# Contemporary Mathematics

March 3, 2024

# Contents

$\mathbf{Set}$	Theory	1
1.1	Set Notation	1
1.2	Subsets and Venn Diagrams	6
1.3		15
1.4		23
Log	;ic	31
2.1	Logic Statements and their Negations	31
2.2		38
2.3		45
2.4		53
Gra	aph Theory	61
3.1	Introduction to Graph Theory	61
3.2		77
3.3		85
3.4		95
Vot	ing Theory	03
4.1		03
4.2		12
4.3		$17^{-}$
Niii	mber Theory	29
TIU		
5.1	Prime Numbers	29
5.1		_
	Modular Arithmetic	$\frac{29}{38}$ $\frac{42}{42}$
	1.1 1.2 1.3 1.4 Log 2.1 2.2 2.3 2.4 Gra 3.1 3.2 3.3 3.4 Vot 4.1 4.2 4.3	1.2 Subsets and Venn Diagrams 1.3 Operations with Sets 1.4 Applications and Survey Analysis  Logic 2.1 Logic Statements and their Negations 2.2 Truth Tables 2.3 Logical Equivalence and De Morgan's Laws 2.4 Valid Arguments and Fallacies  Graph Theory 3.1 Introduction to Graph Theory 3.2 Trees 3.3 Matchings 3.4 Planar Graphs  Voting Theory 4.1 How to Determine a Winner 4.2 Flaws in Voting Methods 4.3 Apportionment 1

iv CONTENTS

## Chapter 1

## Set Theory

### 1.1 Set Notation

**Definition 1.1.1.** A **set** is a collection of objects made up of specified elements, or members.

**Definition 1.1.2. Roster notation** specifies the members of a set by listing all of the elements in the set, separated by commas and surrounded by curly braces.

Example 1.1.3. Use roster notation to represent the following sets.

(a) S is the set of states in the United States that begin with the letter M.

#### (b) Given the sets

{blue, red, green}, {red, white, blue}, {blue, green, aqua}, and {red, white},

let T be the set of sets that contain the element "red."

**Definition 1.1.4** (Equal Sets). Two sets are said to be **equal** if they contain exactly the same elements. If sets A and B are equal, we write A = B.

**Definition 1.1.5** (Cardinal Number). The number of elements contained in a finite set is called the **cardinal number** of the set, or the **cardinality**. The cardinal number of set A is denoted by |A|.

**Definition 1.1.6** (Equivalent Sets). Two sets are said to be **equivalent** if they have the same cardinal number. If set A is equivalent to set B, we write  $A \sim B$ .

**Example 1.1.7.** Determine if the given pairs of sets are equal, equivalent, or neither.

(a)  $A = \{\text{Public Health, International Studies, Mechanical Engineering, Music Education, Political Science}\}$ ,  $B = \{\text{Tim, Gloria, Alan, Warren, Kalif}\}$ .

(b)  $X = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}, Y = \{20, 18, 16, 14, 12, 10, 8, 6, 4, 2\}.$ 

**Example 1.1.8.** Find the cardinality of W and Y. Determine if the sets are equal, equivalent, or neither.

$$W = \{3, 6, 12, 24\}$$
 and  $Y = \{2, 4, 8, 16, 32\}$ 

1.1. SET NOTATION 3

**Definition 1.1.9. Set-builder notation** specifies the members of a set using a variable, a vertical separator, and a rule defining the elements, all surrounded by curly braces. It can be used when the members of the set all share certain properties.

**Example 1.1.10.** The set of all integers is represented by

$$\mathbb{Z} = \{ n \mid n \text{ is an integer} \}$$

and is read,

" $\mathbb{Z}$  is the set of all n such that n is an integer."

**Example 1.1.11.** Use set-builder notation to represent Y, the set of all even integers.

**Exercise 1.1.12.** Represent the set J, which consists of all natural numbers less than 10, using both roster notation and set-builder notation.

**Definition 1.1.13.** The **empty set** is the set that contains no elements. If set A is empty, we write

$$A = \emptyset$$
 or  $A = \{\}.$ 

The cardinality of the empty set is 0.

Example 1.1.14. Determine if the following sets are the empty sets.

(a)  $A = \{x \mid x \text{ is a negative number less than } 100\}.$ 

- (b) The set B of any state that contains the letter "q" in its name.
- (c)  $C = \{ \_ \}.$

**Exercise 1.1.15.** Determine if set Y is the empty set.

 $Y = \{x \mid x \text{ is a US citizen who held the office of president before Barack Obama, and } x \text{ is a woman}\}$ 

1.1. SET NOTATION 5

**Definition 1.1.16.** The set of all elements being considered for any particular situation is called the **universal set** and is denoted by U.

**Definition 1.1.17.** The **complement** of set A consists of all the elements in the given universal set that are not contained in A. The complement of A is denoted A'.

**Example 1.1.18.** According to a recent poll, approximately 30% of American adults have at least one tattoo[Jac19]. Let

 $U = \{x \mid x \text{ is an American adult}\}$   $A = \{x \mid x \text{ is an American adult who has at least one tattoo}\}$   $B = \{x \mid x \text{ is an American adult who has exactly two tattoos}\}$ 

Write the complements of A and B using set-builder notation.

#### Example 1.1.19. Let

 $U = \{x \mid x \text{ is a book published in the US in 2021}\}\$  $A = \{x \mid x \in U \text{ and you read } x \text{ as an e-book}\}.$ 

(a) Find A'.

(b) Is it possible for you to have read a book in A'?

### 1.2 Subsets and Venn Diagrams

**Definition 1.2.1.** A **Venn diagram** is a visualization of the relationships between a collection of sets. In a Venn diagram, the sets are represented by circles (or ovals) contained within a rectangular region that represents the universal set.

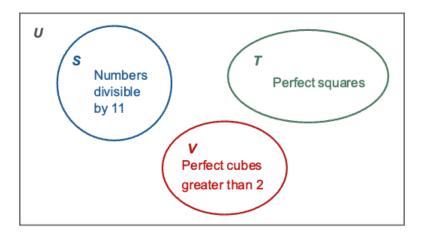
**Example 1.2.2.** The following Venn diagram represents the sets S, T, and V within the universal set

$$U = \{ x \in \mathbb{N} \mid x < 30 \}$$

The sets are defined as

$$S = \{x \mid x \text{ is divisible by } 11\},$$
 
$$T = \{x \mid x \text{ is a perfect square}\},$$
 
$$V = \{x \mid x > 2 \text{ and } x \text{ is a perfect cube}\}.$$

Use the diagram to answer the following questions.



(a) List the elements of the sets S, T, and V in roster notation.

(b) Find |S|, |T|, and |V|.

(c) Find T'.

(d) Is S = V? Is  $S \sim V$ ? Explain your answers.

**Example 1.2.3.** An increasing number of electric vehicles are on the roads in the United States. The number of charging locations available for these cars varies from state to state. The five states with the most public and private electric charging locations are California, New York, Florida, Texas, and Massachusetts. Let

 $U = \{x \mid x \text{ is a public or private electric charging location in the United States}\}$ 

 $C = \{x \mid x \text{ is located in California}\}$ 

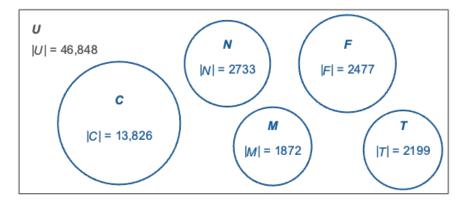
 $N = \{x \mid x \text{ is located in New York}\}$ 

 $F = \{x \mid x \text{ is located in Florida}\}\$ 

 $T = \{x \mid x \text{ is located in Texas}\}$ 

 $M = \{x \mid x \text{ is located in Massachusetts}\}$ 

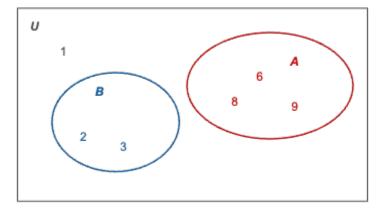
Use the following Venn diagram to answer the following questions. Assume all questions refer to both public and private locations.



- (a) Which state has the most electric charging locations?
- (b) Which state has the second highest number of charging locations?
- (c) How many electric charging locations do these five states have all together?

(d) How many charging locations are in the United States but are not in one of the five states in the diagram?

**Exercise 1.2.4.** Use the Venn diagram below to find the elements in  $A^\prime$ 



**Definition 1.2.5.** Let A and B be sets. The set B is a **subset** of A if every element of B is also an element of A. This is denoted by  $B \subseteq A$ .

Remark 1.2.6. Every set is a subset of itself. The empty set is a subset of every set.

**Example 1.2.7.** The school orchestra is divided into four sections: strings, woodwinds, brass, and percussion. Let S represent the four instruments in the strings section,

 $S = \{ \text{violin, viola, cello, double bass} \}.$ 

List all of the subsets of S.

Exercise 1.2.8. According to the Centers for Disease Control and Prevention (CDC), food allergies affect an estimated 8% of children in the United States[Cen20]. Wheat, soy, and peanuts are some of the most common food allergens. Let

```
U = \{x \mid x \text{ is a child in the United States}\}\
W = \{x \mid x \text{ is allergic to wheat}\}\
Y = \{x \mid x \text{ is allergic to wheat, soy, or peanuts}\}\
```

Draw a Venn diagram to represent the sets U, W, and Y.

#### Exercise 1.2.9. Draw a Venn diagram of the following

$$\begin{split} U &= \{x \mid x \text{ is a computer}\} \\ A &= \{x \mid x \text{ is an iPad}\} \\ B &= \{x \mid x \text{ is a tablet computer}\}\,. \end{split}$$

**Definition 1.2.10.** When  $B \subseteq A$ , and A contains at least one element that is not contained in B, then B is a **proper subset** of A and is denoted by  $B \subset A$ .

**Example 1.2.11.** Let  $M = \{a, b, c, d, e, f\}$ . Determine if the following sets are proper subsets of M.

(a) 
$$N = \{a, b, f\}$$

(b) 
$$P = \{c\}$$

(c) 
$$R = \{a, b, c, d, e, f\}$$

(d) 
$$S = \{a, b, h\}$$

**Example 1.2.12.** Let  $X = \{\text{Brazil, Vietnam, Columbia}\}$ , which are the top three coffee-producing countries in the world (as measured in metric tons). List all the proper subsets of X.

**Exercise 1.2.13.** List all of the proper subsets of the set  $\{a,b,c,d\}$ .

**Theorem 1.2.14** (Number of Subsets and Proper Subsets of a Set). If the cardinal number of a set is n, then the set has  $2^n$  subsets and  $2^n - 1$  proper subsets.

**Example 1.2.15.** Dr. Williams is eating at a local buffet one afternoon and notices a sign that says

"So many possibilities—you could spend a lifetime eating at our buffet and never have the same meal twice!"

He wonders how many different meals he could make from the 16 items on the buffet. He can have all, none, or some of the items. Determine the number of different meals he could make at the buffet.

### 1.3 Operations with Sets

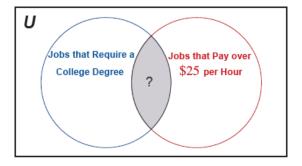
**Definition 1.3.1.** The **intersection** of two sets A and B is the set of all elements common to both A and B. We denote the intersection of A and B as

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

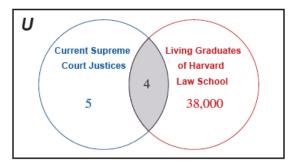
**Example 1.3.2.** Find the intersection of the sets

$$A = \{2, 3, 5, 7, 11, 13\}$$
 and  $B = \{2, 4, 6, 8, 10, 12\}.$ 

**Example 1.3.3.** Interpret the intersection of the sets in the Venn diagram in the following figure

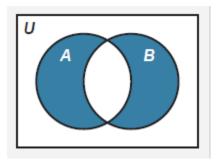


Exercise 1.3.4. Harvard Law School has produced more Supreme Court Justices than any other law school. Use the Venn diagram below to interpret how many of the sitting Justices as of August 2021 graduated from Harvard Law School.



**Exercise 1.3.5.** Let  $A = \{27, 111, 213\}$  and  $B = \{213, 40, 61, 88, 210, 27\}$ . Find  $A \cap B$ .

**Definition 1.3.6.** Two sets A and B are **disjoint** if there are no elements in set A that are also contained in set B. Their intersection is the empty set, denoted by  $A \cap B = \emptyset$ . Disjoint sets are represented by a Venn diagram where the overlap between the sets is empty,



**Example 1.3.7.** Let  $U = \{\text{all students}\}$ ,  $A = \{\text{students with GPA} < 2.5\}$ , and  $B = \{\text{students with GPA} > 3.0\}$ . Determine if sets A and B are disjoint and draw a Venn diagram to illustrate the relationship between sets A and B.

**Definition 1.3.8.** The **union** of two sets A and B is the set of all elements in A or in B. We denote the union of A and B as

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

**Example 1.3.9.** Sarah has lived in Ohio, Pennsylvania, and Michigan. Her friend Trevor has lived in Colorado, Ohio, and Georgia. Her friend Ron has lived in Washington and Idaho. Let the residential locations of each friend be represented by the following sets:

$$S = \{OH, PA, MI\},$$

$$T = \{CO, OH, GA\}, and$$

$$R = \{WA, ID\}.$$

Find the following unions.

(a)  $S \cup T$ 

(b)  $S \cup R$ .

**Example 1.3.10.** Let U be students enrolled at MLK High School,

$$A = \{x \mid x \text{ is in the student band}\}$$
, and  $B = \{x \mid x \text{ is in student government}\}$ .

Find  $A \cup B$ .

**Theorem 1.3.11** (Inclusion-Exclusion Principle). The cardinality of the union of two sets A and B is calculated by adding the number of elements in set A to the number of elements in set B and subtracting the number of elements that appear in both sets.

$$|A \cup B| = |A| + |B| - |A \cap B|$$
.

**Example 1.3.12.** Consider the scenario where a state senate is voting on a bill. The senate has 35 members, of which 15 are Democrats and 20 are Republicans. Five of the 35 members represent urban areas of the state, two of which are Democrats. The bill is expected to receive "Yes" votes from the Democrat members and from members who represent urban areas. Determine how many Yes votes the bill is expected to receive.

**Example 1.3.13.** Let  $U = \{a, b, c, d, e, \dots, z\}$ ,  $M = \{m, a, t, h\}$ ,  $N = \{m, o, n, e, y\}$ , and  $K = \{i, n, v, e, s, t, o, r\}$ . Find the following.

(a)  $M \cup (N \cap K)$ 

(b)  $M \cap (N \cup K)$ .

**Exercise 1.3.14.** Let  $U = \{a, b, c, d, e, \dots, z\}$ ,  $M = \{m, a, t, h\}$ ,  $N = \{m, o, n, e, y\}$ , and  $K = \{i, n, v, e, s, t, o, r\}$ . Find  $K \cap (M \cup N)$ .

**Exercise 1.3.15.** Let  $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ ,  $A = \{1, 2, 3, 4, 5\}$ , and  $B = \{2, 4, 6, 8\}$ . Find the following.

(a)  $(A \cup B)'$ 

(b)  $B' \cap A$ .

**Theorem 1.3.16** (De Morgan's Laws). Let A and B be sets. Then,

$$(A \cup B)' = A' \cap B'$$
 and  $(A \cap B)' = A' \cup B'$ .

Exercise 1.3.17. Let

$$U = \{ x \in \mathbb{N} \mid x \le 10 \}.$$

If set A represents even numbers that are less than or equal to 10 and set B represents prime numbers that are less than or equal to 10, then we can write the sets as follows.

$$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$
$$A = \{2, 4, 6, 8, 10\}$$
$$B = \{2, 3, 5, 7\}$$

Verify that  $(A \cup B)' = A' \cap B'$ .

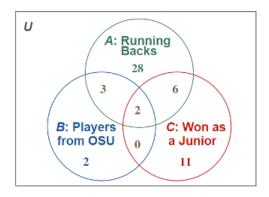
**Exercise 1.3.18.** Given sets  $U = \{a, b, c, d, e, f, g, h, i, j, k, l\}$ ,  $A = \{l, i, k, e\}$ , and  $B = \{c, a, k, e\}$ , verify  $(A \cap B)' = A' \cup B'$ .

## 1.4 Applications and Survey Analysis

Exercise 1.4.1. A survey that asked 500 donors of an artistic nonprofit organization about their musical choices showed that 350 of them listen to jazz, 300 listen to classical, and 200 listen to both. Draw a Venn diagram to illustrate this survey and determine how many donors surveyed don't listen to either jazz or classical music.

**Exercise 1.4.2.** A survey of 400 customers at an ice cream shop showed that 225 customers like chocolate ice cream, 300 like vanilla, and 200 like both. Draw a Venn diagram to illustrate the survey results. How many customers responded that they didn't like either chocolate or vanilla ice cream?

Exercise 1.4.3. The Heisman Trophy, created in 1935, is awarded every year to an outstanding college football player. The Venn diagram below tells us about some of the past winners and contains the number of elements that belong to the three sets A, B, and C. A is the set of winners whose position was that of running back, B is the set of winners from The Ohio State University (OSU), and C is the set of winners who were classified as juniors when they won.

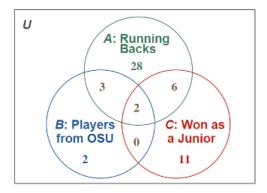


Use the information in the diagram to determine the following and describe what each represents.

(a)  $|A \cap B \cap C|$ .

(b)  $|A \cap B|$ 

Exercise 1.4.4. Use the Venn diagram below to answer the following questions



(a) 
$$|A \cap C|$$

(b) 
$$|B \cap C|$$

Exercise 1.4.5. Draw a Venn diagram to represent the relationships between the sets

$$\begin{split} U &= \{a, b, c, \dots, z\} \\ A &= \{a, e, i, o, u\} \\ B &= \{a, b, c, d, e, f, g, h, i, j, k, l\} \\ C &= \{a, l, u, m, n, i\}. \end{split}$$

Exercise 1.4.6. A group of students majoring in international relations are polled on whether they have taken courses in any of three languages: French, German, and Russian. Every student took at least one of the languages. No student who took French also took Russian, but 39 who took French also took German. Eighty-four students who took German also took Russian. Altogether, 55 reported taking French, 141 reported taking German, and 92 reported taking Russian. Draw a Venn diagram to illustrate this survey and determine how many students were polled.

Exercise 1.4.7. A survey of shoppers at a grocery store found that 225 shoppers like bananas, 198 like apples, and 180 like grapes. All of the shoppers like at least one of the three fruits. Twenty-five shoppers like all three fruits. There are 110 shoppers that like bananas and apples, 58 that like apples and grapes, and 55 that like bananas and grapes. Draw a Venn diagram to illustrate this poll and determine how many shoppers were in the survey.

## Chapter 2

## Logic

## 2.1 Logic Statements and their Negations

**Definition 2.1.1.** A mathematical **statement** is a complete sentence that asserts a claim which is either true or false, but not both at the same time.

Mathematical logic statements are most commonly represented by lower case letters.

**Definition 2.1.2.** A paradox is a sentence that contradicts itself and therefore has no single truth value. A paradox cannot be a mathematical statement.

**Example 2.1.3.** Determine if the following sentences are statements.

a: It is raining outside.

b: Beaches are the most beautiful place to vacation.

c: Today is Monday.

d: Today is Monday and tomorrow is Friday.

e: I lie all the time.

**Definition 2.1.4.** The **negation** of a statement is the logical opposite of that statement, or its denial. Negations always have the opposite truth value of the original statement. Negations are denoted by the symbol  $\sim$ .

Example 2.1.5. Negate the following statements.

- a: Melony is wearing a red raincoat.
- b: The door is not closed.
- c: None of the tourists brought raincoats.
- d: I run less than Cara.

#### Exercise 2.1.6. Negate the statement

"Some of the students completed their assignments."

**Definition 2.1.7.** A **compound statement** is composed of two or more statements joined together by connective words such as "and", "or", or "implies."

**Definition 2.1.8.** If a and b are statements, then "a and b" is a compound statement called a **conjunction**. The symbol  $\wedge$  is used to represent a conjunction.

**Example 2.1.9.** Consider the following statements.

a: Snow is falling.

b: The sun is shining.

Write the following compound statements using logic symbols.

c: Snow is falling and the sun is shining.

d: The sun is shining and snow is not falling.

**Definition 2.1.10.** If a and b are statements, then "a or b" is a compound statement called a **disjunction**. The symbol  $\vee$  is used to represent a disjunction.

**Example 2.1.11.** Consider the following statements.

p: He will go to the movies tonight.

q: He will stay home to give the dog a bath tonight.

Write the following compound statements using logic symbols.

r: He will go to the movies tonight or he will stay home to give the dog a bath tonight.

s: He will not go to the movies to night or he will not stay home to give the dog a bath to night.

Exercise 2.1.12.	Consider	the	following	statements.
------------------	----------	-----	-----------	-------------

- a: I am hungry.
- b: I am tired.
- c: I am in college.

Write the following three compound statements symbolically.

1. I am hungry and tired.

2. I am hungry or I am in college.

3. I am tired and not in college.

**Definition 2.1.13.** If a and b are statements, then "if a, then b" is a compound statement called a **conditional**. The symbol  $\implies$  is used to represent a conditional statement.

Remark 2.1.14. There are many ways to convey  $p \implies q$ . Here are a few:

- "p implies q"
- "if p, then q"
- "p is sufficient for q"
- "q is necessary for p"
- "p will lead to q"
- "q if p"
- "q whenever p"
- "p only if q"

**Example 2.1.15.** Consider the following statements.

s: The water temperature on Saturday is below 76.2°F.

t: You are allowed to wear a wet suit in the triathlon.

Write the following compound statements using logic symbols.

q: If the water temperature on Saturday is below 76.2°F, then you are allowed to wear a wet suit in the triathlon.

r: You are not allowed to wear a wet suit in the triathlon if the water temperature on Saturday is not below 76.2°F.

**Definition 2.1.16.** If a and b are statements, then "a if and only if b" is a compound statement called a **biconditional**. The symbol  $\iff$  is used to represent a biconditional statement.

**Example 2.1.17.** Consider the following statements.

c: Octopuses have three hearts.

d: The platypus does not have a stomach.

Write the following compound statements using logic symbols.

e: The platypus does not have a stomach if and only if octopuses have three hearts.

f: Octopuses do not have three hearts if and only if the platypus has a stomach.

### 2.2 Truth Tables

**Definition 2.2.1.** A **truth table** is a chart with rows and columns that systematically lists out each possible combination of truth values for a statement.

**Example 2.2.2.** The truth table for negation is

$$\begin{array}{c|c} a & \sim a \\ \hline T & F \\ F & T \end{array}$$

**Definition 2.2.3.** If a and b are statements, then the **conjunction** "a and b" is true only when both a and b are true; otherwise, the conjunction is false.

$$\begin{array}{c|ccc} a & b & a \wedge b \\ \hline T & T & T \\ T & F & F \\ F & T & F \\ F & F & F \\ \end{array}$$

**Definition 2.2.4.** If a and b are statements, then the **disjunction** "a or b" is always true unless a and b are both false.

$$\begin{array}{c|ccc} a & b & a \lor b \\ \hline T & T & T \\ T & F & T \\ F & T & T \\ F & F & F \\ \end{array}$$

**Definition 2.2.5.** If a and b are statements, then the **conditional** "if a, then b" is always true unless a is true and b is false.

$$\begin{array}{c|ccc} a & b & a \Longrightarrow b \\ \hline T & T & T \\ T & F & F \\ F & T & T \\ F & F & T \end{array}$$

**Definition 2.2.6.** If a and b are statements, then the **biconditional** "a if and only if b" is true only if a and b have the same truth value; that is, either both are true or both are false.

$$\begin{array}{c|cccc} a & b & a & \Longleftrightarrow & b \\ \hline T & T & & T \\ T & F & & F \\ F & T & & F \\ F & F & & T \\ \end{array}$$

**Example 2.2.7.** Complete the truth table for the conjunction  $\sim (a \wedge b)$  to determine when the statement is true and when it is false.

a	b	$a \wedge b$	$\sim (a \wedge b)$
T	T		
T	F		
F	T		
F	F		

**Example 2.2.8.** Consider the following statements.

f: Arizona is the first state listed alphabetically.

g: Albany is the capital of New York.

Determine the truth value of each statement and then use the truth table from Example 2.2.7 to determine if the statement  $\sim(f\wedge g)$  is true or false.

**Example 2.2.9.** Complete the truth table for the conjunction  $(c \lor d) \implies \sim e$ . to determine when the statement is true and when it is false.

c	d	e	$c \vee d$	$\sim e$	$(c \lor d)$	$\implies \sim e$
T	T	T				
T	T	F				
T	F	T				
T	F	F				
F	T	T				
F	T	F				
F	F	T				
F	F	F				

2.2. TRUTH TABLES 41

Exercise 2.2.10. Construct the truth table for the following compound statement and determine when the statement is true and when it is false.

If you're not making mistakes, then you're not doing anything. —John Wooden

**Exercise 2.2.11.** Construct a truth table for the conditional statement in Example 2.2.10. This time let statements a and b be the following.

a: You are not making mistakes.

b: You are not doing anything.

Does your truth table have the same truth values as the table in Example 2.2.10? Should it?

2.2. TRUTH TABLES 43

**Definition 2.2.12.** A **tautology** is a statement that is true in all possible circumstances.

Example 2.2.13. Construct the truth table for the compound statement

Next year, Imre can take physics or he cannot take physics.

**Example 2.2.14.** Consider the following quote from the movie *The Hunger Games: Catching Fire*[hun14]. Peeta Mellark to Katniss Everdeen:

- "...if you can stop looking at me like I'm wounded, then I can quit acting like it. Then maybe we have a shot at being friends."
- (a) Construct a truth table for Peeta's conditional quote.

(b) Determine if Peeta's statement is a tautology.

## 2.3 Logical Equivalence and De Morgan's Laws

**Definition 2.3.1. Logically equivalent** statements are statements that have exactly the same truth values in all corresponding circumstances. Equivalence is denoted with the symbol  $\equiv$ .

**Example 2.3.2.** Use a truth table to determine if p and  $\sim(\sim p)$  are logically equivalent.

**Example 2.3.3.** Use truth tables to show that  $p \implies q \equiv \sim p \lor q$ .

**Exercise 2.3.4.** Use a truth table to show that  $a \vee a \equiv a$ .

Exercise 2.3.5. Determine if the following statements are logically equivalent to the conditional statement

If it rains on Saturday, we will not go to the ball-game.

1. It is raining on Saturday and we will not go to the ball-game.

2. It is not raining on Saturday or we will not go to the ball-game.

3. If we do go to the ball-game, then it is not raining on Saturday.

**Theorem 2.3.6** (De Morgan's Laws). If p and q are logical statements, then

1. 
$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
, and

2. 
$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$
.

Example 2.3.7. Write the negations of the following statements using De Morgan's laws.

(a) I will exercise or sleep in tomorrow.

(b) Jack and Jill went up the hill.

#### Example 2.3.8. Write the negation of the compound statement

The football team will win or they will be out of the tournament, and their ranking will improve

using De Morgan's laws.

**Theorem 2.3.9** (Negation of Conditionals). If p and q are logical statements, then

$$\sim (p \implies q) \equiv p \land \sim q.$$

Remark 2.3.10. This follows from Example 2.3.3 and De Morgan's laws.

Exercise 2.3.11. Write the negation of the conditional statement

If I go to Moss' Diner, then I get the triple stack pancakes.

#### Exercise 2.3.12. Negate the statement

If the weather gets worse, then we will leave.

Exercise 2.3.13. Use the rule of negation of conditional statements and De Morgan's Laws to negate the conditional statement

$$a \implies (c \wedge d).$$

Remember that the solution will be a compound statement.

51

**Definition 2.3.14.** The **converse** of the conditional statement "if p, then q" is the statement "if q, then p."

$$\begin{array}{c|ccccc} p & q & p \Longrightarrow q & q \Longrightarrow p \\ \hline T & T & T & T & T \\ T & F & F & T \\ F & T & T & F \\ F & F & T & T \end{array}$$

**Definition 2.3.15.** The **inverse** of the conditional statement "if p, then q" is the statement "if not p, then not q."

p	q	$p \implies q$	$ \sim p \implies \sim q$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

**Definition 2.3.16.** The **contrapositive** of the conditional statement "if p, then q" is the statement "if not q, then not p."

p	q	$p \implies q$	$ \sim q \implies \sim p$
$\overline{T}$	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Example 2.3.17. Write the converse, inverse, and contrapositive of the statement

If I save enough money, I will go on a vacation.

State which of these new conditional statements is equivalent to the original statement.

Exercise 2.3.18. Write the converse, inverse, and contrapositive of the statement If I cannot find my phone, then it is in the car.

### 2.4 Valid Arguments and Fallacies

**Definition 2.4.1.** A **logical argument** consists of a series of logical statements.

**Definition 2.4.2.** A **premise** is a statement at the beginning of an argument used to support a particular conclusion.

**Definition 2.4.3.** A **conclusion** is the ending statement of an argument.

**Example 2.4.4.** Identify the premises and conclusion in each of the following arguments.

(a) If we update the technology, then we will have a better product and fewer complaints. Our technology was updated last month, so we will receive fewer complaints this month.

(b) The president of the United States must be younger than 40. Bruce Springsteen is president of the United States. Therefore, Bruce Springsteen must be younger than 40.

Exercise 2.4.5. Identify the premises and conclusion in the following argument. If the weather is warm, we will go the beach. We're at the beach, so it must be warm outside.

**Definition 2.4.6.** A **valid argument** is a deductive argument where the conclusion is always guaranteed from the premises.

**Definition 2.4.7.** An **invalid argument** is a deductive argument where the conclusion is not always guaranteed from the premises.

**Process 2.4.8.** To use a Truth Table to determine the validity of an argument follow these steps.

1. Express the argument in symbolic form as an if-then statement. The if portion will consist of the premises joined together with conjunctions. The then portion is the conclusion. For example, if there are n premises, the statement will be of the form

[(premise 1) 
$$\land$$
 (premise 2)  $\land \cdots \land$  (premise n)]  $\implies$  conclusion.

- 2. Construct a truth table for the if-then statement.
- 3. If the implication is a tautology, then the argument is valid, otherwise the argument is invalid.

**Example 2.4.9.** Decide if the following argument is valid by using a truth table.

If someone lives in the city of Phoenix, Arizona, then they live in the Mountain Standard Time Zone. Sebastian does not live in the Mountain Standard Time Zone. Therefore, Sebastian does not live in the city of Phoenix, Arizona.

Example 2.4.10. Decide if the following argument is valid by using a truth table.

If you work hard, you will succeed. You succeeded, so you must have worked hard.

Exercise 2.4.11. Determine whether the following argument is valid.

If my phone crashes, then I will lose all my photos. My phone did not crash. Therefore, I did not lose my photos.

**Definition 2.4.12.** A **sound argument** is a valid argument using true premises.

**Example 2.4.13.** Use a truth table to determine if the following is a sound argument.

If the President of the United States is unable to carry out his or her constitutional role, then the Vice President becomes the President of the United States. In November 1963, President John F. Kennedy was fatally shot. Therefore, without an election, Vice President Lyndon Johnson became President of the United States.

Exercise 2.4.14. Determine whether the following is a sound argument.

If Canada is north of the United States, then Alaska is in Mexico. Canada is north of the United States. Therefore, Alaska is in Mexico.

**Definition 2.4.15.** A **fallacy** is an error in reasoning that leads to an invalid argument. The following table lists some common fallacies

Type of Fallacy	Description
Post Hoc, Ergo Propter Hoc	Because one thing happened first,
(After This,	it caused the other to happen.
Therefore Because of This)	
Dicto Simpliciter	Making broad, sweeping generalizations
(Hasty Generalization)	based on a few specific occurrences.
Ad Hominem	Attacking someone's person, character,
(Personal Attack)	or motives instead of addressing
	the premise of the argument
Petitio Principii	The premise and conclusion state
(Circular Reasoning)	the same thing.
Non Sequitur	The conclusion does not logically
(It Does Not Follow)	follow from the premise; it follows a diversion.
Straw Man	The distortion of someone's ideas or beliefs
(Exaggerated or Distorted	so that they can easily be knocked down.
View of the Opponent)	
False Dilemma	Argument that rests on the assumption
(Illusion of Limited Choice)	that there are only two choices as a solution.
Argumentum ad Populum	Stating that the majority, or even just a large
(Appeal to the People)	number, of people are doing something
	as the basis for supporting a conclusion.

Example 2.4.16. Identify the type of fallacy used in each of the following statements.

a: If public spending is not reduced, our economy will collapse.

b: Heather just had a new fuel pump put in her car. Forty-eight hours later, her car won't start. Heather's father thinks the mechanic must not have installed the fuel pump correctly.

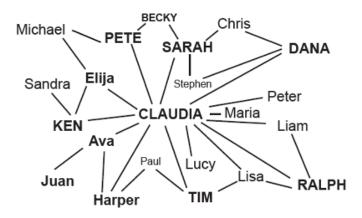
## Chapter 3

# Graph Theory

## 3.1 Introduction to Graph Theory

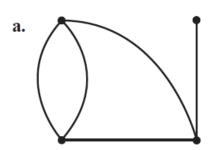
**Definition 3.1.1.** A **graph** consists of a set of vertices and a set of edges that join pairs of vertices together. Graphs are generally represented with a capital letter, such as G.

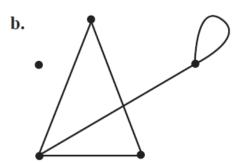
**Example 3.1.2.** In graph A, identify the vertices and edges.



**Definition 3.1.3.** A **loop** is an edge that has the same vertex for both of its ends.

Example 3.1.4. For the given graphs, label each vertex and edge. Identify any loops.

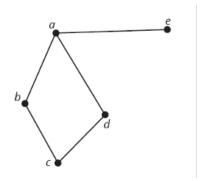




**Definition 3.1.5.** A walk in a graph is a finite list of alternating vertices and connecting edges that begins and ends with a vertex.

We say a walk is **closed** if it starts and ends at the same vertex.

**Example 3.1.6.** Use graph B to answer the following questions.



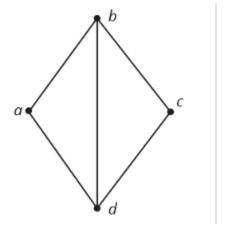
(a) Identify a walk of length 2 that starts at vertex a and ends at vertex c.

(b) Is the walk you just found a closed walk?

**Exercise 3.1.7.** Identify a walk of length 3 in graph B from Example 3.1.6. Start the walk at vertex c.

 $\textbf{Definition 3.1.8.} \ \, \textbf{A} \ \, \textbf{path} \ \, \textbf{is a walk with no repeated edges or vertices}. \\$ 

**Example 3.1.9.** Identify a path of length 3 starting at vertex a and ending at vertex d in graph C.



**Definition 3.1.10.** A graph is **connected** if there is at least one path connecting each pair of distinct vertices.

**Definition 3.1.11.** A graph is **disconnected** if it has at least one pair of vertices that is not connected by a path.

Example 3.1.12. Label each graph as connected or disconnected. Explain your answer.

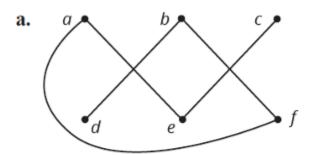


Figure 14.1.20: Graph A

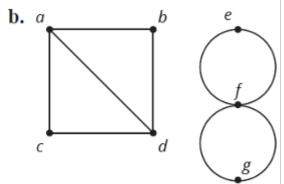


Figure 14.1.21: Graph B

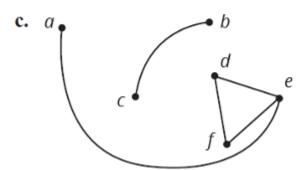
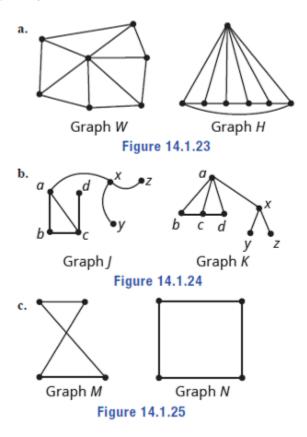


Figure 14.1.22: Graph C

**Example 3.1.13.** Decide whether the pairs of graphs shown could be different views of the same graph or not. Explain your answer.

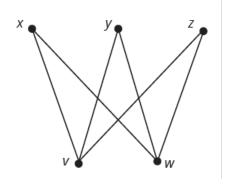


**Definition 3.1.14.** Two vertices that share an edge are **adjacent**.

**Definition 3.1.15.** Two edges that share a vertex are **incident** to one another. Also, a vertex is incident to the edges that have that vertex as an endpoint.

**Definition 3.1.16.** The **degree** of a vertex denoted d(u), is the number of edges that are incident to u.

**Example 3.1.17.** Use Graph A to solve the following problems.

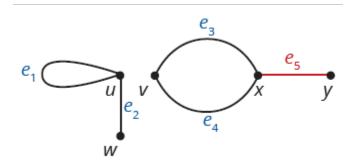


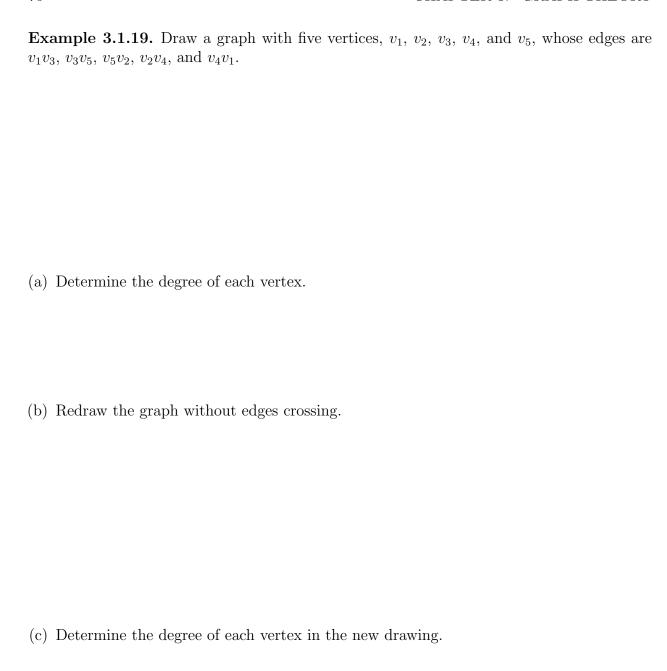
(a) Determine the degree of each of the vertices.

(b) Name the pairs of vertices that are adjacent.

(c) Name the pairs of edges that are incident.

Exercise 3.1.18. Identify all pairs of adjacent vertices and all pairs of incident edges in the graph below.





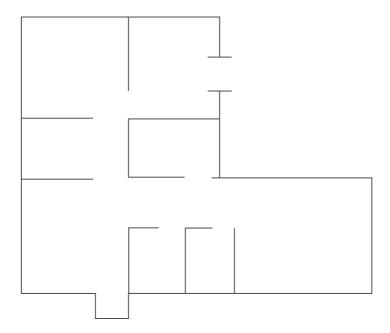
**Example 3.1.20.** A research chemist is analyzing the structure of compounds of aluminum, iron, and oxygen. Each aluminum atom makes three chemical bonds, each oxygen atom makes two chemical bonds, and each iron atom makes six chemical bonds. Create a possible form for a molecule of two aluminum atoms, two oxygen atoms, and one iron atom where no atom makes a chemical bond to itself.

Exercise 3.1.21. Draw a different graph with the same restrictions as in Example 3.1.20: no loops, having two vertices of degree 3, two vertices of degree 2, and one of degree 6.

**Definition 3.1.22.** A **vertex cover** is a set of vertices A so that every vertex in the graph is either in A or adjacent to a vertex in A.

**Definition 3.1.23.** When a vertex cover A is as small as possible, A is called a **minimum** vertex cover.

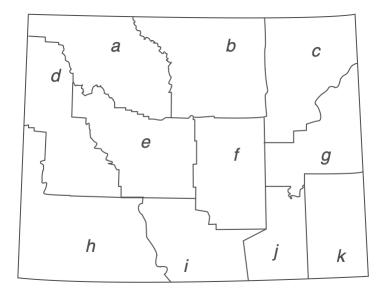
**Example 3.1.24.** Use the blueprint for the museum below to determine the minimum number of security guards that would be needed if one guard can secure one room and all the rooms that share a doorway with it.



**Definition 3.1.25.** A **vertex coloring** of a graph is an assignment of colors to the vertices of the graph so that adjacent vertices receive different colors.

**Definition 3.1.26.** When the number of colors used in a vertex coloring is as small as possible, this number is called the **chromatic number** of a graph and is denoted  $\chi(G)$ , read "chi of G."

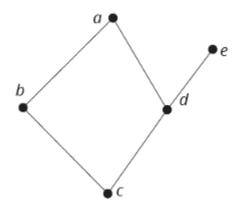
**Example 3.1.27.** A wireless communications service provider needs to place cell towers in all counties of the state shown below.



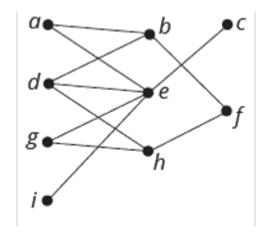
When two cell towers are placed in adjacent counties, they interfere with each other's signal unless they are on different frequencies. To minimize costs, the provider needs to use as few frequencies as possible. Find the lowest cost arrangement of the frequencies of the cell towers for the provider.

**Definition 3.1.28.** A **cycle** is a walk that starts and ends at the same vertex and has no edges or vertices repeated except for the starting vertex.

**Example 3.1.29.** Identify a cycle in graph G and determine its length.



Exercise 3.1.30. Identify a cycle of length 6 in the following graph.

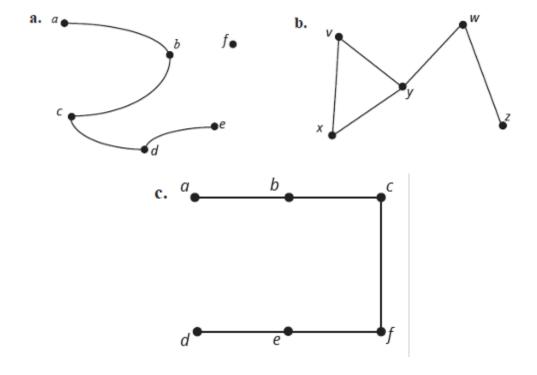


3.2. TREES 77

## 3.2 Trees

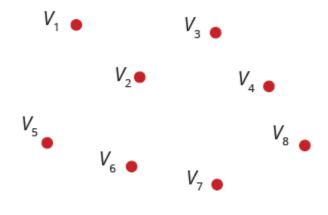
**Definition 3.2.1.** A connected graph with no cycles is called a **tree**.

Example 3.2.2. Determine which of the following graphs is a tree.



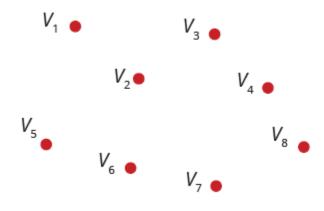
**Theorem 3.2.3.** Let graph T be a tree on v vertices. Then graph T has v-1 edges.

**Example 3.2.4.** Determine the number of edges needed to connect the given vertices so that the resulting graph is a tree.



3.2. TREES 79

Exercise 3.2.5. Construct two different trees with the vertices

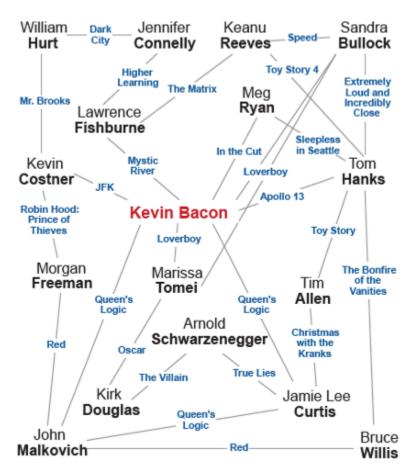


**Definition 3.2.6.** A spanning tree is a subgraph of a connected graph, which is itself connected and contains all the vertices of the original graph, but has no cycles.

**Process 3.2.7.** To construct a spanning tree, follow these steps.

- 1. In a connected graph G, identify a cycle. If more than one cycle exists, choose one at random.
- 2. Choose an edge from the cycle selected and delete it from the graph.
- 3. While the graph contains a cycle, repeat Steps 1 and 2.

**Example 3.2.8.** In an interview in *Premier Magazine* in 1994, Kevin Bacon commented that he had acted together with almost everyone in Hollywood. The game "Six Degrees of Kevin Bacon" was invented based on this comment. The goal is to link any named actor to Kevin Bacon by beginning with the named actor and naming no more than six actors, ending with Kevin Bacon, where each successive pair of actors have appeared in a movie together. Find a spanning tree for the following graph, in which the vertices are actors, and two actors are joined by an edge if they appeared together in a movie, where the edges are labeled with the movie.



3.2. TREES 81

Exercise 3.2.9. Find another spanning tree for the Kevin Bacon graph in Example 3.2.8 by deleting a different set of edges.

**Definition 3.2.10.** A weighted graph is a graph with numbers (called weights) associated to each edge.

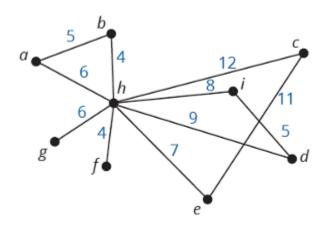
**Definition 3.2.11.** The **weight** of a weighted graph is the sum of all its edge weights.

**Definition 3.2.12.** A minimum-weight spanning tree is a spanning tree with the smallest possible weight.

**Process 3.2.13** (Kruskal's Algorithm). To construct a minimum-weight spanning tree, follow these steps.

- 1. Consider each edge in the graph in order of descending weight.
- 2. If the edge being considered is part of a cycle, remove it. If not, it must remain in the graph, and you can move on to the next edge.
- 3. Repeat Steps 1 and 2 until all edges have been considered.

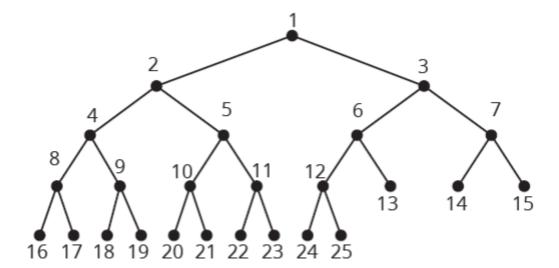
**Example 3.2.14.** SpeedFirst Telecommunications is going to run its fiber optic cable in a new development. The edges in the given graph represent the possible ways that the cable can be run. The weight of each edge is the length of the cable needed, in meters. Find the minimum spanning tree using the algorithm to obtain the most cost-efficient way for SpeedFirst to run the cable. What is the minimum amount of cable that SpeedFirst will need to run in the new development?



3.2. TREES 83

**Definition 3.2.15.** A vertex of degree 1 in a tree is called a **leaf**.

**Example 3.2.16.** Determine the number of leaves on the tree T.



**Theorem 3.2.17.** If a tree has k vertices with degrees  $d_1, d_2, \ldots, d_k$ , each greater than 1, then the number of leaves on the tree is

$$\sum_{i=1}^{k} d_i - 2k + 2 = d_1 + d_2 + \dots + d_k - 2k + 2.$$

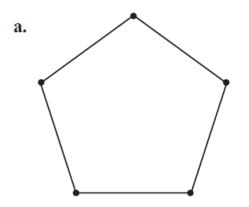
**Example 3.2.18.** Governor Airlines has airport hubs in seven cities. Those seven cities have connecting flights to 2, 3, 6, 8, 7, 4, and 5 cities, respectively. If the graph formed by joining each pair of available flights is a tree, how many different destinations does Governor Airlines fly to?

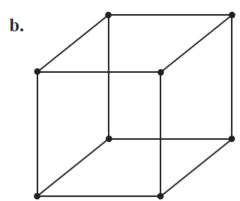
3.3. MATCHINGS 85

#### 3.3 Matchings

**Definition 3.3.1.** A **bipartite graph** is a graph in which the vertices can be partitioned into precisely two subsets so that every edge joins a vertex in one subset to a vertex in the other subset.

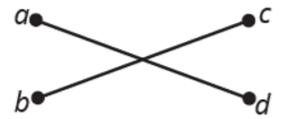
Example 3.3.2. Determine if the following graphs are bipartite.





**Theorem 3.3.3.** A graph is a bipartite graph if and only if its chromatic number is 2.

Exercise 3.3.4. Determine if the following graph is bipartite.



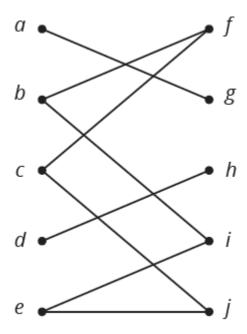
3.3. MATCHINGS 87

**Definition 3.3.5.** A **matching** is a subset of edges in a graph so that each vertex is incident with at most one edge.

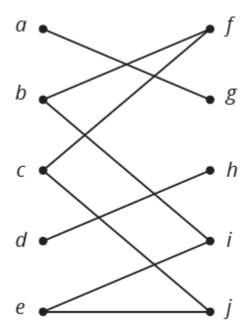
We say a matching with no unmatched vertices is a **perfect matching**.

**Definition 3.3.6.** If we have a set of vertices A, then the **neighborhood** of A, denoted N(A), is the set of all vertices adjacent to a vertex in A.

**Example 3.3.7.** Let A be the set of vertices  $\{d, e\}$ . Identify the neighborhood of A in the Graph below



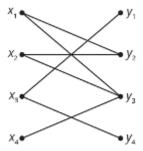
**Exercise 3.3.8.** Let B be the set of vertices  $\{a,b\}$ . Identify the neighborhood of B in the graph below.



3.3. MATCHINGS

**Theorem 3.3.9** (Hall's Marriage Theorem). Let G be a bipartite graph. Then there is a matching of the left-hand vertices into the right-hand vertices if and only if for every subset of left-hand vertices A, the number of vertices in N(A) is at least as large as the number of vertices in A.

**Example 3.3.10.** Use Hall's Marriage Theorem to determine if matching is possible for the graph



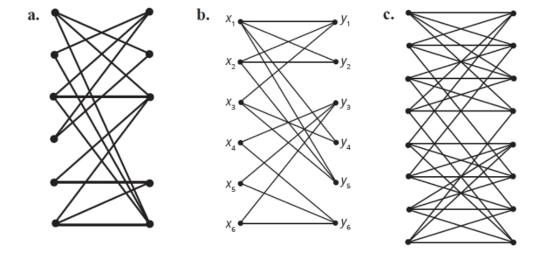
Exercise 3.3.11. Three top prizes are to be given to the three highest salespeople—a new phone, a flight voucher, and a gift card of choice. John, Mo, and Richard have their sights set on the prizes they would prefer to win. John would like either the new phone or the gift card. Mo prefers the flight voucher, while Richard's top pick is the new phone. Is there a way for each salesperson to receive a prize they prefer if there is only one of each prize?

3.3. MATCHINGS 91

**Definition 3.3.12.** A **regular graph** is a graph where every vertex has the same degree.

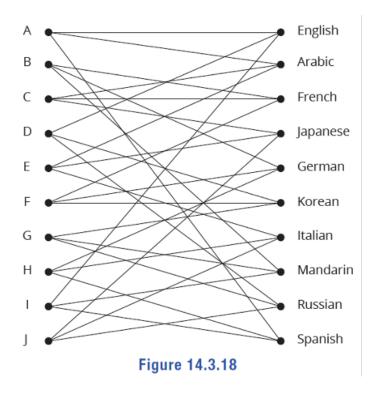
**Definition 3.3.13.** A **regular bipartite graph** is a regular graph with the same number of vertices on both the left-hand side as the right-hand side.

**Example 3.3.14.** Determine whether each graph is a regular bipartite graph.



**Theorem 3.3.15.** A regular bipartite graph has a matching.

**Example 3.3.16.** At the British Museum in London, multimedia tours are offered in English, Korean, Arabic, French, German, Italian, Japanese, Mandarin, Russian, and Spanish. A group of ten students wonder if they can listen to the museum tour in a language they understand with each student listening to a different language. The graph shows which languages each student can understand. Determine if the graph has a matching that would allow the students to each have a unique language for their tour.

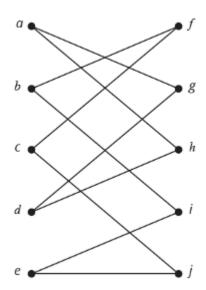


3.3. MATCHINGS 93

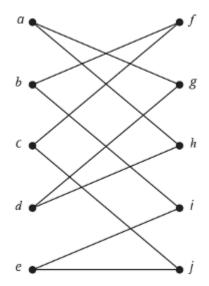
**Process 3.3.17** (Schriver's Algorithm). Steps for Finding a Matching in a Regular Bipartite Graph

- 1. Given a regular bipartite graph G, give every edge in G a weight of 1.
- 2. Let C be a cycle in the edges of positive weight.
  - a. Number the edges of C successively in turn.
  - b. Increase the weight of the even-numbered edges by 1.
  - c. Decrease the weight of the odd-numbered edges by 1.
- 3. Repeat Step 2 until the edges with positive weight contain no cycle.
- 4. The positively weighted edges form a matching.

Example 3.3.18. Find a matching for the following regular bipartite graph



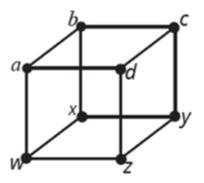
Exercise 3.3.19. Find a different matching for the regular bipartite graph



### 3.4 Planar Graphs

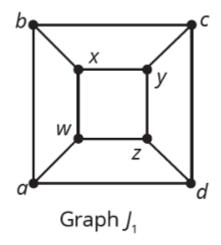
**Definition 3.4.1.** Graphs that can be drawn on a plane without edges crossing are called **planar graphs**.

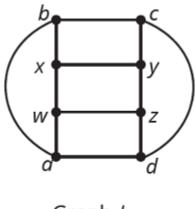
Exercise 3.4.2. Draw the following graph without any edges crossing.



**Definition 3.4.3.** In a planar graph, a **face** is a region inside a cycle of edges or the infinite exterior region on the outside of the graph. We denote the number of faces of a graph by f.

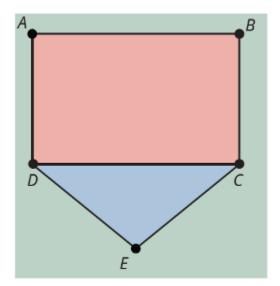
**Example 3.4.4.** Two drawings of the same graph are shown below. Verify that both drawings have the same number of faces.





Graph  $J_2$ 

Exercise 3.4.5. Consider the graph



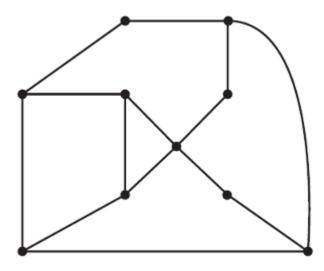
(a) How many faces are there if we remove the edge CE from the following graph?

(b) How many faces are there if we add the edge BD to the following graph?

**Theorem 3.4.6** (Euler's Formula). If G is a connected planar graph with v vertices, e edges, and f faces, then

$$v + f - e = 2.$$

**Exercise 3.4.7.** Confirm Euler's formula for the planar graph G.



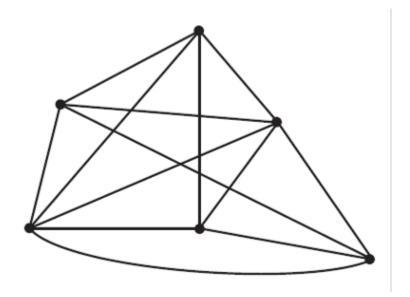
99

**Corollary 3.4.8.** A planar graph G with v vertices has at most 3v-6 edges. That is,  $e \leq 3v-6$ .

**Exercise 3.4.9.** If graph G has 13 vertices, what is the greatest number of edges that graph G can have and be a planar graph?

Exercise 3.4.10. What is the maximum number of edges that a five-vertex graph can have and still be planar? (Hint: Draw a graph to help you find the answer.)

Exercise 3.4.11. Use the corollary of Euler's formula to establish the following graph is not planar.



101

**Definition 3.4.12.** A **complete graph**,  $K_n$ , is the graph on n vertices in which every vertex is joined to every other vertex by a single edge.

**Exercise 3.4.13.** Draw the complete graph  $K_6$ .

Exercise 3.4.14. Draw the complete graph  $K_7$ .

**Definition 3.4.15.** A complete bipartite graph  $K_{m,n}$  is the bipartite graph with m vertices on the left-hand side and n vertices on the right-hand side. Each vertex on the left is joined to every vertex on the right with a single edge.

**Exercise 3.4.16.** Draw the complete bipartite graph  $K_{2,2}$ .

Exercise 3.4.17. Is  $K_{2,2}$  planar?

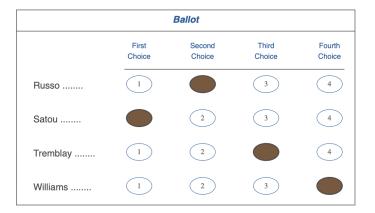
# Chapter 4

# Voting Theory

#### 4.1 How to Determine a Winner

**Definition 4.1.1.** A **preference ballot** is a ballot that allows a voter to rank the items in order of preference from most preferred to least preferred.

**Example 4.1.2** (Preference Ballot). Below is an example of a possible preference ballot.



**Definition 4.1.3.** A **preference table** summarizes all of the individual preference ballots in an election by tallying the number of ballots with the same order of ranking.

**Example 4.1.4** (Preference Table). Below is an example of a possible preference table.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Example 4.1.5.** Use the preference table for the election for Senior Class President at Clarkstown High School to answer the following questions

First	Sydney	Ava	Ava	Carley	Carley
Second	Ryan	Carley	Carley	Zaire	Sydney
Third	Ava	Ryan	Sydney	Ryan	Ava
Fourth	Carley	Zaire	Ryan	Ava	Zaire
Fifth	Zaire	Sydney	Zaire	Sydney	Ryan
Total Votes	15	29	6	24	1

- (a) How many different rankings were possible for the election?
- (b) How many students voted in the election?
- (c) Which candidate had the most first-place votes?
- (d) How many students thought that the order of candidates should be Ava, Carley, Sydney, Ryan, then Zaire?

Exercise 4.1.6. Which candidate in the preference table below had the most rankings for fifth place?

First	Sydney	Ava	Ava	Carley	Carley
Second	Ryan	Carley	Carley	Zaire	Sydney
Third	Ava	Ryan	Sydney	Ryan	Ava
Fourth	Carley	Zaire	Ryan	Ava	Zaire
Fifth	Zaire	Sydney	Zaire	Sydney	Ryan
Total Votes	15	29	6	24	1

**Definition 4.1.7.** Using the **majority rule decision** to declare a winner means that the winner is supported by a majority of the voters; that is, more than 50% of the voters rank a single candidate in first place.

**Example 4.1.8.** Use the majority rule decision to determine the winner in the election results from the preference table below.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Definition 4.1.9.** The **plurality method** states that the candidate with the most first-place votes wins

**Example 4.1.10.** Use the plurality method to determine the winner in the election results from the preference table below.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Definition 4.1.11.** The **Borda count method** assigns each ranking a specific number of points based on how many candidates are in the election.

- 1. Voters rank the candidates from most favorable to least favorable.
- 2. Candidates are awarded votes based on ranking.
  - Each last-place vote is worth 1 point.
  - Each second-from-last-place vote is worth 2 points.
  - Each third-from-last-place vote is worth 3 points.
  - Et cetera.
- 3. The candidate receiving the most points wins.

**Example 4.1.12.** Use the Borda count method to determine the winner in the election results from the preference table below.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Definition 4.1.13.** The **plurality with elimination** method requires the winner to have a majority of the votes and uses a series of eliminations, if necessary, to choose the winner.

- 1. Each voter votes for one candidate.
- 2. If a candidate receives a majority of votes, that candidate is declared the winner.
- 3. If no candidate receives a majority, eliminate the candidate with the fewest votes and hold another election. If there is a tie for the fewest votes, eliminate all the candidates tied for the fewest votes.
- 4. Repeat this process until a candidate receives a majority.

**Example 4.1.14.** Use the plurality with elimination method to determine the winner in the election results from the preference table below.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Definition 4.1.15.** The **pairwise comparison method** pairs each candidate with every other candidate for a head-to-head vote count.

- 1. Voters rank the candidates.
- 2. A series of comparison in which each candidate is compared with each of the other candidates follows.
- 3. If candidate A is preferred to candidate B, then A gets 1 point. If candidate B is preferred to candidate A, then B gets 1 point. If the candidates tie, each receives 1/2 a point.
- 4. After making all comparisons amongst the candidates, the candidate receiving the most points is declared the winner.

**Example 4.1.16.** Use the pairwise comparisons method to determine the winner in the election results from the preference table below.

First	Williams	Tremblay	Satou	Russo
Second	Satou	Satou	Williams	Williams
Third	Tremblay	Williams	Tremblay	Satou
Fourth	Russo	Russo	Russo	Tremblay
Total Votes	132	210	167	267

**Theorem 4.1.17.** The number of pairwise comparisons that must be made if there are n candidates is

$$\frac{n(n-1)}{2}.$$

### 4.2 Flaws in Voting Methods

**Definition 4.2.1.** The **Condorcet criterion** states that if a candidate wins the head-to-head comparison against every other candidate, then he should also win the overall election in a fair voting system.

**Example 4.2.2.** Three students are in an election for president of the National Society of Collegiate Scholars on campus. Members were asked to rank the three candidates. The results of the membership votes are shown in the following preference table.

First	Charles	Charles	Andrew	Bethany
Second	Bethany	Andrew	Charles	Charles
Third	Andrew	Bethany	Bethany	Andrew
Total Votes	30	31	65	21

- (a) Determine the winner if the society used the plurality method for determining the winner.
- (b) Determine the winner if the society used the pairwise comparison method to determine the winner.

(c) Does the plurality method adhere to the Condorcet criterion for this election? Explain your answer.

**Definition 4.2.3.** The **majority criterion** states that if a candidate receives a majority of the votes in an election, that candidate should win.

**Example 4.2.4.** In an election for chairman of the board of directors for a major company, shareholders were given the opportunity to rank the top five nominees. The results are summarized below.

First	H. Beridze	M. Gruber	T. Taylor	T. Taylor
Second	L. Wright	R. Jensen	H. Beridze	H. Beridze
Third	M. Gruber	H. Beridze	M. Gruber	L. Wright
Fourth	T. Taylor	T. Taylor	R. Jensen	M. Gruber
Fifth	R. Jensen	L. Wright	L. Wright	R. Jensen
Total Votes	2300	3100	4000	2200

- (a) Determine the winner of the board elections using the majority rule decision.
- (b) Determine the winner of the board elections using the Borda count method.

(c) Does the Borda count method satisfy the majority criterion for this election? Explain your answer.

**Definition 4.2.5.** The **monotonicity criterion** states that if a candidate wins an early round of an election and only gains support and does not lose support in subsequent rounds, then that candidate should win the election.

**Example 4.2.6.** The city council for the town of Whitman voted to elect a new vice president using the plurality with elimination method. All council members were asked to rank the four candidates in order of preference and the results are tallied below.

First	Clarke	Roberts	Green	Green
Second	Green	Clarke	Roberts	White
Third	Roberts	White	Clarke	Clarke
Fourth	White	Green	White	Roberts
Total Votes	6	5	4	2

Suppose that the two voters in the last column of the original preference table changed their rankings to place Clarke first in a second election.

First	Clarke	Roberts	Green	Clarke
Second	Green	Clarke	Roberts	Green
Third	Roberts	White	Clarke	White
Fourth	White	Green	White	Roberts
Total Votes	6	5	4	2

Show that the monotonicity criterion is violated.

**Definition 4.2.7.** The **irrelevant alternatives** criterion states that if a candidate wins an election, then that same candidate would win the election even if at least one candidate withdraws from the election.

**Example 4.2.8.** As part of the process of choosing the next chancellor of the university, faculty members were asked to rank the four finalists in order of preference. The votes are summarized in the table below.

First	Khan	Khan	Patel	Mason	Mason
Second	Patel	Lewis	Lewis	Lewis	Khan
Third	Mason	Patel	Mason	Khan	Lewis
Fourth	Lewis	Mason	Khan	Patel	Patel
Total Votes	166	290	235	123	236

(a) Use the pairwise comparison method to determine the favorite candidate among the faculty.

(b) Before a chancellor could be named, Patel took a job elsewhere and Lewis decided the university was not the right fit for him after visiting the campus. Consequently, Patel and Lewis withdrew their names from the application pool. Determine the faculty favorite after Patel and Lewis are removed from the ballot.

(c) Based on your solutions to parts a. and b., does this election comply with the irrelevant alternative criterion?

**Definition 4.2.9.** The **dictator criterion** states that no single vote is allowed to decide the outcome of an election.

Below is a table that summarizes how each voting method interacts with the various criteria.

	Condorcet	Majority	Monotonicity	Irrelevant	Dictator
	Criterion	Criterion	Criterion	Alterna-	Criterion
				tives	
				Criterion	
Majority	Never	Never	Never violates	Never	May violate
Rule	violates	violates		violates	
Decision					
Plurality	May violate	Never	Never violates	May violate	Never
		violates			violates
Borda	May violate	May violate	Never violates	May violate	Never
Count					violates
Plurality	May violate	Never	May violate	May violate	Never
with		violates			violates
Elimina-					
tion					
Pairwise	Never	Never	Never violates	May violate	Never
Compari-	violates	violates			violates
son					

**Theorem 4.2.10** (Arrow's Impossibility Theorem). If there are three or more choices on a ballot, there cannot be a voting method that will satisfy all five fairness criteria.

### 4.3 Apportionment

**Definition 4.3.1. Apportionment** is a method of fairly dividing resources or items among individuals or groups.

**Definition 4.3.2.** The **quota rule** states that any fair apportionment method should assign every subgroup either its lower quota or its upper quota.

**Definition 4.3.3.** The **standard divisor** for apportionment is the average number of people per item to be apportioned.

$$\mbox{Standard Divisor} = \frac{\mbox{Total Population}}{\mbox{Number of Items to Be Apportioned}}.$$

Remark 4.3.4. When computing standard divisor, we will round to four decimal places.

**Example 4.3.5.** At the beginning of each school year, the student body is given 9 delegates on the governing board. The delegates are divided among the four classes (freshmen, sophomores, juniors, seniors) according to the student population given in the table below. Calculate the standard divisor that will be used to assign the delegates.

Freshmen	Sophomores	Juniors	Seniors
224	267	135	169

Exercise 4.3.6. A local council has 12 seats. If there are 301,500 people in the district, determine the standard divisor that would be used to apportion the seats.

**Definition 4.3.7.** The **standard quota** for apportionment is the average number of items to be apportioned to each subgroup.

$$\label{eq:Standard Quota} Standard \ Quota = \frac{Subgroup \ population}{Standard \ Divisor}.$$

Remark 4.3.8. When computing standard quota, we will round to four decimal places.

**Example 4.3.9.** At the beginning of each school year, the student body is given 9 delegates on the governing board. The delegates are divided among the four classes (freshmen, sophomores, juniors, seniors) according to the student population given in the table below. Calculate the standard quota of representatives for each class.

Freshmen	Sophomores	Juniors	Seniors
224	267	135	169

Exercise 4.3.10. Three classes have student populations of 87, 52, and 89, respectively. Determine the standard quota for each class given that the standard divisor is 13.4.

119

#### Definition 4.3.11. Hamilton's method of apportionment

- 1. Calculate the standard divisor.
- 2. Calculate the standard quota for each subgroup.
- 3. Calculate the lower quota for each subgroup.
- 4. Assign each subgroup the number of resources based on its lower quota.
- 5. Assign any remaining resources based on the fractional remainder of the standard quotas, in order from largest to smallest.

**Example 4.3.12.** A new suburb of Chicago is seeking a charter to become a city of its own. The suburb will have 25 council members divided among six zones. Use Hamilton's method to determine how the council members will be apportioned between the six zones. The populations for each zone are given in the table below.

Zone	Population
1	2897
2	4538
3	3362
4	14,003
5	8450
6	12,339

### Definition 4.3.13. Jefferson's Method of Apportionment

- 1. Calculate the standard divisor.
- 2. Calculate the standard quota for each subgroup.
- 3. Calculate the lower quota for each subgroup.
- 4. Assign each subgroup the number of resources based on its lower quota.
- 5. If there are remaining resources to be distributed, chose a modified divisor by trial and error until the sum of the lower quotas equals the number of resources to be apportioned.

**Example 4.3.14.** A university has 18 scholarships to be apportioned among 225 math majors, 417 history majors, and 308 computer science majors. Use Jefferson's method to determine how the scholarships should be apportioned among the three major groups.

121

Exercise 4.3.15. Use Hamilton's method to apportion the scholarships in Example 4.3.14.

#### Definition 4.3.16. Webster's Method of Apportionment

- 1. Calculate the standard divisor.
- 2. Calculate the standard quota for each subgroup.
- 3. Round each quota to the nearest integer.
- 4. Assign each subgroup the number of resources based on the rounded quota.
- 5. If there are remaining resources to be distributed, chose a modified divisor by trial and error until the sum of the rounded quotas equals the number of resources to be apportioned.

**Example 4.3.17.** A computer tech firm has three divisions with 135, 98, and 132 employees, respectively. A total of 11 administrative assistants must be allocated to the three divisions according to their size. Use Webster's method to determine how many administrative assistants should be allocated to each division.

123

Exercise 4.3.18. Use Hamilton's method to apportion the administrative assistants in Example 4.3.17.

**Definition 4.3.19.** The **geometric mean** of any two numbers m and n is  $\sqrt{mn}$ .

#### Definition 4.3.20. The Huntington-Hill Method of Apportionment

- 1. Calculate the standard divisor.
- 2. Calculate the standard quota for each subgroup.
- 3. Calculate the geometric mean of the standard quota for each subgroup.
- 4. If the standard quota is less than the geometric mean, round the quota down. If the standard quota is greater than the geometric mean, round the quota up.
- 5. Assign each subgroup the number of resources based on the rounded quota.
- 6. If there are remaining resources to be distributed, chose a modified divisor by trial and error until the sum of the rounded quotas equals the number of resources to be apportioned.

**Example 4.3.21.** After a census, 100 seats in parliament need to be re-apportioned among 5 counties with the following populations. Use the Huntington-Hill method to apportion the seats.

County	Population
1	35,589
2	17,425
3	3658
4	11,457
5	6871
Total	75,000

125

Exercise 4.3.22. Use Hamilton's method to apportion the seats in Example 4.3.21.

**Definition 4.3.23.** The **Alabama paradox** occurs when an increase in the number of items to be apportioned causes a subgroup to lose an item.

**Example 4.3.24.** Due to growth in student population, a school district was given money to hire 10 new middle school teachers for their three middle schools: Brown Middle School, Peachtree Middle School, and MLK Middle School. The teachers will be assigned to the schools based on their student populations using Hamilton's method of apportionment. The student populations are shown below.

Middle School	Student Population
Brown Middle	203
Peachtree Middle	588
MLK Middle	600
Total	1391

(a) Use the Hamilton method to apportion the 10 teachers.

(b) Show that the Alabama paradox occurs if the district is able to hire 11 teachers instead of 10.

**Definition 4.3.25.** The **population paradox** occurs when subgroup A loses an item to subgroup B when the rate of growth of the population of subgroup A is greater than the rate of the growth in subgroup B.

**Example 4.3.26.** Parish council representatives are to be distributed among the parishes they represent according to population. The table below shows the current apportionment of the 17 representatives along with the population growth that has occurred since the last apportionment.

Parish	Former	Apportionment	Percent	Current
	Population		Increase	Population
Eddy	13,877	7	0.8%	13,988
Longly	5080	2	12.7%	5725
Martyn	8109	3	3.0%	8352
Meeds	7592	4	9.0%	8275
Viant	1100	1	17.5%	1293
Total	35,758	17		37,633

Use Hamilton's method to reapportion the 17 representatives with the new populations, showing that the population paradox occurs.

**Definition 4.3.27.** The **new states paradox** occurs when the addition of a new subgroup, with a corresponding increase in the number of available items, can cause a change in the apportionment of items among the other subgroups.

**Example 4.3.28.** A college campus has a student leadership board consisting of 13 representatives from the 3 different branches of student life: academic, social, and service. The members of the board are apportioned based on the student enrollment in the organizations of each of the different branches. The calculations using the Hamilton method, with a standard divisor of 894.7692, are shown in the table below.

Student	Population	Standard	Lower	Apportionment
Life Branch		Quota	Quota	
Academic	3106	3.4713	3	4
Social	5649	6.3134	6	6
Service	2877	3.2154	3	3
Total	11,632			13

The student population has voted to add representation for pre-professional organizations to the leadership board. The standard divisor is 894.7692, which means that there should be 1 representative for every 894.7692, students in pre-professional organizations. Since the new branch has 1363 students, we find  $1363/894.7692 \approx 1.5233$ , and round that down to 1 so that this new branch adds one representative to the board. Show that the new states paradox occurs with this addition.

# Chapter 5

# Number Theory

### 5.1 Prime Numbers

**Definition 5.1.1.** An integer m is a **divisor** or **factor** of another integer n if m divides n with a remainder of zero. That is to say, there exists another integer k such that n = km.

**Example 5.1.2.** The integer 3 is a divisor of the integer -6 because -6 = (-2)3.

**Definition 5.1.3.** A **prime number** is a positive integer that has precisely two divisors: 1 and itself.

**Example 5.1.4.** The integer 3 is a prime number because its only factors are 1 and 3.

**Definition 5.1.5.** A **composite number** is a positive integer that has more than two divisors.

Remark 5.1.6. By convention, the numbers 0 and 1 are neither prime nor composite.

**Example 5.1.7.** The integer 6 is composite because its factors are 1, 2, 3, and 6.

**Process 5.1.8** (Sieve of Eratosthenes). To find all of the prime numbers between 2 and some integer N, perform the following steps.

- 1. List all the positive integers between 2 and N.
- 2. Highlight the smallest number p not crossed out or previously highlighted. This is a prime number.
- 3. Cross out all multiples of p.
- 4. Repeat steps 2 and 3 until all numbers are either highlighted or crossed out.

**Example 5.1.9.** Find all of the prime numbers less than 100.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

	Divisibility R	ules
Divisor	Test	Example
2	The last digit is 0, 2, 4, 6, or 8.	The number 391,574 is divisible by 2
		because the last digit is 4.
3	When the digits of the number are	87408 is divisible by 3 because $8+7+$
	added together, the resulting number	$4+0+8=27 \text{ and } 27=3\times9.$
	is divisible by 3.	
4	The last 2 digits of the number form	316 is divisible by 4 because $16 = 1$
	a number divisible by 4	$4 \times 4$ .
5	The number ends in a 0 or a 5.	23,345 is divisible by 5 because it
		ends in a 5.
6	The number is divisible by both 2	628,116 is divisible by 2 because the
	and 3.	last digit is 6 and divisible by 3 be-
		cause $6 + 2 + 8 + 1 + 1 + 6 = 24$ and
		$24 = 3 \times 8$ . Therefore 628, 116 is di-
		visible by 6
7	Double the last digit, then subtract	819 is divisible by 7 since $2 \times 9 = 18$ ,
	it from the remaining digits of the	$81 - 18 = 63$ , and $63 = 7 \times 9$ .
	number. If the answer is divisible by	
	7, then so is the original number.	
8	The last 3 digits of the number form	2160 is divisible by 8 because 160 =
	a number divisible by 8.	8 × 20
9	When the digits of the number are	189 is divisible by 9 because $1 + 8 +$
	added together, the resulting number	$9 = 18 \text{ and } 18 = 9 \times 2.$
10	is divisible by 9.	
10	The number ends in a 0.	9,145,830 is divisible by 10 because it
		ends in a 0.

**Example 5.1.10.** Determine if the following numbers are prime or composite using the divisibility rules.

(a) 312

(b) 101

(c) 2,344,017

Exercise 5.1.11. Determine if 3,743,216 is prime or composite.

133

**Theorem 5.1.12** (The Fundamental Theorem of Arithmetic). Every positive integer greater than 1 is either a prime number or can be written as a unique product of prime numbers.

**Definition 5.1.13.** The unique product of prime numbers from the Fundamental Theorem of Arithmetic is called its **prime factorization**.

**Example 5.1.14.** Use a factor tree to determine the prime factorization of the number 84.

Remark 5.1.15. Different choices for factor trees may result in different branches, but the prime factorization on the bottom row of factors will always be the same.

Exercise 5.1.16. Write down a factor tree for the number 84 that makes a different first choice and verify that the outcome is the same.

**Theorem 5.1.17.** If n is a composite integer, then there exists a prime number that divides n and is less than or equal to  $\sqrt{n}$ .

**Example 5.1.18.** Use Theorem 5.1.17 to determine whether 197 is prime or composite.

**Definition 5.1.19.** The largest integer that divides two integers m and n without a remainder is called the **greatest common divisor**, gcd(m, n).

**Definition 5.1.20.** If gcd(m, n) = 1, then we say m and n are relatively prime.

**Example 5.1.21.** Use factor trees to find the greatest common divisor of 40 and 60.

**Example 5.1.22.** One way that the Manna Café Pantry serves the hungry of Clarksville, TN, is by distributing boxes of food each week to the local shelters. As part of the stipulation for receiving local governmental funds, all boxes must contain the same number of items from each of the following categories: pasta, canned vegetable, and canned meat. This week, the pantry has the following in supply: 360 pasta items, 540 canned vegetables, and 240 canned meats.

(a) Using all of the food, what is the maximum number of food boxes that the Manna Café Pantry can distribute this week?

(b) How many of each item will be in each box?

**Process 5.1.23** (Euclid's Algorithm). To find the greatest common divisor of two integers, follow these steps.

- 1. Divide the larger of the given numbers by the smaller (the divisor) and note the remainder.
- 2. Divide the original divisor (the smaller of the given numbers) by the remainder found in Step 1.
- 3. Continue dividing the previous divisor by the previous remainder until the remainder is 0.
- 4. The last nonzero remainder is the greatest common divisor of the given numbers.

**Example 5.1.24.** Use the Euclidean Algorithm to find the greatest common divisor of 88 and 300.

137

Exercise 5.1.25. Two college classes, one with 88 students and one with 17, need to be split into smaller groups of equal sizes. Use the Euclidean Algorithm to determine what size the smaller groups could be, if it is possible.

# 5.2 Modular Arithmetic

**Definition 5.2.1.** Fix a positive integer m, called the **modulus**. We say n is **congruent** to r **modulo** m and write  $n \equiv r \pmod{m}$  if r is the remainder when n is divided by m.

Example 5.2.2. Complete the following table.

Remainders Modulo 5					
n	r	$n \equiv r \pmod{5}$			
0	0	$0 \equiv 0 \pmod{5}$			
1	1				
2	2				
3	3				
4	4				
5	0				
6					
7					
8					
9					
10					

Exercise 5.2.3 ((a)). Evaluate the following.

1.  $15 \pmod{6}$ 

2. 72 (mod 13)

3.  $(12+7) \pmod{5}$ 

4.  $(21-18) \pmod{6}$ 

5.  $(35 \times 22) \pmod{10}$ 

6.  $(10 \pmod{4}) + (17 \pmod{4})$ 

7.  $(10+17) \pmod{4}$ 

Application 5.2.4. The International Standard Book Number (ISBN) is a unique string of numbers that conveys such information as the publisher and country of origin



Process 5.2.5. To find the Check-Sum Digit for a 10-digit ISBN

- 1. Multiply the first digit by 10.
- 2. Multiply the second digit by 9.
- 3. Multiply the third digit by 8.
- 4. Multiply the fourth digit by 7.
- 5. Multiply the fifth digit by 6.
- 6. Multiply the sixth digit by 5.

- 7. Multiply the seventh digit by 4.
- 8. Multiply the eighth digit by 3.
- 9. Multiply the ninth digit by 2.
- 10. Add the multiples together.
- 11. The check-sum digit is chosen so that the total of the products and the check-sum digit is 0 modulo 11.

**Example 5.2.6.** Verify the validity of the ISBN below by checking the check-sum digit is 10 (represented by X).



Exercise 5.2.7. Use the check-sum digit to determine the third number in the ISBN below.



# 5.3 Fermat's Little Theorem and Prime Testing

**Theorem 5.3.1** (Fermat's Little Theorem). Let p be any prime number and x be any positive integer. Then,

$$x^p - x \equiv 0 \pmod{p}.$$

**Exercise 5.3.2.** Verify that  $x^p - x \equiv 0 \pmod{p}$  when p = 7 and x = 4.

**Exercise 5.3.3.** Verify that  $x^p - x \equiv 0 \pmod{p}$  when p = 11 and x = 10.

**Theorem 5.3.4** (Contrapositive of Fermat's Little Theorem). Let x and n be positive integers. If  $x^n - x \not\equiv 0 \pmod{n}$ , then n is **not** a prime number.

**Exercise 5.3.5.** Verify that n = 8 is not a prime number using the contrapositive of Fermat's Little Theorem with x = 2.

**Exercise 5.3.6.** Verify that 39 is not a prime number using the contrapositive of Fermat's Little Theorem with x = 2.

# 5.4 Fermat's Little Theorem and Public-Key Encryption

**Theorem 5.4.1** (Euler's Theorem). Let p and q be prime numbers and n = pq. If x and a are any positive integers, then

$$x^{a(p-1)(q-1)+1} - x \equiv 0 \pmod{n}$$
.

**Exercise 5.4.2.** Verify Euler's Theorem with the numbers p = 3, q = 5, x = 2, and a = 1.

**Exercise 5.4.3.** Verify Euler's Theorem with the numbers p = 2, q = 3, x = 2, and a = 1.

**Application 5.4.4** (RSA Encryption). The RSA cryptosystem is a type of Public-Key Encryption that is commonly used to transmit information securely.

1. Choose two (large) prime numbers p and q and compute

$$\lambda = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

Keep these numbers **secret**.

2. Compute n = pq and choose and an integer

$$2 < e < \lambda$$

that is relatively prime to  $\lambda$ , called the **encryption key**. The numbers n and e are form the **public key** that can be shared with anyone who would like to send you a secure message.

3. Find an integer d that satisfies

$$ed \equiv 1 \pmod{\lambda}$$
.

The number d is the **decryption key**. Keep this number **secret**.

4. The sender encrypts their plaintext message, m, by computing the ciphertext

$$c = m^e \pmod{n}$$
.

5. The recipient decodes the ciphertext by computing

$$m = c^d \pmod{n}$$
.

**Example 5.4.5.** Let m=2 be a secret number. Encode m using the public key n=115 and e=17.

**Example 5.4.6.** Decode the ciphertext M = 87 using the private key d = 13 and n = 115.

**Example 5.4.7.** The ideas from the previous two examples can be extended to implement a version of RSA that can transmit actual text using the American Standard Code for Information Interchange (ASCII), that assigns a number to each character in the English language.

ASCII Table					
Character	Integer	Character	Integer		
Space	32				
A	65	a	97		
В	66	b	98		
С	67	С	99		
D	68	d	100		
Е	69	е	101		
F	70	f	102		
G	71	g	103		
Н	72	h	104		
I	73	i	105		
J	74	j	106		
K	75	k	107		
L	76	1	108		
M	77	m	109		
N	78	n	110		
O	79	0	111		
P	80	p	112		
Q	81	q	113		
R	82	r	114		
S	83	S	115		
T	84	t	116		
U	85	u	117		
V	86	V	118		
W	87	W	119		
X	88	X	120		
Y	89	у	121		
Z	90	Z	122		

Suppose Alice and Bob are spies who need to send private messages, but the evil Eve is eavesdropping on their conversations. To thwart Eve, Alice chooses the two prime numbers p=7 and q=23, then computes the modulus n=161 and

$$\lambda = \frac{6 \times 22}{\gcd(6, 22)} = \frac{6 \times 22}{2} = 3 \times 22 = 66.$$

Next, Alice chooses the encryption key e = 17 and checks that

$$17 \times 35 = 595 = 594 + 1 = 66 \times 9 + 1$$

or, equivalently,  $17 \times 35 \equiv 1 \pmod{66}$ . This tells Alice that her decryption key is d = 35. Alice sends the numbers n = 161 and e = 17 to Bob, and tells him to use this public key to encrypt his messages using strings of numbers called the plaintext.

Bob has previous orders to stake out a cafe and transmit the message "The eagle has landed" to Alice upon arrival of an adversary. Not wanting to tip off Eve, Bob first uses the ASCII table to translate this message into the sequence of numbers

```
84, 104, 101, 32, 101, 97, 103, 108, 101, 32, 104, 97, 115, 32, 108, 97, 110, 100, 101, 100.
```

Bob raises each number to the power e = 17 modulo n = 161 and obtains the list

```
84^{17} \equiv 56 \pmod{161}, \ 104^{17} \equiv 55 \pmod{161}, \ 101^{17} \equiv 26 \pmod{161}, \\ 32^{17} \equiv 72 \pmod{161}, \ 101^{17} \equiv 26 \pmod{161}, \ 97^{17} \equiv 153 \pmod{161}, \\ 103^{17} \equiv 129 \pmod{161}, \ 108^{17} \equiv 96 \pmod{161}, \ 101^{17} \equiv 26 \pmod{161}, \\ 32^{17} \equiv 72 \pmod{161}, \ 104^{17} \equiv 55 \pmod{161}, \ 97^{17} \equiv 153 \pmod{161}, \\ 115^{17} \equiv 138 \pmod{161}, \ 32^{17} \equiv 72 \pmod{161}, \ 108^{17} \equiv 96 \pmod{161}, \\ 97^{17} \equiv 153 \pmod{161}, \ 110^{17} \equiv 31 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 26 \pmod{161}, \ 100^{17} \equiv 151 \pmod{161}, \\ 101^{17} \equiv 151 \pmod{161
```

that represents the ciphertext. Bob transmits the string of numbers

```
56, 55, 26, 72, 26, 153, 129, 96, 26, 72, 55, 153, 138, 72, 96, 153, 31, 151, 26, 151
```

to Alice, safe in the knowledge that Eve won't be able to understand the message because she does not possess the decryption key. Indeed, if Eve tried to convert this string to characters using the ASCII table she would get the nonsense message

### 

When Alice receives the message, she raises each of the numbers to the power d=35 modulo n=161 to obtain the sequence of numbers

```
 56^{35} \equiv 84 \pmod{161}, \ 55^{35} \equiv 104 \pmod{161}, \ 26^{35} \equiv 101 \pmod{161}, 
 72^{35} \equiv 32 \pmod{161}, \ 26^{35} \equiv 101 \pmod{161}, \ 153^{35} \equiv 97 \pmod{161}, 
 129^{35} \equiv 103 \pmod{161}, \ 96^{35} \equiv 108 \pmod{161}, \ 26^{35} \equiv 101 \pmod{161}, 
 72^{35} \equiv 32 \pmod{161}, \ 55^{35} \equiv 104 \pmod{161}, \ 153^{35} \equiv 97 \pmod{161}, 
 138^{35} \equiv 115 \pmod{161}, \ 72^{35} \equiv 32 \pmod{161}, \ 96^{35} \equiv 108 \pmod{161}, 
 153^{35} \equiv 97 \pmod{161}, \ 31^{35} \equiv 110 \pmod{161}, \ 151^{35} \equiv 100 \pmod{161}, 
 26^{35} \equiv 101 \pmod{161}, \ 151^{35} \equiv 100 \pmod{161}.
```

Finally, Alice uses the ASCII table to decode this sequence of numbers to the sequence of characters

that represent the secret message "The eagle has landed" transmitted by Bob.

# **Bibliography**

- [Cen20] Centers for Disease Control, *Food allergies*, https://www.cdc.gov/healthyschools/foodallergies/index.htm, June 8, 2020.
- [hun14] The hunger games: Catching fire, 2014.
- [Jac19] Chris Jackson, More americans have tattoos today than seven years ago, https://www.ipsos.com/en-us/news-polls/more-americans-have-tattoos-today, August 29, 2019.