

Elliptic Curves: Cryptography and Mordell–Weil Theorem

Applications of the theory of elliptic curves to cryptography, mathematical aspects and algorithmic aspects of elliptic curves over \mathbb{Q} and \mathbb{F}_q

Sirawit Pongnakintr, under the supervision of Prof. Diego Izquierdo

March 21, 2024

Bachelor of Science, École Polytechnique

Table of contents

1. Asymmetric Cryptography
2. Elliptic curves and applications
3. Over \mathbb{Q}

How to securely encrypt a message?

How to securely encrypt a message?

How does the theory of elliptic curves have to do anything with cryptography?

The goal of this journey!

1. Problems in cryptography and their relations with elliptic curves
2. What about E/\mathbb{Q} ? Can we understand the structure of $E(\mathbb{Q})$?

The goal of this journey!

1. Problems in cryptography and their relations with elliptic curves
2. What about E/\mathbb{Q} ? Can we understand the structure of $E(\mathbb{Q})$?

Expected duration: 20 minutes

Asymmetric Cryptography

The idea

Alice and Bob want to communicate over an insecure channel secretly.

The idea

Alice and Bob want to communicate over an insecure channel secretly.

Bob encrypts the message, then sends the ciphertext to Alice. Alice then decrypts the ciphertext.

Symmetric case

Alice and Bob secretly agrees on a **key** first. After the key agreement, they can encrypt messages using standard procedures such as DES or AES.

Asymmetric case

Alice generates a key pair: a pair of public key and a private key. The public key is distributed publicly. The private key is kept privately.

Asymmetric case

Alice generates a key pair: a pair of public key and a private key. The public key is distributed publicly. The private key is kept privately.

Bob uses the public key to encrypt a message into a ciphertext, and send that ciphertext over the insecure channel to Alice.

Asymmetric case

Alice generates a key pair: a pair of public key and a private key. The public key is distributed publicly. The private key is kept privately.

Bob uses the public key to encrypt a message into a ciphertext, and send that ciphertext over the insecure channel to Alice.

Alice then receives the ciphertext and decrypt using the private key.

1. Choose two prime numbers p and q . Let $n = pq$ and $m = (p - 1)(q - 1)$.

RSA: key generation

1. Choose two prime numbers p and q . Let $n = pq$ and $m = (p - 1)(q - 1)$.
2. Choose an integer e such that $1 < e < m$ and $\gcd(e, m) = 1$.

RSA: key generation

1. Choose two prime numbers p and q . Let $n = pq$ and $m = (p - 1)(q - 1)$.
2. Choose an integer e such that $1 < e < m$ and $\gcd(e, m) = 1$.
3. Compute d such that $1 < d < m$ and $de \equiv 1 \pmod{m}$. (It can be proved that d exists)

Public key: (n, e) . Private key: d .

RSA: encryption and decryption

Bob encrypts a message M (assuming $\gcd(M, n) = 1$ and $1 < M < n$) by computing $c = M^e \bmod n$ and sends c to Alice (over an insecure channel).

RSA: encryption and decryption

Bob encrypts a message M (assuming $\gcd(M, n) = 1$ and $1 < M < n$) by computing $c = M^e \bmod n$ and sends c to Alice (over an insecure channel).

Alice decrypts the ciphertext c by computing $c^d \bmod n$. Suppose $D = c^d \bmod n = (M^e)^d \bmod n$. Since $de \equiv 1 \pmod{m}$, $de - 1 = mk$ for some $k \in \mathbb{Z}$. So $D \equiv M^{mk+1} \pmod{n}$.

RSA: encryption and decryption

Bob encrypts a message M (assuming $\gcd(M, n) = 1$ and $1 < M < n$) by computing $c = M^e \bmod n$ and sends c to Alice (over an insecure channel).

Alice decrypts the ciphertext c by computing $c^d \bmod n$. Suppose $D = c^d \bmod n = (M^e)^d \bmod n$. Since $de \equiv 1 \pmod{m}$, $de - 1 = mk$ for some $k \in \mathbb{Z}$. So $D \equiv M^{mk+1} \pmod{n}$.

Apply Euler's theorem to see that $M^{\varphi(n)} = M^m \equiv 1 \pmod{n}$, so $D \equiv M \pmod{n}$. Alice then recovers the message M from D .

RSA Problem

Given $c, e, n \in \mathbb{Z}$ such that $0 \leq c < n$, $1 < e < m$, $\gcd(e, m) = 1$.
Suppose that there exists (unknown) primes p, q such that $n = pq$,
and there exists (unknown) integer message $0 \leq M < n$ such that
 $M^e \bmod n = c$. The problem is to recover such M .

Integer factorization

If one can solve integer factorization in polynomial time, one could also solve RSA problem in polynomial time.

ElGamal Cryptosystem

Let (G, \cdot) be a group.

1. Alice and Bob agree on an element $C \in G$.
2. Alice select $a \in \mathbb{N}$, which is the secret key, and computes $A := C^a$, which is the public key.
3. Bob wants to encrypt a message $M \in G$. Bob choose a random $k \in \mathbb{N}$.
4. Bob computes

$$B_1 = C^k \quad \text{and} \quad B_2 = MA^k.$$

5. Bob sends (B_1, B_2) through an insecure communication line.
6. Seeing that $B_1^a = (C^k)^a = C^{ak} = (C^a)^k = A^k$, one can compute M as $M = MA^k(A^k)^{-1} = B_2(B_1^a)^{-1}$. Alice can then compute $B_2(B_1^a)^{-1}$ to recover M .

DHP: If Eve wants to eavesdrop the message, how to do that? In other words, given s , s^a and s^b , compute s^{ab} .

DHP: If Eve wants to eavesdrop the message, how to do that? In other words, given s , s^a and s^b , compute s^{ab} .

DLP: Knowing (G, \cdot) and an element $s \in G$ beforehand. Suppose $s^n \in G$ is given (with unknown n). The problem is to recover $n \in \mathbb{Z}$.

- $(\mathbb{Z}/n\mathbb{Z}, +)$: easy.

- $(\mathbb{Z}/n\mathbb{Z}, +)$: easy.
- $(\mathbb{F}_q^\times, \cdot)$: expected to be hard, but nontrivial methods are available. (See *index calculus*.)

DLP on different groups

- $(\mathbb{Z}/n\mathbb{Z}, +)$: easy.
- $(\mathbb{F}_q^\times, \cdot)$: expected to be hard, but nontrivial methods are available. (See *index calculus*.)
- $E(\mathbb{F}_q)$: expected to be hard, no general algorithm exists, currently.

Elliptic curves and applications

The group law on elliptic curves

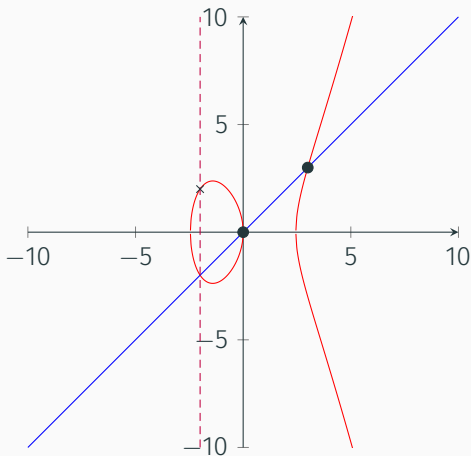


Figure 1: An elliptic curve with two specified points and a line passing through them, where O is the point at infinity. The sum of the two black dots is denoted by \times at $(-2, 2)$.

Other involved algorithms

- Lenstra's elliptic curve factorization algorithm (ECM).
- Schoof's algorithm to count the number of points $\#E(\mathbb{F}_q)$.
- MOV algorithm to reduce ECDLP into DLP of direct product of groups in the form $\mathbb{Z}/n\mathbb{Z}$.

Over \mathbb{Q}

The structure of $E(\mathbb{Q})$

Let $E: y^2 = x^3 + Ax + B$ be defined over \mathbb{Q} , i.e. $A, B \in \mathbb{Q}$ and consider solutions (x, y) where $x, y \in \bar{\mathbb{Q}}$.

The structure of $E(\mathbb{Q})$

Let $E: y^2 = x^3 + Ax + B$ be defined over \mathbb{Q} , i.e. $A, B \in \mathbb{Q}$ and consider solutions (x, y) where $x, y \in \bar{\mathbb{Q}}$.

Theorem 1 (Mordell–Weil)

The group $E(\mathbb{Q})$ is finitely generated.

The structure of $E(\mathbb{Q})$

Let $E: y^2 = x^3 + Ax + B$ be defined over \mathbb{Q} , i.e. $A, B \in \mathbb{Q}$ and consider solutions (x, y) where $x, y \in \bar{\mathbb{Q}}$.

Theorem 1 (Mordell–Weil)

The group $E(\mathbb{Q})$ is finitely generated.

Theorem 2 (Classification of finitely generated abelian groups)

If G is finitely generated and abelian, then there exists an integer $r \geq 1$ and a finite abelian group G_{tors} such that

$$G \cong \mathbb{Z}^r \times G_{\text{tors}},$$

where G_{tors} is equal to the set of torsion points of G , i.e.

$$G_{\text{tors}} = \{g \in G : \exists n \in \mathbb{N}^*, g^n = 1_G\}.$$

Theorem 3 (Weak Mordell–Weil)

For an elliptic curve E/\mathbb{Q} , the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Then, apply the **descent** procedure, which is the following.

1. Equip each point with the notion of a height.
2. Prove that for any bounded constant, there exists only finitely many rational points under that bound.
3. Now, for each point $P \in E(\mathbb{Q})$, write

$$P = R_{\alpha_1} + [2]P_1$$

$$P_1 = R_{\alpha_2} + [2]P_2$$

$$\vdots$$

$$P_{k-1} = R_{\alpha_k} + [2]P_k.$$

Once we prove that this algorithm terminates, i.e. k is finite for all P , such that R_{α_i} 's belong to $E(\mathbb{Q})/2E(\mathbb{Q})$ and P_k has height no more than C , then the set

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cup \{\text{points with height less than or equal to } C\}$$

(which is finite) generates $E(\mathbb{Q})$.

Theorem 4 (Lutz–Nagell)

Let $E/\mathbb{Z}: y^2 = x^3 + Ax + B$. Let $P = (x, y) \in E(\mathbb{Q})$. If P has finite order, then $x, y \in \mathbb{Z}$. If furthermore $y \neq 0$, then $y^2 \mid 4A^3 + 27B^2$.

Any elliptic curve E/\mathbb{Q} is isomorphic to another elliptic curve E'/\mathbb{Z} . This proves that $E(\mathbb{Q})_{\text{tors}}$ is finite, and also gives a way to compute the subgroup.

Next steps

$E(\mathbb{Q})_{\text{tors}}$ can be computed easily, but there is (still) no general algorithm to compute the **rank** of an elliptic curve. Further, the **rank** seems to have some extra properties. This is one possible area of study and research.

Next steps

$E(\mathbb{Q})_{\text{tors}}$ can be computed easily, but there is (still) no general algorithm to compute the **rank** of an elliptic curve. Further, the **rank** seems to have some extra properties. This is one possible area of study and research.

We don't know if RSA problem, integer factorization, DLP, DHP are really hard or actually easy. This also allows further studies in computational complexity theory to classify them as **P**, **NP-complete**, or **NP-intermediate**.





Next steps

$E(\mathbb{Q})_{\text{tors}}$ can be computed easily, but there is (still) no general algorithm to compute the **rank** of an elliptic curve. Further, the **rank** seems to have some extra properties. This is one possible area of study and research.

We don't know if RSA problem, integer factorization, DLP, DHP are really hard or actually easy. This also allows further studies in computational complexity theory to classify them as **P**, **NP-complete**, or **NP-intermediate**.

Mordell–Weil theorem, in full generality, isn't only for $E(\mathbb{Q})$, but also for $E(K)$ for any algebraic number field K (i.e. finite extension of \mathbb{Q}). The statement can be proved in full generality using a little bit of algebraic number theory, which is a possible area of study in the future.

References

-  Izquierdo, Diego (2024). *MAT 562 : Introduction à la géométrie algébrique et courbes elliptiques*.
-  Neukirch, Jürgen (1999). *Algebraic Number Theory*. Springer Berlin Heidelberg. ISBN: 9783662039830. DOI: 10.1007/978-3-662-03983-0. URL: <http://dx.doi.org/10.1007/978-3-662-03983-0>.
-  Silverman, Joseph H. (2009). *The Arithmetic of Elliptic Curves*. Springer New York. DOI: 10.1007/978-0-387-09494-6. URL: <https://doi.org/10.1007/978-0-387-09494-6>.
-  Washington, Lawrence C (2008). *Elliptic curves : number theory and cryptography – 2nd ed*. Discrete Mathematics and Its Applications. Chapman & Hall/CRC.

Appendix

Computation

Theorem 5

If $P_1, P_2 \in E$ with coordinates (x_1, y_1) and (x_2, y_2) respectively, such that $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + a_1 \left(\frac{y_2 - y_1}{x_2 - x_1} \right) - a_2 - x_1 - x_2,$$
$$y(P_1 + P_2) = - \left(\frac{y_2 - y_1}{x_2 - x_1} + a_1 \right) x(P_1 + P_2) - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \right) - a_3.$$

If $P_1 = -P_2$ then $P_1 + P_2 = O$. If $P_1 = P_2$ then consider the following duplication formula for $P = (x, y) \in E$.

$$x([2]P) = \left(\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \right)^2 + a_1 \left(\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \right) - a_2 - 2x,$$
$$y([2]P) = - \left(\frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} + a_1 \right) x([2]P) - \frac{-x^3 + a_4x + 2a_6 - a_3y}{2y + a_1x + a_3} - a_3.$$

This is given in Silverman 2009, Group Law Algorithm III.2.3.