A Premise to the Elliptic Curve Primality Test

Runbao (Frank) Du

University of Chicago

Directed Reading Program
January 15, 2026

Note

This presentation is an overview of elliptic curve and its fundamental properties. This presentation serves as a meaningful transition to the morphism of curves, the degree of a morphism, Hasse's Theorem, and eventually Goldwasser-Kilian with its algorithm.

Presentation Overview

Affine Variety

Affine n-space

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{p = (x_1, \ldots, x_n) \mid x_i \in \bar{k}\}$$

Set of K-rational points in A^n

$$\mathbb{A}^n(k) = \{p = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_i \in k\}$$

Affine Algebraic Set and Ideal

$$V_I = \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all f} \in I\}$$
$$I(V) = \{f \in \bar{k}[x] \mid f(p) = 0 \text{ for all } p \in V\}.$$

1. $\bar{k}[x]$: $\bar{k}[x_1, \ldots, x_n]$

Affine Variety

An affine algebraic set V such that $I(V)$ is a prime ideal in $\bar{k}[x]$

Hilbert's Nullstellensatz for Affine Algebraic Sets

(a) For any algebraic set $X \subset \mathbb{A}^n$, we have

$$V(I(X)) = X.$$

(b) For any ideal $J \subset \bar{k}[x]$, we have

$$I(V(J)) = \sqrt{J}.$$

$$\{\text{algebraic sets in } \mathbb{A}^n\} \longleftrightarrow \{\text{radical ideals in } k[x_1, \ldots, x_n]\}$$

Projective Variety

Projective n-space

$$\mathbb{P}^n(k) := \{[x_0, \ldots, x_n] \mid (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}, \text{ not all } x_i = 0\}$$

- $[x_0 : \cdots : x_n]$ denotes an equivalence class under $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in \bar{k}^*$ such that $x_i = \lambda y_i \ \forall i$.

Homogeneous Polynomial

A polynomial $f \in k[x_0, \ldots, x_n]$ is homogeneous of degree d if

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n) \quad \text{for all } \lambda \in \bar{k}.$$

Homogeneous Ideal

$I \subset k[x_0, \ldots, x_n]$ is homogeneous if it is generated by homogeneous polynomials.

Projective Variety

Projective Algebraic Set and Ideal

$$V_I = \{p \in \mathbb{P}^n(k) \mid f(p) = 0 \text{ for all } f \in I\}, I \text{ homogeneous.}$$
$$I(V) = \{f \in \bar{k}[x] \mid f \text{ homogeneous and } f(p) = 0 \ \forall p \in V\}$$

Projective Variety

A projective algebraic set V such that $I(V)$ is a prime ideal in $k[x]$.

Smoothness

In affine space, let V be a variety, $p \in V$, and let $f_1, \ldots, f_m \in \bar{k}[x]$ be generators of $I(V)$.

- The Jacobian matrix at p is

$$J(p) = \left(\frac{\partial f_i}{\partial x_j}(p) \right)_{1 \le i \le m,\ 1 \le j \le n}.$$

- If $J(p)$ has rank $n - \dim(V)$, then V is nonsingular at p.
- If V is nonsingular at every point, then V is smooth everywhere.

In projective space, let $V \subset \mathbb{P}^n$ be a projective variety and $p \in V$. Choose an affine chart $\mathbb{A}^n \subset \mathbb{P}^n$ with $p \in \mathbb{A}^n$.

- V is nonsingular at p if $V \cap \mathbb{A}^n$ is nonsingular at p.
- This definition is independent of the chosen affine chart.

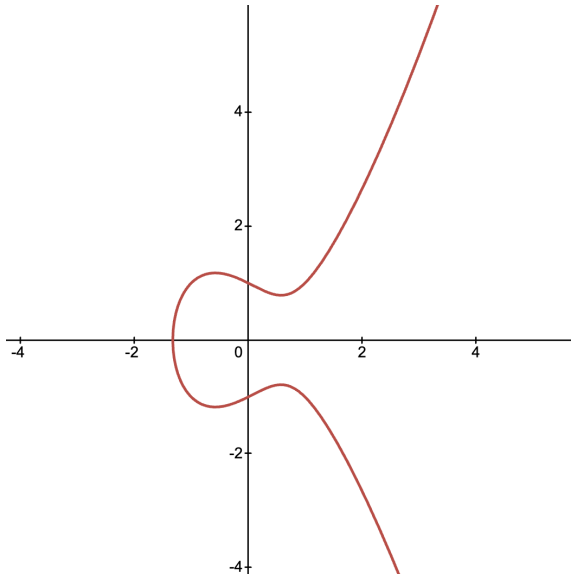
Definition of an Elliptic Curve (EC)

Elliptic Curve

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

Example

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



Projective Plane and Projective Plane Curves

Projective Plane

The set $\mathbb{P}^2(k)$ of all nonzero triples (x, y, z) in k^3 modulo the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z), \quad \lambda \in k^\times$.

- Affine points: $(x : y : 1)$ Points at infinity: $(x : y : 0)$.

Plane Projective Curve

A homogeneous polynomial $f(x, y, z)$ with coefficients in k. The degree of C_f is the degree of $f(x, y, z)$.

K-rational points of C_f

For any field K containing k, the K-rational points of C_f form the set $C_f(K) = \{(x : y : z) \in \mathbb{P}^2(K) \mid f(x, y, z) = 0\}$.

- Smoothness is previously defined.

Weierstrass Equation

Weierstrass Equation

Let $A, B \in k$ with $4A^3 + 27B^2 \neq 0$, and assume $\mathrm{char}(k) \neq 2, 3$. The short Weierstrass equation stated as

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

defines a smooth projective curve of genus 1 over k with the rational point $(0 : 1 : 0)$.

- Up to isomorphism, every elliptic curve over k can be defined this way.
- $y^2z = x^3 + Axz^2 + Bz^3 \Rightarrow z = 0 \Rightarrow x = 0 \Rightarrow (0 : y : 0) \sim (0 : 1 : 0)$

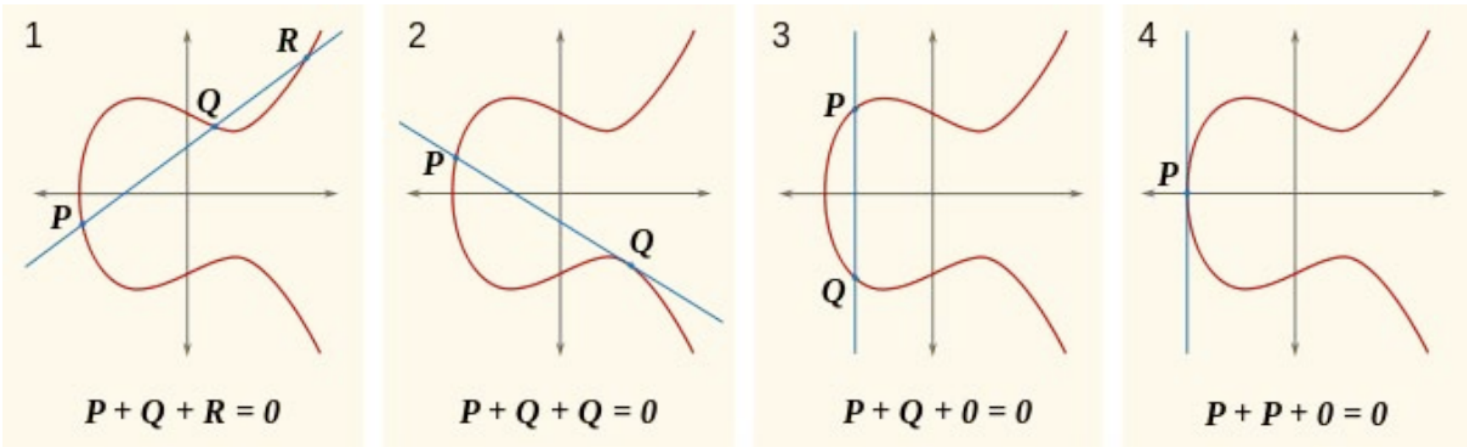
Notice

$4A^3 + 27B^2 = 0$ creates a singular point.

The Group Law

Three points on a line sum to zero.

- (P, Q, R)
- $P + Q = -R$, the reflection of R across the x-axis.



Properties

- Identity: The point $(0:1:0)$ at infinity is the identity element 0.
- Inverse: The inverse of $P = (x:y:z)$ is $-P = (x:-y:z)$.
- Commutativity: $P + Q = Q + P$.
- Associativity: $P + (Q + R) = (P + Q) + R$.
- Scalar Multiplication: $0P = 0$, $nP = P$

Notice

Commutativity is trivial, as the line passing through P and Q is the same as the line passing through Q and P. Associativity, on the other hand, is not so obvious.

The group law is algebraic and field independent. It works over $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{F}_p$.

References

- A. Gathmann, *Algebraic Geometry*, lecture notes, TU Kaiserslautern, 2021/22.
- A. Sutherland, *18.783: Elliptic Curves — Lecture Notes*, Spring 2021, MIT OpenCourseWare, Massachusetts Institute of Technology, https://ocw.mit.edu/courses/18-783-elliptic-curves-spring-2021/pages/lecture-notes-and-worksheets/.
- J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.