1. Khái niệm số học và cấu trúc đại số nền tảng

Ngày 22 tháng 7 năm 2025

1 Các tập số cơ bản

Tập số nguyên (Integers), ký hiệu $\mathbb{Z}$:
Là tập hợp các số nguyên gồm cả số âm, số không, và số dương, ví dụ:

$$\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Tập số hữu tỉ (Rational numbers), ký hiệu $\mathbb{Q}$:
Là tập các số có thể biểu diễn dưới dạng phân số $\frac{a}{b}$ với $a, b \in \mathbb{Z}$ và $b \neq 0$, ví dụ:

$$\{\ldots, 1, \frac{3}{2}, 2, \frac{22}{7}, \ldots\}$$

Tập số thực (Real numbers), ký hiệu $\mathbb{R}$:
Bao gồm tất cả các số hữu tỉ và vô tỉ, ví dụ:

$$\{2, -4, \frac{6}{13}, \pi, \sqrt{2}, \ldots\}$$

Trường hữu hạn (Finite Fields), ký hiệu $\mathbb{F}$ hoặc $\mathbb{Z}_p^*$:
Là tập hữu hạn gồm các phần tử là số nguyên modulo một số nguyên tố p, có hai phép toán cộng và nhân. Mỗi phần tử (khác 0) đều có phần tử nghịch đảo nhân.

2 Phép toán modulo (Modular Arithmetic)

Định nghĩa: n mod k là phần dư khi chia n cho k.
Ví dụ:

$$25 \bmod 3 = 1, \quad 15 \bmod 4 = 3$$

Phần dư luôn là số không âm nhỏ hơn k.

Lớp tương đương (Equivalence classes):
Các số nguyên được phân thành các lớp tương đương theo modulo k.
Ví dụ với $k = 7$, các số $5, 12, 19$ đều cùng lớp vì cùng dư 5 khi chia cho 7.
Các lớp có dạng:

$$i + k\mathbb{Z} = \{i + km \mid m \in \mathbb{Z}\}$$

với $i = 0, 1, \ldots, k - 1$.

Ý nghĩa: Modular arithmetic là nền tảng của các hàm một chiều trong mật mã, vì tính toán modulo thì dễ nhưng đảo ngược (tìm đầu vào) thì khó.

3 Nhóm (Group Theory)

Định nghĩa nhóm:
Một nhóm $(G, \cdot)$ gồm tập G và phép toán nhị phân $\cdot$ thoả mãn:

- **Tính đóng (Closure):** $\forall a, b \in G, \quad a \cdot b \in G$
- **Tính kết hợp (Associativity):** $\forall a, b, c \in G, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- **Phần tử đơn vị (Identity):** $\exists e \in G$ sao cho $\forall a \in G, \quad a \cdot e = e \cdot a = a$
- **Phần tử nghịch đảo (Inverse):** $\forall a \in G, \quad \exists a^{-1} \in G$ sao cho $a \cdot a^{-1} = a^{-1} \cdot a = e$

Nhóm con (Subgroup):
Một tập con của nhóm cũng thoả mãn đầy đủ các tính chất nhóm.

Nhóm tuần hoàn (Cyclic group):
Là nhóm được sinh bởi một phần tử g, tức là:

$$\{g, g^2, g^3, \ldots, g^{-1}, g^{-2}, \ldots\}$$

Ví dụ: nhóm $(\mathbb{Z}, +)$ với phần tử sinh là 1.

4 Trường (Fields)

Định nghĩa trường:
Một trường $\mathbb{F}$ là một tập hợp với hai phép toán cộng $(+)$ và nhân $(\cdot)$ thoả mãn:

- **Tính kết hợp:** $a + (b + c) = (a + b) + c, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Tính giao hoán:** $a + b = b + a, \quad a \cdot b = b \cdot a$
- **Phần tử đơn vị:** $a + 0 = a, \quad a \cdot 1 = a$
- **Phần tử nghịch đảo:**
  - $\forall a \in \mathbb{F}, \quad \exists -a \in \mathbb{F}$ sao cho $a + (-a) = 0$
  - $\forall a \neq 0, \quad \exists a^{-1} \in \mathbb{F}$ sao cho $a \cdot a^{-1} = 1$
- **Tính phân phối:** $a \cdot (b + c) = a \cdot b + a \cdot c$

Trường hữu hạn:
Trường có số phần tử hữu hạn, ví dụ: $\mathbb{Z}_p$ với p là số nguyên tố. Phép cộng và nhân được thực hiện theo modulo p.

Phần tử sinh trong trường hữu hạn:
Tồn tại phần tử g sao cho lũy thừa của g sinh ra toàn bộ các phần tử trong trường (trừ 0 trong nhóm nhân).

Tóm lại

Phần này cung cấp nền tảng toán học về các loại số, phép toán modulo, và các cấu trúc đại số như nhóm và trường. Đây là các công cụ cơ bản để hiểu cách xây dựng các hàm mật mã và hệ thống chứng minh không tiết lộ (Zero Knowledge Proofs).