Elliptic Curves & Cryptography

Ethan Denning

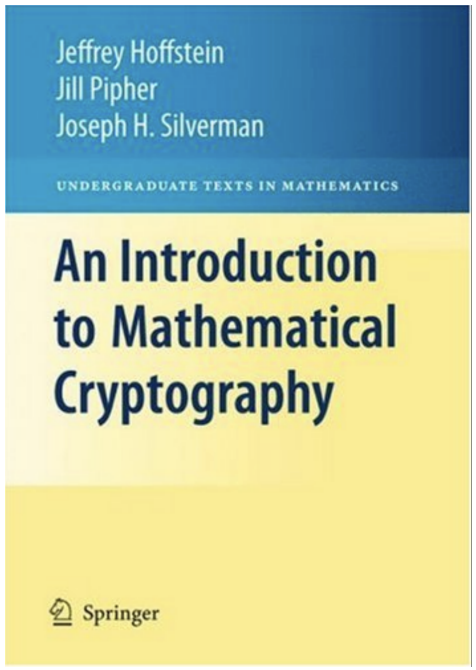
May 7, 2026

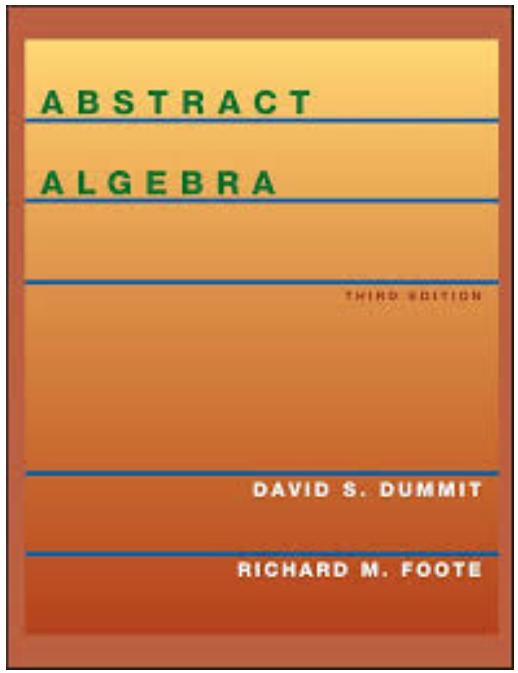
Overview

- Private-Key and Public-Key Cryptography
- The Discrete Log Problem and Diffie-Hellman Key Exchange
- Elliptic Curves
- Addition on Elliptic Curves
- The Elliptic Curve Discrete Log Problem
- Elliptic Curve Diffie-Hellman Key Exchange

References

- *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman.
- *Abstract Algebra* by Dummit and Foote.





Private-Key Cryptography

Private-key cryptography is the classical setup for secure communication. In this case, two parties Alice and Bob already share a secret key which is used for both encryption and decryption.

Example (Shift Cipher)

Suppose Alice and Bob share a secret key $0 \leq K < 26$. To send a message M, Alice first converts each plaintext letter of M into a number using

$$A = 0,\ B = 1,\ \ldots,\ Z = 25,$$

and encrypts each digit of M by computing

$$c \equiv m + K \pmod{26}.$$

Since Bob knows K, he can subtract K from each digit modulo 26 and convert back to plaintext to decrypt the message.

Example

For instance, Alice could encrypt the message

$$\texttt{HELLO}$$

by using the shift cipher with $K = 3$. Here, each letter is shifted three places forward:

$$\texttt{HELLO} \longmapsto \texttt{KHOOR}.$$

Assuming Bob knows that $K = 3$, he can easily decrypt by shifting each letter three places backward.

This algorithm dates back to the Roman Empire, where it was famously used by Julius Caesar for military communications.

Public-Key Cryptography

How can two parties who have never met communicate securely?

Examples: Private emails, cryptocurrency transfers, etc.

Definition

- **Public-key cryptography**, or asymmetric cryptography, is a method of secure communication in which each user has a pair of keys: a **public key** which is used for encryption, and a **private key** which is used for decryption.

Public-key cryptography primarily relies on *one-way functions*, i.e. functions which are easy to compute but difficult to invert. For instance, while we can easily multiply integers, factoring is difficult in general.

The Discrete Log Problem

Let g be an element of a group G. **The Discrete Log Problem** (DLP) for G is the following:

Definition

Discrete Log Problem: Given some element h in the subgroup generated by g, find the smallest integer $m > 0$ which satisfies $h = g^m$.

The smallest m to satisfy $h = g^m$ is known as the *discrete log* of h with respect to g.

Hardness Of The Discrete Log Problem

How hard is the Discrete Log Problem?

It depends upon the group! For example, the best known algorithm to solve the DLP for the group of units

$$\mathbb{F}_p^* = (\mathbb{F}_p \setminus \{0\}, \times)$$

modulo p is of time

$$O\left(e^{\sqrt{(\log p)(\log\log p)^2}}\right).$$

This is known as **subexponential** time (faster than exponential but slower than polynomial).

Diffie-Hellman Key Exchange

The **Diffie-Hellman Key Exchange** is a method of public-key cryptography which relies on the DLP as a one-way function.
Public Information: A group G and an element $g \in G$ of order n.

Algorithm

- Bob and Alice choose secret keys $0 < b < n$ and $0 < a < n$ respectively.
- Bob computes $B = g^b$ and sends it to Alice, and Alice computes $A = g^a$ and sends it to Bob.
- Bob and Alice respectively compute A^b and B^a.

Bob and Alice now have the shared value:

$$A^b = g^{ab} = g^{ba} = B^a$$

Computing the value of g^{ab} without knowing a or b depends on the difficulty of solving the discrete log problem for G.

Example

Let $G = (\mathbb{Z}/941\mathbb{Z})^*$.

- Alice and Bob agree to a primitive root $g = 627 \in G$.
- Alice chooses a secret $a = 347$ and computes $A = 390 \equiv 627^{347} \pmod{941}$
- Similarly, Bob chooses a secret $b = 781$ and computes $B = 691 \equiv 627^{781} \pmod{941}$.
- Finally, they have shared value of

$$A^b \equiv B^a \equiv 627^{347 \cdot 781} \equiv 470 \pmod{941}.$$

This value can then be used as a private key in some private-key cryptographic protocol.

Why Elliptic Curves?

- Elliptic curves with points over finite fields are finite groups. Thus, we can translate traditional cryptography problems to such elliptic curves.
- The group of points on an elliptic curve is "general enough" so there is no especially efficient algorithm to compute its associated discrete log problem.
- Translations of classical cryptography problems such as the discrete log problem to elliptic curves allows for an increase in hardness, smaller key sizes, etc.

Elliptic Curves

Definition

An **elliptic curve** $E(K)$ is a smooth projective curve of genus 1 over a field K with at least one K-rational point.

If $\mathrm{char}(K) \neq 2, 3$, every elliptic curve $E(K)$ can be defined as the set of points $(X, Y) \in K^2$ satisfying a *Weierstrass equation*

$$Y^2 = X^3 + AX + B$$

for coefficients $A, B \in K$ such that

$$4A^3 + 27B^2 \neq 0.$$

We also add a "point at infinity", denoted by $\mathcal{O}$, to $E(K)$.

Complex Elliptic Curves

Amazingly, every elliptic curve over the complex numbers $\mathbb{C}$ is a torus!

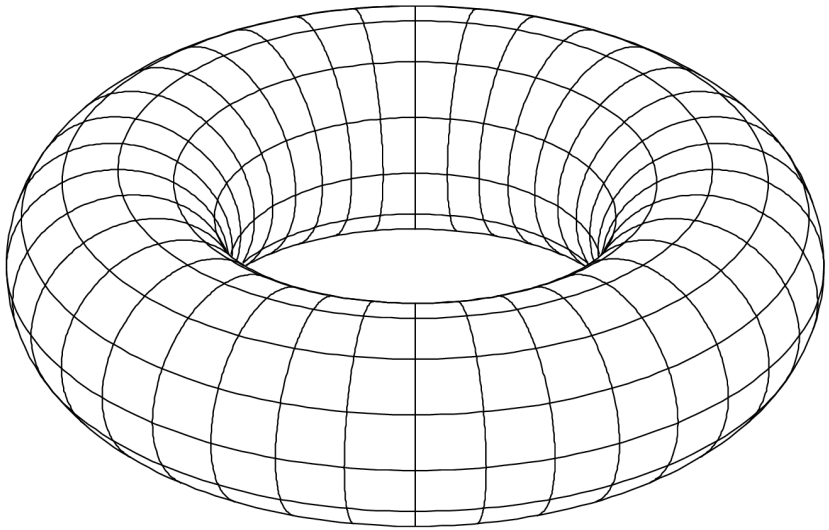


Figure: Torus

More precisely, every complex elliptic curve is of the form $\mathbb{C}/L$ for some lattice $L = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$.

Real Elliptic Curves

Over the real numbers, elliptic curves take one of the following two forms:

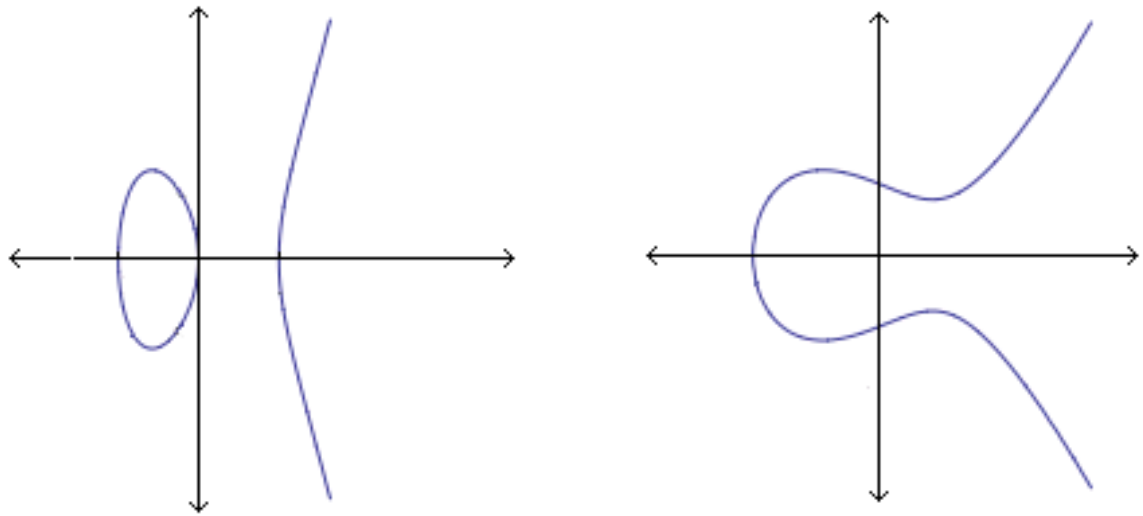
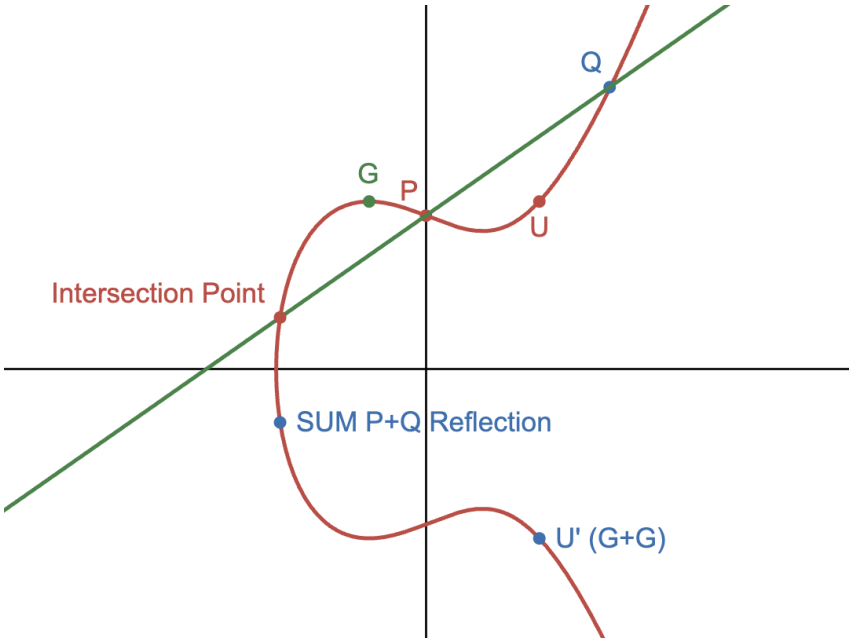


Figure: Examples of real elliptic curves.

Addition on Elliptic Curves

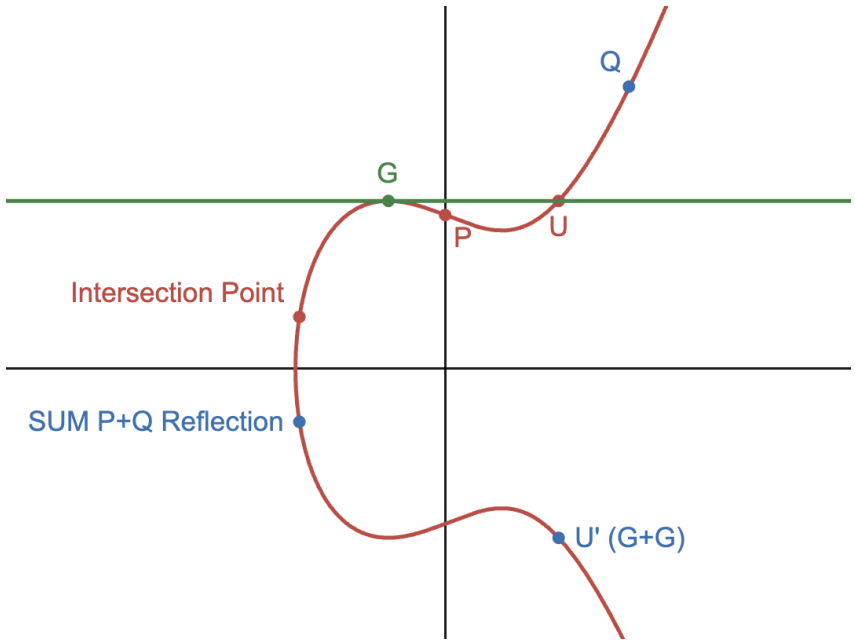
We are interested in adding two points $P, Q \in E(K)$ and obtaining a third point $R \in E(K)$. In the case $K = \mathbb{R}$, this group law can be described geometrically.

First, if P and Q do not lie on a common vertical line, then the secant line through P and Q intersects $E(K)$ at a third point R. We then set $P \oplus Q$ to be the reflection of R across the x-axis:



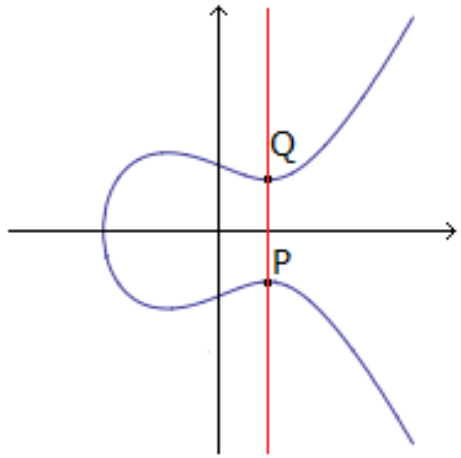
The case $P = Q$

If $P = Q = G$, we consider the analogue of the secant line from calculus, i.e. the tangent line.
In this case, the tangent line through G intersects $E(K)$ at exactly one point U, and we again set $G \oplus G$ to be the reflection of U across the x-axis.



The case P and Q lie on a vertical line

But what about the case that P and Q lie on a vertical line L?



In this case, we say that L intersects $E(K)$ at the additional point at infinity $\mathcal{O}$, and set

$$P \oplus Q = \mathcal{O}.$$

Accordingly, we denote Q by $-P$ in this case.

Addition Formula

Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve, and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E.

Addition Formula

- If $P_1 \neq P_2$ and $x_1 = x_2$, then $P_1 \oplus P_2 = \mathcal{O}$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 \oplus P_2 = 2P_1 = \mathcal{O}$.
- If $P_1 \neq P_2$ and $x_1 \neq x_2$, let $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$.
- If $P_1 = P_2$ and $y_1 \neq 0$, let $\lambda = \frac{3x_1^2 + A}{2y_1}$ and $v = \frac{-x_1^3 + Ax_1 + 2B}{2y_1}$.

Then,

$$P_1 \oplus P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - v).$$

This gives us a way to add points on a general elliptic curve defined over $\mathbb{C}, \mathbb{Q}, \mathbb{F}_p$, etc...

Group Law for Elliptic Curves

One can show that the points on any elliptic curve form an abelian group under $\oplus$ with identity $\mathcal{O}$.

Theorem

The addition law on E has the following properties:

- *Identity Element:* $P \oplus \mathcal{O} = P$.
- *Inverse:* $P \oplus (-P) = \mathcal{O}$.
- *Commutativity:* $P \oplus Q = Q \oplus P$.
- *Associativity:* $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.

While it is straightforward to verify the first three properties, the proof of associativity is unintuitive and somewhat arduous.

Elliptic Curves over Finite Fields

In the context of cryptography, we are particularly interested in elliptic curves over finite fields. For example, consider the elliptic curve

$$E(\mathbb{F}_{13}) : Y^2 = X^3 + 3X + 8.$$

We can find points on $E(\mathbb{F}_{13})$ by checking whether each point in $\mathbb{F}_{13}^2$ satisfies the given Weierstrass equation. For instance, letting $X = 1$, we have

$$(1)^3 + 3(1) + 8 \equiv 12 \pmod{13},$$

where

$$5^2 \equiv 8^2 \equiv 12 \pmod{13},$$

so $(1, 5), (1, 8) \in E(\mathbb{F}_{13})$. More generally, we have

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\}.$$

E($\mathbb{F}_p$) as a group

It is clear that $E(\mathbb{F}_p) \subseteq \mathbb{F}_p^2$ is finite. But how large can we expect it to be in general?

Theorem (Hasse's Theorem)

Let E be an elliptic curve over $\mathbb{F}_p$. Then,

$$\#E(\mathbb{F}_p) = p + 1 - t_p,$$

where t_p is the **trace of the Frobenius**, *and satisfies*

$$|t_p| \leq 2\sqrt{p}.$$

Equivalently,

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Elliptic Curve Discrete Log Problem

Definition (Elliptic Curve Discrete Log Problem (ECDLP))

Let E be an elliptic curve defined over $\mathbb{F}_p$. Then, given points $P, Q \in E(\mathbb{F}_p)$, we must find an integer $0 \leq n < \mathrm{ord}(P)$ such that $Q = nP$.

We call n the **Discrete Logarithm** of Q with base P.

Solving ECDLP

"Brute Force" Method

Compute the values n_1P, n_2P, n_3P until finding that value to satisfy $nP = Q$. The expected running time here is $O(p)$, since $\#E(\mathbb{F}_p) = O(p)$. Not very efficient.

Collision Search

Compute two lists for randomly chosen values $n_1, n_2, n_3, ...$

$$\text{List 1: } n_1P, n_2P, n_3P...$$

$$\text{List 2: } Q - n_1P, Q - n_2P, Q - n_3P...$$

until we find a "collision":

$$n_iP = Q - n_jP$$

"Birthday problem": A collision occurs in running time of $O(\sqrt{p})$.

Solving ECDLP (continued)

- As of today, the fastest known method of solving the ECDLP runs in $O(\sqrt{p})$ time. This means that it is not feasible to solve ECDLP in $E(\mathbb{F}_q)$ if $q > 2^{160}$.
- A standard DLP-equivalent difficulty in $\mathbb{F}_q^*$ requires that $q \approx 2^{1000}$.
- ECDLP with $q \approx 2^{160}$ is about as hard as factoring a 1000-bit integer.

In sum, elliptic curve-based cryptography systems require smaller keys for an equal level of security, improving efficiency.

Elliptic Curve Diffie-Hellman Key Exchange (ECDH)

Algorithm

Two parties Alice and Bob agree on an elliptic curve $E(\mathbb{F}_p)$ and a point $P \in E(\mathbb{F}_p)$. Then, they choose secrets n_A, n_B respectively, and compute

$$Q_A = n_A P \text{ and } Q_B = n_B P$$

Upon exchanging Q_A and Q_B, they use their respective secret values n_A, n_B to compute

$$n_A Q_B = n_B Q_A = n_A n_B P,$$

so that $n_A n_B P$ is their shared secret value.

Example

Suppose Alice wants to send Bob a message using the shift cipher, but Alice and Bob do not already share a shift factor K.
To agree on one, they use ECDH to compute a shared point

$$(x, y) \in E(\mathbb{F}_{3851}),$$

and define their shift factor by $K \equiv x \pmod{26}$.

They publicly decide on the elliptic curve

$$E(\mathbb{F}_{3851}) : Y^2 = X^3 + 324X + 1287$$

and a point

$$P = (920, 303) \in E(\mathbb{F}_{3851}).$$

After deriving K, Alice will encrypt her message and send the resulting ciphertext to Bob.

Example (continued)

Alice and Bob then choose secret values $n_a = 1194$, $n_b = 1759$, and respectively compute

$$Q_A = 1194P = (2067, 2178),$$

$$Q_B = 1759P = (3684, 3125).$$

After exchanging these values, Alice and Bob further compute

$$n_a Q_B = 1194(3684, 3125) = (3347, 1242),$$

$$n_b Q_A = 1759(2067, 2178) = (3347, 1242).$$

Since $3347 \equiv 19 \pmod{26}$, we find that $K = 19$.

Example (continued)

Alice now encrypts her message using the shift cipher with $K = 19$, and sends Bob the ciphertext

$$ATOX\ \ T\ \ ZHHW\ \ LNFFXK.$$

Since Bob independently computed $K = 19$, he can decrypt the ciphertext by subtracting 19 modulo 26 from each letter.

After following this procedure, Bob finds that the decrypted message is...

Example (continued)

Acknowledgments

- I would like to extend my gratitude to the organizers of the Directed Reading Program for making this event possible.
- I would especially like to thank my mentor, Ritik Jain, for all of the help and support through this project.