Discrete Mathematics

Slides based on Susanna Epp's Textbook

Moses A. Boudourides[1]

Visiting Associate Professor of Computer Science
Haverford College

[1] Moses.Boudourides@gmail.com

Fall 2021 and Spring 2022

Contents

1. SPEAKING MATHEMATICALLY

1.1 Variables and Statements

Intuitive definition

A **variable** is a carrier for something, i.e., it is identified to or represented by a symbol which works as a placeholder for expressions or quantities that may vary.

Kinds of statements in mathematics

- **Universal statement** is an expression that something is true for all possible cases to which it refers.
- **Conditional statement** is an expression saying that if one thing is true then some other thing should be necessarily true.
- **Existential statement** is an expression about a given property saying that there is at least something for which the property is true, though there is no universal statement guarantying a priori

1.2 Sets

Notation

- In *Set Theory*, according to the **axiom of extension**, a **set** S is completely defined by describing what its elements are, i.e., describing a property that the elements of the set should satisfy.
- $x \in S$ denotes that x is an element of S.
- $x \notin S$ denotes that x is not an element of S.
- **Set–roster notation of sets**:
  - for a **finite** set, $S = \{x_1, x_2, \ldots, x_n\}$;
  - for an **infinite** set, $S = \{x_1, x_2, \ldots\}$.

Notation of special sets

- $\mathbb{R}$ denotes the set or all real numbers.
- $\mathbb{Z}$ denotes the set or all integers.
- $\mathbb{Q}$ denotes the set or all rational numbers, i.e., quotients of integers.

1.2 Sets: The set–builder notation

Set–builder notation

Let S be a set and, for $x \in S$, let $P(x)$ be a universal statement that prescribes the membership property of x in S, i.e., the property P that elements x of S need to satisfy in order to be elements of S. Then S can be denoted as follows:

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

where by writing "$P(x)$," for $x \in S$, it is meant that "x satisfies property P."

1.2 Sets: Subsets

Definition

- If A and B are two sets, then A is called a **subset** of B or A is said to **be contained** in B, written $A \subseteq B$, if and only if every element of A is also an element of B, i.e.,

$$A \subseteq B \iff \forall x \in A\colon \text{ if } x \in A, \text{ then } x \in B.$$

- $A \nsubseteq B \iff \exists$ at least one $x \in A$ such that $x \notin B$.
- A is called a **proper subset** of B, if and only if every element of A is also in B but there is at least one element of B that is not in A.

1.2 Sets: Cartesian products

Ordered pairs of elements of two or one set

Let A and B two sets; it could be one single set, i.e., $B = A$. Then, given the two elements $a \in A$ and $b \in B$, the symbol (a, b) denotes an **ordered pair** of elements of A and B (or just A, when $B = A$) consisting of a and b together with the specification that a is the first element of the pair and b is the second element. Given two other elements $c \in A$ and $d \in B$, the two ordered pairs (a, b) and (c, d) are **equal**, if and only if $a = c$ and $b = d$ (i.e., $(a, b) = (c, d) \iff a = c$ and $b = d$).

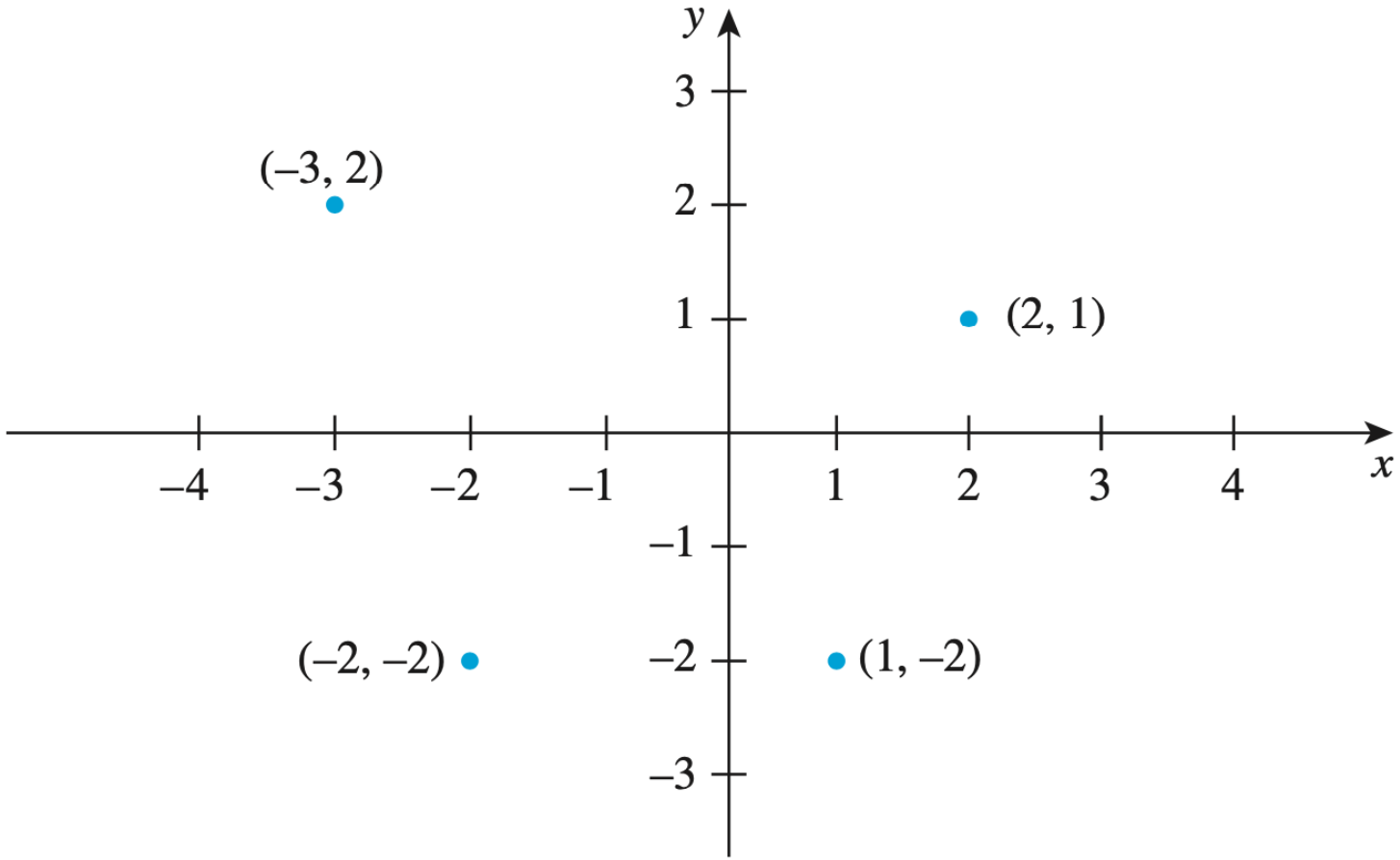
Definition

Let A and B two sets; it could be $B = A$. Then the **Cartesian product of A and B**, denoted $A \times B$, is defined as:

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

In case $B = A$, we get the **Cartesian product of A and**

1.2 Sets: $\mathbb{R}^2$ as the **Cartesian plane** of $\mathbb{R}$ and itself



1.3 Relations

Definition

Let A and B two sets; it could be $B = A$.

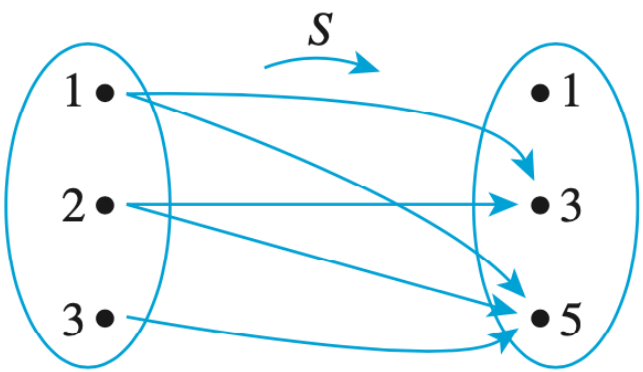
- A **relation** R **from** A **and** B is a subset of $A \times B$.
- Given two elements $x \in A$ and $y \in B$, x **is said to be related to** y **by the relation** R, written $x\,R\,y$, if and only if $(x, y) \in R$ $(\subseteq A \times B)$.
- Moreover, the set A is called the **domain** of relation R and the set B is called the **co–domain** of R.

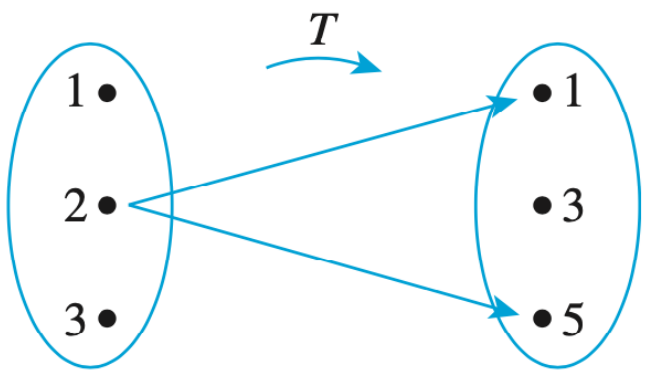
1.3 Relations: Arrow diagrams

The arrow diagram of a relation

Let R be a relation from a set A to a set B (it could be $B = A$). The **arrow diagram for** R is obtained as follows:

1. Represent the elements of A as points in one region and the elements of B as points in another region.
2. For each $x \in A$ and $y \in B$, draw an arrow from x to y, if and only if x is related to y (i.e., symbolically, $(x, y) \in R$).





1.3 Functions

Definition

Let A and B two sets; it could be $B = A$. A **function from A to B** is a relation with domain A and co–domain B that satisfies the following two properties:

1. $\forall x \in A, \exists y \in B$ such that $(x, y) \in F$ (in other words, every element of A is the first element of an ordered pair of F).
2. $\forall x \in A$ and $y, z \in B$, if $(x, y) \in F$ and $(x, z) \in F$, then $y = z$ (in other words, no two distinct ordered pairs in F have the same first element).

Notation of a function as a mapping

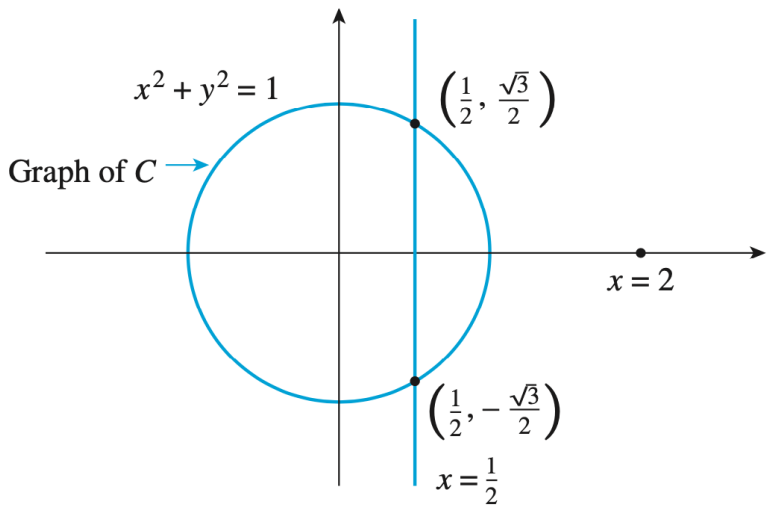
Let A and B two sets; it could be $B = A$. If F is a function from A to be B, then given any element $x \in A$, the unique element in B that is related to x by F is denoted as $F(x)$ (read "F of x") and the function F is denoted as a **mapping** $F : A \longrightarrow B$.

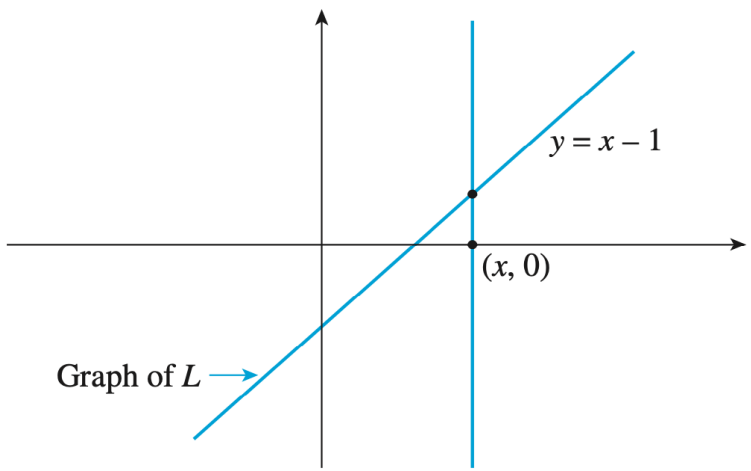
1.3 Graphs of functions

Definition

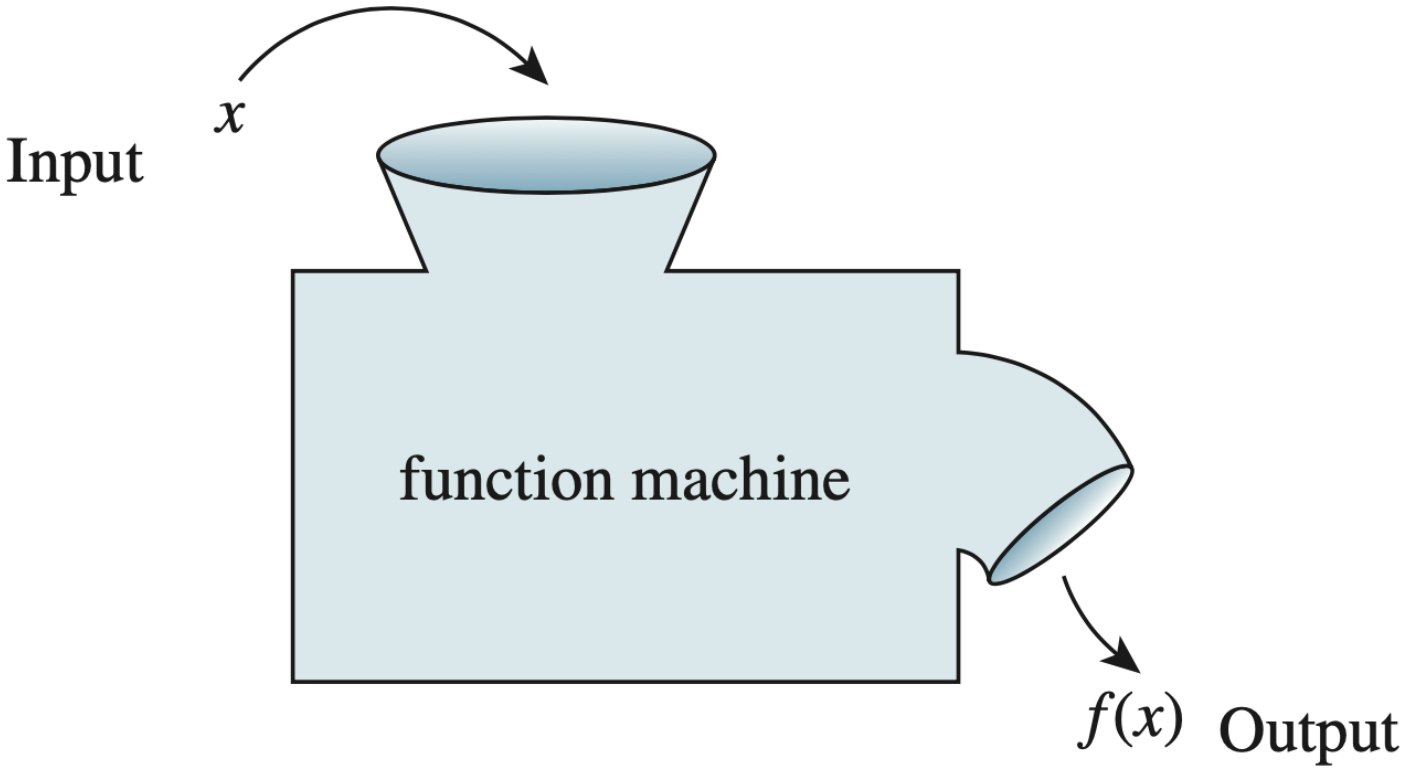
Let A and B two sets (it could be $B = A$) and let F be a function from A to B. The **graph of function** F, denoted $G(F)$, is defined as the corresponding relation from A to B in the definition of F:

$$G(F) = \{(x, F(x)) \mid x \in A\}.$$





1.3 Functions as mappings: Function machines



2. THE LOGIC OF COMPOUND STATEMENTS

2.1 Logical Forms

Definition

A **statement** (or **proposition**) is a sentence that is true or false but not both.

Examples

- Delaware River runs through Pittsburgh. (*False.*)
- $2 + 3 = 7$. (*False.*)
- 4 is a positive number and 3 negative. (*False.*)
- If set S consists of n elements, then it contains 2^n subsets. (*True.*)
- There exists an integer n such that $2^n = n^2$. (*True.*)
- $x + y = y + x$, for every $x, y \in \mathbb{R}$. (*True.*)
- If $A^2 = 0$, then, $A = 0$, for every A. (*Indeterminate.*)
- Every even integer greater than 2 is the sum of two prime numbers. (*Goldbach's Conjecture.*)
- There exist infinitely many integers n such that $2^n + n$ is a prime number. (*Unknown to be true or false.*)

2.1 Logical Connectives

Notation of symbols of common logical connectives

- **Negation (not)** (prefix): $\sim$
- **Conjuction (and)** (prefix): $\wedge$
- **Disjuction (or)** (prefix): $\vee$
- **Conditional (if ..., then ...)**: $\longrightarrow$
- **Biconditional (if and only if)**: $\longleftrightarrow$

Connectives	Precedence
$\sim$	1
$\wedge$	2
$\vee$	3
$\longrightarrow$	4
$\longleftrightarrow$	5

2.1 Truth Tables

Notation of truth values of a statement

- T: True
- F: False

Truth Table for $\sim p$

p	$\sim p$
F	T
T	F

Truth Table for $p \wedge q$, $p \vee q$, $p \longrightarrow q$, $p \longleftrightarrow q$

p	q	$p \wedge q$	$p \vee q$	$p \longrightarrow q$	$p \longleftrightarrow q$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

2.1 The Exclusive Or

Definition

The **exclusive or** (or **XOR**) logical connective of two statement variables p, q, denoted $p \oplus q$, is defined by the composite statement:

$$p \oplus q = (p \vee q) \wedge \sim (p \wedge q).$$

Truth Table for $p \oplus q$

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

2.1 An Example of a Statement Form (Composite Statement)

Truth Table for $(p \wedge q) \vee \sim r$

p	q	r	$p \wedge q$	$\sim r$	$(p \wedge q) \vee \sim r$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

2.1 Tautologies and Contradictions

Definition

- A composite statement is called **tautology** if it is always true for all truth values of the individual statements included in it.
- A composite statement is called **contradiction** if it is always false for all truth values of the individual statements included in it.

Example

The statement form $p \vee \sim p$ is a tautology and the statement form $p \wedge \sim p$ is a contradiction.

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F

2.1 Logical Equivalences

Definition

Two statement forms P and Q are called **logically equivalent**, denoted $P \equiv Q$, if they have identical truth values for each possible substitution of the truth values of all individual statements included in them.

Example: $\sim(\sim p) \equiv p$

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

Example: $\sim(p \wedge q) \not\equiv \sim p \wedge \sim q$

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$\sim p \wedge \sim q$
T	T	F	F	T	F	F
T	F	F	T	F	T	F
F	T	T	F	F	T	F
F	F	T	T	F	T	T

2.1 De Morgan's Laws

Theorem (De Morgan's Laws)

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

Example: $\sim (p \wedge q) \equiv \sim p \vee \sim q$

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

2.1 Summary of Logical Equivalences

Theorem 2.1.1 Logical Equivalences

Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1.	*Commutative laws:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2.	*Associative laws:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3.	*Distributive laws:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4.	*Identity laws:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5.	*Negation laws:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6.	*Double negative law:*	$\sim(\sim p) \equiv p$	
7.	*Idempotent laws:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8.	*Universal bound laws:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9.	*De Morgan's laws:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10.	*Absorption laws:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11.	*Negations of* $\mathbf{t}$ *and* $\mathbf{c}$*:*	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

2.2 Conditional Statements (a)

Definition

- If p and q are two statements, the **conditional of** q **by** p is the statement form "if p then q" or "p implies q" and it is denoted by $p \longrightarrow q$.
- If p is true and q is false, the conditional $p \longrightarrow q$ is false, while in all other truth values of p and q it is true.
- In a conditionial $p \longrightarrow q$, p is called **hypothesis** (or **antecedent**) of the conditional and q is called **conclusion** (or **consequent**) of the conditional.

Truth Table for $p \longrightarrow q$

p	q	$p \longrightarrow q$
F	F	T
F	T	T
T	F	F
T	T	T

2.2 Conditional Statements (b)

Proposition (Representation of Conditional as Or)

$$p \longrightarrow q \equiv \sim p \vee q.$$

Proposition (Negation of Conditional)

$$\sim (p \longrightarrow q) \equiv p \wedge \sim q.$$

2.2 Conditional Statements (c)

Definition

- The **contrapositive** of $p \longrightarrow q$ is $\sim q \longrightarrow \sim p$.
- The **converse** of $p \longrightarrow q$ is $q \longrightarrow p$.
- The **inverse** of $p \longrightarrow q$ is $\sim p \longrightarrow \sim q$.

Proposition

- *A conditional statement is logically equivalent to its contrapositive.*
- *A conditional statement and its converse are not logically equivalent.*
- *A conditional statement and its inverse are not logically equivalent.*
- *The converse and the inverse of a conditional statement are logically equivalent to each other.*

2.2 The Biconditional Statement

Definition

- If p and q are two statements, the **biconditional of p and q** is the statement form "p if and only if q" and it is denoted by $p \longleftrightarrow q$.
- If both p and q have the same truth value, the biconditional $p \longleftrightarrow q$ is true, while otherwise it is false.

Truth Table for $p \longleftrightarrow q$

p	q	$p \longleftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

2.2 Necessary and Sufficient Conditions

Definition

Let r and s be two statements. Then:

- r is a **sufficient condition** for s means "if r then s."
- r is a **necessary condition** for s means "if s then r; it also means "if not r then not s."
- r is a **necessary and sufficient condition** for s means "r if and only if s."

2.3 Arguments (a)

Definition

- An **argument** is a sequence of statements.
- All statements in an argument, except for the final one, are called **premises** (or **assumptions** or **hypotheses**) and the final statement of is called the **conclusion**. The symbol $\therefore$, read "therefore," is normally placed just before the conclusion.
- An argument is **valid** if the conclusion necessarily follows from the premises in the sense that if the premises are all true, then the conclusion is also true.

2.3 Arguments (b)

Example

Is the following argument valid?

$$\begin{aligned} & p \longrightarrow q \vee \sim r \\ & q \longrightarrow p \wedge r \\ \therefore \quad & p \longrightarrow r \end{aligned}$$

2.3 Invalid Argument!

						premises		conclusion
p	q	r	$\sim r$	$q \vee \sim r$	$p \wedge r$	$p \rightarrow q \vee \sim r$	$q \rightarrow p \wedge r$	$p \rightarrow r$
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

2.3 Valid Arguments

Proposition

- **Modus ponens** *(or* **method of affirming***):*

$$\begin{array}{rl} & p \longrightarrow q \\ & p \\ \therefore & q \end{array}$$

- **Modus tollens** *(or* **method of denying***):*

$$\begin{array}{rl} & p \longrightarrow q \\ & \sim q \\ \therefore & \sim p \end{array}$$

2.3 Fallacies

Definition

A **fallacy** is an error in reasoning that results in an invalid argument.

Proposition (Two fallacies)

- **The fallacy of affirming the consequent:**

$$\begin{array}{ll} & p \longrightarrow q \\ & q \\ \therefore & p \end{array}$$

- **The fallacy of denying the antecedent:**

$$\begin{array}{ll} & p \longrightarrow q \\ & \sim p \\ \therefore & \sim q \end{array}$$

2.3 Validity versus Truth

Valid argument with false conclusion

Note that valid and invalid are not synonymous with true and false! The following argument is valid but its conclusion is false:

If John Lennon was a rock star, then John Lennon had red hair.

John Lennon was a rock star.

$\therefore$ John Lennon had red hair.

2.3 Proof by Contradiction

Proposition (Reductio ad impossibile)

If you can show that assuming p is false leads to a contradiction, then you can conclude that p is true. Formally:

$$\begin{aligned} &\sim p \longrightarrow c \\ \therefore \quad &p \end{aligned}$$

Theorem (Euclid's Theorem)

There are infinitely many prime numbers.

Proof: Suppose that $p_1 = 2 < p_2 = 3 < \ldots < p_r$ were all of the primes. Let $P = p_1 p_2 \cdots p_r + 1$ and let p be a prime dividing P. Then p can not be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P - p_1 p_2 \cdots p_r = 1$, which is impossible. So this prime p is still another prime, and $p_1, p_2, \ldots, p_r$ would not be all of the primes. ■

3. THE LOGIC OF QUANTIFIED STATEMENTS

3.1 Predicates

Definition

A **predicate** is an expression that contains a finite number of variables, each one of them defined on some specific **domain**. By assigning a value to each variable (or quantifying it) from the domain of the corresponding value, a predicate becomes a statement (proposition) and as such it may be true or false.

Examples

- Let $P(x)$ be the predicate "$x^2 > x$" (written: $P(x)\colon x^2 > x$), where the domain of variable x is the set $\mathbb{R}$ of real numbers. Apparently, when assigning the value $x = 2$, this predicate is reduced to the statement $4 > 2$, which is true, while for the value $x = \frac{1}{2}$ one gets the statement $\frac{1}{4} > \frac{1}{2}$, which is false.
- Let $P(x, y)$ be the predicate "$x = y$", where the domain of both variables x and y is $\mathbb{R}$. Trivially, $x = 2$ and $y = 2$

3.1 Predicates

Definition

Let $P(x)$ be a predicate with a variable x defined on a domain D. Then the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true, when assigned to the predicate. In other words, the truth set of $P(x)$ is denoted $\{x \in D \mid P(x)\}$.

Examples

- Let the predicate $Q(n)$: n is a factor of 8 with domain the set $\mathbb{Z}$ of all integers. Then the truth set of $Q(n)$ is the set $\{-8, -4, -2, -1, 1, 2, 4, 8\}$.
- The truth set of the predicate $P(x)$: $x^2 > x$ with domain $\mathbb{R}$ is the set $\{x \in \mathbb{R} : x > 1\}$.
- The truth set of the predicate $P(x, y)$: $x = y$ with domain $\mathbb{R}^2$ is the diagonal line in $\mathbb{R}^2$ $\{(x, y) \in \mathbb{R}^2 \mid y = x\}$.

3.1 The Universal Quantifier $\forall$

Definition

Let $Q(x)$ be a predicate and D the domain of x. A **universal statement** is a statement of the form "$\forall x \in D, Q(x)$" (read "for all x in $D, Q(x)$ holds"). This statement is defined to be true if and only if $Q(x)$ is true, for every x in D, and false if and only if $Q(x)$ is false, for at least one x in D. A value for x, for which $Q(x)$ is false, is called **counterexample** to the universal statement. Using the existential quantifier, the universal statement "$\forall x \in D, Q(x)$" is false if and only if "$\exists x$ such that $\sim Q(x)$."

Examples

- Let the predicate $Q(x)\colon x^2 \geq 0$ with domain $\mathbb{R}$. Then the statement "$\forall x \in \mathbb{R}, Q(x)$" is true.
- Let the predicate $P(x)\colon x^2 > x$ with domain $\mathbb{R}$. Then the statement "$\forall x \in \mathbb{R}, P(x)$" is false and a counterexample to this statement is $x = \frac{1}{2}$.

3.1 The Existential Quantifier $\exists$

Definition

Let $Q(x)$ be a predicate and D the domain of x. An **existential statement** is a statement of the form "$\exists x \in D$ such that $Q(x)$" (read "there exists x in D such that $Q(x)$ holds"). This statement is defined to be true if and only if $Q(x)$ is true, for at least one x in D, and false if and only if $Q(x)$ is false, for all x in D.

Examples

- Let the predicate $Q(x)\colon x > 0$ with domain $\mathbb{R}$. Then the statement "$\exists x \in \mathbb{R}$ such that $Q(x)$" is true, for $x = 1$, and false, for $x = -1$.
- Let the predicate $P(x)\colon x^2 = x$ with domain $\mathbb{Z}^+$. Then the statement "$\exists x \in \mathbb{Z}^+$ such that $P(x)$" is true, for $x = 1$, and false, for $x = 2$.

3.2 Negations of Quantified Statements

Theorem (Negation of a Universal Statement)

$$\sim (\forall x \in D, Q(x)) \equiv \exists x \in D \text{ such that } \sim Q(x).$$

Theorem (Negation of an Existential Statement)

$$\sim (\exists x \in D \text{ such that } Q(x)) \equiv \forall x \in D, \sim Q(x).$$

Theorem (Negation of a Universal Conditional Statement)

$$\sim (\forall x, \text{ if } P(x) \text{ and } Q(x)) \equiv \exists x \text{ such that } P(x) \text{ and } \sim Q(x).$$

3.2 The Relation among $\forall, \exists, \wedge$ and $\vee$

Theorem

If $Q(x)$ is a predicate and the domain D of x is the set $\{x_1, x_2, \ldots, x_n\}$, then

$$\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n),$$

$$\exists x \in D \text{ such that } Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n).$$

Definition

A statement of the form

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x)$$

is called **vacuously true** or **true by default** if and only if

$$\forall x \in D, \sim (P(x)).$$

3.3 Statements with Multiple Quantifiers

Possible Statements with Two Quantifiers

$$\forall x \in D, \exists y \in E \text{ such that } P(x, y),$$

$$\exists x \in D \text{ such that } \forall y \in E, P(x, y).$$

Examples

- Let $D = E$ be the set of married persons.
  - $\forall x \in D, \exists y \in D$ such that x is married to y. (True)
  - $\exists x \in D$ such that $\forall y \in D, x$ is married to y. (False)
- Let $D = E = \{1, 2, 3, 4, 5\}$.
  - $\forall x \in D, \exists y \in D$ such that $x + y$ is even. (True)
  - $\exists x \in D$ such that $\forall y \in D, x + y$ is odd. (False)
- Let $D = E = \mathbb{R}$.
  - $\forall x \in D, \exists y \in D$ such that $x > y$. (True)
  - $\exists x \in D$ such that $\forall y \in D, x > y$. (False)
- Let $D = E = \mathbb{R}$.
  - $\forall x \in D, \exists y \in D$ such that $y^2 = x$. (False)
  - $\exists x \in D$ such that $\forall y \in D, y^2 = x$. (False)

3.3 Negation and Order of Multiply–Quantified Statements

Negations of Multiply–Quantified Statements

$\sim (\forall x \in D, \exists y \in E \text{ such that } P(x,y)) \equiv \exists x \in D \text{ such that } \forall y \in E, \sim P(x,y)$,

$\sim (\exists x \in D \text{ such that } \forall y \in E, P(x,y)) \equiv \forall x \in D, \exists y \in E \text{ such that } \sim P(x,y)$.

Order of Multiply–Quantified Statements

- In a statement containing both $\forall$ and $\exists$, changing the order of the quantifiers usually changes the meaning of the statement.
- However, if one quantifier immediately follows another quantifier *of the same type*, then the order of the quantifiers does not affect the meaning.

3.3 Limit of a Sequence

Definition

- A sequence of real numbers $a_1, a_2, a_3, \ldots$ has a limit $L \in \mathbb{R}$ whenever:

  $\forall \varepsilon > 0, \exists N \in \mathbb{Z}^+$ such that $\forall i > N, L - \varepsilon < a_i < L + \varepsilon$.

- The negation that a sequence $a_1, a_2, a_3, \ldots$ has no limit $L \in \mathbb{R}$ is written symbolically as:

  $\exists \varepsilon > 0$ such that $\forall N \in \mathbb{Z}^+, \exists i > N$
  such that $a_i \leq L - \varepsilon \vee L + \varepsilon \leq a_i$.

3.4 Arguments with Quantified Statements

Rule of Universal Instantiation

If some property is true of *everything* in a set, then it is true of *any particular* thing in the set.

$$(\forall x \in D, P(x)) \longrightarrow (a \in D \longrightarrow P(a))$$

Proposition (Universal Modus Ponens)

$$\begin{aligned} &\forall x,\ P(x) \longrightarrow Q(x). \\ &P(a)\ \textit{for a particular } a. \\ \therefore\ &Q(a). \end{aligned}$$

Proposition (Universal Modus Tollens)

$$\begin{aligned} &\forall x,\ P(x) \longrightarrow Q(x). \\ &\sim Q(a)\ \textit{for a particular } a. \\ \therefore\ &\sim P(a). \end{aligned}$$

3.4 Argument Validity

Example

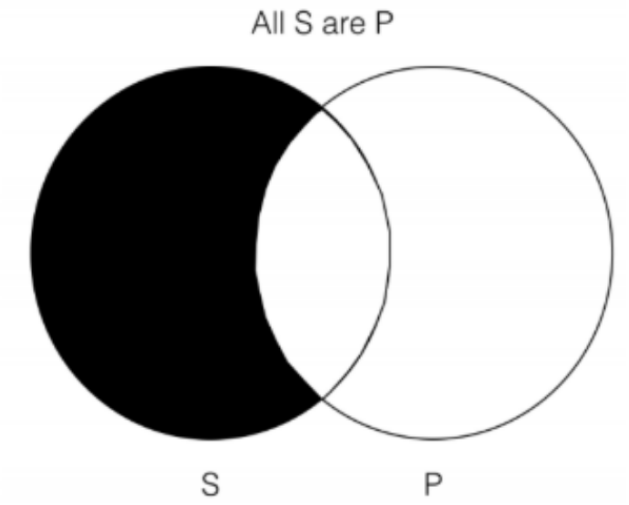
Question: Is this argument valid?

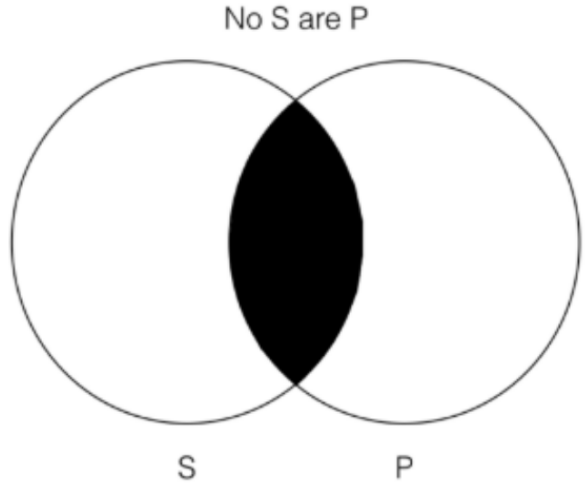
All humans are mortals.
Felix is mortal.
$\therefore$ Felix is human.

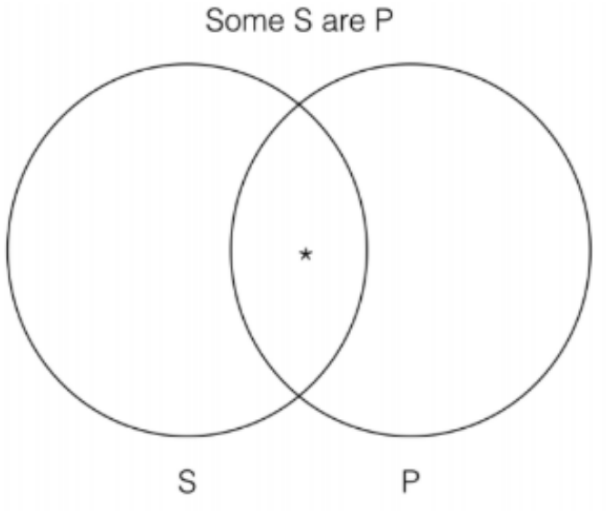
Answer: It is false because of a converse error. You may also see it using a Venn diagram.

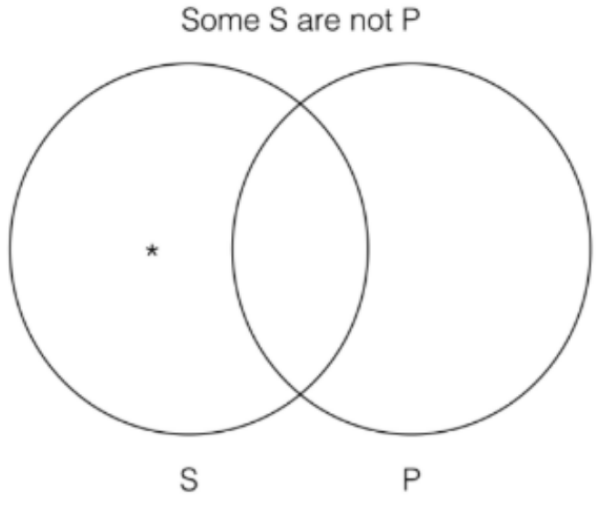
3.4 Using Venn Diagrams to Test for Validity

Any shaded portions of the Venn diagram (by "shaded" one means "blacked out") represent that there is nothing in that area of the category.









3.4 Universal Transitivity

Proposition (Universal Transitivity)

$$\begin{aligned} &\forall x,\ P(x) \longrightarrow Q(x). \\ &\forall x,\ Q(x) \longrightarrow R(x). \\ \therefore\ &\forall x,\ P(x) \longrightarrow R(x). \end{aligned}$$

4. ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

4.1 Direct Proof and Counterexample I: Assumptions

Assumptions

- Familiarity is assumed with the laws of basic algebra (listed in Appendix A of the textbook).
- The three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $\frac{3}{2}$, is not an integer, and $3 \div 0$ is not defined.

4.1 Even, Odd, Prime and Composite Integers

Definition of Even and Odd Integers

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if and only if n equals twice some integer plus 1. Symbolically, if $n \in \mathbb{Z}$, then

- n is even $\iff \exists\ k \in \mathbb{Z}$ such that $n = 2k$.
- n is odd $\iff \exists\ k \in \mathbb{Z}$ such that $n = 2k + 1$.

Definition of Prime and Composite Positive Integers

An integer n is **prime** if and only if $n > 1$ and, for all positive integers r and s, if $n = rs$, then either r or s equals n (and the other, necessarily, to 1). An integer n is **composite** if and only if $n > 1$ and $n = rs$, for some positive integers r and s, with $r < n$ and $s < n$. In symbols: For all $n \in \mathbb{Z}^+$,

- n is prime $\iff \forall\ r, s \in \mathbb{Z}^+$, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.
- n is composite $\iff \exists\ r, s \in \mathbb{Z}^+$ such that $n = rs$ and

Python Code

```
1  def is_evenodd(num):
2      if type(num) != int:
3          print(num,"is not an integer")
4      else:
5          if num%2 == 0:
6              out="%i is an even integer" %num
7  #             print(num,"is an even integer")
8          else:
9              out="%i is an odd integer" %num
10 #             print(num,"is an odd integer")
11     return out
12
13 def is_primecomposite(num):
14     # prime numbers are greater than 1
15     if type(num) != int:
16         print(num,"is not an integer")
17     else:
18         if num <= 1:
19             print(num,"is not an integer > 1")
20         else:
21             if num > 1:
22             # check for factors
23                 for i in range(2,num):
24                     if (num % i) == 0:
25                         out="%i is a composite number, %i = %ix%i" %(num, num,i,num//i)
26                         return out
27                         break
28                 else:
29                     out="%i is a prime number" %num
30                     return out
```

4.1: Constructive and Nonconstructive Proofs of Existence

Definition

- **Constructive proof of existence** is the demonstration of the existence of certain mathematical object by first identifying or constructing such an object.
- **Nonconstructive proof of existence** is the demonstration of the existence of certain mathematical object without providing a specific example or a means for producing the object. Typically a nonconstructive proof of existence involves showing one of the following:
  - Either that the existence of that object is guaranteed by an axiom or a previously proved theorem without constructing that object (**direct nonconstructive proof**).
  - Or that the assumption that there exists no such object leads to a contradiction (**nonconstructive**

4.1: An Example of Constructive Proof of Existence

Example

Show that there exists an even integer n such that n can be written in two ways as a sum of two primes.

```
E100=[n for n in range(2,101) if "even" in is_evenodd(n)]
P100=[n for n in range(2,101) if "prime" in is_primecomposite(n)]
d={}
for n in E100:
    t=[]
    for m1 in P100:
        for m2 in P100:
            if n==m1+m2:
                t.append([m1,m2])
    for s in t:
        if s[::-1] in t and s[0]!=s[1]:
            t.remove(s[::-1])
    if len(t)>1:
        d[n]=t
for k,v in d.items():
    print(k,v)
```

```
10 [[3, 7], [5, 5]]
14 [[3, 11], [7, 7]]
16 [[3, 13], [5, 11]]
18 [[5, 13], [7, 11]]
20 [[3, 17], [7, 13]]
22 [[3, 19], [5, 17], [11, 11]]
24 [[5, 19], [7, 17], [11, 13]]
26 [[3, 23], [7, 19], [13, 13]]
28 [[5, 23], [11, 17]]
30 [[7, 23], [11, 19], [13, 17]]
32 [[3, 29], [13, 19]]
```

4.1: Example of Nonconstructive Proof of Existence by Contradiction

Example (Euclid's Proof that $\sqrt{2}$ is Irrational)

Prove that $\sqrt{2}$ is an irrational number.

Proof: Assume the opposite, i.e., that $\sqrt{2} \in \mathbb{Q}$. This means that $\sqrt{2} = \frac{a}{b}$, for $a, b \in \mathbb{Z}$ $(b \neq 0)$, where we may assume that a and b have no common factors (because otherwise we could cancel them). Squaring, we get $2 = \frac{a^2}{b^2}$ or $a^2 = 2b^2$. Hence, a^2 is even and, necessarily, a is even (because the square of an odd number is odd too), i.e., $a = 2k$, for some $k \in \mathbb{Z}$. Substituting in the expression of a, we get $4k^2 = 2b^2$, i.e., that b^2 is even and hence b should be even too. But if both a and b are even, this is a contradiction to the assumption that they have no common factors. Consequently, $\sqrt{2}$ cannot be rational. ■

4.1: Example of Direct Nonconstructive Proof of Existence

Example

Prove that there exist irrational numbers a and b such that the number a^b is rational number.

Proof: We consider $a = b = \sqrt{2}$. If $\sqrt{2}^{\sqrt{2}}$ is rational, we have found the numbers $a = b = \sqrt{2}$. Otherwise (if $\sqrt{2}^{\sqrt{2}}$ is irrational), we consider $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then $a^b = (\sqrt{2})^{(\sqrt{2} \times \sqrt{2})} = (\sqrt{2})^2 = 2$, which is again rational. Thus, we have proven the statement without finding a unique object which satisfies the property of its definition. ■

4.1: Disproving Universal Statements by Counterexample

Disproof by Counterexample

To disprove a universal statement of the form "$\forall x \in D$, if $P(x)$, then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample**.

Example

Disprove the statement: $\forall x \in \mathbb{R}$, if $x < 2$, then $x^2 < 4$.

Counterexample: For any $x \leq -2$, $x^2 \geq 4$. ■

4.1: Proving Universal Statements by Exhaustion

The Method of Exhaustion

To prove a universal statement of the form "$\forall x \in D, P(x)$," when D is finite and has a very small size, then we may simply verify $P(x)$, for each individual element $x \in D$.

Example

Show that $\forall x \in \{-1, 0, 1\}, x^3 = x$.

Proof by Exhaustion: $(-1)^3 = -1, 0^3 = 0,$ and $1^3 = 1$.
■

4.1: Proving Universal Statements by Generalization

The Principle of Generalization

To prove a universal statement of the form "$\forall x \in D, P(x)$," then one may consider a **generic** element $x \in D$ and correspondingly prove $P(x)$.

Example 1

Show that $\forall x \in \mathbb{R}, x^2 + 1 > 0$.

Proof: Suppose $x \in \mathbb{R}$. Since the square of any real number is nonnegative, we have $x^2 \geq 0$. Hence, $x^2 + 1 \geq 0 + 1 = 1 > 0$. ■

Example 2

Show that the sum of any two even integers is also even.

Proof: Let $m, n \in \mathbb{Z}$ be even. Since, necessarily, $m = 2p$ and $n = 2q$, for some $p, q \in \mathbb{Z}$, it follows that $m + n = 2p + 2q = 2(p + q)$, for $p + q \in \mathbb{Z}$, i.e., $m + n$ is even. ■

4.1: Common Mistakes of Proofs

Common Mistakes

- Arguing from examples:

  Because for the particular $m = 14$ and $n = 6$, $m + n = 20$ even, it does not mean that $\forall m, n, m + n$ is even!
- Using the same letter to mean two different things:

  If $m, n \in \mathbb{Z}$ are even, then writing $m = 2k$ and $n = 2k$, for some (and the same) $k \in \mathbb{Z}$ is wrong!
- Jumping to a conclusion:

  If $m, n \in \mathbb{Z}$ are even, then although $m = 2p$ and $n = 2q$, for some $p, q \in \mathbb{Z}$, it is wrong to say that $m + n$ is even, just because $m + n = 2p + 2q$!
- Assuming what is to be proved:

  When two odd integers are multiplied, their product needs to be proved to be odd, not assumed that it is!
- Confusing what is known with what is to be shown!
- Use of *any* rather than *some*!
- Misuse of *if* (as *when*)!

4.1: Disproving Existential Statements

Recall

To disprove an existential statement is equivalent to proving that its negation is true.

Example 2

Show that the following statement is false:

$$\text{There is a } n \in \mathbb{Z}^+ \text{ such that } n^2 + 3n + 2 \text{ is prime.}$$

Proof: It suffices to show that, for all $n \in \mathbb{Z}^+$, $n^2 + 3n + 2$ is composite. Indeed, $n^2 + 3n + 2$ can be factored as $n^2 + 3n + 2 = (n + 1)(n + 2)$, where both $n + 1$ and $n + 2$ are positive integers greater than 1, and so $n^2 + 3n + 2$ is composite. ■

4.2 Rational Numbers, I

Definition

A real number r is said to be **rational** if $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$. The set of all rational numbers is denoted by $\mathbb{Q}$. Apparently, $\mathbb{Q} \subset \mathbb{R}$.

Theorem

$$\mathbb{Z} \subset \mathbb{Q}.$$

Recognizing Rational Numbers

- Real numbers with finite decimal expansions are rational. Let $x = 78.592$. Then $x = \frac{78592}{1000} \in \mathbb{Q}$.
- Real numbers with repeating decimal expansions are rational.
  - Let $x = 27.\overline{531} = 27.531531\ldots$. So, $1000x = 27531.531531\ldots$ and, hence, $999x = 1000x - x = 27504$. Therefore, $x = \frac{27504}{999} = \frac{3056}{111} \in \mathbb{Q}$.
  - Let $x = 0.35\overline{826} = 0.35826826\ldots$. So, $100000x = 35826.\overline{826}$ and $100x = 35.826$. Hence, $99900x = 100000x - 100x = 35826 - 35 = 35791$. Therefore, $x = \frac{35791}{99900} \in \mathbb{Q}$.

4.2 Rational Numbers, II

Theorem

The sum, product and ratio of two non–zero rational numbers are rational numbers.

Theorem (Expressing rational Numbers in Lowest Terms)

Given $r \in \mathbb{Q}$, *there exist unique* $a, b \in \mathbb{Z}$ *such that* $b > 0$, $\gcd(a, b) = 1$ *and* $r = \frac{a}{b}$.

Theorem (When Decimals Are Rational)

A real number written in decimal form represents a rational number if and only if the decimal part is either finite or repeating. Moreover, a rational number $r = \frac{a}{b}$ *written in lowest terms has a finite decimal expansion if and only if 2 and/or 5 are the only prime divisors of* b. *Otherwise, the decimal part of* r *repeats.*

4.2 Finite and Repeating Decimal Expansions

(A Finite Decimal Expansion)

$$\frac{63}{160} = 0.39375$$

$$\begin{array}{rl}
 & .3\ 9\ 3\ 7\ 5 \\
160\overline{)}\ & 63.0 \\
 & -4\ 8\ 0 \\
\hline
 & 1\ 5\ 0\ 0 \qquad \text{remainder } 150 \\
 & -1\ 4\ 4\ 0 \\
\hline
 & \quad 6\ 0\ 0 \qquad \text{remainder } 60 \\
 & \quad -4\ 8\ 0 \\
\hline
 & \quad 1\ 2\ 0\ 0 \qquad \text{remainder } 120 \\
 & \quad -1\ 1\ 2\ 0 \\
\hline
 & \quad\ \ 8\ 0\ 0 \qquad \text{remainder } 80 \\
 & \quad\ \ -8\ 0\ 0 \\
\hline
 & \quad\ \ \ 0 \qquad \text{remainder } 0 \leftarrow \text{END}
\end{array}$$

The decimal expansion ends when a remainder of 0 is encountered.

(A Repeating-Decimal Expansion)

$$\frac{389}{3700} = 0.10\overline{513}$$

$$\begin{array}{rl}
 & .1\ 0\ 5\ 1\ 3 \\
3700\overline{)}\ & 389.0 \\
 & -\ 3\ 7\ 0\ 0 \\
\hline
 & \quad 1\ 9\ 0\ 0 \qquad \text{remainder } 190 \\
 & \quad -\qquad 0 \\
\hline
 & \quad 1\ 9\ 0\ 0\ 0 \qquad \text{remainder } 1900 \\
 & \quad -1\ 8\ 5\ 0\ 0 \\
\hline
 & \quad\ \ 5\ 0\ 0\ 0 \qquad \text{remainder } 500 \\
 & \quad\ \ -3\ 7\ 0\ 0 \\
\hline
 & \quad\ \ 1\ 3\ 0\ 0\ 0 \qquad \text{remainder } 1300 \\
 & \quad\ \ -1\ 1\ 1\ 0\ 0 \\
\hline
 & \quad\ \ \ 1\ 9\ 0\ 0 \qquad \text{remainder } 1900
\end{array}$$

4.3 Divisibility, I

Definition

Given integers n and d (with $d \neq 0$), we say that d **divides** n, written $d|n$, if $n = dk$ for some integer k. In this case, we also say that n is **divisible** by d, that n is a **multiple** of d, that d is a **divisor** of n, and that d is a **factor** of n. When n is not divisible by d, we write $d \nmid n$.

Theorem (Transitivity of of the Divisibility Relation)

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.

Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. If $a|b$, then $a \leq b$.

4.3 Divisibility, II

Theorem (Fundamental Theorem of Arithmetic)

Any integer $n > 1$ can be written as a product of primes. Moreover, if the primes are written in nondecreasing order, then the factorization is unique. In symbols, if, on the one hand,

$$n = p_1 p_2 \cdots p_i,$$

where $p_1, p_2, \ldots, p_i$ are primes and $p_1 \leq p_2 \leq \cdots \leq p_i$, and, on the other hand,

$$n = p'_1 p'_2 \cdots p'_j,$$

where $p'_1, p'_2, \ldots, p'_j$ are primes and $p'_1 \leq p'_2 \leq \cdots \leq p'_j$, then $i = j$ and

$$p_k = p'_k, \text{ for all } k = 1, 2, \ldots, i.$$

Corollary

Any integer $n > 1$ is divisible by a prime number.

4.3 Divisibility, III

Equivalent Definition of Composite Integers

An integer $n > 1$ is composite if and only if there exists an integer r such that $r|n$ and $1 < r < n$.

Theorem

An integer $n > 1$ is composite if and only if n has a divisor r such that $2 \leq r \leq \sqrt{n}$.

Proof: If $n > 1$ is composite, there exists integer s such that $s|n$ and $1 < s < n$. There are two cases: either $s \leq \sqrt{n}$ or $s > \sqrt{n}$. In the former case, we have reached the conclusion (for $r = s$). In the latter case, since $s|n$, $n = rs$, for a second factor r such that $1 < r < n$. We claim that $r \leq \sqrt{n}$. In fact, assuming the opposite, i.e., that $r > \sqrt{n}$, we would get

$$n = rs > \sqrt{n}\sqrt{n} = n,$$

which is a contradiction. Therefore, $r|n$ and $2 \leq r \leq \sqrt{n}$. Conversely, if n has a divisor r such that $2 \leq r \leq \sqrt{n}$, then, since for $n > 1$, $\sqrt{n} < n$, we have $1 < r < n$, which implies that n is composite. ■

Python Function to Find all Factors of an Integer

To determine whether integer $n > 1$ is prime, one should check whether none of the integers in the interval from 2 to $\lfloor \sqrt{n} \rfloor$ divides n. Otherwise, one would have found a factor of n so that n would be composite.

```
import math
def primefactors(n):
    fl=[]
    while n % 2 == 0:
        fl.append(2)
        n = int(n / 2)
    for i in range(3,int(math.sqrt(n))+1,2):
        while (n % i == 0):
            fl.append(i)
            n = int(n / i)
    if n > 2:
        fl.append(n)
    p=1
    for i in fl:
        p*=i
    return fl, p
```

Practice Excercises, I

Prove the following statements:

1. The difference of any even integer minus any odd integer is odd.
2. If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd.
3. If n is any even integer, then $(-1)^n = 1$.
4. The product of any two odd integers is odd.
5. The product of any two rational numbers is a rational number.
6. The difference of any two rational numbers is a rational number.
7. If r and s are rational, then their average is rational.
8. If m is even and n is odd, then $m^2 + 3n$ is odd.

Practice Excercises, II

Prove the following statements:

9. For all integers a, b, c, if $a|b$ and $a|c$ then $a|(b \pm c)$.
10. For all integers a, b, c, if $a|b$ then $a|bc$.
11. A necessary condition for an integer to be divisible by 6 is that it be divisible by 2.

4.4 The Quotient–Remainder Theorem

Theorem (The Quotient–Remainder Theorem)

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d.$$

Definition

Given an integer n and a positive integer d,

n div d = the integer quotient obtained when n is divided by d, and

$n \bmod d$ = the nonnegative integer remainder obtained when n is divided by d.

Symbolically, if n and d are integers and $d > 0$, then

$$n \text{ div } d = q \text{ and } n \bmod d = r \iff n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

4.4 Modular Arithmetic Example

Example

If, for some integer m, $m \bmod 11 = 6$, what is $4m \bmod 11$?

$m \bmod 11 = 6$ means that $m = 11q + 6$, for some integer $q > 6$. Hence, $4m = 44q + 24$. To factor 11 from 24, we write $24 = 11 \cdot 2 + 2$, which implies that $4m = 11 \cdot 4 \cdot q + 11 \cdot 2 + 2 = 11(4q + 2) + 2$, where $4q + 2$ is a positive integer and the nonnegative remainder $2 < 4q + 2$, since $q > 0$. In other words, $4m \bmod 11 = 2$.

If, for some integer m, $m \bmod 7 = 4$, what is $5m \bmod 7$?

Now, $m = 7q + 4$, for some integer $q > 4$. Hence, $5m = 35q + 20$. To factor 7 from 20, we write $20 = 7 \cdot 2 + 6$, which implies that $5m = 7 \cdot 5 \cdot q + 7 \cdot 2 + 6 = 7(5q+2)+6$, where $5q+2$ is a positive integer and the nonnegative remainder $6 < 5q + 2$, since $q \geq 1 > \frac{4}{5}$. In other words, $5m \bmod 11 = 6$.

4.4 Parity and Consecutiveness of Integers

Definitions

- The **parity** of an integer refers to whether the integer is even or odd.
- Two integers are **consecutive** if their difference is ± 1.

Proposition

Every integer is either even or odd.

Proposition

Any two consecutive integers have opposite parity.

4.4 An Example and Division into Cases

Example

Show that the square of any odd integer is of the form $8m + 1$, for some integer m.

Proof: Let n odd, i.e., $n = 2k + 1$, for some integer k. Then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$. Let us consider the number $k(k+1)$. Since the two integers $k, k + 1$ are cosecutive, the previous proposition implies that one of them should be even and the other odd, meaning that their product should be even and, thus, $k(k + 1) = 2m$, for some integer m. Therefore, $n^2 = 4 \cdot 2m + 1 = 8m + 1$.

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or $\ldots$ or A_n then C," prove all of the following:

If A_1 then C,
If A_2 then C,
$\vdots$
If A_n then C.

Solution of the Example by Cases

Example

Show that the square of any odd integer is of the form $8m + 1$, for some integer m.

Proof: Let n odd, i.e., $n = 2k+1$, for some integer k. However, there are two cases for the integer k: either k is even, i.e., $k = 2p$, for some integer p, or k is odd, i.e., $k = 2q + 1$, for some integer q. Thus, either the odd n is $n = 2(2p)+1 = 4p+1$ (case 1) or it is $n = 2(2q+1)+1 = 4q+3$ (case 2).

Case 1: $n = 4p + 1$ and, hence, $n^2 = (4p + 1)^2 = 16p^2 + 8p + 1 = 8(2p^2+p)+1$, which is of the form $n^2 = 8m+1$, for the integer $m = 2p^2+p$.

Case 2: $n = 4q + 3$ and, hence, $n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = (16q^2 + 24q + 8) + 1 = 8(2q^2 + 3q + 1) + 1$, which is again of the form $n^2 = 8m + 1$, for the integer $m = 2q^2 + 3q + 1$.

Another Example Solved by Cases

Example

Show that, for any integer $n, n^2 - 2$ is not divisible by 5.

Proof: By the quotient-remainder theorem, any number divisible by 5 must take one of the forms:

$$5k, 5k+1, 5k+2, 5k+3, \text{ or } 5k+4,$$

for some integer k (each time different). Therefore, assuming that $n^2 - 2$ was divisible by 5, we would need to negate five cases.

Case 1: $n = 5k$ implying that $n^2 - 2 = 25k^2 - 2 = 25k^2 + (-5+5) - 2 = (25k^2 - 5) + 3 = 5(5k^2 - 1) + 3$, i.e., $(n^2 - 2) \bmod 5 = 3$, which is false, because $n^2 - 2$ being divisible by 5 means that $(n^2 - 2) \bmod 5 = 0$.

Case 2: $n = 5k + 1$ implying that $n^2 - 2 = 25k^2 + 10k + 1 - 2 = 25k^2 + 10k + (-5+5) - 1 = (25k^2 + 10k - 5) + 4 = 5(5k^2 + 2k - 1) + 4$, i.e., $(n^2 - 2) \bmod 5$ is found to be 4, instead of 0, which results something false again.

Case 3: $n = 5k+2$ implying that $n^2 - 2 = 25^2 + 20k + 4 - 2 = 25^2 + 20k + 2 = 5(5k^2 + 4k) + 2$, i.e., $(n^2 - 2) \bmod 5$ is found to be 2, instead of 0, false again.

Case 4: $n = 5k + 3$ implying that $n^2 - 2 = 25^2 + 30k + 9 - 2 = 25^2 + 30k + 5 + 2 = 5(5k^2 + 6k + 1) + 2$, i.e., $(n^2 - 2) \bmod 5$ is found to be 2, instead of 0, false again.

Case 5: $n = 5k + 4$ implying that $n^2 - 2 = 25^2 + 40k + 16 - 2 = 25^2 + 40k + 10 + 4 = 5(5k^2 + 8k + 2) + 4$, i.e., $(n^2 - 2) \bmod 5$ is found to be 4, instead of 0, false again.

4.5 Proof by Contradiction

Method of Proof by Contradiction

1. Suppose that the statement to be proved is false.
2. Then show that this supposition leads to a contradiction.
3. Therefore, the statement to be proved is true.

Examples of Statements Proved by Contradiction

- There is no greater integer.
- There is no integer that is both even and odd.
- The sum of any rational number and any irrational number is irrational.

4.5 An Example of a Proof by Contradiction

Hints how a Particular Proof by Contradiction Works

Prove by contradiction that every integer greater than 11 is a sum of two composite numbers.

Solution Hints:

1. Let us assume there exists an integer n such that $n > 11$ and n is not the sum of two composite numbers. This means that if, for two integers n_1, n_2, we have $n = n_1 + n_2$, both n_1 and n_2 cannot be composite, i.e., one of them has to be prime and the other composite.
2. We need to reach a contradiction each time we are representing n as the sum of two integers. The question is how are we going to select those integers summing up to n? An obvious answer is when we consider $n = (n - m) + m$, where $n - m$ and m are not both composite. For instance, we can take m to be even, but greater than 2, which would necessarily make m to be composite. On the other side, $n - m$ needs to be greater than 2 (in order to be possibly classified as prime) and since m has been already chosen to be an even greater than 2, necessarily, m should be one of 4, 6, and 8 (why?).

4.5 An Example of a Proof by Contradiction (continuation)

4. Therefore, for each one of the three cases $n = (n-4)+4, n = (n-6)+6, n = (n-8)+8$, it is implied that, respectively, the numbers $n-4, n-6, n-8$ are prime.
5. Using the Quotient-Remainder Theorem, since $n > 11$, n should be of the form $n = 3q + r$, for unique integers q, r such that and $0 \leq r < 3$, which means that $r = 0, 1, 2$ are the only possible remainders for the division of such n with 3.
6. The next step is to show that for each of three numbers $n-4, n-6, n-8$ (which are greater than 3, since $n > 11$) one of the possible remainders of their division with 3 contradicts the fact that these three numbers are all prime. Let us consider them separately:
   - 6.1 For the number $n-4$, we have $n-4 = 3q + r - 4$ and then the remainder $r = 1$ makes this number be $n-4 = 3q + 1 - 4 = 3q - 3 = 3(q-1)$, which is compostite and this is a cotradiction to the primeness of $n-4$.
   - 6.2 For the number $n-6$, we have $n-6 = 3q + r - 6$ and then the remainder $r = 0$ makes this number be $n-4 = 3q + 0 - 6 = 3q - 6 = 3(q-2)$, which is compostite and this is a cotradiction to the primeness of $n-6$.
   - 6.3 For the number $n-8$, we have $n-4 = 3q + r - 8$ and then the remainder $r = 2$ makes this number be $n-4 = 3q + 2 - 8 = 3q - 6 = 3(q-2)$, which is compostite

4.5 Proof by Contraposition

Method of Proof by Contraposition

1. Formulate the statement to be proved in the form $\forall x \in D,$ if $P(x),$ then $Q(x)$.
2. Then use a direct proof to show the contraposition that, if $\exists x \in D,$ such that $Q(x)$ was false, then this would imply that $P(x)$ was false too.
3. Therefore, the statement to be proved is true.

Examples of Statements Proved by Contradiction

- For all integers n, if n^2 is even, then n is even.
- For all integers n, if $n^2 - 6n + 5$ is odd, then n is odd.
- For all integers a, b, n, if $n \nmid ab$, then $n \nmid a$ and $n \nmid b$.
- For all $x \in \mathbb{R}$, if $x^3 \leq 0$, then $x \leq 0$.

4.5 An Example of a Proof by Contraposition

An Example of a Proof by Contraposition

Prove by contraposition that, for all integer a, if $a \bmod 6 = 3$ then $a \bmod 3 \neq 2$.

Proof: To use contraposition means that we need to prove the following statement:

$$\exists a \in \mathbb{Z} \text{ such that, if } a \mod 3 = 2, \text{ then } a \mod 6 \neq 3.$$

So, let the number a be any multiple of 3 plus 2 (i.e., $a \in \{5, 8, 11, 14, 17, \ldots\}$). In other words, $a \bmod 3 = 2$, which means that $a = 3q + 2$, for some integer q such that $2 < q$. There are two cases for q: q even (bigger than 4) or q odd (bigger than 3). In the former case, $q = 2k$, for some integer $k > 1$, and, hence, $a = 3(2k) + 2 = 6k + 2$, which means that $a \bmod 6 = 2 \neq 3$. In the latter case, $q = 2k + 1$, for some integer $k > 1$, and, hence, $a = 3(2k + 1) + 2 = 6k + 5$, which means that $a \bmod 6 = 5 \neq 3$.

4.6 Examples of Indirect Arguments

Examples of Indirect Arguments

- $\sqrt{2}$ is irrational.
- $1 + 3\sqrt{2}$ is irrational.
- For any integer a and any prime number p, if $p|a$, then $p \nmid (a + 1)$.
- The set of prime numbers is infinite.

4.6 Uniqueness of Quotient and Remainder

Theorem (Uniqueness of Quotient and Remainder in the Quotient-Remainder Theorem)

If $a, d \in \mathbb{Z}, d > 0$, *and if there exist* $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ *such that*

$$a = dq_1 + r_1, \text{ where } 0 \leq r_1 < d,$$
$$a = dq_2 + r_2, \text{ where } 0 \leq r_2 < d,$$

then

$$q_1 = q_2 \text{ and } r_1 = r_2.$$

Sketch of Proof: First, show that $dq_1 + r_1 = dq_2 + r_2$ (A) implies that $d|(r_2 - r_1)$. Next, show that $|r_2 - r_1| < d$. Why then (A) would imply that $r_2 - r_1 = 0$? Consequently, show that $q_1 = q_2$. Why?

4.6 Uniqueness of Quotient and Remainder

Lemma

For any $a \in \mathbb{Z}$, if $5|a^2$, then $5|a$.

Sketch of Proof: Suppose the opposite, i.e., that there exists $a \in \mathbb{Z}$ such that $5|a^2$ and $5 \nmid a$. The former condition would imply that $a^2 = 5q$, for some $q \in \mathbb{Z}$ (A). The latter condition and the Quotient–Remainder Theorem imply that $a = 5k + r$, for some $k \in \mathbb{Z}$, where $r = 1, 2, 3, 4$. (Why has $r = 0$ been excluded?) Therefore, we have four cases: $a = 5k + 1, a = 5k + 2, a = 5k + 3, a = 5k + 4$. In the first case, $a = 5k + 1$, we get $a^2 = (5k + 1)^2 = 5(5k^2 + 2k) + 1$, which is of the form $a^2 = 5q_1 + 1$, for some $q_1 \in \mathbb{Z}$ (B). However, by the quotient and remainder uniqueness, conditions (A) and (B) are contradictory. Examine the three

Proposition

$\sqrt{5} \notin \mathbb{Q}$.

Sketch of Proof: If $\sqrt{5} \in \mathbb{Q}$, then $\sqrt{5} = \frac{m}{n}$, for some $m, n \in \mathbb{Z}\,(n \neq 0)$ having no common factors. Thus, $5 = \frac{m^2}{n^2}$ or $m^2 = 5n^2$ (A). In other words, $5|m^2$ and, hence, according to the above Lemma, $5|m$ or $m = 5k$, for some $k \in \mathbb{Z}$, which means that $m^2 = (5k)^2 = 5(5k^2)$ (B). Why then (A) and (B) would imply that $n^2 = 5k^2$? Actually, the latter means that $5|n^2$ and, again by the above Lemma, $5|n$. But, then, the assumption that m and n have no common factors would be

4.6 More Propositions (Problems)

Proposition

For any $a \in \mathbb{Z}$, $9 \nmid (a^2 - 3)$.

Sketch of Proof: Assume the opposite, i.e., $a^2 - 3 = 9b$, for some $b \in \mathbb{Z}$, which would imply that $a^2 = 9b + 3 = 3(3b + 1)$ (A) or that $3|a^2$ and, thus, thanks to the Lemma, $3|a$. Then $a = 3c$, for some $c \in \mathbb{Z}$, and, hence, $a^2 = 9c^2 = 3(3c^2)$ (B). Why then would conditions (A) and (B) imply that $3b + 1 = 3c^2$? This would mean that $3|3b + 1$, but together with the obvious fact that $3|3b$, we have reached a contradiction (3 as prime number cannot divide two consecutive integers).

Proposition

$\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Sketch of Proof: Assume the opposite, i.e., $\sqrt{2} + \sqrt{3} = \frac{a}{b}$, for some $a, b \in \mathbb{Z}\,(b \neq 0)$. Thus, $a = (\sqrt{2} + \sqrt{3})b$, from which we get $\sqrt{3} = \frac{a}{b} - \sqrt{2}$. Squaring the latter and multiplying by b^2 yields (fill up details) $b^2 = a^2 - 2ab\sqrt{2}$, something which would represent $\sqrt{2} = \frac{a^2 - b^2}{2ab} \in \mathbb{Q}$ (why?) and this would be a contradiction.

4.6 An Alternative Proof of the Infinitude of Primes

Theorem

The set of prime numbers is infinite.

Sketch of Proof: Suppose not. Then there would exist a finite set of primes $P = \{2, 3, \ldots, p\}$, in which p is the largest prime and there would exist no other prime outside P. Let $M = p! + 1$. Notice that any prime in the finite set P would divide $p!$, but none would divide M (why?). However, we know that any number $M > 1$ should be divisible by a prime (Theorem 4.3.4 of divisibility by a prime), which means that there would exist a prime q such that $q|M$. Now, $q \notin P$, i.e., it would be impossible that prime $q \leq p$, because we have shown that none prime in P would divide M. Therefore, we found a prime q outside P, which is a contradiction.

4.6 Another Proposition (Problem)

Proposition

For any $n \in \mathbb{Z}$, if $n > 2$, then there exists a prime number p such that $n < p < n!$.

Sketch of Proof: By the divisibility by a prime Theorem 4.3.4, $n! - 1$ is divisible by a prime p (why?). Now, the fact that $p|(n! - 1)$ (A) makes $p \leq (n! - 1)$ and, thus, $p \leq n!$. On the other side, either $p > n$ or $p \leq n$. The latter inequality would imply that $p|n!$, but this would lead to a contradiction if it was satisfied together with (A). Hence, the former inequality ($n < p$) is true.

5. SEQUENCES, INDUCTION, AND RECURSION

5.1 Sequences

Definition

A **sequence** of numbers is a finite or infinite set of numbers S. Typically, we understand that the elements of the set S (or the values of the sequence) to be numbers in $\mathbb{Z}$ or in $\mathbb{Q}$ or in $\mathbb{R}$. All the elements of a sequence are called **terms** and the representative form of terms is called **general term** and it is written as a_k (read "a sub k"), where the subscript k in a_k is an integer which is called **index** (of the sequence). A **finite** sequence of n elements is written as $\{a_1, a_2, \ldots, a_n\}$ and an **infinite** sequence as $\{a_1, a_2, \ldots\}$. The set of indices of a sequence is called **domain** (of the sequence) and it is either a finite or an infinite set of integers, depending on whether the sequence is finite or infinite (respectively). The domain of a finite sequence is taken to be the set of all integers between two given $m, n \in \mathbb{Z}$ such that $m \leq n$, while the domain of an infinite sequence is usually taken to be the set of positive integers $\mathbb{Z}^+$. In other words, a sequence is a function with domain either an interval of integers $[m, n]$ or all positive $\mathbb{Z}^+$ and with range, typically, in $\mathbb{R}$. If we know such a function for the general term a_k of a sequence, the formula of this function is said to be the **explicit formula** or **general formula** (for the sequence).

5.1 Finding Sequences

Examples

- *Finding terms of a sequence given its general formula*:
  Example: If $a_k = \frac{k}{10+k}$, for all $k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, then the sequence is infinite with values $a_1 = \frac{1}{11}, a_2 = \frac{2}{12} = \frac{1}{6}, a_3 = \frac{3}{13}, \ldots$, i.e., the sequence is $\frac{1}{11}, \frac{1}{6}, \frac{3}{13}, \ldots$.
- **An alternating sequence** has general formula $c_j = (-1)^j$, for all integers $j \geq 0$, i.e., it is the sequence $1, -1, 1, -1, \ldots$.
- *Finding the general formula of a sequence given its terms*:
  Example: For the finite sequence $0, -\frac{1}{2}, \frac{2}{3}, -\frac{3}{4}, \frac{4}{5}, -\frac{5}{6}, \frac{6}{7}$, the general formula is $a_k = (-1)^{k-1}\left(\frac{k-1}{k}\right)$, for all integers k from 1 to 7.
  Why?

5.1 Summation of Terms of a Finite Sequence

Definition

Let $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ be a finite sequence with domain all integers between integer m and integer n, where $m \leq n$. Then $\sum_{k=m}^{n} a_k$, read **sum(mation) from** k **equals** m **to** n **of sequence** a**–sub–**k is defineed as the sum of terms of the sequence:

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

We call k **index** of the summation, m the **lower limit** of the summation and n the **upper limit** of the summation.

Notice that the summation of a sequence from m to n is a function of m and n.

5.1 Finding Sums

Examples

- *Finding sum of a finite sequence from its general formula*:

  Example: $\sum_{i=1}^{k+1} i(i!) =$

  $1(1!)+2(2!)+3(3!)+\cdots+(k+1)\big((k+1)!\big) = 1+4+18+\cdots+(k+1)^2k!.$

- **A telescoping sum**: For any integer $n \geq 1$,

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1}\right) = 1 - \frac{1}{1+n} \text{ (Why?)}$$

- *Expressing expanded summation to its general formula*:

  Example:

$$(1^3-1)-(2^3-1)+(3^3-1)-(4^3-1)+(5^3-1) = \sum_{k=1}^{5}(-1)^{k+1}(k^3-1)$$

  (**Why?**)

5.1 Product Notation

Definition

Let $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ be a finite sequence between m and n, where m, n are integers and $m \leq n$. Then the symbol $\prod_{k=m}^{n} a_k$, read the **product from** k **equals** m **to** n **of** a**–sub–**k, is the product of all terms of this finite sequence, i.e.:

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdots a_n.$$

Example

$$(1-t) \cdot (1-t^2) \cdot (1-t^3) \cdot (1-t^4) = \prod_{j=1}^{4} (1-t^j).$$

5.1 Properties of Summations and Products

Theorem

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k),$
2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k,$
3. $\left(\prod_{k=m}^{n} a_k \right) \cdot \left(\prod_{k=m}^{n} b_k \right) = \prod_{k=m}^{n} (a_k \cdot b_k).$

5.1 Transforming Sums by Change of Variables, 1

- The index of sequence in summation is a **dummy variable**:

$$\sum_{k=1}^{n} a_k = \sum_{i=1}^{n} a_i = \sum_{j=1}^{n} a_j \text{ and so on.}$$

- **Index change of variable transformation**: Let m, n two integers, $m \leq n$, and suppose that the index k of the sum $\sum_{k=m}^{n} a_k$ changes to a new index j by a transformation $j = \varphi(k)$, which is assumed to be a nondecreasing function with inverse $k = \varphi^{-1}(j)$. Then:

$$\sum_{k=m}^{n} a_k = \sum_{j=\varphi(m)}^{\varphi(n)} a_{\varphi^{-1}(j)}.$$

5.1 Transforming Sums by Change of Variables, 2

Example of Index Transformations

Show that

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{k=0}^{n} \frac{k+1}{n+(k+1)}.$$

Proof:

First, to transform the limits of summation, do the following change of variables in the left–hand sum:

$$j = k - 1 \text{ or } k = j + 1$$

to get

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{j=0}^{n} \frac{j+1}{n+(j+1)}.$$

Next, denoting the dummy variable j as k (in the right–hand side of the last equation), we get:

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{k=0}^{n} \frac{j+1}{n+(k+1)}.$$

5.1 Factorial

Definition

For each positive integer n, the quantity n **factorial**, denoted $n!$, is defined as the following product from k equals 1 to n of the sequence $a_k = k$:

$$n! = \prod_{k=1}^{n} k = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1.$$

Zero factorial, denoted $0!$, is defined to be 1:

$$0! = 1.$$

A (alternative) recursive definition for factorial

$$n! = \begin{cases} 1, & \text{if } n = 0, \\ n \cdot (n-1)!, & \text{if } n \geq 1. \end{cases}$$

5.1 The "n Choose r" Notation

Definition

Let n and r be integers with $0 \leq r \leq n$. The symbol

$$\binom{n}{r},$$

read "n **choose** r", represents the number of subsets of size r that can be chosen from a set with n elements.

Formula for computing $\binom{n}{r}$

For all integers n and r with $0 \leq r \leq n$,

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

5.1 Problems, 1

Exercise 5.1.73

For all nonnegative integers n and r with $r+1 \leq n$,

$$\binom{n}{r+1} = \frac{n-r}{r+1}\binom{n}{r}.$$

Solution:

$$\begin{aligned}
\frac{n-r}{r+1}\binom{n}{r} &= \frac{n-r}{r+1}\frac{n!}{r!(n-r)!} \\
&= \frac{n-r}{r+1}\frac{n!}{r!(n-r)(n-r-1)!} \\
&= \frac{n!}{(r+1)!(n-r-1)!} \\
&= \frac{n!}{(r+1)!(n-(r+1))!} \\
&= \binom{n}{r+1}.
\end{aligned}$$

5.1 Problems, 2

Exercise 5.1.74

If p is a prime number and r an integer such that $0 < r < p$, then $\binom{p}{r}$ is divisible by p.

Solution:

Since

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = \frac{p(p-1)!}{r!(p-r)!},$$

we get

$$p(p-1)! = \binom{p}{r}(r!(p-r)!).$$

Now, $\binom{p}{r}$ is an integer because it equals the number of subsets of size r that can be formed from a set with p elements. Thus, according to the theorem of unique factorization of integers, the right–hand side of the above equation can be expressed as a product of prime numbers. Moreover, since p is a factor of the left–hand side, p should be a factor of the right–hand side too. However, since $0 < r < p$, p cannot be a factor of either $r!$ or $(p-r)!$. Therefore, p must be a factor 0f $\binom{p}{r}$, which means that $\binom{p}{r}$ should be divisible by p.

5.2 Mathematical Induction I, 1

Principle of Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true.

Then the statement

$$\text{for all integers } n \geq a, P(n)$$

is true.

5.2 Mathematical Induction I, Example 1

Exercise 5.2.2

Use mathematical induction to show that any postage of at least 12¢ can be obtained using 3¢ and 7¢ stamps.

Solution:

Let $P(n) = \{$posting of n¢ can be obtained using 3¢ and 7¢ stamps$\}$.

Show that $P(12)$ is true: It is, because $12 = 4 \cdot 3 = 3 + 3 + 3 + 3$.

Show that for all integers $k \geq 12$, if $P(k)$ is true, then $P(k+1)$ is true: It is, because we have two cases: Either there are at least two 3¢ stamps among the k¢ stamps (where $k \geq 12$) (case 1); or there are at least two 7¢ stamps among the k¢ stamps (case 2) (**Why?**). In case 1, replace the two 3¢ stamps with one 7¢ stamp, and in case 2, remove the two 7¢ stamps and replace them with five 3¢ stamps.

5.2 Mathematical Induction I, 2

Theorem (Sum of the First n Integers)

For all integers $n \geq 1$,

$$\sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof: As in book pp. 190-1.

5.2 Mathematical Induction I, 3

Theorem (Sum of the Squares of the First n Integers)

For all integers $n \geq 1$,

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof:

It is true for $k = 1$. Assume that, for $k \geq 1$, $\sum_{j=1}^{k} j^2 = \frac{k(k+1)(2k+1)}{6}$. Then $\sum_{j=1}^{k+1} j^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{1}{6}(k+1)\Big(k(2k+1) + 6(k+1)\Big) = \frac{1}{6}(k+1)(2k^2+k+6k+6) = \frac{1}{6}(k+1)(2k^2+7k+6) = \frac{1}{6}(k+1)(2k^2+4k+3k+6) = \frac{1}{6}(k+1)\Big(2k(k+2) + 3(k+2)\Big) = \frac{1}{6}(k+1)(k+2)(2k+3) = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$.

5.2 Mathematical Induction I, Example 2

Exercise 5.2.11

$$\sum_{k=1}^{n} k^3 = 1^3 + 2^3 + 3^3 + \cdots + n^2 = \left[\frac{n(n+1)}{2}\right]^2.$$

Solution: It is true for $n = 1$. Assume that, for $k \geq 1$, $\sum_{j=1}^{k} j^3 = \frac{1}{4}\Big[n(n+1)\Big]^2$. Then $\sum_{j=1}^{k+1} j^3 = \frac{1}{4}\Big[k(k+1)\Big]^2 + (k+1)^3 = \frac{1}{4}(k+1)^2\Big[k^2 + 4(k+1)\Big] = \frac{1}{4}(k+1)^2\Big[k^2 + 4k + 4\Big] = \frac{1}{4}(k+1)^2(k+2)^2 = \frac{1}{4}\Big[(k+1)(k+2)\Big]^2 = \frac{1}{4}\Big[(k+1)\Big((k+1)+1\Big)\Big]^2$.

5.2 Mathematical Induction I, 4

Theorem (Sum of a Geometric Sequence)

For any real number r except 1 and for any integer $n \geq 0$,

$$\sum_{i=0}^{n} r^i = 1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Proof: As in book pp. 194-5.

5.2 Mathematical Induction I, Example 3

Exercise 5.2.29

Find $1-2+2^2-2^3+\cdots+(-1)^n 2^n$, where n is a positive integer.

Solution: $1-2+2^2-2^3+\cdots+(-1)^n 2^n = 1+(-2)+(-2)^2+(-2)^3+\cdots+(-2)^n$. Therefore, for $r=-2\neq 1$, the formula of the sum of a geometric sequence yields $1-2+2^2-2^3+\cdots+(-1)^n 2^n = \frac{(-2)^{n+1}-1}{(-2)-1} = \frac{(-2)^{n+1}-1}{-3} = \frac{1}{3}\left(1+(-1)^n 2^{n+1}\right)$.

5.3 Mathematical Induction II: Proving a Divisibility Property

Proposition

For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proof: As in the book pp. 201-2.

Exercise 5.3.14

For all integers $n \geq 0$, $n^3 - n$ is divisible by 6.

Sketch of Proof: Let the property $P(n) = \{n^3 - n \text{ is divisible by } 6\}$. First, we observe that $P(0)$ is true (**Why?**). Next, we will prove that, if, for all integers $k \geq 0$, $P(k)$ is true (i.e., if $k^3 - k$ is divisible by 6, which means that $k^3 - k = 6p$, for some integer p), then $P(k+1)$ should be true too (i.e., we need to show that $(k+1)^3 - (k+1)$ is divisible by 6 too). Doing the algebra (**fill up all details**), we get $(k+1)^3 - (k+1) = \ldots = 6p + 3(k(k+1))$. Since $k(k+1)$ is the product of two consequtive integers, necessarily one of the integers has to be even, and, thus, their product has to be even too, i.e., $k(k+1) = 2q$, for some integers q. Therefore, we get $(k+1)^3 - (k+1) = 6(p+q)$, which implies the wanted divisibility property.

5.3 Mathematical Induction II: Proving an Inequality

Proposition

For all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof: As in the book pp. 202-4.

Exercise 5.3.17

For all integers $n \geq 0$, $1 + 3n \leq 4^n$.

Sketch of Proof: Let the property $P(n) = \{1 + 3n \leq 4^n\}$. First, we observe that $P(0)$ is true (**Why?**). Next, we will prove that, if, for all integers $k \geq 0$, $P(k)$ is true (i.e., if $1 + 3k \leq 4^k$), then $P(k + 1)$ should be true too (i.e., we need to show that $1 + 3(k + 1) \leq 4^{k+1}$ too). Apparently, $1 + 3(k + 1) = 1 + 3k + 3 = 4 + 3k \leq 4 + 12k$, since $k \geq 0$. The reason that we have taken $12k$ is that because multiplying the inductive hypothesis $(1 + 3k \leq 4^k)$ with 4 gives $4 + 12 \leq 4 \cdot 4^k = 4^{k+1}$. Therefore, the transitivity property of order implies that $1 + 3(k + 1) \leq 4 + 12k \leq 4^{k+1}$, which is what we wanted to prove and it completes the induction.

5.3 Mathematical Induction II: Proving a Property of a Sequence

Example

Let the sequence $a_1, a_2, a_3, \ldots$ be defined as follows:

$$a_1 = 2,$$

$$a_k = 5a_{k-1}, \text{ for all integers } k \geq 2.$$

Show that $a_n = 2 \cdot 5^{n-1}$, for any integer $n \geq 1$.

Proof: As in the book pp. 204-5.

Exercise 5.3.26

A sequence $c_0, c_1, c_2, \ldots$ is defined by letting $c_0 = 3$ and $c_k = (c_{k-1})^2$, for all integers $k \geq 1$. Show that $c_n = 3^{2^n}$, for all integers $n \geq 0$.

Proof Sketch: Let $P(n) = \{c_n = 3^{2^n}\}$. First, we note that $P(0)$ is true (**Why?**). Next, we will prove that, if, for all integers $k \geq 0$, $P(k)$ is true (i.e., if $c_k = 3^{2^k}$), then $P(k+1)$ should be true (i.e., we need to show that $c_{k+1} = 3^{2^{k+1}}$). Apparently, by the definition of this sequence, $c_{k+1} = (c_k)^2 = (3^{2^k})^2 = 3^{2^k \cdot 2} = 3^{2^{k+1}}$, which is what we wanted to prove and it completes the induction.

5.3 Mathematical Induction II: An Exercise

Exercise 5.3.37

On the outside rim of a circular disk the integers from 1 through 30 are painted in random order. Show that no matter what this order is, there must be three successive integers whose sum is at least 45.

Sketch of Proof: Suppose it is impossible to find three successive integers on the rim of the disk whose sum is at least 45. Then there is some ordering of the integers from 1 to 30, say $x_1, x_2, \ldots, x_{30}$, such that

$$x_k + x_{k+1} + x_{k+2} < 45, \text{ for any } k = 1, 2, \ldots 30,$$

where, by periodicity $x_{31} = x_1, x_{32} = x_2$. Adding these inequalities, $\sum_{k=1}^{30}(x_k + x_{k+1} + x_{k+2}) < 30 \cdot 45 = 1350$, while we note that every term of this sequence appears three times, i.e., $\sum_{k=1}^{30}(x_k + x_{k+1} + x_{k+2}) = 3\sum_{i=1}^{30} x_i$, and, thus, $3\sum_{i=1}^{30} x_i < 1350$. However, $\sum_{i=1}^{30} x_i = \sum_{i=1}^{30} i = \frac{30 \cdot 31}{2} = 465$, which means that $3 \cdot 465 = 1395 < 1350$, which is a contradiction.

5.4 Strong Mathematical Induction: Steps

Proof by Induction

To show that $\forall$ integers $n \geq a, P(n)$:

1. **Basic Step**: Show that $P(a)$ is true.
2. **Inductive Step**: Show that, $\forall$ integers $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true. That is,
   - Suppose $k \geq a$ and that $P(k)$ is true.
   - Show: $P(k+1)$ is true.

Proof by Strong Induction

To show that $\forall$ integers $n \geq a, P(n)$, where $a \leq b$:

1. **Basic Steps**: Show that $P(a), \ldots, P(b)$ are true.
2. **Inductive Step**: Show that, $\forall$ integers $k \geq b$, if $P(a), \ldots, P(k)$ are true, then $P(k+1)$ is true. That is,
   - Suppose $k \geq b$ and that $P(i)$ is true, for all integers $a \leq i \leq k$.
   - Show: $P(k+1)$ is true.

5.4 Strong Mathematical Induction: Application I

Theorem

Every integer greater than 1 has a prime divisor. In symbols:

$$\forall \text{ integers } n \geq 2, \exists\, p \text{ a prime such that } p|n.$$

Proof by Strong Induction:

1. **Basic Step (for $b = a = 2$)**: Certainly, 2 is prime and divides itself.
2. **Inductive Step**: Suppose $k \geq 2$ and that each integer i with $2 \leq i \leq k$ has a prime divisor. (Goal: $k+1$ has a prime divisor.) Two cases:
   - Either $k+1$ is prime: Since, it obviously it divides itself, we have shown the goal.
   - Or $k+1$ is composite: Then $k+1 = rs$, where $2 \leq r \leq k$ and $2 \leq s \leq k$. In particular, the inductive hypothesis applies to the integer r, i.e., r has a prime divisor and, since r is a factor of $k+1$, so does $k+1$ and the goal is shown.

5.4 Strong Mathematical Induction: Application II

Theorem (Fundamental Theorem of Arithmetic)

Every integer n greater than 1 has a (unique) factorization of the form

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_m^{e_m},$$

where m is a positive integer, $p_1 < p_2 < \cdots < p_m$ are primes and $e_1, e_2, \ldots, e_m$ are positive integers (called **standard factorization***).*

Proof by Strong Induction:

1. **Basic Step (for $b = a = 2$)**: Certainly, 2 is prime and $2 = 2^1$ is a standard factorization.
2. **Inductive Step**: Suppose $k \geq 2$ and that each integer i with $2 \leq i \leq k$ has a standard factorization. (Goal: $k+1$ does too.) Two cases:
   - Either $k+1$ is prime: Since, $k+1$ is prime and $k+1 = (k+1)^1$, we have shown the goal.
   - Or $k+1$ is composite: Then $k+1 = rs$, where $2 \leq r \leq k$ and $2 \leq s \leq k$. By the inductive hypothesis, r and s have standard factorizations and, by appropriately grouping the primes in the product rs, so does $k+1$ and the goal is shown.

5.4 Strong Mathematical Induction: Application III

Exercise 5.4.7

Let $g_1, g_2, g_3, \ldots$ be a sequence defined as follows:

$$g_1 = 3, g_2 = 5,$$
$$g_k = 3g_{k-1} - 2g_{k-2}, \text{ for all integers } k \geq 3.$$

Prove that $g_n = 2^n + 1$, for all integers $n \geq 1$.

Proof by Strong Induction (Sketch):

1. **Basic Steps (for $a = 1, b = 2$)**: By definition, $g_1 = 3 = 2^1 + 1, g_2 = 5 = 2^2 + 1$.
2. **Inductive Step**: Suppose $k \geq 1$ and that for all integers i with $1 \leq i \leq k$, $g_i = 2^i + 1$. (Goal: $g_{k+1} = 2^{k+1} + 1$.)

   By definition, $g_{k+1} = 3g_k - 2g_{k-1}$, where, according to the inductive step, $g_k = 2^k + 1$ and $g_{k-1} = 2^{k-1} + 1$. Then, writing $2^k = 2 \cdot 2^{k-1}$, do the algebra to show the goal.

5.4 Strong Mathematical Induction: Application IV

Exercise 5.4.8

Let $h_0, h_1, h_2, \ldots$ be a sequence defined as follows:

$$h_0 = 1, h_1 = 2, h_3 = 3,$$
$$h_k = h_{k-1} + k_{k-2} + h_{k-3}, \text{ for all integers } k \geq 3.$$

Prove that $h_n \leq 3^n$, for all integers $n \geq 0$.

Proof by Strong Induction (Sketch):

1. **Basic Steps (for $a = 0, b = 2$)**: By definition, $h_0 = 1 = 3^0, h_1 = 2 < 3 = 3^1, h_2 = 3 < 9 = 3^2$.
2. **Inductive Step**: Suppose $k \geq 0$ and that for all integers i with $0 \leq i \leq k$, $h_i \leq 3^i$. (Goal: $h_{k+1} \leq 3^{k+1}$.)

   By definition, $h_{k+1} = h_k + k_{k-1} + h_{k-2}$, where, according to the inductive step, $h_k \leq 3^k$, $h_{k-1} \leq 3^{k-1}$ and $h_{k-2} \leq 3^{k-2}$. Then do the algebra to show the goal.

The Fibonacci Sequence

The sequence of numbers

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots,$$

is characterized by the fact that, after the first two terms, each term is obtained as the sum of the previous two. It is called **Fibonacci sequence** and, formally, it is defined as follows:

$$F_0 = 1, F_1 = 1,$$
$$F_n = F_{n-2} + F_{n-1}, \text{ for all integers } n \geq 2.$$

Show that the general formula of the Fibonacci sequence is

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

5.4 Strong Mathematical Induction: Application Vb

Proof the general form of the Fibonacci sequence by Strong Induction:

1. **Basic Steps (for $a = 0, b = 1$)**: Clearly, substituting $n = 0$ and $n = 1$ in the expression to be shown, we get the true values of the first two terms.
2. **Inductive Step**: Suppose that $k \geq 1$ and that

$$F_i = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{i+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{i+1}\right], \text{ for each } 0 \leq i \leq k.$$

(Goal: $F_{k+1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right]$.) Notice that $k + 1 \geq 2$ and that both $k - 1$ and k lie in the interval $[0, k]$. Thus, we obtain:

$$\begin{aligned} F_{k+1} &= F_{k-1} + F_k \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \left(\frac{1-\sqrt{5}}{2}\right)^{k}\right] + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right] \\ &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k} + \left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right] \end{aligned}$$

5.4 Strong Mathematical Induction: Application Vc

Proof the general form of the Fibonacci sequence by Strong Induction (continuation from previous slide):

$$
\begin{aligned}
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(1+\frac{1+\sqrt{5}}{2}\right)-\left(\frac{1-\sqrt{5}}{2}\right)^k\left(1+\frac{1-\sqrt{5}}{2}\right)\right]\\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{3+\sqrt{5}}{2}\right)-\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{3-\sqrt{5}}{2}\right)\right]\\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{1+\sqrt{5}}{2}\right)^2-\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{1-\sqrt{5}}{2}\right)^2\right]\\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+2}-\left(\frac{1-\sqrt{5}}{2}\right)^{k+2}\right],
\end{aligned}
$$

where we have used the identities:

$$
\begin{aligned}
\left(\frac{1+\sqrt{5}}{2}\right)^2 &= \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{2\cdot(3+\sqrt{5})}{2\cdot 2} = \frac{3+\sqrt{5}}{2},\\
\left(\frac{1-\sqrt{5}}{2}\right)^2 &= \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{2\cdot(3-\sqrt{5})}{2\cdot 2} = \frac{3-\sqrt{5}}{2}.
\end{aligned}
$$

5.4 Strong Mathematical Induction: Application VI

Theorem (**The Number of Multiplications Needed to Multiply n Numbers**)

Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots, x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n - 1$.

Proof by Strong Induction (Sketch): For instance, the product of two numbers involves one multiplication, the product of three numbers involves two multiplications, the product of four numbers involves three multiplications and so one. The truth of the basis step follows immediately from the convention about a product with one factor. The inductive step is based on the fact that when several numbers are multiplied together, each step of the process involves multiplying two individual quantities. For instance, the final step for computing $((x_1x_2)x_3)(x_4x_5)$ is to multiply $(x_1x_2)x_3$ and x_4x_5. In general, if $k + 1$ numbers are multiplied, the two quantities in the final step each consist of fewer than $k + 1$ factors. This is what makes it possible to use the inductive hypothesis. For the rest of the proof, see pp. 213–4 in the book.

5.4 Strong Mathematical Induction: Application VIIa

Theorem (Existence and Uniqueness of Binary Integer representations)

Given any positive integer n, n has a unique representation in the form

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.

Proof by Strong Induction: As in the book pp. 216–7.

5.4 Strong Mathematical Induction: Application VIIb

Exercise 5.4.29

Convert in decimal notation: (a) 1110_2, (b) 10111_2, (c) 110110_2, (d) 1100101_2, (e) 1000111_2, (f) 1011011_2.

Solutions In each case, $r =$ number of binary digits $- 1$.

(a) $r = 4 - 1 = 3 \Rightarrow 1110_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 8 + 4 + 2 = 14_{10}$.

(b) $r = 5 - 1 = 4 \Rightarrow 10111_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 16 + 4 + 2 + 1$
$= 23_{10}$.

(c) $r = 6 - 1 = 5 \Rightarrow 110110_2 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$
$= 32 + 16 + 4 + 2 = 54_{10}$.

(d) $r = 7 - 1 = 6 \Rightarrow 1100101_2 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$
$= 64 + 32 + 4 + 1 = 101_{10}$.

(e) $r = 7 - 1 = 6 \Rightarrow 1000111_2 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$
$= 64 + 4 + 2 + 1 = 71_{10}$.

(f) $r = \ ? - 1 = \ ? \ \Rightarrow 1011011_2 = \ ?$.

5.4 Strong Mathematical Induction: Application VIII

Theorem (Well–Ordering Principle for the Integers)

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

Proof by Strong Induction: As in the book pp. 217–8.

5.5 Defining Sequences Recursively (a)

Definition

A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$ through a function F, i.e.,

$$a_k = F(a_{k-1}, a_{k-2}, \ldots, a_{k-i})$$

where i is an integer with $k - i \geq 0$. The **initial conditions** for such a recurrence relation specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$.

The Fibonacci Sequence

$$F_k = F_{k-1} + F_{k-2}, \text{ for all integers } k \geq 2,$$
$$F_0 = 1, F_1 = 1.$$

The next four terms are easily found to be: $F_2 = F_1 + F_0 = 1 + 1 = 2$, $F_3 = F_2 + F_1 = 2 + 1 = 3, F_4 = F_3 + F_2 = 3 + 2 = 5, F_5 = F_4 + F_3 = 5 + 3 = 8, F_6 = F_5 + F_4 = 8 + +5 = 13.$

5.5 Defining Sequences Recursively (b)

The Catalan Sequence

The **Catalan numbers** are defined as

$$C_n = \frac{1}{n+1}\binom{2n}{n}, \text{ for all integers } n \geq 1.$$

Show that the sequence satisfies the recurrence relation $C_k = \frac{4k-2}{k+1}C_{k-1}$, for all integers $k \geq 2$.

First, notice that setting $n = k-1$ in the definition of this sequence, we get $C_{k-1} = \frac{1}{k-1+1}\binom{2(k-1)}{k-1} = \frac{1}{k}\binom{2k-2}{k-1}$. Therefore, to verify the recurence relation, start with the right hand side and replace the previous expression:

$$\begin{aligned}\frac{4k-2}{k+1}C_{k-1} &= \frac{4k-2}{k+1}\frac{1}{k}\binom{2k-2}{k-1} \\ &= \text{ do the algebra as in the book p. 225} \\ &= \frac{1}{k+1}\binom{2k}{k} = C_k.\end{aligned}$$

5.5 Defining Sequences Recursively (c)

Exercise 5.5.14

Let a sequence be defined as

$$d_n = 3^n - 2^n, \text{ for all integers } n \geq 0.$$

Show that the sequence satisfies the recurrence relation $d_k = 5d_{k-1} - 6d_{k-2}$, for all integers $k \geq 2$.

First, notice that by the definition of this sequence $d_{k-1} = 3^{k-1} - 2^{k-1}$ and $d_{k-2} = 3^{k-2} - 2^{k-2}$. Therefore, starting from the right hand side of the recurrence relation that we want to show:

$$\begin{aligned} 5d_{k-1} - 6d_{k-2} &= 5(3^{k-1} - 2^{k-1}) - 6(3^{k-2} - 2^{k-2}) \\ &= \textbf{do the algebra to get} \\ &= 3^k - 2^k = d_k. \end{aligned}$$

5.5 Defining Sequences Recursively (d)

Exercise 5.5.19

Show that in the **four–pole tower of Hanoi**, $s_k \leq 2s_{k-2} + 3$, for all integers $k \geq 3$, where s_k denotes the minimum number of moves needed to transfer the top k disks from the left–most to the right–most pole.

Name the poles A, B, C, and D from left to right. To transfer a tower of k disks from A to D, proceed according to the following successive steps: (1) transfer the top $k-2$ disks from A to B; (2) transfer the second largest disc from A to C; (3) transfer the largest disc from A to D; (4) transfer the second largest disc from C to D; (5) transfer the top $k-2$ disks from B to D. Thus, we obtain (**justify why the following inequalities are true**):

$$\begin{aligned} s_k &\leq s_{k-2} && \text{[Step (1)]} \\ &\quad + 1 && \text{[Step (2)]} \\ &\quad + 1 && \text{[Step (3)]} \\ &\quad + 1 && \text{[Step (4)]} \\ &\quad + s_{k-2} && \text{[Step (5)]} \\ &\leq 2s_{k-2} + 3. \end{aligned}$$

5.5 Defining Sequences Recursively (e)

Exercise 5.5.28

For the Fibonacci sequence, prove that

$$F_{k+1}^2 - F_k^2 - F_{k-1}^2 = 2F_kF_{k-1}, \text{ for all integers } k \geq 1.$$

By definition,

$$\begin{aligned} F_{k+1}^2 - F_k^2 - F_{k-1}^2 &= (F_k + F_{k-1})^2 - F_k^2 - F_{k-1}^2 \\ &= \textbf{do the algebra to get} \\ &= 2F_kF_{k-1} \end{aligned}$$

Exercise 5.5.31

For the Fibonacci sequence, prove that

$$F_n < 2^n, \text{ for all integers } n \geq 1.$$

Proof by Strong Induction (Sketch):

1. **Basic Steps (for $a = 1, b = 2$)**: By definition, $F_1 = 1 < 2 = 2^1, F_2 = 2 = 2^1$.
2. **Inductive Step**: Suppose $k \geq 1$ and that for all integers i with $1 \leq i \leq k$, $F_i < 2^i$. (Goal: $F_{k+1} < 2^{k+1}$.)
   By definition, $F_{k+1} = F_k + F_{k-1}$, where, according to the inductive step, $F_k < 2^k$ and $F_{k-1} < 2^{k-1}$. Then, writing $2^k = 2 \cdot 2^{k-1}$, do the algebra to show the goal.

5.5 Defining Sequences Recursively (f1)

Compound Interest

A person invests a_0 dollars at p percernt interest compounded annually. If A_n represents the amount at the end of n years, find a recurrence relation and initial conditions that define the sequence $A_1, A_2, \ldots$.

At the end of $n-1$ years, the amount is A_{n-1}. At the next year, we will have the amount A_{n-1} plus the interest. Thus,

$$A_n = A_{n-1} + pA_{n-1} = (1+p)A_{n-1}, \text{ for all integers } n \geq 1.$$

Clearly, the initai condition is given as $A_0 = a_0$. Therefore, we obtain:

$$A_1 = (1+p)A_0 = (1+p)a_0,$$

$$A_2 = (1+p)A_1 = (1+p)(1+p)a_0 = (1+p)^2 a_0,$$

$$A_3 = (1+p)A_2 = (1+p)(1+p)(1+p)a_0 = (1+p)^3 a_0,$$

and so on.

In other words, the recurrence rlation is

$$A_n = (1+p)^n a_0, \text{ for all integers } n \geq 1.$$

5.5 Defining Sequences Recursively (f2)

Exercise 5.5.37

Suppose a certain amount of money is deposited in an account paying 3% annual interest compounded monthly. For each positive integer n, let S_n = the amount on deposit at the end of the nth month, and let S_0 be the initial amount deposited. Find a recurrence relation for $S_0, S_1, S_2, \ldots$, assuming no additional deposits or withdrawals during the year.

When 3% interest is compounded monthly, th interest rate per month is $0.03/12 = 0.0025$. If S_k is the amount on deposit at the end of month k, then $S_k = S_{k-1} + 0.0025S_{k-1} = (1 + 0.0025)S_{k-1} = (1.0025)S_{k-1}$, for each integer $k \geq 1$.

5.5 Defining Sequences Recursively (g)

Exercise 5.5.39

A set of blocks contains blocks of heights 1, 2, and 4 centimeters. Imagine constructing towers by piling blocks of different heights directly on top of one another. (A tower of height 6 cm could be obtained using six 1-cm blocks, three 2-cm blocks, one 2-cm block with one 4-cm block on top, one 4-cm block with one 2-cm block on top, and so forth.) Let t_n be the number of ways to construct a tower of height n cm using blocks from the set. (Assume an unlimited supply of blocks of each size.) Find a recurrence relation for $t_1, t_2, t_3, \ldots$.

Let a tower have (total) height k cm and let t_k be the number of ways to construct it. There are three cases for the height h of the bottom block of any tower: (i) $h = 1$ cm, (ii) $h = 2$ cm and (iii) $h = 4$ cm. In any case, the remaining blocks (save the bottom one) make up a tower of height $(k - h)$ cm and, hence, there are t_{k-h} ways to construct it. Apparently, the total number of ways to construct the tower of k cm is equal to the sum of ways in each one of the three cases. In other words, the recurrence relation is $t_k = t_{k-1} + t_{k-2} + t_{k-4}$, for all integers $k \geq 5$.

5.6 Solving Recurrence Relations by Iteration (a)

Definition

A sequence $a_0, a_1, a_2, \ldots$ is called an **arithmetic sequence** if and only if there is a constant d such that

$$a_k = a_{k-1} + d, \text{ for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 + dn, \text{ for all integers } n \geq 0.$$

Definition

A sequence $a_0, a_1, a_2, \ldots$ is called a **geometric sequence** if and only if there is a constant r such that

$$a_k = ra_{k-1}, \text{ for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 r^n, \text{ for all integers } n \geq 1.$$

5.6 Solving Recurrence Relations by Iteration (b)

Exercise 5.5.8 & 33

Guess the formula of the sequence and use induction to verify it:

$$f_k = f_{k-1} + 2^k, \text{ for all integers } k \geq 2,$$
$$f_1 = 1.$$

$$\begin{aligned} f_1 &= 1, \\ f_2 &= f_1 + 2^2 = 1 + 2^2, \\ f_3 &= f_2 + 2^3 = 1 + 2^2 + 2^3, \\ f_4 &= f_3 + 2^4 = 1 + 2^2 + 2^3 + 2^4, \\ f_5 &= f_4 + 2^5 = 1 + 2^2 + 2^3 + 2^4 + 2^5, \\ &\vdots \end{aligned}$$

Guess: $f_n = 1 + 2^2 + 2^3 + \ldots + 2^n = \left(\frac{2^{n+1}-1}{2-1}\right) - 2 = 2^{n+1} - 3, \forall n \geq 1.$

Proof of the inductive step: $f_{k+1} = f_k + 2^{k+1} = 2^{k+1} - 3 + 2^{k+1} = 2 \cdot 2^{k+1} - 3 = 2^{k+2} - 3$. **Fill out all the remaining details.**

5.6 Solving Recurrence Relations by Iteration (c)

Exercise 5.5.10 & 35

Guess the formula of the sequence and use induction to verify it:

$$h_k = 2^k - h_{k-1}, \text{ for all integers } k \geq 1,$$

$$h_0 = 1.$$

$h_0 = 1,$

$h_1 = 2^1 - h_0 = 2^1 - 1,$

$h_2 = 2^2 - h_1 = 2^2 - (2^1 - 1) = 2^2 - 2^1 + 1,$

$h_3 = 2^3 - h_2 = 2^3 - (2^2 - 2^1 + 1) = 2^3 - 2^2 + 2^1 - 1,$

$h_4 = 2^4 - h_3 = 2^4 - (2^3 - 2^2 + 2^1 - 1) = 2^4 - 2^3 + 2^2 - 2^1 + 1,$

$\vdots$

Guess:

$$h_n = 2^n - 2^{n-1} + \ldots + (-1)^n \cdot 1 = (-1)^n[1 - 2 + 2^2 - \ldots + (-1)^n \cdot 2^n]$$

$$= (-1)^n[1 + (-2) + (-2)^2 - \ldots + (-2)^n]$$

$$= (-1)^n \left[\frac{(-2)^{n+1} - 1}{(-2) - 1}\right] = (-1)^n \frac{((-2)^{n+1} - 1)}{(-3)}$$

$$= \frac{(-1)^{n+1}}{(-1)} \cdot \frac{((-2)^{n+1} - 1)}{(-3)} = \frac{1}{3}\left[2^{n+1} - (-1)^{n+1}\right], \forall n \geq 1.$$

5.6 Solving Recurrence Relations by Iteration (c)

Exercise 5.5.10 & 35 (cont.)

Proof of the inductive step:

$$
\begin{aligned}
h_{k+1} &= 2^{k+1} - h_k \\
&= 2^{k+1} - \frac{1}{3}\left[2^{k+1} - (-1)^{k+1}\right] \\
&= \frac{1}{3}\left[3 \cdot 2^{k+1} - 2^{k+1} + (-1)^{k+1}\right] \\
&= \frac{1}{3}\left[2 \cdot 2^{k+1} - (-1)^{k+2}\right] \\
&= \frac{1}{3}\left[2^{k+2} - (-1)^{k+2}\right] \\
&= \frac{1}{3}\left[2^{(k+1)+1} - (-1)^{(k+1)+1}\right].
\end{aligned}
$$

5.6 Solving Recurrence Relations by Iteration (d)

Exercise 5.5.48

Guess the formula of the sequence and use induction to verify it:

$$u_k = u_{k-2} \cdot u_{k-1}, \text{ for all integers } k \geq 2,$$

$$u_0 = u_1 = 2.$$

$$u_0 = 2,$$

$$u_1 = 2,$$

$$u_2 = u_0 \cdot u_1 = 2 \cdot 2 = 2^{1+1} = 2^2,$$

$$u_3 = u_1 \cdot u_2 = 2 \cdot 2^2 = 2^{1+2} = 2^3,$$

$$u_4 = u_2 \cdot u_3 = 2^2 \cdot 2^3 = 2^{2+3} = 2^5,$$

$$u_5 = u_3 \cdot u_4 = 2^3 \cdot 2^5 = 2^{3+5} = 2^8,$$

$$u_6 = u_4 \cdot u_5 = 2^5 \cdot 2^8 = 2^{5+8} = 2^{13},$$

$$\vdots$$

Guess:

$u_n = 2^{F_n}$, where F_n is the nth Fibonacci number, for all integers $n \geq 0$.

5.6 Solving Recurrence Relations by Iteration (d)

Exercise 5.5.49 (cont.)

Proof of the inductive step:

$$\begin{aligned} u_{k+1} &= u_{k-1} \cdot u_k \\ &= 2^{Fk-1} \cdot 2^{Fk} \\ &= 2^{Fk-1+Fk} \\ &= 2^{Fk+1}. \end{aligned}$$

5.6 Solving Recurrence Relations by Iteration (e)

Exercise 5.5.23

Suppose the population of a country increases at a steady rate of 3% per year. If the population is 50 million at a certain time, what will it be 25 years later?

Let, for each integer $n \geq 1$, P_n denote the population at the end of year n. Then, for all integers $k \geq 1$, $k \geq 1$, $P_k = P_{k-1} + (0.03)P_{k-1} = (1.033)P_{k-1}$. Hence, $P_0, P_1, P_2, \ldots$ is a geometric sequence with constant multiplier 1.03 and, so, $P_n = (1.033)^n P_0$, for all integers $n \geq 0$. Since $P_0 = 50$ million, it follows that at the end of 25 years it would be $P_{25} = (1.033)^{25}50 \cong 104.7$ million.

5.6 Solving Recurrence Relations by Iteration (f)

Exercise 5.5.53

A single line divides a plane into two regions. Two lines (by crossing) can divide a plane into four regions; three lines can divide it into seven regions (see the figure in the book). Let P_n be the maximum number of regions into which n lines divide a plane, where n is a positive integer. (i) Derive a recurrence relation for P_k in terms of P_{k-1}, for all integers $k \geq 2$. (ii) Use iteration to guess an explicit formula for P_n.

Let us suppose that there are $k-1$ lines already drawn on the plane in such a way that they divide the plane into a maximum number P_{k-1} of regions. If addition of a new line is to create a maximum number of regions, it must cross all the $k-1$ lines that are already drawn. Furthermore, in this case, one can imagine traveling along the new line from a point before it reaches the first line it crosses to a point after it reaches the last line it crosses. This means that the new line is going to create k new regions. In other words, $P_{k-1} = P_k + k$, for all integers $k \geq 1$ and, thus, we get:

Exercise 5.5.53 (cont.)

$$
\begin{aligned}
P_1 &= 2,\\
P_2 &= P_1 + 2 = 2 + 2,\\
P_3 &= P_2 + 2 = 2 + 2 + 3,\\
P_4 &= P_3 + 2 = 2 + 2 + 3 + 4,\\
P_5 &= P_4 + 2 = 2 + 2 + 3 + 4 + 5,\\
P_6 &= P_5 + 2 = 2 + 2 + 3 + 4 + 5 + 6,\\
&\vdots
\end{aligned}
$$

Guess:

$$
\begin{aligned}
P_n &= 2 + 2 + 3 + 4 + \cdots + n = 1 + 1 + 2 + 3 + 4 + + \cdots + n\\
&= 1 + \frac{1}{2} n(n+1) = \frac{1}{2}\left(n^2 + n + 2\right).
\end{aligned}
$$

6. SET THEORY

6.1 Subsets I

Definition

- $A \subseteq B \iff \forall x,$ if $x \in A,$ then $x \in B.$
- $A \not\subseteq B \iff \exists x$ such that $x \in A$ and $x \notin B.$
- A is a **proper subset** of B, written as $A \subset B, \iff$
  1. $A \subseteq B$ and
  2. there is at least one element in B that is not in $A.$

Proving That One Set Is a Subset of Another

Let X and Y be given. To prove that $X \subseteq Y,$

1. **suppose** that x is a particular but arbitrary chosen element of $X,$
2. **show** that x is an element of $Y.$

6.1 Subsets II

Definition

Given sets A and B, A **equals** B, written $A = B$, if and only if every element of A is in B and every element of B is in A. Symbolically:

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$

Exercise 6.1.1(b)

If $A = \{3, \sqrt{5^2 - 4^2}, 24 \bmod 7\}, B = \{8 \bmod 5\}$, how are sets A, B related?

Compute $\sqrt{5^2 - 4^2}, 24 \bmod 7, 8 \bmod 5$ and find the elements of A, B. Notice that repeated elements do not count.

6.1 Subsets III

Exercise 6.1.7 (a) and (b)

Let $A = \{x \in \mathbb{Z} \mid x = 6a + 4, \text{ for } a \in \mathbb{Z}\}, B = \{y \in \mathbb{Z} \mid y = 18b - 2, \text{ for } b \in \mathbb{Z}\}$. Prove or disprove (a) $A \subseteq B$, (b) $B \subseteq A$.

First, find the integers a, b for which $x = y$. Is this happenning for all $a, b \in \mathbb{Z}$? If it is not, there exist $a, b \in \mathbb{Z}$ such that $x = 6a + 4 \neq 18b - 2 = y$. Which are these pairs of $a, b \in \mathbb{Z}$? Let us denote them as the set $D = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 6a + 4 \neq 18b + 2\}$. After we find the elements of D, we have the following cases:

1. if, for every $a \in \mathbb{Z}$, there exist $b \in \mathbb{Z}$ such that $(a, b) \in D$, then $A \subseteq B$;
2. if there exist $a \in \mathbb{Z}$, for which there exist no $b \in \mathbb{Z}$ such that $(a, b) \in D$, then $A \not\subseteq B$;
3. if, for every $b \in \mathbb{Z}$, there exist $a \in \mathbb{Z}$ such that $(a, b) \in D$, then $B \subseteq A$;
4. if there exist $b \in \mathbb{Z}$, for which there exist no $a \in \mathbb{Z}$ such that $(a, b) \in D$, then $B \not\subseteq A$.

To which case do (a) and (b) correspond?

6.1 Venn Diagramms

For instance, the relationship $A \subseteq B$ can be pictured in one of two ways, as shown in Figure 6.1.1.

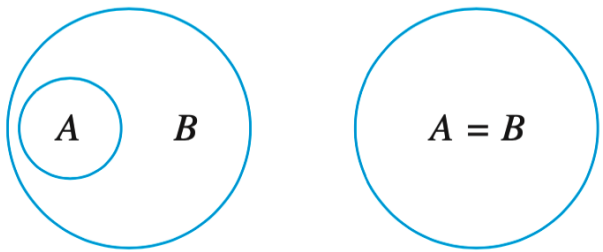


Figure 6.1.1 $A \subseteq B$

The relationship $A \not\subseteq B$ can be represented in three different ways with Venn diagrams, as shown in Figure 6.1.2.

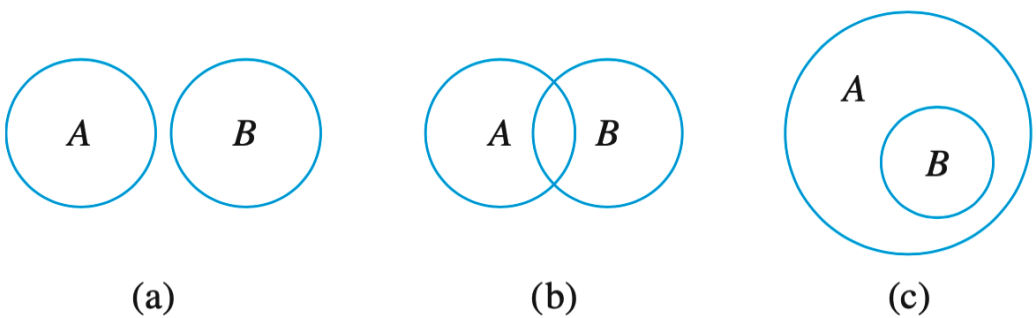


Figure 6.1.2 $A \not\subseteq B$

6.1 Operations on Sets I

Exercise 6.1.14(b)

Draw the Venn diagrams for three sets A, B, C such that $C \subseteq A, B \cap C = \varnothing$.

Definition

Let A, B subsets of a universal set U.

- The **union** of A and B, denoted $A \cup B$, is the set of all elements of U that are in A or/and in B.
- The **intersection** of A and B, denoted $A \cap B$, is the set of all elements of U that are both in A and in B.
- The **difference** of A minus B, denoted $A - B$, is the set of all elements of A that are not in B.
- The **complement** of A, denoted A^c, is the set of all elements of U that are not in A.

6.1 Operations on Sets II

Proposition

$$A - B = A \cap B^c$$

Exercise 6.1.16

Let $A = \{a, b, c\}, B = \{b, c, d\}$ and $C = \{b, c, e\}$. Find $(A - B) - C$ and $A - (B - C)$. Are they equal?

Definition

The **empty set** is the unique set $\{\} = \varnothing$ with no members.

Definition

Two sets A, B are called **disjoint** if they have no elements in common, i.e., if and only if $A \cap B = \varnothing$.

6.1 Operations on Sets III

Definition

A finite or infinite number of sets $A_1, A_2, A_3, \ldots$ are **mutually disjoint** (or **pairwise disjoint** or **nonoverlapping**) if and only if any pair of two different sets is disjoint, i.e., if and only if, for all $i, j = 1, 2, 3, \ldots, A_i \cap A_j = \varnothing$, whenever $i \neq j$.

Definition

A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3, \ldots\}$ is **partition** of a set A if and only if:

1. A is the union of all the A_i, written $A = \bigcup_{i=1,2,\ldots} A_i$, and
2. the sets $A_1, A_2, A_3, \ldots$ are mutually disjoint.

6.1 Operations on Sets IV

Definition

Given a set A, the **power set** of A, denoted $\mathscr{P}(A)$, is the set of all subsets of A.

Definition

Given sets $A_1, A_2, \ldots, A_n$, the **Cartesian product** of $A_1, A_2, \ldots, A_n$, denoted $A_1 \times A_2 \times A_3 \times \cdots \times A_n$, is the set of all ordered n–tuples $\{(a_1, a_2, \ldots, a_n)\}$, where $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$. Symbolically:

$$A_1 \times A_2 \times A_3 \times \cdots \times A_n = \{(a_1, \ldots, a_n) | a_i \in A_i, i = 1, \ldots, n\}.$$

In particular, the Cartesian product of A, B is:

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

6.1 Operations on Sets V

Exercise 6.1.35 (c) and (d)

Let $A = \{a, b\}, B = \{1, 2\}$ and $C = \{2, 3\}$. Find $A \times (B \cap C)$ and $(A \times B) \cap (A \times C)$.

6.2 Properies of Sets I

Theorem (**Some Subset Relations**)

1. *Inclusion of Intersection:* $A \cap B \subseteq A$ *and* $A \cap B \subseteq B$.
2. *Inclusion in Union:* $A \subseteq A \cup B$ *and* $B \subseteq A \cup B$.
3. *Transitive Property of Sets: If* $A \subseteq B$ *and* $B \subseteq C$, *then* $A \subseteq C$.

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,

   (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.

2. *Associative Laws:* For all sets A, B, and C,

   (a) $(A \cup B) \cup C = A \cup (B \cup C)$ and
   (b) $(A \cap B) \cap C = A \cap (B \cap C)$.

3. *Distributive Laws:* For all sets, A, B, and C,

   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

4. *Identity Laws:* For all sets A,

   (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.

6.2 Properies of Sets II

5. *Complement Laws:*

$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$

6. *Double Complement Law:* For all sets A,

$$(A^c)^c = A.$$

7. *Idempotent Laws:* For all sets A,

$$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$

8. *Universal Bound Laws:* For all sets A,

$$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \emptyset = \emptyset.$$

9. *De Morgan's Laws:* For all sets A and B,

$$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$

10. *Absorption Laws:* For all sets A and B,

$$\text{(a) } A \cup (A \cap B) = A \quad \text{and} \quad \text{(b) } A \cap (A \cup B) = A.$$

11. *Complements of U and $\emptyset$:*

$$\text{(a) } U^c = \emptyset \quad \text{and} \quad \text{(b) } \emptyset^c = U.$$

12. *Set Difference Law:* For all sets A and B,

$$A - B = A \cap B^c.$$

6.2 Properies of Sets III

Exercise 6.2.10

$$(A - B) \cap (C - B) = (A \cap C) - B.$$

First, we'll show that $(A - B) \cap (C - B) \subseteq (A \cap C) - B$.

Let $x \in (A - B) \cap (C - B)$. Thus, by definition of intersection, $x \in A - B$ and $x \in C - B$ and, then, by definition of difference, $x \in A$ and $x \notin B$ and $x \in C$ and $x \notin B$. Hence, $x \in A \cap C$ (**why?**), which implies that $x \in (A \cap B) - B$ (**why?**).

Next, we'll show that $(A \cap C) - B \subseteq (A - B) \cap (C - B)$. (Why do these two inclusions suffice?)

Let $x \in (A \cap C) - B$. Then, by definition of difference, $x \in A \cap C$ and $x \notin B$, which also implies that $x \in A$ and $x \in C$ (**why?**). But then $x \in A - B$ and $x \in C - B$ (**why?**), which is what we wanted to show (**why?**).

Exercise 6.2.19

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

First, we'll show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Let $(x, y) \in A \times (B \cap C)$. Thus, by definition of Cartesian product, $x \in A$ and $y \in B$ and $y \in C$ (**why?**). But this means that both statements "$x \in A$ and $y \in B$" and "$x \in A$ and $y \in C$" are true. Therefore (**why?**), $(x, y) \in A \times B$ and $(x, y) \in A \times C$ and thus (**why?**), $(x, y) \in (A \times B) \cap (A \times C)$.

Next, we'll show that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. (Why do these two inclusions suffice?)

Let $(x, y) \in (A \times B) \cap (A \times C)$. Then, by definition of intersection, $(x, y) \in A \times B$ and $(x, y) \in A \times C$, which imply (**why?**) that $x \in A$ and $y \in B$ and $y \in C$. Consequently, the statement "$x \in A$ and both $y \in B$ and $y \in C$" is true, which is translated in saying "$x \in A$ and $y \in B \cap C$" (**why?**). Therefore (**why?**), $(x, y) \in A \times (B \cap C)$.

Exercise 6.2.34

$$\text{If } B \cap C \subseteq A, \text{ then } (C - A) \cap (B - A) = \varnothing.$$

Suppose the opposite is true: $(C-A)\cap(B-A) \neq \varnothing$. This means that there exists a $x \in (C-A)\cap(B-A)$. Then $x \in C$ and $x \notin A$ and $x \in B$ (**why?**). Consequently, $x \in B \cap C$ (**why?**), but, since by hypothesis $B \cap C \subseteq A$, then we get that $x \in A$, which contradicts the previous finding that $x \notin A$.

Lemma

$$(A \times B) \cap (A \times C) = A \times (B \cap C).$$

$(A \times B) \cap (A \times C) = \{(x, y) \mid x \in A, y \in B\} \cap \{(x, y) \mid x \in A, y \in C\} =$
$\{(x, y) \mid x \in A, y \in B \text{ and } y \in C\} = \{(x, y) \mid x \in A, y \in B \cap C\} = A \times (B \cap C).$

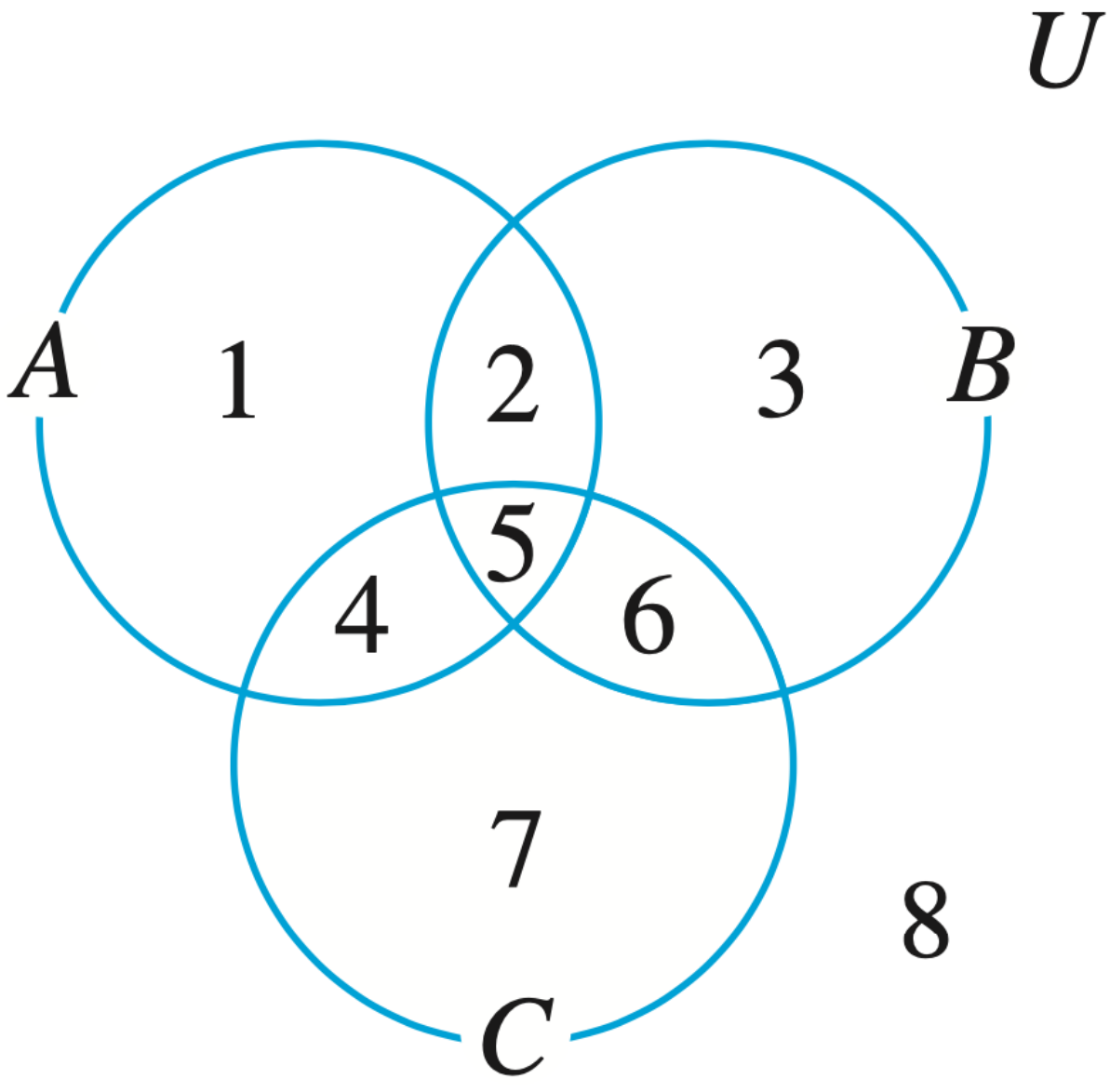
Exercise 6.2.41

For all integers $n \geq 1$, if A and $B_1, B_2, B_3, \ldots$ are any sets, then

$$\bigcap_{i=1}^{n}(A \times B_i) = A \times \left(\bigcap_{i=1}^{n} B_i\right).$$

We will prove it by induction. Certainly it is true for $n = 1$ ($A \times B_1 = A \times B_1$). Assume that, for some $k \geq 1$, $\bigcap_{i=1}^{k}(A \times B_i) = A \times \left(\bigcap_{i=1}^{k} B_i\right)$. Then $\bigcap_{i=1}^{k+1}(A \times B_i) = \left(\bigcap_{i=1}^{k}(A \times B_i)\right) \cap (A \times B_{k+1})$. Hence, by the inductive hypothesis and applying the previous Lemma, $\bigcap_{i=1}^{k+1}(A \times B_i) = \left(A \times \left(\bigcap_{i=1}^{k} B_i\right)\right) \cap (A \times B_{k+1}) = A \times \left(\left(\bigcap_{i=1}^{k} B_i\right) \cap B_{k+1}\right) = A \times \left(\bigcap_{i=1}^{k+1} B_i\right)$.

6.3 Venn Diagram for Three Sets



6.3 Counterexamples

Exercise 6.3.4

Find a counterexample to show that this is false:

$$\text{If } B \cap C \subseteq A, \text{ then } (A - B) \cap (A - C) = \varnothing.$$

Using the Venn diagramm for three sets, let us consider an example such that $B \cap C = \varnothing$. Notice that then the condition $B \cap C \subseteq A$ is satisfied, because $B \cap C = \varnothing \subseteq A$. Such an example would be when $A = \{1, 2, 3\}$, $B = \{2\}$ and $C = \{1\}$. But then $A - B = \{1, 3\}$ (**why?**) and $A - C = \{1, 2\}$ (**why?**) and, thus, $(A - B) \cap (A - C) \neq \varnothing$ (**why?**).

Theorem

For all integers $n \geq 0$, if a set X has n elements, then its power set $\mathscr{P}(X)$ has 2^n elements.

6.3 Power Set

Exercise 6.3.19

$$\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B).$$

Let $X \in \mathscr{P}(A) \cup \mathscr{P}(B)$. Then $X \in \mathscr{P}(A)$ or $X \in \mathscr{P}(B)$. In the former case, $X \subseteq A$ and, thus, $X \subseteq A \cup B$. What about in the latter case? Then, what will we get in either case and what does it mean?

Exercise 6.3.23

Let $S = \{a, b, c\}$ and, for each integer $i = 0, 1, 2, 3$, let S_i be the set of all subsets of S that have i elements. List the elements in S_0, S_1, S_2, and S_3. Is $\{S_0, S_1, S_2, S_3\}$ a partition of $\mathscr{P}(S)$?

$S_0 = \{\varnothing\}, S_1 = \{\{a\}, \ldots\}, S_2 = \{\{a, b\}, \ldots\}, S_3 = \{\ldots\}$. Fill up these sets and explain whether they form a partition of $\mathscr{P}(S)$.

6.3 "Algebraic" Proofs of Set Identities

Set Identities

(a) Commutative Laws
(b) Assosiative Laws
(c) Distributive Laws
(d) Identity Laws
(e) Complement Laws
(f) Double Complement Law
(g) Idempotend Laws
(h) Universal Bound Laws
(i) De Morgan's Laws
(j) Absorption Laws
(k) Complements of U and $\varnothing$
(l) Set Difference Law

Exercise 6.3.28

Solution hint: (a) By Set Difference Law, (b) By Set Difference Law, (c) By Commutative Laws, (d) By De Morgan's Laws, etc. **Fill it up!**

Exercise 6.3.40

Solution hint: (a) By Set Difference Law (used three times), (b) By De Morgan's Laws, (c) By Commutative Laws, etc. **Fill it up!**

6.3 Symmetric Difference

Definition of **Symmetric Difference**

$$A \triangle B = (A - B) \cup (B - A)$$

Exercise 6.3.46 (d)

Apply the above formula. The final solution should be a set of 4 elements.

Exercise 6.3.52

$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$

Method 1. Consider $x \in (A \triangle B) \triangle C$ and then show that x is either exactly in one of the sets A, B, C or x is iall three of them. Start with $x \in A \triangle (B \triangle C)$ and show the same thing as previously.

Method 2. By "algebraic" proof (harder).

6.4 Boolean Algebras I

Logical Equivalences	Set Properties
For all statement variables p, q, and r:	For all sets A, B, and C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv p \wedge (q \wedge r)$ b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	a. $A \cup (B \cup C) = A \cup (B \cup C)$ b. $A \cap (B \cap C) = A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$
a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \emptyset$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \emptyset = \emptyset$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$
a. $p \vee (p \wedge q) \equiv p$ b. $p \wedge (p \vee q) \equiv p$	a. $A \cup (A \cap B) = A$ b. $A \cap (A \cup B) = A$
a. $\sim\mathbf{t} \equiv \mathbf{c}$ b. $\sim\mathbf{c} \equiv \mathbf{t}$	a. $U^c = \emptyset$ b. $\emptyset^c = U$

6.4 Boolean Algebras II

• Definition: Boolean Algebra

A **Boolean algebra** is a set B together with two operations, generally denoted $+$ and $\cdot$, such that for all a and b in B both $a+b$ and $a\cdot b$ are in B and the following properties hold:

1. *Commutative Laws:* For all a and b in B,

$$\text{(a) } a+b=b+a \quad \text{and} \quad \text{(b) } a\cdot b=b\cdot a.$$

2. *Associative Laws:* For all a, b, and c in B,

$$\text{(a) } (a+b)+c=a+(b+c) \quad \text{and} \quad \text{(b) } (a\cdot b)\cdot c=a\cdot(b\cdot c).$$

3. *Distributive Laws:* For all a, b, and c in B,

$$\text{(a) } a+(b\cdot c)=(a+b)\cdot(a+c) \quad \text{and} \quad \text{(b) } a\cdot(b+c)=(a\cdot b)+(a\cdot c).$$

4. *Identity Laws:* There exist distinct elements 0 and 1 in B such that for all a in B,

$$\text{(a) } a+0=a \quad \text{and} \quad \text{(b) } a\cdot 1=a.$$

5. *Complement Laws:* For each a in B, there exists an element in B, denoted $\overline{a}$ and called the **complement** or **negation** of a, such that

$$\text{(a) } a+\overline{a}=1 \quad \text{and} \quad \text{(b) } a\cdot\overline{a}=0.$$

6.4 Boolean Algebras III

Theorem 6.4.1 Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Law:* For all a and x in B, if $a + x = 1$ and $a \cdot x = 0$ then $x = \overline{a}$.
2. *Uniqueness of* 0 *and* 1: If there exists x in B such that $a + x = a$ for all a in B, then $x = 0$, and if there exists y in B such that $a \cdot y = a$ for all a in B, then $y = 1$.
3. *Double Complement Law:* For all $a \in B$, $\overline{(\overline{a})} = a$.
4. *Idempotent Law:* For all $a \in B$,

$$\text{(a) } a + a = a \quad \text{and} \quad \text{(b) } a \cdot a = a.$$

5. *Universal Bound Law:* For all $a \in B$,

$$\text{(a) } a + 1 = 1 \quad \text{and} \quad \text{(b) } a \cdot 0 = 0.$$

6. *De Morgan's Laws:* For all a and $b \in B$,

$$\text{(a) } \overline{a + b} = \overline{a} \cdot \overline{b} \quad \text{and} \quad \text{(b) } \overline{a \cdot b} = \overline{a} + \overline{b}.$$

7. *Absorption Laws:* For all a and $b \in B$,

$$\text{(a) } (a + b) \cdot a = a \quad \text{and} \quad \text{(b) } (a \cdot b) + a = a.$$

8. *Complements of* 0 *and* 1:

$$\text{(a) } \overline{0} = 1 \quad \text{and} \quad \text{(b) } \overline{1} = 0.$$

Exercise 6.4.2

Solution hint: Use the complement and the associative laws for $+$. Which ones when?

Exercise 6.4.10

Solution hint: Use the result of Exercise 6.4.3, the commutative and distributive laws for $+$ and $\cdot$, and the hypothesis. Which ones when?

Exercise 6.4.22

Can there exist a book that refers to all those books and only those books that do not refer to themselves? Explain your answer.

Solution hint: The answer is no. To find it, you need to consider two cases. In the case that such a book did not refer to itself, then it would refer to the set of all books that do not refer to themselves. But this is impossible (**why?**). In the case that the book referred to itself, then it would belong to the set of books to which it refers and this set contains only books which do not refer to themselves. Obviously, this is again impossible (**why?**).

6.4 Russell's Paradox II

Exercise 6.4.25

For any set A, $\mathscr{P}(A) \not\subseteq A$.

Solution hint: Suppose that there exists a set A such that $\mathscr{P}(A) \subseteq A$. Let $B = \{x \in A \mid x \notin x\}$. Then $B \subseteq A$ and, thus, $B \in \mathscr{P}(A)$. Consequently, by what we have assumed in the beginning, i.e., that $\mathscr{P}(A) \subseteq A$, it follows that $B \in A$. Now, either $B \in B$ or $B \notin B$. In the former case, by definition of B, $B \notin B$, but if $B \notin B$, then B satisfies the defining property of B and, so, $B \in B$. Therfeore, both $B \notin B$ and $B \in B$ are true, which is a contradiction.

7. FUNCTIONS

7.1 Functions I

Definition

A **function** f **from a set** X **to a set** Y, denoted $f: X \to Y$, is a relation from X, the **domain** of f, to Y, the **co–domain**, that satisfies two properties:

1. every element in X is related to some element in Y and
2. no element in X is related to more than one element in Y.

The unique element to which f sends an element x in its domain is denoted as $f(x)$ and is called the **value of** f **at** x, or the **image of** x **under** f.

Definition (continue)

The set of all values of f taken together is called the **range of** f or the **image of** X **under** f. Symbolically:

$$\textbf{range of } f = \textbf{image of } X \textbf{ under } f = \\ = \{y \in Y \mid y = f(x), \text{ for some } x \in X\}.$$

Given an element $y \in Y$, there may exist elements $x \in X$ with y as their images. For all these x's, $f(x) = y$, and any such x is called a **preimage of** y or an **inverse image of** y. The set of all inverse images of y is called the **inverse image of** y. Symbolically:

$$\textbf{the inverse image of } y \ = \{x \in X \mid f(x) = y\}.$$

Theorem

If $F\colon X \to Y$ *and* $G\colon X \to Y$ *are functions, then* $F = G$ *if and only if* $F(x) = G(x)$*, for all* $x \in X$*.*

Exercise 7.1.14

Let $J_5 = \{0, 1, 2, 3, 4\}$ and define functions $h\colon J_5 \to J_5$ and $k\colon J_5 \to J_5$ as follows: for each $x \in J_5$,

$$h(x) = (x+3)^3 \mod 5,$$
$$k(x) = (x^3 + 4x^2 + 2x + 2) \mod 5.$$

Is $h = k$? Explain.

Complete the following table and then use the definition of set equality.

x	$(x+3)^3$	$h(x)$	$x^3 + 4x^2 + 2x + 2$	$k(x)$
0	27	$27 \ mod\ 5 = 2$	2	$2 \ mod\ 5 = 2$
1	$4^3 =$	$64 \ mod\ 5 =$	$1^3 + 4\cdot 1^2 + 2\cdot 1 + 2 =$	$9 \ mod\ 5 =$
2	$5^3 =$	$125 \ mod\ 5 =$	$2^3 + 4\cdot 2^2 + 2\cdot 2 + 2 =$	$0 \ mod\ 5 =$
3	$6^3 =$	$216 \ mod\ 5 =$	$3^3 + 4\cdot 3^2 + 2\cdot 3 + 2 =$	$71 \ mod\ 5 =$
4	$7^3 =$	$343 \ mod\ 5 =$	$4^3 + 4\cdot 4^2 + 2\cdot 4 + 2 =$	$138 \ mod\ 5 =$

7.1 Functions III: Logarithms and Logarithmic Functions (a)

Definition (Logaithms and Logarithmic Functions)

Let b be a positive real number with $b \neq 1$. For each positive real x, the **logarithm with base b of x**, written $\log_b x$, is the exponent to which b must be raised to obtain x. Symbolically:

$$\log_b x = y \iff b^y = x.$$

The **logarithmic function with base b** is the function $\log_b \colon \mathbb{R}^+ \to \mathbb{R}$ that takes each positive real number x to its logarithm with base b, i.e., $\log_b(x) = \log_b x$.

7.1 Functions III: Logarithms and Logarithmic Functions (b)

Theorem (Properties of Logarithms)

For any $a, b, c, x, y \in \mathbb{R}, b \neq 1, c \neq 1$, the following hold:

$$\text{(a)}\ \log_b(xy) = \log_b x + \log_b y,$$

$$\text{(b)}\ \log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y,$$

$$\text{(c)}\ \log_b(x^a) = a \log_b x,$$

$$\text{(d)}\ \log_c x = \frac{\log_b x}{\log_b c}.$$

7.1 Functions III: Logarithms and Logarithmic Functions (c)

Exercise 7.1.22

Use the unique factorization for the integers theorem and the definition of logarithm to prove that $\log_3(7)$ is irrational.

Suppose that $\log_3(7)$ is rational, i.e., suppose that $\log_3(7) = \frac{a}{b}$, for some integers a, b with $b \neq 0$. By the definition of logarithm, $\frac{a}{b} > 0$ (**explain!**) and, thus, we can take both $a, b > 0$. Thus, $3^{\frac{a}{b}} = 7$ or $3^a = 7^b$ (**why?**). Let $N = 3^a = 7^b$. Clearly, N is an integer and it is expressed either as $N = 3^a$ or as $N = 7^b$. But then the uniqueness of the integer factorization theorem leads to a contradiction. **Why?**

7.1 Functions IV: Functions Acting on Sets (a)

Definition

If $f : X \to Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

$$f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$$

and

$$f^{-1}(C) = \{x \in X \mid f(x) \in C\}.$$

$f(A)$ is called the **image of** A, and $f^{-1}(C)$ is called the **inverse image of** C.

Exercise 7.1.32

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$. Define $g\colon X \to Y$ as follows: $g(1) = a, g(2) = a, g(3) = a$ and $g(4) = d$.

(a) Draw an arrow diagram for g.

(b) Let $A = \{2, 3\}, C = \{a\}$ and $D = \{b, c\}$. Find $g(A), g(X), g^{-1}(C), g^{-1}(D)$ and $g^{-1}(Y)$.

Apply definitions!

Exercise 7.1.42

Let $F: X \to Y$ be a function and $C \subseteq Y$. Show that

$$F(F^{-1}(C)) \subseteq C.$$

Let $y \in F(F^{-1}(C))$. Then, by definition of image of a set, there exists $x \in F^{-1}(C)$ such that $F(x) = y$. Moreover, because $x \in F^{-1}(C)$, by definition of inverse image, $F(x) \in C$. Thus, since $F(x) = y$ and $F(x) \in C$, we conclude that $y \in C$.

7.1 Functions IV: (d)

Exercise 7.1.43

Given a set S and a subset A, the **characteristic function** of A, denoted χ_A, is the function defined from S to $\mathbb{Z}$ with the property that, for all $u \in S$,

$$\chi_A(u) = \begin{cases} 1, & \text{if } u \in A, \\ 0, & \text{if } u \notin A. \end{cases}$$

Show that each of the following holds for all subsets A and B of S and all $u \in S$.

(a) $\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$.

(b) $\chi_{A \cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$.

a.

$$\begin{aligned}
\chi_A(u)\cdot\chi_B(u) &= \begin{cases} 1\cdot 1 & \text{if } u\in A \text{ and } u\in B \\ 1\cdot 0 & \text{if } u\in A \text{ and } u\notin B \\ 0\cdot 1 & \text{if } u\notin A \text{ and } u\in B \\ 0\cdot 0 & \text{if } u\notin A \text{ and } u\notin B \end{cases} \\
&= \begin{cases} 1 & \text{if } u\in A\cap B \\ 0 & \text{if } u\notin A\cap B \end{cases} \\
&= \chi_{A\cap B}(u)
\end{aligned}$$

b.

$$\begin{aligned}
\chi_A(u)+\chi_B(u)-\chi_A(u)\cdot\chi_B(u) &= \begin{cases} 1+1-1\cdot 1 & \text{if } u\in A \text{ and } u\in B \\ 1+0-1\cdot 0 & \text{if } u\in A \text{ and } u\notin B \\ 0+1-0\cdot 1 & \text{if } u\notin A \text{ and } u\in B \\ 0+0-0\cdot 0 & \text{if } u\notin A \text{ and } u\notin B \end{cases} \\
&= \begin{cases} 1 & \text{if } u\in A \text{ and } u\in B \\ 1 & \text{if } u\in A \text{ and } u\notin B \\ 1 & \text{if } u\notin A \text{ and } u\in B \\ 0 & \text{if } u\notin A \text{ and } u\notin B \end{cases} \\
&= \begin{cases} 1 & \text{if } u\in A\cup B \\ 0 & \text{if } u\notin A\cup B \end{cases} \\
&= \chi_{A\cup B}(u)
\end{aligned}$$

7.2 One–to–One Functions (a)

Definition

A function $F : X \to Y$ is called **one–to–one** (or **injective**) if and only if, for all $x_1, x_2 \in X$,

$$\text{if } F(x_1) = F(x_2), \text{ then } x_1 = x_2,$$

or, equivalently,

$$\text{if } x_1 \neq x_2, \text{ then } F(x_1) \neq F(x_2).$$

Notice that F is **not one–to–one** if and only if there exist $x_1, x_2 \in X$ such that

$$x_1 \neq x_2 \text{ and } F(x_1) = F(x_2).$$

7.2 One–to–One Functions (b)

Exercise 7.2.17

Show that the following function is one–to–one:

$$f(x) = \frac{3x - 1}{x}.$$

Let x_1, x_2 be any non–zero real numbers such that $f(x_1) = f(x_2)$. This means that $\frac{3x_1 - 1}{x} = \frac{3x_2 - 1}{x}$. Then, do the algebra to get $x_1 = x_2$.

7.2 One–to–One Functions (c)

Exercise 7.2.25

Define $F : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ and $G : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ as follows: for all $(n, m) \in \mathbb{Z}^+ \times \mathbb{Z}^+$,

$$F(n, m) = 3^n 5^m \text{ and } G(n, m) = 3^n 6^m.$$

Prove that F and G are one–to–one.

Suppose $F(a, b) = F(c, d)$, for some $(a, b), (c, d) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Then, by definition, $3^a 5^b = 3^c 5^d$. Using the unique integers factorization theorem (**explain how**), we should have $a = c$ and $b = d$, which means $(a, b) = (c, d)$. Similarly, for G, if $G(a, b) = G(c, d)$, we would have $3^a 6^b = 3^c 6^b$ or $3^{a+b} 2^b = 3^{c+d} 2^d$ (**why?**), which again using the unique integers factorization theorem (**explain how**) would imply that $a + b = c + d$ and $b = d$ and, thus, eventually $(a, b) = (c, d)$ (**why?**).

Exercise 7.2.26 (b)

Show that $\log_{16} 9 = \log_4 3$.

Let $x = \log_{16} 9$ and $y = \log_4 3$. Then, by definition of the logarithm, $16^x = 9$ and $4^y = 3$. Now, use the facts that $16 = 4^2$ and $9 = 3^2$ to get $(4^2)^x = (4^y)^2$. Then, **explain how** the last equality would reduce to $x = y$.

7.2 Onto Functions (a)

Definition

A function $F : X \to Y$ is called **onto** (or **surjective**) if and only if, given any $y \in Y$, it is possible to find a $x \in X$ such that $y = F(x)$.

Notice that F is **not onto** if and only if there exists a $y \in Y$ such that, for every $x \in X, F(x) \neq y$.

7.2 Onto Functions (b)

Exercise 7.2.35

If $F: X \to Y$ is onto, then for all $B \subseteq Y, F(F^{-1}(B)) = B$.

First, let $y \in F(F^{-1}(B))$. Then, by definition of the image set, there exists $x \in F^{-1}(B)$ such that $F(x) = y$. Moreover, by definition of the inverse image, since $x \in F^{-1}(B)$, $F(x) \in B$. But $F(x) = y$ and, thus, $y \in B$.

On the other hand, consider a $y \in B$. Because F is onto, there exists $x \in X$ such that $F(x) = y$ and, thus, by definition of inverse image, $x \in F^{-1}(B)$. Therefore, by definition of the image of a set, $F(x) \in F(F^{-1}(B))$ and, since $y = F(x), y \in F(F^{-1}(B))$.

7.2 One–to–One and Onto Functions

Definition

A function $F: X \to Y$ which is both one–to–one and onto is called **one–to–one correspondence** (or **bijection**).

Exercise 7.2.49

Show that the following function is one–to–one and onto, for all $x \in \mathbb{R}, x \neq 1$,

$$y = \frac{x+1}{x-1}.$$

First, let $x_1, x_2 \in \mathbb{R}, x_1 \neq 1, x_2 \neq 1$, be such that $\frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1}$. **Do the algebra** to deduce that $x_1 = x_2$ and, thus, the function is one–to–one.

Next, for any $y \in \mathbb{R}, y \neq 1$, consider the number $x = \frac{y+1}{y-1}$. Obviously, $x \in \mathbb{R}$ and then, **do the algebra** to find that $\frac{x+1}{x-1} = \frac{\frac{y+1}{y-1}+1}{\frac{y+1}{y-1}-1} = \cdots = y$. Therefore, the function is also onto.

7.2 Inverse Functions

Definition (**Theorem**)

If $F: X \to Y$ is one–to–one and onto, then, for any $y \in Y$ there exists an $x \in X$ such that $F(x) = y$ (because F is onto), and this x is unique (because F is one-to-one). This means that there exists a function $F^{-1} : Y \to X$, called **inverse function** for F, which is defined as follows: for any $y \in Y$,

$$F^{-1}(y) = \text{ the unique } x \in X \text{ such that } F(x) = y.$$

In other words,

$$F^{-1}(y) = x \iff y = F(x).$$

Theorem

If $F: X \to Y$ is one–to–one and onto, then $F^{-1}: Y \to X$ is also one–to–one and onto.

7.3 Composition of Functions (a)

Definition

Let $f: X \to Y$ and $g: Y \to Z$ be two functions such that range$(f) \subseteq$ domain(g), then the **composition function** of f and g, denoted as $f \circ g$, is defined as a function $g \circ f: X \to Z$ such that

$$(g \circ f)(x) = g(f(x)), \text{ for all } x \in X.$$

Exercise 7.3.2

Use arrow diagrams, to determine equality of functions.

Exercise 7.3.4

$F(x) = x^5, G(x) = x^{1/5}, x \in \mathbb{R}$.

Do the algebra to show that $(G \circ F)(x) = G(F(x)) = \cdots = x = \cdots = F(G(x)) = (F \circ G)(x)$.

7.3 Composition of Functions (b)

Exercise 7.3.11

$H, H^{-1} : \mathbb{R} - \{1\} \to \mathbb{R} - \{1\}$ are defined as $H(x) = H^{-1}(x) = \frac{x+1}{x-1}$, for all $x \in \mathbb{R} - \{1\}$. **Do the algebra** to find that $(H^{-1} \circ H)(x) = (H \circ H^{-1})(x) = H(\frac{x+1}{x-1}) = \cdots = x$.

Exercise 7.3.20

If $f : W \to X, g : X \to Y, h : Y \to Z$ are three functions, then $h \circ (g \circ f) = (h \circ g) \circ f$.

For every $w \in W$, $[h \circ (g \circ f)](w) = h((g \circ f)(w)) = h(g(f(w))) = h \circ g(f(w)) = [(h \circ g) \circ f](w)$. Thus, by the definition of equality of functions $h \circ (g \circ f) = (h \circ g) \circ f$.

7.3 Composition of Functions (c)

Definition of the Identity Function

The **identity function** on a set X, denoted as I_X, is defined as the function $I_X : X \to X$ such that $I_X(x) = x$, for all $x \in X$.

Theorem (Composition of a Function and its Inverse)

If $f : X \to Y$ is a one–to–one and onto function with inverse function $f^{-1} : Y \to X$, then

$$f^{-1} \circ f = I_X \text{ and}$$
$$f \circ f^{-1} = I_Y.$$

7.3 Composition of Functions (d)

Theorem

If $f: X \to Y$ and $g: Y \to X$ are two functions which are both one–to–one or onto, then their composition $g \circ f: X \to Y$ is one–to–one or onto (respectively).

Exercise 7.3.25

If $f: X \to Y$ and $g: Y \to X$ are two functions such that $g \circ f = I_X$ and $f \circ g = I_Y$, then show that both f and g are one–to–one and onto and $g = f^{-1}$.

Since I_X and I_Y are one–to–one and onto and by hypothesis $g \circ f = I_X$ and $f \circ g = I_Y$, the previous Theorem implies that both f and g are one–to–one and onto. Therefore, both f and g have inverse functions f^{-1} and g^{-1} (respectively). Thus, $f \circ f^{-1} = I_Y = f \circ g$. In other words, for all $y \in Y, f(f^{-1}(y)) = (f \circ f^{-1})(y) = (f \circ g)(y) = f(g(y))$. Now, since f is one–to–one, it follows that $f^{-1}(y) = g(y)$, for all $y \in Y$, and, therefore, by the definition of equality of functions $f^{-1} = g$.

7.4 Cardinlity and Sizes of Sets of Numbers (a)

Definition

Let A and B be sets. We say that A **has the same cardinality as** B if and only if there is a function $f : A \to B$, which is one–to–one and onto.

Definition

Let X be a set.

- X is called **finite** if and only if there is a positive integer n such that X has the same cardinality with the set $[n] = \{1, 2, \ldots, n\}$.
- X is called **countably infinite** if and only if X has the same cardinality with the set $\mathbb{Z}^+$, i.e., the set of positive integers.
- X is called **countable** if and only if it is either finite or countably infinite.
- X is called **uncountable** if and only if it is not countable.

7.4 Cardinlity and Sizes of Sets of Numbers (b)

Theorem (Cantor)

- *The set of all real numbers between 0 and 1 is uncountable.*
- $\mathbb{R}$ *has the same cardinality as the set of all real numbers between 0 and 1.*

8. RELATIONS

8.1 Relations on Sets

Definition

- If A and B are two sets, a **relation** R from A to B is defined as a subset of the Cartesian product $A \times B$. Moreover, given an ordered pair $(x, y) \in A \times B$, we say that x **is related to** y **by** R, written $x\,R\,y$, if and only if $(x, y) \in R$.
- Given a relation R from A to B, the **inverse relation** R^{-1} is defined as the following relation from B to A:

$$R^{-1} = \{(y, x) \in B \times A \,|\, (x, y) \in R\}.$$

- In other words,

$$x\,R^{-1}\,y \iff y\,R\,x.$$

8.1 Relations on Sets: Exercises

Exercise 8.1.11

Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let S be the "divides" relation. This is, for all $(x, y) \in A \times B, x \, S \, y \iff x \,|\, y$. Find explicitly which ordered pairs belong to S and S^{-1}.

Exercise 8.1.17

Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as: for all $x, y \in A, x \, T \, y \iff 3 \,|\, (x - y)$. Find the direct graph of T.

Exercise 8.1.20

Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S as: for all $(x, y) \in A \times B, x \, R \, y \iff |x| = |y|$ and $x \, S \, y \iff x - y$ is even. Find explicitly which ordered pairs belong to $A \times B, R, S, R \cup S$ and $R \cap S$.

8.2 Reflexivity, Symmetry and Transitivity

Definition

Let R be a relation on a set A.

1. R is **reflexive** if and only if, for all $x \in A, x \, R \, x$.
2. R is **symmetric** if and only if, for all $x, y \in A$, if $x \, R \, y$, then $y \, R \, x$.
3. R is **transitive** if and only if, for all $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$.

8.2 Reflexivity, Symmetry and Transitivity: Exercises (a)

Exercise 8.2.17

A relation P is defined on $\mathbb{Z}$ as follows: For all $m, n \in \mathbb{Z}$, $m \, P \, n \iff \exists$ a prime number p such that $p \,|\, m$ and $p \,|\, n$. Is P reflexive, symmetric, transitive?

P is not reflexive: Otherwise, there would exist a prime divisor of any integer. Counterexample: there is no prime dividing 1.

P is symmetric: Trivial. **Why?**

P is not transitive: Counterexample: find three integers m, n, k such that both pairs m, n and n, k have a common prime divisor, but the pair m, k does not.

8.2 Reflexivity, Symmetry and Transitivity: Exercises (b)

Exercise 8.2.19

Define a relation I on $\mathbb{R}$ as follows: For all real numbers x and y, $x\,I\,y \iff x - y$ is irrational. Is I reflexive, symmetric, transitive?

I is not reflexive: For all $x \in \mathbb{R}, x - x = 0$, which is not irrational.

I is symmetric: Trivial. **Why?**

I is not transitive: Counterexample: find three $x, y, z \in \mathbb{R}$ such that

$$x - y \notin \mathbb{Q}, y - z \notin \mathbb{Q}, \text{ but } x - z \in \mathbb{Q}.$$

8.2 Reflexivity, Symmetry and Transitivity: Exercises (c)

Exercise 8.2.22

Let $X = \{a, b, c\}$ and $\mathscr{P}(X)$ be the power set of X. A relation N is defined on $\mathscr{P}(X)$ as follows: For all $A, B \in \mathscr{P}(X)$, $A \, N \, B \iff$ the number of elements in A is not equal to the number of elements in B. Is N reflexive, symmetric, transitive?

N **is not reflexive**: Denoting by $|S|$ the number of elements of set S, for all $A \in \mathscr{P}(X)$, it is false to say that $|A| \neq |A|$.

N **is symmetric**: Trivial. **Why?**

N **is not transitive**: Counterexample: find three sets such that A, B, C such that $|A| \neq |B|, |B| \neq |C|$, but $|A| = |C|$.

8.3 Equivalence Relations I

Definition

- A **partition** of a set A is a collection of nonempty, mutually disjoint subsets of A, whose union is A.
- Given a partition of A, the **relation induced by the partition**, R, is defined on A as follows: For all $x, y \in A, x\,R\,y \iff$ there is a subset A_i of the partition suth that both x and y are in A_i.
- A relation on a set that satisfies the three properties of reflexivity, symmetry and transitivity is called an **equivalence relation**.

Theorem

Any relation on a set induced by a partition is an equivalence relation.

8.3 Equivalence Relations II

Definition

Let R be an equivalence relation on a set A. Then, for each $a \in A$, the **equivalence class of** a, denoted $[a]$ and called the **class of** a for short, is defined as the set of $x \in A$ such that $x \, R \, a$.

Theorem

Let R be an equivalence relation on a set A. Then the following are true:

- *For any $a, b \in A$, if $a \, R \, b$, then $[a] = [b]$.*
- *For any $a, b \in A$, either $[a] \cap [b] = \varnothing$ or $[a] = [b]$.*
- *The distinct equivalence classes of R form a partition of A.*
- *A* **representative** *of a class S of R is any $a \in A$ such that $[a] = S$.*

8.3 Equivalence Relations: Exercises (a)

Exercise 8.3.2 (b) and (c)

In $A = \{0, 1, 2, 3, 4\}$, find the relation R for the partitions (b) $\{0\}, \{1, 3, 4\}, \{2\}$ and (c) $\{0\}, \{1, 2, 3, 4\}$.

Exercise 8.3.4

Let $A = \{a, b, c, d\}$ be a set and $R = \{(a, a), (b, b), (b, d), (c, c), (d, b), (d, d)\}$ be an equivalence relation on A. Find the distinct equivalence classes of R.

Use the definition $[a] = \{x \in A \mid x \, R \, a\}$ for all $a \in A$.

Exercise 8.3.10

Let $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$ and the equivalence relation R is defined on A as follows: For all $m, n \in \mathbb{Z}$, $m \, R \, n \iff 3 \mid (m^2 - n^2)$. Find the distinct equivalence classes of R.

Use the definition $[a] = \{x \in A \mid x \, R \, a\}$ for all $a \in A$.

8.3 Equivalence Relations: Exercises (b)

Exercise 8.3.22

Let the relation D be defined on $\mathbb{Z}$ as follows: For all $m, n \in \mathbb{Z}$, $m \, D \, n \iff 3 \,|\, (m^2 - n^2)$. Prove that D is an equivalence relation and find its distinct equivalence classes.

Reflexivity: Trivial. **Why?**
Symmetry: Notice that $3 \,|\, (m^2 - n^2)$ means that $m^2 - n^2 = 3k$, for some integer k. Then, what about $n^2 - m^2$?
Transitivity: Let $m \, D \, n$ and $n \, D \, p$. Then use the definition of divisibility and some simple manipulation in order to find that $3 \,|\, (m^2 - p^2)$. **Fill in the details!**

To find the equivalence classes of D, first, notice that $m^2 - n^2 = (m - n)(m + n)$, which would imply that $m \, D \, n \iff$ which two divisibility conditions should occur? Subsequently, using the definition of divisibility, express m in terms of n in two ways, which are going to generate two equivalence classes. Which ones?

8.4 Congruence Modulo n I

In specifying time of day, we equate $10+4$ with 2 , we equate $3-7$ with 8 and we equate 1+28 with 5. These equivalences hold because the differences $(10+4)-2, (3-7)-8$ and $(1+28)-5$, respectively, are divisible by 12. In the same way, two dates fall on the same day of the week if and only if the number of days by which they differ is divisible by 7. These types of calculations are sometimes called **modular arithmetic** and they are based on the definition of **congruence modulo** n: If $m, n, d \in \mathbb{Z}$ and $d > 0$, we say that m **is congruent to** n **modulo** d and write $m \equiv n \pmod{d}$ if and only if $d \mid (m-n)$.

Definition

Let m and n be integers and let d be a positive integer. We say that m **is congruent to** n **modulo** d and write $m \equiv n \pmod{d}$ if and only if $d \mid (m-n)$.

8.4 Congruence Modulo n II

Theorem (**Modular Equivalences**)

Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are all equivalent:

1. $a \equiv b \pmod{n}$.
2. $n \mid (a - b)$.
3. $a = b + kn$, *for some* $k \in \mathbb{Z}$.
4. a *and* b *have the same (nonnegative) remainder when divided by* n.
5. $a \bmod n = b \bmod n$.

Theorem

Let $a, c, n, m \in \mathbb{Z}$ and $n > 1$. Then:

- $ma \equiv mc \pmod{n}$,
- $a^m \equiv c^m \pmod{n}$.

8.4 Congruence Modulo n: Exercises (a)

Exercise 8.4.5

Prove the transitivity of modular congruence, i.e., for all $a, b, c, n \in \mathbb{Z}$ with $n > 1$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, by the definition of congruence modulo n, $n \mid (a - b)$ and $n \mid (b - b)$. Then, by definition of divisibility, $a - b = nk$, for some $k \in \mathbb{Z}$, and $b - c = nl$, for some $l \in \mathbb{Z}$. Therefore, as $a - c = (a - b) + (b - c)$, what do you get and then what does the difinition of divisibility imply?

8.4 Congruence Modulo n: Exercises (b)

Exercise 8.3.15 (b)

Prove that, for all integers m and n and any positive integer d, $m \equiv n \pmod{d}$ if and only if $m \bmod d = n \bmod d$.

First, suppose that $m \equiv n \pmod{d}$. By definition of congruence, $d \mid (m-n)$ and, thus, $m - n = dk$, for some integer k. Furthermore, assume that $m \bmod d = r$ or $m = dl + r$, for some integer l. Therefore, after a simple substitution $n = d(l - k) + r$ (**why exactly?**), i.e., $n \bmod d = r = m \bmod d$.

Next, suppose that $m \bmod d = n \bmod d$ and set $r = m \bmod d = n \bmod d$. Then, by definition of mod, $m = dp + r$ and $n = dq + r$, for some integers p and q. Then compute $m - n$ and why would this imply that $d \mid (m - n)$, which is the definition of congruence?

8.4 Congruence Modulo n: Exercises (c)

Exercise 8.4.11

If $a, b, c, n \in \mathbb{Z}$ with $n > 1$, $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then show that $a^m \equiv c^m \pmod{n}$, for all integers $m \geq 1$. (Use strong mathematical induction on m.)

Let property $P(m)$ be the congruence $a^m \equiv c^m \pmod{n}$. $P(1)$ holds by assumption (**why??**). Next, assume that $P(k)$ holds, for all integers $k \geq 1$. (The goal is to prove that $P(k+1)$ holds too). So, assume that, for some integer $k \geq 1$, $a^k \equiv c^k \pmod{n}$. However, the inductive hypothesis $a^k \equiv c^k \pmod{n}$ is translated by the previous Theorem as $a^k = c^k + rn$, for some $r \in \mathbb{Z}$, while, by the same Theorem, $a \equiv c \pmod{n}$ means that $a = c + sn$, for some $s \in \mathbb{Z}$. Therefore, compute $a^{k+1} = a \cdot a^k$ using the previous two equations in order to conclude that $a^{k+1} \equiv c^{k+1} \pmod{n}$. **Fill in all details**.

8.4 Congruence Modulo n: Exercises (d)

Exercise 8.4.12

(a) Prove that for all integers $n \geq 0$, $10^n \equiv (-1)^n \pmod{11}$. (b) Use part (a) to prove that a positive integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

(a) follows directly from the definition of congruence modulo n (**justify!**). For (b), let $a \in \mathbb{Z}, a > 0$. Then the decimal representation of a means that there exists an integer $n \geq 0$ and $n+1$ integers $d_0, d_1, \ldots, d_n$ with $0 \leq d_k < 10$, for $k = 0, 1, \ldots, n$ (the d_k's are the **digits** of a), such that

$$a = \sum_{k=0}^{n} d_k 10^k.$$

Therefore, applying (a) and the Theorem of the properties of modular equivalences,

$$a = \sum_{k=0}^{n} d_k 10^k = \left(\sum_{k=0}^{n} d_k \cdot (-1)^k \right) \pmod{11},$$

which implies that either a or the alternating sum of its digits is divisible by 11 (**because of which property of congruence modulo n??**).

8.4 Congruence Modulo n: Exercises (e)

When an integer is written in ordinary decimal notation, its **units digit** is the digit on its extreme right. For example, the units digit of 247 is 7. The reason 7 is called the "units digit" of 247 is that when 247 is written in expanded form, it becomes $247 = 2 \cdot 100 + 4 \cdot 10 + 7 \cdot 1$. In other words, clearly, the units digit of a number is the remainder of the division with 10.

Exercise 8.4.16

What is the units digit of 3^{1789}?

First, we compute the powers of 3 until the found units digits are repeated: $3^0 = 1$ (i.e., the units digit of 3^0 is 1), $3^1 = 3$ (i.e., the units digit of 3^1 is 3), $3^2 = 9$ (i.e., the units digit of 3^2 is 9), $3^3 = 27$ (i.e., the units digit of 3^3 is 7), $3^4 = 81$ (i.e., the units digit of 3^4 is 1), which terminates the process, because the first units digit is repeated. Hence, $3^4 = 1 (\text{mod } 10)$. Next, we observe that $1789 = 4 \cdot 447 + 1$. Therefore,

$$3^{1789} = 3^{4 \cdot 447 + 1} = (3^4)^{447} \cdot 3^1 \equiv 1^{447} \cdot 3 \equiv 3 \pmod{10}.$$

So, the units digit of 3^{1789} is 3 (**why??**).

8.4 Congruence Modulo n: Exercises (f)

Exercise 8.4.19

Reduce the following two equations by modulo 6 to show that they do not have a simultaneous integer solution:

$$43x + 24y = 39,$$
$$-11x + 48y = 53.$$

We have $43 \equiv 1 \pmod 6, 24 \equiv 0 \pmod 6, 39 \equiv 3 \pmod 6$, $-11 \equiv 1 \pmod 6, 48 \equiv 0 \pmod 6, 53 \equiv 5 \pmod 6$. **Explain the derivation of these congruences**. Thus, what is the reduced system of equations and why do we get two contradictory congruences?

8.5 The Greatest Common Divisor of Two Integers

Definition

Given integers a and b not both zero, their **greatest common divisor**, denoted $\gcd a, b$, is the unique integer d such that:

1. $d > 0$,
2. $d \mid a$ and $d \mid b$,
3. for all positive integers c, if $c \mid a$ and $c \mid b$, then $c \leq d$.

Definition

Two integers a and b are called **relatively prime** if and only if $\gcd(a, b) = 1$.

Examples

- $\gcd(14, 35) = 7$.
- 21 and 8 are relative prime, since $\gcd(21, 8) = 1$.
- Any two successive integers are relatively prime!
- Given integer $k \neq 0, \gcd(k, 0) = |k|$.

8.5 Euclid's Algorithm

Theorem (**GCD Reduction**)

Let a and b two integers such that $a \geq b > 0$. Write $a = bq + r$, where $q, r \in \mathbb{Z}$ with $0 \leq q < b$. Then

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

Example

$$\begin{aligned} \gcd(48, 18) &= \gcd(18, 12) && \text{since } 48 = 18 \cdot 2 + 12 \\ &= \gcd(12, 6) && \text{since } 18 = 12 \cdot 1 + 6 \\ &= \gcd(6, 0) && \text{since } 12 = 6 \cdot 2 + 0 \\ &= 6 \end{aligned}$$

8.5 Euclid's Algorithm: Exercises

Exercise 8.5.7 and 8.5.8

$\gcd(832, 10, 933) = ?, \gcd(4, 131, 2, 431) = ?.$

Exercise 8.5.19

Find $\gcd(2583, 349)$ and express it as a linear combination of two numbers.

Start with $2583 = 349q + r$ and find q, r such that $r = 2583 - 349r$. Then do the same for 349 and r as many consecutive time it is needed to reach $r = 0$. Then substitute back the expressions for the remainder r until you reach the wanted linear combination.

8.5 Factoring

Theorem (**Euclid's Lemma**)

For all integers a, b and c, if a and c are relatively prime and $a \mid bc$, then $a \mid b$.

Corollary

Let a, b and p integers with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Example

Show that, when a, b, n are integers with $n > 0$, if a and b are relatively prime, then a and b^n are relatively prime too.

Let $d = \gcd(a, b^n)$. Suppose $d > 1$. Then, by the prime factorization Theorem, there is a prime p such that $p \mid d$. Hence $p \mid a$ and $p \mid b^n$. So $p \mid \gcd(a, b)$. However, a and b are relatively prime, i.e., $\gcd(a, b) = 1$, and it is impossible to have a prime $p \mid 1$. Therefore, $d = 1$.

8.5 GCD as a Linear Combination

Theorem

Given integers a and b not both 0, there exist integers x and y such that

$$gcd(a, b) = ax + by.$$

Corollary

Two integers a and b are relatively prime if and only if there exist integers x and y such that

$$ax + by = 1.$$

Example

$\gcd(18, 30) = 6$ and $6 = 18 \cdot (-3) + 30 \cdot 2$.

Exercise 8.5.7 and 8.5.23

Find one intger solution of the Diophantine equation $1456x + 693y = 4760$.

9. COUNTING AND PROBABILITY

9.1 Introduction

Definition

- A **sample space** is the set of all possible outcomes of a random process or experiment.
- An **event** is a subset of a sample space.

Equally Likely Probability Formula

If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability** of E, denoted $P(E)$, is

$$P(E) = \frac{\text{the number of outcomes in } E}{\text{the total number of outcomes in } S} = \frac{N(E)}{N(S)},$$

where, for any set X, $N(X)$ denotes *the number of elements of* X, i.e., in another often used notation, $N(X) = |X|$.

Example 9.1.1 Probabilities for a Deck of Cards

An ordinary deck of cards contains 52 cards divided into four *suits*. The *red suits* are diamonds (♦) and hearts (♥) and the *black suits* are clubs (♣) and spades (♠). Each suit contains 13 cards of the following *denominations:* 2, 3, 4, 5, 6, 7, 8, 9, 10, J (jack), Q (queen), K (king), and *A* (ace). The cards J, Q, and K are called *face cards.*

Solution

a. The outcomes in the sample space S are the 52 cards in the deck.

b. Let E be the event that a black face card is chosen. The outcomes in E are the jack, queen, and king of clubs and the jack, queen, and king of spades. Symbolically,

$$E = \{\text{J}\clubsuit, \text{Q}\clubsuit, \text{K}\clubsuit, \text{J}\spadesuit, \text{Q}\spadesuit, \text{K}\spadesuit\}.$$

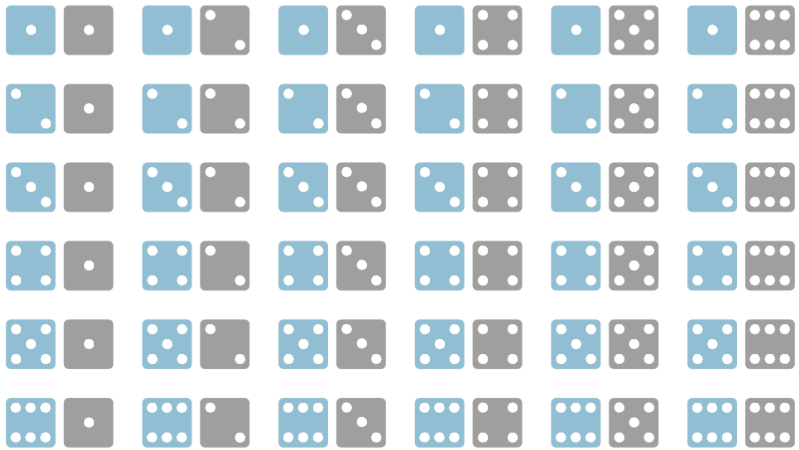
c. By part (b), $N(E) = 6$, and according to the description of the situation, all 52 outcomes in the sample space are equally likely. Therefore, by the equally likely probability formula, the probability that the chosen card is a black face card is

$$P(E) = \frac{N(E)}{N(S)} = \frac{6}{52} \cong 11.5\%.$$

■

Example 9.1.2 Rolling a Pair of Dice

A die is one of a pair of dice. It is a cube with six sides, each containing from one to six dots, called *pips*. Suppose a blue die and a gray die are rolled together, and the numbers of dots that occur face up on each are recorded. The possible outcomes can be listed as follows, where in each case the die on the left is blue and the one on the right is gray.



A more compact notation identifies, say,  with the notation 24,  with 53, and so forth.

a. Use the compact notation to write the sample space S of possible outcomes.

b. Use set notation to write the event E that the numbers showing face up have a sum of 6 and find the probability of this event.

Solution

a. $S = \{11, 12, 13, 14, 15, 16, 21, 22, 23, 24, 25, 26, 31, 32, 33, 34, 35, 36, 41, 42, 43, 44, 45, 46, 51, 52, 53, 54, 55, 56, 61, 62, 63, 64, 65, 66\}$.

b. $E = \{15, 24, 33, 42, 51\}$.

The probability that the sum of the numbers is 6 $= P(E) = \dfrac{N(E)}{N(S)} = \dfrac{5}{36}$. ■

9.1 Exercises (a)

Exercise 9.1.10

In rolling a pair of dice, write the event is that the sum of the numbers showing face–up is at least 9 and compute the probability.

$E = \{36, 45, \ldots\}, N(E) = ?, N(S) = ?, P(E) = ?.$

Exercise 9.1.14 (b) and (c)

Three people have been exposed to a certain illness. Once exposed, a person has a 50–50 chance of actually becoming ill. (b) What is the probability that at least two of the people become ill? (c) What is the probability that none of the three people becomes ill?

The sample space is composed of the following cases: none is ill, one is ill, two, are ill, all are ill. Denoting people by A, B, C, what is $S = \{?\}, N(S) = ?$ In (b) and (c) what are the events $E_b = \{?\}, E_c = \{?\}$ as subsets of S? $N(E_b) = ?, N(E_c) = ?, P(E_b) = ?, P(E_c) = ?$

9.1 Exercises (a)

Exercise 9.1.17

Two faces of a six–sided die are painted red, two are painted blue, and two are painted yellow. The die is rolled three times, and the colors that appear face up on the first, second, and third rolls are recorded. (a) Find the probability of the event that exactly one of the colors that appears face up is red. (b) Find the probability of the event that at least one of the colors that appears face up is red.

Find the sample space $S = \{RRR, \ldots, YYY\}, N(S) =?$ In (a) $E = \{RBB, \ldots\}, N(E) =?, P(E) =?$ In (b), first find the event that none of the faces is red and subsequently the event that at least one is red can be computed by subtraction.

9.1 Counting Elements of a List

Theorem

If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n, inclusive.

Exercise 9.1.22

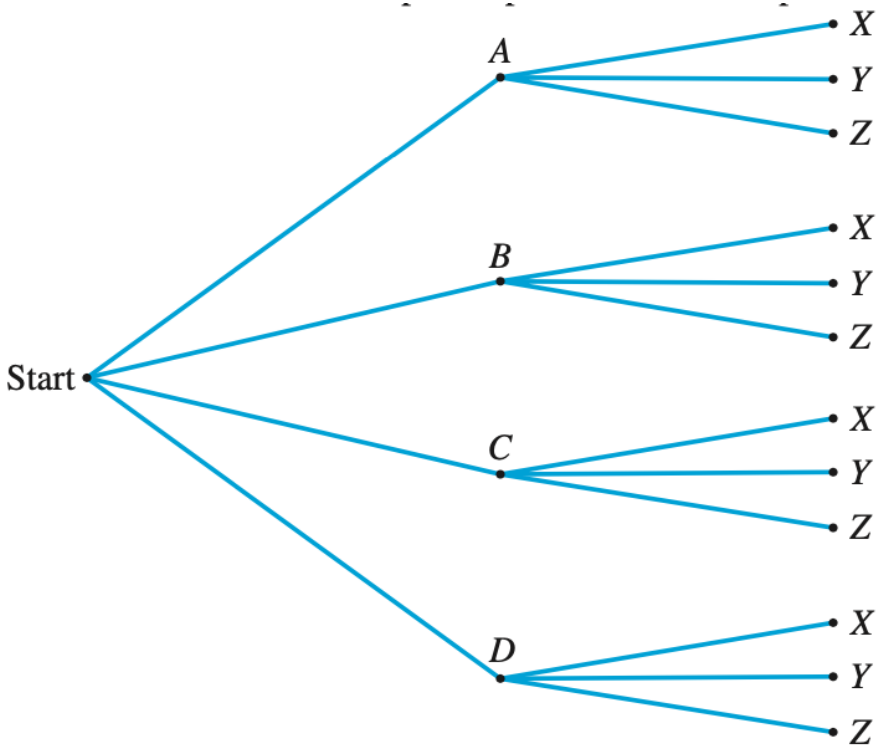
(a) How many positive three–digit integers are multipliers of 6? (b) What is the probability that a randomly chosen positive three–digit integer is a multiple of 6? (c) What is the probability that a randomly chosen positive three–digit integer is a multiple of 7?

Apparently three–digit numbers are between 100 and 999, inclusive. In (a), find the smaller integer m such that $6 \cdot m \geq 100$ and the largest integer n such that $6 \cdot n \leq 999$. The rest is obvious, for (b) too. In (c), do the same for multiples of 7.

9.2 Possibility Trees

An Example

Suppose that we have two sets $\mathscr{A} = \{A, B, C, D\}$ and $\mathscr{X} = \{X, Y, Z\}$. We want to count how many ways we can pair an element of $\mathscr{A}$ with an element of $\mathscr{X}$? To do it, just count the branches of the followig **possibility tree** (in order to find 12 ways):

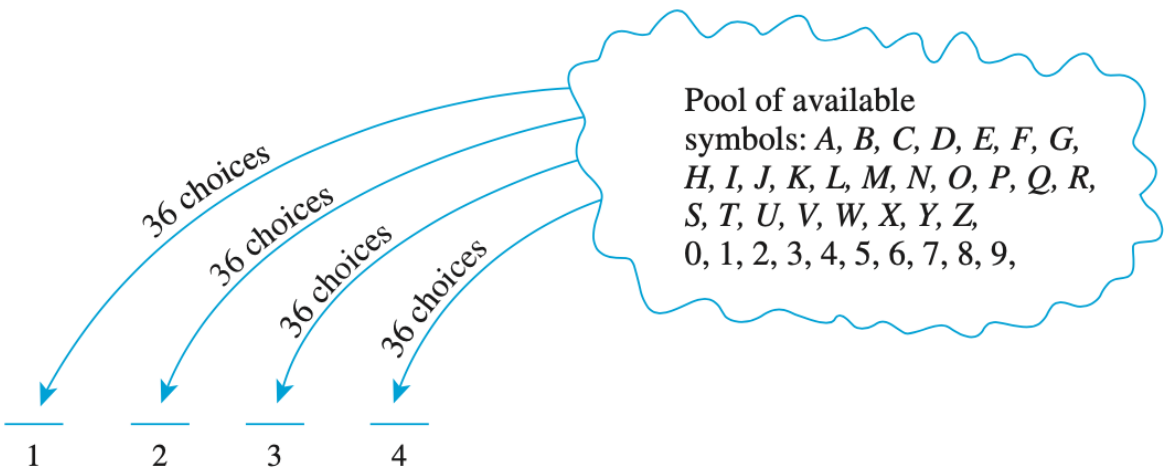


9.2 Possibility Trees and the Multiplication Rule

Theorem (**The Multiplication Rule**)

If an operation consists of k steps and the first step can be performed in n_1 ways, the second step can be performed in n_2 ways (regardless of how the first step was performed), ..., the kth step can be performed in n_k ways (regardless of how the preceding steps were performed), then the entire operation can be performed in $n_1 \cdot n_2 \cdots n_k$ ways.

There are 36^4 possible 4–digit PINs (letters and digits):



9.2 Multiplication Rule Examples

Example 1

Three urns contain colored balls: the first 5 red balls, the second 6 green balls, and the third 4 blue balls. Choosing randomly one ball from each urn, how many colored triplets of balls can be chosen?

Example 2

In rolling a pair of dice, each one having a different color, how many outcomes are possible?

9.2 Possibility Trees Exercises (a)

Exercise 9.2.7

One urn contains one blue ball (labeled B_1) and three red balls (labeled R_1, R_2, and R_3). A second urn contains two red balls (R_4 and R_5) and two blue balls (B_2 and B_3). An experiment is performed in which one of the two urns is chosen at random and then two balls are randomly chosen from it, one after the other without replacement. (a) Construct the possibility tree showing all possible outcomes of this experiment. (b) What is the total number of outcomes of this experiment? (c) What is the probability that two red balls are chosen? For the possibility tree, first consider three steps: (1) choose an urn, (2) choose ball 1 and (3) choose ball 2. Apparently, step (1) involves the set of urns, let us denote it as $\{U_1, U_2\}$. Step (2) involves the set of all **single** balls, blue or red, which are $B_1, \ldots, R_1, \ldots$. However, these balls are distributed differently in the two urns: which (single) balls are in U_1 and which in U_2? Finally, step (3) involves different sets of 3 balls which are **complimentary** to the sets in step (2).

9.2 Possibility Trees Exercises (b)

Exercise 9.2.10

Suppose there are three routes from North Point to Boulder Creek, two routes from Boulder Creek to Beaver Dam, two routes from Beaver Dam to Star Lake, and four routes directly from Boulder Creek to Star Lake. (Draw a sketch.) (a) How many routes from North Point to Star Lake pass through Beaver Dam? (b) How many routes from North Point to Star Lake bypass Beaver Dam?

Set locations as 4 points horizontally (North Point, Boulder Creek, Beaver Dam, Start Lake) and draw routes among two locations as arcs joining the corresponding points. When moving between two locations, think of routes as choices and, thus, count arcs joining them. Then use the multiplication rule.

9.2 Possibility Trees Exercises (c)

Exercise 9.2.13

A coin is tossed four time. Each time the outcome is either H(ead) or T(ails). (a) How many distinct outcomes are possible? (b) What is the probability that exactly two heads occur? (c) What is the probability that exactly one head occurs? Do the computations by writing the sample space and each event. Use the multiplication to count the elements of the sample space.

Exercise 9.2.14

Suppose that in a certain state, all automobile license plates have four letters followed by three digits. (a) How many different license plates are possible? (b) How many license plates could begin with A and end in 0? (c) How many license plates could begin with TGIF? (d) How many license plates are possible in which all the letters and digits are distinct? (e) How many license plates could begin with A B and have all letters and digits distinct?

9.2 Strings

Definition

Given a finite set X, a **string over** X is a finite sequence of elements of X (where repetition of elements of X is allowed). The **length of a string** is the number of elements of X that it contains. Usually, a string is written without parentheses or commas separating its elements. A string over $X = \{0, 1\}$ is called **bit string**.

9.2 Permutations

Definition

A **permutation** of n distinct objects is an ordering of these objects (in a row).

Theorem

There are $n!$ permutations of n objects.

Definition

An r**–permutation** of n distinct objects is an ordering of r objects taken from these objects. The number of r–permutations of n objects is denoted $P(n, r)$.

Theorem

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$$
$$= \frac{n!}{(n-r)!}, \qquad r \leq n.$$

9.2 Permutations: Exercises

Exercise 9.2.33

(a) How many ways can three of the letters of the word ALGORITHM be selected and written in a row?

(b) How many ways can six of the letters of the word ALGORITHM be selected and written in a row?

(c) How many ways can six of the letters of the word ALGORITHM be selected and written in a row if the first letter must be A?

(d) How many ways can six of the letters of the word ALGORITHM be selected and written in a row if the first two letters must be OR?

$N(\text{ALGORITHM}) = 9$ and all letters are distinct. (a) $P(9,3) = ?$. (b) $P(9,6) = ?$. (c) $P(9-1, 6-1) = P(8,5) = ?$. (d) $P(9-2, 6-2) = P(7,4) = ?$. **Explain!**

9.3 Three Counting Principles

Theorem (**The Addition Principle**)

If two finite sets A and B are disjoint, then $N(A \cup B) = N(A) + N(B)$. In general, if k finite sets $A_1, A_2, \ldots, A_k$ are mutually disjoint, then $N(A_1 \cup A_2 \cup \cdots \cup A_k) = N(A_1) + N(A_2) + \ldots + N(A_k)$.

Theorem (**The Difference Principle**)

If A is a finite set and $B \subseteq A$, then $N(A - B) = N(A) - N(B)$.

Theorem (**The Inclusion–Exclusion Principle**)

If A and B are two finite sets, then $N(A \cup B) = N(A) + N(B) - N(A \cap B)$.
If A, B and C are three finite sets, then $N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$.

9.3 Three Counting Principles Examples

Example 1

A person's age is a two-digits numbers divisible by 3 such that the first digit is odd and the second digit is both less than the first digit and less than 5. What are all possible ages of that person?

Example 2

How many positive integers less than 1000 can have two different digits? (It is 973! Why?)

Example 3

How many positive integers less or equal than 300 can be either even or divisible by 3? (It is 200! Why?)

9.3 Counting: Exercises (a)

Exercise 9.3.8

At a certain company, passwords must be from 3–5 symbols long and composed of the 26 letters of the alphabet, the ten digits 0–9, and the 14 symbols !,@,#,$, %, ^, &, ∗, (,), −, +, {, and }. (a) How many passwords are possible if repetition of symbols is allowed? (b) How many passwords contain no repeated symbols? (c) How many passwords have at least one repeated symbol? (d) What is the probability that a password chosen at random has at least one repeated symbol?

How many symbols are used totally? (a) By the addition principle according to the number of symbols (3-5) and in each case using the multiplication principle. (b) Similarly, but numbers shoud be reduced each time! (c) Use the difference principle. (d) By the formula of probability.

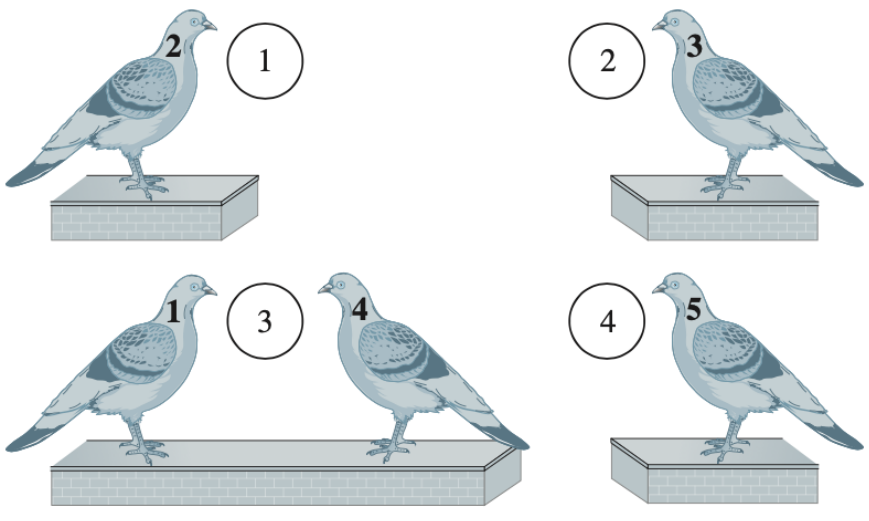
9.3 Counting: Exercises (b)

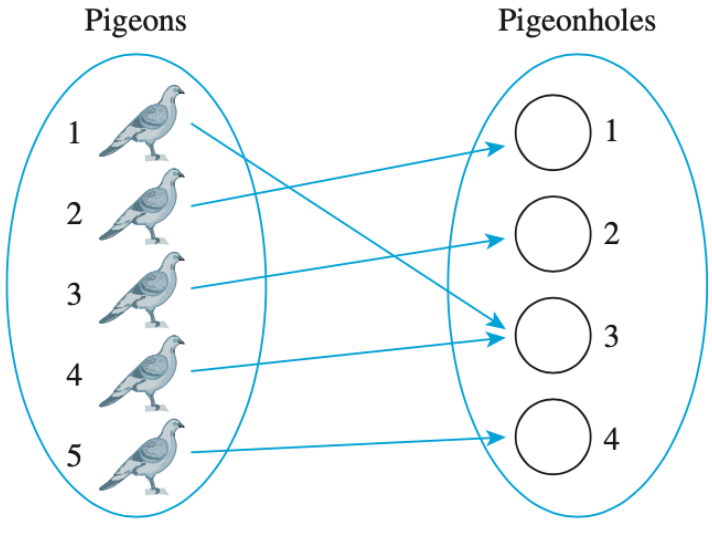
Exercise 9.3.11

(a) How many ways can the letters of the word THEORY be arranged in a row? (b) How many ways can the letters of the word THEORY be arranged in a row if T and H must remain next to each other as either TH or HT?

How many are the letters of this word? Are they distinct? (a) Use permutations! (b) ammounts to the orderings of either TH–E–O–R–Y or HT–E–O–R–Y. How many letters in each case and, thus, how many orderings? As these are two different words, use the addition principle for the total number of orderings.

9.4 The Pigeonhole Principle I





9.4 The Ordinary Pigeonhole Principle II

Theorem (The Ordinary Pigeonhole Principle)

Classical Form: *If n pigeons fly into m pigeonholes, where $m < n$, then there exists a pigeonhole that contains at least two pigeons.*

Function Form: *Given two finite sets X, Y with $|X| = n$ and $|Y| = m$, where $m < n$, and a function $f\colon X \to Y$, then $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X, x_1 \neq x_2$.*

Proof by Contradiction:

Suppose that for any $y \in Y$, there exists at most one $x \in X$ such that $f(x) = y$. This means that either y is not on the range of f or that there exists a unique $x \in X$ such that $f(x) = y$. Notice that Y is trivially partitioned as $Y = Y_1 \cup Y_2$, where $Y_1 = \text{ range}(f)$ and $Y_2 = \text{ range}(f)^c$. Thus, under the previous assumption, $f\colon X \to Y_1$ is one–to–one, which implies that $|Y_1| = |X| = n$ and, consequently, $m = |Y| = |Y_1| + |Y_2| = |X| + |Y_2| \geq |X| = n$. However, deriving $m \geq n$ contradicts the assumption that $m < n$.

9.4 The Generalized Pigeonhole Principle II

Theorem (The Generalized Pigeonhole Principle)

Let two finite sets X, Y with $|X| = n$ and $|Y| = m$, where $m < n$, let a function $f\colon X \to Y$, and let the integer $k = \lceil \frac{n}{m} \rceil$. Then there exist at least k distinct elements of $X, x_1, x_2, \ldots, x_k$ (instead of 2 in the ordinary Pigeonhole Principle), such that $f(x_1) = f(x_2) = \cdots = f(x_k)$.

Proof by Contradiction:

Suppose that for any $y \in Y$, there exist at most $k-1$ distinct $x \in X$ such that $f(x) = y$. Without any loss of generality we may assume that f is onto (**why?**) and let us represent $Y = \{y_1, y_2, \ldots, y_m\}$. This means that there are at most $k-1$ distinct $x \in X$ with $f(x) = y_1$; there are at most $k-1$ distinct $x \in X$ with $f(x) = y_2$; ...; there are at most $k-1$ distinct $x \in X$ with $f(x) = y_m$. Hence, totally, set X must contain at most $m(k-1)$ elements, which means $n < m(k-1)$. However, since $m < n$, $k = \lceil \frac{n}{m} \rceil < \frac{n}{m} + 1$ or $k - 1 < \frac{n}{m}$. Thus, $n < m(k-1) < m\frac{n}{m} = n$, which is a contradiction.

9.4 The Pigeonhole Principle Examples (a)

Example 1

A drawer contains 10 black and 10 white socks. You reach in and pull two out without looking. What is the least number of socks you must pull out to be guaranteed to get a matched pair?

Consider the set X to be the set of socks pulled out and the set Y to be the set of the two colors of the socks. We know that $|Y| = 2$ but we are not sure what $|X| = n$ should be in order to get a matched pair. The function $f\colon X \to Y$ is the categorization of the color of socks. In other words, a first sock is pulled out and it is placed in the "pigeonhole" of its color. Such placement is repeated with all subsequent draws. Then the question is what is the size of X so that it would be certain that at least two socks might be placed in the same "pigeonhole" and, thus, they might have the same color? According to the Pigeonhole Principle, $n > m = 2$. What is the smaller value of n that implies pair matching?

9.4 The Pigeonhole Principle Examples (b)

Example 2

Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. How many integers should be selected from A so that at least one pair of the integers might have sum of 9?

Let X_n be a set of n distinct numbers selected from A. As far as $n \geq 2$, the elements of X_n may create certain pairs of numbers. Considering the set Y to be the set of all possible pairs of numbers in A with sum 9, i.e., $Y = \{\{1, 8\}, \{2, 7\}, \{3, 6\}, \{4, 5\}\}$, the question is what the set X_n should be so that at least one pair of distinct elements of X_n would be an element in Y? Notice that each element of A occurs in exactly one element of Y. Observe that for $X_3 = \{1, 2, 3\}$ all the elements of this set correspond to distinct elements of Y and, thus, X_3 does not include pairs with sum 9. Similarly, the elements of $X_4 = \{2, 4, 6, 8\}$ or of $X_4 = \{1, 3, 5, 7\}$ are associated to distinct elements of Y. Notice that for all the previous sets $n = |X_n| \leq 4$. However, when $n = |X_n| \geq 5$, in any such X_n the Pigeonhole Principle implies that there is at least one pairs of elements associated to the same element in Y and, thus, in any X_n, for $n \geq 5$, sums of pairs equal to 9 are always formed.

9.4 The Pigeonhole Principle Examples (c)

Example 3

- In a group of 6 people, must there be at least two who were born in the same month?
- In a group of 13 people, must there be at least two who were born in the same month?
- In a group of 100 people, what would be the minimum number of them who were born in the same month?

Consider X to be the group of people and Y to be the set of 12 months. The function $f\colon X \to Y$ associates the birthday month to a person. If $|X| = 6$, every person can have birthday on a different month, because $12 = |Y| > 6$. Applying the Pigeonhole Principle, when $|X| = 13 > 12 = |Y|$, necessarily two persons were born in the same month. Finally, according to the Generalized Pigeonhole Principle, when $|X| = 100 > 12 = |Y|$, since $\frac{100}{12} = 8.33$, there must be 9 persons who were born in the same month.

9.4 The Pigeonhole Principle Exercises (a)

Exercise 9.4.19

How many integers from 100 through 999 must you pick in order to be sure that at least two of them have a digit in common? (For example, 256 and 530 have the common digit 5.)

All the numbers from 100 to 999 contain at least one of the nine digits 1, 2, 3, 4, 5, 6, 7, 8, or 9. First, let us consider the case of numbers with distinct digits. For instance, the following *nine* numbers have no common digits: 111, 222, 333, 444, 555, 666, 777, 888, and 999. This is the worst case scenario if we were picking nine numbers. However, if we are picking *ten* numbers, the tenth number is going to have at least a digit common with the previously selected numbers.

9.4 The Pigeonhole Principle Exercises (b)

Exercise 9.4.31

A group of 15 executives are to share 5 assistants. Each executive is assigned exactly 1 assistant, and no assistant is assigned to more than 4 executives. Show that at least 3 assistants are assigned to 3 or more executives.

Let k be the number of assistants assigned to at least three executives. (The target is to show that $k \geq 3$.) These assistants are assigned to at most $4k$ executives (since no assistant is assigned to more than 4 executives). The remaining assistants are $5-k$ and each of them is assigned to 2 executives. Thus, all of the remaining assistants are assigned to at most $2(5-k) = 10-2k$ executives. Therefore, all the assistants are assigned to at most $4k + (10-2k) = 10+2k$ executives. However, since the number of all executives is 15, we should have $15 \leq 10+2k$, i.e., $k \geq 5/2$, and, since k is an integer, we get $k \geq 3$.

9.4 The Pigeonhole Principle Exercises (c)

Exercise 9.4.32

Let A be a set of six (distinct) positive integers each of which is less than 13. Show that there must be two distinct subsets of A whose elements when added up give the same sum. (For example, $A = \{1, 3, 4, 5, 10, 12\}$ and the two sets are $S_1 = \{1, 4, 10\}$ and $S_2 = \{5, 10\}$, both having sum 15.)

Let $\mathscr{X}$ be the set of all nonempty subsets of A. Clearly, $\mathscr{X} \subset \mathscr{P}(A)$. Furthermore, consider the function $F : \mathscr{X} \to \mathbb{Z}^+$ be defined as $F(X) =$ the sum of the elements of X, for any $X \in \mathscr{X}$. We know that the set of all subsets of A has $2^{|A|} = 2^6 = 64$ elements, i.e., $|\mathscr{X}| = 64 - 1 = 63$. Since each element of A is less than 13, the maximum possible sum of elements of any $X \in \mathscr{X}$ is 57 $(= 12 + 11 + 10 + 9 + 8 + 7)$. Since $63 > 57$, the Pigeonhole Principle guarantees that F is not one–to–one. Therefore, there exist distinct sets $A_1, A_2 \in X$ such that $F(A_1) = F(A_2)$.

9.5 Combinations

Definition

A **combination** of k elements from a set of size n is a subset of size k.

Theorem (Counting Combinations = Counting Subsets of Given Size)

The number of combinations of size k from a set of size n, where $k, n \in \mathbb{Z}, 0 \leq k \leq n$, is:

$$\binom{n}{k} = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}.$$

9.5 Combinations: Examples (a)

Example 1

1. What is the number of distinct teams of 5 people chosen from a group of 12?
2. If the group includes 7 women and 5 men, how many 5–person teams can be chosen with 3 men and 2 women?
3. How many 5–person teams contain at least 1 man?
4. How many 5–person teams contain at most 1 man?

1. By definition: $\binom{12}{5} =$ do the algebra $= 792$.
2. By the multiplication rule: $\binom{5}{3} \times \binom{7}{2} =$ do the algebra $= 210$.
3. By the addition rule:
   $\binom{5}{1} \times \binom{7}{4} + \binom{5}{2} \times \binom{7}{3} + \binom{5}{3} \times \binom{7}{2} + \binom{5}{4} \times \binom{7}{1} + \binom{5}{5} \times \binom{7}{0}$
   $=$ do the algebra $= 175 + 350 + 210 + 35 + 1 = 771$. Or **better** by the subtraction rule: this is the number of all 5–person teams minus the number of 5–person teams that contain no men
   $= \binom{12}{5} - \binom{7}{5} =$ do the algebra $= 729 - 21 = 771$.
4. By the addition rule: this is the number of all 5–person teams without any men plus the number of 5–person teams with one man
   $= \binom{5}{0} \times \binom{7}{5} + \binom{5}{1} \times \binom{7}{4} =$ do the algebra $= 21 + 175 = 196$.

9.5 Combinations: Exercises (a)

Exercise 9.5.7

A computer programming team has 13 members. (a) How many ways can a group of seven be chosen to work on a project? (b) Suppose seven members are women and six are men. (b1) How many groups of seven can be chosen that contain four women and three men? (b2) How many groups of seven can be chosen that contain at least one man? (b3) How many groups of seven can be chosen that contain at most three women? (c) Suppose two team members refuse to work together on projects. How many groups of seven can be chosen to work on a project? (d) Suppose two team members insist on either working together or not at all on projects. How many groups of seven can be chosen to work on a project?

(c) Let A, B be these persons. Then this is the number of groups with A and 6 others plus the number of groups with B and 6 others plus the number of groups with neither A nor B. (d) Then this is the number of groups with both A and B plus the number of groups with neither A nor B.

9.5 Combinations: Exercises (b)

Exercise 9.5.10

Two new drugs are to be tested using a group of 60 laboratory mice, each tagged with a number for identification purposes. Drug A is to be given to 22 mice, drug B is to be given to another 22 mice, and the remaining 16 mice are to be used as controls. How many ways can the assignment of treatments to mice be made? (A single assignment involves specifying the treatment for each mouse – whether drug A, drug B, or no drug.)

By the multiplication rule, this is the number of choosing 22 mice out of 60 to receive treatment A times the number of choosing 22 mice out of the remaining 38 to receive treatment B.

9.5 Combinations: Examples (b)

Example 2 (**Poker Hands**)

1. How many five–card poker hands cards contain two pairs?
2. What is the probability of being dealt a hand that contains two pairs?

1. Using the multiplication rule, this is the number of choosing 2 pairs from 13 denominations times the number of choosing the two cards of the first pair from the smaller denomination times the number of choosing the two cards of the first pair from the larger denomination (one pair in each suit) times the the number of choosing one card from those remaining
$= \binom{13}{2} \times \binom{4}{2} \times \binom{4}{2} \times \binom{44}{1} =$ do the algebra $= 123,552.$
2. The total number of five–card hands from an ordinary deck of cards is $\binom{52}{5} = 2,598,960.$ Thus, the the probability of obtaining a hand with two pairs is $\frac{123,552}{2,598,960} \approx 4.75\%.$

9.5 Combinations: Exercises (c)

Exercise 9.5.11

Find the probability that a randomly chosen five–card poker hand has the holdings:

(b) straight flush,

(d) full house,

(e) flush,

(g) three of a kind.

You may use the Internet, but you should justify your solutions.

9.5 Combinations: Examples (c)

Example 3 (**Strings**)

How many eight–bit strings have exactly three 1's?

This is exactly the number of combinations of size 3 from a set of size 8, i.e., it is $= \binom{8}{3} = \ldots = 56$.

Exercise 9.5.13

Tossing a coin ten times, in how many of the possible outcomes the following events are expected to occur?

(b) exactly five heads,

(c) at least eight heads,

(e) at most one head.

These are the answers but you need to justify them (and complete the calculations): (b) $\binom{10}{5}$, (c) $\binom{10}{8} + \binom{10}{9} + \binom{10}{10}$, (e) $\binom{10}{0} + \binom{10}{1}$.

9.5 Combinations: Exercises (d)

Exercise 9.5.22

How many symbols can be represented in the Braille code?

Solution 1: By the difference rule, this is the total number of subsets of a set of 6 elements minus one (for the empty set): $2^6 - 1 = 63$.

Solution 2: By the addition rule, this is the sum of the numbers of subsets of size n chosen among the elements of a set of size 6, for $n = 1, 2, \ldots, 6$: $\sum_{n=1}^{6} \binom{6}{n} = 6 + 15 + 20 + 15 + 6 + 1 = 63$.

9.5 Generalized Permutations

Theorem

Suppose that a set S contains n elements of which n_1 identical elements are of type 1, n_2 identical elements are of type 2, ..., n_k identical elements are of type k, where $n_1 + n_2 + \ldots + n_k = n$. Then the number of orderings of S is

$$\frac{n!}{n_1! n_2! \cdots n_k!}.$$

9.5 Table of Permutations and Combutations

Permutations	n distinct objects	$n!$
	n repeated objects in k types	$\frac{n!}{n_1! \cdot n_2! \cdots n_k!}$
Strings	k out of n symbols	$\frac{n!}{(n-k)!}$
	n symbols in string of length k	n^k
Combinations	subsets of size k in a set of size n	$\binom{n}{k}$
	subsets of size k with repeated elements in a set of size n	$\binom{n+k-1}{n-1}$

9.6 Pascal's Formula

Theorem

Let n and r be positive integers and suppose $r \leq n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

9.6 Pascal's Formula: Exercise

Exercise 9.6.12

Use Pascal's formula repeatedly to show the following formula:

$$\binom{n+3}{r} = \binom{n}{r-3} + 3 \cdot \binom{n}{r-2} + 3 \cdot \binom{n}{r-1} + \binom{n}{r}.$$

$\binom{n+3}{r} = \binom{(n+2)+1}{r} = \binom{n+2}{r-1} + \binom{n+2}{r} = \binom{n+1}{r-2} + \binom{n+1}{r-1} + \binom{n+1}{r-1} + \binom{n+1}{r} = \binom{n+1}{r-2} + 2 \cdot \binom{n+1}{r-1} + \binom{n+1}{r} = \ldots$ etc.

9.6 The Binomial Theorem

Theorem

For any real numbers a and b any nonnegative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k =$$

$$= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

9.6 Pascal's Triangle

Definition

Pascal's triangle is a triangular array of the binomial coefficients, the borders of which consist of 1's and any interior value is the sum of the two numbers above it.

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}
$$

9.6 The Binomial Theorem: Exercises

Exercise 9.6.30 and 32

Find the coefficient of the term x^7 in the expansion of $(2x+3)^{10}$ and the coefficient of the term $u^{16}v^4$ in the expansion of $(u^2-v^2)^{10}$.

For the second, since $u^{16}v^4 = (u^2)^8(-v^2)^2$, the term is $\binom{10}{2}(u^2)^8(-v^2)^2$ and the coefficient is $\binom{10}{2} = \frac{10!}{2!\cdot 8!}\cdot(-1)^2 = 45$. Similarly for the first.

Exercise 9.6.37

For all integers $n \geq 0$,

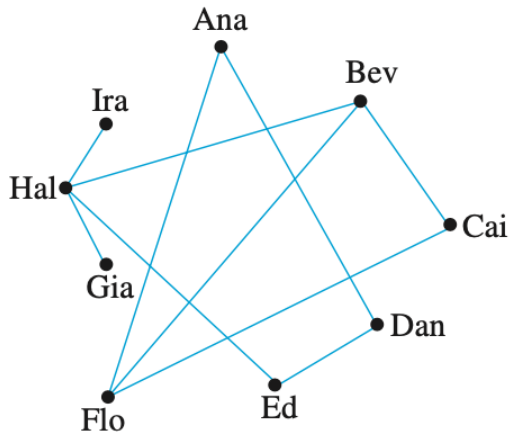
$$3^n = \binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \cdots + 2^n\binom{n}{n}.$$

Apply the Binomial Theorem with $a = 1$ and $b = 2$.

10. INTRODUCTION TO GRAPHS

10.1 Graphs: Definitions and Basic Properties, 1

Name	Past Partners
Ana	Dan, Flo
Bev	Cai, Flo, Hal
Cai	Bev, Flo
Dan	Ana, Ed
Ed	Dan, Hal
Flo	Cai, Bev, Ana
Gia	Hal
Hal	Gia, Ed, Bev, Ira
Ira	Hal



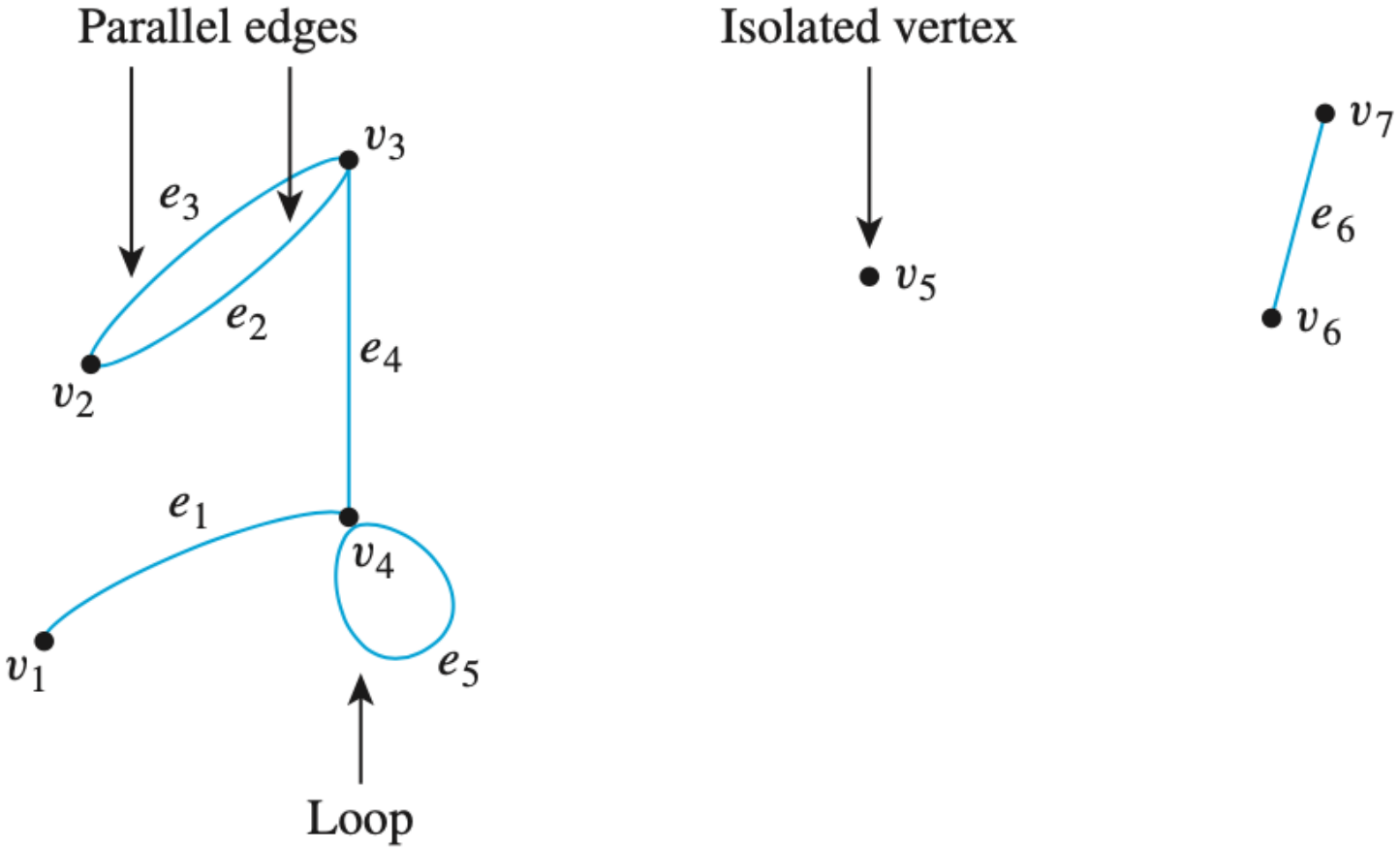
• Definition

A **graph** G consists of two finite sets: a nonempty set $V(G)$ of **vertices** and a set $E(G)$ of **edges,** where each edge is associated with a set consisting of either one or two vertices called its **endpoints.** The correspondence from edges to endpoints is called the **edge-endpoint function.**

An edge with just one endpoint is called a **loop,** and two or more distinct edges with the same set of endpoints are said to be **parallel.** An edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent;** and a vertex that is an endpoint of a loop is said to be **adjacent to itself.**

An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent.** A vertex on which no edges are incident is called **isolated.**

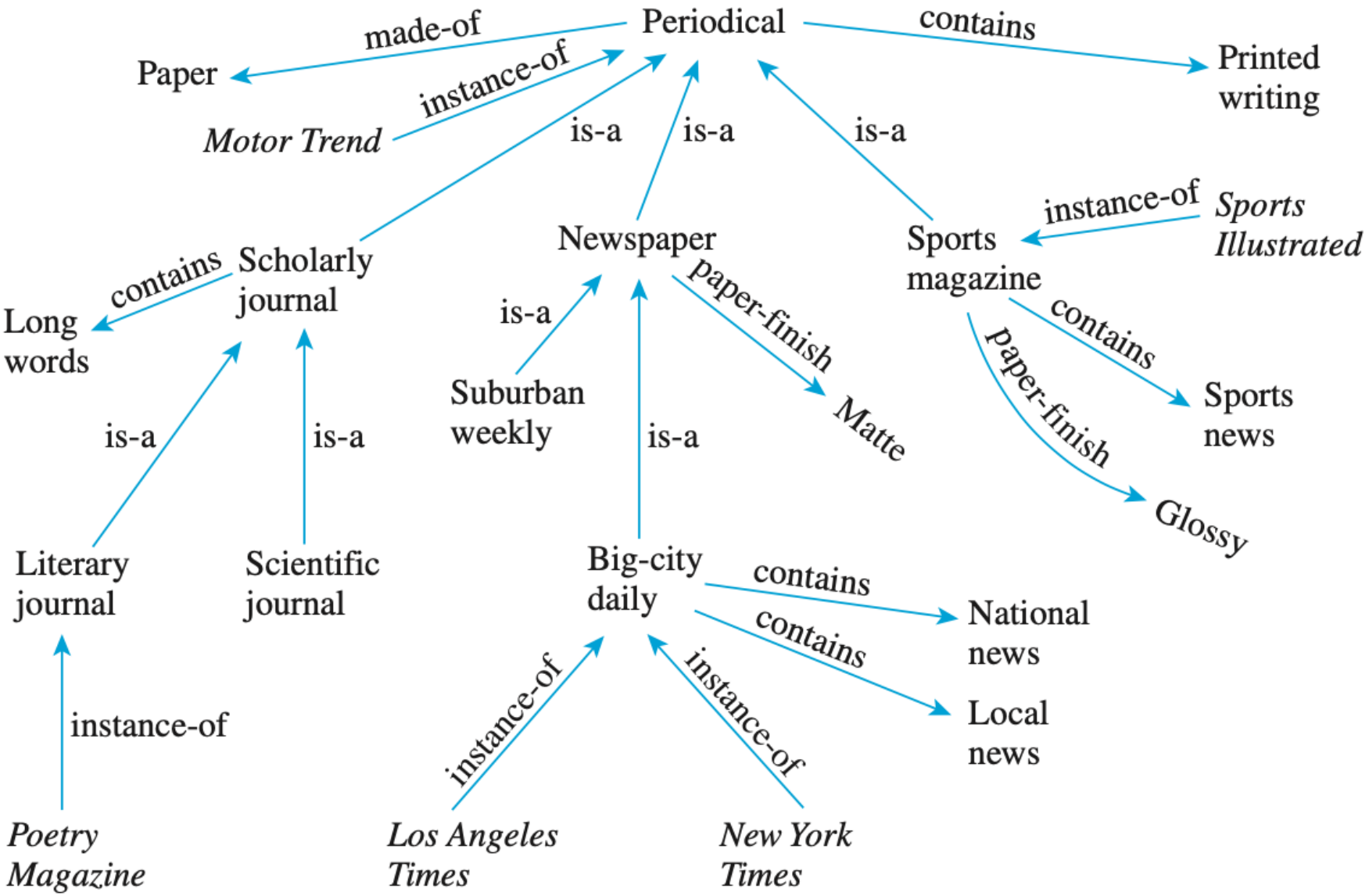
10.1 Graphs: Definitions and Basic Properties, 2



• Definition

A **directed graph,** or **digraph,** consists of two finite sets: a nonempty set $V(G)$ of vertices and a set $D(G)$ of directed edges, where each is associated with an ordered pair of vertices called its **endpoints.** If edge e is associated with the pair (v, w) of vertices, then e is said to be the (**directed**) **edge** from v to w.

10.1 Graphs: Definitions and Basic Properties, 3



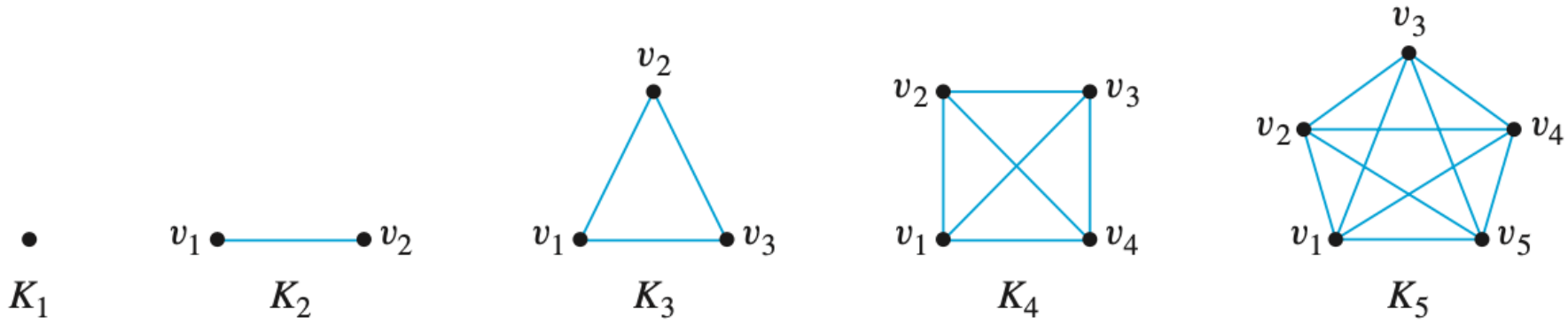
10.1 Graphs: Definitions and Basic Properties, 4

• Definition and Notation

A **simple graph** is a graph that does not have any loops or parallel edges. In a simple graph, an edge with endpoints v and w is denoted $\{v, w\}$.

• Definition

Let n be a positive integer. A **complete graph on n vertices,** denoted $\boldsymbol{K_n}$, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.

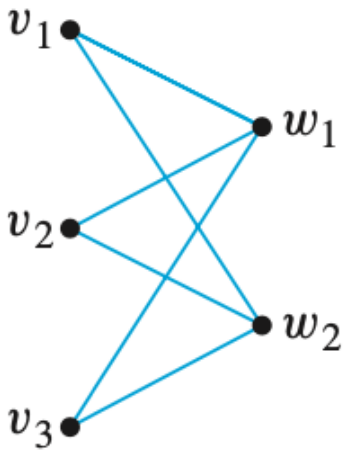


10.1 Graphs: Definitions and Basic Properties, 5

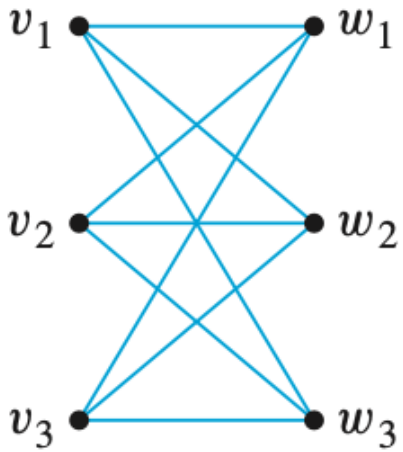
• Definition

Let m and n be positive integers. A **complete bipartite graph on (m, n) vertices,** denoted $\boldsymbol{K_{m,n}}$, is a simple graph with distinct vertices $v_1, v_2, \ldots, v_m$ and $w_1, w_2, \ldots, w_n$ that satisfies the following properties: For all $i, k = 1, 2, \ldots, m$ and for all $j, l = 1, 2, \ldots, n$,

1. There is an edge from each vertex v_i to each vertex w_j.
2. There is no edge from any vertex v_i to any other vertex v_k.
3. There is no edge from any vertex w_j to any other vertex w_l.



$K_{3,2}$

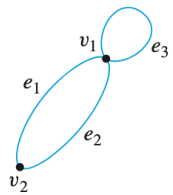


$K_{3,3}$

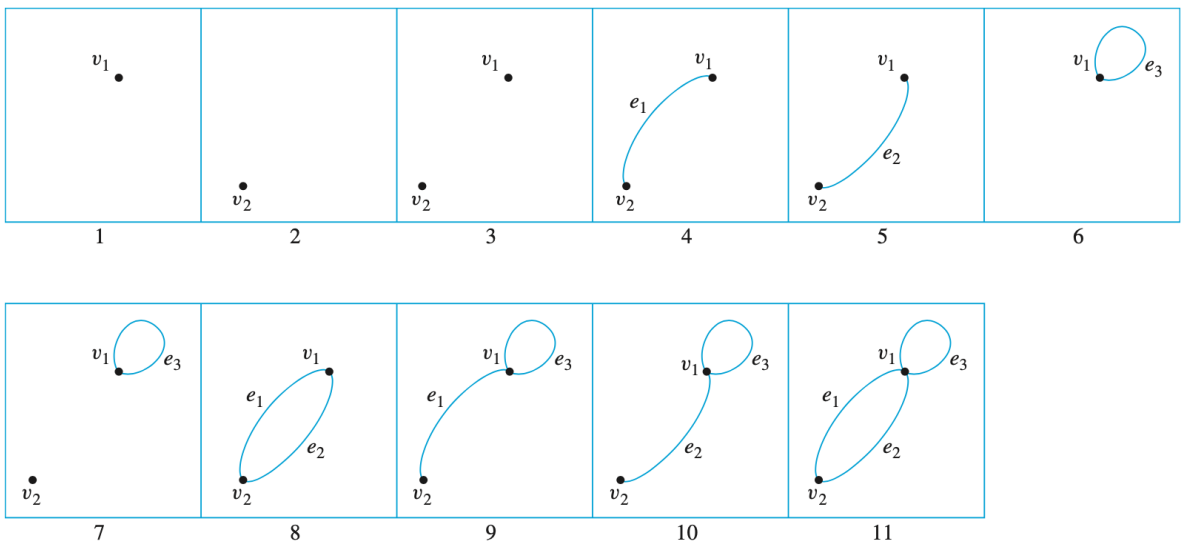
10.1 Graphs: Definitions and Basic Properties, 6

• Definition

A graph H is said to be a **subgraph** of a graph G if, and only if, every vertex in H is also a vertex in G, every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G.



There are 11 subgraphs of G, which can be grouped according to those that do not have any edges, those that have one edge, those that have two edges, and those that have three edges. The 11 subgraphs are shown in Figure 10.1.4.



10.1 Graphs: Definitions and Basic Properties, 7

• Definition

Let G be a graph and v a vertex of G. The **degree of v,** denoted **deg(v),** equals the number of edges that are incident on v, with an edge that is a loop counted twice. The **total degree of G** is the sum of the degrees of all the vertices of G.

Theorem 10.1.1 The Handshake Theorem

If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G. Specifically, if the vertices of G are $v_1, v_2, \ldots, v_n$, where n is a nonnegative integer, then

$$\begin{aligned}\text{the total degree of } G &= \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n)\\ &= 2 \cdot (\text{the number of edges of } G).\end{aligned}$$

Corollary 10.1.2

The total degree of a graph is even.

Proposition 10.1.3

In any graph there are an even number of vertices of odd degree.