

# Discrete Math (क्रिप्टो सिद्धांत)

↳ main base → Set

Number Theory (Crypto, security, probabilistic model, ML/AL etc.)

Graph Theory (Graph networks, google map etc.)

- o -

## What is Set?

↳ an unordered collection of elements

\*  $S_1 = \{2, 4, 6, 10, 8\}$ ,  $|S_1| = 5$  ↗ cardinality of set

\*  $S_{\text{vowel}} = \{a, e, i, o, u\}$  ↗ Roster/Tabular form

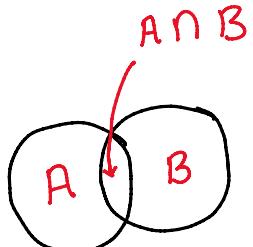
$= \{x : \begin{array}{l} x \text{ is a vowel} \\ \text{in English alphabet} \end{array}\}$  ↗ Set Builder Notation

### Example 1

$S_{\text{name}} = \{s, a, h, i, b\}$ ;  $S_{\text{vowel}} = \{a, e, i, o, u\}$

$\therefore S_{\text{name}} \cap S_{\text{vowel}} = \{a, i\}$

$|S_{\text{name}} \cap S_{\text{vowel}}| = 2$



- o -

## Types of Set

\* Finite Set → size finite.

$\rightarrow S = \{x : 0 < x < 100 \text{ and } x \cdot 2 = 0\}$

\* Infinite Set → size infinite!

$\hookrightarrow S = \{x : x > 0 \text{ and } x \% 2 = 0\}$

\* Subset :  $Y = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$   
 $X = \{1, 4, 7, 9\}$

$$X \subseteq Y$$

\* Proper Subset :  $X \subset Y$

$$X \subseteq Y = X \subset Y \text{ OR } X = Y$$

$$X \subset Y = \dots \text{ AND } |X| < |Y|$$

Power Set

$S = \{1, 2, 3\}$

$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$

$$P(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

$$|P(S)| = 2^{|S|}$$

$${}^3C_0 + {}^3C_1 + {}^3C_2 + {}^3C_3 = 2^3$$

$$1 + 3 + 3 + 1 = 2^3 = 8$$

$${}^nC_n = \frac{n!}{n!(n-n)!}$$

Sum of pascal's  $n^{\text{th}}$  row

$${}^nC_0 + {}^nC_1 + {}^nC_2 + \dots + {}^nC_n = 2^n$$

IEP  $\rightarrow$  Inclusion-Exclusion Principle

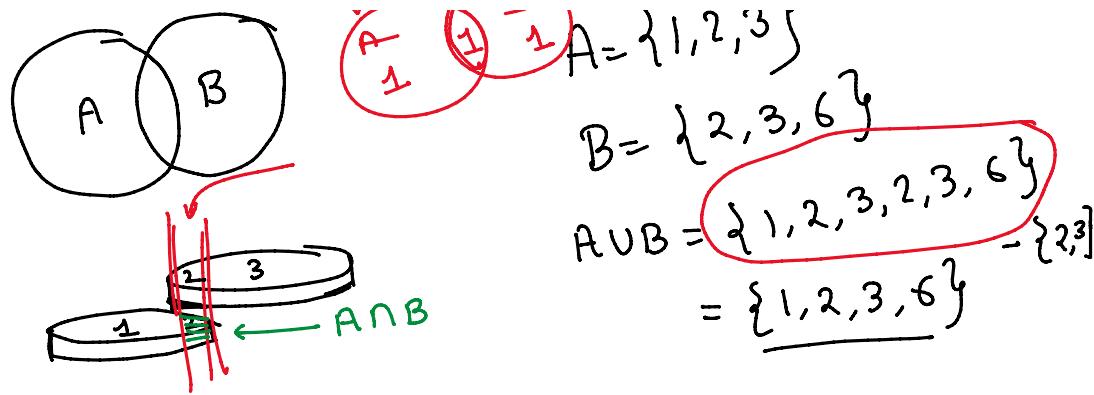
$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$A = \{1, 2, 3\}$

$n(A) = 3$

$n(B) = 2$

$n(A \cap B) = 1$



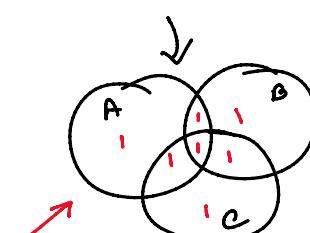
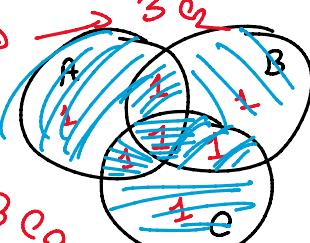
$$\begin{aligned}
 |A \cup B| &= |A| + |B| - |A \cap B| \\
 &= 3 + 3 - 2 \\
 &= 4
 \end{aligned}$$

$$\underbrace{n(A \cup B \cup C)}_{=} = n(A) + n(B) + n(C) \rightarrow 3 \rightarrow 3c_1$$

$$-n(A \cap B) - n(A \cap C) - n(B \cap C) \rightarrow 3 \rightarrow 3c_2$$

$$+ n(A \cap B \cap C) \rightarrow 1 \rightarrow 3c_3$$

$$2^n - 3c_0 = \boxed{2^n - 1}$$



This is our target!

$$\left\lfloor \frac{15}{2} \right\rfloor = 7$$

$$\left\lfloor \frac{15}{3} \right\rfloor = 5$$

$$\left\lfloor \frac{15}{6} \right\rfloor = 2$$

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15$$

$$n(P_1 \cup P_2) = n(P_1) + n(P_2) - n(P_1 \cap P_2)$$

$P_1 = \{2, 4, 6, 8, 10, 12, 14\}$   
 $P_2 = \{3, 6, 9, 12, 15\}$

$$\begin{aligned}
 n(P_1 \cup P_2) &= n(P_1) + n(P_2) - n(P_1 \cap P_2) \\
 &= \left\lfloor \frac{N}{P_1} \right\rfloor + \left\lfloor \frac{N}{P_2} \right\rfloor - \left\lfloor \frac{N}{\text{Lcm}(P_1, P_2)} \right\rfloor
 \end{aligned}$$

$P_2 = \{3, 6, 9, 12, 15\}$   
 $P_1 \cup P_2 = ?$   
 $= \left\lfloor \frac{15}{2} \right\rfloor + \left\lfloor \frac{15}{3} \right\rfloor - \left\lfloor \frac{15}{6} \right\rfloor = 10$

$$N - n(P_1 \cup P_2)$$

Disjoint Set Union: (DSU)

$$|A \cap B| = 0$$

$$A \cap B = \emptyset$$

