference which tells the story from elliptic integrals to the parametrization of elliptic functions is Hancock's *Lectures on the theory of elliptic functions* [Han58].

2.2.4 $E/\mathbb{C}$ as a Torus

$$\{\text{Elliptic Curves over } \mathbb{C}\} \cong \{\mathbb{C}/\Lambda\}$$

When considering the image of a complex argument z under the map $\wp$ for some lattice, z's image is doubly periodic. $\wp(z + \omega_1) = \wp(z + \omega_2) = \wp(z)$. Edges of the lattice are identified and the topology of a torus is the result. That is, $\wp$ is perfectly well defined as a function $\wp : \mathbb{C}/\Lambda \to \mathbb{C}$, rather than as a function on the entire complex plane.

For any curve over a base field with specified characteristic, any elliptic curve can be parametrized into a normal form with a formula given as follows and only a single point where $z = 0$, given as the single point at infinity $\mathcal{O} = (0 : 1 : 0)$. The first of these normal forms is called a Weierstraß equation.

E: $y^2 = x^3 + ax + b$ for fields of characteristic not 2 or 3.

E: $y^2 + a_1xy + a_3y^2 = x^3 + a_2x^2 + a_4x + a_6$ for fields of characteristic = 2,3

A field having characteristic k simply refers to the field having k as the smallest integer which satisfies $1 \cdot k = 0$. In a finite field $\mathbb{F}_q$ the characteristic of the group is the prime p such that $q = p^n$. If no such integer exists, we say that a field has characteristic 0.

With Weierstraß parametrization for elliptic curves and elliptic functions in hand, the elliptic curves over $\mathbb{C}$ had been parametrized through the $\wp$ function's differential equation, which is in turn parametrized with respect to a torus given as $\Lambda = \mathbb{Z}\omega_1 \times \mathbb{Z}\omega_2$. This not only introduces the geometric notion of arithmetic genus, the number of holes in the complex solution space to elliptic curves, but establishes an equivalence between complex elliptic curves and genus one curves.

Having the normal forms in hand, we can define the discriminant Δ and j-invariant, which respectively measure whether or not a curve is singular and the isomorphism class of an elliptic curve in an algebraically closed field.

When an elliptic curve can be made isomorphic to one of the form $E\colon y^2 = x^3 + ax + b$ we construct the Δ discriminant and j-invariant like so

$$\Delta(E) = 4a^3 + 27b^2, \qquad j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

$\Delta(E) = 0$ implies that E is singular, and $j(E) = j(E')$ if and only if E and E' are isomorphic over the algebraic closure of k, the base field for the elliptic curve.

The discriminant is a quantity we can associate to a polynomial which measures when the roots of the polynomial are equal, and in the more general definition can be expressed including a $\Pi_{i\neq j}(r_i - r_j)$ term, where the product is over all roots in the algebraic closure of the base field. If two or more roots $x^3 + ax + b$ are equal in the algebraic closure, then both this product expression and the discriminant formula taken as $4a^3 - 27b^2$ both become zero, and we know that the curve $y^2 = x^3 + ax + b$ is singular.

The discriminant and j-invariant can also be defined for elliptic curves over fields of arbitrary characteristic, and while there are certainly ideas worth considering in how these formulas came to be, we will refer the reader with continued interest in these functions to [Sil86]

The Weierstraß equation, the discriminant, and the j-function associated to elliptic curves required the development of a thorough understanding of elliptic integrals, advancements in complex analysis, and now connections through the theory of Riemann surfaces to topology. The early appearance of elliptic integrals and elliptic functions in the theory of analysis are just the beginning of elliptic curves and analysis' relationship. However, moving into late 19th century, Galois' work had been posthumously published and algebraic headway was imminent.

2.3 Rational Elliptic Curves $E/\mathbb{Q}$

$$E(\mathbb{Q}) \cong \text{Torsion} \times \mathbb{Z}^r$$

The rational points of elliptic curves, while a subject of early fascination, have only just begun to be understood. Their structure as a group is an early 20th century result, and yet we still do not know how large the infinite structure of a rational elliptic curve could be. Faltings showed that curves of genus one, equivalently the elliptic curves, were distinct from curves of all other genus in that they could have either finitely or infinitely many rational points. This section introduces three major theorems exposing the subtlty of the structure of the rational points of elliptic curves.

Fermat's method of descent, a theme to both the Mordel-Weil Theorem and Fermat's work, is presented next. Before modern investigation of the rational points of elliptic

curves, ideas surrounding Fermat's descent inspired intrigue in the subject and which began to shed light on the subtlty of elliptic curves' structure. There are few equations which inspire more intrigue than the Fermat curves, and their connection to elliptic curves through both the Mordell-Weil Theorem and Wiles' proof of Fermat's Last Theorem is another feature of the subject at which we may marvel.

Definition. A group is a set G with a binary operation $\cdot$ with the following properties

i. There exists an identity, 1, such that $1 \cdot g = g \cdot 1 = g$ for every g in G.

ii. Inverses exist for every element such that $g^{-1}g = gg^{-1} = 1$ for every g in G.

iii. The group operation is associative such that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$.

iv. The group is closed under $\cdot$ such that $a \cdot b \in G$ for all $a, b \in G$.

v. A group is abelian if $a \cdot b = b \cdot a$ for all $a, b \in G$.

vi. A group is finitely generated if for some finite subset $S \subseteq G$ every element in G can be written as a word in the elements of S.

While group structure is a natural notion under a modern algebraic inspection of the results of Bezout's theorem in the context of elliptic curves, the language of groups is a relatively recent invention, and not something known to mathematicians in the 17th and 18th centuries. The associativity property required for a group, namely that $(a + (b + c))$ and $((a+b)+c)$ are equal for any choice of a, b, c in the group, was not shown for points on elliptic curves until 1886 when the Cayley–Bacharach theorem was proven, which states that two projective degree three cubics which intersect in 8 points also intersect at a 9th point [EGH96].

The conditions of a group being finitely generated and abelian are quite strong: the fundamental theorem of finitely generated abelian groups states that such groups are direct products of cyclic groups, including $\mathbb{Z}/n\mathbb{Z}$ for any $n \in \mathbb{Z}$, and $\mathbb{Z}$ itself. Such groups are composed of finite cyclic subgroups, together called the torsion subgroup, and a finite number of infinite cyclic subgroups, together called the free part.

2.3.1 Fermat's Descent

Fermat's Last Theorem can be interpreted as the statement that neither

$F_n : x^n + y^n = z^n$ in projective coordinates, nor

$F_n : x^n + y^n = 1$ in affine coordinates

have nontrivial solutions $(x, y > 0)$ for $n \geq 3$. Fermat's conjecture and his claim of proof in the margin of his copy of Diophantus' *Arithmetica* is a part one of the most famous stories in mathematics, but a less well known part of this story is that he truly had proven his conjecture for F_4, also in the margin of *Arithmetica*.

First, we will need Diophantus' parametrization of all rational primitive Pythagorean triples.

Definition. A triple (a, b, c) is a primitive Pythagorean triple if $a^2 + b^2 = c^2$ and the greatest common divisor of a, b, and c is 1.

Theorem. Let m and n be two relatively prime natural numbers such that $m - n$ is positive and odd. Then $(m^2 - n^2, 2mn, n^2 + m^2)$ is a primitive Pythagorean triple, and every primitive Pythagorean triple can be constructed this way.

Now we may easy demonstrate Fermat's Last Theorem for F_4 using a simple contradiction argument.

Theorem. F_4 has no nontrivial solutions.

Proof. If $x^4 + y^4 = z^4$ had solutions, then $x^4 + y^4 = z^2$ has solutions. If $x^4 + y^4 = z^2$ had solutions with x, y positive integers, then there would be a minimal solution with z minimal (x, y, z) from which we will be able to find a secondary triple (a^2, b^2, c) contradicting the minimality assumption describing our original solution. First, we apply Diophantus' parametrization of primitive Pythagorean triples to (x, y, z) to yield

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad z = m^2 + n^2.$$

This forms another primitive Pythagorean triple, given by (x, n, m). Again, we can use Diophantus' parametrization to find

$$x = t^2 - s^2, \qquad n = 2ts, \qquad m = t^2 + s^2.$$

In order for this triple and the original triple to be primitive, s and t must have no common factor, and so we can deduce from $y^2 = 2mn = 4st(s^2 + t^2)$ that

$$s = a^2, \qquad t = b^2, \qquad c^2 = t^2 + s^2 \qquad \text{for some } c$$

Finally, we may compute the following

$$z = m^2 + n^2 = (t^2 + s^2)^2 + 4t^2s^2 = (a^4 + b^4) + 4a^4b^4 > (a^4 + b^4)^2 = c^2.$$

With this inequality, we establish that the triple (a^2, b^2, c) contradicts the minimality assumption made with respect to (x, y, z). □

This proof comes from a section in the 6th chapter on a *Proof of Mordell's Finite Generation Theorem* Husemöller's book *Elliptic Curves* [Hus04].

2.3.2 Mordell-Weil Theorem

$$E(\mathbb{Q}) \cong \underbrace{E(\mathbb{Q})_{\text{Tors}}}_{\text{a finite subgroup}} + \underbrace{\mathbb{Z} + \mathbb{Z} + \cdots + \mathbb{Z}}_{r<\infty \text{ times}}$$

In 1922, Louis Mordell proved that an the group of rational points on an elliptic curve over $\mathbb{Q}$ is a finitely generated abelian group.

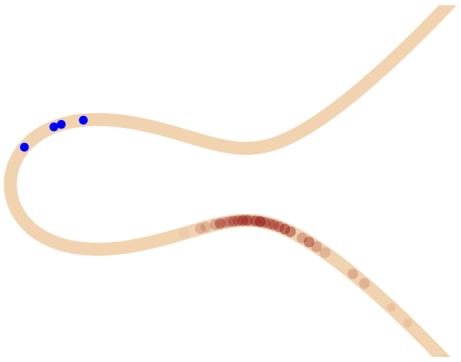


Figure 2.7: An Elliptic Curve with 4 Free Generators

The proof of this is dependent upon four lemmas. To explain the meaning of these lemmas, we require the notion of a height of a point $h(P)$, which is taken as the logarithm of the greater of the absolute values of the numerator and denominator of the x coordinate, such that if $P(x, y) = (m/n, y)$ then $h(P) = \log(\max(|m|, |n|))$. The first lemma is a statement that the elliptic curves points which have height under some bound is a finite set. The second lemma states that point addition yields a point with height bounded above in a way dependent on the original points. The third lemma states that point doubling yields a point of four times the height, with some adjustment. The fourth is a weak finite basis theorem stating that the points which are doubles of others, $2E(\mathbb{Q})$, make up a subgroup with finite index in $E(\mathbb{Q})$. Finally, taking the last and prior lemmas together, we are able to argue that we may always make the descent to a set from which all other rational points of an elliptic curve can be generated. The proof of this is subtle, algebraic, and motivated not least by Fermat's descent. For the details, we refer readers to Silverman and Tate's *Rational Points on Elliptic Curves* [ST15] and Silverman's *The Arithmetic of Elliptic Curves* [Sil86].

Lemma 1. Given an elliptic curve E, for every real number M the set

$$\{P \in E(\mathbb{Q}) : h(P) \leq M\} \text{ is finite.}$$

Lemma 2. Given P_0 a point in $E(\mathbb{Q})$, there is a constant such that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \text{ for all } P \in E(\mathbb{Q}).$$

Lemma 3. There is a constant κ, depending on E, such that

$$h(2P) \geq 4h(P) - \kappa \text{ for all } P \in E(\mathbb{Q}).$$

Lemma 4. The index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ is finite.

The Mordell-Weil theorem was originally posed by Poincaré in 1908, and later generalized by André Weil in his dissertation to higher genus curves to demonstrate that an abelian variety over a number field is a finitely generated abelian group.

2.3.3 Nagell-Lutz Theorem

Given a rational elliptic curve E and its discriminant $\Delta(E)$, if $P = (x, y)$ is a torsion point, i.e. a point of finite order such that $nP = \mathcal{O}$ for some integer $n < \infty$, then x and y are integers and either $y = 0$ or y^2 divides $\Delta(E)$.

It is remarkable that given an abstract point assumed to be torsion, we know that it will have integer coordinates. However, the converse is not true. Given a point with integer coordinates, it need not be a torsion point.

2.3.4 Mazur's Theorem

Mazur's Theorem states that for any rational elliptic curve, its torsion subgroup is one of the fifteen following groups.

$$\mathbb{Z}/n\mathbb{Z}, \text{ where } 1 \leq n \leq 10 \text{ or } n = 12, \text{ or}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \text{ where } n \in \{2, 4, 6, 8\}.$$

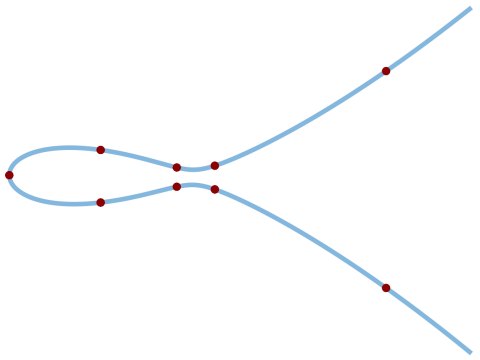


Figure 2.8: An Elliptic Curve with $E(\mathbb{Q})_{\text{Tors}} \cong \mathbb{Z}/10\mathbb{Z}$

While the torsion part of elliptic curves is relatively well understood, the free infinite part of some rank, that part which is isomorphic to $\mathbb{Z}^r \cong E(\mathbb{Q})/E(\mathbb{Q})_{\text{Tors}}$, remains mysterious. It is a topic of many conjectures, which investigate ideas including the the distributions of ranks r, the maximum possible value of r, and other seemingly simple yet unanswered questions.

Brown and Myers article *Elliptic curves from Mordell to Diophantus and back* is certainly recommended reading for an introduction to the algebraic structure of rational elliptic curves [BM02]. Additionally, Silverberg's Ranks Cheat Sheet is a brief and dense introduction to both known theory and unproven conjectures surrounding the rank of rational elliptic curves [Sil13].

2.4 Elliptic Curves over Finite Fields $E/\mathbb{F}_q$

While elliptic curves' rational points may still yet be mysterious, tremendous work and progress have resulted from the investigation of elliptic curves over finite fields. There are strict bounds known with regards to the size of finite field elliptic curves. L-series are one way mathematicians try to understand the size of embeddings of an elliptic curve into all the finite fields, and the relationship between L-functions and the algebraic rank of an elliptic curve remains one of the most significant problems in mathematics. They are not just theoretically fascinating, but have found applications in cryptography and

integer factorization. In the early 21st century, finite field elliptic curve based cryptography is everywhere around us. Finite field elliptic curves certainly have been subject to increadible headway in the past century. Nonetheless, they will continue to be the subject of mathematical intrigue for a long time to come.

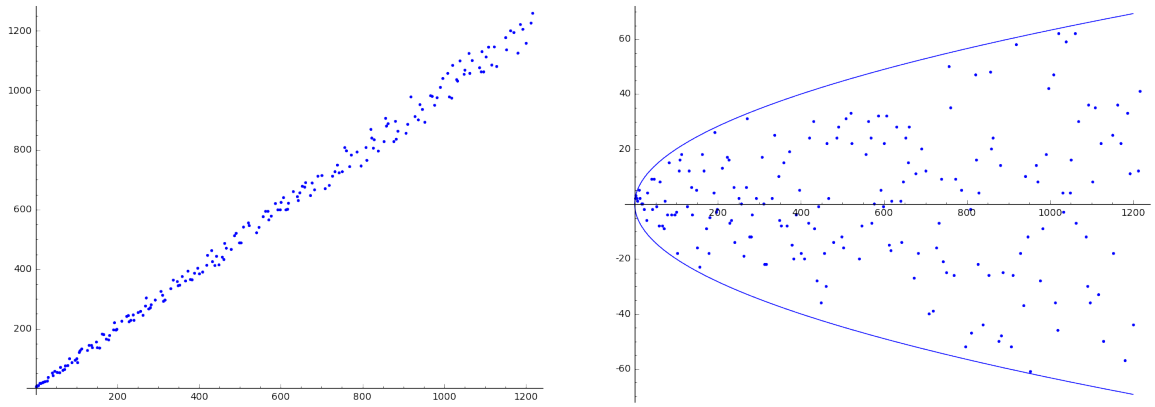
The order of any finite field $\mathbb{F}_q$ is a positive integer power n of some prime number p such that $q = p^n$. While each of them may be finite, what they make up for in size is number: since there are infinitely many primes there are infinitely many finite fields for which we can consider elliptic curves.

Definition. A finite field elliptic curve $E/\mathbb{F}_q$ is a degree three plane curve with $\Delta(E) \neq 0$ in $\mathbb{F}_q$. We denote the number of points on a finite field elliptic curve by $|E(\mathbb{F}_q)|$.

2.4.1 Hasse's Bound

It is incredible how well we can explain the bounding on the size of finite field elliptic curves. For any elliptic curve, the number of points in a finite field with q elements is approximately $q + 1$ within an error of $\pm 2\sqrt{q}$.

$$|E(\mathbb{F}_q)| - (q+1) \leq 2\sqrt{q}$$



$(p, |E(\mathbb{F}_p|)$ $(p, |E(\mathbb{F}_p)| - p - 1)$

Figure 2.9: A graph of $E(\mathbb{F}_p)$ and its normalization

2.4.2 Sato-Tate Theorem

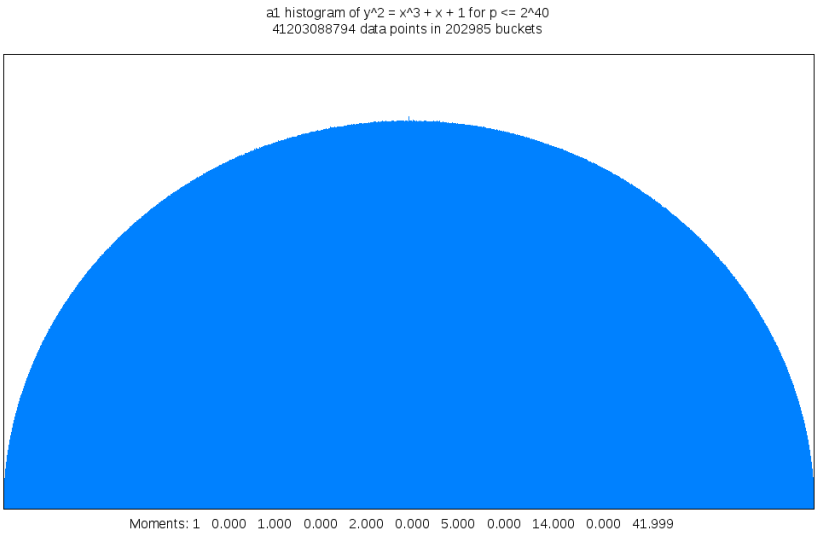


Figure 2.10: A Sato-Tate Distribution for $y^2 = x^3 + x + 1$

The above plot was produced as part of Kedlaya and Sutherland's work on *Computing L-series of Hyperelliptic Curves* and its associated software package smalljac [KS08]. Notably the odd statistical moments are converging to the Catalan numbers, a combinatorially derived sequence which seems a long way from home here.

It was conjectured in the early 60s that the distribution of the size of certain finite field elliptic curves normalized by the size of the field + 1 were distributed in a very particular, nearly semicircular, way. The proof of the Sato-Tate theorem was recently announced in 2006. For an introduction to this subject, Mazur's paper *Finding Meaning In Error Terms* is a friendly starting point [Maz08]. First, we construct the error term from the normalization.

$$a_p = p + 1 - N_p \text{ where } N_p = |E(\mathbb{F}_p)|$$

Then define θ_p to solve

$$p + 1 - N_p = 2\sqrt{p}\cos\theta_p.$$

If E be an elliptic curve without complex multiplication (a property an elliptic curve has when it has an endomorphism ring larger than the integers), then for every two real numbers α and β for which $0 \leq \alpha < \beta \leq \pi$,

$$\lim_{N\to\infty} \frac{\#\{p \leq N : \alpha \leq \theta_p \leq \beta\}}{\#\{p \leq N\}} = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2\theta d\theta.$$

This yields the semicircle in the limit, illustrated in the plot above.

2.4.3 The Birch and Swinnerton-Dyer Conjecture

While the modern formulation of the Birch and Swinnerton-Dyer Conjecture is much more technical than the details presented here, it is born out of a simpler conjecture relating the analytic rank of an elliptic curve's L-series to its algebraic rank, denoted before as r.

An elliptic curve's L-series is given in terms of its Weierstraß equation and information about the reduction of the curve at each prime. Given an elliptic curve, we may find that the discriminant is nonzero in $\mathbb{Q}$ but zero in a finite field. An elliptic curve has good reduction at p if its reduction into $\mathbb{F}_p$ is a nonsingular curve. If the reduction has a cusp, we call this additive reduction, and likewise for a node we call this multiplicative reduction. If a curve has multiplicative reduction at p, and if the slopes of the tangent lines to the node in the algebraic closure are also in $\mathbb{F}_p$ we call this split multiplicative reduction, and non-split otherwise. First, we define the local part of the L-series at p, and then we define an elliptic curve's L-series as an infinite product of these parts.

$$L_p(T) = \begin{cases} 1 - a_p T + pT^2 & \text{if } E \text{ has good reduction at } p, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ 1 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

$$L(E, s) = \prod_p \frac{1}{L_p(p^{-s})},$$

At the heart of the Birch and Swinnerton-Dyer conjecture is the idea that an elliptic curve's analytic rank, the order of vanishing at one for its L-function, is equal to the algebraic rank, the degree of the infinite cyclic part. Similar to Riemann's famous zeta function, the subject of another Millenium Prize Problem, the L-series of an elliptic curve has an analytic continuation to the entire complex plane. It is this analytically continued L-series which not only is the subject of Birch and Swinnerton-Dyer's conjecture, but the subject of attention considered in conjectures such as the parity and root-number conjectures.

2.4.4 Lenstra's Factorization Algorithm

Lenstra's factorization algorithm is a sub-exponential algorithm for integer factorization and while it is the third fastest (behind the multiple polynomial quadratic sieve and general number field sieve methods) for general purpose factoring, it is the fastest method for factoring out prime factors less than 20 to 25 digits. Its performance for small integers is not nearly as competitive as using a database lookup, but for many integers Lenstra's algorithm is presently the fastest known option. Pomerance's paper *A Tale of Two Sieves* in the Notices of the AMS is a historical narrative of progress in integer factorization

methods [Pom96]. Naturally since integer factorization is so closely related to primality, it is a subject of great interest to number theorists and resources like *Prime Numbers, A Computational Perspective* by Crandall and Pomerance exist [CP05]. Integer factorization is one of many subjects encompassed within computational number theory.

Lenstra's factorization algorithm likens finding divisors of a number n within the group structure of $\mathbb{Z}/n\mathbb{Z}$ as multiplicatively non-invertible elements to finding points on an elliptic curve modulo n for which addition fails to be possible. Addition can fail to be possible when the slope of the line intersecting two points contains a non-invertible element modulo n in the denominator. For the details and a more careful explanation, Section 4.4 in [ST15] exposits the subject well. With slight alteration, the following table describing Lenstra's algorithm also comes from Silverman and Tate.

0.	Let $n \geq 2$ be a composite integer to be factored.
1.	Check that $\gcd(n, 6) = 1$ and that n is not a perfect power.
2.	Choose random integers b, x_1, and y_1 modulo n.
3.	Set $P = (x_1, y_1)$ and $c = y_1^2 - x_1^3 - bx_1 \pmod{n}$.
4.	Let E be the elliptic curve $E : y^2 = x^3 + bx + c$.
5.	Repeat Step 6 through 9 for $d = 2, 3, 4, \ldots$ up to a specified bound.
6.	Compute $Q = dP \pmod{n}$ and set $P = Q$.
7.	If the computation of Step 6 fails then we have found a divisor, $g = \gcd(x(Q) - x(P), n)$.
8.	If $g < n$, then we find g is a factor of n.
9.	If $g = n$, go back to step 2 and pick a different curve and point.
10.	If all factors have not yet been found, go back to step 2 and try again.

Table 2.2: Lenstra's Factorization Algorithm

2.4.5 Elliptic Curve Cryptography

The discrete logarithm problem is one which is hard, and that is why it is found in the foundations of RSA cryptography. The guaranteed difficulty of this problem and related ones is what is used to ensure the security of encrypted communications in many modern and recent cryptography schemes.

Definition. The Discrete Logarithm Problem. Given $b \pmod{p}$ and $b^n \pmod{p}$, find n. Equivalently, compute $\log_b(a)$ for $a, b \in \mathbb{Z}/p\mathbb{Z}$.

To find such a number, some arithmetic must be done, and thus given b it is measurably difficult to back out its factors.

Elliptic curve cryptography is based on a similar idea.

Definition. Elliptic Curve Discrete Logarithm Problem. Given a point P and another point Q on an elliptic curve, find n such that $nQ = P$.

While elliptic curves may have been the subject of mathematicians' intrigue for centuries, their utility has only recently become widely available through algorithms implemented at massive scale. Koblitz and Miller suggested elliptic curve cryptography in 1985, and since 2004 to 2005 elliptic curve crypotography has become a popular standard.

2.5 Modular Forms

Modular forms capture endless attention from number theorists. They are not only considered a beautiful subject, but also one which connects areas and subjects within mathematics in unanticipated ways. Connections which include everything from Diophantine equations, complex analysis, representation theory, class field theory, number theory, and more appear simultaneously within the theory of modular forms. The relationship between elliptic curves and modular forms is one of many profound insights in mathematics into just how interconnected the abstract world is.

The Eisenstein series $G_{2k}(\tau)$, j-function, and the discriminant Δ previously introduced are examples of modular forms. Modular forms are complex functions satisfying certain symmetry requirements under the action of a particular matrix group. To define a modular form, we again will need a concept from complex analysis: holomorphy. A function is holomorphic if its derivative exists everywhere in the complex plane.

Definition. A modular form of weight k for the modular group

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a,b,c,d \in \mathbb{Z},\ ad-bc=1 \right\}$$

is a complex-valued function f on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$, satisfying the following three conditions:

- f is a holomorphic function on $\mathbb{H}$.
- For any $z \in \mathbb{H}$ and any matrix in $\mathrm{SL}(2,\mathbb{Z})$, we have: $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$
- f is required to be holomorphic as $z \to i\infty$.

The discriminant and j-invariant may also be expressed as follows.

$$\Delta(z) = g_2^3 - 27g_3^2, \qquad j(z) = 1728\frac{g_2^3}{\Delta},$$

The Eisenstein series, Δ, and the j-invariant are taken here to be functions of the complex upper half plane in a single argument $z \in \mathbb{H}$, just as if the lattice had been normalized to have 1 as a generating number.

Ramanujan first saw that the discriminant Δ should be expressed as an infinite product in terms of $q = e^{2\pi i\tau}$. The discriminant can be rewritten as a product expression, and

Ramanujan used this to define the τ function as the nth coefficient in the Fourier series expansion of Δ.

$$\Delta(\tau) = (2\pi)^{12} q \prod_{r=1}^{\infty} (1 - q^r)^{24}.$$

$$\Delta(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n.$$

The following are three famous conjectures by Ramanujan on the properties of τ:

- $\tau(mn) = \tau(m)\tau(n)$ if $\gcd(m, n) = 1$.
- $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$ for p prime and $r > 0$.
- $|\tau(p)| \leq 2p^{11/2}$ for all primes p.

Each these were later proven. The third required Deligne's proof of the Riemann Hypothesis for abelian varieties over finite fields, and in particular elliptic curves over finite fields. The Riemann Hypothesis for abelian varieties over finite fields is one part of the Weil Conjectures, which included the conjectures that local zeta functions should be rational functions, should satisfy a functional equation, and should have zeroes lying on a critical line.

For further reference on modular forms, the textbooks *Introduction to Elliptic Curves and Modular Forms* by Koblitz and *A first course in Modular Forms* by Diamond and Shurman are both excellent resources.

2.5.1 Modularity Theorem

Undoubtedly, Fermat's Last Theorem is one of the most famous stories known to non-mathematicians and mathematicians alike, yet its proof's impact extends far beyond Fermat's family of curves. While Andrew Wiles and others' work to prove Fermat's conjecture contains a large number of details which are specific techniques not easily applied to similar problems, the Modularity Theorem is a correspondence established between rational elliptic curves and an incredibly distant seeming subject, modular forms, which will continue to shape research in elliptic curves for many years to come.

2.5.2 MacDonald's Equation

If taking the author's word for the beauty of modular forms sits uneasily with the reader, I offer the following formula as evidence. This formula is due to MacDonald and was included in a lecture by Dyson in 1972 titled *Missed Opportunities* in which Ramanujan's τ function is expressed in a most beautiful way.

$$\tau(n) = \sum \frac{(a-b)(a-c)(a-d)(a-e)(b-c)(b-d)(b-e)(c-e)(d-e)}{1!2!3!4!},$$

summed over all sets of integers a, b, c, d, e, with

$$\begin{aligned} a, b, c, d, e &= 1, 2, 3, 4, 5 \pmod 5, \\ a + b + c + d + e &= 0, \\ a^2 + b^2 + c^2 + d^2 + e^2 &= 10n. \end{aligned}$$

2.6 On the Present

As algebraic geometry, number theory, and all other subjects of mathematics have been conjured into their intricate modern forms, so too have elliptic curves become an intricate and subtle subject. They are connected to analysis, algebra, topology, and number theory. Their properties, group law and others, appear behind the scenes throughout society, not only in the calculus students' homework problems, but in the security of modern communication. Many problems, conjectures, and questions remain to be solved, but the utility, subtlty, and significance of elliptic curves have been firmly established and are here to stay.

3 Introduction to Elliptic Curves in SageMath

I would suggest that anybody interested in computational mathematics try out SageMath. The proximity of the language to Python makes it easy to pick up, and there are wonderful libraries like numpy, pandas, and matplotlib which make working with data in SageMath a delight. To get help in Sage, I use ?, help, dir, and the inspect module's getsource function. For example, `EllipticCurve?` will return Sage documentation pages for the elliptic curve constructor. Help returns Python object documentation, dir returns a Python object's list of methods, and getsource let's you take a look at a Python method's source code.

```
We can use the EllipticCurve constructor in a
variety of ways. Using LMFDB or Cremona's labels,
through a-invariants (long or short), polynomially,
or by the j-invariant are all options.
E = EllipticCurve('496a1')
E = EllipticCurve([0, 0, 0, 1, 1])
E = EllipticCurve([1,1])
var('x y'); E = EllipticCurve(y^2 == x^3 + x + 1)
E = EllipticCurve_from_j(6912/31)
Elliptic Curve defined by y^2 = x^3 - x
over Rational Field

Point arithmetic works great!
E(1,0) + E(2,2)
(1 : -1 : 1)
2*E(2,2)
(21/25 : -56/125 : 1)

Any commutative ring may be used to construct
elliptic curves.
R.<a> = PolynomialRing(QQ, 'a')
EllipticCurve(R, [0,0,1,a,0])
Elliptic Curve defined by y^2 + y = x^3 + a*x over
Univariate Polynomial Ring in a over Rational Field

E = EllipticCurve(FiniteField(3), [1,1])
Elliptic Curve defined by y^2 = x^3 + x + 1
over Finite Field of size 3

E.change_ring(QQ)
Elliptic Curve defined by y^2 = x^3 + x + 1 over
Rational Field

EllipticCurve(pAdicField(p=5, prec=20), [1,-1])
Elliptic Curve defined by y^2 = x^3 +
(1+O(5^20))*x + (1+O(5^20)) over 5-adic Field
with capped relative precision 20

EllipticCurve(QQ, [1,1]).reduction(3)
Elliptic Curve defined by y^2 = x^3 + x + 1 over
Finite Field of size 3
```

```
Plotting E over ℝ, ℚ, and 𝔽_p is no problem.
E.plot()

We can easily compute many features of any E/ℚ
E.ainvs()           # a-invariants
E.analytic_rank()   # ord_{s=1} L(E,s)
E.conductor()       # conductor of E
E.discriminant()    # discriminant Δ
E.gens()            # free generators of E(ℚ)
E.has_cm()          # check for complex multiplication
E.j_invariant()     # j-invariant
E.lseries()         # L(E,s)
E.Np(p)             # |E(𝔽_p)| for prime argument
E.rank()            # rank of E
E.torsion_points()  # finite order points
E.integral_points() # integer coordinate points

We can get specifically structured curves from
sage.schemes.elliptic_curves.ec_database
elliptic_curves.rank(n=3, rank=3, tors=2, labels=True)
['59450i1', '59450i2', '61376c1']

Using the @parallel decorator, we convert a normal
function into one which runs on lists of input in
parallel. The function returns a generator,
which when iterated on returns the values as they
are computed in parallel, with their arguments
and results listed.
@parallel
def parallel_Np(E,p): return E.Np(p)
l = zip(elliptic_curves.rank(0), primes_first_n(10))
for answer in parallel_Np(l): print answer
(((Elliptic Curve defined by y^2 + y = x^3 - x^2 -
7820*x -263580 over Rational Field, 3), {}), 5)
(((Elliptic Curve defined by y^2 + y = x^3 - x^2 -
10*x - 20 over Rational Field, 2), {}), 5)
(((Elliptic Curve defined by y^2 + y = x^3 - x^2
over Rational Field, 5), {}), 5)
...
```

4 A Numerical Investigation

All mathematicians must compute data. By computing data we verify hypotheses, test conjectures, and observe new phenomena. Computation is an integral part of science, and for a mathematician in the 21st century there are few better tools available in the aid of computation than the modern computer. Through use of programming languages to construct, test, and analyze entire experiments, and supercomputers on which to deploy these experiments, the scale at which we may view the phenomena in the world of numbers is made orders of magnitude larger. In the next chapter, I would like to invite the reader on a journey through data. In particular, I am interested in understanding the relationship between the infinite rational points of elliptic curves and their reduction into finite field elliptic curves.

4.1 Reducing $E(\mathbb{Q})$ into $E(\mathbb{F}_p)$

Let $E/\mathbb{Q}$ be an elliptic curve with positive rank r, such that the free part of E is isomorphic to $\mathbb{Z}^r$. Each of the infinitely many points is a rational point, each of which we could denote $(m_1/n_1, m_2/n_2)$. Whenever n_1 and n_2 are not divisible by p for some prime p, then we may construct n_1^{-1} and n_2^{-1} within $\mathbb{F}_p$. Having done so, we may then replace division with multiplication by the inverse such that $(m_1/n_1, m_2/n_2)$ reduces into $\mathbb{F}_p \times \mathbb{F}_p$ as $(m_1 n_1^{-1}, m_1 n_1^{-1})$. It is from this sense in which we might describe $E(\mathbb{Q})$ reduced into $E(\mathbb{F}_p)$, denoted here $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$. Computationally, we will take specifically the free-generators for $E(\mathbb{Q})$, reduce them individually into $E(\mathbb{F}_p)$, and see what subgroup they construct. When E has positive rank this is a reduction of an infinite group into a finite one.

While this behavior might be highly erratic varying from prime to prime, it is standard in number theory into look to the limiting behavior of a distribution when the original data is seemingly meaningless. While my notion of interest is the ratio of the reduced points to $E(\mathbb{F}_p)$, the more traditional quantity is algebraic index where $[E(\mathbb{F}_p) : S] = |E(\mathbb{F}_p)|/|S|$ for any subgroup S of $E(\mathbb{F}_p)$. Consider the following function, and what it might do in the limit.

$$F_E(p) = \frac{\sum_{\text{primes } p} |E(\mathbb{F}_p)|}{\sum_{\text{primes } p} |E(\mathbb{Q}) \text{ reduced into } E(\mathbb{F}_p)|}.$$

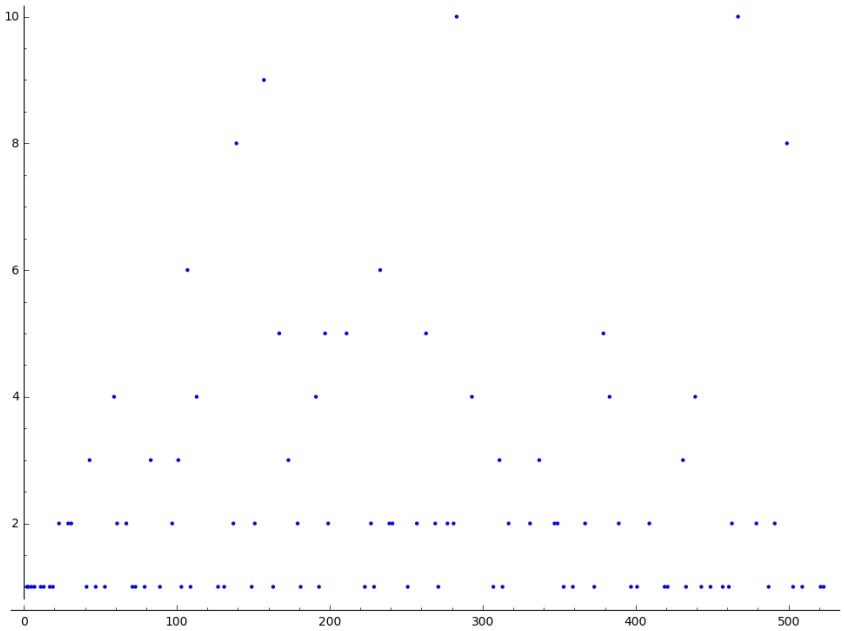


Figure 4.1: The graph of $(p, [E(\mathbb{F}_p) : E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)])$ for 37a a rank one curve given by $y^2 + y = x^3 - x$.

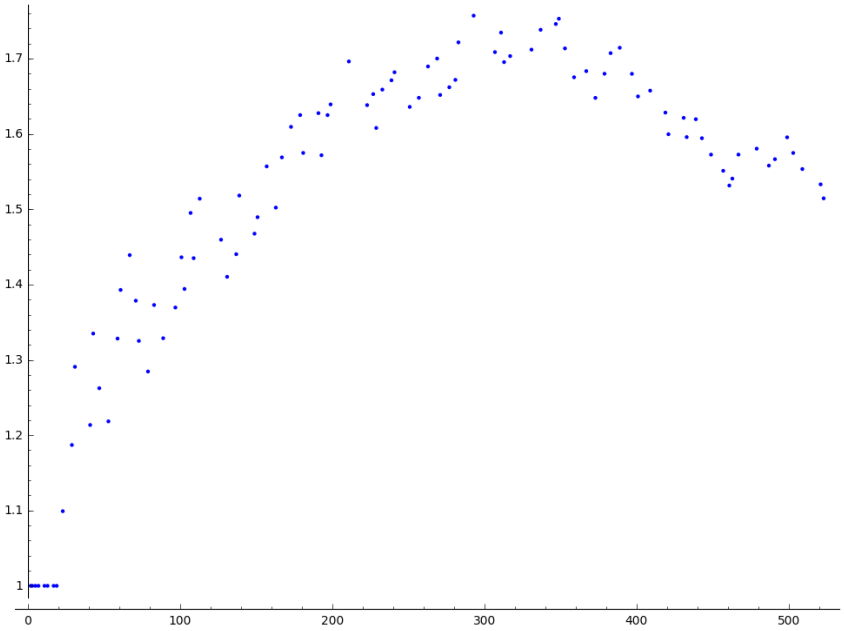


Figure 4.2: The graph of $(p, F_E(p))$ for `E = EllipticCurve('37a')`.

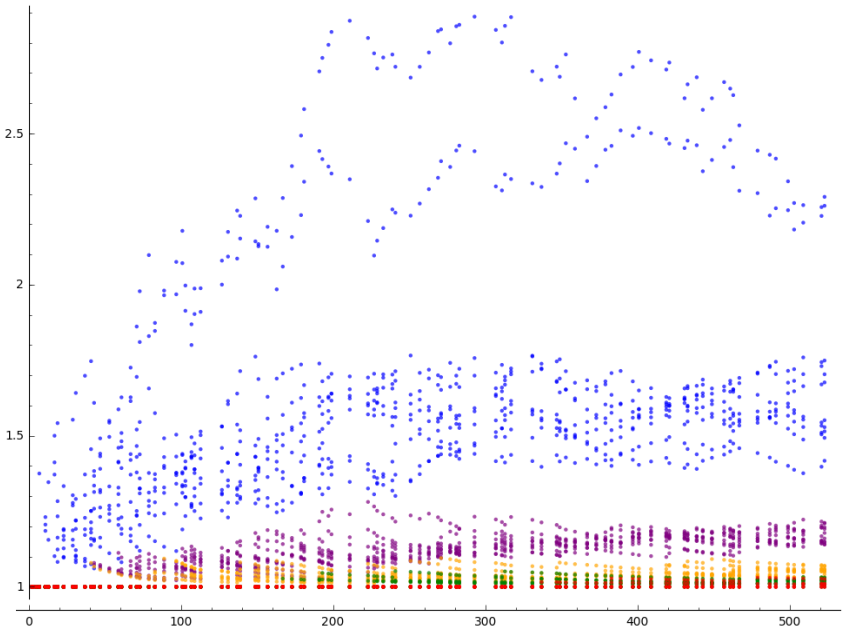
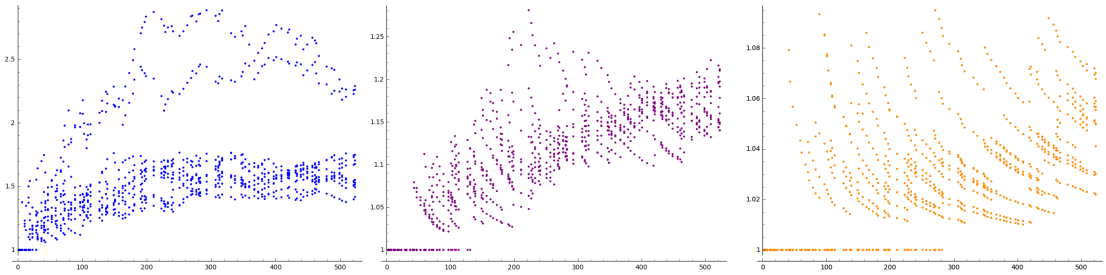
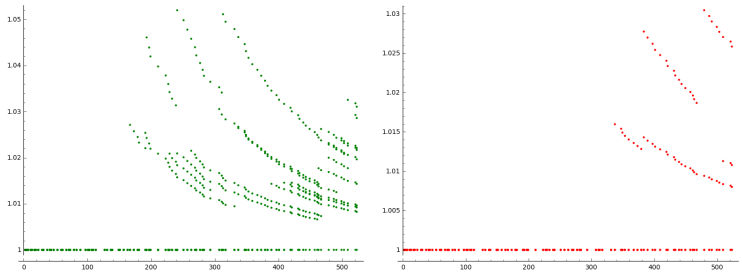


Figure 4.3: Graphs of $(p, F_E(p))$ for 50 curves, 10 of each rank



rank 1 rank 2 rank 3



rank 4 rank 5

Blue denotes rank 1, purple rank 2, orange rank 3, green rank 4, and red rank 5. While I am not surprised to see that when there are more generators that the subgroup becomes larger, I am surprised that even for rank 4 and rank 5 the data does not appear convergent. Rather, as the prime becomes larger we see the ratio shift away from one in favor of jumping up in quantity, where there must have been at least one point in $E(\mathbb{F}_p)$ not in the reduction

of $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$ at certain primes. While rank 2, 3, 4, and 5 appear to each occupy a fairly small range of values, within these ranges it does not appear that one quantity is strongly preferred over others. It should be noted that the individual plots are each on their own scale, such that rank 3, 4, and 5 have magnified y-axes to see the detail of their behavior. It certainly seems difficult to reason from these plot if this ratio converges for any elliptic curves in the limit.

It appears that generally $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$ often has index one until a certain prime where it skips. The horizontal lines at one indicate that the order of the subgroup of $E(\mathbb{F}_p)$ generated by the free generators of $E(\mathbb{Q})$ is and has been equal to $|E(\mathbb{F}_p)|$ for primes less than or equal to the n^{th} prime. Then, at a particular prime the free-generators fail to generate the whole finite field elliptic curve, so the accumulation function skips upward. However, in large rank curves it seems that $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$ and $E(\mathbb{F}_p)$ are equal often, and thus we see a steady decay acting on each of the curves' accumulation functions after such a skip.

So, I did the sane thing to do, and I computed the largest data set I could in a few hours on my computer. Additionally, I inverted the ratio back to my original notion of the ratio of the number of reduced points from $E(\mathbb{Q})$ to the number of points in $E(\mathbb{F}_p)$ so that the graphs wouldn't be unbounded. In many of the following graphs, the horizontal axis denotes the n^{th} prime p.

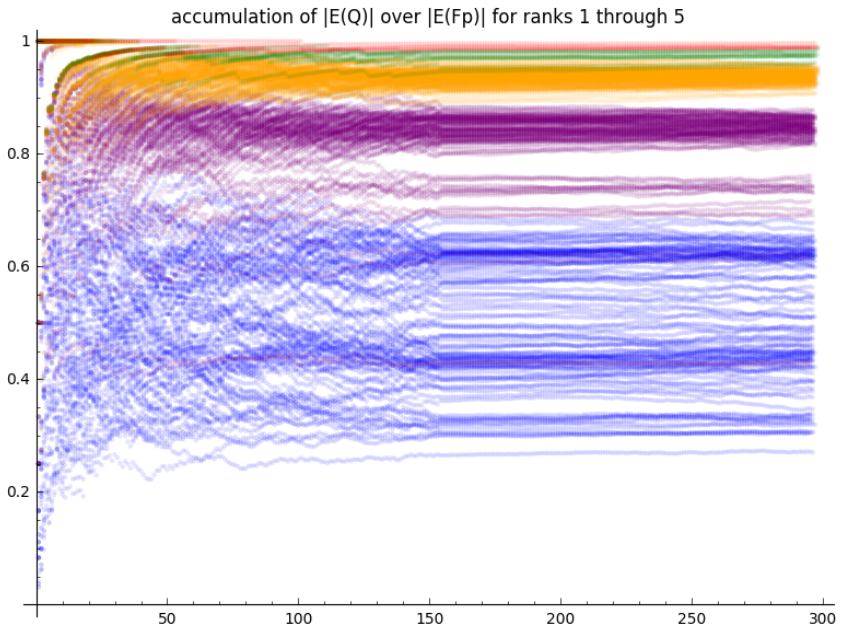


Figure 4.5: The graph of $(n, \frac{1}{F_E(p)})$.

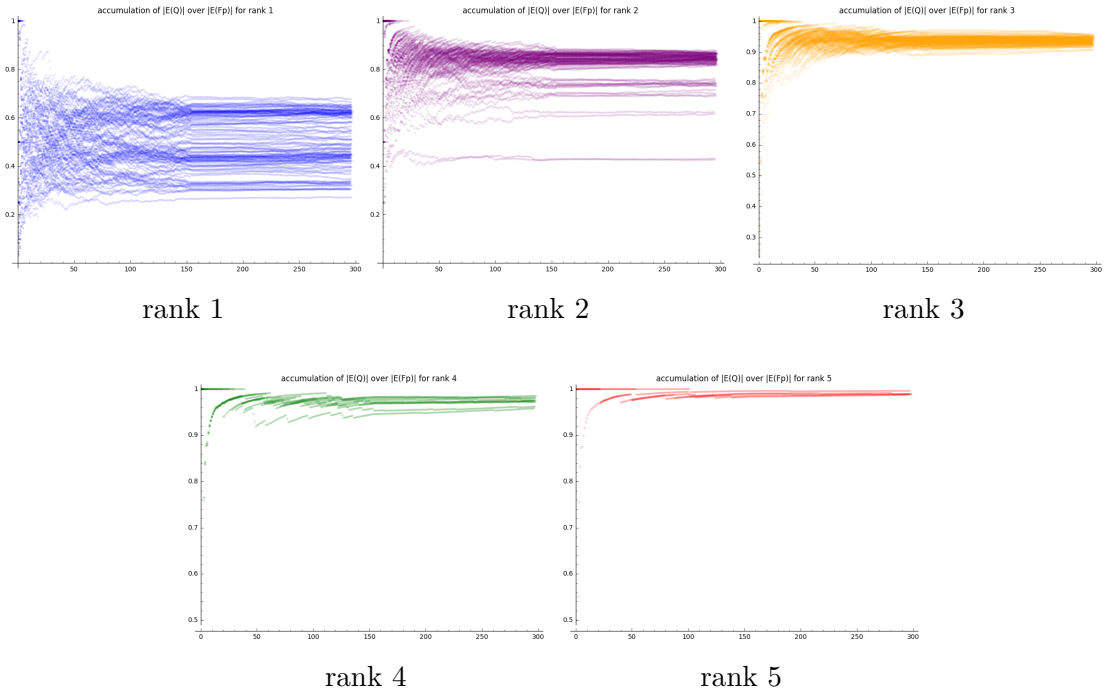


Figure 4.6: Accumulation Function $\frac{1}{F_E(p)}$ separated for each rank

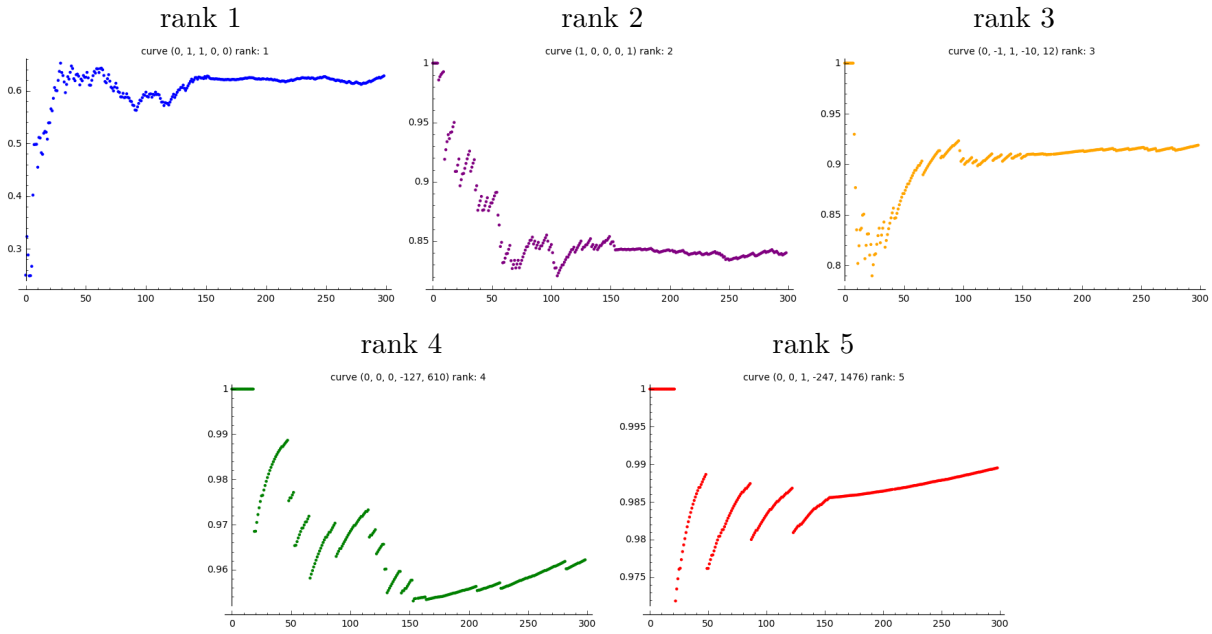


Figure 4.7: Examples of $\frac{1}{F_E(p)}$ for one curve of each rank 1-5

I have used 315 curves to make these plots, 100 of ranks 1, 2, 3, and then I used all the rank 4 and rank 5 curves presently in the Sage sage.schemes.elliptic_curves.ec_database.

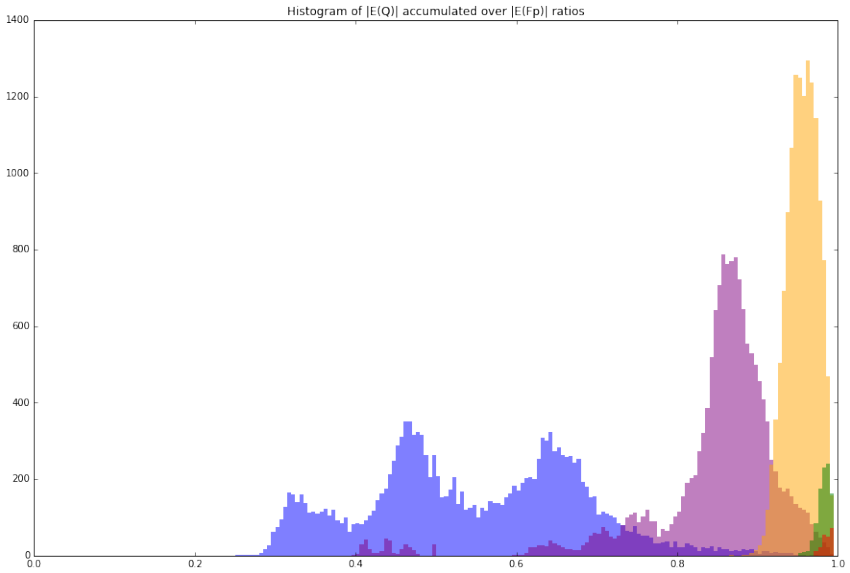


Figure 4.8: And then I histogrammed.

Perhaps it is because there are simply more generators for larger rank curves that the value of peaks descend in order of rank 5 to rank 1. However, besides this simple argument, I can do little to explain this data. Why is rank 1 trimodal? Why are there so many peaks for ranks 1 and 2? What governs the decay of these distributions? I do not know.

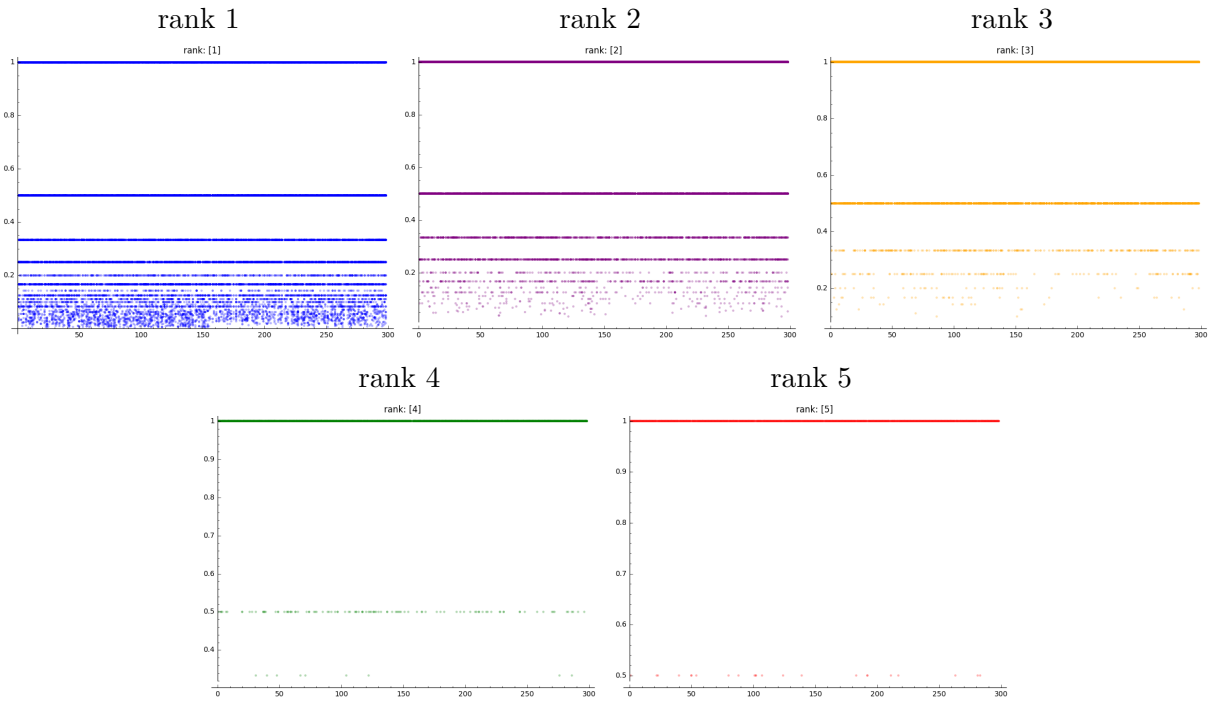


Figure 4.9: $|E(\mathbb{F}_p)|/|E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)|$ at the n^{th} prime

Not making significant progress in understanding the distribution of the accumulation function, I was driven to find simpler patterns. In the last plots I believe I have been successful. Rank 5 in figure 4.9 characterizes the skipping behavior I had noticed previously, and there are some interesting lower bounds on these graphs for rank 4 and 5. I do not have any explanation for why rank four $E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)$ subgroups appear in my data as a third of the whole group or greater, or similarly why the rank 5 subgroups appear only as half or the whole. In effort to understand this and find motivation for it, I plotted $|E(\mathbb{Q}) \hookrightarrow E(\mathbb{F}_p)|$ for a single curve.

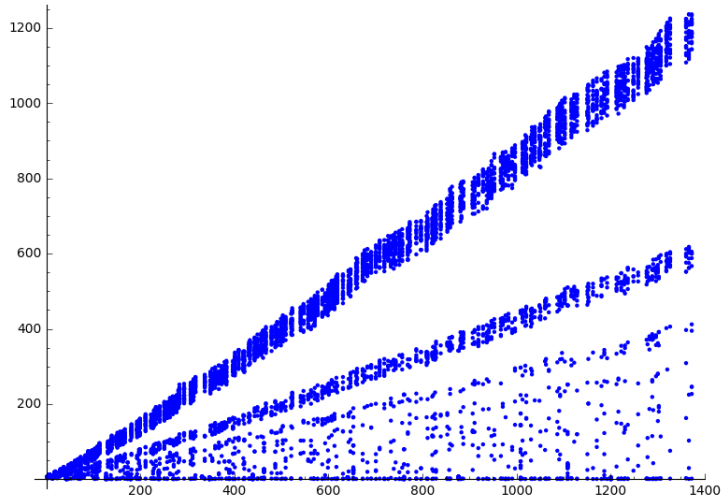


Figure 4.10: $|E(\mathbb{Q}) \hookrightarrow E(F_p)|$ for 37a

The thickest large blue band is visually almost exactly the Hasse bound plot in figure Figure 2.9, and indeed corresponds with when the point $(0, -1)$ on $y^2 + y = x^3 - x$ generates all of $E(\mathbb{F}_p)$. This is plot is certainly visually striking, but I believe it only tells me what I already knew: the ratio of rank one curves' reduced-$E(\mathbb{Q})$ groups' size to the corresponding $|E(\mathbb{F}_p)|$ value is highly scattered and difficult to predict.

These plots are certainly not completely random, and rank 5 in figure 4.9 exemplifies the "skipping" behavior I have described. However, more than anything else I have simply confirmed for myself that understanding the rank of elliptic curves is truly subtle and hard. At this point, I knew I needed simpler questions if I wanted simpler answers.

There is one feature which particularly stands out to me in my data that I ask the reader not to forget–the horizontal lines at one present in figures 4.2, 4.5, and 4.9. This is when reduction of $E(\mathbb{Q})$ is onto $E(\mathbb{F}_p)$.

4.2 Generating a Subgroup with $(0,0)$

Rank is hard to understand and use experimentally, so we will pivot away from using it in favor of experiments with less choice involved for the experimenter (such as the choice of sampling). In an effort to replace the original problem, I now want to measure $\langle P \rangle \subseteq E(\mathbb{F}_p)$, where P is some point of interest and easier to find than the generators of $E(\mathbb{Q})$. In response to this, my advisors suggested using the following family with which we can new define functions at each prime measuring more refined accumulated quantities.

$$\{E_{A,B} : y^2 + y = x^3 + Ax^2 + Bx \text{ for } A, B \in \mathbb{F}_p \text{ and } \Delta(E_{A,B}) \neq 0\},$$

$$\Delta(E_{A,B}) = 16A^2B^2 - 16A^3 - 64B^3 + 72AB - 27.$$

Notice conveniently, the reduction of $E_{A,B}$ into $\mathbb{F}_p$ always contains the point $(0,0)$. In particular, we will define the following functions at each prime number.

$$F_1(p) = \sum_{A,B \pmod p} |E_{A,B}(\mathbb{F}_p)|,$$

$$F_2(p) = \sum_{A,B \pmod p} |\langle (0,0) \in E_{A,B}(\mathbb{F}_p) \rangle|,$$

$$F_3(p) = \sum_{A,B \pmod p} [E_{A,B}(\mathbb{F}_p) : \langle (0,0) \rangle],$$

$$F_4(p) = \sum_{A,B \pmod p} 1/[E_{A,B}(\mathbb{F}_p) : \langle (0,0) \rangle].$$

Why is this a suitable refinement of our original question about reducing $E(\mathbb{Q})$? Because often enough $(0,0)$ is one of the free generators of the rational points on an elliptic curve parametrized by $y^2 + y = x^3 + Ax^2 + Bx$. This can be verified for any prime (and in particular $p = 17$) through the following code snippet.

```
from itertools import product
for (A,B) in product(range(17), range(17)):
    try:
        E = EllipticCurve([0,A,1,B,0])
        print E.gens()
    except:
        pass
```

```
[]
[(0 : 0 : 1)]
[(2 : 3 : 1)]
[(0 : 0 : 1)]
[(0 : 0 : 1), (1/4 : 5/8 : 1)]
[(0 : 0 : 1), (1 : 2 : 1)]
...
```

Since there are approximately $p + 1$ points on any $E_{A,B}(\mathbb{F}_p)$, and there are p choices for each of A and B, we should expect that F_1 will grow cubically with p. F_2 is bounded above by F_1, and since $|\langle (0,0) \rangle| \geq 1$, we can expect it to grow at least as fast as quadratically with respect to p. F_3 and F_4 are more subtle, although intimately related to each other as accumulation functions of each others' inversed summand.

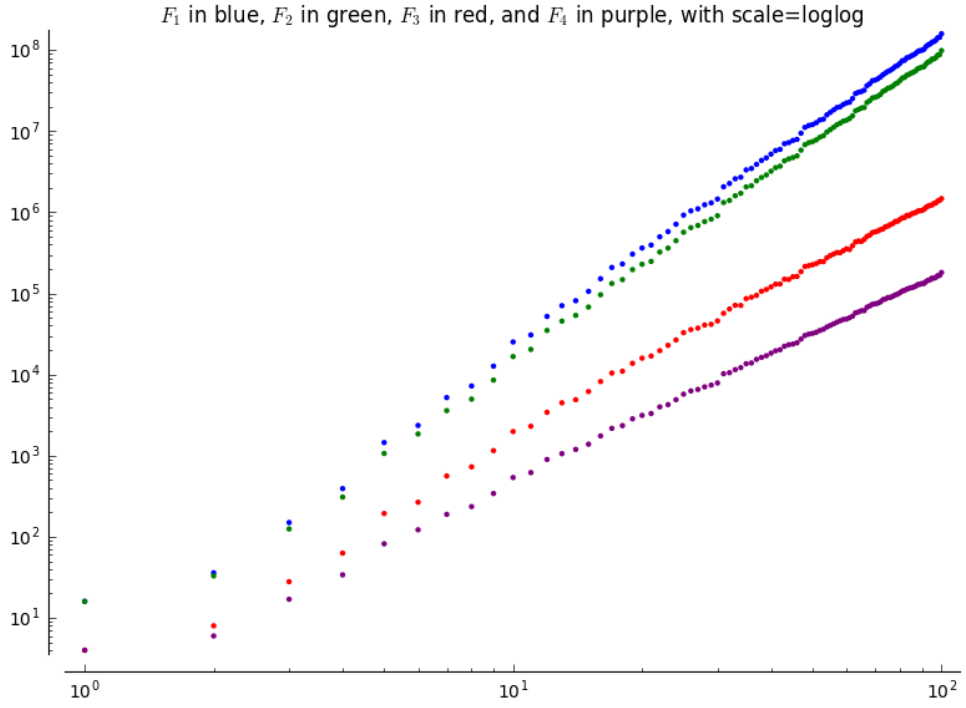
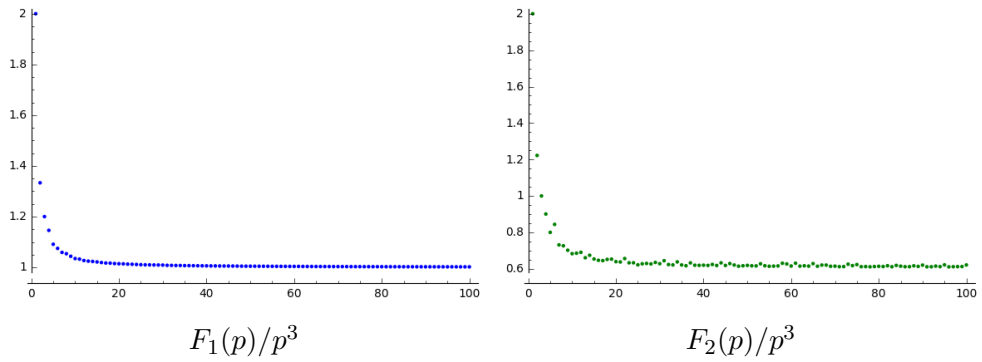
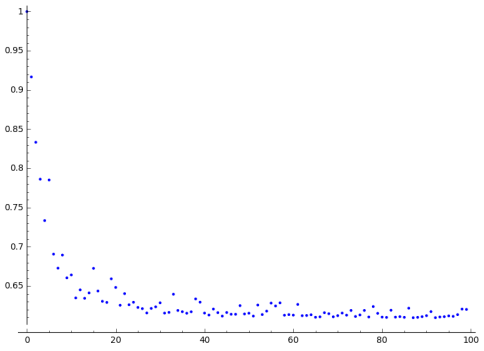


Figure 4.11: F_1, F_2, F_3, F_4 plotted as functions of n^{th} primes on a loglog plot



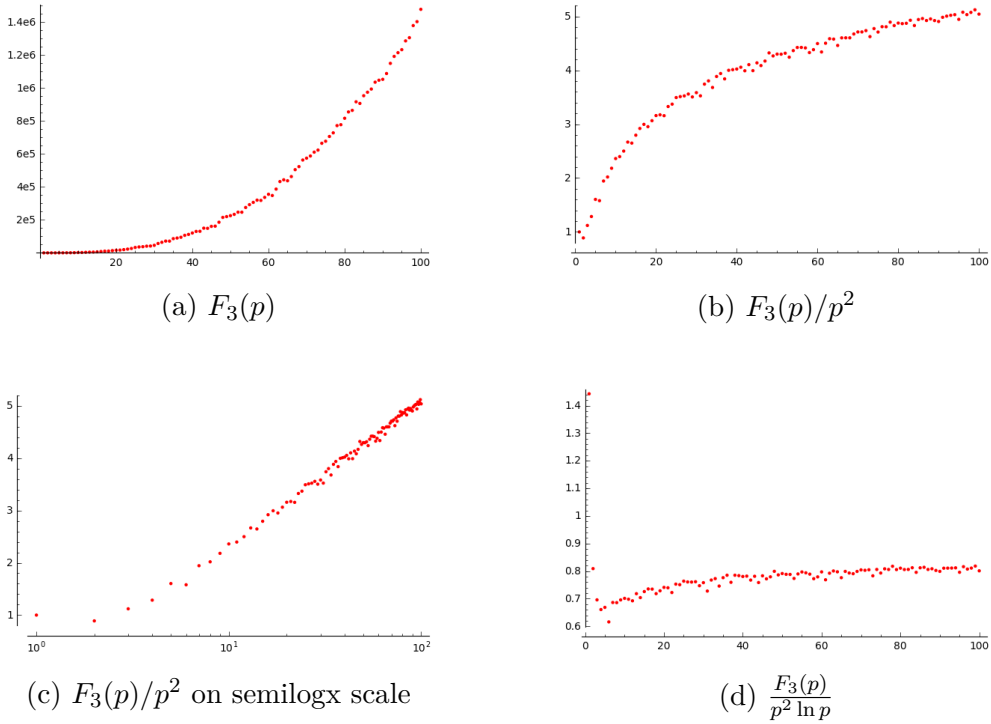
$F_1(p)/p^3$ $F_2(p)/p^3$



$F_2(p)/F_1(p)$

Figure 4.12: Analysis of F_1 and F_2 for 100 Primes

With figure 4.12, we find that $F_1(p) \sim p^3$, $F_2(p) \sim 0.61p^3$, and $\frac{F_2(p)}{F_1(p)} \sim 0.61$. Continuing on, we will take a look at F_3, and skip over F_4 since its information is nearly equivalent.



(a) $F_3(p)$

(b) $F_3(p)/p^2$

(c) $F_3(p)/p^2$ on semilogx scale

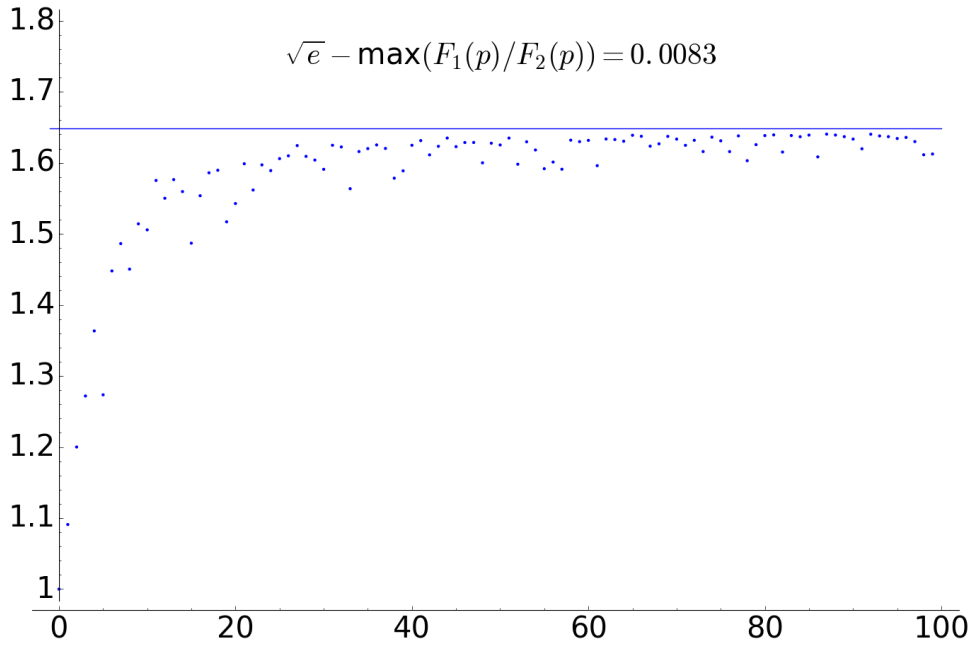
(d) $\frac{F_3(p)}{p^2 \ln p}$

Figure 4.13: Analyzing F_3 for 100 Primes

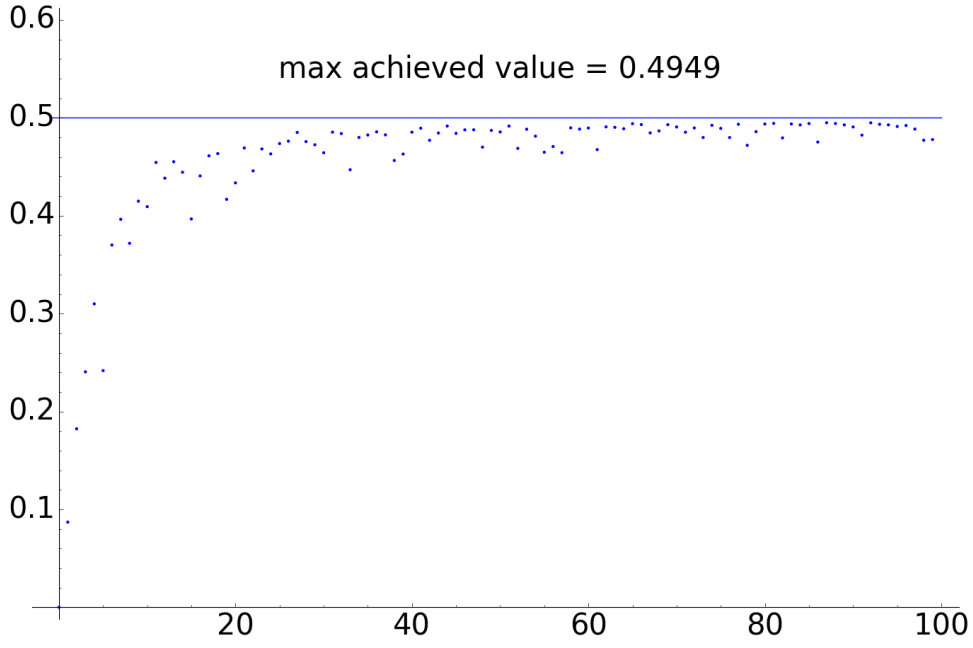
We expect that F_3 cannot possibly grow as fast as p^3, since the generated subgroup is often not the whole group. However, as we reasoned before, it should be faster than p^2, since $|\langle(0,0)\rangle|$ is always at least one, but usually larger. In the above plots, we normalize F_3 by p^2, and find that the remaining normalized plot is straight on a semilogx plot. In Sage, whenever constructing a scatter plot with `points`, it's easy to use the parameters `scale='semilogx'`, `scale='semilogy'`, `scale='loglog'` to check out if data grows exponentially, logarithmically, or according to power laws. After determining the data grows logarithmically, we normalize by a logarithm and find that in the last plot $\frac{F_3(p)}{p^2 \ln p} \sim .82$.

While this data is encouraging in that it is clearly convergent, these ratios do not immediately yield the truth. 61% and 82% are just approximations of the limits I believe exist, However, these limits' computation is, for the moment, inaccessible to me.

Rather, what I have found instead of a limit value is an incredible apparent bound above the ratio $F_1(p)/F_2(p)$.



(a) $F_1(p)/F_2(p)$ is Less Than $\sqrt{e}$ for 100 Primes



(b) $\ln(F_1(p)/F_2(p))$ is Less Than 1/2 for 100 Primes

Figure 4.14: F_1 and F_2 Revisited with Logarithms

I originally plotted $F_2(p)/F_1(p)$ because I reasoned that as a ratio of the group, the order of $\langle(0, 0)\rangle$ might have regular behavior. However, $F_1(p)/F_2(p)$ resembles the algebraic index much more, and has been highly worth investigating. Noticing that it is bounded by $\sqrt{e}$ has startled me incredibly. After seeing this, I found I was even better able to capture this

bound with a plot of $(F_1(p), F_2(p))$. The next plot is bounded and hugged so nicely by the plot of $y = \frac{x}{\sqrt{e}}$ out to 10^8, although the proximity to the line seems to be decaying.

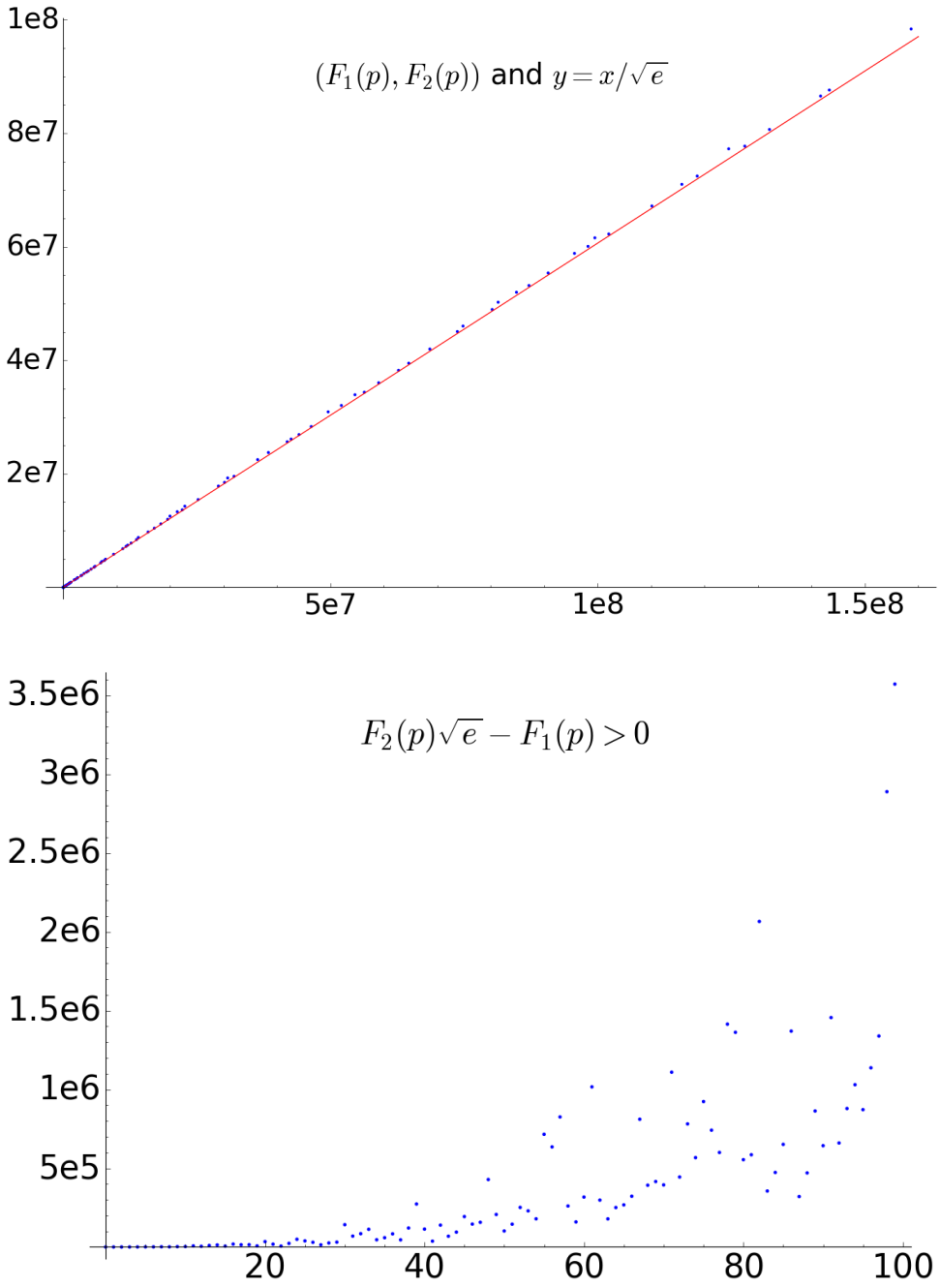


Figure 4.15: Graphs of $(F_1(\mathrm{p}), F_2(p))$ and $(p, F_2(p)\sqrt{e} - F_1(p))$

Why any of this happens, I do not know. It seems perfectly reasonable to me that the data could tend to a number less than or near $\sqrt{e}$ in the limit. However, it has surprised me to find such a strong apparent bound at all in the first 100 values of the ratio of F_1/F_2.

4.3 When is the Subgroup the Group?

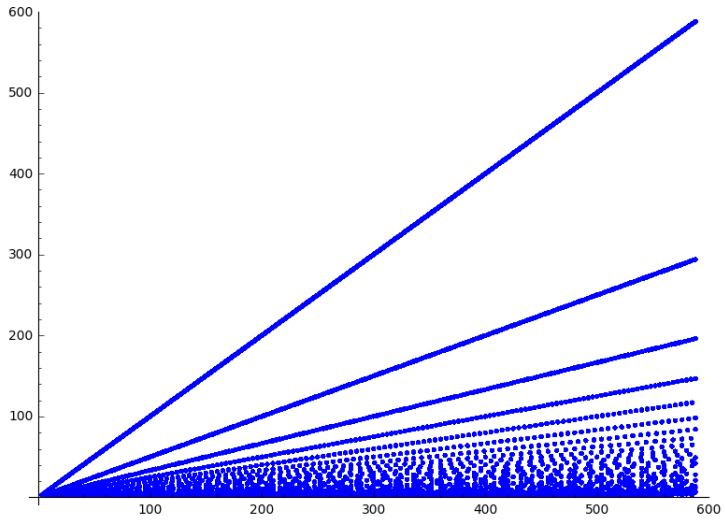


Figure 4.16: A Graph of $(|E_{A,B}(\mathbb{F}_p)|, |\langle(0,0)\rangle|)$ for 100 Primes

While the previous experiments have confounded, confused, and bewildered me at times, I have found a way forward. In figure 4.16, there is a ray extending from the origin at slope 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, and so on. Each of the rays extending from the origin makes up some proportion of the graph. Not only is it feasible to measure this proportion, but in some cases we may easily uncover the limiting behavior of the proportion. Now is when I would like the reader to recollect the horizontal lines at one from *Reducing* $E(\mathbb{Q})$ *into* $E(\mathbb{F}_p)$, because the first natural question in this new investigation is how often is $\langle(0,0)\rangle = E(\mathbb{F}_p)$. This frequency is exactly the proportion of the graph at each prime in figure 4.16 which has slope one.

To make my question more precise, I will investigate the following function to the best of my ability.

$$\tilde{F}(p,n) = \frac{\#\{A,B \pmod p \text{ such that } n \text{ divides } [E_{A,B}\colon \langle(0,0)\rangle]\}}{\#\{\text{nonsingular } E_{A,B} \pmod p\}}$$

We will consider separately how often $\langle(0,0)\rangle = E_{A,B}(\mathbb{F}_p)$, and for all values of $n > 1$ the function $\tilde{F}(p,n)$ measures for each prime family the proportion of curves which would appear in figure 4.16 on the rays with inverse slope divisible by n.

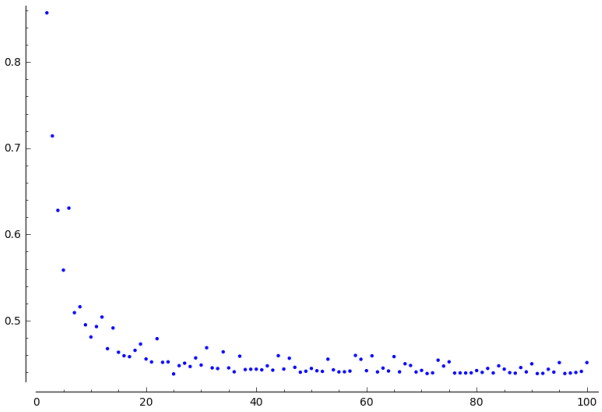


Figure 4.17: How Often is $\langle(0,0)\rangle = E_{A,B}(\mathbb{F}_p)$?

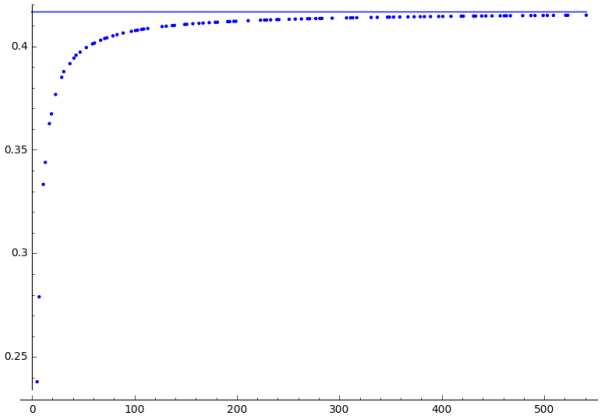


Figure 4.18: $\tilde{F}(p,2)$

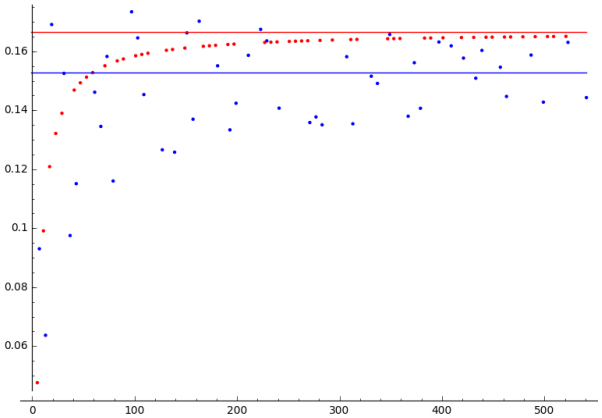
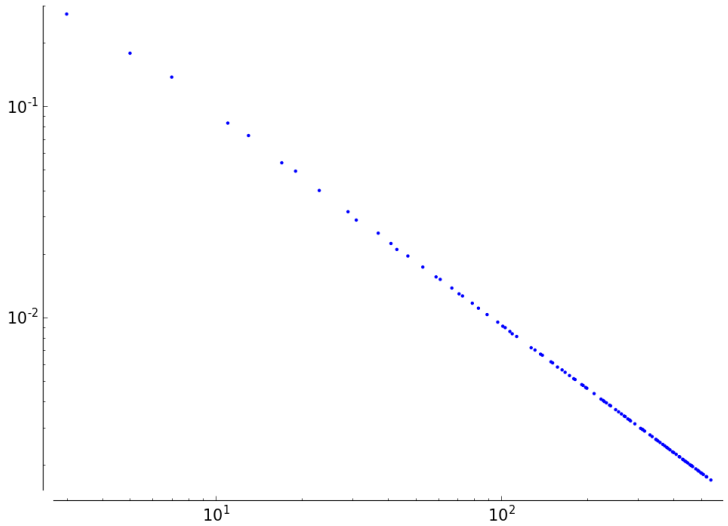


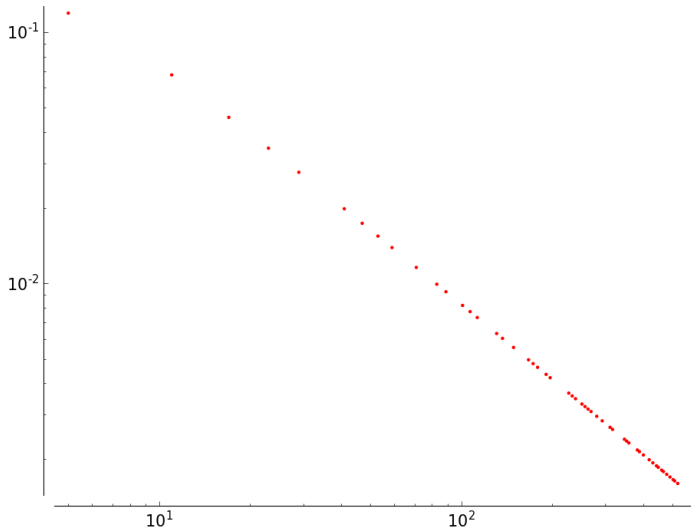
Figure 4.19: $\tilde{F}(p,3)$

It appears that the ratio of curves in our families for each prime with $\langle(0,0)\rangle = E_{A,B}(\mathbb{F}_p)$ converges to approximately 44%. Further, for 2-divisibility and 3-divisibility, three distinct limits have been computed for which I have found that the data converges to according to an inverse power law. For $\tilde{F}(p,3)$, I had to divide the primes into those which are 1 (mod 3) and 2 (mod 3) to make sense of the data.

$$\tilde{F}(p,2) \sim \frac{10}{24}, \qquad \tilde{F}(p = 1 \pmod 3, 3) \sim \frac{33}{216}, \qquad \tilde{F}(p = 2 \pmod 3, 3) \sim \frac{36}{216}.$$



Error $\frac{10}{24} - \tilde{F}(p,2)$ on a loglog plot



Error $\frac{36}{216} - \tilde{F}(p = 2 \pmod 3, 3)$ on a loglog plot

Figure 4.20: Error Decays Exponentially

A Galois theoretical heuristic also supports these claims. Through using the group structure of $E(\mathbb{F}_p)$ and the doubling formula we may calculate how and when we should expect the $(0,0)$ point to appear in the group's multiplication table. Through the study of the roots of particular polynomials, perhaps we will find a method to compute the limit value of $\tilde{F}(p,n)$ for any n. However, that is for another paper.

I have yet to find a direct argument for the ratio of each prime family of curves which have the property that $\langle(0,0)\rangle = E(\mathbb{F}_p)$. However, in answering how often the index is two-divisible and three-divisible, one more path forward in investigation of the subgroups of $E(\mathbb{F}_p)$ generated by $E(\mathbb{Q})$'s free-generators is established. Given the values of $\tilde{F}(p,n)$ for all integers $n > 1$, the ratio for which $\langle(0,0)\rangle = E(\mathbb{F}_p)$ becomes a simple inclusion/exclusion principle based computation. Understanding this ratio is one way we may soon know something more about the relationship between the infinite free part of elliptic curves and their finite field reductions.

Conclusion of Experiments

What do we make of our experiments in sum? Is the failure to understand the reduction of rational elliptic curves $E(\mathbb{Q})$ into finite field elliptic curves $E(\mathbb{F}_p)$ equivalent to having learned nothing? Is understanding $E(\mathbb{F}_p)$ all we can hope for, and that the rank of an elliptic curve is and forever will be beyond us? No. While elliptic curves will remain mysterious until we can more fully understand the rank, it is through interrelating the rank of elliptic curves to objects which we more thoroughly understand that we will be able to uncover the explanations to elliptic curve's rank. In our first experiment we have verified through computation that understanding the rank of an elliptic curve and its influence on the curves behavior is no small task. In the second experiment, we have demonstrated that we can meaningfully connect the theory of the free part of rational elliptic curves to finite field elliptic curves. Finally, in the third experiment, we demonstrate concrete means to use this connection to uncover the laws governing part of an elliptic curves behavior. In sum, we have performed a small investigation into the relationship between an elliptic curve's free part and the curves algebraic behavior in finite field reductions.

4.4 On Progress

Never before have the means of scientific discovery been so accessible as they are now in mathematics. SageMath and all other programming languages make it such that any individual may begin on the path to discovery, and hope for success. Having discovered the remarkable apparent $\sqrt{e}$ bound, a few limit values for $\tilde{F}(p,n)$, and several beautiful plots along the way, it is evident that progress through numerical investigation is truly viable. Elliptic curves may remain mysterious for a long time to come, but progress is undoubtedly certain, perhaps from amateurs and professionals alike.

Bibliography

[Ayo84] Raymond Ayoub. "The lemniscate and Fagnano's contributions to elliptic integrals". In: *Arch. Hist. Exact Sci.* 29.2 (1984), pp. 131–149. ISSN: 0003-9519. DOI: 10.1007/BF00348244. URL: http://dx.doi.org/10.1007/BF00348244.

[Bar09] Jose Barrios. *A Brief History of Elliptic Integral Addition Theorems*. 2009. URL: https://www.rose-hulman.edu/mathjournal/archives/2009/vol10-n2/paper2/v10n2-2pd.pdf.

[Bas97] I. G. Bashmakova. *Diophantus and Diophantine equations*. Vol. 20. The Dolciani Mathematical Expositions. Translated from the 1972 Russian original by Abe Shenitzer and updated by Joseph Silverman. Mathematical Association of America, Washington, DC, 1997, pp. xiv+90. ISBN: 0-88385-526-7. URL: http://links.jstor.org/sici?sici=0002-9890(199903)106:3%3C260:TLCOVA%3E2.0.CO;2-2&origin=MSN.

[BM02] Ezra Brown and Bruce T. Myers. "Elliptic curves from Mordell to Diophantus and back". In: *Amer. Math. Monthly* 109.7 (2002), pp. 639–649. ISSN: 0002-9890. DOI: 10.2307/3072428. URL: http://dx.doi.org/10.2307/3072428.

[CP05] Richard Crandall and Carl Pomerance. *Prime numbers*. Second. A computational perspective. Springer, New York, 2005, pp. xvi+597. ISBN: 978-0-387-25282-7; 0-387-25282-7.

[EGH96] David Eisenbud, Mark Green, and Joe Harris. "Cayley-Bacharach theorems and conjectures". In: *Bull. Amer. Math. Soc. (N.S.)* 33.3 (1996), pp. 295–324. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-96-00666-0. URL: http://dx.doi.org/10.1090/S0273-0979-96-00666-0.

[Han58] Harris Hancock. *Lectures on the theory of elliptic functions: Analysis*. Dover Publications, Inc., New York, 1958, pp. xxiv+498.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[Hus04] Dale Husemöller. *Elliptic curves*. Second. Vol. 111. Graduate Texts in Mathematics. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Springer-Verlag, New York, 2004, pp. xxii+487. ISBN: 0-387-95490-2.

[KS08] Kiran S. Kedlaya and Andrew V. Sutherland. "Computing L-series of hyperelliptic curves". In: *Algorithmic number theory*. Vol. 5011. Lecture Notes in Comput. Sci. Springer, Berlin, 2008, pp. 312–326. DOI: 10.1007/978-3-540-79456-1_21. URL: http://dx.doi.org/10.1007/978-3-540-79456-1_21.

[Lan87] Serge Lang. *Elliptic functions*. Second. Vol. 112. Graduate Texts in Mathematics. With an appendix by J. Tate. Springer-Verlag, New York, 1987, pp. xii+326. ISBN: 0-387-96508-4. DOI: 10.1007/978-1-4612-4752-4. URL: http://dx.doi.org/10.1007/978-1-4612-4752-4.

[Maz08] Barry Mazur. "Finding meaning in error terms". In: *Bull. Amer. Math. Soc. (N.S.)* 45.2 (2008), pp. 185–228. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-08-01207-X. URL: http://dx.doi.org/10.1090/S0273-0979-08-01207-X.

[Pom96] Carl Pomerance. "A tale of two sieves". In: *Notices Amer. Math. Soc.* 43.12 (1996), pp. 1473–1485. ISSN: 0002-9920.

[Sil13] Alice Silverberg. "Ranks "cheat sheet"". In: *Women in numbers 2: research directions in number theory*. Vol. 606. Contemp. Math. Amer. Math. Soc., Providence, RI, 2013, pp. 101–110. DOI: 10.1090/conm/606/12142. URL: http://dx.doi.org/10.1090/conm/606/12142.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986, pp. xii+400. ISBN: 0-387-96203-4. DOI: 10.1007/978-1-4757-1920-8. URL: http://dx.doi.org/10.1007/978-1-4757-1920-8.

[ST15] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Second. Undergraduate Texts in Mathematics. Springer, Cham, 2015, pp. xxii+332. ISBN: 978-3-319-18587-3; 978-3-319-18588-0. DOI: 10.1007/978-3-319-18588-0. URL: http://dx.doi.org/10.1007/978-3-319-18588-0.

[Sti10] John Stillwell. *Mathematics and its history*. Third. Undergraduate Texts in Mathematics. Springer, New York, 2010, pp. xxii+660. ISBN: 978-1-4419-6052-8. DOI: 10.1007/978-1-4419-6053-5. URL: http://dx.doi.org/10.1007/978-1-4419-6053-5.