

1 | The Foundations: Logic and Proofs

1.1 Logical Connectives

Definition 1.1.1. A **proposition** or **statement** is

Notation. A **true statement** is denoted by

A **false statement** is denoted by

Example 1.1.1. Which of the following is a proposition?

(a) $2 + 2 = 5$

(b) $x^3 - x = 0$

(c) Every even number greater than 2 is the sum of two primes.

Note. We do not necessarily need to

Connectives. We may use connectives (such as negation, disjunction, conjunction, implication) to connect propositions and make new compound propositions.

Definition 1.1.2 (Negation). The **negation** of a proposition p is denoted by (read:) and is defined by the following truth table:

p	

Example 1.1.2. Let p be the proposition “It’s raining today!”. Then

Definition 1.1.3 (Conjunction). The **conjunction** of two propositions p and q is denoted by $p \wedge q$ (read: p and q) and is defined by the following truth table:

p	q	

Definition 1.1.4 (Disjunction - also called Inclusive OR). The **disjunction** or **inclusive or** of two propositions p and q is denoted by $p \vee q$ (read: p or q) and is defined by the following truth table:

p	q	

Definition 1.1.5 (Exclusive OR). The **exclusive or** of two propositions p and q is denoted by $p \oplus q$ (read: p xor q) and is defined by the following truth table:

p	q	

Note (Inclusive OR vs Exclusive OR in English).

Definition 1.1.6 (Implication). Let p and q be two propositions. The proposition (read:) is called an **implication** and is defined by the following truth table:

p	q	

Different ways of expressing $p \rightarrow q$:

Example 1.1.3. Determine whether the following statements are the same by identifying the hypothesis and the conclusion first.

- (a) If I am sick then I'll stay home.
- (b) I stay home only if I am sick.
- (c) I'll stay home whenever I am sick.
- (d) I stay home unless I am not sick.

Definition 1.1.7 (Converse, Inverse, Contrapositive).

The **converse** of the implication $p \rightarrow q$ is

The **inverse** of the implication $p \rightarrow q$ is

The **contrapositive** of the implication $p \rightarrow q$ is

Definition 1.1.8 (Biconditional). Let p and q be two propositions. The proposition (read:) is called a **biconditional** proposition and is defined by the following truth table:

p	q	

Definition 1.1.9. Two propositions are called **equivalent** if

Example 1.1.4. Use the truth table to show that implication is equivalent to its contrapositive but is not equivalent to either its converse nor its inverse.

p	q						

1.2 Applications of Propositional Logic

Steps to convert English to Logic

1. Identify

2. Identify

Example 1.2.1. Convert to propositional logic:

“If I go to Harry’s or the country, I will not go shopping.”

Example 1.2.2. Let

p : “A vehicle uses the HOV lane.”
 q : “A vehicle has a single passenger.”
 r : “A vehicle has a special permit.”

The proposition “To use the HOV lane, there must be at least two passengers in the vehicle unless the vehicle has a special permit.” using the p, q, r and logical connectives can be expressed as

(a) $(q \wedge \neg r) \rightarrow \neg p$

(b) $(p \wedge q) \rightarrow r$

(c) $p \rightarrow (r \vee \neg q)$

(d)

Definition 1.2.1 (Consistent System Specifications). A list of of propositions is **consistent** if

Example 1.2.3. Are these specifications consistent?

1. “The diagnostic message is stored in the buffer or is retransmitted.”
2. “The diagnostic message is not stored in the buffer.”
3. “If the diagnostic message is stored in the buffer, then it is retransmitted.”

What if we add 4. “The diagnostic message is not retransmitted.”?

Puzzle. An island has two kinds of inhabitants, *knight*s, who always tell the truth, and *knave*s, who always lie. You go to the island and meet A and B.

- A says “B is a knave.”
- B says “The two of us are both knights.”

What are the types of A and B ? Give your reasoning.

1.3 Propositional Equivalence

Definition 1.3.1 (Tautology).

Definition 1.3.2 (Contradiction).

Definition 1.3.3 (Contingency).

Recall two P and Q propositions are equivalent if

$$P \equiv Q \text{ iff}$$

Example 1.3.1. Use the truth table to show that

$$p \rightarrow q \equiv \neg p \vee q$$

TABLE 6 Logical Equivalences.

<i>Equivalence</i>	<i>Name</i>
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 7 Logical Equivalences Involving Conditional Statements.

$$\begin{aligned}
p \rightarrow q &\equiv \neg p \vee q \\
p \rightarrow q &\equiv \neg q \rightarrow \neg p \\
p \vee q &\equiv \neg p \rightarrow q \\
p \wedge q &\equiv \neg(p \rightarrow \neg q) \\
\neg(p \rightarrow q) &\equiv p \wedge \neg q \\
(p \rightarrow q) \wedge (p \rightarrow r) &\equiv p \rightarrow (q \wedge r) \\
(p \rightarrow r) \wedge (q \rightarrow r) &\equiv (p \vee q) \rightarrow r \\
(p \rightarrow q) \vee (p \rightarrow r) &\equiv p \rightarrow (q \vee r) \\
(p \rightarrow r) \vee (q \rightarrow r) &\equiv (p \wedge q) \rightarrow r
\end{aligned}$$

TABLE 3 Truth Tables for $\neg(p \vee q)$ and $\neg p \wedge \neg q$.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

TABLE 8 Logical Equivalences Involving Biconditional Statements.

$$\begin{aligned}
p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p) \\
p \leftrightarrow q &\equiv \neg p \leftrightarrow \neg q \\
p \leftrightarrow q &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) \\
\neg(p \leftrightarrow q) &\equiv p \leftrightarrow \neg q
\end{aligned}$$

Example 1.3.2. Is “Mary is not rich and happy” the negation of “Mary is rich and happy”? Explain.

Example 1.3.3. Use logical equivalences (from the tables above) to prove $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge q$.

Exercise 1.3.4. Show that $(p \wedge q) \rightarrow (p \vee q)$ is tautology.

Definition 1.3.4 (Satisfiable). A compound proposition is *satisfiable* if

Example 1.3.5. $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable because

Note (Satisfiable vs. Consistent).

Note (Unsatisfiable vs. Contradiction).

Example 1.3.6. Determine whether $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$ is satisfiable or not.

Notation. $\bigvee_{i=1}^n p_i$

$\bigwedge_{i=1}^n p_i$

Exercise 1.3.7. Show that a (9×9) Sudoku puzzle is a satisfiability problem with 729 variables.

(Hint: Consider 729 variables $p_{i,j,n}$ (with $1 \leq i, j, n \leq 9$) which is defined to be true when number n appears in the cell that is in row i and column j .)

	2	9				4		
			5			1		
	4							
				4	2			
6							7	
5								
7			3					5
	1			9				
							6	

1.4 Predicates and Quantifiers

The sentence “ $x > 0$ ” is not a proposition. This sentence has two parts:

- 1.
- 2.

Such sentences are called *predicates* and become propositions when we assign value(s) from a certain domain to the variable(s).

Example 1.4.1. Let $P(x)$ be “ $x > 0$ ”.

Example 1.4.2. Let $R(x, y, z)$ be $x^2 + y^2 = z^2$.

We may also use **quantifiers** to write statements:

Universal quantifier

Existential quantifier

Checking the truth of a propositions with quantifiers and counterexamples:

To show “ $\forall x P(x)$ ” is false:

To show “ $\forall x P(x)$ ” is true:

To show “ $\exists x P(x)$ ” is true:

To show “ $\exists x P(x)$ ” is false:

Example 1.4.3. True or False?

- (a) $\forall x (x^2 \neq x)$
- (b) $\forall x (x^2 \neq x \vee x = 1)$
- (c) $\forall x (x^2 \neq x \vee x = 1 \vee x = 0)$
- (d) $\exists x (x^2 \leq 0)$
- (e) $\exists x (x^2 + x + 1 = 0 \wedge x \text{ is a real number})$

Negating Quantifiers:

$\neg(\forall x f(x)) \equiv \exists x \neg f(x)$
$\neg(\exists x f(x)) \equiv \forall x \neg f(x)$

Example 1.4.4. Let

$$\begin{aligned} S(x) &: \text{“}x \text{ is a student in this class”} \\ J(x) &: \text{“}x \text{ has taken course in Java”} \end{aligned}$$

Determine which logical proposition translates “Every student in this class has taken Java”.

- (a) $\forall x J(x)$

(b) $\forall x (S(x) \rightarrow J(x))$

(c) $\forall x (S(x) \wedge J(x))$

Example 1.4.5. True or False?

(a) $\forall x > 1 (x^3 > x^2)$

(b) $\forall x (x > 1 \rightarrow x^3 > x^2)$

(c) $\forall n \in \{1, 2, 3\} (5^n + 3 \text{ is divisible by } 4)$

Example 1.4.6. Translate into logical expressions in three different ways: “No one in your school owns both a bicycle and a motorcycle.” using predicates, quantifiers, and logical connectives. Then express its negation in both English and logic.

1.5 Nested Quantifiers

Example 1.5.1. Let $P(x, y)$ be the proposition “ $\frac{x}{y} = 2$ ”. Determine the truth value of each proposition below:

(a) $\exists x \exists y P(x, y)$

(b) $\forall x \forall y P(x, y)$

(c) $\forall x \exists y P(x, y)$

(d) $\exists x \forall y P(x, y)$

Example 1.5.2. Let $C(x)$ be “ x has a car” and $F(x, y)$ be “ x and y are friends”. Translate each proposition to English.

(a) $\forall x (C(x) \vee \exists y (C(y) \wedge F(x, y)))$

(b) $\exists x \forall y \forall z ((F(x, y) \wedge F(x, z) \wedge (y \neq z)) \rightarrow \neg F(y, z))$

Example 1.5.3. Translate each proposition to a logical expression. Clearly, identify the domain of each variable used.

(a) The difference of two negative integers is not necessarily negative.

(b) There is a student in this class that has taken every CS course.

Example 1.5.4. Write the negation of each logical expression of the Example 1.5.3 above.

Example 1.5.5. Determine the truth value of each proposition below. Assume that the domain of each variable consists of all real numbers.

(a) $\exists x \exists y (x + 2y = 2 \wedge 2x + 4y = 5)$

(b) $\forall x \forall y \exists z (z = (x + y)/2)$

(c) $\forall x \exists y (x + y = 1)$

(d) $\exists x \forall y (y \neq 0 \rightarrow xy = 1)$

Exercise 1.5.6. Write the negation of $\exists x \forall y (Q(x, y) \leftrightarrow Q(y, x))$ so that all negation symbols precede predicates.

1.7 Introduction to Proofs

Definition 1.7.1 (Theorem).

To prove $p \rightarrow q$ is true, we have the following options:

1. **Direct proof:**
2. **Proof by contraposition:**
3. **Proof by contradiction:**

Theorem 1.7.1. *The difference of two rational numbers is rational.*

Proof.

Theorem 1.7.2. *If n is an integer and $5n + 2$ is even then n is even.*

Proof.

Theorem 1.7.3. *An integer n is odd if and only if n^2 is odd.*

Proof.

Theorem 1.7.4. $\sqrt{3}$ is irrational.

Proof.

1.8 Proof Methods and Strategies

“Proof by Cases” technique: To prove a conditional statement of the form

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$$

use the following equivalence:

Example 1.8.1. Suppose n is a positive integer. Prove that $n^3 + n^2 \neq 100$.

“Without Loss of Generality (WLOG)” technique:

Example 1.8.2. Show that if xy and $x + y$ are both even then x and y are both even.

“Constructive Existence Proof” technique: To prove a statement of the form $\exists x P(x)$ is true

Example 1.8.3. Show that there is a positive integer that can be written as the sum of two cubes in two different ways.

“Non-Constructive Existence Proof” technique: Sometimes, to prove a statement of the form $\exists x P(x)$ is true

Example 1.8.4. Show that there exist irrational numbers x and y so that x^y is rational!

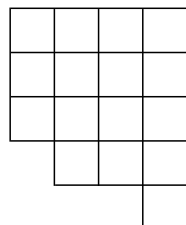
“Counterexample” technique: To prove a statement of the form $\forall x P(x)$ is false, or equivalently to show $\neg(\forall x P(x))$ is true

Example 1.8.5. Prove or disprove: For every non-negative integer n , $n^2 + n + 41$ is a prime number.

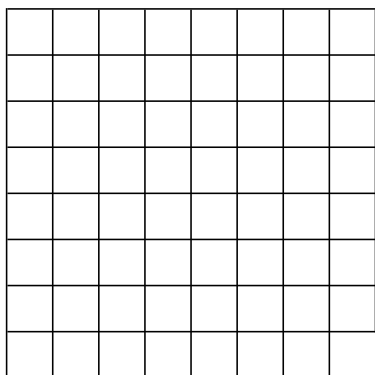
Proof Strategies for Proving a Conditional Statement $p \rightarrow q$: Forward vs. Backward

Example 1.8.6. Suppose that two people play a game taking turns removing 1, 2, or 3 stones at a time from a pile that contains 15 stones initially. The person who removes the last stone wins. Show that the first player can always win.

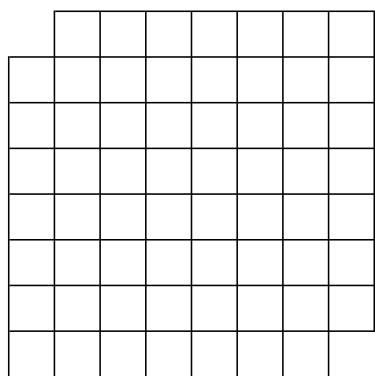
Example 1.8.7. Can you tile the following board using 1×2 dominoes?



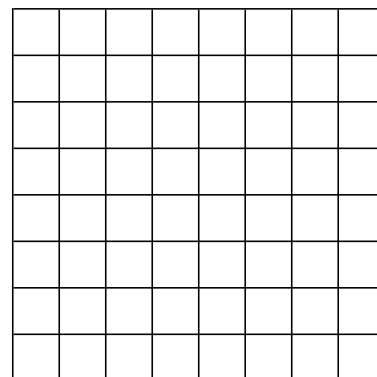
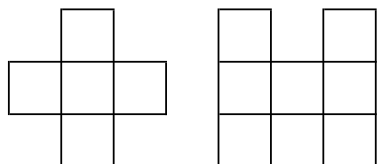
Example 1.8.8. Can you tile an 8×8 board with a removed corner using 1×2 dominoes?



Example 1.8.9. Can you tile an 8×8 board with a opposite corners removed using 1×2 dominoes?



Example 1.8.10. Can you tile an 8×8 board with a removed corner using the following “cross”-type and “ H ”-type dominoes?



2 | Basic Structures: Sets, Functions, Sequences, Sums

2.1 Sets

Sets are fundamental objects in mathematics. Set theory is a fundamental subject in mathematic, but here we only look at the “naive” set theory.

Definition 2.1.1 (Set). A **set** is

Notation ($\in$ and $\notin$).

A set may be defined by

1. Roster method:

2. Set-builder notation:

Some important sets:

$\mathbb{N}$ = the set of all natural (positive integer) numbers = $\{1, 2, 3, \dots\}$

$\mathbb{Z}$ = the set of all integers

$\mathbb{Q}$ = the set of all rational numbers

$\mathbb{R}$ = the set of all real numbers

$\mathbb{R} \setminus \mathbb{Q}$ =

Intervals of real numbers:

$$\begin{aligned}[a, b] &= \{x \mid a \leq x \leq b\} \\ (a, b) &= \{x \mid a < x < b\} \\ [a, b) &= \{x \mid a \leq x < b\} \\ [a, \infty) &= \{x \mid a \leq x\} \\ (-\infty, b) &= \{x \mid x < b\}\end{aligned}$$

Definition 2.1.2 (Universal set, Empty set).

Note. Sets can be elements of sets.

Note. The empty set is different from the set that contains the empty set.

Example 2.1.1 (Russel's Paradox).

Definition 2.1.3 (Subset, Proper Subset, Equal Sets).

Example 2.1.2. Let S be a set. Show that $\emptyset \subseteq S$ and $S \subseteq S$.

Definition 2.1.4 (Finite Sets, Cardinality, Infinite Sets).

Example 2.1.3. Find the cardinality of the following sets: $\{1, 2, 4\}$, $\emptyset$, $\{\{1, 2, 3\}\}$, and $\{\emptyset\}$.

Definition 2.1.5 (Power Set).

Example 2.1.4. Let $A = \{1, 4\}$ and $B = \{1, 2, 3\}$. Find $\mathcal{P}(A)$ and $\mathcal{P}(B)$.

Theorem 2.1.1 (Cardinality of Power Set).

Definition 2.1.6 (n -tuple).

Definition 2.1.7 (Cartesian Product).

Example 2.1.5. Let $A = \{2\}$ and $B = \{x, y\}$. Find $B \times A \times B$.

Theorem 2.1.2 (Cardinality of Cartesian Product).

2.2 Set Operations

Definition 2.2.1 (Union, Intersection, Difference, Complement. Disjoint).

Note (Universal set needed for complement).

Theorem 2.2.1 (The Cardinality of Union).

Example 2.2.1. Let $A = \{1, 2, 4\}$ and $B = \{2, 4, 5, 6\}$.

The formula above can be generalized:

Notation (Generalized Union and Intersection).

Example 2.2.2. For each $i \in \mathbb{Z}$ with $i \geq 0$, let $A_i = \{i, i + 1, i + 2, \dots\}$. Find $\bigcup_{i=0}^{\infty} A_i$ and $\bigcap_{i=0}^{\infty} A_i$.

Set Identities:

Identity Laws:		
Domination Laws:		
Complementation Law:		
Commutative Laws:		
Associative Laws:		
Distributive Laws:		
Complement Laws:		
De Morgan's Laws:		
Absorption Laws:		

Proving Identities:

- 1.
- 2.
- 3.

Proof of the 2nd De Morgan's Law:

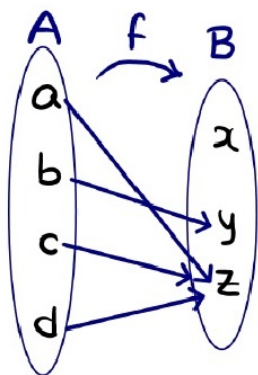
2.3 Functions

Definition 2.3.1 (Function).

Example 2.3.1 (Student's grades).

Definition 2.3.2 (Domain, Codomain, image, pre-image, range).

Example 2.3.2. Consider the function $f : A \rightarrow B$ illustrated below. Find



(a) domain of f

(b) codomain of f

(c) range of f

(d) $f(A)$

(e) The image of d

(f) $f(a)$

(g) The pre-image(s) of y

(h) The pre-image(s) of z

(i) $f(\{b, c\})$

(j) $f(\{a, d\})$

Definition 2.3.3 (Equal Functions).

Example 2.3.3.

Representing functions:

Explicit:

Formula:

Computer Program:

Definition 2.3.4 (Surjective or Onto).

Definition 2.3.5 (Injective or One-to-One).

Definition 2.3.6 (Bijective).

Example 2.3.4. Determine whether each function below is only injective, only surjective, or bijective.

(a) $\begin{cases} f : \mathbb{R} \rightarrow \mathbb{R} \\ f(x) = x^2 \end{cases}$

(b) $\begin{cases} g : \mathbb{R}^+ \rightarrow \mathbb{R}^+ \\ g(x) = x^2 \end{cases}$

(c) $\begin{cases} h : \mathbb{R} \setminus \{3/2\} \rightarrow \mathbb{R} \setminus \{1/2\} \\ h(x) = \frac{x}{2x-3} \end{cases}$

Definition 2.3.7 (Inverse Function).

Example 2.3.5. Find f^{-1} , where $\begin{cases} f : \{1, 2, 3\} \rightarrow \{2, 5, 10\} \\ f(x) = x^2 + 1 \end{cases}$.

Example 2.3.6. Find h^{-1} , where $\begin{cases} h : \mathbb{R} \setminus \{3/2\} \rightarrow \mathbb{R} \setminus \{1/2\} \\ h(x) = \frac{x}{2x-3} \end{cases}$.

Definition 2.3.8 (Composition of Functions).

Example 2.3.7. Let $\begin{cases} f : \mathbb{Z} \rightarrow \mathbb{R} \\ f(x) = x^2 + 1 \end{cases}$ and $\begin{cases} g : \mathbb{R} \rightarrow \mathbb{R}^+ \\ g(x) = |x| + 5 \end{cases}$. Find $g \circ f$ and $f \circ g$, if possible.

Note (Identity Function).

Definition 2.3.9 (The Graph of Functions).

Example 2.3.8. Graph the following functions.

(a) $\begin{cases} f : \mathbb{Z} \rightarrow \mathbb{Z} \\ f(n) = 2n + 1 \end{cases}$

(b) $\begin{cases} g : \mathbb{Z}^+ \rightarrow \mathbb{Z} \\ g(n) = n^2 \end{cases}$

Some Important Functions: The factorial function; the floor function; the ceiling function

Example 2.3.9. Prove that if $x \in \mathbb{R}$ then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

2.4 Sequences and Summations

Sequences are ordered list of numbers. For example, $(5, 7, 9, 11, 13, \dots)$ is a sequence. Formally:

Definition 2.4.1 (Sequence, n -th term, Sequence representation).

Example 2.4.1. $a_n = \frac{1}{n}$.

Definition 2.4.2 (Geometric Progression).

Example 2.4.2. Write the first 5 terms of a geometric progression with the given initial value a and common ratio r .

(a) $a = 10, r = -1$

(b) $a = 2, r = 5$

(c) $a = 6, r = 1/3$

Definition 2.4.3 (Arithmetic Progression).

Example 2.4.3. Write the first 5 terms of an arithmetic progression with the given initial value a and common difference d .

(a) $a = -1, d = 4$

(b) $a = 7, d = -3$

(c) $a = 1, d = 2$

Definition 2.4.4 (Recurrence Relations).

Example 2.4.4 (Geometric and Arithmetic Progressions).

Example 2.4.5. Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \dots$ with $a_0 = 2$. Find a_1, a_2 , and a_3 . Conjecture a closed form for a_n .

Example 2.4.6 (Fibonacci Sequence).

Solving A Recurrence Relation: There are several methods to solve a recurrence relation. By solving a recurrence relation, we mean finding a closed form for the n -th term of the sequence. Here, we look at two basic methods: • Forward Substitution • Backward Substitution.

Example 2.4.7. Find a solution for the recurrence relation give by $a_n = a_{n-1} + 2n + 1$ with $a_0 = 4$.

Summation Notation: To express the summation $a_m + a_{m+1} + \cdots + a_n$, we may use the more precise notation

Example 2.4.8. Express using the $\sum$ notation.

(a) $1 + r + r^2 + \cdots + r^n$

(b) $1 + \frac{1}{2} + \frac{1}{3} + \cdots$

(c) $2^2 + 3^2 + 5^2 + 7^2$

Theorem 2.4.1 (Geometric Series). *Let $a, r \in \mathbb{R}$ with $r \neq 0, 1$. Then*

$$a + ar + ar^2 + \cdots + ar^n = \sum_{j=0}^n ar^j = \frac{a(1 - r^{n+1})}{1 - r}.$$

Proof.

Example 2.4.9. Compute $\sum_{j=0}^8 5 \cdot (0.5)^j + 3 \cdot 2^j$.

Example 2.4.10. Compute $\sum_{i=0}^{10} \sum_{j=0}^8 i \cdot 2^j$.

TABLE 2 Some Useful Summation Formulae.

<i>Sum</i>	<i>Closed Form</i>
$\sum_{k=0}^n ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^n k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^n k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^n k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, x < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, x < 1$	$\frac{1}{(1-x)^2}$

3 | Algorithms

We will only cover section 3.2 from this chapter.

3.2 The Growth of Functions

In computer science, we are often interested in the questions “How long does an algorithm take to finish (as a function of the input size)? How much storage (memory) is needed (based on the input size)?”. To answer these questions, we need to decide mathematically that how fast a given functions grows.

Definition 3.2.1 (The Big-O Notation).

Note (The non-uniqueness of witnesses C and k).

Example 3.2.1. Show that $f(x) = x^2 + 3x + 2$ is $O(x^2)$.

Example 3.2.2. Show that n^2 is not $O(n)$.

Theorem 3.2.1 (The Big-O Estimates for Polynomials). *Let*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where $a_n, a_{n-1}, \dots, a_1, a_0$ are constants with $a_n \neq 0$, be a polynomial of degree n . Then $p(x)$ is $O(x^n)$.

Proof.

Example 3.2.3. Find a big-O estimate for the summation $1 + 2 + 3 + \dots + n$.

Example 3.2.4. Find a big-O estimate for the $n!$.

Theorem 3.2.2. Suppose $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1 + f_2)(x)$ is $O(\max\{g_1(x), g_2(x)\})$ and $(f_1 \cdot f_2)(x)$ is $O(g_1(x) \cdot g_2(x))$.

Proof.

Corollary. If $f_1(x)$ and $f_2(x)$ are both $O(g(x))$ then $(f_1 + f_2)(x)$ is also $O(g(x))$.

Example 3.2.5. Give a big-O estimate for $f(x) = (x + 2) \log(x^2 + 3) + 5x^2$.

Example 3.2.6. Put the functions below in order so that each function is big-O of the next function on the list.

$$f_1(n) = (1.5)^n$$

$$f_2(n) = 8n^3 + 17n^2 + 11$$

$$f_3(n) = (\log n)^2$$

$$f_4(n) = 2^n$$

$$f_5(n) = \log(\log n)$$

$$f_6(n) = n^2(\log n)^2$$

$$f_7(n) = 2^n(n^2 + 1)$$

$$f_8(n) = n^3 + n(\log n)^2$$

$$f_9(n) = 10000$$

$$f_{10}(n) = n!$$

Definition 3.2.2 (The Big- Ω Notation).

Note (Big-O vs. Big- Ω).

Example 3.2.7. Show that $f(x) = 6x^3 + 4x^2 + 5$ is $\Omega(x^2)$.

Definition 3.2.3 (The Big- Θ Notation; Same Order).

Example 3.2.8. Show that $1 + 2 + \cdots + n$ is $\Theta(n^2)$.

Example 3.2.9. Show that $5x^2 + 3x \log x$ is $\Theta(x^2)$.

Theorem 3.2.3 (The Big- Θ Estimates for Polynomials). *Let*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where $a_n, a_{n-1}, \dots, a_1, a_0$ are constants with $a_n \neq 0$, be a polynomial of degree n . Then $p(x)$ is $\Theta(x^n)$.

4 | Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

Definition 4.1.1 (Divides; Divisor, factor, multiple).

Note. $a|b \iff \frac{a}{b} \in \mathbb{Z}$.

Theorem 4.1.1. *Let $a, b, c \in \mathbb{Z}$, $a \neq 0$. Then*

(i) if $a|b$ and $a|c$ then $a|b + c$.

(ii) if $a|b$ then $a|bc$.

(iii) if $a|b$ and $b|c$ then $a|c$.

Proof.

Corollary. *If $a|b$ and $a|c$ then $a|mb + nc$ for all $m, n \in \mathbb{Z}$.
($mb + nc$ is called an integer linear combination of b and c .)*

Theorem 4.1.2 (Division Algorithm). *Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there exist unique integers q and r such that*

$$a = q \cdot d + r \quad \text{and} \quad 0 \leq r < d.$$

In this theorem, a is called the , q is called the , d is called the , and r is called the .

Notation. $a \mathbf{div} d =$ $a \mathbf{mod} d =$

Example 4.1.1. Find $-10 \mathbf{div} 4$ and $-10 \mathbf{mod} 4$.

Definition 4.1.2 (Congruent modulo; Congruence; Modulus).

Example 4.1.2. Determine whether (a) 23 is congruent to 5 modulo 6, and (b) 30 is congruent to 20 modulo 6.

The following theorem shows that two numbers are congruent to each other modulo m iff you can obtain one from the other one by adding (or subtracting) a few m 's.

Theorem 4.1.3. *Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then*

$$a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z} : a = b + mk.$$

Proof.

The following theorem gives the relationship between the two notations $a \equiv b \pmod{m}$ and $a \bmod m$. It essentially shows that two numbers are congruent to each other modulo m iff they have the same remainder when divided by m .

Theorem 4.1.4. *Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then*

$$a \equiv b \pmod{m} \iff a \bmod m = b \bmod m.$$

Proof.

The following theorem is very useful for finding the remainder of a division.

Theorem 4.1.5. *Let $a, b, c, d \in \mathbb{Z}$ and $m, n \in \mathbb{Z}^+$ be so that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then*

$$(i) \quad a + c \equiv b + d \pmod{m}$$

$$(ii) \quad a \cdot c \equiv b \cdot d \pmod{m}$$

$$(iii) \quad a^n \equiv b^n \pmod{m}$$

Proof.

Corollary. *Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then*

$$\begin{aligned}(a + b) \bmod m &= \left((a \bmod m) + (b \bmod m) \right) \bmod m \\ (a \cdot b) \bmod m &= \left((a \bmod m) \cdot (b \bmod m) \right) \bmod m\end{aligned}$$

Example 4.1.3. Find $1982 \times 673 \bmod 5$.

Example 4.1.4. Find $2^{31} + 8 \cdot 5^{21} \bmod 3$.

Definition 4.1.3 $(\mathbb{Z}_m, +_m, \cdot_m)$.

Example 4.1.5. Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Properties of arithmetic modulo m

Closure:

Associativity:

Commutativity:

Identity Elements:

Distributivity:

Additive Inverse:

Example 4.1.6. Does 6 have a multiplicative inverse in $\mathbb{Z}_{14}$?

4.2 Integer Representations and Algorithms

Keywords: Decimal, Binary, Octal, Hexadecimal

Typically, we use decimals (base 10) notation to represent integers. For example when we write 965 we mean

The following theorem shows that we can use any positive integer b greater than 1 (and not just $b = 10$) as the base to represent any positive integer:

Theorem 4.2.1. *Let $b \in \mathbb{Z}$ with $b > 1$ and let $n \in \mathbb{Z}^+$. We can uniquely express n as*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where $a_k \neq 0$ and $a_k, a_{k-1}, \dots, a_1, a_0 \in \mathbb{Z}_b$, that is

Definition 4.2.1 (Base- b Digits of a Representation; Base- b Expansion).

Example 4.2.1. What is the decimal expansion of the integer with $(11011)_2$ as its binary representation?

Example 4.2.2. What is the decimal expansion of the integer with octal expansion $(7016)_8$?

Example 4.2.3. What is the decimal expansion of the integer with hexadecimal expansion $(AE3B)_{16}$? (We use the digits 0, 1, $\dots$, 9, A, B, C, D, E, F for base 16).

Base Conversion: To convert a positive integer n (given in a decimal expansion form) to a base- b expansion form for any $b > 1$, do the following:

Example 4.2.4. Find the octal expansion of $(12345)_{10}$.

Conversion from Binary to Octal and Hexadecimal:

Example 4.2.5. Find the octal expansion of $(11111010111100)_2$.

Example 4.2.6. Find the hexadecimal expansion of $(11111010111100)_2$.

Example 4.2.7. Find the time complexity of each algorithm below.

ALGORITHM 2 Addition of Integers.

```

procedure add( $a, b$ : positive integers)
{the binary expansions of  $a$  and  $b$  are  $(a_{n-1}a_{n-2} \dots a_1a_0)_2$ 
and  $(b_{n-1}b_{n-2} \dots b_1b_0)_2$ , respectively}
 $c := 0$ 
for  $j := 0$  to  $n - 1$ 
     $d := \lfloor (a_j + b_j + c)/2 \rfloor$ 
     $s_j := a_j + b_j + c - 2d$ 
     $c := d$ 
 $s_n := c$ 
return  $(s_0, s_1, \dots, s_n)$  {the binary expansion of the sum is  $(s_ns_{n-1} \dots s_0)_2$ }

```

ALGORITHM 3 Multiplication of Integers.

```

procedure multiply( $a, b$ : positive integers)
{the binary expansions of  $a$  and  $b$  are  $(a_{n-1}a_{n-2} \dots a_1a_0)_2$ 
and  $(b_{n-1}b_{n-2} \dots b_1b_0)_2$ , respectively}
for  $j := 0$  to  $n - 1$ 
    if  $b_j = 1$  then  $c_j := a$  shifted  $j$  places
    else  $c_j := 0$ 
{ $c_0, c_1, \dots, c_{n-1}$  are the partial products}
 $p := 0$ 
for  $j := 0$  to  $n - 1$ 
     $p := p + c_j$ 
return  $p$  { $p$  is the value of  $ab$ }

```

ALGORITHM 5 Modular Exponentiation.

```

procedure modular exponentiation( $b$ : integer,  $n = (a_{k-1}a_{k-2} \dots a_1a_0)_2$ ,
 $m$ : positive integers)
 $x := 1$ 
 $power := b \bmod m$ 
for  $i := 0$  to  $k - 1$ 
    if  $a_i = 1$  then  $x := (x \cdot power) \bmod m$ 
     $power := (power \cdot power) \bmod m$ 
return  $x$  { $x$  equals  $b^n \bmod m$ }

```

4.3 Primes and Greatest Common Divisor

Definition 4.3.1 (Prime; Composite).

Theorem 4.3.1 (The Fundamental Theorem of Arithmetic).

Example 4.3.1. Write the unique prime factorization of 600.

Theorem 4.3.2 ($\sqrt{n}$).

Proof.

Example 4.3.2. Show that 97 is prime.

The Sieve of Eratosthenes:

List all prime numbers that are less or equal to a given integer n (say $n = 20$).

Theorem 4.3.3. *There are infinitely many prime numbers.*

Proof.

Theorem 4.3.4. *There are infinitely many composite numbers.*

Proof.

Definition 4.3.2 (Mersenne Primes).

Example 4.3.3. Determine whether 7 and 11 are Mersenne prime numbers.

Theorem 4.3.5. *If $2^p - 1$ is prime then p must be prime.*

Proof.

Distribution of Primes: Mathematicians have been always interested in the distribution of prime numbers. The following result was proved in the 19th century.

Theorem 4.3.6 (The Prime Number Theorem). *Let $\pi(x)$ denote the number of prime numbers not exceeding x . Then the ratio of $\pi(x)$ and $\frac{x}{\ln x}$ approaches 1 as x grows without bound. In other words:*

Example 4.3.4. Compare $\pi(1000000)$ and $\frac{1000000}{\ln 1000000}$.

Corollary. *Given a positive integer n , the odds that a randomly chosen number from the set $\{1, 2, \dots, n\}$ is prime is approximately*

Open Problems: Many unsolved problems in mathematics involve prime numbers. For example:

Goldbach Conjecture. Every even greater than 2 can be written as a sum of two prime numbers.

Twin Prime Conjecture. There are infinitely many “twin” primes. (Two primes are called twins if they differ by 2.)

Definition 4.3.3 (GCD).

Example 4.3.5. Find $\gcd(24, 36)$ and $\gcd(18, 25)$.

Definition 4.3.4 (Relatively Prime; Relatively Prime List).

Example 4.3.6. Determine whether 18, 25, and 27 are relatively prime.

Finding GCD using Prime Factorization:

Example 4.3.7. We know $145200 = 2^4 \cdot 3^1 \cdot 5^2 \cdot 11^2$ and $138915 = 3^4 \cdot 5^7 \cdot 7^3$. Find $\gcd(145200, 138915)$.

Definition 4.3.5 (LCM).

Finding LCM using Prime Factorization:

Example 4.3.8. Find $\text{lcm}(24, 36)$.

Theorem 4.3.7 (GCD · LCM).

Proof.

The Euclidean Algorithm:

The Euclidean algorithm is a more efficient way to find GCD of two number is using the division algorithm repeatedly, as explained in the example below.

Example 4.3.9. Find $\gcd(287, 91)$ using the Euclidean algorithm.

Exercise 4.3.10. Given $a > b$, what is the time complexity of finding $\gcd(a, b)$ using the Euclidean algorithm?

Correctness of the Euclidean Algorithm: First we prove the following crucial theorem.

Theorem 4.3.8. *Let $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof.

Now, to show the correctness of the Euclidean algorithm, let $a \geq b$ and put $r_0 = a$ and $r_1 = b$. The Euclidean algorithm gives:

GCD as Integer Linear Combination:**Theorem 4.3.9** (Bézout's Theorem).*Proof.***Definition 4.3.6** (Bézout Coefficients; Bézout Identity).**Example 4.3.11.** We know $\gcd(6, 14) = 2$. Write 2 as an integer linear combination of 14 and 6 in two different ways.**Example 4.3.12.** Express $\gcd(252, 198) = 18$ as an integer linear combination of 252 and 198 in two different ways.

Consequences of Bézout's Theorem:

Lemma 4.3.10. *If $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a|bc$ then*

Proof.

Lemma 4.3.11. *If p is prime and $p|a_1a_2 \cdots a_n$ then*

Theorem 4.3.12 (Uniqueness of Prime Factorization). *The prime factorization of any positive integer n is unique.*

Proof.

Dividing Congruences by an Integer:

Dividing both sides of a congruence by an integer does not always produce a valid congruence. For example, $21 \equiv 15 \pmod{6}$ but $7 \not\equiv 5 \pmod{2}$. However, we are allowed to divide by an integer that is relatively prime to the modulus:

Theorem 4.3.13. *Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$ be such that $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$. Then $a \equiv b \pmod{m}$.*

Proof.

4.4 Solving Congruences

Definition 4.4.1 (Inverse of a Modulo m).

Example 4.4.1. The inverse of 3 modulo 7 is

The existence of the inverse of a modulo m is guaranteed if a and m are relatively prime:

Theorem 4.4.1. *If $\gcd(a, m) = 1$ and $m > 1$ then $\bar{a}$ exists. That is, there exists a number $\bar{a}$ such that $a\bar{a} \equiv 1 \pmod{m}$.*

Proof.

Finding the inverse of a modulo m :

Example 4.4.2. Using Euclidean algorithm, find the inverse of 3 of modulo 7.

Definition 4.4.2 (Linear Congruence).

Two Methods for Finding the Solution of Linear Congruences:

Example 4.4.3. Solve the congruence $5x \equiv 6 \pmod{9}$.

Example 4.4.4. Solve the congruence $4x \equiv 1 \pmod{2}$.

Example 4.4.5. Solve the congruence $4x \equiv 0 \pmod{2}$.

Solving Non-Linear Congruences:

Example 4.4.6. Solve the congruence $5x^2 \equiv 8 \pmod{9}$.

In the 1st century Sun-Tsu asked the following question: find a number (integer) so that when it is divided by 3 the remainder is 2, when it is divided by 5 the remainder is 3 and when it is divided by 7 the remainder is 2. This problem can be written as a system of linear congruences:

The proof of the following theorem gives a method for solving a system of linear congruences.

Theorem 4.4.2 (The Chinese Remainder Theorem). *Let $m_1, m_2, \dots, m_k$ be pairiwise relatively prime integers greater than 1. Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$. Then the system*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_k$. That is, there is a unique solution x with $0 \leq x \leq M - 1$ and all other solutions are congruent this x modulo M .

Proof.

Example 4.4.7. Solve the system using the Chinese Remainder Theorem:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

There is a second method, called Back Substitution, to solve a system of linear congruences. We explain this method in the example below:

Example 4.4.8. Solve the system using Back Substitution:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

The following theorem enables us to evaluate a^y modulo a prime number p efficiently.

Theorem 4.4.3 (Fermat's Little Theorem). *Let p be prime and assume $a \in \mathbb{Z}$ is not a multiple of p . Then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, if a is any integer then $a^p \equiv a \pmod{p}$.*

Example 4.4.9. Find 7^{222} modulo 11.

Definition 4.4.3 (Pseudo Prime Base a).

By Fermat's Little Theorem, if p is prime and a is not a multiple of p then

Question. Is there a number n and a number a so that n is pseudo prime base a , but n is not prime?

Fermat's Little Theorem also gives an efficient method to determine whether a given number n is not prime:

Definition 4.4.4 (Primitive Roots of $\mathbb{Z}_p$).

Example 4.4.10. Show that 2 is a primitive root of $\mathbb{Z}_{11}$, but 3 is not a primitive root of $\mathbb{Z}_{11}$.

Definition 4.4.5 (Discrete Logarithm of n base r (modulo p)).

Example 4.4.11. Find the discrete logarithm of 9 base 2 (modulo 11).

4.6 Cryptography

In this section, we explore some number theoretical methods to encode/decode a message.

Shift Encryption/Decryption ((Ceasar Cipher/Decipher):

Affine Encryption/Decryption:

RSA Encryption:

Example 4.6.1. Encrypt the integer 3 using the RSA encryption with $(n, e) = (33, 13)$.

RSA Decryption:

Example 4.6.2. Decrypt the integer 27 using the RSA encryption with $(n, e) = (33, 13)$.

5 | Induction

5.1 Mathematical Induction

Example 5.1.1 (The Babies Example).

Example 5.1.2 (The Ladder Example).

Theorem 5.1.1 (Principle of Mathematical Induction). *To prove a statement a statement $P(n)$ is true for every integer $n \geq 1$, it suffices to show the following*

(a) $P(1)$ is true.

(b) The implication $P(k) \rightarrow P(k+1)$ is true, where $k \geq 1$ is an arbitrary integer.

Note. We may change the number 1 (in $n \geq 1$, $P(1)$, and $k \geq 1$) to some other integer m in the Principle of Mathematical Induction and theorem will remain true.

Note. In the Principle of Mathematical Induction, both steps (the basis step and the inductive step) are crucial!

Example 5.1.3. Let $n \geq 1$ be an integer. Prove that $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Example 5.1.4. Consider the recursion $a_{n+1} = a_n + \frac{1}{2^{n+1}}$ with $a_1 = \frac{1}{2}$.

- (a) Find a_2, a_3 , and a_4 .
- (b) Based on your answers in (a), conjecture an explicit formula for a_n .
- (c) Use mathematical induction to prove your conjecture.

Example 5.1.5. Let $n \geq 7$ be an integer. Prove that $3^n < n!$.

Example 5.1.6. Let n be a non-negative integer. Prove that 3 divides $n^3 - n$.

Example 5.1.7. Let n be a positive integer. Prove that $4^{n+1} + 5^{2n-1} \equiv 0 \pmod{21}$.

Example 5.1.8. What is wrong with this “proof” that all horses are the same colour?

Let $P(n)$ be the statement that all horses in a set of n horses are the same colour.

Base Step: $P(1)$ is certainly true, since with just one horse, all horses have the same colour.

Inductive Step: Assume $P(k)$, which is the statement that k horses all have the same colour (inductive hypothesis). Given a set of $k + 1$ horses $\{h_1, h_2, \dots, h_{k+1}\}$, we can exclude the last horse in the set and apply the inductive hypothesis just to the first k horses $\{h_1, \dots, h_k\}$, deducing that they all have the same colour. Similarly, we can conclude that the last k horses $\{h_2, \dots, h_{k+1}\}$ all have the same colour. But now the “middle” horses $\{h_2, \dots, h_k\}$ (i.e., all but the first and the last) belong to both of these sets, so they have the same colour as horse h_1 and horse h_{k+1} . It follows, therefore, that all $k + 1$ horses have the same colour. Thus, by the principle of induction, all horses have the same colour.

5.2 Strong Induction

Theorem 5.2.1 (Principle of Strong Induction). *To prove a statement a statement $P(n)$ is true for every integer $n \geq 1$, it suffices to show the following*

- (a) $P(1)$ is true.
- (b) The implication $P(1) \wedge P(2) \wedge \cdots \wedge P(k) \rightarrow P(k+1)$ is true, where $k \geq 1$ is an arbitrary integer.

Example 5.2.1. Prove that every integer $n \geq 1$ can be written as a sum of distinct powers of 2 (e.g. 41 can be written as $2^0 + 2^3 + 2^5$).

Example 5.2.2. Let $n \geq 8$. Prove that a postage of n cents can always be formed using just 3-cent and 5-cent stamps.

6 | Counting

6.1 Basics of Counting

The Product Rule:

Example 6.1.1 (Roads).

Example 6.1.2 (Bit Strings).

The Sum Rule:

Example 6.1.3. How many ternary strings (strings with 0, 1, 2) of length n start with either 0 or 2?

Note. The following statements are equivalent to the product rule and sum rule: Let A and B be two finite sets. Then

Example 6.1.4. How many bit strings of length n start with a 1 and end with a 0?

Example 6.1.5. How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits?

Example 6.1.6. Suppose A and B are two finite sets with $|A| = m$ and $|B| = n$.

- (a) How many different functions $f : A \rightarrow B$ can be made?
- (b) How many different one-to-one functions $f : A \rightarrow B$ can be made?
- (c) How many different onto functions $f : A \rightarrow B$ can be made?

The Subtraction Rule:

Example 6.1.7. How many bit strings of length 20 start or end with a 01?

The Division Rule:

Example 6.1.8. In how many different ways can 3 people sit around a circular desk? Two seatings are considered the same when each person has the same immediate left and immediate right neighbour. How about with 4 people? n people?

Example 6.1.9. How many positive integers less than 1000

- (a) are divisible by 7?
- (b) are divisible by 7 but not 11?
- (c) are divisible by both 7 and 11?
- (d) are divisible by either 7 or 11?
- (e) are divisible by exactly one of 7 and 11?
- (f) are divisible by neither 7 nor 11?
- (g) have distinct digits?
- (h) have distinct digits and are even?

Example 6.1.10. The name of a variable in the C programming language is a string that can contain uppercase letters, lowercase letters, digits, or underscores. Further, the first character in the string must be a letter, either uppercase or lowercase, or an underscore. If the name of a variable determined by its first eight characters, how many different variables can be made in C? (Note that the name of a variable may contain fewer than eight characters.)

Example 6.1.11. How many ways are there to seat four of a group of ten people around a circular table where two seatings are considered the same when everyone has the same immediate left and immediate right neighbour?

Example 6.1.12. How many bit strings of length 10 contain either five consecutive 0s or five consecutive 1s?

6.2 The Pigeonhole Principle

The Pigeonhole Principle:

Example 6.2.1. Determine whether the following statement are true or false.

- (a) In any group of 367 people at least two people must have the same birthday.
- (b) In any class of 12 students, at least two students will receive the same letter grade.

The Generalized Pigeonhole Principle: If we place N objects into k boxes then at least one of the boxes contains $\left\lceil \frac{N}{k} \right\rceil$ objects or more.

Proof.

Example 6.2.2. Among 15 people, at least how many are born on the same day of the week?

Example 6.2.3. Show that there are at least 21 people in British Columbia (population: 5 million) with the same two initials who were born on the same day of the year. Assume that everyone has two initials.

Example 6.2.4. What is the least number of area codes needed to guarantee that the 25 million phones in a province can be assigned distinct 10-digit telephone numbers? (Assume that telephone numbers are of the form NXX-NXX-XXXX, where the first three digits form the area code, N represents a digit from 2 to 9 and X represents any digit.)

Example 6.2.5. Let $(x_i, y_i), i = 1, 2, 3, 4, 5$, be a set of five distinct points with integer coordinates in the xy plane. Show that the midpoint of the line joining at least one pair of these points has integer coordinates.

Example 6.2.6. Prove that at any party (with 2 or more people) there are at least two people who know the same number of other people there.

Exercise 6.2.7. Assume that in a group of six people, each pair of individuals consists of two friends or two enemies. Show that there are either three mutual friends or three mutual enemies in the group.

Exercise 6.2.8. Show that whenever 25 girls and 25 boys are seated around a circular table there is always a person both of whose neighbours are boys.

6.3 Permutations and Combinations

Definition 6.3.1 (Permutation; r -Permutation; $P(n, r)$).

Example 6.3.1. Let $S = \{1, 2, 3\}$. List all r -permutations of S for $r \in \{1, 2, 3\}$.

Theorem 6.3.1. Let n and r be integers such that $1 \leq r \leq n$. Then $P(n, r) = \frac{n!}{(n-r)!}$.
Proof.

Example 6.3.2. How many permutations of the letters A, B, C, D, E, F, G

(a) are there?

(b) contain the string AB?

(c) contain the string AC and DE?

(d) contain the string AB and have exactly 5 letters?

Definition 6.3.2 (r -Combination; $C(n, r)$).

Example 6.3.3. Let $S = \{1, 2, 3, 4\}$. List all r -combinations of S for $r \in \{0, 1, 2, 3, 4\}$.

Theorem 6.3.2. Let n and r be integers such that $0 \leq r \leq n$. Then $C(n, r) = \frac{n!}{(n-r)!r!}$.
Proof.

Example 6.3.4. How many bit strings of length 10 have
(a) exactly three 0s?

(b) more 0s than 1s?

(c) at least seven 1s?

(d) at least three 1s? (*evaluate the exact number*)

Example 6.3.5. How many bit strings contain exactly five 0s and fourteen 1s if every 0 must be immediately followed by two 1s?

Example 6.3.6. Prove that $C(n, r) = C(n, n - r)$ using three different techniques (algebraic proof, double counting proof, and bijective proof).

Exercise 6.3.7. Prove

(a) $\sum_{r=0}^n C(n, r) = 2^n$

(b) $\sum_{x=0}^r C(m, x)C(w, r-x) = C(m+w, r)$

6.4 Binomial Theorem

Theorem 6.4.1 (Binomial Theorem).

Example 6.4.1. Expand $(x + y)^4$ using the binomial theorem.

Example 6.4.2. Find the coefficient of $x^{49}y^{51}$ and $x^{72}y^{29}$ in $(x + y)^{100}$.

Example 6.4.3. Find the coefficient of a^4b^9 in $(2a - 3b)^{13}$.

Example 6.4.4. Use the Binomial Theorem to prove

$$\sum_{0 \leq i \leq n, i: \text{ even}} C(n, i) = \sum_{0 \leq i \leq n, i: \text{ odd}} C(n, i).$$

6.5 Generalized Permutations and Combinations

Theorem 6.5.1. *The number of r -permutations of a set of n objects with repetition allowed is n^r .*

Proof.

Theorem 6.5.2. *The number of r -combinations of a set of n objects with repetition allowed is $C(n + r - 1, r)$.*

Before, we prove this theorem, let us look at the following example:

Example 6.5.1. In how many different ways can we choose 5 cookies at a shop that sells three different kind of cookies?

Proof.

Example 6.5.2. Find the number of integer solutions of each of the following equations:

(a) $x_1 + x_2 = 10$ with $x_1 \geq 0$ and $x_2 \geq 0$.

(b) $x_1 + x_2 + x_3 = 10$ with $x_1 \geq 0$, $x_2 \geq 0$, $x_3 \geq 2$.

(c) $x_1 + x_2 + x_3 + x_4 = 20$ with $x_1 \geq 3$, $x_2 \geq -5$, $x_3 \geq 0$, $x_4 \geq 1$.

(d) $x_1 + x_2 + x_3 \leq 7$ with $x_1 \geq 2$, $x_2 \geq 0$, $x_3 \geq -1$.

(e) $x_1 + x_2 + x_3 = 20$ with $x_1 \geq 0$, $0 \leq x_2 \leq 7$, $x_3 \geq 0$.

(f) $x_1 + x_2 = 10$ with $x_1 \geq 0$ and $0 \leq x_2 \leq 7$

(g) $x_1 + x_2 + x_3 = 20$ with $x_1 \geq 0, x_2 \geq 0, x_3 \geq 0, x_1, x_2, x_3$: even.

Theorem 6.5.3. *The number of permutations of n_1 1's, n_2 2's, $\dots, n_k$ k's is*

$$\frac{(n_1 + n_2 + \dots + n_k)!}{n_1!n_2! \dots n_k!}$$

Example 6.5.3. How many words using three A's and two B's can you make?

Example 6.5.4. How many words of length 17 can you make with the letters of the word INDISTINGUISHABLE?