Elliptic Curve Cryptography

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 23 Dec 2021,
elliptic.tex, r1949

Contents

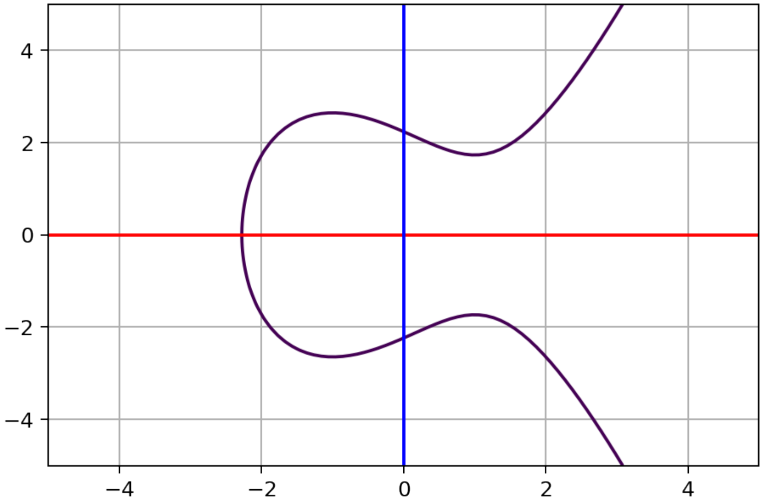
Elliptic Curve (definition)

An elliptic curve is defined by:

$$y^2 = x^3 + ax + b$$

(with some constraints of constants a and b)

Elliptic Curve for $y^2 = x^3 - 3x + 5$



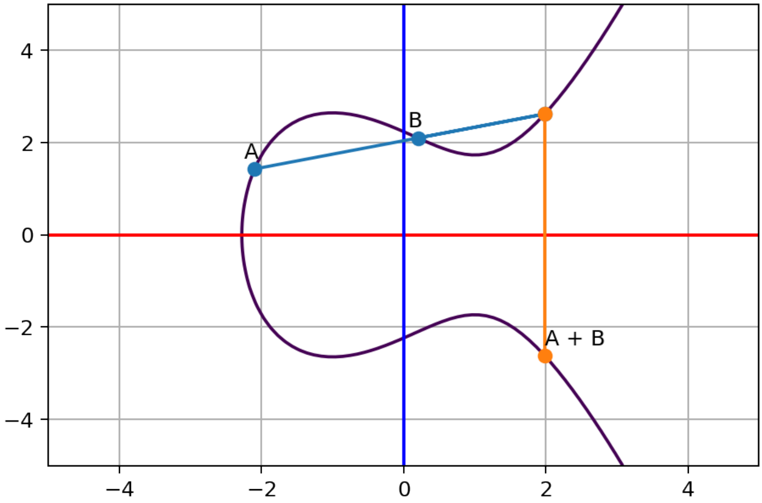
Credit: Generated based on MIT Licensed code by Fang-Pen Lin

Addition Operation with an Elliptic Curve (definition)

Select two points on the curve, A and B, and draw a straight line through them. The line will intersect with the curve at a third point, R (and no other points). The horizontal inverse of point R, is defined as the addition of A and B.

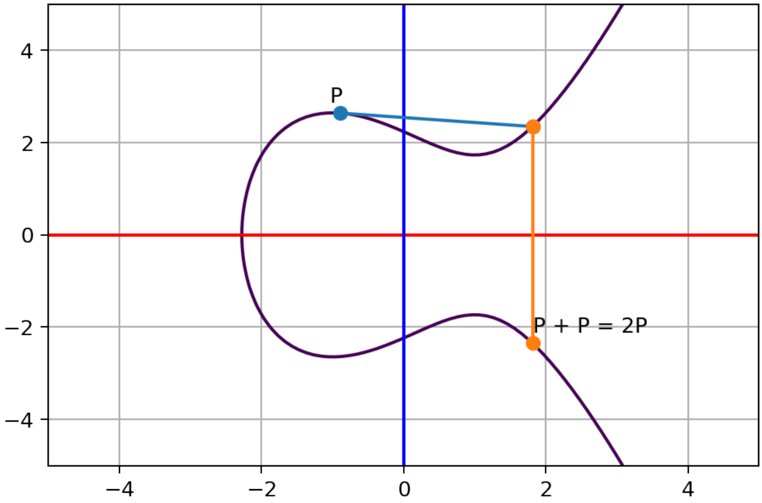
$$A + B = -R$$

Addition Operation on Elliptic Curve



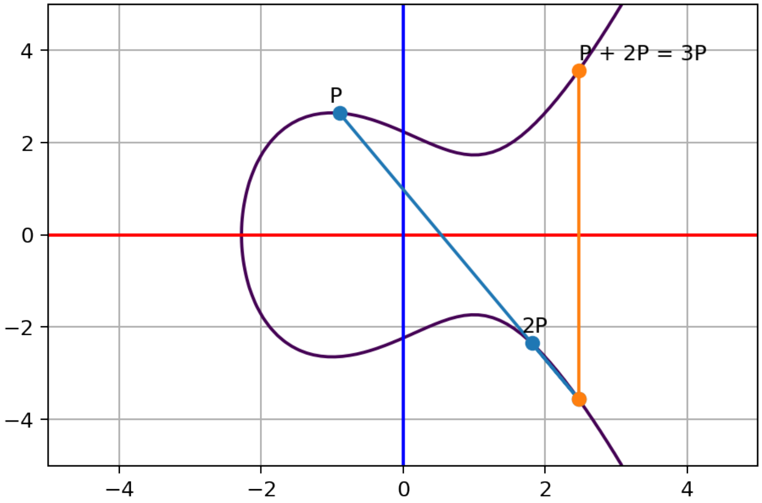
Credit: Generated based on MIT Licensed code by Fang-Pen Lin

Self Addition on Elliptic Curve



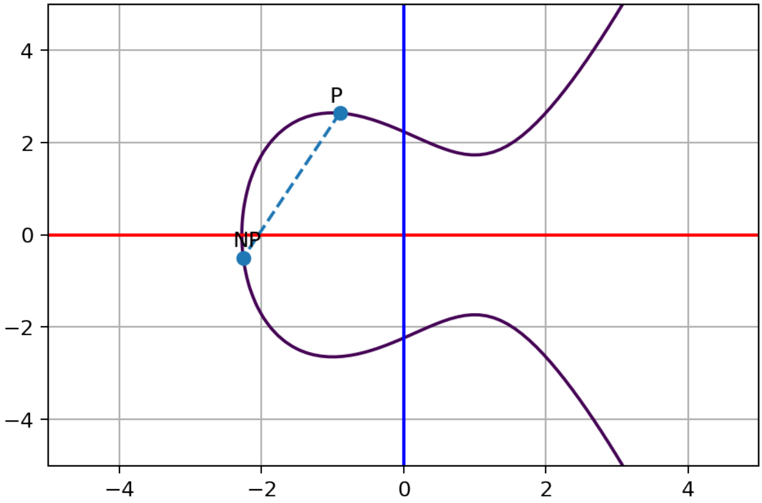
Credit: Generated based on MIT Licensed code by Fang-Pen Lin

P + 2P on Elliptic Curve



Credit: Generated based on MIT Licensed code by Fang-Pen Lin

NP on Elliptic Curve



Credit: Generated based on MIT Licensed code by Fang-Pen Lin

How is Point Addition used in Elliptic Curve Cryptography?

- User chooses a point P (global public parameter)
- User chooses a large, random N (private key)
- User calculates NP (public key)
  - Easy, since there is a shortcut (described shortly)
- Challenge for attacker: given NP, find N
  - Computationally hard for large N

Shortcut for Calculating NP

- Assume N is large, e.g. 256-bit random number
- Naive point addition: $P + P + P + P + \ldots + P + P$ ($2^{256} - 1$ additions)
- Shortcut algorithm for point addition:
  - Calculate P, $P + P = 2P = 2^1 P$, $2P + 2P = 4P = 2^2 P$, $4P + 4P = 8P = 2^3 P$, $\ldots$, $2^{255} P$ (255 additions)
  - Write N as binary expansion, e.g.:
    - $N = 233 = 2^7 + 2^6 + 2^5 + 2^3 + 2^0$
    - $NP = 2^7 P + 2^6 P + 2^5 P + 2^3 P + 2^0 P$
    - In this example, there are 4 point additions
    - Maximum number of point additions for 256-bit N is 255
  - Calculate NP using the binary expansion
  - Maximum number of point additions for 256-bit N: $255 + 255 = 510$

Elliptic Curve with Modular Arithmetic

- The above discussed a normal elliptic curve
- But to ensure all values contained within finite coordinate space, modular arithmetic is used
- $y^2 \bmod p = (x^3 + ax + b) \bmod p$
- p is a prime number

Contents

Applications of ECC

- Secret key exchange, e.g. ECDH, ECMQV
- Digital signatures, e.g. ECDSA, EC-KCDSA
- Public key encryption, e.g. ECIES, PSEC

Elliptic Curve Diffie-Hellman Key Exchange (algorithm)

Assume users A and B have EC key pairs: $PU_A = NP$, $PR_A = N$, $PU_B = MP$, $PR_B = M$.

1. User A calculates secret $S_A = N \cdot PU_B = NMP$ using shortcut point addition.
2. User B calculates secret $S_B = M \cdot PU_A = MNP$ using shortcut point addition.

Choosing Parameters for ECC

- Parameters for ECC are usually standardised
  - Base point, P (also referred to as generator, G)
  - Curve parameters, a and b
  - Prime, p
  - Other parameters also included
- Common curves (see also `https://safecurves.cr.yp.to/`):
  - NIST FIPS 186: P-256, P-384 and 13 others
  - SECG: secp160k1, secp160r1, ... (NIST curves are a subset)
  - ANSI X9.62: prime192, prime256, ...
  - Other curves: Curve25519, Brainpool

Contents