MATH1064 Study Notes

University of Sydney
Semester 2, 2025
MATH1064

Happy studying!

Contents

1 Introduction to Discrete Maths and Set Theory

1.1 Introduction to Discrete Maths

Discrete maths is the study of "discrete structures", this includes objects which are:

- Countable or listable
- Distinct and unconnected.

There are two objectives of MATH1064:

1. Develop mathematical reasoning skills. This involves using **logic and proofs**, and **rigorously** (exhausting all possibilities) finding solutions to problems.
2. Study **discrete structures** and their properties including:
    - Sets and functions
    - Prime numbers and modular arithmetic
    - Graphs and networks
    - Counting and probability.

1.2 Introduction to Set Theory

1.2.1 Definitions

Definition 1 (Set)**.** A **set** S is a collection of objects, called **elements** of S.

- If x is an element of S, $x \in S$
- If not, then $x \notin S$.

Sets can be finite or infinite:

- Example (finite): $S = \{2, 3, 5\}$
- Example (infinite): $S = \{0, 1, 2, \dots\} = \mathbb{N}$

Definition 2 (Set Equivalence)**.** Two sets S and T are said to be equal if they contain the same elements, regardless of **order** or **repetition**.

- Example 1:

$$S = \{1, 1, 5, 3\}$$
$$T = \{1, 3, 5\}$$
$$S = T$$

- Example 2:

$$S = \{-1, 0, 1, \dots\}$$
$$T = \{0, 1, \dots\}$$
$$S \neq T$$

Definition 3 (Empty Set)**.** The **empty set** is a unique set containing no elements. $\emptyset = \{\}$.

Definition 4 (Singlton Set)**.** A **singleton set** has only one element, e.g. $S = \{x\}$ or $S = \{x, x, x\}$

1.2.2 Unpacking Sets

Sets can contain other sets as elements, inner sets are considered distinct elements even if their contents are the same as other elements in the outer set. This is because when we unpack sets, we only remove outer curly braces { }.

$$S = \{1, 2, \{1\}\}$$
$$|S| = 3 \text{ distinct elements}$$

1.2.3 Sets with Properties

We can describe sets using **set builder notion** which indicates the properties of a set.

$$A = \{x \in S \mid P(x)\}$$

"The set A consists of all elements x of S such that x has property P".

Examples:

$$\{x \in \mathbb{N} \mid 3 \leq x \leq 5\} = \{3, 4, 5\}$$
$$\{y \in \mathbb{Z} \mid y = 2k \text{ for some } k \in \mathbb{Z}\} = \{\dots, -2, 0, 2, \dots\}$$
$$\{2z + 1 \mid z \in \mathbb{N}\} = \{1, 3, 5, \dots\}$$

1.2.4 Russel's Paradox

Define a set $T = \{S, set \mid S \notin S\}$. The set T contains any set S which does not contain itself.

Consider if $T \in T$:

- If $T \in T$: T does not satisfy the condition.
- If $T \notin T$: T does satisfy the condition, thus $T \in T$ according to our definition.

This induces a contradiction, hence demonstrating that we need **axioms** which **rigorously** state how to define and build sets.

1.2.5 Operations on Sets

Definition 5 (Union)**.** Given two sets S and T, the **union** of S and T is the set containing all elements from S and T. This is written as $S \cup T$ where $x \in S$ **OR** $x \in T$.

- Example 1: $\{1,2,3\} \cup \{2,5\} = \{1,2,3,5\}$
- Example 2: $\{0,1,2,\dots\} \cup \{0,-1,-2,\dots\} = \mathbb{Z}$

Definition 6 (Intersection)**.** Given two sets S and T, the **intersection** of S and T is the set of elements belonging to both S and T. This is written as $S \cap T$ where $x \in S$ **AND** $x \in T$.

- Example 1: $\{1,2,3\} \cap \{2,5\} = \{2\}$
- Example 2: $\{1,2,3,\dots\} \cap \{-1,-2,-3,\dots\} = \emptyset$

Multiple unions and intersections can be taken at a time.

$$\begin{aligned}\bigcup_{i=1}^{3}\{i,2i\} &= \{1,2\} \cup \{2,4\} \cup \{3,6\} \\ &= \{1,2,3,4,6\}\end{aligned}$$

$$\begin{aligned}\bigcap_{i=1}^{3}\{i,i+1,i+2\} &= \{1,2,3\} \cap \{2,3,4\} \cap \{3,4,5\} \\ &= \{3\}\end{aligned}$$

Formally, for sets $A_1, A_2, \dots, A_i$ we define the set A_i as:

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_k \text{ for SOME } k \geq 1\}$$

That is for an infinite series of unions, x is an element that appears **at least once** in the sets A_k for $k \geq 1$.

And similarly for intersections, we define the set A_i as:

$$\bigcap_{i=1}^{\infty} A_i = \{x \mid x \in A_k \text{ for ALL } k \geq 1\}$$

That is, for an infinite series of intersections, x is an element which appears in **all** sets A_k for $k \geq 1$.

1.2.6 Subsets

Definition 7 (Subsets)**.** A set S is a **subset** of another set T if every element of S is an element of T. This is written as $S \subset T$.

Additionally, if S is a subset of T but is not equal to T, then it is considered a **proper subset**, denoted as $S \subseteq T$.

For example,

$$S = \{2, 4, 6\}$$
$$T = \{2, 4, 6, 8\}$$
$$S \subseteq T, \text{ since } 8 \notin S$$

1.2.7 Proving Subset Relationships

To prove $S \subseteq T$, we need to:

1. Take an arbitrary element of S, which we call x
2. Show that $x \in T$

Example: Let S and T be sets where,

$$S = \{2n \mid n \in \mathbb{N}, n \geq 1\}$$
$$T = \{2^m \mid m \in \mathbb{N}\}$$

Proof. Let $x \in S$, by definition $x = 2^n$ for some $n \geq 1$.

$$x = 2^n$$
$$x = 2(2^{n-1}), \text{ rewriting } x$$

Since $n \geq 1$, $n - 1 \geq 0$ meaning that $n - 1 \in \mathbb{N} \implies 2^{n-1} \in \mathbb{N}$. Because 2^{n-1} is a natural number, we can rewrite $x = 2m$ where $m = 2^{n-1}$ as we know $m \in \mathbb{N}$, $x \in T \implies S \subseteq T$. □

1.2.8 Proving Equality Relationships

To prove that $S = T$, we need a **"double containment proof"** which shows that both sets have the same elements, that is:

1. Every $x \in S$ also satisifes $x \in T$
2. Every $x \in T$ also satisfies $x \in S$

Example: Let S and T be sets where,

$$S = \{2m + 1 \mid m \in \mathbb{Z}\}$$
$$T = \{2r - 1 \mid r \in \mathbb{Z}\}$$

Proof. Show $S \subseteq T$. Let $x \in S$, then $x = 2m + 1$ for some $m \in Z$.
Let $r = m + 1$.

$$\begin{aligned} x &= 2m + 1 \\ x &= 2m + 2 - 1, \text{ rewriting } x \\ x &= 2(m + 1) - 1, \text{ notice } m + 1 = r \\ x &= 2r - 1, \text{this is the same as } x \in T \end{aligned}$$

$x = 2r - 1$ for some $r \in \mathbb{Z}$. Thus, $x \in T \implies S \subseteq T$. □

Proof. Show $T \subset S$. Let $x \in T$, then $x = 2r - 1$ for some $r \in \mathbb{Z}$.
Let $m = r - 1$.

$$\begin{aligned} x &= 2r - 1 \\ x &= 2r - 2 + 1 \\ x &= 2(r - 1) + 1 \\ x &= 2m + 1 \end{aligned}$$

$x = 2m + 1$ for some $m \in \mathbb{Z}$. Thus, $x \in S \implies T \subseteq T$. □

Since $S \subseteq T$ and $T \subseteq S$, the two sets must have the same elements and are equal, $S = T$.

1.3 More Set Theory

1.3.1 Cardinality

The **cardinality** of a set S in a rough sense refers to the size of S, i.e. the no. of elements in S.

- If S is finite, then $|S|$ is the number of distinct elements in S.
- If S is infinite, then we write $|S| = \infty$.

Note that there can be **different infinite cardinalities**, or sizes of infinities. A basic example of this is the set of natural numbers $\mathbb{N}$ compared to the set of real numbers $\mathbb{R}$.

1.3.2 Set Differences

Definition 8 (Set Difference)**.** Given two sets S and T, the **set difference** is the set of elements $x \in S$ and $x \notin S$. This is written as $S \backslash T$ or $S - T$.

- Example 1: $\{1, 2, 3\} \backslash \{2, 5\} = \{1, 3\}$
- Example 2: $\{0, 1, 2, \dots\} \backslash \{0, -1, -2, \dots\} = \{1, 2, \dots\}$
- Example 3: $\mathbb{N} \backslash \mathbb{Z} = \emptyset$

1.3.3 Universal Set

Definition 9 (Universal Set)**.** Let $\mathbb{U}$ be some **universal set** which is the set containing all elements of which other sets are subsets. The universal set is context dependent.

- $\mathbb{U} = \mathbb{Z}$, if working with number theory
- $\mathbb{U} = \mathbb{R}^2$, if working with plane geometry

1.3.4 Complementary Set

Definition 10 (Complement)**.** For a set $S \subseteq \mathbb{U}$, the **complement** of $S \in \mathbb{U}$ is given by $x \in \mathbb{U}$ where $x \notin S$. This is written as $\overline{S}$ or $S^{\complement}$.

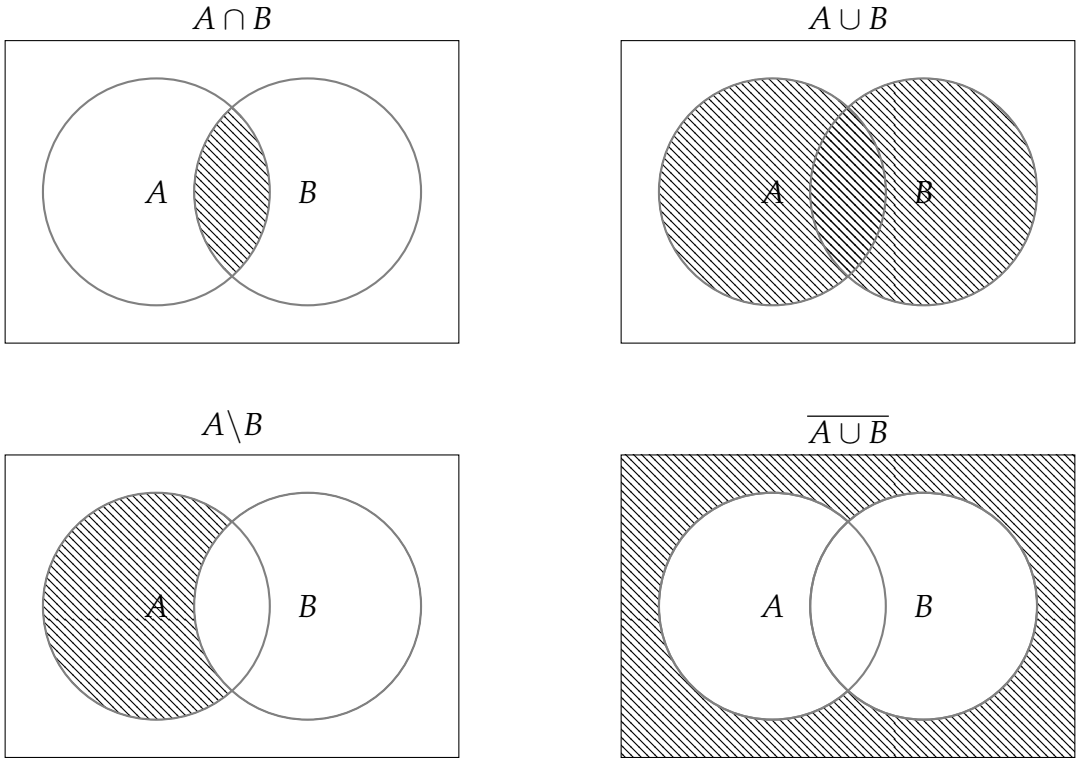
In other words, $\overline{S}$ is the set containing all elements not in S, where the range of elements considered is constrained by $\mathbb{U}$. This resolves the Russel Paradox.

For example, if $\mathbb{U} = \mathbb{Z}$:

- $\overline{\{1,2,3\}} = \{\ldots,-1,0,4,\ldots\}$
- $\overline{\{x \in \mathbb{Z} \mid x > 0\}} = \{x \in \mathbb{Z} \mid x < 0\}$
- $\overline{\mathbb{Z}} = \varnothing$

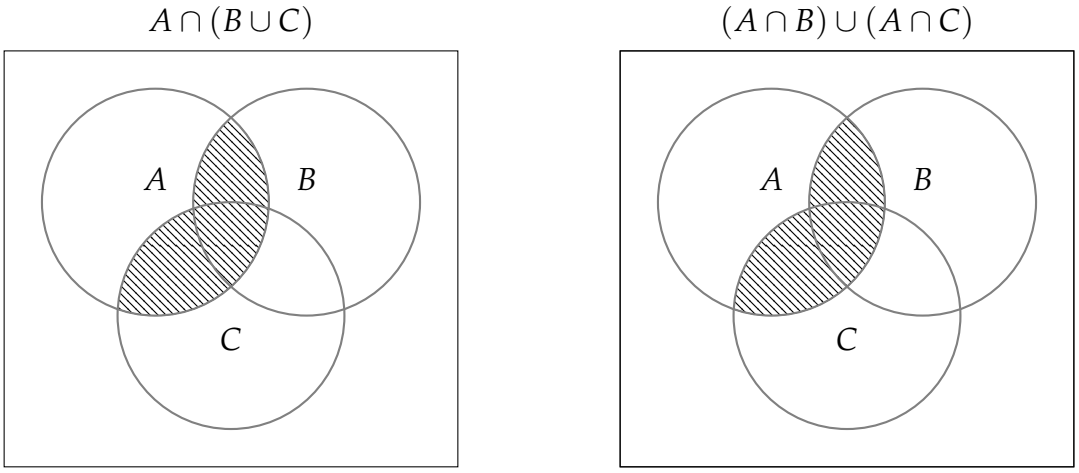
1.3.5 Venn Diagrams

Venn Diagrams are tools used to visualise relationships between sets.



Venn diagrams are useful for intuition and can be used to guide proofs, but are not sufficient as rigorous proofs in of themselves.

Example: Prove if $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



Proof. Double Containment. First, show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.
Let $x \in A \cap (B \cup C)$:

$$\begin{aligned} \text{Then } x \in A \text{ and } x \in (B \cup C) \\ x \in (B \cup C) &\implies x \in B \text{ or } x \in C \\ \text{if } x \in B, x \in (A \cap B) &\implies x \in (A \cap B) \cup (A \cap C) \\ \text{if } x \in C, x \in (A \cap C) &\implies x \in (A \cap C) \cup (A \cap B) \\ &\implies A \cup (B \cap C) \subseteq (A \cap B) \cup (A \cap C) \end{aligned}$$

This proof works because we know that if $x \in (A \cap B)$, then suppose we expand the set $(A \cap B)$ by including another arbitrary set, say $(A \cap C)$. We can implicitly assume x is an element of $(A \cap B) \cup (A \cap C)$ since we are simply expanding the scope of the set.

Second, show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
Let $x \in (A \cap B) \cup (A \cap C)$:

$$\begin{aligned} \text{Then } x \in A \text{ and } x \in B \\ &\implies x \in (B \cup C) \\ &\implies x \in A \cap (B \cup C) \end{aligned}$$

$$\begin{aligned} &\text{Then } x \in A \text{ and } x \in C \\ &\implies x \in (C \cup B) \\ &\implies x \in A \cap (C \cup B) \end{aligned}$$

Thus, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, indicating that both sets are equal.

□

1.3.6 Set Identities

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $A \cap (A \cup B) = A$

2 Week 2

2.1 Power Sets and Cartesian Planes

2.1.1 Power Set

Definition 11 (Power Set)**.** For a set S the **power set** of S is the set which contains all possible subsets of S. This is denoted as $P(S) = \{A \mid A \subseteq S\}$.

For example,

- $S = \{a, b\} \implies P(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $S = \emptyset \implies P(S) = \{\emptyset\}$
- $S = \{1, 2, 3\} \implies P(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Theorem 1 (Cardinality of the Power Set)**.** *Let S be a finite set with $|S| = n$, then $|P(S)| = 2^n$*

2.1.2 Cartesian Product

Definition 12 (Cartesian Product)**.** For two sets A and B, the cartesian product $A \times B$ is given by the set of ordered pairs, $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Note: in ordered pairs, the order of elements, and repetition matter (like cartesian coordinates).

Example: $A = a, b. B = 1, 2$

- $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$
- $B \times A = \{(1, a), (1, b), (2, a), (2, b)\}$

Theorem 2 (Cardinality of Cross Product)**.** *The cardinality of the cross product of two sets A and B is given by $|n \times m|$ where $|A| = n$ and $|B| = m$.*

The cross product of an empty set is always the empty set. For example, if $A = \emptyset$, $B = \{1, 2\}$, then $A \times B = \emptyset$.

$A \times B = B \times A \iff A = B$ or when A or $B = \emptyset$.

Proof. If A or $B = \emptyset$, then there is nothing to prove.

Otherwise, assume $A \times B = B \times A$.

Show $A \subseteq B$.
Let $x \in A$ and choose some $y \in B$:

$$\begin{aligned} &\text{Then } (x,y) \in A \times B \\ A \times B = B \times A \implies &(x,y) \in B \times A \\ \implies &x \in B \\ \implies &A \subseteq B \end{aligned}$$

Show $B \subseteq A$.

$$\begin{aligned} &(y,x) \in B \times A \\ A \times B = B \times A \implies &(y,x) \in A \times B \\ \implies &y \in A \\ \implies &B \subseteq A \end{aligned}$$

Therefore, $A = B$ by double containment.

□

2.1.3 Functions

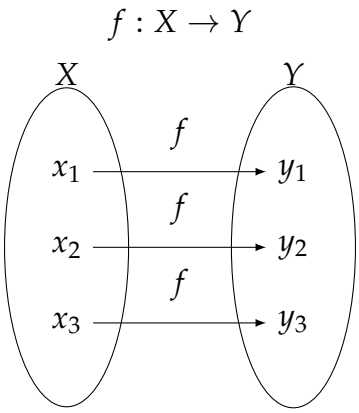
Definition 13 (Function)**.** Given two sets X and Y, the function f from X to Y, written as $f : X \to Y$, maps each $x \in X$ to exactly one $y \in Y$ (see vertical line test).

Important Criteria:

- Every $x \in X$ maps somewhere, i.e. $X \to Y$.
- Every $x \in X$ maps to **at most one** $y \in Y$.

Examples:

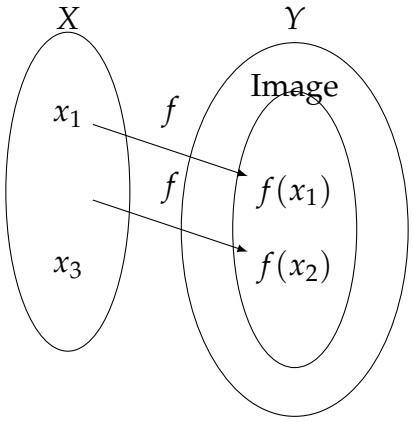
- $f : \mathbb{N} \to \mathbb{N}, f(n) = n!$ is a function
- $f : \mathbb{R} \to \mathbb{R}, f(x) = \ln x$ is not a function as $f(x)$ is undefined for $x < 0$
- $f : \mathbb{Q} \to \mathbb{N}, f(\frac{n}{m}) = n$ is not a function as there are multiple ways to write the same input with different outputs, e.g. $\frac{3}{2} = 3$ but $\frac{6}{4} = 6$.



2.1.4 Function Terminology

Let $f : X \to Y$ be a function. Then we say:

- X is called the **domain** of f
- Y is called the **co-domain** of f
- $f(x) \in Y$ is called the **image** of X (also called range).



Similarly, the **pre-image** of a y is the set of all input values which map to the co-domain Y. This is written as $f^{-1}(y) = \{x \in X \mid f(x) = y\} \subseteq X$. In essence, it explains where does y come from under the function $f(x)$.

2.1.5 Identity Function

Definition 14 (Identity Function)**.** The **identity function** is a function which maps a set to iteself. For any set S, $i_x : X \to X$ is defined by $i_x(a) = a, a \in X$.

2.1.6 Floors and Ceilings

Definition 15 (Floor)**.** For $x \in \mathbb{R}$, the floor of x is the unique integer n such that $n \leq x \leq n+1$. In essence, it is "rounding down" x in terms of value. It is written as $\lfloor x \rfloor$.

Definition 16 (Ceiling)**.** For $x \in \mathbb{R}$, the ceiling of x is the unique integer m such that $m-1 \leq x \leq m$. In essence, it is "rounding up" x in terms of value. It is written as $\lceil x \rceil$.

Note: both floor and ceiling are functions $f : \mathbb{R} \to \mathbb{Z}$. Additionally, for $x < 0$, the rounding up/down of these functions are reversed.

Examples:

- $\lfloor 2.5 \rfloor = 2$
- $\lfloor -2.5 \rfloor = -3$
- $\lceil 2.5 \rceil = 3$
- $\lceil -2.5 \rceil = -2$

2.2 Properties of Functions

2.2.1 Equality of Functions

Definition 17 (Equal Functions)**.** Two functions, $f : X \to Y$ and $g : X \to Y$ are said to be equal if $f(x) = g(x)$ for all $x \in X$.

Example: f and g are equal.

- $f(x) = n!$
- $g(x) = \frac{(n+1)!}{n+1} = \frac{(n+1)n!}{n+1} = n!$

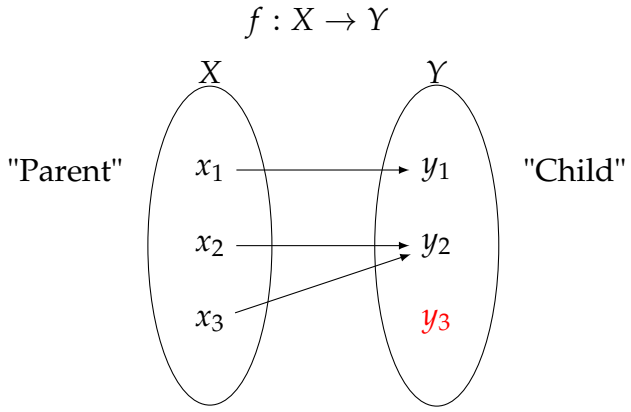
Example: f and g are not equal (not same co-domain).

- $f : \mathbb{N} \to \mathbb{N}, f(n) = n^2$
- $g : \mathbb{N} \to \mathbb{R}, f(n) = n^2$

2.2.2 Surjective/Onto

Definition 18. A function $f : X \to Y$ is considered **onto** or **surjective** if for all $y \in Y$, there exists some $f(x) = y$, $x \in X$. In other words, the co-domain has no orphans; every y is the image of at least one $f(x)$.

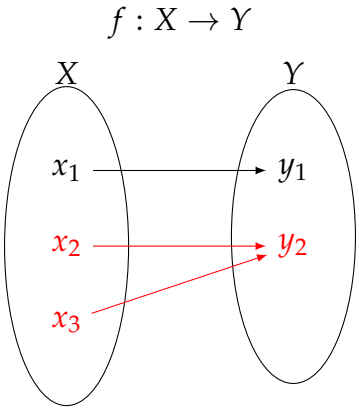
Example:
The below function is **not** a surjective function since y_3 is "orphaned".



2.2.3 Injective/One-to-One

Definition 19. A function $f : X \to Y$ is considered **one-to-one** or **injective** if $f(x_1) = f(x_2)$ implies $x_1 = x_2$ for all $x_1, x_2 \in X$. In other words, different elements in X must map to different images in Y (two elements can't map to same place).

Example: The function below is **not** an injective function since x_2 and x_3 map to y_2, and $x_2 \neq x_3$.

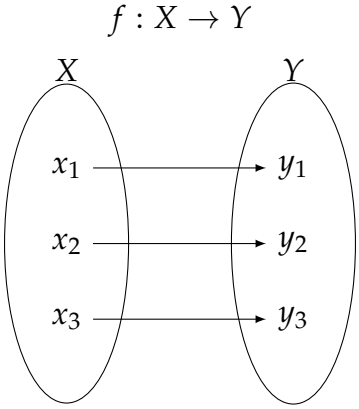


2.2.4 Bijective

Definition 20. A function is said to have a **one-to-one correspondence** or **bijective** if it is both injective and surjective. In other words, if all elements $x \in X$ are paired

with a unique $y \in Y$.

Example: The below function is bijective.



2.2.5 Proving Properties of Functions

Property	**Proving**	**Disproving**
Surjective	Take any arbitrary $y \in Y$, construct some $x \in X$ so that $f(x) = y$	Find a counterexample, $y \in Y$ and show $y \neq f(x)$ for any $x \in X$
Injective	Assume $f(x_1) = f(x_2)$and deduce $x_1 = x_2$	Find a counterexample, $x_1, x_2 \in X$, where $x_1 \neq x_2$ but $f(x_1) = f(x_2)$
Bijective	Prove both	Disprove at least one

Example: Let $f, g : \mathbb{N} \to \mathbb{N}$. Prove if f and g are injective and surjective.

$f(n) = n^2$	
Surjective?	No, the function is not surjective as the image of x only covers squares, whilst the codomain is $y \in \mathbb{N}$. For example, let y be 3, then $f(n) = 3$, $n = \pm\sqrt{3}$, but $\pm\sqrt{3} \notin \mathbb{N}$.
Injective?	Yes the function is injective according to the proof. $\begin{aligned} \text{Assume } f(n) &= f(m) \\ \implies n^2 &= m^2 \\ n^2 - m^2 &= 0 \\ (n+m)(n-m) &= 0 \\ \implies n = -m \text{ or } m &= -n \\ \text{but } n \in \mathbb{N}, \text{ so } n &\neq -m \end{aligned}$ Since n can only equal m, we know that the function is injective.

$g(n) = \lvert n - 1 \rvert$	
Surjective?	Yes, the function is surjective according to the proof. $\begin{aligned} \text{Let } y &\in \mathbb{N} \\ \text{If } y \in \mathbb{N}, \text{ then } y+1 &\in \mathbb{N} \\ g(y+1) &= \lvert (y+1) - 1 \rvert \\ &= \lvert y \rvert \\ &= y \end{aligned}$
Injective?	No, the function is not injective, consider $g(n) = 1$, then $g(0)$ and $g(2)$ both satisfy $f(n) = 1$, but $0 \neq 2$.

2.2.6 Functions and Finite Sets

Let X, Y be two finite sets, and $f : X \to Y$.

- If f is **injective**, then $|X| \leq |Y|$
- If f is **surjective**, then $|X| \geq |Y|$
- If f is **bijective**, then $|X| = |Y|$

2.2.7 Compositions of Functions

Definition 21 (Composite Function)**.** Let $f : X \to Y$ $g : Y \to Z$ be two functions. The composition is written $g \circ f : X \to Z$

Example: Let $f : \mathbb{R}^2 \to \mathbb{R}, f(x,y) = xy$ and $g : \mathbb{R} \to \mathbb{R}^2, g(x) = (\sin x, x)$ be functions.

$$\begin{aligned} f \circ g &: \mathbb{R}^2 \to R^2 \\ f(g(x)) &= f((\sin x, x)) \\ &= \sin x \times x \end{aligned}$$

$$\begin{aligned} g \circ f &: \mathbb{R} \to \mathbb{R} \\ g(f(x)) &= g(xy) \\ &= (\sin xy, xy) \end{aligned}$$

2.3 Sequences

2.3.1 Sequences

Definition 22 (Sequence)**.** A **sequence** is an ordered list of data. That is, given a set S, a sequence in S is a function $f : I \to S$ where $I \subseteq \mathbb{Z}$ (we can assign a numerical order for elements in the set S).

Notation: we use letters and subscripts to indicate elements of a sequence, for example $a_1 = f(1), a_2 = f(2), a_n = f(n)$. The terms of a sequence are its elements.

2.3.2 Equality of Sequences

To prove that two sequences, p_n and b_n are equal sequences, we need b_n in closed form, and p_n as a recursive sequence. Then we need to show that b_n satisfies the recursion relation and initial condition.

Example:

- Let $(p_n) = (2p_{n-1} + 1)$, where $p_1 = 1$
- Let $(b_n)_{n \geq 1} = (2^n - 1)$

Prove $p_n = b_n$
Initial condition: $b_1 = (2^1 - 1) = 1 = p_1 = 1$

Recursive relation: Sub b_{n-1} into p_n if it equals b_n then it is a recursive relation.

$$\begin{aligned} 2(b_{n-1}) + 1 &= 2(2^{n-1} - 1) + 1 \\ &= 2^{n-1+1} - 2 + 1 \\ &= 2^n - 1 \\ &= b_n \end{aligned}$$

2.3.3 Summatiom

Definition 23. The summation of a sequence a_n is given by $\sum_{i=1}^{N} a_n$. In discrete math, we are interested in finite summations and the closed formulas for them

Example: Find a closed formula for $\sum_{i=1}^{N} i = 1 + 2 + \cdots + N$.
Claim: $\sum_{i=1}^{N} i = \frac{N(N+1)}{2}$

Proof. Let $M = \sum_{i=1}^{N} i$.
Then,

$$\begin{aligned} 2M &= 2 \times \sum_{i=1}^{N} i \\ &= \sum_{i=1}^{N} i + \sum_{k=1}^{N} k \end{aligned}$$

$$\begin{aligned} \sum_{k=1}^{N} k &= N + (N-1) + (N-2) + \cdots + 1 \\ &= \sum_{k=1}^{N} (N - k + 1) \end{aligned}$$

$$\begin{aligned} 2M &= \sum_{i=1}^{N} i + \sum_{k=1}^{N} (N - k + 1) \\ &= \sum_{i=1}^{N} N + 1 = N(N+1) \\ M &= \frac{N(N+1)}{2} \end{aligned}$$

Note$_1$: we changed variable i to k in the second summation.
Note$_2$: the variables i and k are equal to each other, so when we add them in the final $2M$ calculation they cancel each other out. □

3 Week 3

3.1 Divisibility and Modular Arithmetic

3.1.1 Divides

Remark: When discussing division, we only use integers $\mathbb{Z}$.

Definition 24 (Divides)**.** For two integers a and b, we say that a **divides** b, written as $a \mid b$, if there exists some integer $k \in \mathbb{Z}$ such that $b = ak$. Otherwise, if a does not divide b we write $a \nmid b$.

Examples:

- $-3 \mid 12$ since $-4(-3) = 12$
- $4 \nmid 7$ since there is not integer such that $7 = 4k$
- $1 \mid n$ for all $n \in \mathbb{Z}$ since $n = 1(k)$
- $n \mid 0$ for all n since $0 = n(0)$

3.1.2 Properties of Divisibility

Let $a, b, c \in \mathbb{Z}$, and $a \neq 0$:

1. If $a \mid b$ and $a \mid c$, $\implies a \mid (b + c)$
2. If $a \mid b$, $\implies a \mid bc$
3. If $a \mid b$, $b \neq 0$ and $b \mid c$, $\implies a \mid c$

Proof. Property 1. Assume $a \mid b$, and $a \mid c$.
Then there exists some integers $k, j \in \mathbb{Z}$ such that:

$$b = ak$$
$$c = aj$$

Then, $b + c$ can be expressed as:

$$\begin{aligned} b + c &= ak + aj \\ &= a(k + j) \end{aligned}$$

Which fits our definition of divisibility, thus $a \mid (b + c)$. □

Proof. Property 2. Assume $a \mid b$.
Then it follows that $a \mid bc$ since $bc = (ak)c = a(kc)$. Which fits our definition of divisibility. □

Proof. Property 3. Assume that $a \mid b$, $b \neq 0$ and $b \mid c$.
Then, we say:

$$\begin{aligned} b &= ak \text{ for some } \{k \in \mathbb{Z} \mid k \neq 0\} \\ c &= bj \text{ for some } \{j \in \mathbb{Z}\} \\ &= (ak)j \end{aligned}$$

This fits our definition of divisibility, thus $a \mid c$. □

3.1.3 The Remainder Theorem

The remainder theorem is applied when $a \nmid b$.

Theorem 3 (Remainder Theorem)**.** *Let $n, d, \in \mathbb{Z}$ be two integers with $d > 0$. Then there are unique integers q, r with $0 \leq r < d$. Such that $n = dq + r$.*

Note: Remainders must be:

- Non-negative $0 \leq r$
- Less than the divisor $r < d$

Example 1: $12 \nmid 51$

$$\begin{aligned} 51 &= 12(4) + 3 \\ d = 12, q &= 4, r = 3 \end{aligned}$$

Example 2:
An application of this is determing if there is an integer n such that $\{n^2 \in Z \mid$ ends with $7\}$ Some examples are shown below:

0^2	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2
0	1	4	9	16	25	36	49	64	81	100

We notice that the pattern starts repeating after 9 digits, none end in 7.
Let $n \in \mathbb{Z}$, then $n = 10q + r$, where r is the last digit of $n \implies 0 \leq r < 10$.

$$\begin{aligned} n^2 &= (10q + r)(10q + r) \\ &= (100q^2 + 20qr + r^2) \\ &= 10(10q^2 + 2qr) + r^2 \end{aligned}$$

The last digit of n^2 is determined by r^2. From the examples above, we know r will not equal 7, thus there is no integer n such that n^2 ends with 7.

3.1.4 Modular Arithmetic

Definition 25 (Congruence Modulo)**.** If two integers $n, m \in \mathbb{Z}$ have the same remainder when divided by d, we say n and m are **congruent modulo d** and write $m \equiv n \mod d$. In other words,

$$\begin{aligned} n &= q_1(d) + r \\ m &= q_2(d) + r \\ &\implies n \equiv m \mod d \end{aligned}$$

Properties of Congruence Modulo:

1. $n = qd + r \implies n \equiv r \mod d$
2. $n \equiv m \mod d \iff d \mid (n - m)$
3. $n \equiv 0 \mod \iff d \mid n$

3.2 Prime Numbers, GCD, LCM

3.2.1 Prime Numbers

Definition 26 (Prime Number)**.** A number $p \in \mathbb{N}$ is **prime** if $p > 1$ and the only divisors of p are ± 1 and $\pm p$. Otherwise, p is called **composite**.

Examples:

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 are prime numbers
- 4, 6, 8, 9, 10, 12, 14, 15, 16, 18 are composite numbers

3.2.2 Fundamental Theorem of Arithmetic

Theorem 4 (Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be uniquely written as a product of primes.*

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} = \prod_{i=1}^{m} p_i^{k_i}$$

3.2.3 Positive Divisors of n

If we know the prime decomposition of n we can determine the number of positive divisors of n.

For example $72 = 2^3 \times 3^2$. There are:

- 4 choices for the power of 2: $2^0, 2^1, 2^2, 2^3$
- 3 choices for the power of 3: $3^0, 3^1, 3^2$

Thus, in total there are $4(2) + 3(3) = 12$ possible positive divisors of 72.

3.2.4 GCD

Definition 27 (Greatest Common Divisor)**.** The **greatest common divisor** of two integers $a, b \in \mathbb{Z}$, not both zero, is the largest integer d such that $d \mid a$ and $d \mid b$. It is written as $\gcd(a, b)$ or (a, b).

3.2.5 LCM

Definition 28 (Least Common Multiple)**.** is the smallest positive integer m such that $a \mid m$ and $b \mid m$. It is written as $\text{lcm}(a, b)$.

3.2.6 Computing GCD and LCM using Prime Factorisation

Let $a, b \in \mathbb{Z}$. Then the GCD and LCM can be computing using their prime factorisations:

- **For GCD:** take the minimum power of all primes **in common between** a and b, ignore negative signs.
- **For LCM:** take the maximum power of all primes in a and b.

Example: Two integers are given:

- $576 = 2^6 \times 3^2$
- $78408 = 2^3 \times 3^4 \times 11^2$

Their GCF and LCM are given:

- $\gcd(576, 78408) = 2^3 \times 3^2$

- $\text{lcm}(576, 78408) = 2^6 \times 3^4 \times 11^2$

3.3 Euclidean Algorithm

3.3.1 Euclidean Algorithm

Definition 29 (co-prime)**.** Two integers $a, b \in \mathbb{Z}$ are said to be **co-prime** if $\gcd(a, b) = 1$, e.g. $\gcd(5, 7) = 1$

Theorem 5. $\gcd(a, b) = \gcd(b, r)$.

Proof. Suppose there exists some $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$,

$$d \mid (a + qb), \{q \in \mathbb{Z}\}$$
$$d \mid r \text{ since } r = a - qb$$

Note: $(a + qb)$ follows the property 1 of divisibility $d \mid (a + b)$
Now consider the existence of some $c \in \mathbb{Z}$ such that $c \mid b$ and $c \mid r$.

$$c \mid (r + qb)$$
$$c \mid ((a - qb) + qb) \text{ since } r = a - qb$$
$$c \mid a$$

Now both d and c share common divisors, thus $\gcd(a, b) = \gcd(b, r)$. □

3.3.2 Application of Euclidean Algorithm

To Find $\gcd(a, b)$ **with** $a \geq b \geq 0$**:**

1. Write $a = qb + r$ by division algorithm
2. If $r = 0$, then $\gcd(a, b) = b$. Stop.
3. Otherwise if $r \neq 0$, then replace a by b and repeat.

Example: See assignment 1 Q3.

3.3.3 Base b Expansions

Definition 30 (Base b Expansion)**.** Numbers are typically denoted "decimally", i.e. in "base1-10".

$$n = a_0 \times 10^0 + a_1 \times 10^1 + a_2 \times 10^2 + \cdots + a_k \times 10^k$$

Let $b > 1$ be a positive integer. Then every positive integer n can be uniquely expressed as:

$$n = a_0 \times b^0 + a_1 \times b^1 + a_2 \times b^2 + \cdots + a_k \times b^k$$

Example 1: Convert 78_{10} to base 2.

$$\begin{aligned} 78 &= 2(39) + 0 \\ 39 &= 2(19) + 1 \\ 19 &= 2(9) + 1 \\ 9 &= 2(4) + 1 \\ 4 &= 2(2) + 0 \\ 2 &= 2(1) + 0 \\ 1 &= 2(0) + 1 \\ &\implies 78_{10} = 1001110_2 \end{aligned}$$

Here, we take the remainder from bottom to top to get the base 2 representation.

Example 2: Convert $(245)_8$ to base 10.

$$\begin{aligned} 245_8 &= (5 \times 8^0) + (4 \times 8^1) + (5 \times 8^2) \\ &= 5 + 32 + 128 \\ &= 165_{10} \end{aligned}$$

3.3.4 Base b Arithmetic

Base b expressions are positional. The usual arithmetic operations work, but you need to "carry over" b instead of 10.

4 Week 4

5 Week 5