# Elliptic Curves and the Probability of Prime Torsion

Zoe Daunt

Northeastern University

Saturday, January 23rd, 2021

# NCUWM: Brought to you by Elliptic Curves

Zoe Daunt

Northeastern University

Saturday, January 23rd, 2021

# Projective Spaces

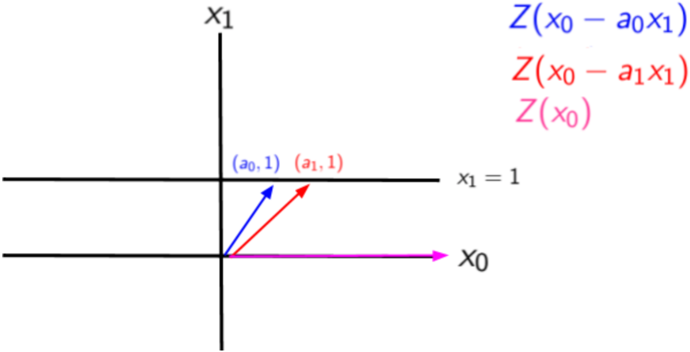
Let $k$ be an algebraically closed field.

**Definition:** For $n \in \mathbb{Z}, \geq 0$, we define projective n-space as the quotient of $k^{n+1} - \{0\}$ by the equivalence relation $\sim$ , where $a \sim b \iff \exists \lambda \in k^x$ such that $b = \lambda a$
**Notation:** Let $q : k^{n+1} - \{0\} \to \mathbb{P}^n$ be the quotient map which takes $(a_0, ..., a_n)$ in $k^{n+1} - \{0\}$ to $(a_0 : ... : a_n)$

**Examples:**
i. $\mathbb{P}^0 = (k^1 - \{0\})/ \sim = \{(1)\}$, a 1-point set
ii. $\mathbb{P}^1 = \{(a_0, a_1) \in k^2 : (a_0, a_1) \neq (0, 0)\}/ \sim = \{(a : 1) : a \in k\} \sqcup \{(1 : 0)\} = \mathbb{A}^1 \sqcup \{\infty\}$
iii. $\mathbb{P}^n = \{(a_0 : ... : a_{n-1} : 1) : a_0, ..., a_{n-1} \in k\} \sqcup \{(a_0 : ... : a_{n-1} : 0) : 0 \neq (a_0, ..., a_{n-1} \in k^n\} = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$

# Projective Spaces

$$\mathbb{P}^1 = \{(a:1) : a \in k\} \sqcup \{(1:0)\} = \mathbb{A}^1 \sqcup \{\infty\}$$




$$\mathbb{P}^1 = \mathbb{A}^1 \sqcup \{\infty\}$$

# Projective Space

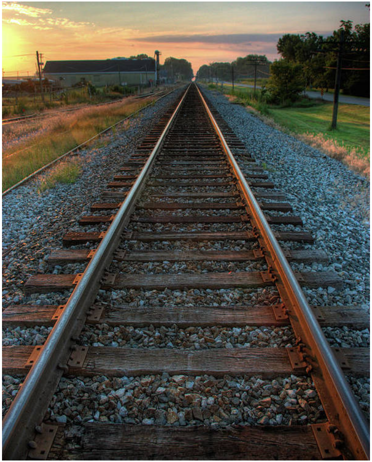
The **Projective Plane** is the set of triples $[a_0, a_1, a_2]$ with $a_0, a_1, a_2$ not all zero with the following equivalence relation $\sim$:

$$[a_0, a_1, a_2] \sim [a_0', a_1', a_2'] \text{ if } a_0 = \lambda a_0', a_1 = \lambda a_1', a_2 = \lambda a_2' \text{ for some } \lambda \neq 0.$$

| Algebraic definition of $\mathbb{P}^2$ | | Geometric definition of $\mathbb{P}^2$ |
|---|---|---|
| $\frac{\{[a_0,a_1,a_2]:a_0,a_1,a_2 \ \ not \ \ all \ \ zero\}}{\sim}$ | $\leftrightarrow$ | $\mathbb{A}^2 \cup \mathbb{P}^1$ |
| $[a_0, a_1, a_2]$ | $\rightarrow$ | $\begin{cases} (\frac{a_0}{a_2}, \frac{a_1}{a_2}) \in \mathbb{A}^2 & if \ \ a_2 \neq 0 \\ [a_0, a_1] \in \mathbb{P}^1 & if \ \ a_2 = 0 \end{cases}$ |
| [x,y,1] | $\leftarrow$ | (x,y) $\in \mathbb{A}^2$ |
| $[A, B, 0]$ | $\leftarrow$ | $[A, B] \in \mathbb{P}^1$ |

Joseph H. Silverman, John T. Tate, *Rational Points on Elliptic Curves*, Springer, 2015.

# Projective Spaces



$\mathbb{P}^2 = \mathbb{A}^2 \sqcup \mathbb{P}^1$, which is our line at $\infty$

# Plane Cubics and Elliptic Curves

A **cubic plane curve** in the projective plane $\mathbb{P}^2(k)$ is defined by the set of solutions to the following equation

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

where a, b, c,..., i, and j $\in k$

An **elliptic curve E** has the form

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

An elliptic curve is a smooth projective curve of genus 1 with a distinguished point.

# Elliptic Curves

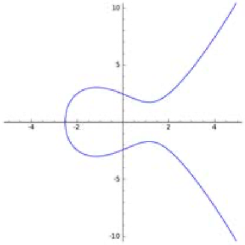
If a curve $E$ is of the form

$$E : F(x, y) = 0$$

It's **rational points** are denoted by

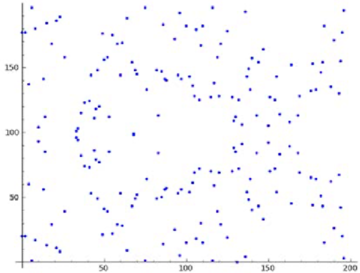
$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \text{ and } F(x, y) = 0\}$$

# Examples




$$y^2 = x^3 - 4x + 6$$

over $\mathbb{R}$

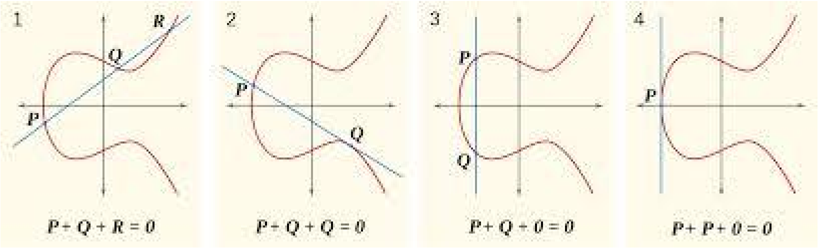



$$y^2 = x^3 - 4x + 6$$

over $\mathbb{F}_{197}$

From Bezout's theorem, every line in the projective plane intersects an elliptic curve in three points, counting multiplicity.

# Group Law on Elliptic Curves




- Identity: the point $(0 : 1 : 0)$ at infinity
- Inverse: the inverse of point $P = (x : y : z)$ is the point $-P = (x : -y : z)$
- Commutativity: $A + B = B + A$
- Associativity: $A + (B + C) = (A + B) + C$

# Isogenies

An isogeny $\phi : E_1 \to E_2$ 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 $E_2$.

# Examples

1. The negation map $\phi_1$: P $\rightarrow$ -P, where (x : y : z) $\mapsto$ (x : -y : z)

2. **The multiplication-by-n map,**

$$\begin{aligned}[n] : E &\rightarrow E \\ P &\mapsto n \cdot P\end{aligned}$$

3. The frobenius endomorphism: Let $\mathbb{F}_p$ be a finite field of prime order p, the Frobenius endomorphism $\pi : \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ is the map x $\mapsto$ $x^p$

# Structure of Torsion Subgroups

Let $E/k$ be an elliptic curve of characteristic $p > 0$, $p$ prime.

$E[n]$ is the $n$-torsion subgroup of $E$ consisting of all points $P$ in $E(\overline{k})$ such that $nP = 0$, i.e. the kernel of $[n]$.

$$E[n] = \{P \in E(\overline{k}) : nP = 0\}$$

$E(k)[n] = \{P \in E(k) : nP = 0\}$

# Probability of $\ell$-torsion

**Goal:** Determine the probability that a random elliptic curve $E/\mathbb{F}_p$ has an $\mathbb{F}_p$ point of prime order $\ell$, where $p$ is either a fixed prime much larger than $\ell$, or a prime varying over some large interval.

# Probability of $\ell$-torsion

**Goal:** Determine the probability that a **random** elliptic curve $E/\mathbb{F}_p$ has an $\mathbb{F}_p$ **point** of prime order $\ell$, where $p$ is either a fixed prime much larger than $\ell$, or a prime varying over some large interval.

- "Random Elliptic Curve $E/\mathbb{F}_p$": Random A and B for $y^2 = x^3 + Ax + B$

- An $\mathbb{F}_p$-point is a point on $E/\mathbb{F}_p$ with coordinates in $\mathbb{F}_p$
- An $\mathbb{F}_p$ point, say $P$, of order $\ell$ is an $\ell$-torsion point ($\ell \cdot P = 0$) with coordinates in $\mathbb{F}_p$.

# Probability of $\ell$-torsion: STEP 3

For a fixed $p$, we need to consider two cases: when $p \equiv 1 \bmod \ell$ and when $p \not\equiv 1 \bmod \ell$. From part a, we know that there are $\ell(\ell^2 - 1)$ matrices in $GL_2(\mathbb{F}_\ell)$ with determinant $p \bmod \ell$.
For $p \equiv 1 \bmod \ell$, There are $\ell^2$ possibilities, and thus

$$Pr_{fixed \equiv 1} = \frac{\ell^2}{\ell(\ell^2-1)}$$

For $p \not\equiv 1 \bmod \ell$, There are $\ell^2 + \ell$ possibilities, and thus

$$Pr_{fixed \not\equiv 1} = \frac{\ell^2+l}{\ell(\ell^2-1)}$$

# Probability of $\ell$-torsion: STEP 3

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

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

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

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

Therefore our total probability of $\ell$-torsion for varying $p$ is

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

# Probability of $\ell$-torsion: STEP 3

## Combinatorial Formula

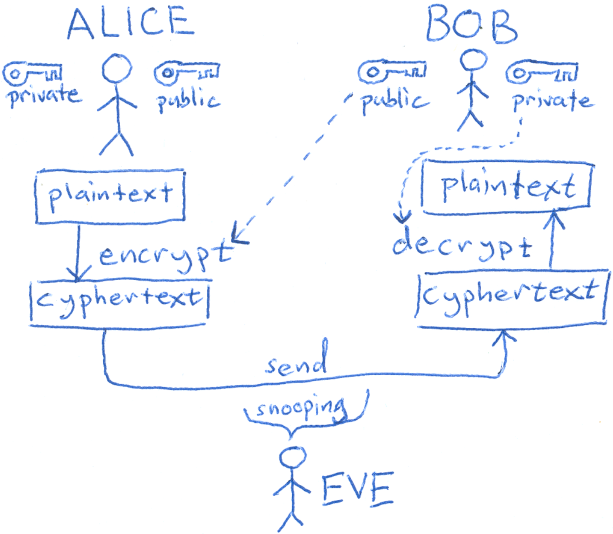
$$f(\ell) = \frac{\ell^2}{\ell(\ell^2-1)} * \left(\frac{1}{\ell-1}\right) + \frac{\ell^2+l}{\ell(\ell^2-1)} * \left(\frac{\ell-2}{\ell-1}\right) = \frac{\ell^2-2}{\ell^3-\ell^2-\ell+1}$$

$$f(3) = \frac{7}{16}$$
$$f(5) = \frac{23}{96}$$
$$f(7) = \frac{47}{288}$$

## Sage Script

```
For varying p, probability of 3-torsion is 7/16
For varying p, probability of 5-torsion is 23/96
For varying p, probability of 7-torsion is 47/288
```

# Public Key Cryptography



*****Public Key Cryptography*****

**The Discrete Logarithm Problem:** Let $G$ be a group and let $g \in G$ be an element of finite order $n$. Given a power $h$ of $g$, the discrete logarithm problem is to find an exponent $x \in \mathbb{Z}/(n)$ with $g^x = h$.

# Probability of $\ell$-torsion: Applications

**The Elliptic Curve Discrete Logarithm Problem:** Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Given $P, Q \in E(\mathbb{F}_p)$, find an integer $x$ such that $xP = Q$.

# Probability of $\ell$-torsion: Applications