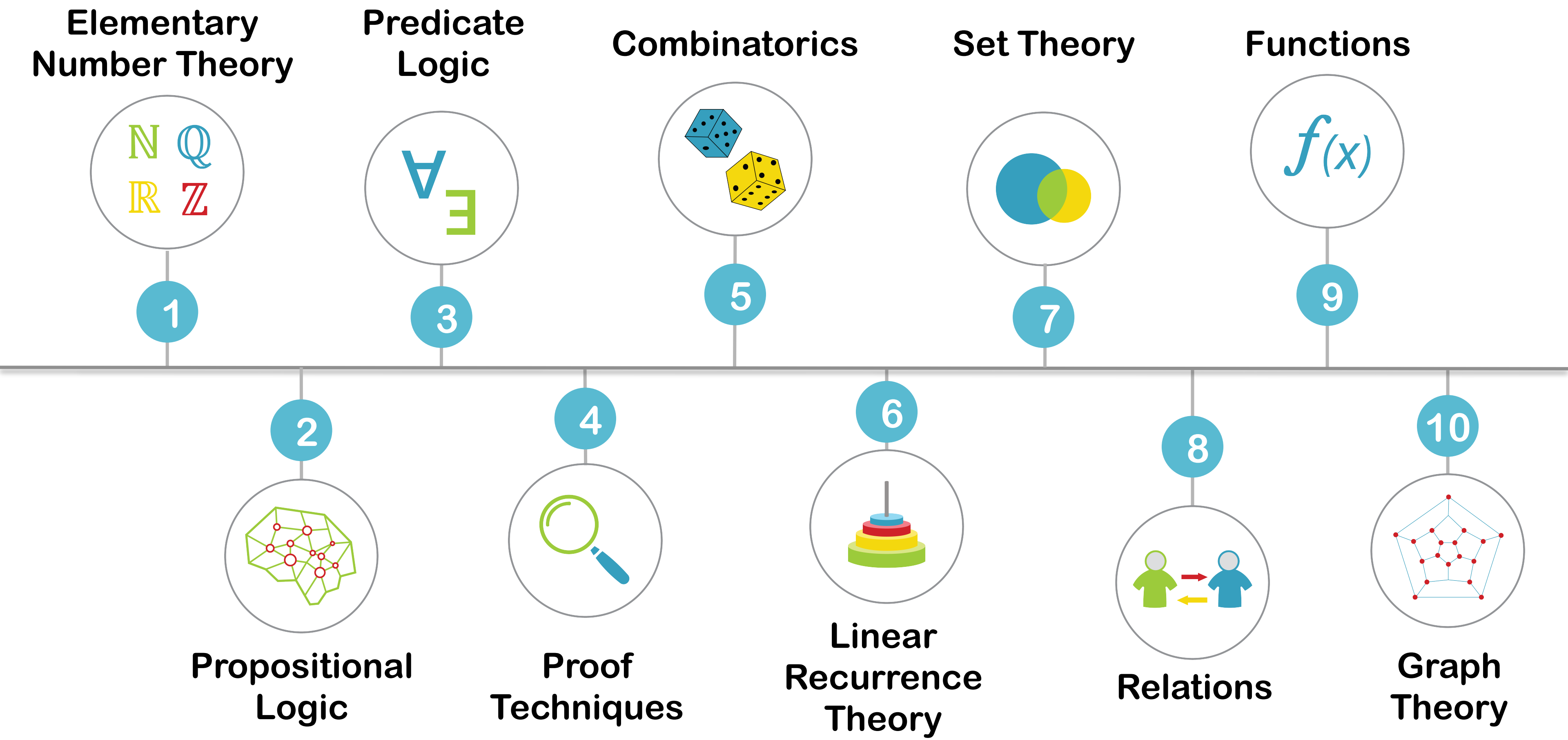
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Discrete Mathematics
MH1812

Final Review

Dr. Guo Jian

Your Learning Roadmap



Elementary Number Theory

- Recognise different types of numbers (natural, integer, real, rational, irrational, prime, even, modulo n).
- Use Euclidean division to find the remainder.
- Determine which integers are congruent modulo a positive integer.
- Decide whether particular sets of numbers are closed under a given operator.

mod 3

$\{0, 1, 2\}$

5 mod 3

= 2

$\lfloor \frac{10}{3} \rfloor = 3$

$10 - 3 * 3 = 1$

$\lfloor \frac{5}{3} \rfloor = 1$

$5 - 1 * 3 = 2$

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

"$\triangle$" $\quad x \triangle y = x \cdot y \bmod 4$

Is "$\triangle$" closed under A

$\bmod 4 \Rightarrow \{0, 1, 2, 3\}$

$\underset{\underset{x}{\Downarrow}}{2} * \underset{\underset{y}{\Downarrow}}{2} \bmod 4 = 0 \notin A$

$\therefore$ "$\triangle$" is not closed.

$$\{12x + 25y \mid x, y \in \mathbb{Z}\} \overset{?}{=} \mathbb{Z} \; ?$$

$$\begin{cases} x = -2 \\ y = 1 \end{cases} \Rightarrow \boxed{12 \cdot (-2) + 25 \cdot 1} = 1$$

To find $a \in \mathbb{Z}$

$$a = a \cdot 1 = a \cdot (12 \cdot (-2) + 25 \cdot 1)$$

$$= 12 \cdot \underbrace{(-2a)}_{x} + 25 \cdot \underbrace{a}_{y}$$

$5^{2018} \bmod 7$

$5^1 \bmod 7 = 5$

$5^2 \bmod 7 = 4$

$5^3 \bmod 7 = 6$

$5^4 \bmod 7 = 2$

$5^5 \bmod 7 = 3$

$5^{\boxed{6}} \bmod 7 = \boxed{1}$

$5^{2018} \bmod 7$

$= 5^{\underline{2018 \bmod 6}} \bmod 7$

$= 5^2 \bmod 7$

$= \boxed{4}$

Propositional Logic

Proposition (Compound Propositions)

Paradox

Contradiction

Tautology

Equivalent Expressions

Basic logical operators (and De Morgan's laws):

Negation $\neg$

Conjunction $\wedge$

Disjunction $\vee$

$\neg(A \wedge B) = \neg A \vee \neg B$

$\neg(A \cup B) = \neg A \wedge \neg B$

- Useful logical equivalence laws:
  - Proving equivalence using these laws
- Conditional and biconditional operators:
  - Sufficient and necessary conditions
- Operator precedence

If A, then B

$A \to B$

Only if A, then B

$A \leftarrow B$

A if and only if B

$A \leftrightarrow B$

- Arguments:
  - Valid arguments
  - Invalid arguments
  - Counterexample
  - Fallacy
- Inference rules:
  - Derive conclusions from a bunch of information
  - Some basic inference rules

Predicate Logic

- Predicates:
  - Statements with variables
- Quantifiers:
  - Use to express a property about "all" and "some"
  - Universal $\forall$
  - Existential $\exists$

- Negation of quantification

$\neg(\forall x, P(x))$
$\equiv \exists x, \neg P(x)$

$\neg(\exists x, P(x))$
$\equiv \forall x, \neg P(x)$

- Determining truth value of a quantification:
  - Methods for proving quantified statements

- Conditional quantification

Basic Inference Rules

$\exists x, p(x)$

$p(a)$

Existential Instantiation

Any a $p(a)$

$\equiv \forall x, p(x)$

Universal Generalisation

$p(a)$

$\exists x, p(x)$

Existential Generalisation

$\forall x, p(x)$

any a

$p(a)$

Universal Instantiation

Proof Techniques

- Generic proof techniques:
  - Direct proof
  - Mathematical induction (complete induction)
  - Contradiction (contrapositive)

$p \to q \qquad \neg q \to \neg p$

$$\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

$n \geq 1, n \in \mathbb{Z}$

Basis Step $n = 1$

$\text{LHS} = \sum_{i=1}^{n=1} i = 1 = \cancel{\frac{1 \cdot (1+1)}{2}}$

$\text{RHS} = \frac{1 \cdot (1+1)}{2} = 1$

$\text{LHS} = \text{RHS}$

Inductive Step:

$n = k$

$$\boxed{\sum_{i=1}^{n=k} i = \frac{k \cdot (k+1)}{2}}$$

Then for $n = k+1$

$$\text{LHS} = \sum_{i=1}^{n=k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k \cdot (k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2} = \text{RHS}$$

Combinatorics

- **Principle of counting**
- **Permutations (with order)**
- **Combinations (without order)**

$$C(n,r) = \frac{n \cdot (n-1) \cdot \cdots (n-r+1)}{r \cdot (r-1) \cdot (r-2) \cdot \cdots \cdot 1}$$

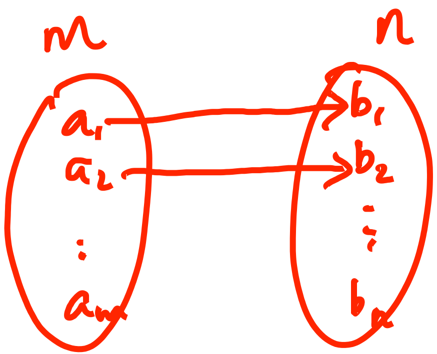
$$= \frac{n!}{(n-r)! \cdot r!}$$

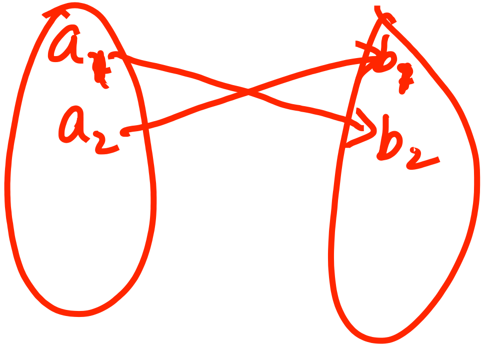
$$P(n,r) = n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)$$

$$= \frac{n!}{(n-r)!}$$

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 1$$

injective functions





$P(n, m)$

Linear Recurrence

- Definition of linear recurrence
- Backtracking
- Characteristic equation

$a_1 = 2. \quad a_2 = 4$

$a_n = 5a_{n-1} - 6a_{n-2}$

1. $\boxed{x^2 = 5x - 6}$

$x^2 - 5x + 6 = 0$

2. $\boxed{(x-2)(x-3) = 0}$

two solutions

3. $\boxed{x = 2, \quad x = 3}$

4. $\boxed{a_n = u \cdot 2^n + v \cdot 3^n}$

5. $a_1 = 2 = u \cdot 2^1 + v \cdot 3$

$= 2u + 3v$

$a_2 = 4 = u \cdot 2^2 + v \cdot 3^2$

$= 4u + 9v$

Solving it: 6. $\boxed{u = 1, \quad v = 0}$

7. $\boxed{a_n = 2^n}$

Set Theory

- **Principle of counting**

- **Permutations (with order)**

- **Combinations (without order)**

- **Set identities**

- **Prove set identities:**
  3 – **Each others' subset**
  2. – **Set identity theorems**
  1 – **Membership table**

(# sets ≤ 4)

write the name of the theorems

$A - B = A \cap \overline{B}$

$\forall x \in A - B \supseteq$

$x \in A$ ~~and~~ AND $x \notin B$

$x \in A$ AND $x \in \overline{B}$

$x \in A \cap \overline{B}$

Relations

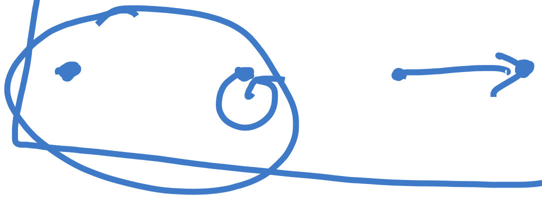
- Binary relations:
  - Inverse and composition
  - Graphical representation
- Properties:
  - Reflexivity
  - Symmetry
  - Transitivity
- Equivalence relations: equivalence class
- Partial order: antisymmetry

$\forall x \in A$ Reflexive

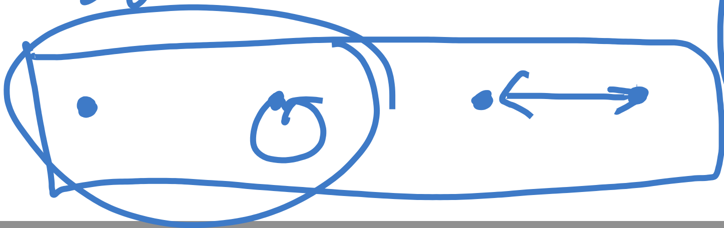
$(x,x) \in R$?

for all x

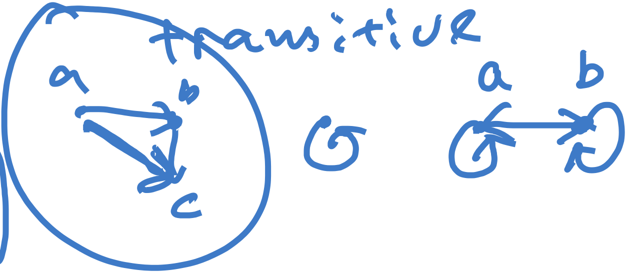
Anti-Sym



Sym



transitive



- **Equivalence relations: equivalence class** R S T

- **Partial order: antisymmetry** R A T

Functions

$f \circ \boxed{g(x)}$

- Functions:
  - Domain
  - Codomain
  - Image
  - Preimage
  - Range

$f(x) = x^2$

- Injective functions (one-to-one)
- Surjective functions (onto)

$\boxed{f(x_1) = f(x_2)} \overset{?}{\Rightarrow} \boxed{x_1 = x_2}$

$x_1^2 = x_2^2 \Rightarrow x_1^2 - x_2^2 = 0,\quad (x_1 - x_2)\cdot(x_1 + x_2) = 0$

$x_1 = x_2$ $\boxed{\text{or} \quad x_1 = -x_2}$

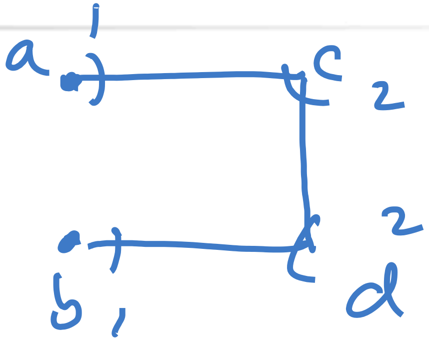
- Bijective functions
- Identify and inverse functions
- Composition of functions and their properties
- Ceiling and floor functions
- Pigeonhole principle
- Countable and uncountable sets

$\lceil \frac{n}{x} \rceil$

n pigeon

x ~~pigeonhole~~

Graph Theory



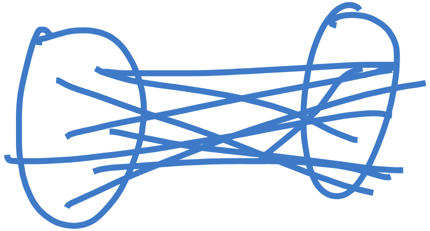
- Types of graphs:
  - Simple graph
  - Multigraph
  - Directed (multi) graph

- Euler path, Euler circuit and Euler theorem

2e = total degree

go through every edge exactly once

- Types of graphs:
  - Complete graph
  - Bipartite graph



- Handshaking theorem

- A graph represented by a matrix

- Basic definitions: graph, vertex (node), edge, loop
- Node degree, graph degree, handshaking theorem
- Types of graphs: simple, multigraph, (un)directed, complete, bipartite
- Euler path and circuit
- Hamiltonian path and circuit
- Adjacency matrix and graph isomorphism

1 MO

Extra

Tutorial

CA