Points on Elliptic Curves

Jessica He, Annie Wang, Max Xu

Mentor: Konstantin Jakob

December, 2021

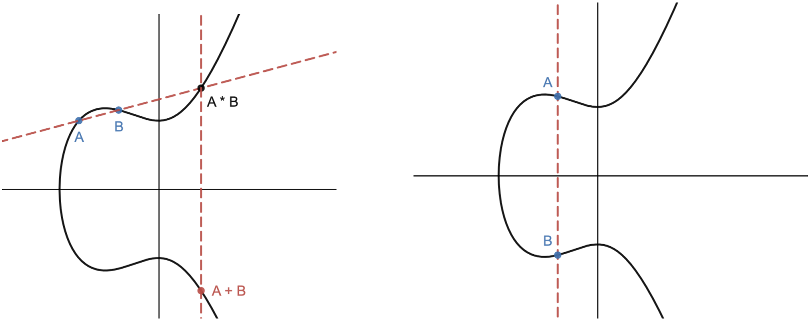
Motivation and Definition

- Looking at the solutions to equations over different fields
- Looking at the structure of the above solutions
- Lines and Conics are polynomials of degree 1 and 2 in two variables
- Advancing to cubics in two variables

Definition (Elliptic Curve)

An elliptic curve is a curve that is isomorphic to a curve of the form $y^2 = p(x)$, where $p(x)$ is a polynomial of degree 3 with nonzero discriminant.

Illustration of the Group Law



Explicit Rules for the Group Law

Given an elliptic curve $y^2 = x^3 + ax^2 + bx + c$, we can define the group law between two points $(x_1, y_1), (x_2, y_2)$ explicitly with

$$x_3 = \lambda^2 - a - x_1 - x_2$$
$$y_3 = \lambda x_3 + v$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$v = y_1 - \lambda x_1$$

Defining the Group Law

How do the points on an elliptic curve using the group law satisfy the group axioms?

Group Axioms

1. Closure
2. Identity - Point $\mathcal{O}$ at infinity
3. Inverses
4. Associativity

This group is also abelian since the group composition is commutative.

Points of Finite vs. Infinite Order

We want to explore the group of torsion points on elliptic curves. Take an elliptic curve C.

Definition (Order of a Point)

A point P on C has order m if $mP = \underbrace{P + \ldots + P}_{\text{m times}} = \mathcal{O}$ but $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$.

Definition (Finite and Infinite Order)

When such an m exists as above, then P has finite order. Otherwise, P has infinite order.

Note: By definition, $\mathcal{O}$ is a point of finite order.

Example for Points of Finite Order

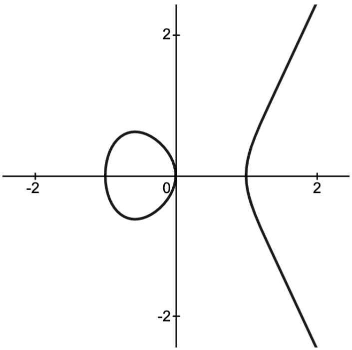
Proposition (Points of Order Two)

Take a point $P = (x, y) \neq \mathcal{O}$ *on* C*. Then* P *has order* 2 *if and only if* $y = 0$.

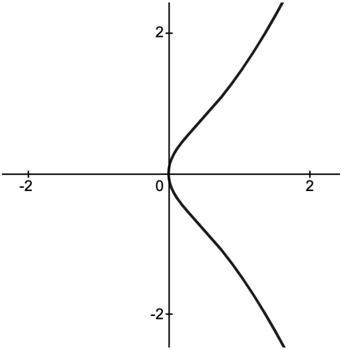
Proof.

The points of order 2, or 2−torsion points, are given by $2P = \mathcal{O}$. Rewriting gives $P = -P$, or $(x, y) = (x, -y)$. This implies that $y = 0$, so the x−coordinates of the 2−torsion points are the complex roots of the cubic $f(x)$. □

An Illustration



$y^2 = x^3 - x$



$y^2 = x^3 + x$

The Statement of the Nagell-Lutz Theorem

Take an elliptic curve $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ with integers a, b, c. The discriminant of the cubic is

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

When we factor $f(x)$ over the complex numbers to get

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

we can find the discriminant to be

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

Theorem (Nagell-Lutz Theorem)

Let $P = (x, y)$ be a rational point of finite order. Then, x and y are integers and either $y = 0$ (in which P has order 2) or y divides D.

Applying the Nagell-Lutz Theorem

Example

$$C : y^2 = x^3 - x^2 + x$$

The only rational points of finite order are $(0,0), (1,1)$, and $(1,-1)$.

Let a point of finite order on C be (x, y). By the Nagell-Lutz Theorem, either $y = 0$ or $y | D = -3$. Thus, the only possibilities are $y = 0, \pm 1, \pm 3$:

1. For $y = 0$: $(0,0)$ is the only rational point of order 2.
2. For $y = \pm 1$: we have the solutions $(1,1)$ and $(1,-1)$.
3. For $y = \pm 3$: there are no rational solutions.

Because the converse of the Nagell-Lutz Theorem is not true, we check that $P_1 = (1,1)$ and $P_2 = (1,-1)$ actually have finite order: they have order 4.

An Introduction to the Mordell's Theorem

Theorem (Group of Rational Points)

Let the set of rational points on an elliptic curve C be $C(\mathbb{Q})$. Then, $C(\mathbb{Q})$ forms a group.

Theorem (Mordell's Theorem)

Let the group of rational points on an elliptic curve C be $C(\mathbb{Q})$. Then $C(\mathbb{Q})$ is finitely generated.

Finitely generated simply means that there is some **finite** set of points $S \subset C(\mathbb{Q})$ such that every point in $C(\mathbb{Q})$ can be written as an integer combination of these points.

An Outline of the Proof

We begin by defining the notion of the height of both a rational number and a point.

Definition

Define the height, $H(x)$, of a rational number $x = \frac{a}{b}$, written in simplest form, as:

$$H(x) = \max(|a|, |b|).$$

Further define $h(x) = \log(H(x))$, and for a point $P = (x, y)$, define $H(P) = H(x)$ and $h(P) = h(x)$.

An Outline of the Proof

Lemma 1

The set $\{P \in C(\mathbb{Q}) : h(P) \leq M\}$ is finite for all positive real M.

Lemma 2

Let $P_0 \in C(\mathbb{Q})$ be fixed. Then, there exists a constant κ_0, depending on only P_0 and C, such that for any $P \in C(\mathbb{Q})$, $h(P + P_0) \leq 2h(P) + \kappa_0$.

Lemma 3

There exists a constant κ, depending only on C, such that for any $P \in C(\mathbb{Q})$, $h(2P) \geq 4h(P) + \kappa$.

Lemma 4

The subgroup of $C(\mathbb{Q})$, $2C(\mathbb{Q})$, has finite index in $C(\mathbb{Q})$.

The argument from here is a descent argument.

Over Finite Fields?

Given an elliptic curve $C : F(x, y) = 0$, what do they look like over finite fields?

Example

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

Solutions: $C(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}$

1. $C(\mathbb{F}_p)$ is a group.
2. This group structure is a cyclic group of order 9 (i.e. generator could be $(0, 1)$)

Rational Points on an Elliptic Curve over Finite Fields

If we simply substitute x, for each $f(x) \in \mathbb{F}_p$, there is on average one corresponding y value that works.

Theorem (Hasse Theorem)

If C is an elliptic curve defined over a finite field $\mathbb{F}_p$, then the number of points on C with coordinates in $\mathbb{F}_p$ is equal to $p + 1 - \epsilon$, where the "error term" ϵ satisfies $|\epsilon| \leq 2\sqrt{p}$.

Elliptic Curve Cryptography

Discrete Logarithm Problem

Let p be a prime, and let a and b be non-zero numbers modulo p. Then, find an integer m that solves the following congruence:

$$a^m \equiv b \text{ (mod p)}$$

Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given P, Q $\in C(\mathbb{F}_p)$ for some elliptic curve C,

$$mP = Q$$

Applications of the DLP: Elgamal Cryptosystem

Elgamal Cryptosystem

A group G and an element $g \in G$ is chosen publicly.

- Alice picks a privately, calculates $A = g^a$, then announces A publicly.
- Bob picks $m \in G$ to send and random integer k. He calculates $c_1 = g^k$ and $c_2 = mA^k$, then sends to Alice.
- Alice computes $c_2 c_1^{-a} = mA^k (g^k)^{-a} = mg^{am} g^{-am} = m$

Bob calculates A^b, Alice calculates B^a, both getting $k = g^{ab}$.

If someone can solve the DLP for a, they can calculate m.

Acknowledgements

A huge thank you to

- Our mentor Konstantin Jakob
- The PRIMES program
- Dr. Pavel Etingof, Dr. Slava Gerovitch, and Dr. Tanya Khovanova
- Our families
- Silverman and Tate