Elliptic Curves and Probability of ℓ-Torsion

by Xiaoying He, Xuyang Li, Zoe Daunt

Final report for Northeastern Summer Mathematics Research Program

July 3rd, 2020

Mentored by

Lei Yang

Acknowledgements

We would like to thank our Mentor, Lei Yang, for all her help over the past two months. We truly appreciate the patience and understanding she showed us. We would also like to thank Rob Silversmith and Robin Walters for all the work they put in to organizing this program, especially given the unprecedented circumstances.

Abstract

The goal of our project is to answer Problem 3 of Andrew Sutherland's Elliptic Curves Problem Set 4 [1]. That is, we want to determine the probability that a random elliptic curve defined over a finite field $\mathbb{F}_p$ has an $\mathbb{F}_p$ point of prime order ℓ, where p is either a fixed prime much larger than ℓ, or a prime varying over some large interval. In order to do so, we must review some key concepts and theorems to gain a thorough understanding of elliptic curves. In the first part of this report, we will lead you through these key concepts and present a summary of the background material we studied throughout the course of our REU. In the second part, we will guide you through a problem on the probability of ℓ-torsion and share our findings. Our methods included deriving combinatorial formulas to describe probabilities, as well as writing Sage scripts to verify our results.

Chapter 1

Introduction to Elliptic Curves

1.1 The Projective Spaces

Definition 1.1.1 Projective Spaces Let k be a field, and let V be a vector space of dimension $n+1$ over the field k. The projective space $\mathbb{P}^n(k)$ is the set of equivalence classes of nonzero elements in the vector field V under the equivalence relation $\sim$ where $v_1 \sim v_2$ if $v_1, v_2 \in V$ and there exists some $\lambda \in k$ such that $v_1 = \lambda v_2$.

The projective plane is the set $\mathbb{P}^2(k)$ of all nonzero triples $(x, y, z) \in k^3$ modulo the equivalence relation defined above. Given a projective plane, the notation of a projective point $(x : y : z)$ denotes the equivalence class of $(x, y, z) \in k^3$.

Remark 1.1.2 Let $\mathbb{P}^2(k)$ be a projective plane over the field k. All points of the form $(x : y : 1) \in \mathbb{P}^2(k)$ form the affine plane of $\mathbb{P}^2(k)$, where $x, y \in k$ and 1 denotes the multiplicative identity of k. All points of the form $(x : y : 0) \in \mathbb{P}^2(k)$ form the line at infinity of $\mathbb{P}^2(k)$, where $x, y \in k$ and 0 denotes the additive identity of k.

Projective plane Let $\mathbb{A}$ be the affine space of an algebraically closed field k. The projective plane of $\mathbb{A}$ is represented by $\mathbb{P}^2(\mathbb{A}) = \mathbb{A}^2 \sqcup \mathbb{A} \sqcup \{\infty\}$.

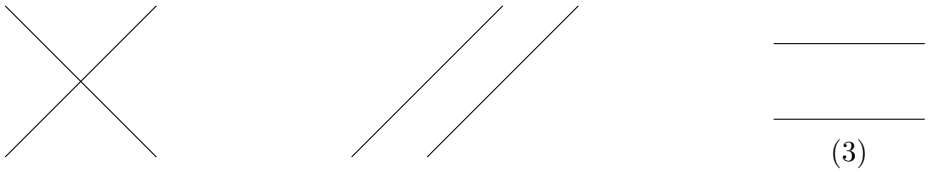
A point in the projective plane $\mathbb{P}^2(\mathbb{A})$ is either a point on the plane $\mathbb{A}^2$, or a point on the line at infinity $\mathbb{A}$, or the point at infinity $\{\infty\}$. A line in the projective plane $\mathbb{P}^2(\mathbb{A})$ is either the zero set of a polynomial $f(x, y, z) = ax + by + cz = 0$ where a, b, c are elements in the algebraically closed field k, or the line at infinity.

Proposition 1.1.3 Let A be an affine space. Any two lines in the projective space $\mathbb{P}^2(\mathbb{A}) = \mathbb{A}^2 \sqcup \mathbb{A} \sqcup \{0\}$ intersect at exactly one point.

1. Two non-parallel lines in $\mathbb{A}^2$ intersect at some point in the affine plane $\mathbb{A}^2$.
2. Two parallel lines in $\mathbb{A}^2$ that are not parallel to $y = 0$ intersect at some point in the line at infinity $\mathbb{A}$.
3. Two parallel lines in $\mathbb{A}^2$ that are parallel to $y = 0$ intersect at the point at infinity $\{\infty\}$.
4. A line in $\mathbb{A}^2$ and the line at infinity intersect at some point in the line at infinity $\mathbb{A}$.

Examples

1. Two non-parallel lines $x + y = 0$ and $x - y = 0$ incident at exactly one point $[x : y : z] = [0 : 0 : 1]$ on the affine plane in the real projective plane $\mathbb{P}^2(\mathbb{R})$.
2. Two parallel lines $x - y = 0$ and $x - y = z$ incident at exactly one point $[x : y : z] = [1 : 1 : 0]$ on the line at infinity in the real projective plane $\mathbb{P}^2(\mathbb{R})$.
3. Two parallel lines $y = 0$ and $y = z$ incident at the point at infinity $[x : y : z] = [1 : 0 : 0]$ in the real projective plane $\mathbb{P}^2(\mathbb{R})$.
4. The line $x + y = 0$ and the line at infinity $z = 0$ incident at exactly one point $[x : y : z] = [-1 : 1 : 0]$ on the line at infinity in the real projective plane $\mathbb{P}^2(\mathbb{R})$.



(1) (2) (3)

Definition 1.1.4 Conics Let k be an algebraically closed field. A conic in the projective plane $\mathbb{P}^2(k)$ is the zero set of a polynomial $f(x, y, z) = ax^2 + by^2 + cz^2 + dxy + eyz + fxz = 0$ where a, b, c, d, e, f are elements in the algebraically closed field k.

Consider the zero set of a given polynomial, the multiplicity of a root is the number of occurrence of this root.

Proposition 1.1.5 Let k be an algebraically closed field. Any two conics in the projective space $\mathbb{P}^2(k)$ intersect at exactly four points with multiplicity counted. A conic and a line in $\mathbb{P}^2(k)$ intersect at exactly two points with multiplicity counted.

Examples Two conics $x^2 + y^2 = z^2$ and $x^2 + (y - z)^2 = z^2$ intersect at two distinct points $[x : y : z] = [\sqrt{2} : \sqrt{2} : 2]$ and $[x : y : z] = [-\sqrt{2} : \sqrt{2} : 2]$ in $\mathbb{P}^2(\mathbb{R})$, whereas two conics $x^2 + y^2 = z^2$ and $x^2 + (y - 2z)^2 = z^2$ intersect at one point $[x : y : z] = [0 : 1 : 1]$ in $\mathbb{P}^2(\mathbb{R})$ with multiplicity two.

Remark 1.1.6 This example appears to contradict the above proposition. However, the field of real numbers $\mathbb{R}$ is not an algebraically closed field.

If we consider the algebraic closure $\mathbb{C}$ of $\mathbb{R}$, in the projective plane $\mathbb{P}^2(\mathbb{C})$ the curves $x^2+y^2=z^2$ and $x^2+(y-z)^2=z^2$ intersect at four points $[\sqrt{2}:\sqrt{2}:2]$, $[-\sqrt{2}:\sqrt{2}:2]$, $[1:i:0]$, $[1:-i:0]$, and the curves $x^2+y^2=z^2$ and $x^2+(y-2z)^2=z^2$ intersect at $[0:1:1]$ with multiplicity 2 as well as at $[1:i:0]$ and $[1:-i:0]$ with multiplicity 1.

Theorem 1.1.7 Bezout's Theorem Consider an algebraically closed field k and two homogeneous polynomials $f, g \in k[x,y,z]$ that do not have a common factor. The degrees of f and g are denoted by m and n, respectively. Then the curves $f=0$ and $g=0$ intersect at exactly mn points in $\mathbb{P}^2(k)$ with multiplicity counted.

Now that we have seen some important properties of plane projective curves, we will examine a special kind of plane projective curves of out interest, elliptic curves.

Definition 1.1.8 k-rational Points Let k be an arbitrary field, and let $\overline{k}$ be the algebraic closure of k. Let E be a projective curve defined as $E=\{(x:y:z)\in\mathbb{P}^2(\overline{k}); f(x,y,z)=0\}$ where $f(x,y,z)\in\overline{k}[x,y,z]$ is a polynomial. The k-rational points of E is defined as the set $E(k)=\{(x:y:z)\in\mathbb{P}^2(k); f(x,y,z)=0\}$, which is a subset of E.

Definition 1.1.9 Singular Point Let k be a field, and C and plane projective curve defined over k. C is singular at a point P if $\frac{\partial P}{\partial x}$ and $\frac{\partial P}{\partial y}$ vanish simultaneously.

Definition 1.1.10 Smooth Projective Curve A plane projective curve is smooth if it has no singular point.

Definition 1.1.9 Elliptic Curve Let k be a field. An elliptic curve over k is a smooth plane projective curve of genus 1 with a k-rational distinguished point.

1.2 The Group Law

Theorem 1.2.1 The Abelian Group Structure Consider an elliptic curve E defined over an algebraically closed field. Fix a point O on the curve E as the identity point. Let P be any point on E. If O and P is the same point, then the line OP denotes the tangent line to E on P. The line OP and the curve E intersect at exactly three points with multiplicity counted, where O and P are two of the three intersecting points. Then $-P$ denote the third intersecting point of the line OP and the curve E. Consider any two points A, B on E. If A and B is the same point, then the line OP denotes the tangent line to E on A. The line AB and the curve E intersect at exactly three points with multiplicity counted, where A and B are two of the three intersecting points. Let C denote the third intersecting point of the line AB and the curve E. The commutative binary operation $+$ is defined by $A + B = -C$.

All points on the curve E form an abelian group with the commutative binary operation $+$ defined above, where O is the identity element such that $O + P = P$ for any point P on E and $-P$ is the inverse of P. The operation $+$ is also associative, which means that $(A + B) + C = A + (B + C)$ for any points A, B, C on E.

By the group law, any three points A, B, C on an elliptic curve in the projective plane $\mathbb{P}^2(k)$ satisfy the equation $A + B + C = 0$ if and only if A, B, C are collinear.

Definition 1.2.2 Weierstrass Equation Let k be a field whose characteristic is not 2 or 3. A Weierstrass equation is an equation of the form $y^2z - x^3 - axz^2 - bz^3 = 0$ where $a, b \in k$. The corresponding affine equation in the affine plane $z = 1$ is $y^2 = x^3 + ax + b$.

Proposition 1.2.3 Every smooth cubic in $\mathbb{P}^2(k)$ can be transformed in a change of coordinates to some Weierstrass equation.

The Group Law in Algebraic terms Consider an elliptic curve $E : y^2z - x^3 - axz^2 - bz^3 = 0$ with corresponding affine equation $y^2 = x^3 + ax + b$. Let $A : [x : y : z] = [x_1 : y_1 : 1]$ and $B : [x : y : z] = [x_2 : y_2 : 1]$ be two points on the embedded affine plane. Let the point at infinity $O : [0 : 1 : 0]$ be the identity point on the curve E, which is the only point on E on the line of infinity. Given a point $P : [x : y : z]$ on E, we have $-P : [x : -y : z]$ and $O + P = P$.

Case 1: Suppose $x_1 \neq x_2$. Then $m = \frac{y_1 - y_2}{x_1 - x_2}$ is the slope of the line $\overline{AB}$. Let $y = mx + t$ be the equation of the line $\overline{AB}$. Plugging it into the affine equation $y^2 = x^3 + ax + b$, we get

$$x^3 - m^2x^2 - cx - d = 0$$

for some coefficients c and d. Let $C : [x : y : z] = [x_3 : y_3 : 1]$ be the third point incidents on the elliptic curve E and the line $\overline{PQ}$. Then x_1, x_2, x_3 are the three roots of the polynomial $x^3 - m^2x^2 - cx - d = 0$, and therefore

$$x^3 - m^2x^2 - cx - d = (x - x_1)(x - x_2)(x - x_3).$$

Expanding the right hand side, we get $x_1 + x_2 + x_3 = m^2$. Therefore, we have

$$x_3 = m^2 - x_1 - x_2.$$

Since the slope

$$\frac{y_3 - y_1}{x_3 - x_1} = m,$$

we have

$$y_3 = m(x_3 - x_1) + y_1.$$

According to the simplified group law, we get $A + B = -C = (x_3, -y_3)$, where $m = \frac{y_1 - y_2}{x_1 - x_2}$, $x_3 = m^2 - x_1 - x_2$, and $y_3 = m(x_3 - x_1) + y_1$.

Case 2: Suppose $x_1 = x_2$ and $y_1 = y_2 \neq 0$. Then A and B is the same point, so the line passing through $A = B$ is tangent to the elliptic curve E on the point $A = B$. The corresponding affine equation of the curve $E : y^2z - x^3 - axz^2 - bz^3 = 0$ is $y^2 - x^3 - ax - b = 0$ where $z = 1$ is the affine plane. Through derivative, we obtain $(2y)dy - (3x^2)dx - a = 0$, so the slope

$$m = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}.$$

For the same argument as in Case 1, we get $A + B = -C = (x_3, -y_3)$, where $m = \frac{3x_1^2 + a}{2y_1}$, $x_3 = m^2 - 2x_1$, and $y_3 = m(x_3 - x_1) + y_1$.

Case 3: Suppose $x_1 = x_2$ and $y_1 = -y_2$, including $y_1 = y_2 = 0$. Then the line $\overline{AB}$ is parallel to the y-axis. Since every line parallel to the y-axis passes through the point at infinity $O : [0 : 1 : 0]$, we have $A + B = O$ where O is the identity.

1.3 Isogeny of Elliptic Curves

Definition 1.3.1 Function Field Let k be a field, f a nonconstant homogeneous polynomial from $k[x, y, z]$ that is irreducible in $\overline{k}[x, y, z]$, and C be the plane projective curve defined by f. The function field $k(C)$ is the set of equivalence classes of rational functions g/h such that:

i) g and h are homogeneous polynomials in $k[x, y, z]$ of the same degree.

ii) h is not in the ideal generated by f

iii) g_1/h_1 is equivalent to g_2/h_2 if $g_1h_2 - g_2h_1 \in (f)$

Notice that $k(C)$ is a ring under addition and multiplication of rational functions.

Remark 1.3.2 Let k be a field and C a plane projective curve defined over k. Notice that $k(C)$ denotes the function field, whereas $C(k)$ denotes the k-rational points of C.

Definition 1.3.3 Let k be a field, C a projective curve over k, and $\alpha \in k(C)$. An element $\alpha \in k(C)$ is defined at a point $P \in C(\overline{k})$ if it can be represented as g/h for some $g, h \in k[x, y, z]$ and h does not vanish at P.

Definition 1.3.4 Rational Map Let C_1 and C_2 be plane projective curves defined over a field k. A rational map ϕ: $C_1 \to C_2$ is a projective triple $(\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2(k(C_1))$ such that $\phi_x(P), \phi_y(P), \phi_z(P)$ are defined $\forall P \in C_1(\overline{k})$ and not all zero, and $(\phi_x(P) : \phi_y(P) : \phi_z(P)) \in C_2(\overline{k})$.

Definition 1.3.5 A rational map ϕ is regular or defined at $P \in C_1(\overline{k})$ is there exists a nonzero element $\lambda \in k(C_1)$ such that $\lambda\phi_x$, $\lambda\phi_y$, $\lambda\phi_z$ are all defined at P and do not vanish simultaneously.

Definition 1.3.6 Morphism Between Plane Projective Curves A rational map that is defined everywhere is called a morphism or a regular map.

Theorem 1.3.7 Every rational map from a smooth projective curve to a projective curve is a morphism. [1]

Theorem 1.3.8 A morphism of projective curves is either surjective or constant. [1]

Definition 1.3.9 Isogeny An isogeny ϕ: $E_1 \to E_2$ of elliptic curves defined over k is a non-constant rational map that sends the distinguished point of E_1 to the distinguished point of E_2, which induces a group homomorphism $E_1(\overline{k}) \to E_2(\overline{k})$.

Lemma 1.3.10 Standard Form of Isogeny Let E_1 and E_2 be elliptic curves over k, and let $\alpha : E_1 \to E_2$ be an isogeny. Then α can be defined by an affine rational map of the form

$$\alpha(x, y) = (\frac{u(x)}{v(x)}, y\frac{s(x)}{t(x)})$$

where $u, v, s, t \in k[x]$ with u, v coprime to each other and s, t coprime to each other. The proof of this lemma can be found in lecture 5, page 7 of [1].

Definition 1.3.11 Degree and Separability of Isogenies Let $\alpha(x, y) = (\frac{u(x)}{v(x)}, y\frac{s(x)}{t(x)})$ be an isogeny written in standard form, the degree of α is $deg(\alpha) := max\{deg(u), deg(v)\}$, and α is separable if $\frac{d}{dx}\frac{u(x)}{v(x)} = 0$, and inseparable otherwise.

Examples i) The multiplication-by-2 map: Let E be an elliptic curve over a field k and writtenin short Weistrass form $y^2 = x^3 + Ax + B$. The multiplication-by-2 map is ϕ: $E \to E$ where $P \mapsto 2P = P + P$.

Recall the group law in algebraic terms, we can represent the doubling of the points with the following rational functions

$$\phi_x(x, y) = \frac{(3x^2 + A)^2 - 8xy^2}{4y^2}$$

$$phi_y(x, y) = \frac{12xy^2(3x^2 + A) - (3x^2 + A)^3 - 8y^4}{8y^3}$$

We can find the standard form, which is

$$\alpha(x, y) = (\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}, \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2}{8(x^3 + Ax + B)^2}y)$$

the calculation is omitted, see [1] lecture 5, page 10. The degree of this isogeny is 4, and it is separable.

We can further extend the result to a multiplication-by-n map. The multiplication-by-n

map $\phi : E \to E$ where $P \mapsto nP$ has degree n^2. It is separable if and only if n is not divisible by the chracteristic of the field k, the proof can be found in [1] lecture 6, page 14.

ii) The Frobenius endomorphism: Consider the finite field $\mathbb{F}_p$ where p is a prime. Let E be an elliptic curve over $\mathbb{F}_p$. The Frobenius endomorphism of E is the map $\pi_E : (x : y : z) \mapsto (x^p, y^p, z^p)$.

First let's show that it is a morphism. Consider E in Weistrass form, $y^2z = x^3 + Axz^2 + Bz^3$. Raise both sides to the pth power, we have:

$$(y^2z)^p = (x^3 + Axz^2 + Bz^3)^p$$

$$(y^p)^2z^p = (x^p)^3 + Ax^p(z^p)^2 + B(z^p)^3$$

the calculation is omitted, see [1] lecture 5, page 10. Therefore $(x^p : y^p, z^p) \in E(\overline{\mathbb{F}_p}$, and we have $A^p = A$, $B^p = B$ since $A, Bin\mathbb{F}_p$.

The standard form of the Frobenius endomorphism of an elliptic curve E over a field $\mathbb{F}_p$ is

$$\pi_E(x, y) = (x^p, (x^3 + Ax + B)^{(p-1)/2}y)$$

we can see that the degree p, and it is inseparable since $(x^p)' = px^{p-1} = 0$ in $\mathbb{F}_p$

1.4 The Endomorphism Ring

Definition 1.4.1 Degree of Isogeny Let α be a non-zero isogeny between elliptic curves with a standard affine form $\alpha(x, y) = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y)$. The degree of α is defined as the maximum of the degree of $u(x)$ and the degree of $v(x)$.

For example, if $u(x)$ is a polynomial of degree 2 and $v(x)$ is a polynomial of degree 3, then the degree of α is $\max\{2, 3\} = 3$.

Theorem 1.4.2 Decomposition of Isogeny Let E_1 and E_2 be elliptic curves over an algebraically closed field k of characteristic $p > 0$. Let $\alpha : E_1 \to E_2$ be an isogeny between elliptic curves. Then α can be represented as the composition of some separable isogeny and some power of the p-power Frobenius map defined by $\pi : (x, y, z) \mapsto (x^p, y^p, z^p)$.

Proposition 1.4.3 Let α, β and γ be three isogenies where $\alpha = \beta \circ \gamma$. Then $deg(\alpha) = deg(\beta) \cdot deg(\gamma)$.

Lemma 1.4.4 If α is an isogeny over an algebraically closed field k of characteristic $p > 0$ and $\alpha = \alpha_{sep} \circ \pi^n$ where α_{sep} is a separable isogeny and π is the p-power Frobenius map $\pi : (x, y, z) \mapsto (x^p, y^p, z^p)$, then following from the previous proposition and $deg(\pi) = p$, we have $deg(\alpha) = deg(\alpha_{sep}) \cdot p^n$.

Theorem 1.4.5 The order of the kernel of an isogeny is its separable degree.

This is because the p-power Frobenius map $\pi : (x, y, z) \mapsto (x^p, y^p, z^p)$ has trivial kernel, and the order of the kernel of a separable isogeny is its degree.

Theorem 1.4.6 Let E be an elliptic curve over an algebraically closed field k. Let G be a finite subgroup of $E(k)$. Then there exists a separable isogeny $\phi : E \to E_0$ whose kernel is G, where the elliptic curve E_0 and the separable isogeny ϕ are unique up to isomorphism.

That is, if $\phi_1 : E \to E_1$ and $\phi_2 : E \to E_2$ are separable isogenies with the same kernel, then there exists a group isomorphism $i : E_1 \to E_2$ where $\phi_2 = i \circ \phi_1$.

Definition 1.4.7 n-torsion subgroup Let E be an elliptic curve over an algebraically closed field k. The n-torsion subgroup of E is the kernel of the multiplication-by-n map defined by taking each point P in E to the point nP in E, and it is denoted by $E[n] = \{P \in E : nP = 0\}$.

Lemma 1.4.8 Let E be an elliptic curve over an algebraically closed field k of characteristic $p > 0$. Let $E[n]$ be the n-torsion subgroup of E.

1. If e is a positive integer, then the p^e-torsion subgroup $E(p^e)$ is either trivial or isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$.

2. If ℓ is a prime other than p, then the ℓ^e-torsion subgroup $E(\ell^e)$ is isomorphic to $\mathbb{Z}/\ell^e\mathbb{Z} \oplus \mathbb{Z}/\ell^e\mathbb{Z}$.

Proposition 1.4.9 Let E be an elliptic curve over an algebraically closed field k of characteristic $p > 0$. Then every finite subgroup of $E(k)$ can be written as the direct sum of at most two cyclic groups whose orders are not both divisible by p.

Corollary 1.4.10 If $k = \mathbb{F}_q$ is a finite field of characteristic $p > 0$, then $E(\mathbb{F}_q)$ can be written as the direct sum of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ where m is divisible by n and m is not divisible by p.

Definition 1.4.11 Group of homomorphisms Let E_1 and E_2 be elliptic curves over an algebraically closed field k. The isogenies from E_1 to E_2 form an abelian group $Hom(E_1, E_2)$ with the zero morphism as the identity element.

For any two elements $\alpha, \beta \in Hom(E_1, E_2)$ and any point $P \in E_1$, the addition is defined by $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$.

Proposition 1.4.12 For any integer n, let $[n] : E_1 \to E_2$ denote the multiplication-by-n map in the abelian group $Hom(E_1, E_2)$. Then $[n]$ is in the center of $Hom(E_1, E_2)$.

Definition 1.4.13 Endomorphism ring Let E be an elliptic curve over an algebraically closed field k. All endomorphisms from E to E forms an endomorphism ring $End(E) = Hom(E, E)$.

For any two elements $\alpha, \beta \in End(E)$ and any point $P \in E$, the addition is defined by $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$ and the multiplication is defined by $(\alpha \circ \beta)(P) = \alpha(\beta(P))$.

Matrix representation Let E be an elliptic curve over an algebraically closed field k of characteristic $p > 0$. Let n be some positive integer that is not divisible by p. Followed from Lemma 1.4.8, the n-torsion subgroup $E(n)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Thus there exists two elements P_1 and P_2 from the n-torsion subgroup such that any element in the n-torsion subgroup can be written uniquely as the linear combination of P_1 and P_2. For any endomorphism α from E to E, let α_n denote the restriction of α to the n-torsion subgroup. Since α is a group homomorphism, it maps n-torsion points to n-torsion points, and thus α_n is an endomorphism of $E[n]$. For a fixed basis $< P_1, P_2 >$, the subgroup α_n can be represented as a 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.4.14 Let α be an endomorphism of an elliptic curve E/k and let n be a positive integer prime to the characteristic of k. Then

$$\mathrm{tr}\alpha \equiv \mathrm{tr}\alpha_n \bmod n \quad \text{and} \quad \deg\alpha \equiv \det\alpha_n \bmod n$$

Proof. See [1, Lecture 7, Theorem 7.20] □

Chapter 2

Problem on Probability of ℓ-Torsion

2.1 Preface

Recall that the goal of our project is to determine the probability that a **random** elliptic curve $E/\mathbb{F}_p$ has an $\mathbb{F}_p$-point of prime order ℓ, where p is either a fixed prime much larger than ℓ, or a prime varying over some large interval.

To clarify, a random elliptic curve $E/\mathbb{F}_p$ just means that we choose a random A and B in the finite field $\mathbb{F}_p$ for our curve equation $y^2 = x^3 + Ax + B$. In order to answer the question, we'll establish some important notations and heuristic assumptions that we will refer to throughout the rest of the report:

Notation: Let π be the Frobenius endomorphism of E, and $\pi_\ell \in GL_2(\mathbb{F}_\ell)$ denote the matrix corresponding to the action of the Frobenius endomorphism of E on the ℓ-torsion subgroup $E[\ell]$. See Definition 1.4.1.

Assumption 2.1.1: π_ℓ is uniformly distributed over $GL_2(\mathbb{F}_\ell)$ as E varies over elliptic curves defined over $\mathbb{F}_p$ and p varies over prime integers in some large interval.

Assumption 2.1.2: When varying p over some large interval, every value of $p \bmod \ell$ occurs equally often.

It can be proven that the distribution of π_ℓ converges to the uniform distribution on $GL_2(\mathbb{F}_\ell)$ as $p \to \infty$. [1] Since our problem is more relevant for large prime p, it is an appropriate assumption.

We will divide the problem into three steps...

2.2 Step 1

Our first step is to determine the probability that $E(\mathbb{F}_p)[\ell] = E[\ell]$, both for a fixed p and varying p over some large interval. Recall that the ℓ-torsion subgroup $E[\ell]$ equals $\{P \in E(\overline{\mathbb{F}_p}) : \ell \cdot P = 0\}$, so it consists of the $\mathbb{F}_p$ rational points on E with order dividing ℓ. $E(\mathbb{F}_p)[\ell]$ equals $\{P \in E(\mathbb{F}_p) : \ell \cdot P = 0\}$, the set of $\mathbb{F}_p$ points on E with order ℓ. You can think of $E(\mathbb{F}_p)[\ell]$ as the intersection $E[\ell] \cap E(\mathbb{F}_p)$.

Theorem 2.2.1: $E(\mathbb{F}_p)[\ell] = E[\ell]$ if and only if π fixes $E[\ell]$ and thus the matrix π_ℓ is the identity matrix. [1]

Theorem 2.2.1 implies that to determine the probability that $E(\mathbb{F}_p)[\ell] = E[\ell]$, we can look at the probability that π_ℓ is the identity matrix. We must consider this for fixed and varying p.

For **fixed** p, Theorem 1.4.23 implies that $\det\pi_\ell \equiv \deg\pi \bmod\ell$ since π is an endomorphism of E and ℓ is prime to p. Since $\deg\pi = p$, $\det\pi_\ell \equiv$ p $\bmod\ell$. So, we need to find the number of matrices in $GL_2(\mathbb{F}_\ell)$ that have determinant p $\bmod\ell$. We can write $GL_2(\mathbb{F}_\ell)$ as $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_\ell \text{ and } ad - bc \neq 0\}$

Then we want $ad - bc \equiv p \bmod\ell$:

We can consider two cases, when $a = 0$ and when $a \neq 0$:

Case 1) $a = 0$: When $a = 0$, $bc \equiv p \bmod\ell$. Since (a, b) cannot equal $(0, 0)$, and $a, b, c, d \in \mathbb{F}_\ell$ there are $\ell - 1$ options for b. There exists a unique $c \in \mathbb{F}_\ell$ such that $c = \frac{p}{b}$

modℓ, and thus there is 1 option for c. Since $a = 0$, d can be any number, so there are ℓ options for d. Therefore, there are a total of $\ell(\ell - 1)$ possibilities.

Case 2) $a \neq 0$: When $a \neq 0$, there are $\ell - 1$ options for a, and thus ℓ options for b. In order for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to be invertible, (c, d) must be linearly independent to (a, b), but since $a \neq 0$, there are ℓ options for c. There exists a unique $d \in \mathbb{F}_\ell$ such that $ad \equiv (p + bc)$ modℓ, namely $d = \frac{p+bc}{a} \in \mathbb{F}_\ell$, and thus there is 1 option for d. Therefore, there are a total of $\ell^2(\ell - 1)$ possibilities.

So all together, there are $\ell(\ell - 1) + \ell^2(\ell - 1) = (\ell - 1)(\ell^2 + l) = \ell(\ell^2 - 1)$ possibilities, and thus the probability

$$Pr_{fixed}(E(\mathbb{F}_p)[\ell] = E[\ell]) \text{ is equal to } \tfrac{1}{\ell(\ell^2-1)}.$$

For a p **varying** over some large interval, we can consider any matrix in $GL_2(\mathbb{F}_\ell)$, since we assumed every value of p modℓ occurs equally often. Again, we'll write $GL_2(\mathbb{F}_\ell)$ as $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_\ell \text{ and } ad - bc \neq 0\}$. There are ℓ^2 possible values (a, b), but in order for the matrix to be invertible (a, b) cannot equal $(0, 0)$. Thus there are $\ell^2 - 1$ options. Then (c, d) can be anything except for a scalar multiple of (a, b), so we have $\ell^2 - \ell$ options since there are ℓ possible scalar multiples of (a, b). Therefore there are $(\ell^2 - 1)(\ell^2 - \ell)$ matrices in $GL_2(\mathbb{F}_\ell)$, and the probability that π_ℓ is the identity is $\frac{1}{(\ell^2-1)(\ell^2-\ell)}$.

We use Sage to compute the probability when ℓ is bounded by 50, 100, 200, 500 with the following code, where p is the probability, and m is set to be the bound:

```
p=1.0
m = 50
P=prime_range(0,m)

for l in P:
```

```
    p = p*((l*(l**2-1)-1)/(l*(l**2 -1)))
print(p)
```

which returns:

```
for m = 50, probability = 0.788194911989887
for m = 100, probability = 0.788170493994749
for m = 200, probability = 0.788164003202117
for m = 500, probability = 0.788162725606979
```

2.3 Step 2

Our second step is proving the following lemma, which is essential to determining the probability of ℓ-torsion.

Lemma 2.3.1: A necessary and sufficient condition for $E(\mathbb{F}_p)[\ell] \neq \{0\}$ is

$$\mathrm{tr}\pi_\ell \equiv \det\pi_\ell + 1 \ (\mathrm{mod}\ell).$$

In order to prove this lemma, we will use the following theorems:

Theorem 2.3.2 Let E/k be an elliptic curve. Every finite subgroup of $E(\overline{k})$ can be written as the direct sum of at most two cyclic subgroups, at most one of which has order divisble by the characteristic k. In particular, when $k = \mathbb{F}_q$ is a finite field of characteristic p we have

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

for some positive integers m, n with $m|n$ and $p \nmid m$.

Proof. See [1, Lecture 7, Corollary 7.4] □

Hasse's Theorem: Let $E/\mathbb{F}_q$ be an elliptic curve over a finite field. Then

$$\#E(\mathbb{F}_q) = q + 1 - \mathrm{tr}\pi.$$

Proof. See [1, Lecture 8, Theorem 8.3] □

Now we will prove Lemma 2.3.1.

Proof. Recall $E(\mathbb{F}_p)[\ell] = \{P \in E(\mathbb{F}_p) : \ell P = 0\}$.

The multiplication-by-ℓ map $[\ell]$ acts on $E(\mathbb{F}_p)$ as follows:

$$[\ell] : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$$
$$(x, y) \mapsto (\ell x, \ell y)$$

Thus, $E(\mathbb{F}_p)[\ell] = \{(x, y) \in E(\mathbb{F}_p) : (\ell x, \ell y) = 0\}$

By Theorem 2.3.2, $E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, where $m|n$, $p \nmid m$. In order for $E(\mathbb{F}_p)[\ell] \neq \{0\}$ to hold, we need some $(x, y) \neq (0, 0) \in E(\mathbb{F}_p)[\ell]$.

Since ℓ is prime, there exists a non-zero $(x, y) \in E(\mathbb{F}_p)[\ell]$ if and only if either x or y is non-zero and has order ℓ, which is true if and only if $\ell|m$ or $\ell|n$. This is in turn equivalent to $\ell|m \cdot n$.

Since $E(\mathbb{F}_p)$ is a direct sum, $\#E(\mathbb{F}_p) = m \cdot n$.

By Hasse's Theorem,

$$\#E(\mathbb{F}_p) = p + 1 - tr\pi$$

So $\ell|m \cdot n \iff l|(p + 1 - tr\pi) \iff tr\pi \equiv p + 1 \pmod{\ell}$

By Theorem 1.4.23, $tr\pi_\ell \equiv tr\pi \bmod \ell$ and $det\pi_\ell \equiv deg\pi \equiv p \bmod \ell$, so

$tr\pi \equiv p + 1 \pmod{\ell} \iff tr\pi_\ell \equiv deg\pi + 1 \pmod{\ell} \iff tr\pi_\ell \equiv det\pi_\ell + 1 \pmod{\ell}$

□

2.4 Step 3

Our third and final step is to determine the probability that $E(\mathbb{F}_p)$ contains a point of order ℓ (i.e. $E(\mathbb{F}_p)[\ell] \neq \{0\}$). To do this, we will:

- Derive a **combinatorial formula** for this probability as a rational function in ℓ, and

- Create a **Sage script** to verify our formula.

To derive a combinatorial formula for the probability that $E(\mathbb{F}_p)$ contains a point of order ℓ, we need to count the matrices π_ℓ in $GL_2(\mathbb{F}_\ell)$ such that Lemma 2.3.1 is satisfied, i.e.

$$\#\pi_\ell \text{ such that } \mathrm{tr}\pi_\ell \equiv \det\pi_\ell + 1 \ (\mathrm{mod}\ell)$$

Again, we have to consider this condition for a **fixed** value of p and p **varying** over a large interval.

For a fixed p, we need to consider two cases: when $p \equiv 1 \ \mathrm{mod}\ell$ and when $p \not\equiv 1 \ \mathrm{mod}\ell$.

Case 1: For $p \equiv 1 \ \mathrm{mod}\ell$, since $\det\pi_\ell \equiv p \mathrm{mod}\ell$, we want $\det\pi_\ell = ad - bc \equiv 1 \ \mathrm{mod}\ell$, and we want $\mathrm{tr}\pi_\ell = a + d \equiv 2 \ \mathrm{mod}\ \ell$. We can consider three sub cases. When $a, c \neq 0$, there are $\ell - 1$ options for a, and d depends on a since $a + d = 2$, so that leaves 1 option for d. $c \neq 0$ implies that there are $\ell - 1$ options for c, and since $bc \equiv ad - 1 \ \mathrm{mod}\ell$, there is a unique value for b, so 1 option. Thus when $a, c \neq 0$, we have $(\ell - 1)^2$ possibilities.

If $a = 0$ and $c \neq 0$, we must have $d = 2$. Since $c \neq 0$ there are $\ell - 1$ options for c, and given $-bc \equiv 1 \ \mathrm{mod}\ell$, one unique value left for b. So, when $a = 0$ and $c \neq 0$, we have $\ell - 1$ options.

When $a \neq 0$ and $c = 0$, there are ℓ options for b. We have $ad \equiv 1 \ \mathrm{mod}\ell$, and since $a + d = 2$, then $(2 - d)(d) \equiv 1 \ \mathrm{mod}\ell \implies d^2 - 2d + 1 \equiv 0 \ \mathrm{mod}\ell \implies (d - 1)(d - 1) \equiv 0$ $\mathrm{mod}\ell$. This implies that $d = 1$, and thus $a = 1$. So when $a \neq 0$ and $c = 0$, we have ℓ options. If we add these all together, we get $\ell + (\ell - 1) + (\ell - 1)^2 = \ell^2$ possibilities. From Step 1, we know that there are $\ell(\ell^2 - 1)$ matrices in $GL_2(\mathbb{F}_\ell)$ with determinant $p \ \mathrm{mod}\ell$. Thus the probability

$$Pr_{fixed\ p \equiv 1}(E(\mathbb{F}_p)[\ell] \neq \{0\}) = \frac{\ell^2}{\ell(\ell^2-1)} = \frac{\ell}{\ell^2-1}$$

Case 2: For $p \not\equiv 1 \ \mathrm{mod}\ell$, we get a similar answer. For our first two cases, $a, c \neq 0$ and $a = 0$ and $c \neq 0$, the same argument holds.

However, when $a \neq 0$ and $c = 0$, we want to solve the set of equations in $\mathbb{F}_\ell$

$$ad = p \text{ and}$$

$$a + d = p + 1$$

This implies $(p+1-d)(d) = p$. Rewriting this gives $d^2-(p+1)(d)+p = (d-1)(d-p) = 0$. The roots are $d = 1$ and $d = p$, so if $p \equiv 1 \bmod \ell$ there is one root, otherwise there are two roots. There are ℓ options for b, and thus when $p \not\equiv 1 \bmod \ell$ there are 2ℓ options. Adding together all our options, we get $2\ell + (\ell - 1) + (\ell - 1)^2 = \ell^2 + \ell$, and thus the probability

$$Pr_{fixed\ p\not\equiv 1}(E(\mathbb{F}_p)[\ell] \neq \{0\}) = \frac{\ell^2+\ell}{\ell(\ell^2-1)} = \frac{1}{\ell-1}$$

For varying p, we use the probabilities we just found for fixed p and incorporate the probabilities of the occurrence of each $p \bmod \ell$. We assumed each value of $p \bmod \ell$ occurs equally often, so the probability that $p \equiv 1 \bmod \ell$ is

$$Pr(p \equiv 1) = \frac{1}{\ell-1}$$

And the probability that $p \not\equiv 1 \bmod \ell$ is

$$Pr(p \not\equiv 1) = \frac{\ell-2}{\ell-1}$$

Therefore our total probability of ℓ-torsion for varying p is

$$\Pr(\ell\text{-torsion}) = \frac{\ell}{\ell^2-1} * (\frac{1}{\ell-1}) + \frac{1}{\ell-1} * (\frac{\ell-2}{\ell-1}) = \frac{\ell^2-2}{\ell^3-\ell^2-\ell+1}$$

In order to test this formula, we wrote a Sage script that counted the number of matrices π_ℓ in $GL_2(\mathbb{F}_\ell)$ such that Lemma 2.3.1 is satisfied, i.e.

$$\#\pi_\ell \text{ such that } \mathrm{tr}\pi_\ell \equiv \det\pi_\ell + 1 \pmod{\ell}.$$

With the following implementation, we can compute our results:

```
l = 3
k = GL(2,GF(l))
lst = []
for i in k:
    lst.append(i)
```

```
len = len(lst)

varyingp = 0
for j in range(1,l):
    cnt = 0.0
    total = 0
    for i in k:
        A = matrix(i)
        d = A.determinant()
        t = A.trace()
        if d == j :
            total += 1
            if t == j+1:
                cnt += 1
    prob = cnt/total
    print("For p =" + str(j) + mod l", cnt =" + str(cnt) + ", total =" +
   str(total))
    print("prob = "+ str(prob))
    varyingp += cnt

prob2 = varyingp/len
print("For varying p, probability of " + str(l) + "-torsion is " + str(
   prob2))
```

which returns

```
For p =1 mod l, cnt =9.00000000000000, total =24
prob = 0.375000000000000
For p =2 mod l, cnt =12.0000000000000, total =24
prob = 0.500000000000000
For varying p, probability of 3-torsion is 0.437500000000000
```

We can set m = 5, which returns:

```
For p =1 mod l, cnt =25.0000000000000, total =120
```

```
prob = 0.208333333333333
For p =2 mod l, cnt =30.0000000000000, total =120
prob = 0.250000000000000
For p =3 mod l, cnt =30.0000000000000, total =120
prob = 0.250000000000000
For p =4 mod l, cnt =30.0000000000000, total =120
prob = 0.250000000000000
For varying p, probability of 5-torsion is 0.239583333333333
```

and for m = 7,

```
For p =1 mod l, cnt =49.0000000000000, total =336
prob = 0.145833333333333
For p =2 mod l, cnt =56.0000000000000, total =336
prob = 0.166666666666667
For p =3 mod l, cnt =56.0000000000000, total =336
prob = 0.166666666666667
For p =4 mod l, cnt =56.0000000000000, total =336
prob = 0.166666666666667
For p =5 mod l, cnt =56.0000000000000, total =336
prob = 0.166666666666667
For p =6 mod l, cnt =56.0000000000000, total =336
prob = 0.166666666666667
For varying p, probability of 7-torsion is 0.163194444444444
```

Here are the formula results:

$f(\ell) = \frac{\ell^2-2}{\ell^3-\ell^2-\ell+1}$

$f(3) = \frac{7}{16}$

$f(5) = \frac{23}{96}$

$f(7) = \frac{47}{288}$

This shows that our formulas were correct. Therefore, the probability that $E(\mathbb{F}_p)$ contains a point of order ℓ for a **fixed** prime p is

$$Pr_{fixed}(E(\mathbb{F}_p)[\ell] \neq \{0\}) = \begin{cases} \frac{\ell}{\ell^2-1} & \text{if } p \equiv 1 \bmod \ell \\ \frac{1}{\ell-1} & \text{if } p \not\equiv 1 \bmod \ell \end{cases}$$

And the probability that $E(\mathbb{F}_p)$ contains a point of order ℓ for a **varying** prime p over a large interval is

$$Pr_{varying}(E(\mathbb{F}_p)[\ell] \neq \{0\}) = \frac{\ell^2-2}{\ell^3-\ell^2-\ell+1}$$

2.5 Step 4

Now to validate our formula from the previous step, we will pick two random primes p_1, p_2 from the range $[2^{29}, 2^{30}]$, with $p_1 \equiv 1 \bmod \ell$ and $p_2 \not\equiv 1 \bmod \ell$. We next randomly generate 1000 elliptic curves over $\mathbb{F}_{p_1}$ and $\mathbb{F}_{p_2}$, and count how often the number of $\mathbb{F}_{p_i}$-rational points is divisible by ℓ for $i = 1, 2$

```
ell=3
p1=0;p2=1
while p1%ell !=1:
    p1=random_prime(2^30,True,2^29)
while p2%ell ==1:
    p2=random_prime(2^30,True,2^29)
print (p1,p2)

F1=GF(p1)
num1=0
for j in range(1,1000):
    aa=F1.random_element(); bb=F1.random_element()
    if (EllipticCurve([aa,bb]).order())%ell == 0:
        num1=num1+1
F2=GF(p2)
num2=0
```

```
for j in range(1,1000):
    aa=F2.random_element(); bb=F2.random_element()
    if (EllipticCurve([aa,bb]).order())%ell == 0:
        num2=num2+1
print ("the experimental probability when p1="+str(p1)+", l="+str(ell)+",
   with p1 mod l  =1 is "
       + str(num1/1000.0)+ "\n"+
       "the experimental probability when p2="+str(p2)+", l="+str(ell)+",
   with p2 mod l !=1 is "
       + str(num2/1000.0)
      )
```

for $\ell = 3$, we have

```
p1 = 754748737 p2 = 868213487
the experimental probability when p1=754748737, l=3, with p1 mod l  =1 is
   0.359000000000000
the experimental probability when p2=868213487, l=3, with p2 mod l !=1 is
   0.499000000000000
```

for $\ell = 5$, we have

```
p1 = 637617971 p2 = 623986247
the experimental probability when p1=637617971, l=5, with p1 mod l  =1 is
   0.189000000000000
the experimental probability when p2=623986247, l=5, with p2 mod l !=1 is
   0.248000000000000
```

for $\ell = 7$, we have

```
p1 = 603220031 p2 = 950453551
the experimental probability when p1=603220031, l=7, with p1 mod l  =1 is
   0.152000000000000
the experimental probability when p2=950453551, l=7, with p2 mod l !=1 is
   0.165000000000000
```

Since the primes and the elliptic curves were randomly generated, each execution might

return slightly different value, but we can see that it is fairly close to our prediction from previous step. Therefore the formulas we derived are appropriate under our heuristic assumptions.

Bibliography

[1] Andrew Sutherland, *18.783 Elliptic Curves* , MITOpenCourseWare, 2019.