


Spring 2019

The Conditional Probability That an Elliptic Curve Has a Rational Subgroup of Order 5 or 7

Meagan Kenney
Bard College

Follow this and additional works at: https://digitalcommons.bard.edu/senproj_s2019

 Part of the [Algebra Commons](#), and the [Number Theory Commons](#)



This work is licensed under a [Creative Commons Attribution-NonCommercial-No Derivative Works 4.0 License](#).

Recommended Citation

Kenney, Meagan, "The Conditional Probability That an Elliptic Curve Has a Rational Subgroup of Order 5 or 7" (2019). *Senior Projects Spring 2019*. 202.

https://digitalcommons.bard.edu/senproj_s2019/202

This Open Access work is protected by copyright and/or related rights. It has been provided to you by Bard College's Stevenson Library with permission from the rights-holder(s). You are free to use this work in any way that is permitted by the copyright and related rights. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself. For more information, please contact digitalcommons@bard.edu.

The Conditional Probability That an Elliptic Curve Has a Rational Subgroup of Order 5 or 7

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

by
Meagan Kenney

Annandale-on-Hudson, New York
May, 2019

Abstract

Given an elliptic curve E with ℓ -torsion, it is guaranteed that E has local ℓ -divisibility. While the converse does not hold, from Katz [9] we are able to get a partial converse up to isogeny. That is, given an elliptic curve E with local ℓ -divisibility, there exists an elliptic curve E' , that is isogenous to E , such that E' has ℓ -torsion. From this partial converse the question arises: What is the probability, denoted P_ℓ , that given a curve E with local ℓ -divisibility, that E will have ℓ -torsion? Cullinan and Voight [3] proved that this probability exists for all relevant ℓ , and showed that $P_3 \approx 51\%$ and $P_4 \approx 27\%$. In this paper we will prove that $P_5 = \frac{5}{6}$ and conjecture that $P_7 = \frac{\sqrt{7}}{\sqrt{7}+1}$.

Contents

Abstract	iii
Dedication	vii
Acknowledgments	ix
1 Introduction	1
2 Background	9
2.1 Equations of Elliptic Curves	9
2.2 The Group Law on Elliptic Curves	17
2.3 Reducing a Curve Modulo p	25
2.4 Our Question	26
3 Parameterizations of Elliptic Curves	31
3.1 The Tate Normal Form	32
3.2 Curves with a Rational Subgroup of Order 5	33
3.3 Curves with a Rational Subgroup of Order 7	36
4 Isogenies	39
4.1 Exploring Isogenies	39

4.2	Vélu's Algorithm	47
4.3	Paramaterization of Curves with Local 5-Divisibility	49
4.4	Paramaterization of Curves with Local 7-Divisibility	53
4.5	Accountability of Models	56
5	Sieving and Overcounting	59
5.1	Isomorphism Classes of Elliptic Curves	60
5.2	Sieving	64
5.3	Considering $\ell = 7$	78
6	Results	79
6.1	Outline of Proof for Determining P_5	79
6.2	Experimenting with Equations	80
6.3	Rotating Curves	83
6.4	Rotating and Reflecting $A'_5(X)$	86
6.5	Rotating and Reflecting $B'_5(X)$	89
6.6	Comparing the Areas of Specified Regions	93
6.7	Conjecture for $\ell = 7$	96
	Bibliography	99

Dedication

To my sister, Lauren, for being the spark that ignited my love of mathematics and for always being there to remind me to not underestimate myself.

Acknowledgments

Thank you to John Cullinan for being a phenomenal advisor that I could always depend on, and for helping me to make something of which I can be proud. Thank you to all of the faculty of the math department at Bard for going out of your way to show me the beauty of mathematics and to remind me that sleeping is important. Additionally, I would like to express how grateful I am to Jeremy Rouse for introducing me to the beautiful subject of elliptic curves, and Riad Masri for helping me to solidify my desire to continue studying topics in number theory.

I would like to thank all of The Aggressive Apple Snatchers for making breaks from work feel worthwhile and fun, and therefore for keeping me sane. In particular I would like to thank Leah for being there when the sleep deprivation hit to remind me that multiplication is commutative, and Noah for being there always. Finally, thank you to all of my parents and my sister for helping me to believe in myself, and for all of your willingness to listen and help even with the most irrational of stresses. None of this would be possible without the help of all of you.

1

Introduction

An elliptic curve is defined to be the set of solutions to a cubic equation of a certain form. The collection of all of the solutions to this certain cubic equation, however, form more than just a set. In fact, the solutions actually maintain a surprising amount of structure, which makes elliptic curves particularly useful and relevant to a variety of diverse mathematical problems. A modern example of the applications of elliptic curves can be seen in cryptography. Recall that, given some group G , the discrete logarithm problem (DLP) attempts to determine $m \in \mathbf{Z}^+$ such that $x^m = y$ for some particular $x, y \in G$ where $y \in \langle x \rangle$ [13, p.376]. There is an analogous problem over the elliptic curves, aptly named the elliptic curve discrete logarithm problem (ECDLP), that relies on the fact that the solutions to the cubic defining an elliptic curve actually form a group, as will be shown later. Similarly to the DLP, the ECDLP is computationally difficult to solve, and can in fact be more computationally difficult to solve than the DLP, making it a desirable cryptographic tool [13, p.377]. To motivate our interest in elliptic curves, we will now explore some further applications of elliptic curves that are not directly related to the project, but rely on some similar structural characteristics of elliptic curves that we will be examining. One such example is the connection between elliptic curves and the congruent number problem,

which stems from the ability to phrase the congruent number problem in a way that relies on a certain cubic equation that defines an elliptic curve.

A congruent number, is a rational number n for which there exists a right triangle with rational side lengths that has area n [10, p.3]. For example 6 is a congruent number because the right triangle with rational sides of length 3, 4, and 5 has area 6. More interestingly, one gets that 7 is a congruent number by considering the right triangle with side lengths $\frac{35}{12}$, $\frac{24}{5}$, and $\frac{337}{60}$. Certainly identifying the triangle necessary to prove that 7 is a congruent number may be less obvious to find than the one necessary to show that 6 is a congruent number. So we ask if there is another way to determine whether or not a positive, rational number is a congruent number or not. We can do so by transferring this to a problem concerning elliptic curves.

Theorem 1.0.1. [10, p.4] *Let $n \in \mathbf{Q}^+$, then there is a one to one correspondence between each of the triples and each of the pairs in the following two sets:*

$$C = \{a, b, c \mid a^2 + b^2 = c \text{ and } \frac{ab}{2} = n\}, \quad E = \{(x, y) \mid y^2 = x^3 - n^2x \text{ and } y \neq 0\}.$$

Let $(a, b, c) \in C$, and let $(x, y) \in E$ be the corresponding pair to the triple (a, b, c) . Then $a, b, c \in \mathbf{Q}$ if and only if $x, y \in \mathbf{Q}$.

This theorem tells us that there are the same number of rational right triangles with side lengths a, b , and c with area n , as there are rational solutions to the equation $y^2 = x^3 - n^2x$ where $y \neq 0$. From Theorem 1.0.1 we get the following proposition instructing how to rephrase the congruent number problem into a problem concerning elliptic curves.

Proposition 1.0.2. [10, p.7] *Let $n \in \mathbf{Q}^+$. We get that n is a congruent number if and only if the elliptic curve given by the equation $y^2 = x^3 - n^2x$ has a rational point $P = (x_1, y_1)$ that satisfies the equation such that $y_1 \neq 0$.*

Outside of cryptography and the congruent number problem, elliptic curves have been most notably used in Andrew Wiles's proof of Fermat's Last Theorem, which relied on the modularity

theorem for elliptic curves. Certainly, elliptic curves play an important role in modern mathematics, but these algebraic structures have been interesting to mathematicians since the first elliptic curve surfaced unintentionally in ancient Greece through a problem posed by Diophantus.

Problem 24 from Diophantus's Arithmetica Book IV:[2, p.640] *“To divide a given number into two numbers such that their product is a cube minus its side”*

If we take a to be our given number this will result in the equation

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

so that x^3 is our cube and thus the measure of a side of this cube can be given by x . Now if a is odd, we can write $a = 2y + 1$ for some $y \in \mathbb{Z}$ and therefore we can split a into the consecutive numbers y and $a - y = y + 1$ to get the equation

$$y(y + 1) = x^3 - x.$$

Note that $x^3 - x$ factors to give us the equation

$$y(y + 1) = (x - 1)x(x + 1),$$

and thus this problem is sometimes presented as a search for integers such that the product of two consecutive numbers is equal to the product of three consecutive numbers. This equation

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

is actually an elliptic curve. Therefore the solutions to Diophantus's question when considering the given number to be odd, can also provide the answer to how many integral points are on the curve E given by the equation $E : y^2 + y = x^3 - x$.

For this specific elliptic curve E , which is given the label 37.a1 in the LMFDB[11], the integral solutions are given by the LMFDB as follows:

$$(-1, -1), \quad (-1, 0), \quad (0, -1), \quad (0, 0), \quad (1, -1),$$

$$(1, 0), \quad (2, -3), \quad (2, 2), \quad (6, -15), \quad (6, 14).$$

From Siegel's theorem, [6, p.353] we get that elliptic curves have finitely many integral points. However, the number of rational points on an elliptic curve is not necessarily finite. The genus of a curve is a rough measure of the complexity of its rational solutions.

Definition 1.0.3. [6, p.67] Let C be a curve defined over \mathbf{C} , which is both projective and nonsingular. The **genus** of C is given by how many "holes" exist on the Riemann surface $C(\mathbf{C})$. △

The different types of genera of curves will directly affect the answer to the question of how many rational points exist on a certain curve. Note that given a curve, the category of algebraic curves to which this curve belongs is dependent on the genus. For example, if you have a smooth, projective algebraic curve with a rational point, then this curve is an elliptic curve if and only if it has genus 1.

Theorem 1.0.4. [6, p.68] *Let K be a number field, and let C be a smooth projective curve defined over K . Suppose that $C(K) \neq \emptyset$, where $C(K)$ denotes the K -rational points on the curve C .*

a) If C has genus 0, then the number of K -rational points on C/K is arithmetically given by $\mathbf{P}^1(K)$. Thus the set of K -rational points on C/K is infinite if and only if the number of points on the projective line over K is infinite.

(b) If C has genus 1, then the set of K -rational points on C/K can be given by a finitely generated group.

(c) If C has genus 2 then the set of K -rational points on C/K is finite.

Remark 1.0.5. Note that for the case of (b) in the above theorem, though C has genus 1, it is not necessarily an elliptic curve, as it is possible to have a curve of genus 1 with no rational points. An elliptic curve requires the presence of at least one rational point. ◇

From Theorem 1.0.4 we can see that the set of rational points on an elliptic curve E , denoted $E(\mathbf{Q})$, actually forms a finitely generated group. This group is called the Mordell-Weil group of a curve and is actually an abelian group. The binary operation of this group, which we will denote by \oplus , is slightly complicated and will be described both geometrically and algebraically in detail later in Section 2.2. As the Mordell-Weil group is a finitely generated abelian group, we get that $E(\mathbf{Q})$ is isomorphic to the product of a finite number of cyclic groups together with finitely many copies of the integers. If there is a cyclic group in this product, then this group will have been generated by a point on the elliptic curve that has finite order. A point on an elliptic curve has finite order if it is periodic with respect to the group law defined on the points of the elliptic curve. We call these points of finite order torsion points. We denote the group of all torsion points of E over \mathbf{Q} by $E(\mathbf{Q})_{\text{tor}}$. This is where the project begins as we explore certain kinds of torsion structure on elliptic curves.

Let P be a point of finite order on an elliptic curve E . We denote $[m]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{m \text{ summands}}$. As we are working with a group, we know there exists some identity in the set of rational points. Let \mathcal{O} denote the identity of our group. Suppose that P has order m , then we say P is an m -torsion point and can conclude that $[m]P = \mathcal{O}$.

Let E/\mathbf{Q} be an elliptic curve with a point P of order m ; that is, let E be the set of solutions to a certain cubic equation where P is one of those solutions and $[m]P = \mathcal{O}$. Let G be the group of points on E generated by the point P . Clearly every point in G will have finite order and thus $G \subseteq E(\mathbf{Q})_{\text{tor}}$, in fact, G is a subgroup of $E(\mathbf{Q})_{\text{tor}}$. Now given a finite set A we will denote the number of elements of A by $\#A$. By the definition of G we know that $\#G = \ell$. As $G \leq E(\mathbf{Q})_{\text{tor}}$, then by Lagrange's Theorem, we get that $\ell \mid \#E(\mathbf{Q})_{\text{tor}}$.

Furthermore, the group structure on E is preserved by reduction modulo p , for all but finitely many primes p , that is the map that reduces an elliptic curve modulo p is actually a homomorphism. Therefore through this reduction map the order of torsion points is preserved. From [13, p.192], we know that for all but finitely many primes p there exists an injection

$E(\mathbf{Q})_{\text{tor}} \rightarrow E(\mathbf{F}_p)$. As reduction modulo p is a homomorphism and $E(\mathbf{Q})_{\text{tor}}$ is a group, then the image of $E(\mathbf{Q})_{\text{tor}}$ under this homomorphism is a group, that is, the image of the torsion subgroup of E is in fact a subgroup of $E(\mathbf{F}_p)$. Therefore, again, by Lagrange's Theorem we get that $\#E(\mathbf{Q})_{\text{tor}} \mid \#E(\mathbf{F}_p)$ and therefore the fact that $\ell \mid \#E(\mathbf{Q})_{\text{tor}}$ implies that $\ell \mid \#E(\mathbf{F}_p)$. When $\ell \mid \#E(\mathbf{F}_p)$ for all but finitely many primes p , we say that E has local ℓ -divisibility.

Remark 1.0.6. From this we can conclude that any elliptic curve with a torsion point of order ℓ has local ℓ -divisibility. However, the converse of this statement does not hold. That is, given an elliptic curve E with local ℓ -divisibility, we cannot conclude that E necessarily has ℓ -torsion. \diamond

While local ℓ -divisibility on a curve does not imply ℓ -torsion on that same curve, from Katz [9] we get a partial converse that holds up to isogeny. The partial converse asserts that given an elliptic curve E such that $\ell \mid \#E(\mathbf{F}_p)$ for all but finitely many primes p there exists another curve E' , which is isogenous to the curve E , such that $\ell \mid \#E'(\mathbf{Q})_{\text{tor}}$, and thus E' has a torsion point of order ℓ . Note that an elliptic curve is isogenous to itself, and so in some cases the curve satisfying $\ell \mid \#E'(\mathbf{Q})_{\text{tor}}$ is simply E itself, in which case the original curve E has ℓ -torsion.

Using the language of torsion and divisibility, we can now restate the theorem of Katz to conclude that given a curve E with local ℓ -divisibility, there exists a curve E' in the isogeny class of E such that E' has ℓ -torsion. But when will the original elliptic curve with ℓ -divisibility not just be isomorphic to a curve with ℓ -torsion, but will actually have ℓ -torsion itself?

We have now arrived at the question motivating this project:

Given $\ell = 5$ or $\ell = 7$ and an elliptic curve E with local ℓ -divisibility, what is the probability that E has ℓ -torsion?

To formalize this question we require some notation from the paper of Voight and Cullinan [3]. To calculate this probability we will need to use a method of counting elliptic curves. One way to count elliptic curves is by ordering them based on their height.

Definition 1.0.7. Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + Ax + B.$$

Then the **height** of E , denoted $\text{ht } E$, is defined by the equation

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

△

Though this definition of height will only work for elliptic curves defined by an equation of the form $y^2 = x^3 + Ax + B$, this will not be an issue for conducting our count as we will only be required to count what are called minimal models of elliptic curves that we will be able to define by equations of this form. Now, let \mathcal{E} be the set of all minimal models for elliptic curves E over \mathbf{Q} . As in [3, p.1] we define the set

$$\mathcal{E}_{\leq H} = \{E \in \mathcal{E} \mid \text{ht } E \leq H\},$$

which by definition is the set of all minimal models of elliptic curves with height less than or equal to H . Similarly, we define

$$\mathcal{E}_{\ell?} = \{E \in \mathcal{E} \mid \ell \mid \#E(\mathbf{F}_p) \text{ for a set of primes } p \text{ of density } 1\}.$$

Thus $\mathcal{E}_{\ell?}$ is the set of all minimal models of elliptic curves with local ℓ -divisibility.

Under this notation we denote the following probability

$$P_\ell = \lim_{H \rightarrow \infty} \frac{\#\{E \in \mathcal{E}_{\leq H} \mid \ell \mid \#E(\mathbf{Q})_{\text{tor}}\}}{\#\{E \in \mathcal{E}_{\leq H} \cap \mathcal{E}_{\ell?}\}}.$$

The numerator of P_ℓ is simply the number of minimal models of elliptic curves with ℓ -torsion up to some height, while the denominator is the set of all minimal models of elliptic curves with local ℓ -divisibility up to that same height. Note that this will determine the probability that an elliptic curve with local ℓ -divisibility also has ℓ -torsion.

Note that P_ℓ exists if and only if the limit exists. In fact, this probability only makes sense for certain values of ℓ . There are only finitely many possible orders that a torsion point may have on an elliptic curve, which can be shown through the restrictions on the possible structure of $E(\mathbf{Q})_{\text{tor}}$.

Theorem 1.0.8. (Mazur) [13, p.242] *Let E be an elliptic curve over \mathbf{Q} . Then the torsion subgroup of $E(\mathbf{Q})$ will have one of the following structures*

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/n\mathbf{Z} \text{ such that } 1 \leq n \leq 10 \text{ or } n = 12$$

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \text{ such that } n = 1, 2, 3, 4.$$

Voight and Cullinan in [3] proved that the probability that a curve with local ℓ -divisibility has ℓ -torsion is computable for all relevant ℓ , that is all ℓ for which an elliptic curve could possibly have a torsion point of order ℓ given by 2.2.10.

In [3] they calculate $P_3 \approx 51\%$. This proves that an elliptic curve with local 3-divisibility is slightly more likely than not to also have 3-torsion. Cullinan and Voight [3] also prove that $P_4 \approx 27\%$, which implies that an elliptic curve with local 4-divisibility is more likely to not have 4-torsion. Note that trivially we get that $P_1 = 1$ and $P_2 = 1$. Here I will calculate P_5 , provide a conjecture for P_7 , and explain the necessary theoretical and computational background that went into exploring these probabilities.

Theorem 1.0.9. *We have that $P_5 = \frac{5}{6}$.*

Conjecture 1.0.10. *We conjecture that $P_7 = \frac{\sqrt{7}}{1+\sqrt{7}}$.*

Note we used Sage [15] and PARI [12] to perform computations for this paper. Additionally, all of the figures in this paper were made in GeoGebra[8].

2

Background

2.1 Equations of Elliptic Curves

In order to study elliptic curves it is first important to acquire a deeper understanding of the equations that define them and what these equations can tell us about the structure of the curve that they define.

Let K be a field and let $P_1(x_1, \dots, x_n), P_2(x_1, \dots, x_n), \dots, P_m(x_1, \dots, x_n)$ be polynomials with coefficients in K , that is we say the P_j are *defined over* K for all $j \in \{1, \dots, m\}$. Fix an algebraic closure \overline{K} of K .

Definition 2.1.1. [10, p.52] An affine algebraic variety V is the set of common solutions in \overline{K} to the following system of equations:

$$P_1(x_1, \dots, x_n) = 0$$

$$P_2(x_1, \dots, x_n) = 0$$

$$\vdots = \vdots$$

$$P_m(x_1, \dots, x_n) = 0.$$

△

Definition 2.1.2. [13, p. 2] Let V be the algebraic variety made up of the system of equations $\{P_k = 0\}_{k=1}^m$. We say that a point of V is **K -rational** if its coordinates lie in K . That is, if there is a common solution (y_1, \dots, y_n) to the collection of polynomial equations $\{P_k = 0\}_{k=1}^m$ defining V such that $y_j \in K$ for all $j \in \{1, \dots, n\}$. \triangle

In this project we will primarily be working with affine curves to assist in our computations; however, the proper definition of elliptic curves requires the notion of projective space, particularly projective varieties. We can get a projective variety by taking the projective closure of an affine variety, on which the affine patch will be the original affine variety. Informally, projective space is simply affine space with additional, so-called, points at infinity.

Definition 2.1.3. [13, p. 6] We define **Projective n -space over \mathbf{K}** to be the set of all $(n+1)$ -tuples in the affine space of dimension $n+1$ such that at least one coordinate is nonzero. Within \mathbf{P}^n there exists an equivalence relation such that given $A = (x_0, \dots, x_n)$ and $B = (y_0, \dots, y_n)$, then $A \sim B$ if there exists some $\lambda \in \bar{K}^*$ such that B can be rewritten as $B = (\lambda x_0, \dots, \lambda x_n)$. \triangle

As an example consider Projective 2-space, that is, the projective plane, which is especially relevant to the study of elliptic curves.

Example 2.1.4. The projective plane, over a field K , which we will denote \mathbf{P}^2 , is simply the collection of all nonzero triples with K -rational coordinates of the form $[x_0 : x_1 : x_2]$, that satisfy the equivalence relation given by $[x_0 : x_1 : x_2] \sim [y_0 : y_1 : y_2]$ if and only if $x_0 = \gamma y_0$, $x_1 = \gamma y_1$ and $x_2 = \gamma y_2$ for some $\gamma \in \bar{K}^*$, which denotes the set of all units of \bar{K} . \diamond

Proposition 2.1.5. [13, p.42] *In the projective plane we can define elliptic curves over a field K with non-singular equations to be of the form*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (2.1.1)$$

where $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$.

This, however, is not the general Weierstrass equation from which we normally consider elliptic curves. To find such an equation we must bring this curve into the affine plane to get an equation for the curve in two variables. To do so we must consider the equivalence classes of all the projective points that lie on the projective curve E given by equation 2.1.1.

Let $P = [X_P : Y_P : Z_P]$ be a point satisfying equation 2.1.1 such that $Z_P \neq 0$. Then by the equivalence relation on the points in \mathbf{P}^2 we know that

$$[X_P : Y_P : Z_P] \sim [X_P/Z_P : Y_P/Z_P : 1],$$

which we get by multiplying all of the coordinates of our first triple by $\frac{1}{Z_P}$. Now the affine part of the projective curve E consists precisely of the points satisfying equation 2.1.1 that have a 1 as their third coordinate value, that is the points on the curve that intersect the $Z = 1$ plane in the projective plane. Thus all points P on the projective curve E of the form $[X_P : Y_P : Z_P]$ where $Z_P \neq 0$, are equivalent to a point in the affine part of the projective curve. Using this method we generally take the coordinate changes $x = X/Z$ and $y = Y/Z$ to rewrite our equation 2.1.1 of our elliptic curve to be in affine space resulting in an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (2.1.2)$$

which will be satisfied by a representative from each equivalence class of points that satisfy equation 2.1.1 except for the points whose Z -coordinate is 0.

So now we must consider any remaining points $Q = [X_Q, Y_Q, Z_Q]$ that satisfy the projective equation for E , but cannot be brought into the affine part of the projective curve E , that is points $Q = [X_Q, Y_Q, Z_Q]$ where $Z_Q = 0$. These points could not be brought into affine space by the scaling of the third coordinate as we could not divide all of the coordinates by 0. As Q satisfies equation 2.1.1, plugging in $Z_Q = 0$ into the equation gives us that $X_Q = 0$ and therefore $Q = [0 : Y_Q : 0]$. Again, by the equivalence relation in the projective plane, we get that

$$[0 : Y_Q : 0] \sim [0 : 1 : 0]$$

by dividing each coordinate by Y_Q , which will be well-defined as it must be the case that $Y_Q \neq 0$ in order for Q to be a point in the projective plane. Thus every point Q of the form $Q = [X_Q, Y_Q, Z_Q]$ such that $Z_Q = 0$ is equivalent to the point $[0, 1, 0]$, which we will call the point at infinity, denoted \mathcal{O} . Therefore if we take all of the points satisfying 2.1.2 in addition to the point at infinity, then we will have a representative from each equivalence class of points that lie on the projective curve E .

Definition 2.1.6. An **elliptic curve** E over a field K , denoted E/K , is a projective, non-singular algebraic curve of genus 1 that contains an additional K -rational point. Equivalently, from [13, p.42] the equation for E/K is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.1.3)$$

such that $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$ along with \mathcal{O} , the point at infinity. \triangle

Remark 2.1.7. It is important to know that given an elliptic curve E/\mathbf{Q} defined by the equation

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

we can actually conclude that $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}$. This will be an important facet to many of our computations. \diamond

The possible solutions on an elliptic curve E are dependent on the field over which one is looking for solutions. You may have solutions over some fields, while other fields yield no solutions other than the point at infinity. Given an elliptic curve E and a field K we denote the set of points on E that are K -rational by $E(K)$.

Example 2.1.8. Consider the curve $V : x^2 + y^2 + 1 = 0$. Note that $V(\mathbf{R}) = \emptyset$ as there are no real solutions on the curve V because that would imply that the square of a real number was negative. However $0^2 + i^2 + 1 = -1 + 1 = 0$ and thus $(0, i)$ is a solution to V . Therefore $(0, i) \in V(\mathbf{C})$ and thus $V(\mathbf{C}) \neq \emptyset$. So certainly $V(\mathbf{R}) \neq V(\mathbf{C})$. \diamond

Given an elliptic curve E , graphing $E(\mathbf{R})$ will always result in a curve of either one or two components that will resemble one of the two images below:

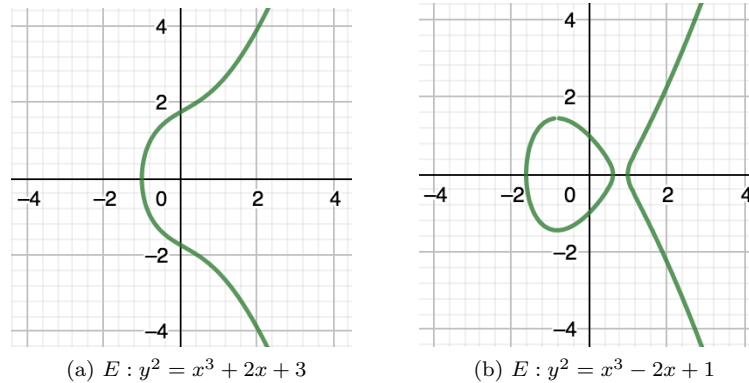


Figure 2.1.1: The graphs of \mathbf{R} -rational solutions of elliptic curves have one or two components.

One can consider an elliptic curve over many different fields. Given a field K , such that $\text{char}(K) \neq 2, 3$, and an elliptic curve E/K , one can make algebraic substitutions to take the equation for the curve into a different form called the short Weierstrass form. We will mainly be focused with elliptic curves over \mathbf{Q} . Note that when we are considering elliptic curves over \mathbf{Q} we will always be able to make these algebraic substitutions for our curves as $\text{char}(\mathbf{Q}) = 0$. We will now explain the algorithm that is used to get the short Weierstrass form for an equation of an elliptic curve.

Algorithm 2.1.9. Let E/K be an elliptic curve over K where $\text{char}(K) \neq 2, 3$, given by the equation

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

Define

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \quad (2.1.4)$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \quad (2.1.5)$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \quad (2.1.6)$$

From these substitutions we get that

$$E : y^2 = x^3 + Ax + B,$$

where $A = -27c_4$ and $B = -54c_6$. ◇

Definition 2.1.10. An elliptic curve E/K given by the equation

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in \bar{K}$ is said to be in **short Weierstrass form**. △

The short Weierstrass form of E provides the equation for an elliptic curve E' that is isomorphic to E . The concept of isomorphic elliptic curves will be explored more later. What is important for now is that we will eventually only consider curves in short Weierstrass form for our count. To conduct our count and determine our probabilities we will actually be counting the number of isomorphism classes of curves that satisfy certain characteristics. Thus only considering curves in short Weierstrass form will not impact our calculation of the probability because within every isomorphism class of elliptic curves there will be one so-called minimal model in short Weierstrass form.

Example 2.1.11. We will take the elliptic curve given by the equation

$$E : y^2 + xy + y = x^3 - x$$

into short Weierstrass form. From the notation above we have $a_1 = 1, a_2 = 0, a_3 = 1, a_4 = -1$, and $a_6 = 0$. This gives us

$$b_2 = a_1^2 + 4a_2 = (1)^2 + 4(0) = 1, \quad b_4 = 2a_4 + a_1a_3 = 2(-1) + (1)(1) = -1,$$

$$b_6 = a_3^2 + 4a_6 = (1)^2 + 4(0) = 1,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = (1)^2(0) + 4(0)(0) - (1)(1)(-1) + (0)(1)^2 - (-1)^2 = 2$$

$$c_4 = b_2^2 - 24b_4 = (1)^2 - 24(-1) = 25,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6 = -(1)^3 + 36(1)(-1) - 216(1) = -253.$$

Substituting in these values will yield the curve

$$E : y^2 = x^3 - 27c_4x + -54c_6,$$

which gives

$$E : y^2 = x^3 - 675x + 13662.$$

◇

The equations for the variables used to bring an elliptic curve equation into short Weierstrass form, given in 2.1.5 and 2.1.6, will be used to define a variety of concepts concerning elliptic curves. The equations in 2.1.5 and 2.1.6 are very connected to the characteristics of an elliptic curve as they are defined using the coefficients of the curve itself. For example, we can now define the discriminant of a curve based on these equations.

Definition 2.1.12. Let E be an elliptic curve given by the equation

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

then

$$\Delta(E) = -b_2^2b_8 = 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where $b_2, b_4,$ and b_6 are defined as in equations 2.1.5. △

Remark 2.1.13. If E is in short Weierstrass form and thus can be defined by an equation of the form

$$E : y^2 = x^3 + Ax + B,$$

then

$$\Delta(E) = -16(4A^3 + 27B^2).$$

◇

Recall that if E is an elliptic curve, then by definition E is non-singular. We can detect whether or not a curve is non-singular by looking at the discriminant of the equation defining the curve. The way in which the discriminant can reveal whether or not a curve is singular depends on its relationship to the partial derivatives of the function defining the curve. These partial derivatives determine where and where not a curve is singular.

Proposition 2.1.14. [13, p.44] *Let E be a curve defined by the equation $f(x, y) = 0$. Then there exists a point $P = (x_0, y_0)$ on E such that P is a singular point if and only if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$.*

There are multiple ways in which singularities occur on curves. From [13, p.43], if a curve does contain singular points then these singularities would manifest geometrically as a cusp or a node as seen below.

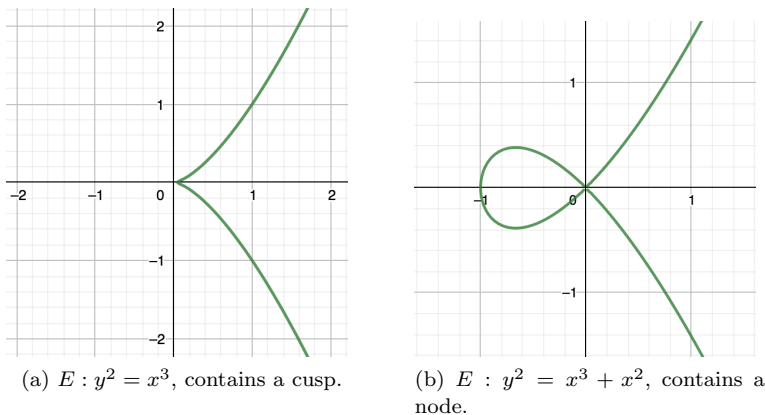


Figure 2.1.2: Singular Curves Have Either a Cusp or Node.

Let C be a curve defined by the equation $f(x, y) = 0$. From Proposition 2.1.14 we can conclude that if for all points P on the curve C we have that $\nabla f(P)$ is not the zero vector, then C is nonsingular. Note that by a change of variables on our curve we get that if $\nabla f = \vec{0}$ then $\Delta(C) = 0$ [13, p.46]. Additionally, if we suppose that $\Delta(C) = 0$ we get that $\nabla f = \vec{0}$ due to the fact that when $\Delta(C) = 0$ this implies that the curve C has a double root at some point on the curve [13, p.47]. Thus we can conclude that $\nabla f = \vec{0}$ if and only if $\Delta(C) = 0$, which leads us to the following proposition.

Proposition 2.1.15. [13, p.45] *Given a curve C , defined by a Weierstrass equation we get that C is nonsingular if and only if $\Delta(C) \neq 0$.*

Note that this proposition is written incorrectly in [13, p.45] where it states that a curve C is nonsingular if and only if $\Delta(C) = 0$. It appears that the word “nonsingular” was meant to be recorded as “singular”.

As an example of Proposition 2.1.15, consider the left image of Figure 2.1.2 where we have graphed the curve given by the equation $C_1 : y^2 = x^3$, note that C_1 is in short Weierstrass form. Thus we can easily calculate

$$\Delta(C_1) = -16(4A^3 + 27B^2) = -16(0) = 0.$$

As $\Delta(C_1) = 0$, this tells us that C_1 is singular, which can be seen by the presence of the cusp in the graph.

2.2 The Group Law on Elliptic Curves

One aspect of elliptic curves that makes them interesting to study is their group structure that forms by using a kind of composition of points, sometimes called “addition,” given by the Composition Law on the points of an elliptic curve. Let E/K be an elliptic curve given by the equation

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

such that $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$.

Given two points P and Q on the elliptic curve E , the binary operation which calls on the use of the Composition Law on these two points is denoted $P \oplus Q$. To explain how we calculate $P \oplus Q$, we must first recall Bézout’s Theorem.

Theorem 2.2.1 (Bézout’s Theorem). [10, p.32] *Given two curves C_1 and C_2 of degree m and n , respectively, the sum of the multiplicities at each of the points of the intersection of C_1 and C_2 is equal to mn .*

Let E be an elliptic curve. Let P and Q be points on E . Suppose for this case that $P \neq Q$. Let ℓ be the line through P and Q . Note that $\dim E = 3$ and $\dim \ell = 1$. Therefore by Bézout’s Theorem the multiplicities of the points of intersection of E and ℓ will sum to 3. Note that as ℓ is the line through P and Q that ℓ intersects those points with multiplicity at least 1. Therefore ℓ will intersect E at a third point. Call this point R . Let ℓ' be the vertical line through the point R and \mathcal{O} , the point at infinity. Similarly to before, ℓ' will intersect E at a third point, which we will call S . The Composition Law [13, p.51] gives us that

$$P \oplus Q = S.$$

This process for the Composition law when $P \neq Q$ can be seen in Figure 2.2.1 below.

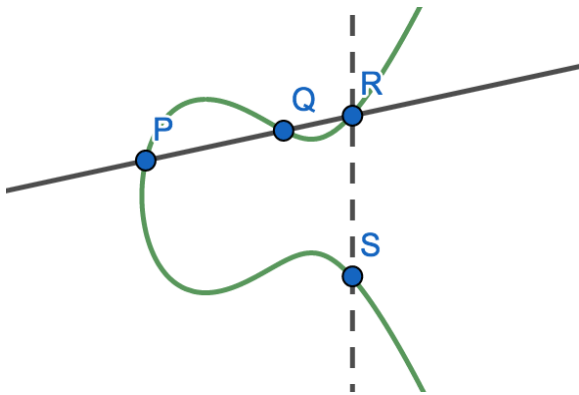


Figure 2.2.1: The Composition Law on Two Distinct Points.

Still working on our elliptic curve E we would again like to find $P \oplus Q$, but now suppose that $P = Q$. That is, we would like to evaluate $P \oplus P$. In this case, we take the line ℓ that intersects P with multiplicity 2, that is ℓ is the tangent line to E at P . As ℓ intersects P with multiplicity 2, again by Bézout’s Theorem we get that ℓ will then intersect E at a third point which we will call R . Again we let ℓ' be the vertical line through R and \mathcal{O} and let S be the third point on E

that is intersected by ℓ' . We arrive at the result of the Composition Law [13, p.51]

$$P \oplus Q = P \oplus P = S.$$

A geometric example of adding a point to itself is shown below in Figure 2.2.2.

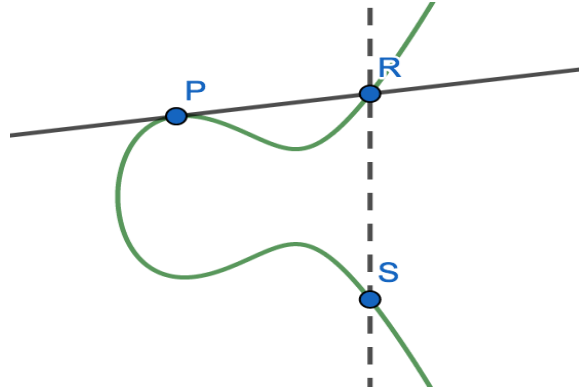


Figure 2.2.2: The Composition Law on a Single Point.

There are now a couple special cases that could occur when computing $P \oplus Q$. All of the cases still follow the Composition Law, and so we mention them only to clear up any confusion these specific cases may bring about how the Composition Law works.

Remark 2.2.2. Note that when evaluating $P \oplus Q$ that the point R , at which the line through P and Q will intersect E at a third point, is not necessarily distinct from the points P or Q . It is possible for the line ℓ to be tangent to E at one of these points such that ℓ at P or ℓ at Q has multiplicity 2 on E . However, if $R = P$ or $R = Q$, this will not impact how we proceed. Similarly, S is not necessarily distinct from R and \mathcal{O} , but again this does not impact the algorithm of the Composition Law. \diamond

Remark 2.2.3. It is also important to note that when calculating $P \oplus Q$, that if ℓ is vertical, the other point of intersection with E will be \mathcal{O} , the point at infinity, as the point at infinity is the point at which all vertical lines intersect. In this case, the result of the addition is simply the point at infinity. \diamond

Proposition 2.2.4. [13, p.51] *Let E be an elliptic curve. This Composition Law of points that was just described holds the following properties:*

(a) *Let ℓ be a line that intersects E at the points P , Q , and R , then regardless of whether or not these points are distinct we get that*

$$(P \oplus Q) \oplus R = \mathcal{O}.$$

(b) *The Composition Law has an identity. Let $P \in E$. Then $P \oplus \mathcal{O} = P$ and $\mathcal{O} \oplus P = P$.*

(c) *The Composition Law is commutative. Let $P, Q \in E$. Then $P \oplus Q = Q \oplus P$.*

(d) *The Composition Law has inverses. Let $P \in E$. Then by the Composition Law there exists another point of E , which we will denote $(-P)$ such that*

$$P \oplus (-P) = \mathcal{O},$$

(e) *The Composition Law is associative. Let $P, Q, R \in E$. Then*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

We have previously claimed that using this binary operation, defined by the Composition Law, on an elliptic curve will result in a group structure. Thus we require closure, an identity, inverses, and associativity. From the explanation of the Composition Law it is clear that given points P and Q on E , then the result of $P \oplus Q$ is a point on E . Thus this binary operation is closed on the elliptic curve. Therefore parts (b), (d), and (e) of 2.2.4 will give us that the set of points on an elliptic curve under the binary operation of the composition law will form a group. From part (c) we get that this is not just a group, but actually an abelian group.

Proof of Proposition. 2.2.4 We follow the proof as given in [13, p.52] with slight adjustments.

(a) Let P , Q , and R be collinear points on E . To calculate $P \oplus Q$ let ℓ be the line through P and Q . As P , Q , and R are collinear, we know that the third point of intersection of ℓ and

E will be precisely the point R . Suppose that $P \oplus Q = S$. Then by construction S will be the point of intersection on E of the vertical line intersecting R and \mathcal{O} . Therefore to compute $S \oplus R$ the line through S and R will be the vertical line for which the third point of intersection on E will be at \mathcal{O} . Therefore we get that

$$(P \oplus Q) \oplus R = S \oplus R = \mathcal{O}.$$

(b) Let P be a point on E . To calculate $P \oplus \mathcal{O}$ we let ℓ be the line through P and \mathcal{O} . Let R be the third point of intersection of E and ℓ . If you then let ℓ' be the vertical line through R and \mathcal{O} , the third point of intersection on E will certainly be P . Thus $P \oplus \mathcal{O} = P$, and from (c) we get that $\mathcal{O} \oplus P = P$. Note all of this holds regardless of whether or not $P = R$.

(c) Let P and Q be points on E . When computing $P \oplus Q$ versus $Q \oplus P$, the line that intersects both points in order to find the third point of intersection will not be altered. Therefore their results are the same so that $P \oplus Q = Q \oplus P$.

(d) Let P be a point on E . Let ℓ be the line passing through P and \mathcal{O} . Let R be the third point of intersection of ℓ with the elliptic curve E . Note then that P , \mathcal{O} , and R are collinear, and thus from (a) we get that

$$\mathcal{O} = (P \oplus \mathcal{O}) \oplus R = P \oplus R.$$

Thus we get that R is the inverse of P under our binary operation.

(e) The proof of this part is a little too complex and lengthy to include. A proof of the associativity of the Composition Law can be found in [14, p.19-20]. \square

Remark 2.2.5. If our elliptic curve E is in short Weierstrass form, and therefore given by some equation of the form

$$E : y^2 = x^3 + Ax + B,$$

then our elliptic curve is symmetric about the x -axis, which is clear from the equation of E . This provides a lot of nice shortcuts for the Composition Law. For example, given a point $P = (x, y)$ on an elliptic curve E , we can show that the inverse of P , denoted $-P$ is given exactly by $-P = (x, -y)$, which by the symmetry of E will also be a rational point on our elliptic curve. Let L be the line through P and $-P$. By construction L is certainly a vertical line and thus this line will intersect E at \mathcal{O} , as the point at infinity is the point at which all vertical lines will intersect. \diamond

In addition to the geometric perspective that we have given on how to apply the Composition Law to points on an elliptic curve there is an algorithm that can be used to algebraically calculate the exact coordinates of the point that results from the composition of two points on an elliptic curve. We will take the Group Law Algorithm as given in [13, p. 54].

Algorithm 2.2.6 (Group Law Algorithm). [13, p. 54] Let E be an elliptic curve with the following Weierstrass equation

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

and suppose that $P_1 \oplus P_2 = P_3$ where $P_i = (x_i, y_i)$ for all $i \in \{1, 2, 3\}$.

(a) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$ we get that $P_1 \oplus P_2 = \mathcal{O}$.

(b) If $x_1 \neq x_2$ then

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + a_1 \left(\frac{y_2 - y_1}{x_2 - x_1} \right) - a_2 - x_1 - x_2,$$

$$y_3 = - \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right) + a_1 \right) x_3 - \left(\frac{y_1x_2 - y_2x_1}{x_2 - x_1} \right) - a_3.$$

(c) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 \neq 0$ then

$$x_3 = \left(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \right)^2 + a_1 \left(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \right) - a_2 - x_1 - x_2,$$

$$y_3 = - \left(\left(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \right) + a_1 \right) x_3 - \left(\frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \right) - a_3.$$

From (c) we can look at the special case when $P_1 = P_2$, Silverman in [13, p.54] gives the duplication formula for $P = (x, y)$ so that for all $P \in E$ we get

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

where b_2, b_4, b_6 , and b_8 are defined as in equations 2.1.5, and $x([2]P)$ simply denotes the x -coordinate of the point $[2]P$. ◇

As shown above by the duplication formula, it is possible to add a point to itself. Sometimes we may wish to add a point to itself numerous times. We will denote this $[m]P = \underbrace{(P \oplus P \oplus \cdots \oplus P)}_{m \text{ summands}}$.

Definition 2.2.7. Given a point $P \in E$, suppose that $m[P] = \mathcal{O}$ for some $m \in \mathbb{Z}$, then we say that the point P is a **torsion point** of E . If m is minimal, that is if $[\ell]P \neq \mathcal{O}$ for all $\ell \in \mathbf{N}$ such that $0 < \ell < m$, then we say that P has order m and also call P an **m -torsion point**. △

Definition 2.2.8. Let E be an elliptic curve. The set of all points on E with order m is called the **m -torsion subgroup** of E and is denoted

$$E[m] = \{P \in E \mid [m]P = \mathcal{O}\}.$$

△

Note that it is not a coincidence that we called this set of points a subgroup. If you compose two points of order m , the resulting point will still be of order m , which makes this set closed under the binary operation given by the Composition Law. And certainly all of the rest of the necessary items to make this set a group will hold by Proposition 2.2.4.

Definition 2.2.9. The set of all torsion points on E over \mathbf{Q} , is called the **torsion subgroup of E** and is denoted $E(\mathbf{Q})_{\text{tor}}$. △

This structure of this subgroup will play a large role in determining the structure of $E(\mathbf{Q})$, the set of all rational points on an elliptic curve E . Recall that we provided a theorem of Mazur's, which tells us that there are only finitely many ways in which an elliptic curve can have torsion.

Theorem 2.2.10 (Mazur). [13, p.242] *Let E be an elliptic curve over \mathbf{Q} . Then the torsion subgroup of $E(\mathbf{Q})$ will have one of the following structures*

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/n\mathbf{Z} \text{ such that } 1 \leq n \leq 10 \text{ or } n = 12$$

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \text{ such that } n = 1, 2, 3, 4.$$

Determining the structure of $E(\mathbf{Q})_{\text{tor}}$ can be done easily once all torsion points are identified. Note there are always finitely many torsion points as can be deduced by Theorem 2.2.10. Nagell-Lutz Theorem provides a simple way to look for and identify torsion points on elliptic curves in short Weierstrass form.

Theorem 2.2.11 (Nagell-Lutz Theorem). [14, p.56] *Given an elliptic curve E/\mathbf{Q} in the form*

$$E : y^2 = x^3 + Ax + B,$$

then if $P \in E(\mathbf{Q})_{\text{tor}}$ and $P = (x, y)$, we get that $x, y \in \mathbf{Z}$ and either $y = 0$, in which case P is a finite point of order 2, or y divides the discriminant of the curve E .

If we find a torsion point of order m , and there are no rational points of order 2, other than m itself when $m = 2$, then we know that $E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/m\mathbf{Z}$. If there is a rational point of order 2 in addition to our rational point of order m then $E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. Once we have determined the structure of $E(\mathbf{Q})_{\text{tor}}$ we can begin to determine the structure of $E(\mathbf{Q})$ by the Mordell-Weil Theorem.

Theorem 2.2.12 (Mordell-Weil Theorem). [13, p.207] *The group of rational points on an elliptic curve E , denoted $E(\mathbf{Q})$, is finitely generated such that $E(\mathbf{Q}) \cong \mathbf{Z}^r \times E(\mathbf{Q})_{\text{tor}}$, where r is the rank of $E(\mathbf{Q})$.*

2.3 Reducing a Curve Modulo p

Given an elliptic curve E/\mathbf{Q} defined by the equation

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

then E also defines an equation modulo p as well, which we will denote \widehat{E} . However, \widehat{E} is not necessarily an elliptic curve, as that would require that \widehat{E} be non-singular. Therefore in order for \widehat{E} to be an elliptic curve, the discriminant of \widehat{E} must be nonzero. We call primes p such that $p \nmid \Delta(E)$ good primes. These p are called good primes because if we reduce an elliptic curve modulo p such that p does not divide the discriminant of E , then the discriminant of \widehat{E} will also be nonzero such that \widehat{E} is non-singular and thus \widehat{E} is an elliptic curve. If $p \mid \Delta(E)$, then we say E has bad reduction at p since E reduced modulo p will have a discriminant of zero and will therefore be singular and thus not an elliptic curve.

For this project we will be using the process of reducing elliptic curves modulo p to deduce whether an elliptic curve does or does not have local ℓ -divisibility. The curves for which we perform this reduction will mainly be in short Weierstrass form based on the models that we will be using to parameterize curves with each kind of divisibility. So we will mainly discuss what reducing an elliptic curve modulo p would mean for curves in Short Weierstrass form.

Theorem 2.3.1. Reduction Modulo p Theorem [14, p.123] *Let E/\mathbf{Q} be an elliptic curve given by the equation*

$$E : y^2 = x^3 + Ax + B.$$

Let $\Delta(E)$ be the discriminant of E . Let

$$\widehat{E} : y^2 = x^3 + \widehat{A}x + \widehat{B}$$

where $A \equiv \widehat{A} \pmod{p}$ and $B \equiv \widehat{B} \pmod{p}$. Then reduction modulo p map with $E(\mathbf{Q})_{tors}$ as its domain is a isomorphism that maps $E(\mathbf{Q})_{tors}$ to a subgroup of $\widehat{E}(\mathbf{F}_p)$ provided that $p \nmid \Delta(E)$.

Note that this reduction modulo p will be undefined only if we try to reduce a rational number with a denominator that vanishes modulo p . From Remark 2.1.7 we know that for the elliptic curve E/Q above we have that $A, B \in \mathbf{Z}$. Therefore the reduction modulo p on these coefficients will be well-defined modulo all primes p . This does not suggest that the curve resulting from reducing an elliptic curve over the rationals modulo a prime p will always be an elliptic curve though as it could still be the case that $p|\Delta(E)$.

Remark 2.3.2. From Theorem 2.3.1 we get that when p is a good prime, then by Lagrange's Theorem we have that $\#E(\mathbf{Q})_{\text{tor}}|\#E(\mathbf{F}_p)$. This follows from the fact that the image of the torsion subgroup under the natural reduction map on E will form a subgroup of $\#E(\mathbf{F}_p)$ and we know that this map is injective, and thus the size of the image of $E(\mathbf{Q})_{\text{tor}}$ under this natural reduction map is the same size as $E(\mathbf{Q})_{\text{tor}}$ itself. Thus we can deduce that given some $\ell \in \mathbb{N}$ such that $\ell|\#E(\mathbf{Q})_{\text{tor}}$ then $\ell|\#E(\mathbf{F}_p)$ for all good primes p . This fact is a key facet with which this project is concerned ◇

2.4 Our Question

We must define a few more characteristics of elliptic curves in order to understand the problem that we are trying to work with. One such characteristic is called isogeny.

Definition 2.4.1. [13, p.66] Given two elliptic curves E_1 and E_2 , a morphism $\phi : E_1 \rightarrow E_2$ such that $\phi(\mathcal{O}) = \mathcal{O}$ is called an **isogeny**. △

Definition 2.4.2. Let E_1 and E_2 be two elliptic curves. Then E_1 and E_2 are in the same isogeny class, that is they are **isogenous**, if and only if there exists a nonzero isogeny $\phi : E_1 \rightarrow E_2$. △

Remark 2.4.3. Note that local divisibility is preserved by isogeny, as we will show in Chapter 4, and thus one way to prove a curve has local ℓ -divisibility is to prove that it is isogenous to a different curve with local ℓ -divisibility. ◇

Theorem 2.4.4. *Given $\ell \in \mathbb{N}$ and elliptic curve E over \mathbf{Q} then if E has an ℓ -torsion point, that is if ℓ divides $\#E(\mathbf{Q})_{\text{tor}}$, then ℓ divides $\#E(\mathbf{F}_p)$ for all good primes p .*

Proof. This theorem follows easily from the fact that for all good primes p we get that the map $E(\mathbf{Q})_{\text{tor}} \rightarrow E(\mathbf{F}_p)$ is injective. The explanation of why Theorem 2.4.4 follows from this injective property of the reduction map is explained in Remark 2.3.2 \square

It is Theorem 2.4.4 that gives us the fact that curves with an ℓ -torsion point will always have local ℓ -divisibility. However, the converse is not necessarily true. An elliptic curve can have local ℓ -divisibility without having ℓ -torsion. Furthermore, a result of Katz [9, Theorem 2] says that if m is the gcd of $\#E(\mathbf{F}_p)$ over all good primes p , then there exists some E' isogenous to E such that E' has a rational subgroup of order m .

Example 2.4.5. To see an example of these relationships between curves with different kinds of divisibility consider the elliptic curve E defined by the equation

$$E : y^2 + y = x^3 - x^2 - 7820x - 263580.$$

Note that E does not have 5-torsion, that is E has no points of order 5, which can be shown easily by a simple computation in PARI. Additionally by Remark 2.4.3, we can show that E has local 5-divisibility by finding an isogenous elliptic curve with local 5-divisibility as local divisibility is preserved by isogenies.

Let E' be an elliptic curve defined by the equation

$$E' : y^2 + y = x^3 - x^2.$$

Note that E is isogenous to E' . Furthermore, E' contains the point $P = (0, 0)$, which on this curve is a point of order 5 as simple calculations in PARI show that $[5]P = \mathcal{O}$. Thus we can conclude that E' has 5-torsion and therefore local 5-divisibility, and thus E will have local 5-

divisibility. Thus we can conclude that E is an elliptic curve with local 5-divisibility and no 5-torsion. \diamond

Now that we have a better understanding of elliptic curves we will restate the problem:

Given an elliptic curve E such that 5 or 7 divides the number of points on E over F_p , for all good primes p , what is the probability that E has a 5 or 7 torsion point, respectively?

In order to find this probability we must count the elliptic curves that satisfy this property in comparison to those that do not satisfy the property. We will count elliptic curves by counting the number of isomorphism classes, which we will define later, of elliptic curves up to some height. Recall from Definition 1.0.7 that given an elliptic curve E over \mathbf{Q} defined by the equation $y^2 = x^3 + Ax + B$, then the height of E , denoted $\text{ht } E$ is given by the equation

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

Furthermore, recall the notation of the following sets. We denote the set of all minimal models of elliptic curves up to some height H

$$\mathcal{E}_{\leq H} = \{E \in \mathcal{E} \mid \text{ht } E \leq H\},$$

and we denote the set of all minimal models of elliptic curves that have local ℓ -divisibility

$$\mathcal{E}_{\ell?} = \{E \in \mathcal{E} \mid \ell \mid \#E(\mathbf{F}_p) \text{ for a set of primes } p \text{ of density } 1\}.$$

Using this notation, we define the probability to be the limit of the sequence of quotients

$$P_\ell = \lim_{H \rightarrow \infty} \frac{\#\{E \in \mathcal{E}_{\leq H} \mid \ell \mid \#E(\mathbf{Q})_{\text{tor}}\}}{\#\{E \in \mathcal{E}_{\leq H} \cap \mathcal{E}_{\ell?}\}}.$$

Thus P_ℓ gives the probability that a curve has ℓ -torsion assuming that it has a local ℓ -divisibility modulo all good primes p .

In [3] Cullinan and Voight prove that this probability exists. To show that this probability exists it is important to note that if you take a finite number X , there will only be finitely many curves of height less than or equal to X . This follows from the fact that considering a maximum height results in a maximum value allowed on the coefficients of an elliptic curve E given by the equation

$$E : y^2 = x^3 + Ax + B.$$

As $A, B \in \mathbf{Z}$ and both must be less than a finite value, this leaves a finite number of options for A and B and thus finitely many curves that will satisfy the assumption that they have height less than or equal to some height X . Note that the number of elliptic curves with local m -divisibility of height less than or equal to X will certainly also be finite for all all finite values of X , as will the number of elliptic curves with local m -torsion. Thus this quotient, for all finite X , will always be the quotient of two finite numbers. Therefore we know that this sequence of quotients will make sense to compute in order to give us our desired probability. We will now work to compute the probabilities P_5 and P_7 , which represent the probability that an elliptic curve with local ℓ -divisibility has a rational subgroup of order ℓ , for $\ell = 5$ and $\ell = 7$.

3

Parameterizations of Elliptic Curves

Recall that we are working to determine

$$P_\ell = \lim_{H \rightarrow \infty} \frac{\#\{E \in \mathcal{E}_{\leq H} \mid \ell \mid \#E(\mathbf{Q})_{\text{tor}}\}}{\#\{E \in \mathcal{E}_{\leq H} \cap \mathcal{E}_{\ell^?}\}}.$$

for $\ell = 5$ and $\ell = 7$. By the formula for P_ℓ , to calculate this ratio requires that we are able to count the number of minimal models of elliptic curves which have ℓ -torsion, and the number of minimal models of elliptic curves which have local ℓ -divisibility without ℓ -torsion, both up to some height X . For now it is important to note that every isomorphism class of elliptic curves contains one minimal model of an elliptic curve in short Weierstrass form, and therefore counting the number of minimal models satisfying a certain characteristic is equivalent to counting the number of isomorphism classes satisfying that same certain characteristic. Note that this means we will only count one representative from each isomorphism class in our count.

Thus we will start by working with a universal model for elliptic curves that will contain a representative from each isomorphism class of elliptic curves with ℓ -torsion. We know these models exist as they are used in the paper [4], which works with the Tate normal form in relation to certain torsion subgroups of elliptic curves.

Theorem 3.0.1. [4, p.80] *Let E be an elliptic curve with a torsion point of order ℓ where $\ell \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, then the equation that defines E is isomorphic to an elliptic curve E' that lies in a one-parameter family of curves, called the Tate normal form, where this one-parameter family accounts for all elliptic curves, up to isomorphism, that have ℓ -torsion.*

To determine our desired probabilities we will consider the universal models of the one-parameter families that contain, up to isomorphism, all curves with 5-torsion and all curves with 7-torsion. Again, we are only counting one curve from each isomorphism class, and thus we can then take these universal models to an isomorphic curve in short Weierstrass form. Recall that given an elliptic curve E in short Weierstrass form defined by the equation

$$E : y^2 = x^3 + Ax + B$$

that $ht(E) = \max\{|4A|^3, |27B|^2\}$. Therefore considering these parameterizations in short Weierstrass form, we can then count all isomorphism classes of curves with our prescribed torsion up to a certain height X because the height is dependent only on the values of the coefficients of the equations for our universal models that we will be using. To achieve these parameterizations we start by considering the Tate normal form of an elliptic curve as defined in [7, p.93].

3.1 The Tate Normal Form

Definition 3.1.1. [7, p. 85] Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. The **Tate normal form** of an elliptic curve E with a torsion point of order m is given by the equation

$$E = E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where the polynomial conditions that must be satisfied by b and c are determined by the exact value of m . △

Remark 3.1.2. Let E be an elliptic curve in Tate Normal Form with m -torsion. Suppose P is the point of order m on E . Then by the construction of the Tate normal form we get that $P = (0, 0)$. \diamond

As our point of order m will always be at $(0, 0)$, regardless of the value of m , we can then add P to itself any finite number of times and evaluate this point addition in terms of the coefficients of the elliptic curve in the generalized Tate normal form. In the equation for the Tate normal form these coefficients are written as polynomials of the variables b and c . This results in some of the following equations:

$$P = (0, 0), \quad 2P = (b, bc), \quad 3P = (c, b - c), \quad 4P = \left(\frac{b}{c} \left(\frac{b}{c} - 1 \right), \left(\frac{b}{c} \right)^2 \left(c - \frac{b}{c} + 1 \right) \right),$$

$$-P = (0, b), \quad -2P = (b, 0), \quad -3P = (c, c^2), \quad -4P = \left(\frac{b}{c} \left(\frac{b}{c} - 1 \right), \frac{b}{c} \left(\frac{b}{c} - 1 \right)^2 \right).$$

These equations for the multiples of P evaluated on the general equation for the Tate normal form will allow us to solve for the polynomial values of b and c that will result in our desired torsion. We find these polynomials by setting equal the multiples of P which are equivalent when P has a certain torsion order. For example, as we will see in the subsequent section, when we would like a model with 5-torsion, then the point given by $2P$ should result in the same point as $-3P$ as $2 \equiv -3 \pmod{5}$.

3.2 Curves with a Rational Subgroup of Order 5

We start with the elliptic curve E in Tate Normal Form

$$E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

given in [7, p.94].

Note, as given above, that if we would like P to be a point of order 5 it must be true that $2P = -3P$. Note

$$2P = (b, bc) \quad \text{and} \quad -3P = (c, c^2).$$

Therefore $(b, bc) = (c, c^2)$. So clearly we require that $b = c$. This explanation can be found on [7, p.94].

Therefore from [4, p. 80] we get that an elliptic curve with a point of order 5 can be given by the following general equation in Tate Normal form

$$E : y^2 + (1 - t)xy - ty = x^3 - tx^2$$

for some $t \in \mathbf{Q}$.

Recall that we defined the height of an elliptic curve E to be calculated by looking at the coefficients of the equation for E in short Weierstrass form. As we would like to eventually find models that will allow us to order elliptic curves based on their height, we will find the short Weierstrass model of the Tate normal form equation for elliptic curves with 5-torsion. Doing so will allow us to easily assess the height for all curves in this universal model, and therefore we will be able to efficiently conduct our count of the isomorphism classes of elliptic curves with 5-torsion.

Using Algorithm 2.1.9 we let

$$\begin{aligned} a_1 &= 1 - t, & a_2 &= -t, & a_3 &= -t, & a_4 &= 0, & a_5 &= 0 \\ b_2 &= a_1^2 + 4a_2, & b_4 &= 2a_4 + a_1a_3, & b_6 &= a_3^2 + 4a_6 \\ c_4 &= b_2^2 - 24b_4, & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Then we get that

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Rewriting this equation to get the short Weierstrass form with coefficients that are functions of t , we get that the general equation for a curve E over \mathbf{Q} with a point of order 5 is given by the equation

$$E : y^2 = x^3 + f(t)x + g(t),$$

$$f(t) = -27c_4 = -27t^4 + 324t^3 - 378t^2 - 324t - 27,$$

$$g(t) = -54c_6 = 54t^6 - 972t^5 + 4050t^2 + 972t + 54.$$

However for these equations it need only be the case that $t \in \mathbf{Q}$. We would like an integral model of these equations. Thus we set $t = \frac{a}{b}$ assuming that $a, b \in \mathbf{Z}$ and with some simple algebra get the following integral model for the general equation of an elliptic curve E with a point of order 5:

$$y^2 = x^3 + A(a, b)x + B(a, b),$$

$$A(a, b) = -27a^4 + 324a^3b - 378a^2b^2 - 324ab^3 - 27b^4, \quad (3.2.1)$$

$$B(a, b) = 54a^6 - 972a^5b + 4050a^4b^2 + 4050a^2b^4 + 972ab^5 + 54b^6, \quad (3.2.2)$$

Example 3.2.1. Let $a = 2$ and $b = 7$. We will now consider the elliptic curve E given by the equation

$$E : y^2 = x^3 + A(a, b)x + B(a, b),$$

and show that E has 5-torsion. We get that $A(a, b) = -343467$ and $B(a, b) = 80882982$, which yields the equation

$$E : y^2 = x^3 - 343467x + 80882982.$$

Let $P = (-93, 10584)$. Note that $P \in E(\mathbf{Q})$. The following points arise as multiples of P :

$$2P = (411, -3024), \quad 3P = (411, 3024), \quad 4P = (-93, -10584), \quad 5P = \mathcal{O}.$$

Therefore we get that P is a torsion point of order 5, and thus E has 5-torsion by construction as was desired. \diamond

3.3 Curves with a Rational Subgroup of Order 7

Similar to our work with $\ell = 5$ we begin by examining the Tate normal form for a curve with 7-torsion.

Recall from [7, p.94] that given the elliptic curve E in Tate normal form

$$E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

we get the following

$$P = (0, 0), \quad 2P = (b, bc), \quad 3P = (c, b - c), \quad 4P = \left(\frac{b}{c} \left(\frac{b}{c} - 1 \right), \left(\frac{b}{c} \right)^2 \left(c - \frac{b}{c} + 1 \right) \right),$$

$$-P = (0, b), \quad -2P = (b, 0), \quad -3P = (c, c^2), \quad -4P = \left(\frac{b}{c} \left(\frac{b}{c} - 1 \right), \frac{b}{c} \left(\frac{b}{c} - 1 \right)^2 \right).$$

As $4 \equiv -3 \pmod{7}$, then in order for P to be a torsion point of order 7 we require that $4P = -3P$, that is, we want

$$\left(\frac{b}{c} \left(\frac{b}{c} - 1 \right), \left(\frac{b}{c} \right)^2 \left(c - \frac{b}{c} + 1 \right) \right) = (c, c^2).$$

Thus some simple calculations yield $c^3 = b^2 - bc$, which then gives the polynomial equations $c = t^2 - t$ and $b = t^3 - t^2$ for some $t \in \mathbf{Q}$. More details of this can be found in [7, p.95].

Therefore from [4, p. 80] we get that an elliptic curve with a point of order 7 can be given by the general equation in Tate Normal form

$$E : y^2 + (1 - t^2 + t)xy - (t^3 - t^2)y = x^3 - (t^3 - t^2)x^2.$$

We will than use the same method from [13, p. 42] to get the short Weierstrass model for this Tate normal form equation.

To use this method, as was done in 2.1.9 we define the following variables

$$a_1 = 1 - t^2 + t, \quad a_2 = t^3 - t^2, \quad a_3 = t^3 - t^2, \quad a_4 = 0, \quad a_5 = 0 \quad (3.3.1)$$

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \quad (3.3.2)$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \quad (3.3.3)$$

Then from 2.1.9 we get that

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Plugging in our values for c_4 and c_6 , we get that the general equation for a curve E over \mathbf{Q} with a point of order 7 is given by the equation

$$\begin{aligned} y^2 &= x^3 + f(t)x + g(t), \\ f(t) &= -27t^8 + 324t^7 - 1134t^6 + 1512t^5 - 945t^4 + 378t^2 - 108t - 27, \\ g(t) &= 54t^{12} - 972t^{11} + 6318t^{10} - 19116t^9 + 30780t^8 - 26244t^7 \\ &\quad + 14742t^6 - 11988t^5 + 9396t^4 - 2484t^3 - 810t^2 + 324t + 54. \end{aligned}$$

However, in these equations it need only be the case that $t \in \mathbf{Q}$. We would like an integral model of these equations. Thus we set $t = \frac{a}{b}$ assuming that $a, b \in \mathbf{Z}$ and get the following integral model for the general equation of an elliptic curve E with a point of order 7

$$\begin{aligned} y^2 &= x^3 + A(a, b)x + B(a, b), \\ A(a, b) &= -27a^8 + 324a^7b - 1134a^6b^2 + 1512a^5b^3 - 945a^4b^4 + 378a^2b^6 - 108ab^7 - 27b^8, \\ B(a, b) &= 54a^{12} - 972a^{11}b + 6318a^{10}b^2 - 19116a^9b^3 + 30780a^8b^4 - 26244a^7b^5 \\ &\quad + 14742a^6b^6 - 11988a^5b^7 + 9396a^4b^8 - 2484a^3b^9 - 810a^2b^{10} + 324ab^{11} + 54b^{12}. \end{aligned}$$

Example 3.3.1. Let $a = 2$ and $b = 7$. We will now consider the elliptic curve E given by the equation

$$E : y^2 = x^3 + A(a, b)x + B(a, b),$$

and show that E has 7-torsion. We get that $A(a, b) = -178629867$ and $B(a, b) = 932750547174$, which yields the equation

$$E : y^2 = x^3 - 178629867x + 932750547174.$$

Let $P = (-5517, 1323000)$. The following points arise as multiples of P :

$$2P = (12123, -740880), \quad 3P = (7083, 151200), \quad 4P = (7083, -151200),$$

$$5P = (12123, 740880), \quad 6P = (-5517, -1323000), \quad 7P = \mathcal{O}.$$

Therefore we get that P is a torsion point of order 7 and thus E has 7-torsion as desired. \diamond

We have established parameterizations for elliptic curves with our desired ℓ -torsion. Therefore to work towards computing our desired probabilities, we will now need to create a universal model for elliptic curves with ℓ -divisibility, but no ℓ -torsion for both $\ell = 5$ and $\ell = 7$. We will do so by using methods from [17] to calculate certain isogenous curves and then making use of the geometry that these isogenies provide.

4

Isogenies

Now that we have established universal models for elliptic curves with 5 and 7 torsion using Tate Normal Form, we require universal models for curves that have local ℓ -divisibility without ℓ torsion for $\ell = 5$ and $\ell = 7$. By a theorem of Katz [9], we get that every curve with local ℓ -divisibility is isogenous to a curve with rational ℓ -torsion. We use the method of Vélú to take our Tate Normal Form curves and get the corresponding isogenous curves that will preserve local ℓ -divisibility, but not ℓ -torsion. Therefore we start by exploring the concept of isogeny.

4.1 Exploring Isogenies

As we are looking for maps that preserve a part of the group structure of the curves it is natural to consider morphisms, which are simply rational maps that are regular at every point on the domain on which they are defined. Therefore before we can define morphisms we will define rational maps and what it means to be regular.

To begin we start by defining a function field. Recall that we denote the algebraic closure of a field K by \bar{K} . And $K[x, y, z]$ denotes the set of all functions on the variables x , y , and z with coefficients in the field K .

Definition 4.1.1. [13, p.11] Let K be a field. Let C/K be a curve in the projective plane given by the equation $f(x, y, z) = 0$ such that $f \in K[x, y, z]$ and f is irreducible in $\bar{K}[x, y, z]$. Then we define the **function field of C over K** , denoted $K(C)$, to be the set of all rational functions $F(x, y, z) = \frac{g(x, y, z)}{h(x, y, z)}$ where

(i) $g, h \in K[x, y, z]$ and also g and h are both homogenous polynomials of the same degree.

(ii) the function h is not divisibly by the function f , that is, h is not in the ideal generated by f .

(iii) for all $F_1, F_2 \in K(C)$, we get that $F_1 = \frac{g_1}{h_1}$ is equivalent to $F_2 = \frac{g_2}{h_2}$ if and only if $g_1 h_2 - g_2 h_1$ is a function in the ideal of f . △

Claim 4.1.2. Note that from (i) we get that given $P_1, P_2 \in E(K)$, if P_1 is equivalent to P_2 in the projective plane then $F(P_1) = F(P_2)$ for all $F \in K(C)$.

Proof. Let $F \in K(C)$ such that $F = g/h$ for some $g, h \in K[x, y, z]$ such that both g and h are homogenous of degree d . Let $P_1 = (x_1, x_2, x_3)$ and let $P_2 = (y_1, y_2, y_3)$ and suppose that P_1 is equivalent to P_2 . Then there exists some $\gamma \in \bar{K}^*$ such that $x_i = \gamma y_i$ for all $i \in \{1, 2, 3\}$. Then

$$F(P_2) = \frac{g(y_1, y_2, y_3)}{h(y_1, y_2, y_3)} = \frac{g(\gamma x_1, \gamma x_2, \gamma x_3)}{h(\gamma x_1, \gamma x_2, \gamma x_3)} = \frac{\gamma^d g(x_1, x_2, x_3)}{\gamma^d h(x_1, x_2, x_3)} = \frac{g(x_1, x_2, x_3)}{h(x_1, x_2, x_3)} = F(P_1).$$

□

Now that we understand what a function field is, we are able to define rational maps. Rational maps will be maps that coordinate-wise can be written as functions contained within a certain function field.

Definition 4.1.3. [13, p.11] Given two curves C_1 and C_2 in the projective plane along with a function $\phi : C_1 \rightarrow C_2$, then we say that ϕ is a **rational map** between the two curves if ϕ can be split up into coordinate-wise functions by the triple $(\phi_x(x, y, z) : \phi_y(x, y, z) : \phi_z(x, y, z)) \in$

$\mathbf{P}^2(K(C))$ so that for all $P \in C_1(\bar{K})$ we get that $\phi_x(P), \phi(P)_y, \phi(P)_z$ are defined and nonzero, and $(\phi_x(P), \phi(P), \phi(P)) \in C_2(\bar{K})$. \triangle

Now that we have an understanding of a function field and rational maps, we need to understand what it means for a rational map, that is an element of a function field, to be regular at a point P on the relevant curve. We must be careful here to not confuse $K(C)$, which is the function field of C over K , with $C(K)$, which is the set of all K -rational points on the curve C .

Definition 4.1.4. [13, p.12] Let C/K be a curve in the projective plane. Let $F \in K(C)$ and let $P \in C(\bar{K})$. Suppose that $F = \frac{g}{h}$ for some rational maps $g, h \in K[x, y, z]$. Then we say that F is **regular**, or defined, at P given that $h(P) \neq 0$. \triangle

Definition 4.1.5. [13, p.13] A **morphism** is a rational map that is defined everywhere. \triangle

Remark 4.1.6. Let E_1 and E_2 be elliptic curves. Let $\phi : E_1 \rightarrow E_2$ be a rational map. In order to be a morphism, it must be the case that ϕ is regular for all points P on the elliptic curve E_1 . Let P be a point on E_1 . Note that E_1 is an elliptic curve and is therefore a smooth curve. Thus we know that P is a smooth point. Therefore from [13, p.19] we know that ϕ is regular on P . So ϕ is a rational map that is regular at every point on E_1 and thus ϕ is a morphism. Hence to find morphisms between elliptic curves we need only look for rational maps, which are then, by construction, morphisms. \diamond

Definition 4.1.7. [13, p.66] Given two elliptic curves E_1 and E_2 , a morphism $\phi : E_1 \rightarrow E_2$ such that $\phi(\mathcal{O}) = \mathcal{O}$ is called an **isogeny**. \triangle

Given an isogeny $\phi : E_1 \rightarrow E_2$, we know from [13, p.20] that ϕ is either constant or surjective. Therefore since $\phi(\mathcal{O}) = \mathcal{O}$ it must be the case that ϕ satisfies either $\phi(E_1) = \mathcal{O}$ or $\phi(E_1) = E_2$. The former isogeny is called the zero isogeny defined by $\phi(P) = \mathcal{O}$ for all $P \in E_1$.

Definition 4.1.8. Two elliptic curves E_1 and E_2 are **isogenous** if there exists a nonzero isogeny $\phi : E_1 \rightarrow E_2$. \triangle

To find examples of isogenies it is natural to turn to rational maps on elliptic curves that we have already encountered. For example, the equations given by the Group Law Algorithm [13, p.54] for adding points on elliptic curves are defined by rational functions in local coordinates as can be seen in Algorithm 2.2.6. As the Group Law Algorithm provides rational maps for adding points on an elliptic curve, then adding a point to itself any finite number of times can be defined as a rational map through the composition of a finite number of rational maps taken from the Group Law Algorithm. Therefore the rational map that gives the formula for the point that results from adding a point to itself a finite number of times will be a morphism. Thus we get the following example of an isogeny.

Example 4.1.9. [13, p.67] Let $m \in \mathbf{Z}$. Consider the *multiplication-by- m map* defined by

$$[m] : E \rightarrow E \text{ such that } m(P) = \begin{cases} P \oplus P \oplus \cdots \oplus P, & \text{if } m > 0 \\ (-P) \oplus (-P) \oplus \cdots \oplus (-P), & \text{if } m < 0 \\ \mathcal{O} & \text{if } m = 0. \end{cases}$$

We have already established that the map defined by adding a point to itself a finite number of times is a morphism, and clearly $m(\mathcal{O}) = \mathcal{O}$ for all $m \in \mathbf{Z}$. Thus the multiplication-by- m map is indeed an isogeny. Note that if $m = 0$ then we get the zero-isogeny, but if $m \neq 0$ then we have a nonzero isogeny. \diamond

In addition to the multiplication-by- m map, another important map that is relevant in discussing isogenies on elliptic curves is the translation-by- Q map.

Example 4.1.10. [13, p.71] Given an elliptic curve E/K and some point $Q \in E$, the *translation-by- Q map* is defined by

$$\tau_Q : E \rightarrow E, \quad \text{where} \quad \tau_Q(P) = P \oplus Q \text{ for all } P \in E.$$

Note that

$$\tau_Q(\mathcal{O}) = \mathcal{O} \oplus Q = Q$$

and thus the translation-by- Q map is a morphism, but not an isogeny unless $Q = \mathcal{O}$ as to be an isogeny the map must preserve the distinguished point at infinity. While not an isogeny, the translation-by- Q map maintains some nice properties as each translation-by- Q map has an inverse map, namely the translation-by- $(-Q)$ map. Therefore τ_Q is an isomorphism for all $Q \in E$.

Even though the translation-by- Q map is not an isogeny, it can be used to form a composition of maps that is an isogeny. Given two elliptic curves E_1 and E_2 , and some morphism $\phi : E_1 \rightarrow E_2$, we get that $\psi = \tau_{-\phi(\mathcal{O})} \circ \phi$ is an isogeny between E_1 and E_2 as by definition ψ is a composition of morphisms, and thus a morphism itself, for which

$$\psi(\mathcal{O}) = \tau_{-\phi(\mathcal{O})} \circ \phi(\mathcal{O}) = \tau_{-\phi(\mathcal{O})}(\phi(\mathcal{O})) = \phi(\mathcal{O}) \oplus (-\phi(\mathcal{O})) = \mathcal{O}.$$

◇

Another way we can create an isogeny is by taking the sum of other isogenies.

Remark 4.1.11. [13, p.67] Given two isogenes $\phi, \psi : E_1 \rightarrow E_2$, the sum of the isogenies is defined by

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

for all $P \in E_1$. Note that ϕ and ψ must be morphisms so $\phi + \psi$ is also a morphism. Similarly $\phi(\mathcal{O}) = \mathcal{O}$ and $\psi(\mathcal{O}) = \mathcal{O}$ so this gives us that $(\phi + \psi)(\mathcal{O}) = \mathcal{O}$. Therefore $\phi + \psi$ is an isogeny.

From this we can conclude that any finite sum of isogenies is itself an isogeny. ◇

One can consider whether two curves are isogenous over a specific field K by taking the curves E_1 and E_2 that are desired to be isogenous, and attempting to find an isogeny between E_1/K and E_2/K . Note that if two curves are isogenous then they are isogenous over \mathbf{F}_p for all good prime p . This comes from the following theorem.

Theorem 4.1.12. *Isogenies are well-defined modulo all but finitely many primes.*

Proof. Note this holds as given an isogeny ϕ , since ϕ is a rational map we get that ϕ can be broken up coordinate-wise so that for some point $P \in E_1(K)$ we get that $\phi(P) = (\phi_x(P), \phi_y(P)) \in E_2(K)$. Here we have that $\phi_x, \phi_y \in K(C)$ Thus there exists polynomial functions g_x, h_x, g_y, h_y such that $\phi_x = \frac{g_x}{h_x}$ and $\phi_y = \frac{g_y}{h_y}$. The only problems in reducing ϕ modulo a prime p will occur when ϕ_x or ϕ_y are undefined, that is when $h_x(P) = 0$ or $h_y(P) = 0$ for some $P \in E(K)$. Note for all fixed isogenies this will only occur for finitely many primes p and therefore we can indeed apply reduction modulo p to isogenies for all but finitely many primes p . \square

Based on our ability to perform a reduction of an isogeny modulo a prime p , we are able to make a statement on how isogenies preserve local divisibility, which will be essential in the construction of our universal models of curves with local ℓ -divisibility, but no ℓ -torsion. But first we require a deep theorem concerning elliptic curves that are isogenous over finite fields.

Theorem 4.1.13. [13, p.153, Exr. 5.4] *Let E_1/\mathbf{F}_p and E_2/\mathbf{F}_p be elliptic curves. Then E_1 and E_2 are isogenous over \mathbf{F}_p if and only if*

$$\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p).$$

From Theorem 4.1.13 we are able to make an important statement concerning how isogenies preserve local divisibility on elliptic curves. This will help us to ensure that the isogenous models that we define in this chapter will have our desired local ℓ -divisibility.

Theorem 4.1.14. *Let E_1 and E_2 be elliptic curves such that the curve E_1 has local m -divisibility. Suppose that E_1 is isogenous to E_2 , then E_2 also has local m -divisibility.*

Proof. This follows from the fact that if E_1 and E_2 are isogenous curves, then by 4.1.12 they are isogenous over the finite field \mathbf{F}_p for all but finitely many primes p . Therefore for all but finitely many primes p we get from 4.1.13 that $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$. Because we stated that E_1 has local m -divisibility, we know that $m|\#E_1(\mathbf{F}_p)$ for all but finitely many primes p . Therefore

we get that $m \mid \#E_2(\mathbf{F}_p)$ for all but finitely many primes p , and therefore by definition, our curve E_2 has local m -divisibility. \square

Suppose that E_1 is an elliptic curve with m torsion. Then we know E_1 has local m -divisibility, and thus from Theorem 4.1.14 we get that any curve E_2 that is isogenous to E_1 will also have local m -divisibility.

Remark 4.1.15. Note that given two elliptic curves E_1 and E_2 , both with local ℓ -divisibility, we do not necessarily get that E_1 is isogenous to E_2 , that is the converse of 4.1.14 does not hold. Let E_1 and E_2 be the two elliptic curves given by the equations

$$E_1 : y^2 + y = x^3 - x^2 - 10x - 20, \quad E_2 : y^2 + xy + y = x^3 + x^2 + 1.$$

Let $P = (5, 5)$ and let $Q = (-1, 1)$. Note that $P \in E_1(\mathbf{Q})$ and $Q \in E_2(\mathbf{Q})$. A simple calculation in PARI shows that $[5]P = \mathcal{O}$ on E_1 and $[5]Q = \mathcal{O}$ on E_2 . Thus we get that E_1 and E_2 both have 5-torsion. Therefore we know that both curves also have local 5-divisibility. Note that from the LMFDB [11] we can see that E_1 and E_2 are in different isogeny classes and thus are not isogenous to one another. Hence E_1 is not isogenous to E_2 though both curves have local 5-divisibility. \diamond

Theorem 4.1.16. [13, p.71] *Let E_1 and E_2 be isogenous elliptic curves and let ϕ be the isogeny between them. Then ϕ is a group homomorphism, that is*

$$\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$$

for all $P, Q \in E_1$.

Note this statement is different than the remark concerning how we think about the sum of isogenies. If ϕ is the isogeny between two isogenous curves with E as its domain, since ϕ is a group homomorphism we can conclude that $\ker \phi$ is a subgroup of E .

Remark 4.1.17. Certainly this gives us that if ϕ is a nonzero isogeny between two isogenous curves then $\#\ker\phi$ is finite. Some sources will use this to present the definition of an isogeny to be a surjective morphism with a finite kernel. \diamond

Corollary 4.1.18. [13, p.72] *Let E_1 and E_2 be isogenous elliptic curves and let ϕ be the nonzero isogeny between them then $\ker\phi$ is a finite subgroup of E_1 .*

This follows from the fact that if ϕ defines an isogeny between two isogenous curves, then ϕ must be a nonzero isogeny and thus has a finite kernel. As the kernel of an isogeny from E_1 to E_2 is always a finite subgroup of E_1 , it is a natural question to ask for which finite subgroups F of E_1 there exists an isogeny ϕ such that $\ker\phi = F$.

Proposition 4.1.19. [13, p.74] *Given an elliptic curve E and F , a finite subgroup of E , there exists a unique elliptic curve E' and a separable isogeny ϕ where*

$$\phi : E \rightarrow E' \quad \text{satisfies } \ker\phi = F.$$

Often the curve satisfying these properties is denoted E/F .

Note that here E/F is not an elliptic curve defined over F , as this notation has previously been used to denote, but instead the isogenous curve to E such that the isogeny between E and E/F has kernel F . We will have to differentiate between these two similar notations by context.

Taking E to be an elliptic curve in Tate normal form with ℓ -torsion, we can now use the methods from [17] to find the isogenous curve E/F , where F is the group generated by a certain ℓ -torsion point. This gives us that if ϕ is the isogeny from E to E/F , then $\ker\phi = F$. Note that the curve E/F will not have ℓ -torsion; however, by construction E/F is isogenous to E . As E has ℓ -torsion and therefore local ℓ -divisibility, we know that E/F will also have local ℓ -divisibility.

4.2 Vélu's Algorithm

Let E be an elliptic curve defined over \mathbf{Q} given by the Weierstrass equation:

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

and let F be a finite subgroup of E . Then if $\widehat{E} = E/F$, which we know exists by 4.1.19, then by [17, p.240], we get that \widehat{E} is given by the equation

$$\widehat{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W),$$

where b_2 is defined as in equation 2.1.5 and where the values of T and W will take some work to find, but will now be explained.

Let F be a finite subgroup of E of size ℓ , such that ℓ is prime. Note that the process is slightly altered if ℓ is even. We are only concerned with the two cases where the size of F is either 5 or 7, and thus for the sake of this paper will only take the time to explain the process for odd orders ℓ . Doing so allows us to ignore any points in the algorithm where Vélu requires a special case for the set of all points in F of order 2.

Let $P \in E$. Let $x(P)$ and $y(P)$ denote the x -coordinate of P and y -coordinate of P , respectively. Let X and Y be the functions defined by

$$X(P) = x(P) + \sum_{Q \in F - \{\mathcal{O}\}} [x(P \oplus Q) - x(Q)],$$

$$Y(P) = y(P) + \sum_{Q \in F - \{\mathcal{O}\}} [y(P \oplus Q) - y(Q)]$$

for all $P \in E$. Let ϕ be the function defined by

$$\phi : E \rightarrow \widehat{E}, \quad (x(P), y(P)) \rightarrow (X(P), Y(P))$$

for all $P \in E$.

Remark 4.2.1. Note that X and Y are morphisms and thus ϕ is a morphism and observe

$$X(\mathcal{O}) = x(\mathcal{O}) + \sum_{Q \in F - \{\mathcal{O}\}} [x(\mathcal{O} \oplus Q) - x(Q)] = x(\mathcal{O}) + \sum_{Q \in F - \{\mathcal{O}\}} [x(Q) - x(Q)] = x(\mathcal{O})$$

and

$$Y(\mathcal{O}) = y(\mathcal{O}) + \sum_{Q \in F - \{\mathcal{O}\}} [y(\mathcal{O} \oplus Q) - y(Q)] = y(\mathcal{O}) + \sum_{Q \in F - \{\mathcal{O}\}} [y(Q) - y(Q)] = y(\mathcal{O}).$$

Therefore $\phi(\mathcal{O}) = \mathcal{O}$. Thus we do indeed get that ϕ is an isogeny. Note that it is a nonzero isogeny and thus the curve \widehat{E} that results from applying ϕ to E is indeed isogenous to E . This isogeny combines many of the examples of morphisms and isogenies discussed earlier in the chapter such as translation maps and isogenies built off of addition of points. Based on those examples one may be able to see how these coordinate mappings could be given by ratios of polynomial maps. \diamond

Let R and $(-R)$ be subsets of $F - \{\mathcal{O}\}$ such that $R \cup (-R) = F - \{\mathcal{O}\}$ and if $P \in R$ for some P on the elliptic curve E , then $-P \notin R$ where $P \oplus (-P) = \mathcal{O}$. Thus we know that $R \cap (-R) = \emptyset$ as we have no points of order 2 in our cyclically generated finite subgroup F of odd order.

Let $Q \in F$ and define

$$t_Q = 6x_Q^2 + b_2x_Q + b_4, \quad u_Q = 4x_Q^3 + b_2x_Q^2 + 2b_4x_Q + b_6, \quad (4.2.1)$$

$$g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q, \quad g_Q^y = -2y_Q - a_1x_Q - a_3 \quad (4.2.2)$$

where x_Q and y_Q denote the x -coordinate and y -coordinate of Q , respectively, and b_2, b_4 , and b_6 are defined as they were in equation 2.1.5. From [17, p.239] we get that the functions X and Y that are used to construct our isogeny ϕ , can be redefined using formulas from the Group Law Algorithm, along with our new variables to be

$$X = x + \sum_{Q \in R} \left[\frac{t_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2} \right]$$

and

$$Y = y - \sum_{Q \in R} \left[u_Q \frac{2y + a_1x + a_3}{(x - x_Q)^3} + t_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^r g_Q^y}{(x - x_Q)^2} \right].$$

Certainly these maps above are rational maps. The way in which we can redefine our isogeny in these variables allows us to get the equation of the isogenous curve \widehat{E} given by

$$\widehat{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W),$$

where we can now define

$$T = \sum_{Q \in R} t_Q, \quad W = \sum_{Q \in R} (u_Q + x_Q t_Q). \quad (4.2.3)$$

We will use this algorithm of Vélú to get our universal model for curves with local ℓ -divisibility, but no ℓ -torsion for $\ell = 5$ and $\ell = 7$. We will do so by letting F be the cyclic subgroup of our curves in Tate normal form where F is generated by a point of order 5, and then repeat this process for a point of order 7.

4.3 Paramaterization of Curves with Local 5-Divisibility

We will now find the universal model for a curve that is isogenous to the universal model, given by the Tate normal form, of elliptic curves with 5-torsion. Let E be an elliptic curve in Tate normal form with a point of order 5. Recall then that E is given by the equation

$$E : y^2 + (1 - t)xy - ty = x^3 - tx^2, \quad (4.3.1)$$

[4] for some $t \in \mathbf{Q}$. To compute the desired isogenous curve we follow the methods used in [17], which we have outlined in the previous section. Thus we first require a subgroup of E . In this computation our finite subgroup will actually be a subgroup of $E(\mathbf{Q}(t))$. As we know that $E(\mathbf{Q}(t))$ has a point of order 5, we can conclude that the group generated by a point of order 5 is a subgroup of $E(\mathbf{Q}(t))$. So we take F to be the subgroup of E generated by the point $P = (0, 0)$, which is a point of order 5 on E due to the fact that E is in the Tate normal

form. Thus $F = \{P, 2P, 3P, 4P, \mathcal{O}\}$, that is F is a subgroup of $E(\mathbf{Q}(t))_{\text{tor}}$ generated by P . Let $R = \{P, 2P\}$, then $-R = \{3P, 4P\}$, and note that this then satisfies the proper conditions that every point in R has its inverse in $-R$, and $R \cup (-R) = F - \{\mathcal{O}\}$ and $R \cap (-R) = \emptyset$.

To follow the algorithm of Vélú to get an isogenous curve to our parameterized curve with 5-torsion, set

$$a_1 = 1 - t, \quad a_2 = -t, \quad a_3 = -t, \quad a_4 = 0, \quad a_6 = 0,$$

which are simply the coefficients of E . From [17] we know that our isogenous curve \widehat{E} over F is given by the equation

$$\widehat{E} : y^2 + a_1xy + a_3y = x_3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W).$$

We will now solve for T and W .

From $P = (0, 0)$ and the duplication formula we get that

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6} = \frac{-b_8}{b_6} = \frac{-(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2)}{a_3^2 + 4a_6} = \frac{-a_2a_3^2}{a_3^2} = -a_2 = t.$$

Thus we get an equation to solve for y in terms of t by plugging in $x = t$ into equation 4.3.1:

$$\begin{aligned} y^2 + (1-t)ty - ty &= t^3 - t^3 \\ 0 &= y^2 + (1-t)ty - ty \\ 0 &= y^2 + ty - t^2y - ty \\ 0 &= y^2 - t^2y \\ y^2 &= t^2y \\ y &= t^2. \end{aligned}$$

So if $P = (0, 0)$, then $2P = (t, t^2)$. Thus we get

$$x_P = 0 \quad \text{and} \quad x_{2P} = t.$$

Then from equations 4.2.1 we get that

$$t_P = 6x_P^2 + b_2x_P + b_4 = 6(0)^2 + b_2(0) + b_4 = b_4,$$

$$t_{2P} = 6x_{2P}^2 + b_2x_{2P} + b_4 = 6t^2 + b_2t + b_4.$$

Therefore

$$T = \sum_{Q \in S} t_Q = t_P + t_{2P} = b_4 + 6t^2 + b_2t + b_4 = 2b_4 + 6t^2 + b_2t.$$

Next, again from equations 4.2.1 we compute

$$u_P = 4x_P^3 + b_2x_P^2 + 2b_4x_P + b_6 = 4(0)^3 + b_2(0)^2 + 2b_4(0) + b_6 = b_6,$$

$$u_{2P} = 4x_{2P}^3 + b_2x_{2P}^2 + 2b_4x_{2P} + b_6 = 4t^3 + b_2t^2 + 2b_4t + b_6.$$

We can now plug in our values for $t_P, t_{2P}, u_P,$ and u_{2P} to evaluate

$$\begin{aligned} W &= \sum_{Q \in S} (u_Q + x_Q t_Q) \\ &= (u_P + x_P t_P) + (u_{2P} + x_{2P} t_{2P}) \\ &= (b_6 + (0)b_4) + (4t^3 + b_2t^2 + 2b_4t + b_6 + (t)6t^2 + b_2t + b_4) \\ &= b_6 + 4t^3 + b_2t^2 + 2b_4t + b_6 + 6t^3 + b_2t^2 + b_4t \\ &= 10t^3 + 2b_2t^2 + 3b_4t + 2b_6. \end{aligned}$$

Now we can input the actual values of $b_2, b_4,$ and b_6 into these equations for T and W to get that

$$T = t^3 + 2t^2 - t, \quad W = 2t^4 - 2t^3 + 7t^2 - 3t.$$

We will now put the values we have computed for $a_1, a_3, a_2, a_4, T,$ and W back into our equation for the curve given by

$$\widehat{E} : y^2 + a_1xy + a_3y = x_3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W)$$

to get that

$$\widehat{E} : y^2 + (1-t)xy - ty = x^3 - tx^2 + (-5t^3 - 10t^2 + 5t)x + (-t^5 - 10t^4 + 26t^3 - 57t^2 + 22t).$$

This provides an elliptic curve defined over \mathbf{Q} parameterized by t , which by construction will have local 5-divisibility without 5-torsion. As $\text{char}(\mathbf{Q}) \neq 0$, we can use the method proved in [13, p.42] to get our universal model for curves with 5-divisibility and no 5-torsion in short Weierstrass form. Applying this method we get that an elliptic curve with 5-divisibility and no 5-torsion can be given by the following general formula for any $t \in \mathbf{Q}$:

$$\begin{aligned} y^2 &= x^3 + \widehat{f}(t)x + \widehat{g}(t), \\ \widehat{f}(t) &= -27t^4 - 6156t^3 - 13338t^2 + 6156t - 27, \\ \widehat{g}(t) &= 54t^6 - 28188t^5 - 540270t^4 - 540270t^2 + 28188t + 54. \end{aligned}$$

As we would like an integral model of these equations, we set $t = \frac{a}{b}$ assuming that $a, b \in \mathbf{Z}$ and with some simple algebra get the following integral model that will provide the general equation of an elliptic curve E with local 5-divisibility, without 5-torsion:

$$\begin{aligned} y^2 &= x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b), \\ \widehat{A}(a, b) &= -27a^4 - 6156a^3b - 13338a^2b^2 + 6156ab^3 - 27b^4, \end{aligned} \tag{4.3.2}$$

$$\widehat{B}(a, b) = 54a^6 - 28188a^5b - 540270a^4b^2 - 540270a^2b^4 + 28188ab^5 + 54b^6. \tag{4.3.3}$$

Example 4.3.1. Let $a = 2$ and $b = 7$. We will now consider the elliptic curve E given by the equation

$$E : y^2 = x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b).$$

We get that $\widehat{A}(a, b) = 1198773$ and $\widehat{B}(a, b) = -4664770938$, which yields the equation

$$\widehat{E} : y^2 = x^3 + 1198773x - 4664770938.$$

A simple calculation in PARI will show that \widehat{E} does not have 5-torsion. Note that by construction \widehat{E} is isogenous to a curve in the form $y^2 = x^3 + A(2, 7)x + B(2, 7)$. Thus \widehat{E} is isogenous to the

elliptic curve E given by the equation

$$E : y^2 = x^3 - 343467x + 80882982.$$

Let $P = (-93, 10584)$. Note that $P \in E(\mathbf{Q})$ and also $[5]P = \mathcal{O}$. Therefore E has 5-torsion, as expected, and thus it must also have local 5-divisibility. As local divisibility is preserved by isogeny this gives us that \widehat{E} has local 5-divisibility. \diamond

4.4 Paramaterization of Curves with Local 7-Divisibility

Recall from [4] that the Tate normal form for curves with 7-torsion is given by the equation:

$$E : y^2 + (1 - t^2 + t)xy - (t^3 - t^2)y = x^3 - (t^3 - t^2)x^2.$$

Again, we let $P = (0, 0)$ and take F to the subgroup of $E(\mathbf{Q}(t))$ generated by the point P . We know that P has order 7 by construction of the Tate normal form. Thus $F = \{P, 2P, 3P, 4P, 5P, 6P, \mathcal{O}\}$. Let $R = \{P, 2P, 3P\}$ and then $-R = \{4P, 5P, 6P\}$ so that we satisfy the condition that $F - \{\mathcal{O}\} = R \cup (-R)$ and $R \cap (-R) = \emptyset$.

Now, to use the method of Vélú we again let

$$a_1 = 1 - t^2 + t, \quad a_2 = t^2 - t^3, \quad a_3 = t^2 - t^3, \quad a_4 = 0, \quad a_6 = 0$$

such that the isogenous curve \widehat{E} over F is given by the equation

$$\widehat{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W)$$

where b_2 is given it's usual definition from equation 2.1.5, and T and W are defined as in equation 4.2.3.

Using calculations similar to those used in the previous section to compute multiples of P we get that

$$P = (0, 0), \quad 2P = (t^3 - t^2, t^5 - 2t^4 + t^3), \quad \text{and } 3P = (t^2 - t, t^3 - 2t^2 + t).$$

We can now easily calculate t_P, t_{2P} , and t_{3P} to get

$$T = \sum_{Q \in S} t_Q = t_P + t_{2P} + t_{3P} = t^7 - 7t^5 + 14t^4 - 14t^3 + 7t^2 - t$$

where t_Q is defined as in equation 4.2.1. Finally we can calculate u_P, u_{2P} , and u_{3P} to get

$$\begin{aligned} W &= \sum_{Q \in S} (u_Q + x_Q t_Q) \\ &= (u_P + x_P t_P) + (u_{2P} + x_{2P} t_{2P}) + (u_{3P} + x_{3P} t_{3P}) \\ &= 2t^{10} - 6t^9 + 7t^8 - 12t^7 + 32t^6 - 47t^5 + 35t^4 - 13t^3 + 2t^2, \end{aligned}$$

where u_Q and t_Q are defined as in equation 4.2.1.

Now we can input these equations for T and W into Vélú's model

$$\widehat{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W).$$

to get the equation

$$\begin{aligned} \widehat{E} : y^2 + (1 - t^2 + t)xy + (t^2 - t^3)y &= x^3 + (t^2 - t^3)x^2 + (-5t^7 + 35t^5 - 70t^4 + 70t^3 - 35t^2 + 5t)x \\ &\quad + (-t^{11} - 8t^{10} + 46t^9 - 107t^8 + 202t^7 - 343t^6 + 393t^5 \\ &\quad - 258t^4 + 94t^3 - 19t^2 + t). \end{aligned}$$

This provides an elliptic curve defined over \mathbf{Q} parameterized by t , which by construction will have local 7-divisibility without 7-torsion. We now use the method from [13, p.42] to get this equation into short Weierstrass form, which gives us the following universal model for curves with local 7-divisibility, but no 7-torsion:

$$\begin{aligned} y^2 &= x^3 + \widehat{A}(t)x + \widehat{B}(t) \\ \widehat{A}(t) &= -27t^8 - 6156t^7 - 1134t^6 + 46872t^5 - 91665t^4 + 90720t^3 - 44982t^2 + 6372t - 27, \\ \widehat{B}(t) &= 54t^{12} - 28188t^{11} + 2049300t^9 - 3833892t^8 + 7104348t^7 - 13674906t^6 + 17079660t^5 \\ &\quad - 11775132t^4 + 4324860t^3 - 790074t^2 + 27540t + 54. \end{aligned}$$

Now to get an integral model, we set $t = \frac{a}{b}$ assuming that $a, b \in \mathbf{Z}$, and use the same method as previously used to get the following integral model for an elliptic curve with local 7-divisibility, but no 7-torsion:

$$y^2 = x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b)$$

$$\widehat{A}(a, b) = -27a^8 - 6156a^7b - 1134a^6b^2 + 46872a^5b^3 - 91665a^4b^4 + 90720a^3b^5 - 44982a^2b^6 + 6372ab^7 - 27b^8,$$

$$\widehat{B}(a, b) = 54a^{12} - 28188a^{11}b - 483570a^{10}b^2 + 2049300a^9b^3 - 3833892a^8b^4 + 7104348a^7b^5 - 13674906a^6b^6$$

$$+ 17079660a^5b^7 - 11775132a^4b^8 + 4324860a^3b^9 - 790074a^2b^{10} + 27540ab^{11} + 54b^{12}.$$

Example 4.4.1. Let $a = 4$ and $b = 11$. We will now consider the elliptic curve E given by the equation

$$E : y^2 = x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b).$$

We get that $\widehat{A}(a, b) = -130395961323$ and $\widehat{B}(a, b) = -32479678409224986$, which yields the equation

$$\widehat{E} : y^2 = x^3 - 130395961323 - 32479678409224986.$$

A simple calculation in PARI will show that \widehat{E} does not have 7-torsion. Note that by construction \widehat{E} isogenous to a curve in the form $y^2 = x^3 + A(4, 11)x + B(4, 11)$. Thus \widehat{E} is isogenous to the elliptic curve E given by the equation

$$E : y^2 = x^3 - 5478331563 + 165972985340454.$$

Let $P = (37035, 3725568)$. Note that $P \in E(\mathbf{Q})$ and also $[7]P = \mathcal{O}$. Therefore E has 7-torsion, as expected, and thus it must also have local 7-divisibility. As local divisibility is preserved by isogeny this gives us that \widehat{E} has local 7-divisibility. \diamond

4.5 Accountability of Models

As the construction of our universal models for curves with ℓ -torsion was built using the Tate normal form, we know that every such elliptic curve with ℓ -torsion will be isomorphic to some elliptic curve whose equation will lie in the one-parameter family of the Tate normal form. And we know that the Tate normal form will account for all such curves, up to isomorphism, with ℓ -torsion by Theorem 3.0.1. Therefore when we count the number of isomorphism classes of elliptic curves with ℓ -torsion, each isomorphism class will have a representative in our universal models, which we will be able to easily find and count. Now we must ask the same question for our models of curves with local ℓ -divisibility without ℓ -torsion.

Corollary 4.5.1. [3, p.5] *Let E be an elliptic curve such that $\ell \in \mathbb{N}$ be a prime that is considered relevant by Theorem 2.2.10, then if $\ell \mid \#E(\mathbf{F}_p)$ for all but finitely many primes p , that is if E has local ℓ -divisibility, then at least one of the following will result*

- (i) E has ℓ -torsion,
- (ii) E is ℓ -isogenous to a curve E' , such that E' has ℓ -torsion.

Claim 4.5.2. *Let $\ell = 5$ or $\ell = 7$. Similarly to how every elliptic curve with ℓ -torsion is isomorphic to an elliptic curve in the Tate normal form associated with ℓ -torsion, an elliptic curve E with local ℓ -divisibility without ℓ -torsion will always be isomorphic to an elliptic curve that lies in our universal model for curves with local ℓ -divisibility and no ℓ -torsion.*

Let $\ell = 5$ or $\ell = 7$. Suppose that there exists some elliptic curve E with local ℓ -divisibility without ℓ -torsion. From Corollary 4.5.1 there exists some elliptic curve E' that is isogenous to E that has ℓ -torsion. Note that from Theorem 3.0.1 we know that the equation for E' will be isomorphic to a curve E'' that satisfies our universal model for curves with ℓ -torsion for some $a, b \in \mathbf{Z}$. Therefore, E'' can be written in the Tate normal form, and thus the isogenous model of E' , which will be in the same isomorphism class of E , will certainly lie in the universal model

for elliptic curves with local ℓ -divisibility and no ℓ -torsion as this model was taken exactly to be the family of isogenous curves to the Tate normal form curves that have ℓ -torsion. Thus when we count the number of isomorphism classes of elliptic curves with local ℓ -divisibility and no ℓ -torsion, each isomorphism class will have a representative in these universal models, which we will be able to easily find and count. Now we are ready to begin counting these isomorphism classes.

5

Sieving and Overcounting

We will now use our universal models for curves with ℓ -torsion and curves with local ℓ -divisibility without ℓ -torsion, to count the number of isomorphism classes of each type of elliptic curve up to a certain height. Taking a certain ratio involving these counts will allow us to determine our desired probability. Simply counting the number of elliptic curves belonging to each universal model up to some height X would be an overcount of these isomorphism classes as will be discussed later on in this chapter. Thus, in order to correct for this overcount and properly count only one curve per isomorphism class, we will have to get rid of what are called non-minimal Weierstrass models from our total count. Getting rid of these non-minimal models to properly get our count is an example of a sieve method. We will evoke the sieve method for both types of elliptic curves, those with ℓ -torsion and those with local ℓ -divisibility without ℓ -torsion. The sieving method applied to both cases will not displace the ratio that depends on the two counts, but will instead phrase our desired ratio as a computable ratio of areas of compact regions. In order to properly understand how to only count one curve per isomorphism class we must begin by understanding what makes two elliptic curves isomorphic.

5.1 Isomorphism Classes of Elliptic Curves

Definition 5.1.1. [13, p. 13] Let E_1 and E_2 be elliptic curves. Then E_1 is **isomorphic** to E_2 , denoted $E_1 \cong E_2$, when there exists morphisms $\phi : E_1 \rightarrow E_2$ and $\psi : E_2 \rightarrow E_1$ such that

$$\psi \circ \phi = \mathbf{1}_{E_1} \text{ and } \phi \circ \psi = \mathbf{1}_{E_2}.$$

△

Remark 5.1.2. Given E_1/K and E_2/K , we say E_1 is isomorphic to E_2 over K if ϕ and ψ as defined above can be defined over K . ◇

Note that two elliptic curves defined by equations in short Weierstrass form are isomorphic if and only if they satisfy a certain change of variables that can be defined by an invertible morphism. This change of variables is described below, and will serve as a useful tool for determining if two curves are isomorphic.

Remark 5.1.3. [13, p.45] Given an elliptic curve E defined by the equation $E : y^2 = x^3 + Ax + B$. The unique change of variables of the equation for E that results in another Short Weierstrass equation of an isomorphic elliptic curve is given by

$$x = u^2x' \quad \text{and} \quad y = u^3y',$$

which results in

$$u^4A' = A, \quad u^6B' = B, \quad u^{12}\Delta'(E') = \Delta(E),$$

which yields the equation of the isomorphic elliptic curve

$$E' : y^2 = x^3 + A'x^2 + B'.$$

Note that if this isomorphism is over K then $x', y', A, D', \Delta(E') \in \bar{K}$. We will mainly consider isomorphisms over the rationals and therefore from Remark 2.1.7 we get that $x', y', A, D', \Delta(E') \in \mathbf{Z}$. Clearly sending $x \rightarrow u^2x'$ and $y \rightarrow u^3y'$ provides coordinate-wise rational maps of a morphism.

More interestingly this morphism has an inverse morphism given by the mappings $x \rightarrow u^{-2}x$ and $y \rightarrow u^{-3}y$. Certainly composing these two morphisms gives the identities for E and E' , respectively. Therefore, by definition, we get that E and E' are isomorphic elliptic curves. \diamond

Note that in \mathbf{Q} , in order to send $x \rightarrow u^2x'$ and $y \rightarrow u^3y'$ requires that $u^2|x$ and $u^3|y$. There are only finitely many u such that you can keep applying variations of this change of variables to get a new short Weierstrass equation over the rationals, and therefore with integral coefficients. Thus eventually we will get to an elliptic curve given by the equation $\widehat{E} : y^2 = x^3 + \widehat{A}x^2 + \widehat{B}$ such that $u^2 \nmid \widehat{A}$ and $u^3 \nmid \widehat{B}$ for all possible values of $u \in \mathbf{Z}$.

Definition 5.1.4. [13, p.186] Let E/K be an elliptic curve, and let $\Delta(E)$ be the discriminant of E . Then the Weierstrass equation that defines E is called a **minimal model** if and only if $p^{12} \nmid \Delta(E)$ for all primes p . \triangle

Note that elliptic curves for which the change of variables between isomorphic curves as described cannot be performed, that is elliptic curves $E : y^2 = x^3 + Ax + B$, such that $u^4 \nmid A$ and $u^6 \nmid B$ for all $u \in \mathbb{N}$, are exactly these elliptic curves given by minimal models. This follows from the fact that given an elliptic curve defined by the equation $E : y^2 = x^3 + Ax + B$, if we assume that $u^4 \nmid A$ and $u^6 \nmid B$ for all $u \in \mathbb{N}$, this implies that $p^{12} \nmid \Delta(E)$ for all primes p .

Remark 5.1.5. To check if the discriminant of a curve is not divisible by any powers of 12, we need only factor the discriminant and check the exponents on each prime in its prime factorization. \diamond

Example 5.1.6. The elliptic curve given by the equation $E : y^2 = x^3 + 729x + 729$ is not a minimal model. This can be seen through the prime factorization of the discriminant of E . Observe $\Delta(E) = -25024493808 = -2^4 \cdot 3^{15} \cdot 109$. Therefore $3^{12} | (\Delta(E))$. Thus to make our desired change of variables that sends $x \rightarrow u^2x'$ and $y \rightarrow u^3y'$ for some maximal value of u , we have exactly that $u = 3$ as $2^{12} \nmid \Delta(E)$ and $109^{12} \nmid \Delta(E)$.

Consider the map that sends $(x, y) \rightarrow (3^2x, 3^3y)$. Then $y^2 = x^3 + 729x + 729$ gets mapped to $729y^2 = 729x^3 + 729(9)x + 729$. Dividing through this equation by 729 yields the minimal model for E given by the equation $E' : y^2 = x^3 + 9x + 1$, and we know this model is minimal as $\Delta(E') = -47088 = 2^4 \cdot 3^3 \cdot 109$ and therefore none of the exponents on the prime factorization of the discriminant of E' are greater than or equal to 12. Therefore $p^{12} \nmid \Delta(E')$ for all primes p . Additionally E is isomorphic to E' , which can be seen by defining the morphisms $\phi : E \rightarrow E'$ and $\psi : E' \rightarrow E$ so that ϕ sends $(x, y) \rightarrow (3^2x, 3^3y)$ and ψ sends $(x, y) \rightarrow (\frac{1}{3^2}x, \frac{1}{3^3}y)$. Certainly

$$\psi \circ \phi = \mathbf{1}_E \text{ and } \phi \circ \psi = \mathbf{1}_{E'}$$

and thus E is isomorphic to E' by definition. ◇

One way to detect whether or not two curves are isomorphic simply from characteristics of their equations is to look at the j -invariants of the two potentially isomorphic curves.

Definition 5.1.7. Given an elliptic curve E over some field K defined by

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

the j -invariant of E is given by the equation

$$j(E) = \frac{c_4^3}{\Delta(E)},$$

where c_4 is defined as in 2.1.6 and $\Delta(E)$ is the discriminant of E as defined in 2.1.12. △

Note that by definition an elliptic curve is non-singular, which implies that $\Delta(E) \neq 0$. Therefore the equation for the j -invariant will be well defined for all elliptic curves.

Remark 5.1.8. If our elliptic curve E can be given in short Weierstrass form, that is E is defined by an equation of the form

$$E : y^2 = x^3 + Ax + B,$$

then $j(E)$ can be given by a simpler formula:

$$j(E) = -1728 \frac{(4A)^3}{-16(4A^3 + 27B^2)}.$$

◇

Proposition 5.1.9. [13, p.45] *Let E_1 and E_2 be elliptic curves over K . Then E_1 and E_2 are isomorphic over \bar{K} , the algebraic closure of K , if and only if $j(E_1) = j(E_2)$, that is to say, they have equal j -invariants.*

Example 5.1.10. Take the elliptic curves

$$E : y^2 = x^3 + 729x + 729 \text{ and } E' : y^2 = x^3 + 9x + 1$$

from 5.1.6. By construction we know that E and E' are isomorphic. Note that

$$j(E) = -1728 \frac{4(729)^3}{-16(4(729)^3 + 27(729)^2)} = \frac{11664}{109},$$

and

$$j(E') = -1728 \frac{4(9)^3}{-16(4(9)^3 + 27(1)^2)} = \frac{11664}{109}.$$

Thus we get that $j(E) = j(E')$ as desired.

◇

To conduct our count and compute the desired probability we will sieve out the non-minimal equations of elliptic curves with height less than or equal to X . Doing so allows us to simply count only the minimal equations of elliptic curves satisfying our property with height less than or equal to X . Note that each isomorphism class will contain a unique minimal model. Therefore counting the number of minimal models will allow us to count the number of isomorphism classes as each minimal model will act as a kind of representative of each isomorphism class.

An explanation of this process can be found in a paper of Harron and Snowden [5], which will be further explained and used throughout this chapter. It is important to note for the remainder of the chapter that Harron and Snowden are working with a slightly different definition of

height and therefore some of their results and proofs require minor alterations to fit this project. However, their results still hold for our modified definition of height.

5.2 Sieving

Harron and Snowden in [5] are able to provide formulas for the number of isomorphism classes of elliptic curves with certain prescribed torsion of height less than or equal to X . Specifically they provide counting formulas for elliptic curves with trivial torsion, 2-torsion, and 3-torsion. The formulas given in [5] that we mimic for the $\ell = 5$ case rely only on the degrees of the coefficients of our universal model for curves with 5-torsion. Note that we have the same respective degrees for the coefficients of our universal model for curves with local 5-divisibility without 5-torsion; therefore, we can extend these results to get a similar equation for the number of isomorphism classes of these elliptic curves that have height less than or equal to X , even though these elliptic curves by construction will not have torsion.

Proposition 5.2.1. [5, p.6] *Let $f, g \in \mathbf{Q}[t]$ be polynomials that are coprime such that $\deg f = r$ and $\deg g = s$. Assuming that $\max\{r, s\} > 0$ we write*

$$\max\left\{\frac{r}{4}, \frac{s}{6}\right\} = \frac{n}{m},$$

where $\gcd(m, n) = 1$. Suppose that $n = 1$ or $m = 1$. Let $S(X)$ denote the set of pairs $(A, B) \in \mathbf{Z}^2$ such that $y^2 = x^3 + Ax + B$ is a smooth, minimal model for an elliptic curve of height less than or equal to X for which there exists some $u, t \in \mathbf{Q}$ such that $A = u^4 f(t)$ and $B = u^6 g(t)$. Then

$$\#S(X) \asymp X^{\frac{m+1}{12n}}.$$

That is, there exists some $a, b \in \mathbf{R}^+$ such that

$$aX^{\frac{m+1}{12n}} \leq \#S(X) \leq bX^{\frac{m+1}{12n}}.$$

This proposition from [5] allows us to take models of elliptic curves E given by equations of the form $E : y^2 = x^3 + f(t)x + g(t)$ and find the asymptotic growth for the number of minimal models that fit this form of equation up to some height X .

Claim 5.2.2. *Let $S_5(X)$ be the set of all elliptic curves with 5-torsion, then*

$$\#S_5(X) \asymp X^{1/6}$$

for all $X \in \mathbf{R}^+$. In other words the number of elliptic curves with a 5 torsion point up to height X is $O(X^{1/6})$.

Proof. From [4] we have shown that all elliptic curves E with 5-torsion can be defined by an equation of the form

$$\begin{aligned} E : y^2 &= x^3 + f(t)x + g(t), \\ f(t) &= -27t^4 + 324t^3 - 378t^2 - 324t - 27, \\ g(t) &= 54t^6 - 972t^5 + 4050t^2 + 972t + 54. \end{aligned}$$

By construction all curves of this form are elliptic curves in $S_5(X)$. Note this equation is in the proper form to apply Proposition 5.2.1. We have $\deg f = 4$ and $\deg g = 6$. Thus we take $\max(\frac{4}{4}, \frac{6}{6}) = \frac{1}{1}$. Then from Proposition 5.2.1 we get that

$$\#S_5(X) \asymp X^{1/6}.$$

□

Claim 5.2.3. *Let $S'_5(X)$ be the set of all elliptic curves with local 5-divisibility and no 5-torsion, then*

$$\#S'_5(X) \asymp X^{1/6}$$

for all $X \in \mathbf{R}^+$.

Proof. From [4] we have shown that all elliptic curves E with local 5-divisibility and no 5-torsion can be defined by an equation of the form

$$\begin{aligned} E : y^2 &= x^3 + \widehat{f}(t)x + \widehat{g}(t), \\ \widehat{f}(t) &= -27t^4 - 6156t^3 - 13338t^2 + 6156t - 27, \\ \widehat{g}(t) &= 54t^6 - 28188t^5 - 540270t^4 - 540270t^2 + 28188t + 54. \end{aligned}$$

By construction all curves of this form are elliptic curves in $S'_5(X)$. Now again we have $\deg \widehat{f} = 4$ and $\deg \widehat{g} = 6$. Then from Proposition 5.2.1 and using the same argument as in Claim 5.2.2 we get that

$$\#S'_5(X) \asymp X^{1/6}.$$

□

From Claims 5.2.2 and 5.2.3 we can expect to see that the number of minimal models of elliptic curves with 5-torsion, and similarly the number of minimal models of elliptic curves with local 5-divisibility without 5-torsion to be equal to $C_i X^{1/6}$ for constants C_i plus some error term of smaller order than $X^{1/6}$ for $i = 5$ and $i = 5'$. Therefore when just counting the number of Weierstrass equations in each model up to some height X , this number of isomorphism classes has the same asymptotic growth for both of our models for $\ell = 5$. Recall that

$$P_5 = \lim_{H \rightarrow \infty} \frac{\#\{E \in \mathcal{E}_{\leq H} \mid 5 \mid \#E(\mathbf{Q})_{\text{tor}}\}}{\#\{E \in \mathcal{E}_{\leq H} \cap \mathcal{E}_{5?}\}}.$$

This limit within our probability exists precisely when the two sets of curves have the same asymptotics. Therefore Claims 5.2.2 and 5.2.3 give us that this probability is well-defined. Now we will work to compare the number of minimal models of elliptic curves up to some height X contained within each set of curves.

Define the regions

$$R_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |A(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |B(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (5.2.1)$$

where $A(a, b)$ and $B(a, b)$ are defined as in 3.2.1 and 3.2.2, and

$$R'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (5.2.2)$$

where $\widehat{A}(a, b)$ and $\widehat{B}(a, b)$ are defined as in 4.3.2 and 4.3.3.

Proposition 5.2.4. *The region $R_5(X)$ is homogeneous such that*

$$\text{Area}(R_5(X)) = X^{1/6} \text{Area}(R_5(1)).$$

Proof. Let $a, b \in \mathbf{Z}$ such that $(a, b) \in R_5(X)$. Then $4|A(a, b)|^3 \leq X$ and $27|B(a, b)|^2 \leq X$.

We now perform the change of variables that sends

$$a \rightarrow a \sqrt[12]{X} \text{ and } b \rightarrow b \sqrt[12]{X}$$

for all pairs $(a, b) \in R_5(X)$.

Suppose that $(a \sqrt[12]{X}, b \sqrt[12]{X}) \in R_5(X)$. Then

$$4|A(a \sqrt[12]{X}, b \sqrt[12]{X})|^3 \leq X \text{ and } 27|B(a \sqrt[12]{X}, b \sqrt[12]{X})|^2 \leq X.$$

As $A(a, b)$ is a homogenous polynomial of degree 4, we get that $A(ca, cb) = c^4 A(a, b)$ for all $c \in \mathbf{R}$. Therefore

$$4|A(a \sqrt[12]{X}, b \sqrt[12]{X})|^3 \leq X$$

$$4|\sqrt[3]{X} A(a, b)|^3 \leq X$$

$$4X|A(a, b)|^3 \leq X$$

$$4|A(a, b)|^3 \leq 1.$$

Similarly as $B(a, b)$ is a homogenous polynomial of degree 6 we have

$$27|B(a \sqrt[12]{X}, b \sqrt[12]{X})|^2 \leq X$$

$$27|\sqrt[2]{X}B(a, b)|^2 \leq X$$

$$27X|B(a, b)|^2 \leq X$$

$$27|B(a, b)|^2 \leq 1.$$

Therefore $R_5(X)$ is mapped into the region $R_5(1)$ by this change of variables as we have $|A(a, b)| \leq (\frac{1}{4})^{1/3}$ and $|B(a, b)| \leq (\frac{1}{27})^{1/2}$. We will now determine the change in area that occurs as a result of this change of variables. We will do so by considering the determinant of the Jacobian, as is done in [16, p.894-896].

For simplicity denote $f(a, b) = a \sqrt[12]{X}$ and $g(a, b) = b \sqrt[12]{X}$. From [16], the Jacobian corresponding to these functions that provide our change of variables is given by

$$J = \begin{vmatrix} \frac{\partial f}{\partial a} & \frac{\partial f}{\partial b} \\ \frac{\partial g}{\partial a} & \frac{\partial g}{\partial b} \end{vmatrix} = \begin{vmatrix} \sqrt[12]{X} & 0 \\ 0 & \sqrt[12]{X} \end{vmatrix} = \sqrt[6]{X}.$$

From [16, p.894] we know that the area of our original region, before the change of variables, is equal to the area of our new region, resulting from the change of variables, multiplied by a scaling factor that is given by the Jacobian corresponding to this change of variables. Thus as $J = \sqrt[6]{X}$ we get

$$Area(R_5(X)) = X^{1/6}Area(R_5(1)).$$

□

Proposition 5.2.5. *Similarly the region $R'_5(X)$ is homogeneous such that*

$$Area(R'_5(X)) = X^{1/6}Area(R'_5(1)).$$

Proof. Note that the equations defining both of our curves $\widehat{A}(a, b) \leq \left(\frac{X}{4}\right)^{1/3}$ and $\widehat{B}(a, b) \leq \left(\frac{X}{27}\right)^{1/2}$ are homogeneous of degree 4 and degree 6, respectively. Thus this proposition follows the same proof structure as is used to prove Proposition 5.2.4 through the same change of variables that sends $a \rightarrow \sqrt[12]{a}$ and $b \rightarrow \sqrt[12]{b}$. \square

Note that the number of integral points in $R_5(X)$, which we will denote $r_5(X)$, is the number of equations of elliptic curves in short Weierstrass form that have 5-torsion with height less than or equal to X . Similarly, the number of integral points in $R'_5(X)$, denoted $r'_5(X)$, is the number of equations of elliptic curves in short Weierstrass form that have local 5-divisibility without 5-torsion with height less than or equal to X . The number of integral points in a compact region is directly related to the area of this region as is shown by the Principle of Lipschitz.

Proposition 5.2.6. *The Principle of Lipschitz states that the area of a compact region is equal to the number of integral points in the region plus a small error term.*

Therefore the areas of $R_5(X)$ and $R'_5(X)$ will provide the number of integral points in these regions and therefore the number of minimal models of elliptic curves within each of our different sets of curves. Our ability to count these minimal models will allow us to evaluate our probability P_5 . We now define e_5 to be the maximal length of the projections of $R_5(X)$ onto the coordinate axes. Similarly, define e'_5 to be the maximal length of the projections of $R'_5(X)$ onto the coordinate axes. Let $(a, b) \in R_5(X)$ be a point that realizes the maximal length. Note that since $(a, b) \in R_5(X)$ this gives us that

$$4|(A(a, b))|^3 = 4|-27a^4 + 324ba^3 - 378b^2a^4 - 324b^3a - 27b^4|^3 \leq X.$$

From this equation we can conclude that $a \leq O(X^{1/12})$ and $b \leq O(X^{1/12})$. From this we get that $e_5 = 12$. A slight variation on this argument can be used to show $e'_5 = 12$. The values e_5 and e'_5 are used in the small error term that appears in the relationship between the area and number of integral points as is implied in the Principle of Lipschitz.

From the Principle of Lipschitz we get that

$$r_5(X) = \text{Area}(R_5(X)) + O(X^{1/e_5}) = \text{Area}(R_5(X)) + O(X^{1/12})$$

and

$$r'_5(X) = \text{Area}(R'_5(X)) + O(X^{1/e_{5'}}) = \text{Area}(R'_5(X)) + O(X^{1/12}).$$

Using Propositions 5.2.4, 5.2.5, and the equations above allows us to write

$$r_5(X) = \text{Area}(R_5(1))X^{1/6} + O(X^{1/12}) \text{ and } r'_5(X) = \text{Area}(R'_5(1))X^{1/6} + O(X^{1/12}). \quad (5.2.3)$$

Both $r_5(X)$ and $r'_5(X)$ consist of all equations of elliptic curves within their respective regions and therefore include non-minimal equations. Therefore we must address this overcount that occurs in both of these regions and sieve out the non-minimal equations. We define the following notation to match the analogous notation in [5, p.15]:

$$\begin{aligned} T_5(a, b) &= (-27a^4 + 324a^3b - 378a^2b^2 - 324ab^3 - 27b^4, \\ &\quad 54a^6 - 972a^5b + 4050a^4b^2 + 4050a^2b^4 + 972ab^5 + 54b^6) \\ T'_5(a, b) &= (-27a^4 - 6156a^3b - 13338a^2b^2 + 6156ab^3 - 27b^4, \\ &\quad 54a^6 - 28188a^5b - 540270a^4b^2 - 540270a^2b^4 + 28188ab^5 + 54b^6). \end{aligned}$$

That is

$$T_5(a, b) = (A(a, b), B(a, b)) \text{ and } T'_5(a, b) = (\hat{A}(a, b), \hat{B}(a, b)).$$

Let $\mathcal{E}_i(X)$ be the set of all equations of elliptic curves in the form $y^2 = x^3 + Ax + B$ such that $(A, B) = T_i(a, b)$ for some $a, b \in R_i(X) \cap \mathbf{Z}^2$. So $\mathcal{E}_5(X)$ contains all equations of elliptic curves E/\mathbf{Q} with 5 torsion of the form $E : y^2 = x^3 + Ax + B$ such that $\text{ht } E \leq X$, and $\mathcal{E}'_5(X)$ contains all equations of elliptic curves E/\mathbf{Q} with local 5-divisibility and no 5 torsion of the form $E : y^2 = x^3 + Ax + B$ such that $\text{ht } E \leq X$. Again $\mathcal{E}_i(X)$ will be an overcount as it will contain non-minimal models of curves for both $i = 5$ and $i = 5'$. Therefore we must begin to determine

the overcount by discussing the different points in each of our regions that will define the exact same equation for an elliptic curve.

Lemma 5.2.7. [5, p.15] *If M is the number of pairs (A, B) for which there exists more than one pair $(a, b) \in R_5(X) \cap \mathbf{Z}^2$ such that $(A, B) = T_5(a, b)$, then $M = O(X^{1/e_5})$. Similarly if M' is the number of pairs (A, B) for which there exists more than one pair $(a, b) \in R'_5(X) \cap \mathbf{Z}^2$ such that $(A, B) = T'_5(a, b)$, then $M' = O(X^{1/e_{5'}})$.*

This lemma is proved for $i = 1, 2, 3$ in [5] and can be shown to also hold for $i = 5$ and $i = 5'$ as stated above using similar strategies. Recall that as we are working with $i = 5$ and $i = 5'$ we have that $e_5 = 12$ and $e'_{5'} = 12$.

Using Lemma 5.2.7, from [5, p.15] we get that

$$\#\mathcal{E}_5(X) = r_5(X) + O(X^{1/12}). \quad (5.2.4)$$

And similarly

$$\#\mathcal{E}'_5(X) = r'_5(X) + O(X^{1/12}).$$

Notation: We define $N_G(X)$ to be the number of isomorphism classes of elliptic curves E/\mathbf{Q} such that $\text{ht } E \leq X$ and $E(\mathbf{Q})_{\text{tors}} \cong G$.

Harron and Snowden prove an analogous theorem to the following specifically for $N_{\mathbf{Z}/2\mathbf{Z}}(X)$ and $N_{\mathbf{Z}/3\mathbf{Z}}(X)$. We will prove the following theorem for $N_{\mathbf{Z}/5\mathbf{Z}}(X)$, and then consequently show it will also hold for the count of curves with local 5-divisibility without 5-torsion which we will denote $\widehat{N}_5(X)$.

Theorem 5.2.8. [5, p.15] *We have that*

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \frac{\text{Area}(R_5(1))}{\zeta(2)} X^{1/6} + O(X^{1/12}),$$

where ζ is the Riemann-zeta function.

We follow the proof presented for Theorem 5.5 in [5] by altering the proof specifically for $i = 5$ and provide details that were excluded from the original proof.

Proof. As we can represent each isomorphism class by a minimal model, we get that $N_G(X)$ is precisely the number of minimal models of elliptic curves with our desired torsion and with height less than or equal to X . Thus to determine $N_{\mathbf{Z}/5\mathbf{Z}}(X)$ we must start with $\#\mathcal{E}_5(X)$ and sieve out the number of non-minimal models contained in this set.

Notation: Let $E_{A,B}$ denote the equation of an elliptic curve in short Weierstrass form with coefficients A and B , that is, $E_{A,B} : y^2 = x^3 + Ax + B$.

Notation: We define $E_d(X)$ to be all equations of elliptic curves in the form E_{d^4A,d^6B} such that $E_{d^4A,d^6B} \in \mathcal{E}_5(X)$.

Remark 5.2.9. Note that all non-minimal models of elliptic curves in $\mathcal{E}_5(X)$ will belong to $E_d(X)$ for some $d \in \mathbb{N}$ such that $2 \leq d \leq X^{1/12}$. This will be true because if $E_{A,B}$ is a non-minimal model, then there exists some $u \in \mathbb{N}$ such that $A = u^4A'$ and $B = u^6B'$ where $A', B' \in \mathbf{Z}$. Furthermore we know that $2 \leq u \leq X^{1/12}$ because given some $u > X^{1/12}$ then $ht(E_{u^4A,u^6B}) > X^{1/12}$ such that $E_{u^4A,u^6B} \notin \mathcal{E}_5(X)$. Thus the only non-minimal models that could possibly be within our height constraint will be in a set $E_d(X)$ for some $2 \leq d \leq X^{1/12}$. \diamond

Therefore we get that

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \#\mathcal{E}_5(X) - \left| \bigcup_{d=2}^{X^{1/12}} E_d(X) \right|. \quad (5.2.5)$$

Let $P_X = \{p_1, p_2, \dots, p_r\}$ be the set of all primes less than or equal to $X^{1/12}$. Let $d \in \mathbb{N}$ such that $2 \leq d \leq X^{1/12}$. Then there exists some $i \in \{1, \dots, r\}$ such that $p_i | d$.

Claim 5.2.10. *Let p prime such that $p | d$. Then $E_d(X) \subseteq E_p(X)$.*

We will now explain why this claim is true. Let $E_{A,B} \in E_d$. Suppose as above that $p_i | d$ for some $p_i \in P_X$. Then $A = d^4A'$ and $B = d^6B'$ for some $A', B' \in \mathbf{Z}$. However since $p_i | d$ we also

know that $A = p_i^4 A''$ and $B = p_i^6 B''$ for some $A'', B'' \in \mathbf{Z}$. Therefore $E_{A,B} \in E_{p_i}$. Therefore $E_d \subseteq E_{p_i}$.

From proving this claim we now have that

$$\bigcup_{d=2}^{X^{1/12}} E_d(X) = \bigcup_{i=1}^r E_{p_i}(X)$$

and thus

$$\left| \bigcup_{d=2}^{X^{1/12}} E_d(X) \right| = \left| \bigcup_{i=1}^r E_{p_i}(X) \right|.$$

Therefore we get that

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \mathcal{E}_5(X) - \left| \bigcup_{i=1}^r E_{p_i}(X) \right|. \quad (5.2.6)$$

Now by the Inclusion-Exclusion Principle

$$- \left| \bigcup_{i=1}^r E_{p_i}(X) \right| = \sum_{\emptyset \neq J \subseteq P_X} (-1)^{|J|} \left| \bigcap_{j \in J} E_j(X) \right|. \quad (5.2.7)$$

Let $J \subseteq P_X$ then $J = \{\ell_1, \ell_2, \dots, \ell_t\}$ such that for all $i \in \{1, \dots, t\}$ we can conclude that $\ell_i = p_k$ for some $k \in \{1, \dots, r\}$. We define $D_J = \ell_1 \ell_2 \cdots \ell_t$.

Claim 5.2.11. *Note that $E_{\ell_1}(X) \cap E_{\ell_2}(X) \cap \cdots \cap E_{\ell_t}(X) = E_{\ell_1 \ell_2 \cdots \ell_t}(X)$.*

This holds as given an equation of an elliptic curve $E_{A,B} \in E_{\ell_1}(X) \cap E_{\ell_2}(X) \cap \cdots \cap E_{\ell_t}(X)$ where $(\ell_i, \ell_j) = 1$ for all $i, j \in \{1, \dots, t\}$, then $\ell_i^4 | A$ and $\ell_i^6 | B$ for all $i \in \{1, \dots, t\}$. Due to the coprimality of each of these factors we get that $(\ell_1 \ell_2 \cdots \ell_t)^4 | A$ and $(\ell_1 \ell_2 \cdots \ell_t)^6 | B$ so that $E_{A,B} \in E_{\ell_1 \ell_2 \cdots \ell_t}(X)$. Similarly if $E_{A,B} \in E_{\ell_1 \ell_2 \cdots \ell_t}(X)$ where the ℓ_i are prime, then $(\ell_1 \ell_2 \cdots \ell_t)^4 | A$ and $(\ell_1 \ell_2 \cdots \ell_t)^6 | B$ imply that $\ell_i^4 | A$ and $\ell_i^6 | B$ for all $i \in \{1, \dots, t\}$. Thus $E_{A,B} \in E_{\ell_1}(X) \cap E_{\ell_2}(X) \cap \cdots \cap E_{\ell_t}(X)$. This proves the claim.

Then for all $J \subseteq P_X$ such that $J \neq \emptyset$, we get from Claim 5.2.11 that

$$\bigcap_{j \in J} E_j(X) = E_{\ell_1}(X) \cap E_{\ell_2}(X) \cap \cdots \cap E_{\ell_t}(X) = E_{\ell_1 \ell_2 \cdots \ell_t}(X) = E_{D_J}(X).$$

Thus we can rewrite equation 5.2.7 as

$$-\left| \bigcup_{i=1}^r E_{p_i}(X) \right| = \sum_{\emptyset \neq J \subseteq P_X} (-1)^{|J|} \#E_{D_J}(X). \quad (5.2.8)$$

To move forward we must recall the definition of the Möbius function.

Definition 5.2.12. The Möbius function $\mu : \mathbf{N} \rightarrow \mathbf{C}$ is defined by

$$\mu(d) = \begin{cases} 1, & \text{if } d = 1 \\ (-1)^r, & \text{if } d = p_1 \cdots p_r \text{ such that } p_i \neq p_j \text{ for all } i, j \in \{1, \dots, r\} \\ 0, & \text{if any squares divide } d. \end{cases}$$

△

Again let $J \subseteq P_X$ such that $J = \{\ell_1, \ell_2, \dots, \ell_t\}$. Thus $D_J = \ell_1 \ell_2 \cdots \ell_t$. Note that $(-1)^{|J|} = (-1)^t$ as $|J| = t$. Also as $D_J = \ell_1 \ell_2 \cdots \ell_t$ where ℓ_i is prime and $\ell_i \neq \ell_j$ when $i \neq j$ for all $i, j \in \{1, \dots, t\}$, then by the definition of the Möbius function we get that $\mu(D_J) = (-1)^t$. Thus we get that $(-1)^{|J|} = \mu(D_J)$ for all $J \subseteq P_X$ where $J \neq \emptyset$.

Thus we can now rewrite equation 5.2.8 to get

$$-\left| \bigcup_{i=1}^r E_{p_i}(X) \right| = \sum_{\emptyset \neq J \subseteq P_X} \mu(D_J) \#E_{D_J}(X). \quad (5.2.9)$$

Suppose that $D_J > X^{1/12}$. Let $E_{A,B}$ be an elliptic curve in $E_{D_J}(X)$. Then $A = D_J^4 A'$ and $B = D_J^6 B'$ where $A', B' \in \mathbf{Z}$, but then $A > (\frac{X}{4})^{1/3}$ and $B > (\frac{X}{27})^{1/2}$ as $D_J^4 A' > (\frac{X}{4})^{1/3}$ and also $D_J^6 B' > (\frac{X}{27})^{1/2}$. If that were the case that would imply that $ht(E_{A,B}) > X$, a contradiction. Therefore $E_{D_J}(X) = \emptyset$, and thus $\#E_{D_J} = 0$ when $D_J > X^{1/12}$. Therefore we need only consider $D_J \leq X^{1/12}$. Thus we get that

$$-\left| \bigcup_{i=1}^r E_{p_i}(X) \right| = \sum_{\substack{\emptyset \neq J \subseteq P_X \\ D_J \leq X^{1/12}}} \mu(D_J) \#E_{D_J}(X). \quad (5.2.10)$$

Let $d \in \mathbf{N}$ be such that $1 < d \leq X^{1/12}$ and $p^2 \nmid d$ for all primes p . Recall that $P_X = \{p_1, p_2, \dots, p_r\}$ is the set of all primes less than or equal to $X^{1/12}$. Therefore as $d \leq X^{1/12}$, we can write the prime factorization of d to be $d = \ell_1 \ell_2 \cdots \ell_t$ such that for all $i \in \{1, \dots, t\}$ we have that $\ell_i = p_k$ for some $k \in \{1, \dots, r\}$. Note that $J = \{\ell_1, \ell_2, \dots, \ell_t\}$ is a subset of P_X as

otherwise this would imply that $d > X^{1/12}$. So every d between 2 and $X^{1/12}$ such that $p^2 \nmid d$ for all primes p , will be represented by a unique D_J term and thus corresponds to a unique subset of P_X . For simplicity let $S_x = \{d \mid 1 < d \leq X^{1/12} \text{ and } p^2 \nmid d \text{ for some prime } p\}$. Thus we can now rewrite equation 5.2.10 as

$$-\left| \bigcup_{i=1}^r E_{p_i}(X) \right| = \sum_{\substack{d=2 \\ d \notin S_X}}^{X^{1/12}} \mu(d) \#E_d(X). \quad (5.2.11)$$

We now plug this equality into equation 5.2.6 to get that

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \mathcal{E}_5(X) + \sum_{\substack{d=2 \\ d \notin S_X}}^{X^{1/12}} \mu(d) \#E_d(X). \quad (5.2.12)$$

Now take some $d \in S_X$. Then there exists some prime p such that $p^2 \mid d$, and thus we get that $\mu(d) = 0$. Also note that $\mathcal{E}_5(X) = E_1(X)$ and $\mu(1) = 1$. Thus we can now write

$$\begin{aligned} N_{\mathbf{Z}/5\mathbf{Z}}(X) &= \# \mathcal{E}_5(X) + \sum_{\substack{d=2 \\ d \notin S_X}}^{X^{1/12}} \mu(d) \#E_d(X) \\ &= 1 \cdot \#E_1(X) + \sum_{\substack{d=2 \\ d \notin S_X}}^{X^{1/12}} \mu(d) \#E_d(X) + \sum_{\substack{d=2 \\ d \in S_X}}^{X^{1/12}} 0 \cdot \#E_d(X) \\ &= \mu(1) \cdot \#E_1(X) + \sum_{\substack{d=2 \\ d \notin S_X}}^{X^{1/12}} \mu(d) \#E_d(X) + \sum_{\substack{d=2 \\ d \in S_X}}^{X^{1/12}} \mu(d) \#E_d(X) \\ &= \sum_{d=1}^{X^{1/12}} \mu(d) \#E_d(X). \end{aligned} \quad (5.2.13)$$

Claim 5.2.13. *We now claim that $\#E_d(X) = \#\mathcal{E}_5\left(\frac{X}{d^{12}}\right)$.*

Let $E_{A,B} \in \#E_d(X)$. Then $A = d^4 A'$ and $B = d^6 B'$ for some $A', B' \in \mathbf{Z}$. Therefore

$$ht(E_{A,B}) = \max\{4A^3, 27B^2\} = \max\{4(d^4 A')^3, 27(d^6 B')^2\} = d^{12} \max\{4A'^3, 27B'^2\} \quad (5.2.14)$$

Now we know that $ht(E_{A,B}) \leq X$, and thus $d^{12} \max\{4A'^3, 27B'^2\} = d^{12} ht(E_{A',B'}) \leq X$.

This gives that $ht(E_{A',B'}) \leq \frac{X}{d^{12}}$. Therefore $E_{A',B'} \in \mathcal{E}_5(X)$. From this we can conclude that $\#E_d(X) \leq \#\mathcal{E}_5\left(\frac{X}{d^{12}}\right)$. Similarly, one can show that $\#E_d(X) \geq \#\mathcal{E}_5\left(\frac{X}{d^{12}}\right)$. Therefore we get that

$\#E_d(X) = \#\mathcal{E}_5\left(\frac{X}{d^{12}}\right)$. Using this equality we can then rewrite 5.2.13 to get

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \sum_{d=1}^{X^{1/12}} \mu(d) \#\mathcal{E}_5\left(\frac{X}{d^{12}}\right). \quad (5.2.15)$$

From equations 5.2.3 and 5.2.4 we get that

$$\#\mathcal{E}_5\left(\frac{X}{d^{12}}\right) = \text{Area}(R_5(1)) \left(\frac{X}{d^{12}}\right)^{1/6} + O\left(\left(\frac{X}{d^{12}}\right)^{1/12}\right).$$

Thus equation 5.2.15 becomes

$$\begin{aligned} N_{\mathbf{Z}/5\mathbf{Z}}(X) &= \sum_{d=1}^{X^{1/12}} \mu(d) \left(\text{Area}(R_5(1)) \left(\frac{X}{d^{12}}\right)^{1/6} + O\left(\left(\frac{X}{d^{12}}\right)^{1/12}\right) \right) \\ &= \text{Area}(R_5(1)) X^{1/6} \sum_{d=1}^{X^{1/12}} \frac{\mu(d)}{d^2} + O(X^{1/12}). \end{aligned}$$

Now recall the fact that

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},$$

where ζ is the Riemann-zeta function. Therefore we have

$$\sum_{d=1}^{X^{1/12}} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} + O(X^{1/12}).$$

Therefore we get the desired result

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \frac{\text{Area}(R_5(1)) X^{1/6}}{\zeta(2)} + O(X^{1/12}).$$

□

Now let $\widehat{N}_5(X)$ be the number of all isomorphism classes of elliptic curves with local 5-divisibility and no 5-torsion, which have height less than or equal to X .

Theorem 5.2.14. *We have that*

$$\widehat{N}_5(X) = \frac{\text{Area}(R'_5(1)) X^{1/6}}{\zeta(2)} + O(X^{1/12}).$$

Proof. This proof follows from the proof of 5.2.8. \square

Remark 5.2.15. Recall that by definition $N_{\mathbf{Z}/5\mathbf{Z}}(X)$ provides the number of all minimal models of elliptic curves up to height X that have 5-torsion, and $\widehat{N}_5(X)$ provides the number of all minimal models of elliptic curves up to height X that have local 5-divisibility without 5-torsion. As we have mentioned 5-torsion implies local 5-divisibility and thus all of the curves accounted for by $N_{\mathbf{Z}/5\mathbf{Z}}(X)$ also have local 5-divisibility. Therefore the total number of minimal models of elliptic curves with local 5-divisibility up to height X will be given by $N_{\mathbf{Z}/5\mathbf{Z}}(X) + \widehat{N}_5(X)$. Thus we can rewrite our probability using this notation as

$$P_5 = \lim_{X \rightarrow \infty} \frac{N_{\mathbf{Z}/5\mathbf{Z}}(X)}{N_{\mathbf{Z}/5\mathbf{Z}}(X) + \widehat{N}_5(X)},$$

where from Theorem 5.2.8 we get that

$$N_{\mathbf{Z}/5\mathbf{Z}}(X) = \frac{\text{Area}(R_5(1))}{\zeta(2)} X^{1/6} + O(X^{1/12}),$$

and from Theorem 5.2.14 we get that

$$\widehat{N}_5(X) = \frac{\text{Area}(R'_5(1))X^{1/6}}{\zeta(2)} + O(X^{1/12}).$$

Using the results from Theorem 5.2.8 and Theorem 5.2.14 in our equation for P_5 and simplifying the resulting equation, we are able to eliminate X from our equation of P_5 and thus get rid of the limit within the definition of our probability. Following this simplification we get that

$$P_5 = \frac{\text{Area}(R_5(1))}{\text{Area}(R_5(1)) + \text{Area}(\widehat{R}_5(1))}. \quad (5.2.16)$$

\diamond

This tells us that our probability can be determined by comparing $\text{Area}(R_5(1))$ and $\text{Area}(R'_5(1))$. We will determine this ratio in the following chapter.

5.3 Considering $\ell = 7$

We cannot use this same procedure for $\ell = 7$ as we are able to for $\ell = 5$ for a variety of reasons. One example of why these methods for $\ell = 5$ will not work for $\ell = 7$ is a result of the fact that $d_7 = 12$. Therefore when trying to prove a similar version of Theorem 5.2.8, but for $N_{\mathbf{Z}/7\mathbf{Z}}$ we would need to evaluate

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},$$

where we would have that $s = 1$, but when $s = 1$ this sum doesn't converge and therefore the strategy falls a part. Additionally, the error term in this proof is not fine enough for the case where $\ell = 7$. While we have not calculated the asymptotics for when $\ell = 7$, we still believe that minor alterations to these methods used in [5] could be used to find the asymptotics for the $\ell = 7$ case.

6

Results

6.1 Outline of Proof for Determining P_5

We have already completed many of the necessary steps to work towards computing P_5 . The strategy that we use to compute the desired probability can be outlined in the following steps:

- I. Compute universal models using the Tate normal form to parameterize elliptic curves E/\mathbf{Q} with a 5-torsion point, and perform a change of variables to get the isomorphic curve in short Weierstrass form that will also have 5-torsion.
- II. Create an associated family of isogenous curves that have local 5-divisibility, but do not have 5-torsion using the algorithm of Vélú from [17].
- III. Use the methods of Harron and Snowden in [5] to sieve out the non-minimal models in our count of both types of elliptic curves.
- IV. Show that the difference in the number of isomorphism classes of each type of elliptic curve can be given through a comparison of the areas of regions associated with each universal model.

V. Determine the difference in area between the region implied by the model of curves with local 5-divisibility, but no 5-torsion up to height X and the region given by the models of curves with 5-torsion up to height X .

VI. Combine our findings to determine P_5 .

6.2 Experimenting with Equations

Recall that given a pair of points $a, b \in \mathbf{Z}$, we can define a curve with 5-torsion given by the equation

$$\begin{aligned} E : y^2 &= x^3 + A(a, b)x + B(a, b), \\ A(a, b) &= -27a^4 + 324a^3b - 378a^2b^2 - 324ab^3 - 27b^4, \\ B(a, b) &= 54a^6 - 972a^5b + 4050a^4b^2 + 4050a^2b^4 + 972ab^5 + 54b^6, \end{aligned}$$

and a curve with local 5-divisibility that does not have 5-torsion given by the equation

$$\begin{aligned} \widehat{E} : y^2 &= x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b), \\ \widehat{A}(a, b) &= -27a^4 - 6156a^3b - 13338a^2b^2 + 6156ab^3 - 27b^4, \\ \widehat{B}(a, b) &= 54a^6 - 28188a^5b - 540270a^4b^2 - 540270a^2b^4 + 28188ab^5 + 54b^6. \end{aligned}$$

Remark 6.2.1. Recall from Definition 1.0.7 that $\text{ht } E$ denotes the height of an elliptic curve E , such that if E is given by the equation $E : y^2 = x^3 + Ax + B$, then

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

Note that while considering curves up to a certain height X , that if $a, b \in \mathbf{Z}$ define an elliptic curve $E : y^2 = x^3 + A(a, b)x + B(a, b)$ such that $\text{ht } E < X$, that does not necessarily imply that the elliptic curve $\widehat{E} : y^2 = x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b)$ defined using the same a and b will also satisfy $\text{ht } \widehat{E} < X$. In other words if $a, b \in \mathbf{Z}$ satisfy that

$$\max(|4(A(a, b))^3|, |27(B(a, b))^2|) \leq X,$$

it is possible that

$$\max(|4(\widehat{A}(a,b))^3|, |27(\widehat{B}(a,b))^2|) > X.$$

◇

It is the possible disparity in the heights of these sets of curves that makes considering the number of isomorphism classes within each model up to a certain height interesting. Before calculating the specific ratio we wrote code in Sage to count the number of curves with 5-torsion, denoted #Tors in the table below, and then also counted the number of curves with local 5-divisibility and no 5-torsion, denoted #Divs in the table below. For each iteration we counted the number of elliptic curves of each type both up to height $X = 10^n$. The final column of the table provides the ratio of these two counts.

$n, X = 10^n$	# Tors	#Divs	Ratio
9	0	0	-
10	1	0	-
11	2	0	-
12	4	0	-
13	7	0	-
14	14	1	14
15	20	1	20
16	30	3	10
17	42	5	8.4
18	72	8	9
19	100	13	7.692
20	162	23	7.043
21	230	35	6.571
22	347	56	6.196
23	516	84	6.143
24	762	132	5.773
25	1144	199	5.749
26	1691	303	5.581
27	2492	451	5.525
28	3670	680	5.397
29	5411	1012	5.347
30	7950	1505	5.282

From the experimental data we conjectured that given an elliptic curve E with local 5-divisibility, it is about 5 times more likely that E will also have a torsion point of order 5 than not. To formalize and confirm this conjecture we turn to a more rigorous way of considering the counts.

Recall from equation 5.2.16 we have deduced that

$$P_5 = \frac{\text{Area}(R_5(1))}{\text{Area}(R_5(1)) + \text{Area}(\widehat{R}_5(1))},$$

where from equations 5.2.1 and 5.2.2 we get that

$$R_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |A(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |B(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (6.2.1)$$

$$R'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}. \quad (6.2.2)$$

Theorem 6.2.2. *We can show that $\text{Area}(R_5(X)) = 5 \cdot \text{Area}(R'_5(X))$.*

We will start proving this theorem by splitting up both of our regions $R_5(X)$ and $R'_5(X)$ in order to facilitate an easier comparison of their areas. We define

$$A_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |A(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \right\}, \quad (6.2.3)$$

$$B_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |B(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (6.2.4)$$

$$A'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \right\}, \quad (6.2.5)$$

$$B'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{B}(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}. \quad (6.2.6)$$

Note that

$$R_5(X) = A_5(X) \cap B_5(X) \quad \text{and} \quad R'_5(X) = A'_5(X) \cap B'_5(X).$$

For $X = 1$ we get the following two intersections:

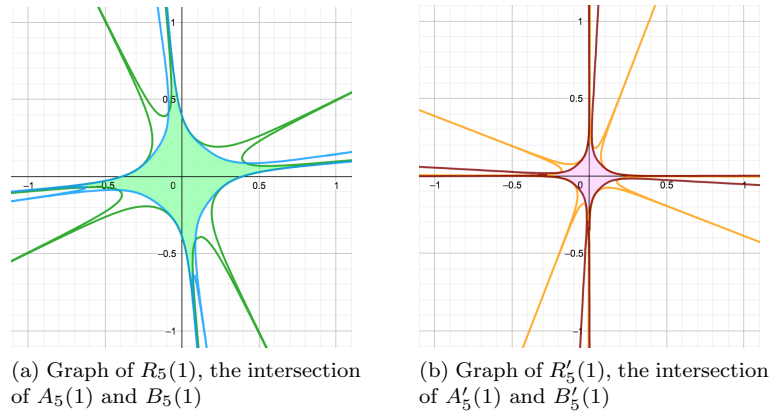


Figure 6.2.1: The shaded regions above are exactly the intersections in which we are interested.

Graphing the regions $R_5(X)$ and $R'_5(X)$ as above and observing the similarities between the regions led to the conjecture that one of these regions could be altered through a simple process of rotation, reflection, and scaling in order to get the regions to be the same. This would imply that the area of the regions differ only by a scalar factor. As we will be concerned with the areas of these compact regions it is important to note that reflecting and rotating regions does not change their area. To perform the rotation on the regions, we must begin by understanding how one can algebraically rotate a curve. We will rotate and apply a reflection to the region $R'_5(X)$ so that it is only different from the region $R_5(X)$ by a unique scaling factor, which the experimental data suggests will be 5.

6.3 Rotating Curves

To begin searching for the appropriate rotations of our region $R'_5(X)$, we must start with a simple explanation of how one rotates a curve.

Theorem 6.3.1. [1, p.262] *To rotate a curve $f(x, y) = 0$ by an angle of θ , set $X = x \cos(\theta) - y \sin(\theta)$ and $Y = y \sin(\theta) + x \cos(\theta)$. Then compute $f(X, Y)$ at θ to get your newly rotated region in terms of x and y .*

For our circumstances we are not given our angle of rotation and must find a way to compute the appropriate angle. We will look for an angle of rotation that makes the coefficients defining both of our two regions differ only by a scaling factor. To explore how one may find the appropriate angle of rotation, we provide an example for which we will work to find the angle that will rotate an ellipse that is not symmetric about the axes to be symmetric on the axes.

Example 6.3.2. Take the ellipse C given by

$$C : 2x^2 - 2xy + 2y^2 = 7.$$

Suppose that we would like to find the equation of the rotated ellipse such that after rotation the ellipse is located symmetrically on the axes. Suppose that we would like the angle of rotation to be positive and minimal. First we must find the correct angle of rotation. We will call this desired angle θ .

Step 1: Set

$$x = X \cos(\theta) - Y \sin(\theta) \quad \text{and} \quad y = X \sin(\theta) + Y \cos(\theta).$$

Step 2: Plug our new x and y values into our equation for C to get

$$\begin{aligned} (2 \cos^2(\theta) - 2 \sin(\theta) \cos(\theta) + 2 \sin^2(\theta))X^2 + (-2 \cos^2(\theta) + 2 \sin^2(\theta))XY \\ + (2 \cos^2(\theta) + 2 \sin(\theta) \cos(\theta) + 2 \sin^2(\theta))Y^2 = 7. \end{aligned}$$

Step 3: Find our θ . We want our graph to be symmetric about the axes and therefore if the point (X, Y) is on our rotated region then $(-X, Y)$, $(X, -Y)$ and $(-X, -Y)$ should also be on our rotated region. To get this symmetry we need to get rid of any terms where X or Y have an odd degree. This will require that the coefficient on the XY term be 0, because in this example the only term that has an X or Y of odd degree is precisely the term XY . So we set

the coefficient of XY equal to 0. Which provides the solvable equation for θ given by

$$-2 \cos^2(\theta) + 2 \sin^2(\theta) = 0 \quad (6.3.1)$$

$$\sin^2(\theta) = \cos^2(\theta)$$

$$\theta = \frac{\pi}{4}.$$

Note that there are multiple values for θ that would result in our desired symmetry, we decided to look for the smallest positive value for θ .

Step 4: Plug our values for θ into our new equation. This results in the equation of our rotated ellipse given by:

$$X^2 + 3Y^2 = 7.$$

To check that we have properly rotated this ellipse refer to the images below:

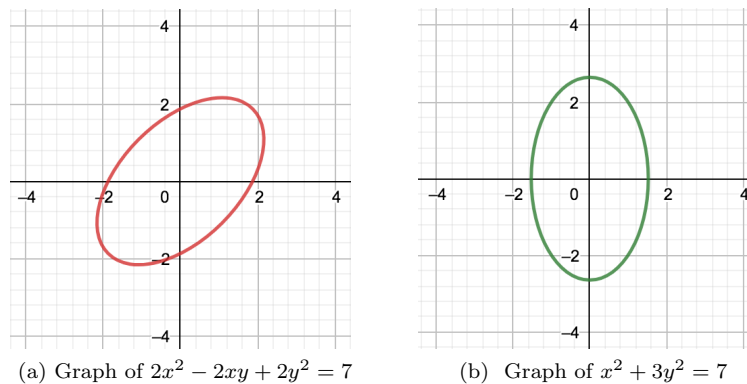


Figure 6.3.1: Rotation of an Ellipse by $\frac{\pi}{4}$.

◇

As we now understand how curves are rotated, we can begin to rotate our regions. However instead of rotating with the goal of obtaining a region that is symmetric about the axes, we will aim to rotate $R'_5(X)$ so that if we were to scale the region by a factor of 5 then we would obtain the region $R_5(X)$.

6.4 Rotating and Reflecting $A'_5(X)$

In order to work towards rotating $R'_5(X)$ we will begin by rotating the region

$$A'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \right\}. \quad (6.4.1)$$

By the definition of the region, rotating the curve $|\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{1/3}$ will rotate the region $A'_5(X)$. As an example of the regions we are rotating, for $X = 1$ we get the following two images:

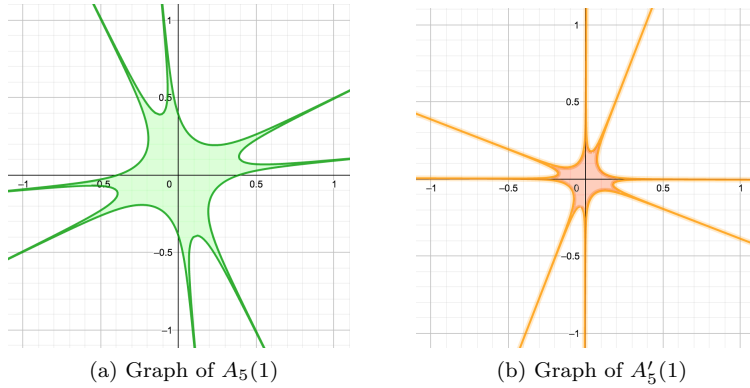


Figure 6.4.1: Comparing the Regions $A_5(1)$ and $A'_5(1)$.

Again by simply observing the graphs in Figure 6.4.1, it certainly seems possible that a simple rotation of the graph $A'_5(1)$ will result in a scaled version of the graph $A_5(X)$.

Proposition 6.4.1. *Let $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11}\right)$ be our angle of rotation. Then*

$$\widehat{A}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi))) = A(\sqrt{5}x, \sqrt{5}y).$$

Note that $\widehat{A}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi)))$ is simply the curve $\widehat{A}(x, y)$ that has been rotated by an angle of ϕ and then reflected across the x -axis.

Proof. We will begin with the rotation. Let $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11}\right)$. Recall that

$$\widehat{A}(X, Y) = -27X^4 - 6156X^3Y - 13338X^2Y^2 + 6156XY^3 - 27Y^4.$$

As shown before, to rotate a region by ϕ , we must start by setting

$$X = x \cos(\phi) - y \sin(\phi) \text{ and } Y = y \sin(\phi) + x \cos(\phi).$$

Thus we can now write $A(X, Y)$ in terms of x and y and relabel this new equation $\widehat{A}_R(x, y)$ defined by

$$\begin{aligned} \widehat{A}_R(x, y) = & (-27 \cos^4(\phi) - 6156 \sin(\phi) \cos^3(\phi) - 13338 \sin^2(\phi) \cos^2(\phi) + 6156 \sin^3(\phi) \cos(\phi) - 27 \sin^4(\phi))x^4 \\ & + (-6156 \cos^4(\phi) - 26568 \sin(\phi) \cos^3(\phi) + 36936 \sin^2(\phi) \cos^2(\phi) \\ & + 26568 \sin^3(\phi) \cos(\phi) - 6156 \sin^4(\phi))yx^3 \\ & + (-13338 \cos^4(\phi) + 36936 \sin(\phi) \cos^3(\phi) + 53028 \sin^2(\phi) \cos^2(\phi) \\ & - 36936 \sin^3(\phi) \cos(\phi) - 13338 \sin^4(\phi))y^2x^2 \\ & + (6156 \cos^4(\phi) + 26568 \sin(\phi) \cos^3(\phi) - 36936 \sin^2(\phi) \cos^2(\phi) \\ & - 26568 \sin^3(\phi) \cos(\phi) + 6156 \sin^4(\phi))y^3x \\ & + (-27 \cos^4(\phi) - 6156 \sin(\phi) \cos^3(\phi) - 13338 \sin^2(\phi) \cos^2(\phi) + 6156 \sin^3(\phi) \cos(\phi) - 27 \sin^4(\phi))y^4. \end{aligned} \tag{6.4.2}$$

For ease of notation we relabel this equation

$$\widehat{A}_R(x, y) = f(\phi)x^4 + g(\phi)yx^3 + h(\phi)y^2x^2 - g(\phi)y^3x + f(\phi)y^4$$

where

$$f(\phi) = -27 \cos^4(\phi) - 6156 \sin(\phi) \cos^3(\phi) - 13338 \sin^2(\phi) \cos^2(\phi) + 6156 \sin^3(\phi) \cos(\phi) - 27 \sin^4(\phi),$$

$$g(\phi) = -6156 \cos^4(\phi) - 26568 \sin(\phi) \cos^3(\phi) + 36936 \sin^2(\phi) \cos^2(\phi) + 26568 \sin^3(\phi) \cos(\phi) - 6156 \sin^4(\phi),$$

$$h(\phi) = -13338 \cos^4(\phi) + 36936 \sin(\phi) \cos^3(\phi) + 53028 \sin^2(\phi) \cos^2(\phi) - 36936 \sin^3(\phi) \cos(\phi) - 13338 \sin^4(\phi).$$

Evaluating these polynomial coefficients at $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$ yields

$$f(\phi) = -675, \quad g(\phi) = -8100, \text{ and } h(\phi) = -9450.$$

Thus we can write

$$\widehat{A}_R(x, y) = -675x^4 - 8100yx^3 - 9450y^2x^4 + 8100y^3x - 675y^4.$$

Now we will reflect our region over the x -axis by sending $y \rightarrow -y$ resulting in the curve $\widehat{A}_R(x, -y)$. Recall the definition

$$A(x, y) = -27x^4 + 324yx^3 - 378y^2x^4 - 324y^3x - 27y^4.$$

From here we can relate $\widehat{A}_R(x, -y)$ to $A(x, y)$ by the following:

$$\begin{aligned} \widehat{A}_R(x, -y) &= -675x^4 + 8100yx^3 - 9450y^2x^4 - 8100y^3x - 675y^4 \\ &= 25(-27x^4 + 324yx^3 - 378y^2x^4 - 324y^3x - 27y^4) \\ &= -27(\sqrt{5}x)^4 + 324(\sqrt{5}y)(\sqrt{5}x)^3 - 378(\sqrt{5}y)^2(\sqrt{5}x)^4 - 324(\sqrt{5}y)^3(\sqrt{5}x) - 27(\sqrt{5}y)^4 \\ &= A(\sqrt{5}x, \sqrt{5}y). \end{aligned}$$

Note that $\widehat{A}_R(x, -y) = \widehat{A}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi)))$. Thus we can conclude that

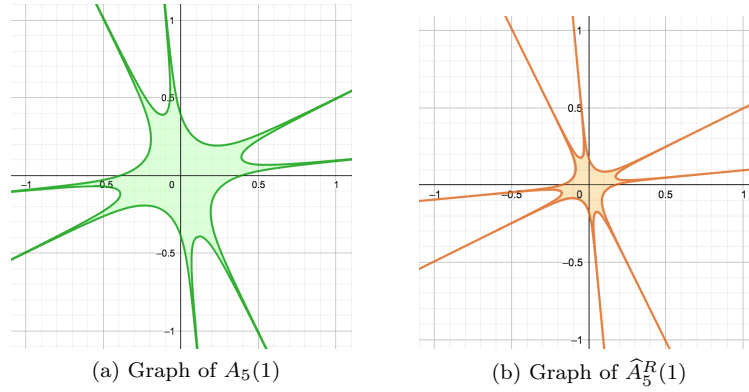
$$\widehat{A}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi))) = A(\sqrt{5}x, \sqrt{5}y).$$

□

Define a new region, denoted $\widehat{A}_5^R(X)$, using the rotated and reflected curve that we have obtained:

$$\widehat{A}_5^R(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}_R(a, -b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \right\}. \quad (6.4.3)$$

Following this rotation and reflection we are left with the two regions in Figure 6.4.2 below

Figure 6.4.2: Comparison of $A_5(X)$ to our new region $\widehat{A}_5^R(X)$.

From this comparison of graphs and equations one can begin to see that, if scaled, our new region $\widehat{A}_5^R(X)$ will be identical to $A_5(X)$. As $R'_5(X) = A'_5(X) \cap B'_5(X)$, in order to fully rotate $R_5(X)$ we will now have to rotate and reflect $B'_5(X)$. In order to not alter the area of the intersection of $A'_5(X)$ and $B'_5(X)$, the ways in which we rotate and reflect $B'_5(X)$ must mirror the changes that we made to $A'_5(X)$.

6.5 Rotating and Reflecting $B'_5(X)$

To complete our rotation of $R'_5(X)$, we will now rotate and reflect $B'_5(X)$. Recall that the region $B'_5(X)$ is defined by

$$B'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{B}(a, b)| \leq \left(\frac{X}{27} \right)^{(1/2)} \right\}. \quad (6.5.1)$$

From this definition of the region $B'_5(X)$ we see that we can rotate this region by rotating the curve $|\widehat{B}(x, y)| \leq \left(\frac{X}{27} \right)^{(1/2)}$.

As an example of the regions we are rotating, for $X = 1$ we get the following two images:

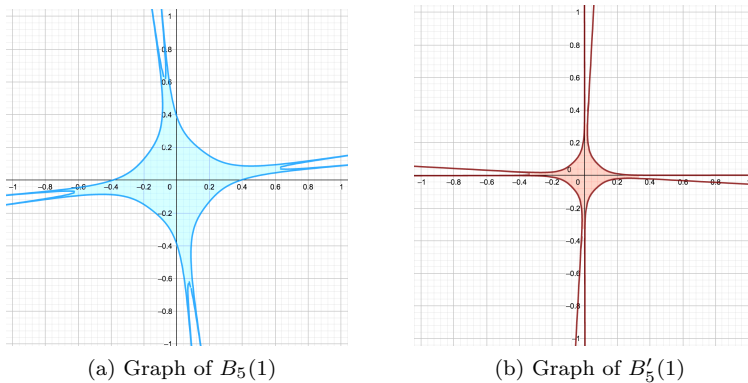


Figure 6.5.1: Comparing the Regions $B_5(1)$ and $B'_5(1)$.

We will now show that the region $B'_5(X)$ is simply a rotation, reflection, and scaling of $B_5(X)$.

Proposition 6.5.1. *Let $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$ be our angle of rotation. Then*

$$\widehat{B}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi))) = B(\sqrt{5}x, \sqrt{5}y).$$

Remark 6.5.2. It is important to note that this angle $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$, is the same angle of rotation as was used in the previous section to rotate $A'_5(X)$. Rotating $A'_5(X)$ and $B'_5(X)$ by the same angle of rotation will leave the area of their intersection unaffected. \diamond

Proof. We will begin with the rotation. Let $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$.

Recall that

$$\widehat{B}(X, Y) = 54X^6 - 28188X^5Y - 540270X^4Y^2 - 540270X^2Y^4 + 28188XY^5 + 54Y^6.$$

As shown before, to rotate a region by ϕ , we must start by setting

$$X = x \cos(\phi) - y \sin(\phi) \text{ and } Y = y \sin(\phi) + x \cos(\phi).$$

Thus we can now write $\widehat{B}(X, Y)$ in terms of x and y to and relabel this new equation $\widehat{B}_R(x, y)$ defined by

$$\begin{aligned}
\widehat{B}_R(x, y) = & (54 \cos^6(\phi) - 28188 \sin(\phi) \cos^5(\phi) - 540270 \sin^2(\phi) \cos^4(\phi) \\
& - 540270 \sin^4(\phi) \cos^2(\phi) + 28188 \sin^5(\phi) \cos(\phi) + 54 \sin^6(\phi))x^6 \\
& + (-28188 \cos^6(\phi) - 1080864 \sin(\phi) \cos^5(\phi) + 140940 \sin^2(\phi) \cos^4(\phi) \\
& + 140940 \sin^4(\phi) \cos^2(\phi) + 1080864 \sin^5(\phi) \cos(\phi) - 28188 \sin^6(\phi))yx^5 \\
& + (-540270 \cos^6(\phi) + 140940 \sin \cos^5(\phi) + 1081350 \sin^2(\phi) \cos^4(\phi) \\
& + 1081350 \sin^4(\phi) \cos^2(\phi) - 140940 \sin^5(\phi) \cos(\phi) - 540270 \sin^6(\phi))y^2x^4 \\
& + (-540270 \cos^6(\phi) + 140940 \sin(\phi) \cos^5(\phi) + 1081350 \sin^2(\phi) \cos^4(\phi) \\
& + 1081350 \sin^4(\phi) \cos^2(\phi) - 140940 \sin^5(\phi) \cos(\phi) - 540270 \sin^6(\phi))y^4x^2 \\
& + (28188 \cos^6(\phi) + 1080864 \sin(\phi) \cos^5(\phi) - 140940 \sin^2(\phi) \cos^4(\phi) \\
& - 140940 \sin^4(\phi) \cos^2(\phi) - 1080864 \sin^5(\phi) \cos(\phi) + 28188 \sin^6(\phi))y^5x \\
& + (54 \cos^6(\phi) - 28188 \sin(\phi) \cos^5(\phi) - 540270 \sin^2(\phi) \cos^4(\phi) \\
& - 540270 \sin^4(\phi) \cos^2(\phi) + 28188 \sin^5(\phi) \cos(\phi) + 54 \sin^6(\phi))y^6. \tag{6.5.2}
\end{aligned}$$

For ease of notation we relabel this equation

$$\widehat{B}_R(x, y) = \widehat{f}(\phi)x^4 + \widehat{g}(\phi)yx^3 + \widehat{h}(\phi)y^2x^4 - \widehat{g}(\phi)y^3x + \widehat{f}(\phi)y^4,$$

where

$$\begin{aligned}
\widehat{f}(\phi) = & 54 \cos^6(\phi) - 28188 \sin(\phi) \cos^5(\phi) - 540270 \sin^2(\phi) \cos^4(\phi) - 540270 \sin^4(\phi) \cos^2(\phi) \\
& + 28188 \sin^5(\phi) \cos(\phi) + 54 \sin^6(\phi),
\end{aligned}$$

$$\begin{aligned}
\widehat{g}(\phi) = & -28188 \cos^6(\phi) - 1080864 \sin(\phi) \cos^5(\phi) + 140940 \sin^2(\phi) \cos^4(\phi) + 140940 \sin^4(\phi) \cos^2(\phi) \\
& + 1080864 \sin^5(\phi) \cos(\phi) - 28188 \sin^6(\phi),
\end{aligned}$$

$$\begin{aligned}
\widehat{h}(\phi) = & -540270 \cos^6(\phi) + 140940 \sin \cos^5(\phi) + 1081350 \sin^2(\phi) \cos^4(\phi) + 1081350 \sin^4(\phi) \cos^2(\phi) \\
& - 140940 \sin^5(\phi) \cos(\phi) - 540270 \sin^6(\phi).
\end{aligned}$$

Note that evaluating these polynomial coefficients at $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$ will yield

$$\widehat{f}(\phi) = -6750, \quad \widehat{g}(\phi) = -121500, \quad \text{and} \quad \widehat{h}(\phi) = -506250.$$

Thus we can write

$$\widehat{B}_R(x, y) = -6750x^6 - 121500yx^5 - 506250y^2x^4 - 506250y^4x^2 + 121500y^5x - 6750y^6.$$

Now we will reflect our region over the x -axis by sending $y \rightarrow -y$ to get $\widehat{B}_R(x, -y) \leq \left(\frac{X}{27} \right)^{1/2}$.

Recall the definition

$$B(x, y) = 54x^6 - 972yx^5 + 4050y^2x^4 + 4050y^4x^2 + 972y^5x + 54y^6.$$

From here we can relate $\widehat{B}_R(x, -y)$ to $B(x, y)$ by the following:

$$\begin{aligned} \widehat{B}_R(x, -y) &= -125(54x^6 - 972yx^5 + 4050y^2x^4 + 4050y^4x^2 + 972y^5x + 54y^6) \\ &= 54(\sqrt{5}x)^6 - 972(\sqrt{5}y)(\sqrt{5}x)^5 + 4050(\sqrt{5}y)^2(\sqrt{5}x)^4 \\ &\quad + 4050(\sqrt{5}y)^4(\sqrt{5}x)^2 + 972(\sqrt{5}y)^5(\sqrt{5}x) + 54(\sqrt{5}y)^6 \\ &= B(\sqrt{5}x, \sqrt{5}y). \end{aligned}$$

Note that $\widehat{B}_R(x, -y) = \widehat{B}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi)))$. Thus we can conclude that

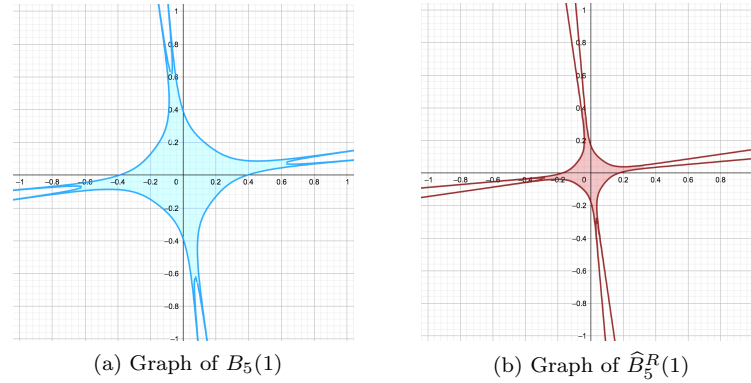
$$\widehat{B}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi))) = B(\sqrt{5}x, \sqrt{5}y).$$

□

Define a new region, denoted $\widehat{B}_5^R(X)$, using our new rotated and reflected curve that we have obtained:

$$\widehat{B}_5^R(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{B}_R(a, -b)| \leq \left(\frac{X}{27} \right)^{(1/2)} \right\}. \quad (6.5.3)$$

Following this rotation we are left with the two regions as shown in Figure 6.5.2.

Figure 6.5.2: Comparison of $B_5(X)$ to our new region $\widehat{B}_5^R(X)$.

Similarly to the preceding section, from this comparison one can begin to see that, if scaled, our new region $\widehat{B}_5^R(X)$, will be identical to $B_5(X)$. Now that we have rotated and reflected both of our regions whose intersection is $R'_5(X)$, we begin to discuss the changes that these rotations and reflections have on their intersection.

6.6 Comparing the Areas of Specified Regions

Recall that

$$R'_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}. \quad (6.6.1)$$

Note that if we rotate two different regions by the same angle ϕ and reflect both regions across the x -axis, then since we are applying the same changes to both regions, the intersection of these two regions will simply be rotated by that same angle and reflected across the x -axis as well. Thus rotating $\widehat{A}(x, y)$ and $\widehat{B}(x, y)$ by $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$ and then reflecting over the x -axis, will also rotate their intersection, which is given by $R'_5(X)$, by $\phi = \frac{1}{2} \tan^{-1} \left(\frac{2}{11} \right)$ and then reflect $R'_5(X)$ across the x -axis. This reflection and rotation of $R'_5(X)$ yields the new region

$$\widehat{R}_5^R(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}_R(a, -b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}_R(a, -b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (6.6.2)$$

Remark 6.6.1. Note that by construction $\widehat{R}_5^R(X)$ is simply a rotation and reflection of $R_5'(X)$.

Thus we get that

$$\text{Area}(\widehat{R}_5^R(X)) = \text{Area}(R_5'(X)).$$

◇

Proposition 6.6.2. *We get that*

$$\text{Area}(R_5(X)) = 5 \cdot \text{Area}(\widehat{R}_5^R(X)).$$

Proof. From the previous sections we have that

$$\widehat{A}_R(x, -y) = A(\sqrt{5}x, \sqrt{5}y) \text{ and } \widehat{B}_R(x, -y) = B(\sqrt{5}x, \sqrt{5}y), \quad (6.6.3)$$

where

$$\widehat{A}_R(x, -y) = \widehat{A}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi)))$$

and

$$\widehat{B}_R(x, -y) = \widehat{B}_5(x \cos(\phi) - y \sin(\phi), -(x \sin(\phi) + y \sin(\phi))).$$

Therefore we can write the region $\widehat{R}_5^R(X)$ in a different way to get

$$\begin{aligned} \widehat{R}_5^R(X) &= \left\{ (a, b) \in \mathbf{R}^2 \mid |\widehat{A}_R(a, -b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}_R(a, -b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\} \\ &= \left\{ (a, b) \in \mathbf{R}^2 \mid |A(\sqrt{5}a, \sqrt{5}b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |B(\sqrt{5}a, \sqrt{5}b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}. \end{aligned}$$

Now recall that

$$R_5(X) = \left\{ (a, b) \in \mathbf{R}^2 \mid |A(a, b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |B(a, b)| \leq \left(\frac{X}{27}\right)^{(1/2)} \right\}, \quad (6.6.4)$$

Let T be the transformation of the region $R_5(X)$ given by $f(a, b) = \sqrt{5}a$, the function transforming the first coordinates of the points in $R_5(X)$, and $g(a, b) = \sqrt{5}b$, the function transforming the second coordinates of the points in $R_5(X)$. Note that applying T to $R_5(X)$ certainly results

in the region $\widehat{R}_5^R(X)$. We will now use similar techniques from the previous chapter to compare these areas. From [16, p.894], the Jacobian of the transformation T is given by

$$\frac{\partial(f, g)}{\partial(a, b)} = \begin{vmatrix} \frac{\partial f}{\partial a} & \frac{\partial f}{\partial b} \\ \frac{\partial g}{\partial a} & \frac{\partial g}{\partial b} \end{vmatrix} = \begin{vmatrix} \sqrt{5} & 0 \\ 0 & \sqrt{5} \end{vmatrix} = 5.$$

Therefore from [16, p. 8.94] we know that the area of our original region is 5 times the size of the area of the region resulting from our change of variables. This gives us that

$$Area(R_5(X)) = 5 \cdot Area(\widehat{R}_5^R(X))$$

as desired. □

Theorem 6.6.3. *We get that*

$$Area(R_5(X)) = 5 \cdot Area(R'_5(X)).$$

Proof. This follows simply from the combination of Remark 6.6.1 and Proposition 6.6.2. □

Corollary 6.6.4. *As a specific case of Theorem 6.6.3 we get that*

$$Area(R_5(1)) = 5 \cdot Area(R'_5(1)).$$

From equation 5.2.16 along with our ratio of areas as given in Corollary 6.6.4 we arrive at our main theorem.

Theorem 6.6.5. *We have that*

$$P_5 = \frac{5}{6}.$$

Proof. From equation 5.2.16 we have that

$$P_5 = \frac{Area(R_5(1))}{Area(R_5(1)) + Area(\widehat{R}_5(1))}.$$

Note that we can substitute $Area(R_5(1)) = 5 \cdot Area(R'_5(1))$ to get the following chain of equations that provides our desired probability. Observe

$$P_5 = \frac{Area(R_5(1))}{Area(R_5(1)) + Area(\widehat{R}_5(1))} = \frac{5 \cdot Area(R'_5(1))}{5 \cdot Area(R'_5(1)) + Area(\widehat{R}_5(1))} = \frac{5 \cdot Area(R'_5(1))}{(5+1)Area(R'_5(1))} = \frac{5}{6}.$$

Therefore we have determined that $P_5 = \frac{5}{6}$. \square

6.7 Conjecture for $\ell = 7$

Recall that given a pair of points $a, b \in \mathbf{Z}$, we can define a curve with 7-torsion given by

$$y^2 = x^3 + A(a, b)x + B(a, b),$$

$$A(a, b) = -27a^8 + 324a^7b - 1134a^6b^2 + 1512a^5b^3 - 945a^4b^4 + 378a^2b^6 - 108ab^7 - 27b^8,$$

$$B(a, b) = 54a^{12} - 972a^{11}b + 6318a^{10}b^2 - 19116a^9b^3 + 30780a^8b^4 - 26244a^7b^5 \\ + 14742a^6b^6 - 11988a^5b^7 + 9396a^4b^8 - 2484a^3b^9 - 810a^2b^{10} + 324ab^{11} + 54b^{12}.$$

and a curve with local 7-divisibility that does not have 7-torsion given by the equation

$$y^2 = x^3 + \widehat{A}(a, b)x + \widehat{B}(a, b)$$

$$\widehat{A}(a, b) = -27a^8 - 6156a^7b - 1134a^6b^2 + 46872a^5b^3 - 91665a^4b^4 + 90720a^3b^5 - 44982a^2b^6 + 6372ab^7 - 27b^8,$$

$$\widehat{B}(a, b) = 54a^{12} - 28188a^{11}b - 483570a^{10}b^2 + 2049300a^9b^3 - 3833892a^8b^4 + 7104348a^7b^5 - 13674906a^6b^6 \\ + 17079660a^5b^7 - 11775132a^4b^8 + 4324860a^3b^9 - 790074a^2b^{10} + 27540ab^{11} + 54b^{12}.$$

Again there is a disparity in the heights of these sets of curves that makes considering the number of isomorphism classes in each set of curves up to some height interesting. We used very similar code from the $\ell = 5$ case to count the number of curves with 7-torsion, denoted $\#\text{Tors}$ in the table below, and then also counted the number of curves with local 7-divisibility and no 7-torsion, denoted $\#\text{Divs}$ in the table below, both up to height $X = 10^n$. The final column of the table provides the ratio of these two counts.

$n, X = 10^n$	# Tors	#Divs	Ratio
30	129	41	3.146
31	160	51	3.137
32	205	68	3.015
33	243	84	2.893
34	290	103	2.816
35	367	123	2.984
36	446	150	2.973
37	545	184	2.962
38	658	225	2.924
39	801	280	2.861
40	975	343	2.843
41	1190	413	2.881
42	1448	513	2.823
43	1748	622	2.810
44	2133	765	2.788
45	2568	930	2.761
46	3137	1136	2.761
47	3813	1393	2.737
48	4626	1687	2.742
49	5613	2051	2.737
50	6821	2499	2.729

It appears to be that these ratios may be approaching $\sqrt{7} \approx 2.646$. Therefore from the experimental data we conjectured that given an elliptic curve E with local 7-divisibility it is about $\sqrt{7}$ times more likely that E will also have a torsion point of order 7 than not. Therefore we arrive at the following conjecture for the value of P_7 .

Conjecture 6.7.1. *We conjecture that $P_7 = \frac{\sqrt{7}}{\sqrt{7}+1}$.*

As previously discussed in relation to the methods of Harron and Snowden in [5], we are unable to follow identical methods for the $\ell = 7$ case as we perform for $\ell = 5$. Examples of where our method for $\ell = 7$ falls apart can be found in the equation for the number of isomorphism classes given in [5], and also in the rotation of regions. We were unable to determine a simple alteration of the regions that wouldn't affect the area, but would allow one region to be simply a scaled version of the other. We believe that by altering some of these methods used for when $\ell = 5$, we will be able to prove this conjecture for the $\ell = 7$ case in the future.

Bibliography

- [1] H. Anton and C. Rorres, *Elementary Linear Algebra, Eleventh Edition*, Wiley, 2014.
- [2] E. Brown and B. Myers, *Elliptic Curves from Mordell to Diophantus and Back*, The American Mathematical Monthly **109** (2002), 639-649.
- [3] J. Cullinan and J. Voight, *On a probabilistic local-global principle for torsion on elliptic curves*, In preparation.
- [4] I. Garcia-Selfa, M. A Olalla, and J. M. Tornero, *Computing the Rational Torsion of an Elliptic Curve Using Tate Normal Form*, Journal of Number Theory **96** (2002), 76-88.
- [5] R. Harron and A. Snowden, *Counting Elliptic Curves with Prescribed Torsion*, Crelles Journal **729** (2017), 151-170.
- [6] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer-Verlag New York, 2000.
- [7] D. Husemöller, *Elliptic Curves, Second Edition*, New York: Springer Verlag, 2004.
- [8] International GeoGebra Institute, *GeoGebra Graphing Calculator (Version 6.0.528)*, 2019, <http://www.geogebra.org>.
- [9] N. Katz, *Galois properties of torsion points on abelian varieties*, Inventiones Mathematicae **62** (1981), 481-502.
- [10] N Koblitz, *Introduction to Elliptic Curves and Modular Forms, Second Edition*, New York: Springer Verlag, 1993.
- [11] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2013, <http://www.lmfdb.org>.
- [12] The PARI Group, *PARI/GP (Version 2.11.0)*, Univ. Bordeaux, 2018, <http://pari.math.u-bordeaux.fr/>.
- [13] J. H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, New York: Springer-Verlag, 2009.
- [14] J. H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag New York, 1992.

- [15] W. Stein, *SageMath, the Sage Mathematics Software System (Version 8.4)*, 2018, <http://www.sagemath.org/>.
- [16] J. Stewart, *Calculus: Concepts and Contexts, Fourth Edition*, Richard Stratton, 2010.
- [17] J. Vélou, *Isogénies entre courbes elliptiques*, Comptes Rendus de l'Académie des Sciences des Paris **273** (1971), 238–241.