Elliptic Curve Arithmetic

Toni Bluher

Outline

An elliptic curve E over a field F is given by a cubic equation of special form. Assume for simplicity $\mathrm{char}(F) \neq 2, 3$, then

$$E: \; y^2 = x^3 + Ax + B, \text{where } A, B \in F, \; 4A^3 + 27B^2 \neq \tag{1}$$

The points of E can be made into a group!

Group Identity is "the point at infinity", denoted $\mathcal{O}$.

Extension fields If K/F is field extension, then $E(K)$ is group:

$$E(K) = \{\mathcal{O}\} \cup \{(x_0, y_0) \in K \times K : y_0^2 = x_0^3 + Ax_0 + B\}.$$

Cryptographic applications

For cryptography take F to be a finite field $\mathbb{F}_q$.

Applications Williamson/Diffie-Hellman key exchange,
elliptic curve digital signature algorithm,
identity-based encryption

Unit Circle Group (Warm-up to EC group)

Unit Circle Group $x^2 + y^2 = 1$

Parameterization $(\cos\theta, \sin\theta)$

Addition $(\cos\theta_1, \sin\theta_1) + (\cos\theta_2, \sin\theta_2) = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2))$.

Algebraic group $(a, b) + (c, d) = (ac - bd, ad + bc)$, by trig formulas. Group law given by polynomials (or rational functions) in coords of points.

Rationality If (a, b) and (c, d) have coords in field K then so does sum. K-rational points form group.

Elliptic Curves mirror these properties.

Group Law (Geometric description)

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

Addition Rule If $E \cap L = \{P, Q, R\}$, then $P + Q + R = \mathcal{O}$. (L a line).

Most lines pass through 3 distinct points.

Vertical line $\{x = x_0\}$ passes through only two points, (x_0, y_0) and $(x_0, -y_0)$. So $(x_0, y_0) + (x_0, -y_0) = \mathcal{O}$.

Tangents If L is tangent to P and also passes through Q then $L \cap E = \{P, P, Q\}$, and $2P + Q = \mathcal{O}$.

Group Law (Algebraic description)

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E$.

Negation If $P_2 = (x_1, -y_1)$ then $P_1 + P_2 = \mathcal{O}$. So $-(x_1, y_1) = (x_1, -y_1)$.

Doubling If $P_1 = P_2$ and $y_1 \neq 0$ then let $m = (3x_1^2 + A)/(2y_1)$, $b = y_1 - mx_1$. Then $2P_1 = (x_3, -(mx_3 + b))$.

Generic If none of above cases hold then $m := (y_2 - y_1)/(x_2 - x_1)$, $b := y_1 - mx_1$, $x_3 := m^2 - x_1 - x_2$. $P_1 + P_2 = (x_3, -(mx_3 + b))$.

Example

- $E : y^2 = x^3 - x$ over $\mathbb{F}_5$. Compute $(2,1) + (-1,0)$.
- In $\mathbb{F}_5$: $2 \cdot 3 = 1$, $1/2 = 3$, $1/3 = 2$, $1/4 = 4$.
- Points are $\mathcal{O}$, $(0,0)$, $(1,0)$, $(2,\pm 1)$, $(-2,\pm 2)$, $(-1,0)$.
- Line is $(y - 0) = m(x + 1)$, where $m = (1 - 0)/(2 + 1) = 1/3 = 2$.
- $y = 2x + 2$ passes through $(2,1)$, $(-1,0)$, and (x_3, y_3).
- $x^3 - x - (2x + 2)^2 = x^3 - x + x^2 + 2x + 1 = (x - 2)(x + 1)(x - x_3)$.
- From coef of x^2, $-2 + 1 - x_3 = 1$, $x_3 = 3$, $y_3 = 2x_3 + 2 = 3$.
- $(2,1) + (-1,0) = (x_3, -y_3) = (3,2)$.

Reference

L. C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd Edition, Chapman & Hall/CRC, 2008. Easy to read yet covers a lot!