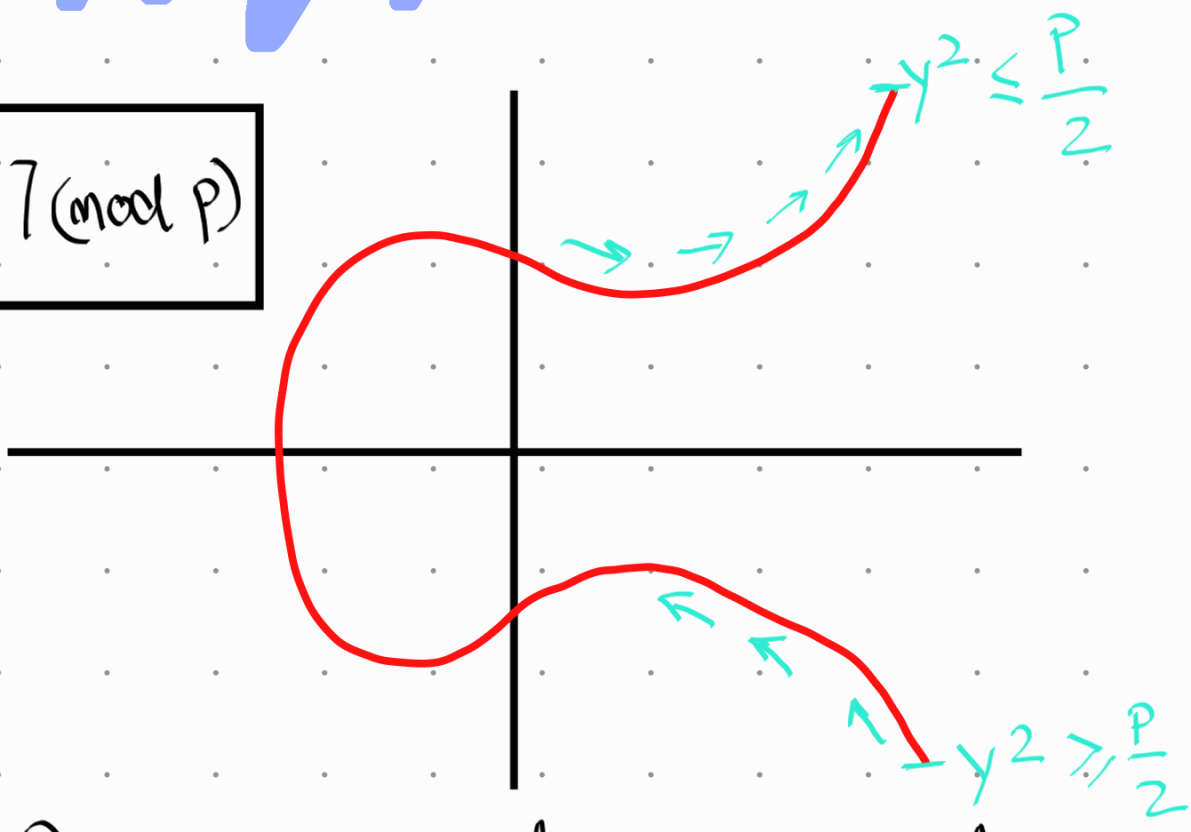
Description : elliptic curve cryptography

SECP256K1 Elliptic Curve

$$y^2 = x^3 + 7 \pmod{p}$$



Where p is a very large prime Number

Group Theory

SECP256K1 → A group of points on a curve

$\{(x, y), (x_1, y_2), \ldots\}$

Where actual coordinates of points will be very large numbers as they are modded with p.

Group Properties

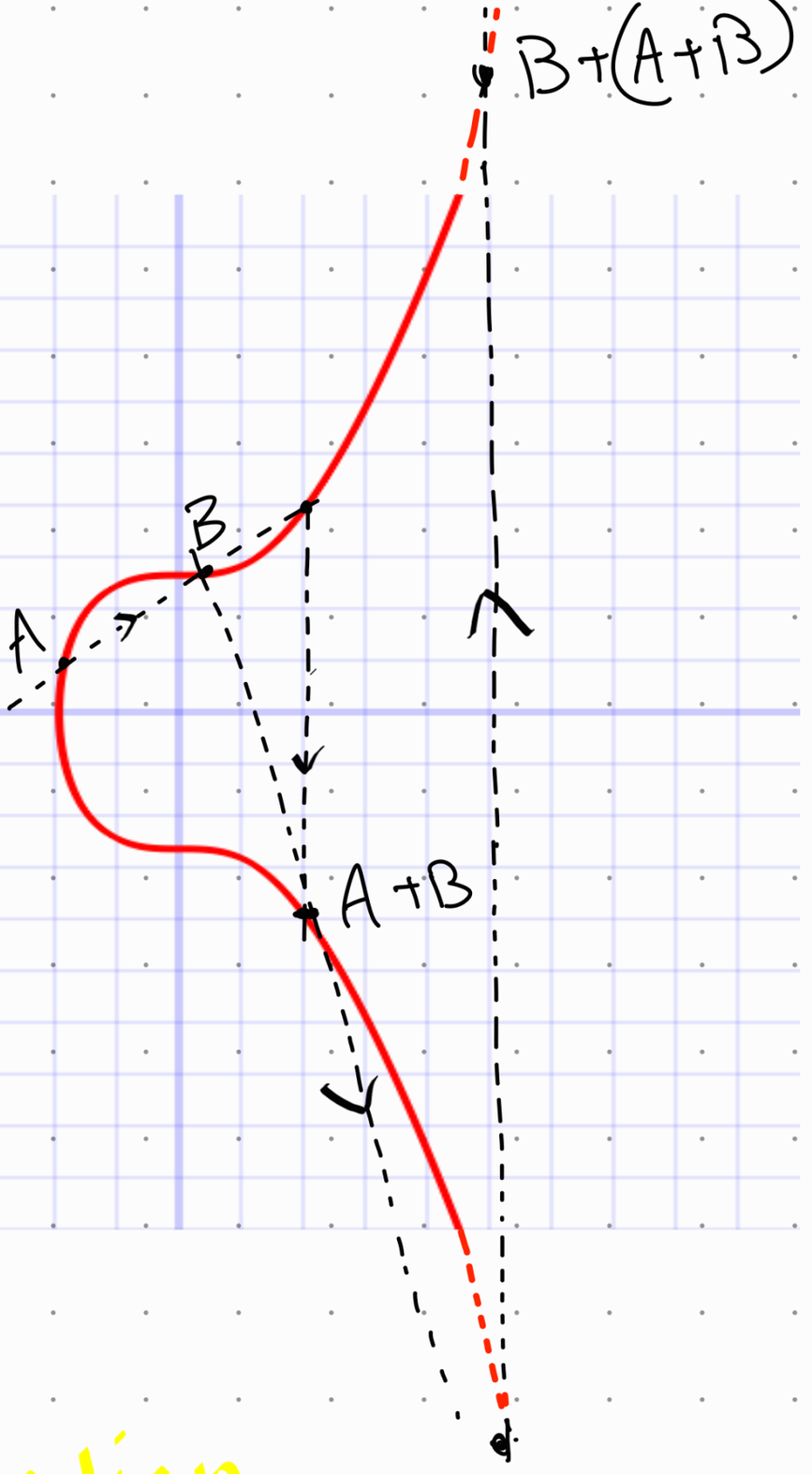
- order (n)

n = no. of points on elliptic curve

n is prime

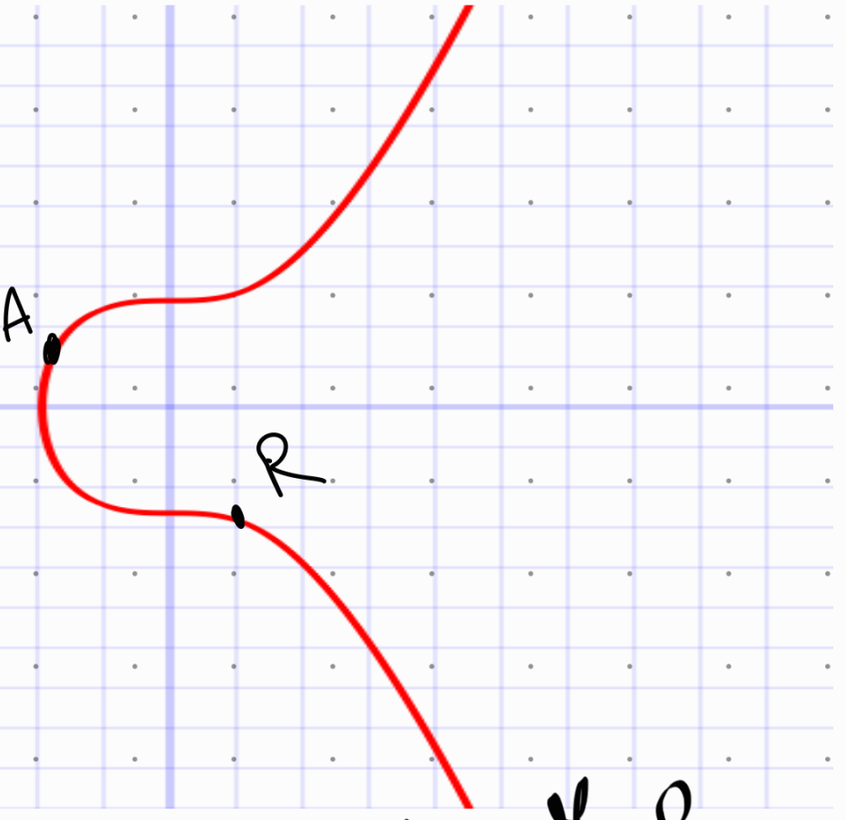
Group Operations

- Addition



- Multiplication

If An = R



if you have the value of R it would be insanely hard to get value of **n** such that $An = R$.