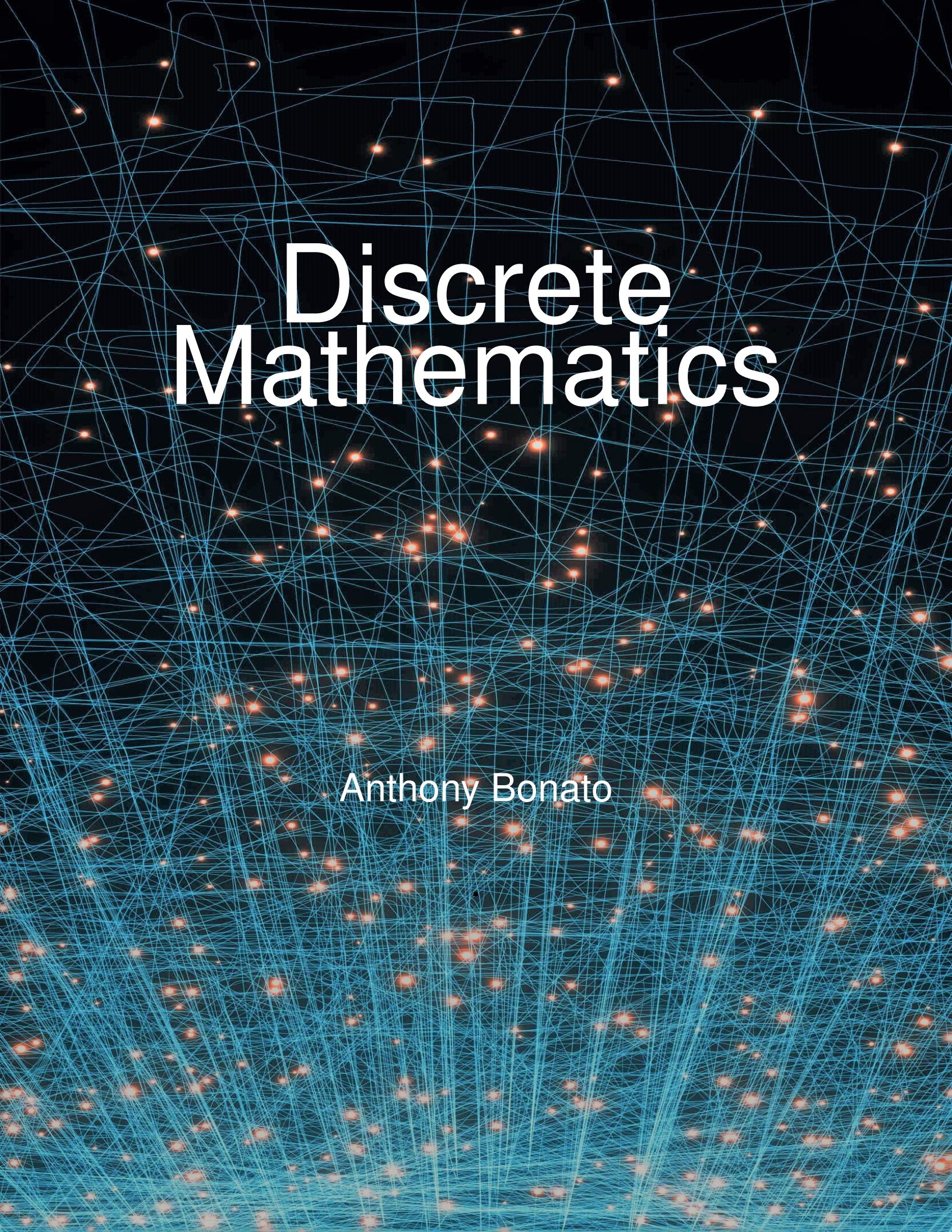

Discrete
Mathematics
Anthony Bonato

ISBN 978-1-77136-997-8

Cover design by Anthony Bonato

Published by Anthony Bonato

Table of contents

1 Sets and Logic 7

1.1 Introduction 7

1.2 Sets 7

1.3 Operations on Sets 10

1.4 Countable and Uncountable Sets 16

1.5 Logic 18

1.6 Exercises 23

1.7 Selected Answers and Hints 28

2 Graphs and Trees 30

2.1 Introduction to Graphs 30

2.2 Degrees 33

2.3 Subgraphs and Connected Graphs 34

2.4 Trees 39

2.5 Coloring and Domination 41

2.6 Directed Graphs 44

2.7 Exercises 46

2.8 Selected Answers and Hints 52

3 Relations and Functions 54

3.1 Introduction to Relations 54

3.2 Properties of Relations 56

3.3 Partial Orders 59

3.4 Functions 62
3.5 Exercises 65
3.6 Selected Answers and Hints 69

4 Combinatorics 71
4.1 Introduction 71
4.2 Sum Rule 71
4.3 Product Rule 74
4.4 The Pigeonhole Principle 75
4.5 Permutations 77
4.6 Combinations 77
4.7 Pascal's Triangle 81
4.8 Sequences 82
4.9 Exercises 85
4.10 Selected Answers and Hints 89

5 Number Theory 91
5.1 Introduction to Number Theory 91
5.2 Divisors 93
5.3 The Euclidean Algorithm 96
5.4 Linear Diophantine Equations 98
5.5 Congruences 100
5.6 Exercises 103
5.7 Selected Answers and Hints 108

6 Induction 110
6.1 Introducing Induction 110
6.2 Examples of induction 112
6.3 Strong induction 116
6.4 Recurrence relations 119
6.5 Exercises 122

Preface

Discrete mathematics focuses at its core on objects that can be separated and studied individually, in contrast to continuous objects such as functions or spaces in calculus or geometry. These objects may be graphs, sets, or numbers. The tools and techniques of discrete mathematics are distinct from those of other fields of mathematics, and often take on a *combinatorial* flavor, where we focus on counting objects.

The focus of the present book is to give an introduction to each of the topics of sets and logics, graphs, relations, functions, combinatorics, and number theory. Sets underlie all of modern mathematics, while logic is a kind of grammar that allows us to talk meaningfully about mathematical concepts. Graphs measure interactions between objects, from friendship links on Twitter, to transactions between Bitcoin users, and to the flow of energy in a food chain. Graph theory is a robust topic within mathematics, and sets out to formalize the science of interactions. Equivalence relations come up all over mathematics, and partial orders give us a method to compare and rank objects. Functions appear in all of mathematics, from calculus to linear algebra, to more advance topics. Counting or combinatorics is the science and art of counting objects, and is used in nearly all branches of mathematics. Number theory focuses on the structure and properties of the natural numbers, with a special emphasis on prime numbers and divisors. Number theory is the foundation for security applications in banking, internet security, and cryptocurrency. Induction is a fundamental tool in discrete mathematics for proving various statements about the natural numbers.

The topics of the book may be covered in a one semester course, taken in sequence from sets and logic through to number theory. The chapters may be read independently, although a grasp of Chapter 1 on sets and logic is important to everything that follows.

The book contains 180 exercises ranging in difficulty from easier to more challenging. Solutions are included at the end of each chapter for almost all the exercises. In some cases, only hints towards the solutions are provided. There are dozens of examples and figures that will aid in the comprehension of the material.

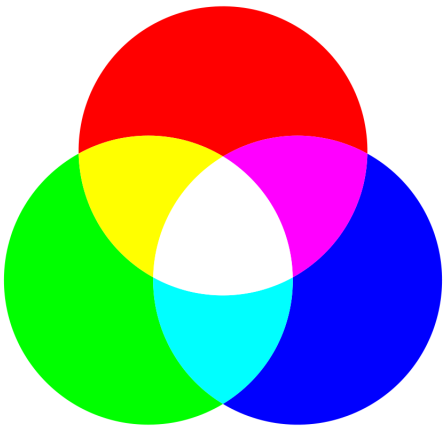
I wrote this book to make the topics of elementary discrete mathematics clear and succinct, without distracting the reader's time on unnecessary material such as history or random applications. As someone who's worked in discrete mathematics for over twenty years, the material in this book, if mastered, will give you all the tools you need to study any application of the topic in either mathematics, science, or engineering.

The book is available as an electronic pdf through Gumroad at a very competitive price. The book is sold at cost, and I would kindly ask you not to duplicate, share, or post it.

Finally, a big thank you to the readers of the book, present and future. I hope it will help successfully guide you through an introduction to the fascinating and beautiful world of discrete mathematics.

Chapter 1

Sets and Logic



1.1 Introduction

Sets are basic to all of mathematics, and they give us a language to state any mathematical definition or theorem. Our goal for studying sets will be to give a foundation for all the topics covered in the remainder of the book.

Logic is another foundational topic, underpinning every proof, method, or argument in mathematics. For that reason, we give a brief introduction to logic, including propositional logic and the logic of quantifiers.

1.2 Sets

A *set* is a collection of objects. This is a very general notion that applies to most (or arguably all) concepts in mathematics. We avoid the formal foundations of set theory and focus instead on properties and operations on sets. The objects within a set are called *elements*. We will typically use capital letters such as X and Y to represent sets. If X is a set and u is an element of X, then we write $u \in X$.

We may list the elements in a set using curly brackets { and }.

Example 1.1 The set consisting of the integers 1, 2, and 3 is $\{1, 2, 3\}$.

A typical way to represent the elements of a set is to describe them using set-builder notation. If P is some property of mathematics, then we write

$$\{u : u \text{ has property } P\}.$$

For example, we could consider

$$\{x : x \text{ is an integer}\},$$

which is the set of all integers. An important set is the one with no elements, called the *empty set*, written $\varnothing$.

Definition 1.1 The number of elements of the set X, written $|X|$, is its *cardinality*.

From the definition, $|\{1,2,3\}| = 3$. Also, $|\varnothing| = 0$.

Definition 1.2

1. Given sets X and Y, we say X is a *subset* of Y if every element of X is also an element of Y. We write $X \subseteq Y$, and refer to the symbol $\subseteq$ as *inclusion*.
2. If there is an element of Y that is not an element of X, we say that X is a *proper subset* of Y, written $X \subsetneq Y$. Note that if $X \subsetneq Y$, then we also have that $X \subseteq Y$.

Example 1.2 The set

$$\{1,3,4\} \subseteq \{1,2,3,4\},$$

and it is also the case that

$$\{1,3,4\} \subsetneq \{1,2,3,4\}.$$

Definition 1.3 We say that two sets X and Y are *equal* if X and Y share the exact same elements.

Note that the equality of sets is equivalent to $X \subseteq Y$ and $Y \subseteq X$. Further, if $X = Y$, then $|X| = |Y|$.

Example 1.3 The sets $\{1,1,2\}$ and $\{2,1\}$ are equal as they have the same elements. In general, if an element of a set is repeated, we can remove extra copies of it and the set is unchanged.

The following transitive property of inclusion is simple but important.

Theorem 1.1 **(Transitivity of inclusion)**: Let X, Y, and Z be sets. If $X \subseteq Y$, and $Y \subseteq Z$, then $X \subseteq Z$.

Proof. Let u be an element of X. Since $X \subseteq Y$, u is an element of Y. As $Y \subseteq Z$, then u is an element of Z. As u was arbitrary, we have that $X \subseteq Z$. □

Sometimes when discussing sets, it is convenient to specify a larger set containing them, which we refer to as the *universe*, written U. The elements of U will depend on the context in which it is discussed.

Venn diagrams are a useful way to represent interactions between sets, including the operations defined above. These are two or more circles or other shapes that overlap and may

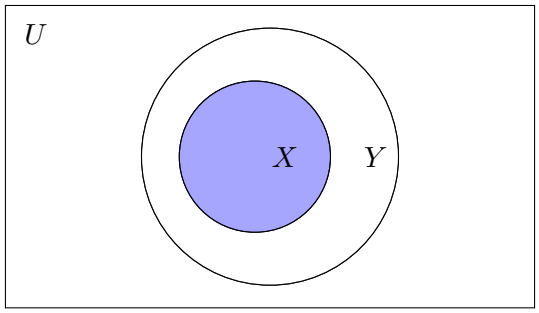


Figure 1.1: Sets $X \subseteq Y$ in the universe U. The set X is shaded.

be shaded to emphasize certain relations between sets. Elements may or may not be listed in the shapes. See Figure 1.1 for an example of a Venn diagram.

Definition 1.4

1. Sets with a single element are called *singletons*. These are written $\{u\}$, where u is the sole element of the set.
2. In the case that the set has two elements, we refer to this as a *doubleton* or *unordered pair*, and write $\{u, v\}$. Note that the order of the elements in an unordered pair does not matter, so $\{u, v\} = \{v, u\}$.
3. If the order does matter, then we have an *ordered pair*, written (u, v). Note that $(u, v) \neq (v, u)$.

Example 1.4 The set $\{1, 2\}$ is a doubleton, while $\{1\}$ is a singleton. The set $(5, 7)$ is an ordered pair.

Definition 1.5 A set is *finite* if it is empty or its elements can be listed as

$$\{u_1, u_2, \ldots, u_n\}$$

for a positive integer n. The set is infinite, otherwise.

Number systems form common examples of infinite sets. A few of the most important such number systems are in the following example.

Example 1.5

1. The set of natural numbers, written

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Note that in our definition, $\mathbb{N}$ contains 0 but there is no universal consensus on this point. We write $\mathbb{N}^+$ for the positive natural numbers.

2. The set of integers, written

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}.$$

3. The set of rational numbers, written $\mathbb{Q}$, which are of the form p/q, where p and q are integers with $q \neq 0$.

4. The set of real numbers, written $\mathbb{R}$, which are numbers with a decimal expansion.

Note that

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R},$$

and each of these are proper subsets.

1.3 Operations on Sets

We may put sets together using several operations.

Definition 1.6 Let X and Y be sets in a universe U.

1. The *intersection* of X and Y, written $X \cap Y$, is the set consisting of elements in both X and Y. We write

$$X \cap Y = \{u \in U : u \in X \text{ and } u \in Y\}.$$

2. The *union* of X and Y, written $X \cup Y$, is the set consisting of elements in X or Y. We write

$$X \cup Y = \{u \in U : u \in X \text{ or } u \in Y\}.$$

3. The *difference* of X with Y, written $X \setminus Y$, is the set consisting of elements in X but not in Y. We write

$$X \setminus Y = \{u \in U : u \in X \text{ and } u \notin Y\}.$$

4. The *complement* of X, written X^c, is the set of elements of U not in X. We write

$$X^c = \{u \in U : u \notin X\}.$$

There are other, operations we may also define.

Definition 1.7 Let X and Y be sets. The *symmetric difference* of X and Y, written $X \triangle Y$, is the set

$$(X \setminus Y) \cup (Y \setminus X).$$

Example 1.6 Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $X = \{2, 5, 7\}$ and $Y = \{1, 2, 4, 6, 7\}$. We then have the following.

1. $X \cup Y = \{1, 2, 4, 5, 6, 7\}$.
2. $X \cap Y = \{2, 7\}$.
3. $X^c = \{1, 3, 4, 6, 8, 9\}$ and $Y^c = \{3, 5, 8, 9\}$.
4. $X \setminus Y = \{5\}$ and $Y \setminus X = \{1, 4, 6\}$.
5. $X \triangle Y = \{1, 4, 5, 6\}$.

Definition 1.8 We say that X and Y are *disjoint* if $X \cap Y = \varnothing$. Sets $X_1, X_2, \ldots, X_n$ are *mutually* (or *pairwise*) *disjoint* if for all distinct i and j in $\{1, 2, \ldots, n\}$, we have that X_i and X_j are disjoint.

Example 1.7 The set $\{1, 2\}$ is disjoint from $\{3, 4\}$. The sets $\{1, 2\}$, $\{3, 4\}$, $\{7, 8\}$ are mutually disjoint.

We represent the set operations of intersection, union, and difference by Venn diagrams.

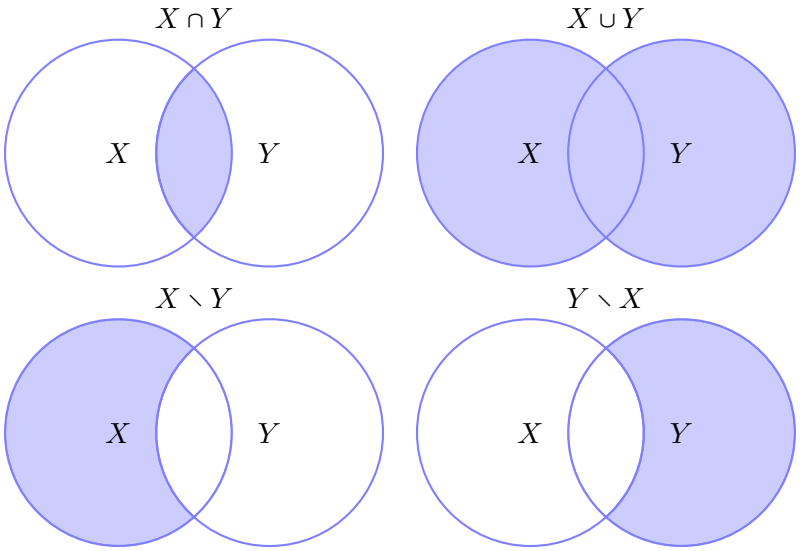


Figure 1.2: Venn diagrams of the sets $X \cap Y$, $X \cup Y$, $X \setminus Y$, and $Y \setminus X$.

We collect the main properties of sets in the following. We give a few of the proofs here and save others for the exercises; other properties not mentioned here are also discussed in the exercises. In each of the proofs, we use the *element method*, where we show the left side and right side share the same elements.

Theorem 1.2 (Laws of set operations) Let X, Y, and Z be sets contained in a universe U.

1. Complement laws:
$$X \cup X^c = U \quad \text{and} \quad X \cap X^c = \varnothing.$$
2. Identity laws:
$$X \cup \varnothing = X \quad \text{and} \quad X \cap U = X.$$
$$X \cap \varnothing = \varnothing \quad \text{and} \quad X \cup U = U.$$
3. Idempotent laws:
$$X \cup X = X \quad \text{and} \quad X \cap X = X.$$
4. Double complement laws:
$$(X^c)^c = X.$$
5. Commutative laws:
$$X \cup Y = Y \cup X \quad \text{and} \quad X \cap Y = Y \cap X.$$

6. Associative laws:

$$(X \cup Y) \cup Z = X \cup (Y \cup Z) \quad \text{and} \quad (X \cap Y) \cap Z = X \cap (Y \cap Z).$$

7. Distributive laws:

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \quad \text{and} \quad X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

8. DeMorgan's laws:

$$(X \cup Y)^c = X^c \cap Y^c \quad \text{and} \quad (X \cap Y)^c = X^c \cup Y^c.$$

9. Set difference law:

$$X \setminus Y = X \cap Y^c.$$

Proof. We give the proofs of (4) and (8).

For item (4), let $u \in (X^c)^c$. We then have that $u \notin X^c$, and so $u \in X$. Thus, $(X^c)^c \subseteq X$. Now let $u \in X$, and so $u \notin X^c$. It follows that $u \in (X^c)^c$. (Do you see why?) Hence, $X \subseteq (X^c)^c$, and so we have equality.

For item (8), we only prove the first identity: $(X \cup Y)^c = X^c \cap Y^c$. For this, let $u \in (X \cup Y)^c$. We then have that $u \notin X \cup Y$. Thus, $u \notin X$ and $u \notin Y$, so $u \in X^c \cap Y^c$, and so $(X \cup Y)^c \subseteq X^c \cap Y^c$. Now let $u \in X^c \cap Y^c$. We then have that $u \in X^c$ and $u \in Y^c$, and so u is not in $X \cup Y$. Hence, $u \in (X \cup Y)^c$ and so $X^c \cap Y^c \subseteq (X \cup Y)^c$. The identity follows. □

Example 1.8 Let X, Y be sets. We use the laws of set operations to show that

$$X \cap ((Y \cup X^c) \cap Y^c) = \varnothing.$$

To see this, we note that

$$\begin{aligned} X \cap ((Y \cup X^c) \cap Y^c) &= ((Y \cup X^c) \cap Y^c) \cap X \text{ (Commutative law)} \\ &= (Y \cup X^c) \cap (Y^c \cap X) \text{ (Associative law)} \\ &= (Y \cap Y^c \cap X) \cup (X^c \cap Y^c \cap X) \text{ (Distributive law)} \\ &= (Y \cap Y^c \cap X) \cup (X^c \cap X \cap Y^c) \text{ (Commutative law)} \\ &= (\varnothing \cap X) \cup (\varnothing \cap Y^c) \text{ (Complement law)} \\ &= \varnothing \cup \varnothing \text{ (Identity law)} \\ &= \varnothing \text{ (Idempotent law).} \end{aligned}$$

We may generalize the operations of union and intersection in the following ways.

Definition 1.9 Let X_i be sets in universe U, where $i \geq 1$ is an integer. We define

$$\bigcup_{i=1}^{n} X_i = \{x \in U : x \in X_i \text{ for some } i, \text{where } 1 \leq i \leq n\},$$

$$\bigcap_{i=1}^{n} X_i = \{x \in U : x \in X_i \text{ for all } i, \text{where } 1 \leq i \leq n\}.$$

These definitions also generalize to infinite unions and intersections:

$$\bigcup_{i=1}^{\infty} X_i = \{x \in U : x \in X_i \text{ for some } i, \text{where } i \geq 1\},$$

$$\bigcap_{i=1}^{\infty} X_i = \{x \in U : x \in X_i \text{ for all } i, \text{where } i \geq 1\}.$$

Example 1.9 For real numbers $a < b$, we define

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\},$$

$$(a, b) = \{x \in \mathbb{R} : a < x < b\},$$

and

$$(a, b] = \{x \in \mathbb{R} : a < x \leq b\}.$$

We define $[a, b)$ similarly. These are called *intervals* of real numbers.

For example, consider $X_i = [0, 1/i)$, where $i \geq 1$. We then have that

$$\bigcap_{i=1}^{\infty} X_i = \{0\},$$

since 0 is the only real number in every one of the sets $[0, 1/i)$. We also have that

$$\bigcup_{i=1}^{\infty} X_i = [0, 1),$$

since every nonnegative real number strictly less than 1 is in some X_i. The sets X_i are what are called *nested sets* as for all $i \geq 1$, $X_{i+1} \subseteq X_i$.

Definition 1.10 For a set X, the *power set* of X, written $\mathcal{P}(X)$, is the set consisting of all subsets of X.

Example 1.10

1. If $X = \{1, 2\}$, then

$$\mathcal{P}(X) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}.$$

2. If $Y = \{a, b, c\}$, then

$$\mathcal{P}(Y) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Note that the empty set and the set X itself are always elements of $\mathcal{P}(X)$. Another key fact is that for a finite set S with cardinality n, we have that $|\mathcal{P}(X)| = 2^n$. This generalizes to infinite sets also, but we will not discuss that direction here.

We finish the section with the notion of Cartesian products of sets.

Definition 1.11 For sets X and Y, the *Cartesian product* of X and Y, written $X \times Y$, is the set of ordered pairs with first entry in X and second in Y. We write

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Example 1.11 If $X = \{1, 2\}$ and $Y = \{a, b, c\}$, then

$$X \times Y = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\},$$

and

$$Y \times X = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}.$$

Note that the order matters in Cartesian products: $X \times Y \neq Y \times X$, in general, as we saw in the previous example.

1.4 Countable and Uncountable Sets

We consider ways of measuring the cardinalities of infinite sets. Not all infinite sets have the same cardinality.

Definition 1.12 A set X is *countable* if its elements can be listed: $x_1, x_2, x_3, \ldots$.

Example 1.12

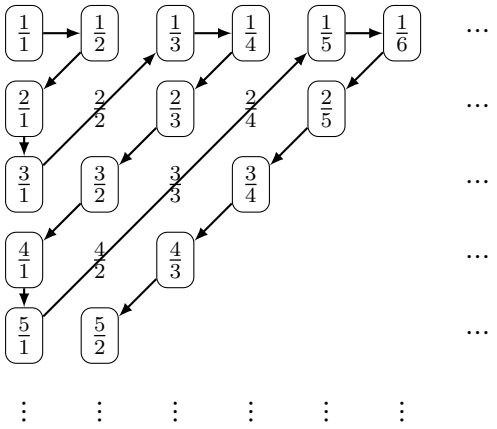
1. The empty set is countable, as it has no elements to list.
2. A finite set is countable, as all its elements can be listed as $x_1, x_2, x_3, \ldots, x_n$, where n is some nonnegative integer.
3. The set of natural numbers $\mathbb{N}$ is countable, as its elements are listed as $0, 1, 2, 3, \ldots$.

By the third example, infinite sets may be countable. In fact, there are many other examples of countable, infinite sets.

Example 1.13 The set of integers $\mathbb{Z}$ is countable. To see this, consider the listing of it elements as:

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots.$$

If we consider the rational numbers $\mathbb{Q}$, then this set is also countable. The idea behind the proof is to list all the fractions. This may be done for the positive rationals in the following way:



Notice in the figure that only the circled rational numbers are included in the listing, as the noncircled ones (such as $\frac{2}{2}$) are redundant and so are excluded in the list. We can modify the list to allow negative fractions by inserting $-r$ adjacent to r in the list.

While $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are each countable, we next show that the set of real numbers $\mathbb{R}$ is not countable, or *uncountable*. In a certain sense, the infinity of the real numbers is strictly bigger than the one for the natural numbers.

Theorem 1.3 The set of real numbers $\mathbb{R}$ is uncountable.

We give only a sketch of the proof. For a contradiction, suppose that every real number can be listed as follows:

$$\begin{aligned} r_1 &= t_1.s_{11}s_{12}s_{13}s_{14}\ldots \\ r_2 &= t_2.s_{21}s_{22}s_{23}s_{24}\ldots \\ r_3 &= t_3.s_{31}s_{32}s_{33}s_{34}\ldots \\ r_4 &= t_4.s_{41}s_{42}s_{43}s_{44}\ldots \\ &\vdots \end{aligned}$$

The real number $r_1 = t_1.s_{11}s_{12}s_{13}s_{14}\ldots$ is expressed as its decimal expansion, with t_1 an integer, then decimals $s_{11}, s_{12}, \ldots$. The idea is to define a new real number

$$r = 0.s_1s_2s_3s_4\ldots,$$

where s_j is chosen to be distinct from s_{jj}. For example, if $s_{jj} = 1$, then let $s_j = 2$. In other

cases, let $s_j = 1$.

We then have that s_j is distinct from the "diagonal" decimals s_{jj} for all j, and so r is distinct from each r_j, for $j \geq 1$. That conclusion contradicts the assumption that $\mathbb{R}$ is countable; hence, $\mathbb{R}$ is uncountable.

The approach here is called *diagonalization*, since we defined our "new" real number by modifying the diagonal elements in our list of real numbers.

1.5 Logic

Logic is at the core of mathematics: we use it in proofs, in examples, and when stating theorems. We give a review of elementary propositional and quantifier logic in this section, focusing on the key concepts. We will not cover truth tables or length logical derivations, as our aim is to explain the logic used in mathematical discussion throughout the book. One of the main takeaways is learning about the five logical connectives:

$$\wedge, \vee, \rightarrow, \leftrightarrow, \neg$$

A final focus will be on the quantifiers $\forall, \exists$. Along the way, we will learn about contradictions, contrapositives, as well as necessary and sufficient conditions. Each of these concepts will be critical when we are doing proofs later in the book.

Definition 1.13 A *statement* is any sentence which is either true or false.

Almost all of mathematics can be expressed as statements.

Example 1.14

1. The function $y = f(x)$ is continuous.
2. The set X is empty.
3. If the determinant of the matrix A is nonzero, then A is invertible.

We may put statements together via logical operators called *connectives*. Our focus is on the following five connectives, and how they fit together to make *compound statements*.

Definition 1.14 Let P and Q be statements. We define the following.

1. $P \wedge Q$, which means P and Q, and is called a *conjunction*.
2. $P \vee Q$, which means P or Q, and is called a *disjunction*.
3. $P \to Q$, which means if P, then Q, and called an *implication* or *conditional*. In an implication $P \to Q$, P is the *hypothesis* and Q is the *conclusion*.
4. $P \leftrightarrow Q$, which means P if and only if Q, and called a *biconditional*.
5. $\neg P$, which means not P, and called a *negation*.

Example 1.15 If P, Q, and R are statements, then the following is a statement

$$((\neg P \vee Q) \wedge R) \to \neg(\neg R).$$

The *truth value* of a compound statement depends on its connectives.

Definition 1.15 Let P and Q be statements. We then have the following.

1. $P \wedge Q$ is true exactly when both P and Q are true.
2. $P \vee Q$ is true exactly when at least one of P or Q are true.
3. $P \to Q$ is false exactly when P is true and Q is false; in all other cases, it is true.
4. $P \leftrightarrow Q$ is true exactly when either P and Q are both true, or when P and Q are both false.
5. $\neg P$ is true exactly when P is false.

Example 1.16 Let P be the statement: "The sky is blue," and let Q be the statement: "There are white clouds in the sky." In this case, $P \wedge Q$ is: "The sky is blue and there are white clouds in the sky."
The statement $Q \to \neg P$ is: "If there are white clouds in the sky, then the sky is not blue."

Definition 1.16 Two statements P and Q are logically equivalent when P and Q share the same truth values. We write this as $P \equiv Q$.

The following captures important logical equivalences.

Theorem 1.4 **(Laws of connectives)** Let P, Q, and R be statements. We then have the following.

1. Idempotent laws:
$$P \wedge P \equiv P \quad \text{and} \quad P \vee P \equiv P.$$

2. Double Negation law:
$$\neg(\neg P) \equiv P.$$

3. Commutative laws:
$$P \vee Q \equiv Q \vee P \quad \text{and} \quad P \wedge Q \equiv Q \wedge P.$$

4. Associative laws:
$$(P \vee Q) \vee R \equiv P \vee (Q \vee R) \quad \text{and} \quad (P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R).$$

5. Distributive laws:
$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \quad \text{and} \quad P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R).$$

6. De Morgan's laws:
$$\neg(P \wedge Q) \equiv \neg P \vee \neg Q \quad \text{and} \quad \neg(P \vee Q) \equiv \neg P \wedge \neg Q.$$

7. Absorption laws:
$$P \vee (P \wedge Q) \equiv P \quad \text{and} \quad P \wedge (P \vee Q) \equiv P.$$

8. Implication law:
$$P \to Q \equiv \neg P \vee Q.$$

Example 1.17 Let P, Q, and R be statements. We have the following equivalences.

$$\begin{aligned} (R \wedge (P \vee Q)) \to Q &\equiv \neg(R \wedge (P \vee Q)) \vee Q \text{ (Implication law)} \\ &\equiv \neg((R \wedge P) \vee (R \wedge Q)) \vee Q \text{ (Distributive law).} \end{aligned}$$

Example 1.18 For x a real number, let P be the statement $-8 < x$, let Q be the statement that $x = 10$, and let R be the statement $x < 10$. In symbols, the statement

$$-8 < x \leq 10,$$

is

$$P \wedge (Q \vee R).$$

Definition 1.17

1. A *tautology* is a statement that is always true regardless of the truth values of the individual statements substituted for its statement variables.
2. A *contradiction* is a statement that is always false regardless of the truth values of the individual statements substituted for its statement variables.

In proofs by contradiction, we assume the opposite of the given conclusion and derive a contradiction. We will come back to these kinds of proof in other chapters.

Example 1.19

1. The statement: "$1 + 1 = 2$" is a tautology.
2. The statement: "$0 = 1$" is a contradiction.
3. The statement: "$r < s$ for real numbers r, s" is neither a contradiction nor a tautology.

Definition 1.18

1. The *converse* of an implication $P \to Q$ is the implication $Q \to P$.
2. The *contrapositive* of an implication $P \to Q$ is the statement $\neg Q \to \neg P$.

An implication and its contrapositive are logically equivalent (they are either both true or both false). Sometimes when doing proofs, we will see that we prove the contrapositive statement. We will call this *proof by contraposition*.

Example 1.20 The contrapositive of the statement: "If a function $y = f(x)$ is differentiable, then it is continuous," is: "If a function $y = f(x)$ is not continuous, then it is not differentiable."

Definition 1.19 1. The statement P is *necessary* for Q means that $Q \to P$.

2. The statement P is *sufficient* for Q means that $P \to Q$.

Note that P and Q are both necessary and sufficient exactly when $P \leftrightarrow Q$.

Example 1.21 1. My bicycle will work only if it has air in its tires. Here P is having air in the bike's tires, and Q is having the bike work. We then have that P is necessary for Q and $Q \to P$.

2. A necessary condition for a computer program to be correct is that it not produce error messages when compiling. Here P is not producing errors when compiling and Q is the program being correct.

3. A sufficient condition to view a website is to have internet. If you do not have internet, then you will not be able to view a website.

Definition 1.20 A *predicate* is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The *domain* of a predicate variable is the set of all values that may be substituted in place of the variable.

Example 1.22 The predicate $P(x)$ has domain the real numbers, and states: $1/x > x$. This is true for $x = 1/2$, but false for $x = 2$.

Definition 1.21 1. The *universal quantifier* is $\forall$ and is read "for all" or "every." A universal statement $\forall x P(x)$, where $P(x)$ is a predicate, means that for all x in the domain, $P(x)$ holds.

For $\forall x P(x)$ to be true, it must be true for every x in the domain. For $\forall x P(x)$ to be false, it must be false for some x in the domain. Such an x is called a *counterexample*.

2. The *existential quantifier* is $\exists$ and is read "there exists" or "there is." An existential statement $\exists x P(x)$, where $P(x)$ is a predicate, means that for some x in the domain, $P(x)$ holds.

For $\exists x P(x)$ to be true, it must be true for some x in the domain. For $\exists x P(x)$ to

be false, it must be false for every x in the domain.

Note that we may include brackets in quantified expressions for clarity; for example, we may write $\forall x(x > 0)$. We have the following equivalences: $\neg\forall x P(x)$ is equivalent to $\exists x \neg P(x)$, and $\neg\exists x P(x)$ is equivalent to $\forall x \neg P(x)$.

We may also have multiple quantifiers.

Example 1.23

1. For all nonzero real numbers x, there is a number y such that $xy = 1$.
2. There exists a matrix A and there exists a matrix B such that $AB = BA$.

Note that the order of quantifiers matters: read them from left to right.

Example 1.24

1. Consider the quantified statement: For all real numbers x, there exists a real number y such that $x < y$. This is true for all real numbers, as there is no largest real number.
2. However, the quantified statement: There exists a real number y such that for all nonzero real numbers $x, x < y$, is false, as there is no largest real number.
3. The following universally quantified statement is false: For all real numbers x, $1/x$ is defined. The number 0 is a counterexample.

1.6 Exercises

(1.1) Determine the cardinality of the following sets.

(a) $\{\varnothing\}$.

(b) $\{\{\varnothing\}\}$.

(c) $\{\{\varnothing\}, \varnothing\}$.

(d) $\{\varnothing, \{\varnothing\}, \varnothing\}$.

(1.2) Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$, and $U = \{1, 2, 3, 4, 5, 6\}$. Find the following sets.

(a) $A \cup B$.

(b) $A \cap B$.

(c) $A \setminus B$.

(d) A^c.

(e) $A \triangle B$.

(f) $B \triangle A$.

(g) $A \times B$.

(1.3) For each of the sets (a) - (f) in the previous exercise, draw the corresponding Venn diagram.

(1.4) Find the following sets.

(a)
$$\bigcap_{i=1}^{\infty} \left(-\frac{1}{i}, \frac{1}{i}\right).$$

(b)
$$\bigcap_{i=1}^{\infty} \left[0, \frac{1}{i}\right).$$

(c)
$$\bigcup_{i=1}^{\infty} \left[-\frac{1}{i}, \frac{1}{i}\right).$$

(1.5) Find the power set of each of the following sets.

(a) $\varnothing$.

(b) $\{1\}$.

(c) $\{1, 2, 3\}$.

(1.6) Determine the following set
$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))).$$

(1.7) Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 3, 5, 7\}$, $B = \{6, 7, 10\}$, and $C = \{4, 5, 6, 7\}$. Find
$$A \triangle (B \triangle C).$$

(1.8) Using elements, prove that for sets A, B, and C, if $A \subseteq C$, and $B \subseteq C$, then $A \cup B \subseteq C$.

(1.9) Prove that for every set A that $\varnothing \subseteq A$. (**Hint**: Use a proof by contraposition.)

(1.10) Can it happen that for sets A and B, $A \subsetneq B$ and $B \subsetneq A$? Prove it or give a counterexample.

(1.11) Let
$$A = \{x \in \mathbb{Z} : x = 10b + 7, \text{ for some } b \in \mathbb{Z}\}$$

and

$$B = \{y \in \mathbb{Z} : y = 10c - 3, \text{ for some } c \in \mathbb{Z}\}.$$

Prove that $A = B$.

(1.12) Show that if $X \subseteq Y$, then

$$\mathcal{P}(X) \subseteq \mathcal{P}(Y).$$

(1.13) Using the element method, prove that for sets A, B, and C, if $A \subseteq B$, and $B \cap C = \varnothing$, then $A \cap C = \varnothing$.

(1.14) Using the element method, prove the following.

(a) Complement laws:

$$X \cup X^c = U \quad \text{and} \quad X \cap X^c = \varnothing.$$

(b) Identity laws:

$$X \cup \varnothing = X \quad \text{and} \quad X \cap U = X.$$

(c) Set difference law:

$$X \setminus Y = X \cap Y^c.$$

(1.15) If X and Y are countable sets, then prove that $X \cup Y$ is countable.

(1.16) If Y is a countable set and $X \subseteq Y$, then show that X is countable.

(1.17) Show that if X and Y are countable sets, then $X \cap Y$ is countable.

(1.18) If X is an uncountable set and $X \subseteq Y$, then show that Y is uncountable.

(1.19) Show that the interval $[0, 1]$ is uncountable. (**Hint**: Adapt the diagonalization proof of Theorem 1.3.)

(1.20) Explain why the following sets are countable by listing their elements.

(a) The even integers.

(b) $\mathbb{N} \times \mathbb{N}$. (**Hint**: use a similar listing to the rational numbers.)

(c) The odd, positive integers that have a remainder of 1 when divided by 3.

(d) The set of all positive rational numbers with denominator a power of 2.

(1.21) Translate the following compound into symbols using statements P and Q and logical connectives.

(a) It is not both hot and cold.

(b) It is hot or cold.

(c) It is hot but not cold.

(1.22) (a) Write the following statement in symbolic form: $-1 < x < 2$, where A is $-1 < x$ and B is $x < 2$.

(b) Negate the statement in (a).

(c) Repeat (a) and (b) for: $-1 \leq x < 2$, with C the statement $x = -1$.

(1.23) Use the contrapositive to rewrite the following statement in two ways: Being age at least 16 is a necessary condition to take a driver's test.

(1.24) Rewrite the following statements in the form: If P, then Q.

(a) Being a differentiable function is a sufficient condition to be a continuous function.

(b) A number being even is necessary condition for the number to be a multiple of 2.

(c) A sufficient condition for a person to vote is to be at least 18.

(d) A necessary condition for a person to vote is to be at least 18.

(1.25) If P and Q are statements, then write the negation of $P \to Q$ using only the connectives $\wedge$ and $\neg$.

(1.26) Simplify the following statements using only the connectives $\wedge$, $\vee$ and $\neg$.

(a) $\neg(\neg P \to Q)$.

(b) $(P \wedge \neg Q) \to \neg(\neg Q \vee P)$.

(c) $\neg((\neg Q \wedge P) \vee \neg(T \vee \neg R))$.

(d) $(\neg P \vee \neg R) \to \neg(\neg R \wedge Q)$.

(1.27) Rewrite the following sentences using quantifiers.

(a) There is no largest real number.

(b) There is a smallest natural number.

(c) Every nonnegative integer has a square root.

(1.28) Show that each of the following universally quantified statements is false by finding a single counterexample.

(a) $\forall y \in \mathbb{R}, e^y < y$.

(b) $\forall x \in \mathbb{Z}, 1/x \in \mathbb{Z}$.

(c) $\forall x, y \in \mathbb{R}, \cos(x + y) = \cos(x) + \cos(y)$.

(1.29) Simplify the following statements so negations occur within the quantified statements.

(a) $\neg(\exists x \forall y(\neg P(x) \vee Q(y)))$.

(b) $\neg(\forall x \neg \forall y(x > y \wedge \exists z(x > z \vee y > z)))$.

(1.30) Negate the following statements. Negations should occur within the quantified statements, but you do not have to distribute the negation symbol there.

(a) $\forall y \exists x (x \vee \neg y)$.

(b) $\exists y (P(y) \to Q(y))$.

(c) $\forall x \neg \exists y (x > y \vee \exists z (x < z < y))$.

1.7 Selected Answers and Hints

(1.1) (a) 1. (b) 1. (c) 2. (d) 2.

(1.2) (a) $A \cup B = \{1,2,3,4,5\}$. (b) $A \cap B = \{3\}$. (c) $A \setminus B = \{1,2\}$. (d) $A^c = \{4,5,6\}$. (e) $A \triangle B = \{1,2,4,5\}$. (f) $B \triangle A = \{1,2,4,5\}$. (g)

$$A \times B = \{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,3),(3,4),(3,5)\}.$$

(1.4) (a) $\{0\}$. (b) $\{0\}$. (c) $[-1,1)$.

(1.5) (a) $\{\varnothing\}$. (b) $\{\varnothing,\{1\}\}$. (c) $\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$.

(1.6) $\mathcal{P}(\varnothing) = \{\varnothing\}$, $\mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing,\{\varnothing\}\}$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))) = \{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$.

(1.7) $B \triangle C = \{4,5,10\}$, $A \triangle (B \triangle C) = \{1,3,4,7,10\}$.

(1.8) An element of $A \cup B$ is an element of A and B, and both sets are contained in C.

(1.9) An element not in A is not in $\varnothing$.

(1.10) No, this is impossible. If A is proper subset of B, then some element of B is not in A. From this, we cannot have that B is a subset of A.

(1.11) If we take an element $x = 10b + 7$ of A and set it equal to $10c - 3$, we can solve for c to show $x \in B$. Repeat by taking an element $y = 10c - 3$, and showing it is in A.

(1.12) Show that each subset X is also a subset of Y.

(1.13) By the element method, we have that $A \cap C \subseteq B \cap C$. As $B \cap C = \varnothing$, the proof follows.

(1.15) List the elements of X as $x_1, x_2, \ldots$ and Y as $y_1, y_2, \ldots$. We may then list the elements of $X \cup Y$ as $x_1, y_1, x_2, y_2, \ldots$.

(1.16) If we list the elements of Y, then restricting this to X, we have a listing of elements of X.

(1.17) Apply Exercise (1.16) to $X \cap Y \subseteq Y$.

(1.18) For a contradiction, suppose that Y is countable. By Exercise (1.17), this then implies that X is countable, which is a contradiction.

(1.19) Proceed as in the proof of Theorem 1.3, but in the proof by contradiction, list the elements of $[0,1]$ as $r_i = 0.s_{i1}s_{i2}s_{i3}s_{i4}\ldots$.

(1.20) (a): list the elements as $0, -2, 2, -4, 4, -6, 6, \ldots$.

(b): use a similar listing to $\mathbb{Q}$, replacing a fraction p/q by (p, q).

(c): list these as $1, 4, 7, 10, 13, \ldots$.

(d): use a similar listing to $\mathbb{Q}$, where the ith row has denominator $j/2^i$.

(1.21) Let P be the statement "It is hot," and Q be the statement "It is cold."

(a): $\neg(P \wedge Q)$. (b): $P \vee Q$. (c): $P \wedge \neg Q$.

(1.22) (a): $A \wedge B$. (b) $\neg(A \wedge B)$. This is equivalent to $\neg A \vee \neg B$.

(c): the statement is $(A \vee C) \wedge B$, with negation $\neg((A \vee C) \wedge B)$.

(1.23) Being under age 16 implies that you cannot take a driver's test.

(1.24) (a): If a function is differentiable, then it is continuous. (b): If an integer is a multiple of 2, then it is even. (c): If a person is at least 18, then they vote. (d): If a person votes, then they are at least 18.

(1.26) (a): $\neg P \wedge \neg Q$. (b): $(\neg P \vee Q) \vee (Q \wedge \neg P)$. (c): $(Q \vee \neg P) \wedge (T \vee \neg R)$. (d) $P \wedge R) \vee (R \vee \neg Q)$.

(1.27) (a): $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x < y$. (b): $\exists x \in \mathbb{N}$ such that $\forall y \in \mathbb{N}$, $x \leq y$. (c): $\forall x \in \mathbb{N}$, $\exists y \in \mathbb{R}$ such that $x = \sqrt{y}$.

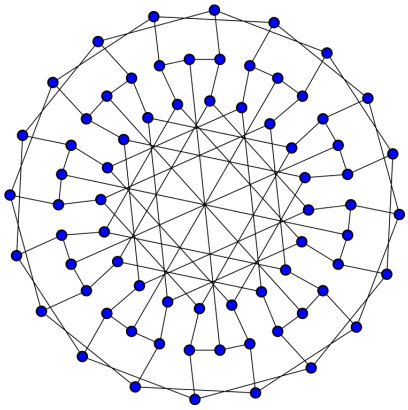
(1.28) Note that in each part, the answer provided not unique. (a): $y = 2$. (b): $x = 5$. (c): $x = 0$, $y = \pi$.

(1.29) (a): $\forall x \exists y (P(x) \wedge \neg Q(y))$. (b): $\exists x \forall y (x > y \wedge \exists z (x > z \vee y > z))$.

(1.30) (a): $\exists y \forall x (\neg x \wedge y)$. Note that negations were distributed here. (b): $\forall y \neg (P(y) \to Q(y))$. (c): $\exists x \exists y (x > y \vee \exists z (x < z < y))$.

Chapter 2

Graphs and Trees



2.1 Introduction to Graphs

Graph theory is one of the most important topics in discrete mathematics. Graphs capture interactions between objects; as such, they come up everywhere in the natural world. From friends and followers on social media, to Bitcoin transactions, and to how circuits interact, graphs appear everywhere.

The goal in the current chapter is to introduce graphs from scratch and discuss their core properties. We introduce graphs and the main notation and elementary theory used in their study. The background gained from Chapter 1 on sets and logic will serve us well while studying graphs.

Definition 2.1

1. A *graph* G is a pair consisting of a *vertex set* $V(G)$, and an *edge set* $E(G)$ containing pairs of distinct vertices. If G is clear from context, then we write $G = (V, E)$.
2. We write uv if vertices u and v form an edge, and say that u and v are *adjacent*.
3. We say u and v are *incident* with the edge uv, and that u and v are *endpoints* of the edge uv.
4. The *order* of a graph G is $|V(G)|$, and its *size* is $|E(G)|$.

We will always assume that graphs are finite, meaning that their order and size are finite. All the graphs we consider are *simple* in the sense that there are no edges from a vertex to itself (called *loops*), and there is at most one edge between two vertices.

Graphs are often depicted by their *drawings*, which consist of dots (usually solid but they do not have to be) representing vertices, and edges represented as lines between dots. Notice that you can think of the lines as elastic: they can shrink, stretch, or move and not change the graph; however, you cannot break the elastics. See Figure 2.1.

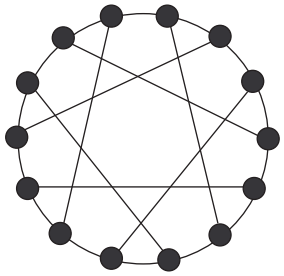


Figure 2.1: A graph with order 14 and size 21.

You can reposition vertices and edges in a drawing and not change the graph. You are not allowed to add or delete vertices or edges, however.

Graphs are defined abstractly, but they also appear everywhere in the real-world. The *web graph* has vertices corresponding to websites and edges corresponding to links between websites. The web graph is enormous, with trillions of vertices and many more edges. See Figure 2.2 for a visualization of part of the web graph, with vertices scaled by the number of edges touching them. Note that in this drawing and others, vertices may or may not have labels, which may be letters, numbers, words, or phrases.

Another example comes from Twitter, where we take keywords and make them adjacent if they appear in the same tweet. See Figure 2.3 for the keyword network taken from a sample of ex-US President Donald Trump's tweets. For example, if the keywords "media" and "news" appeared in the same tweet, then they were adjacent. Notice how the keywords are grouped into thematically related clusters or communities, which are represented by different colors. The size of a keyword is proportional to the number of edges incident to it.

We may think of graphs $G = (V, E)$ more formally as a kind of binary relation, as we will explore in Chapter 3. In this setting, E is a set of ordered pairs on V with the extra property of *symmetry*: for all $(x, y) \in E$, we have that $(y, x) \in E$.

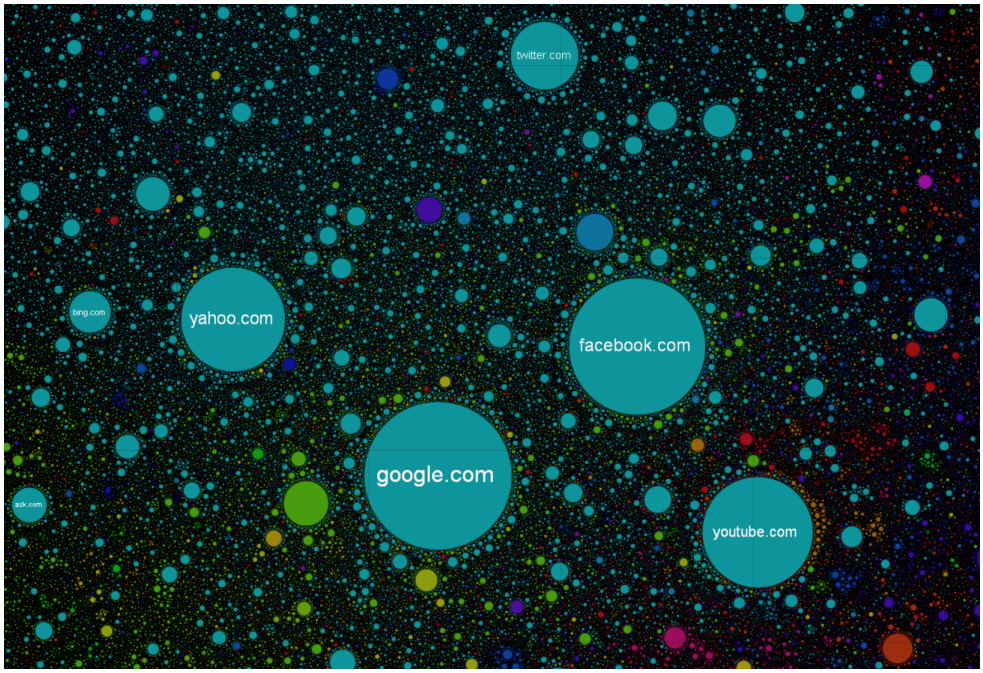


Figure 2.2: A fragment of the web graph, from the internet map.

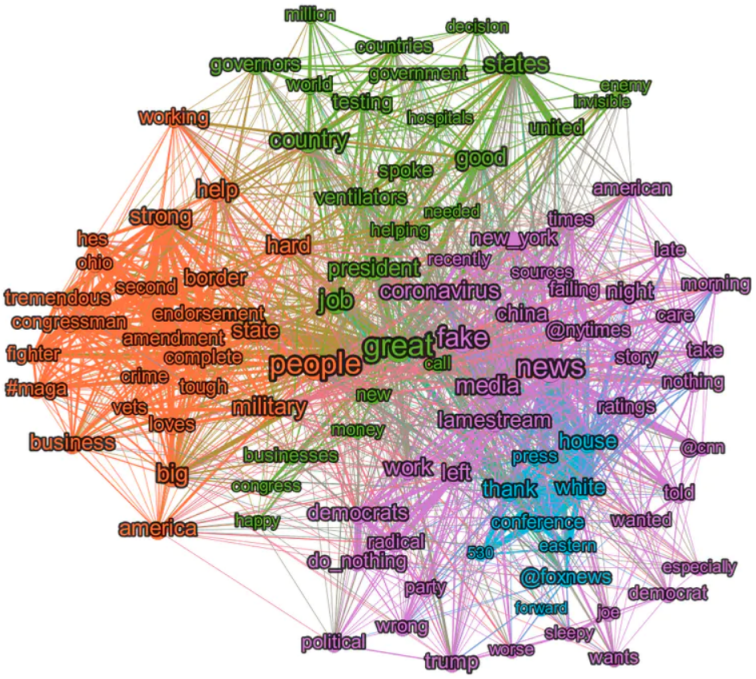


Figure 2.3: Donald Trump's Twitter keyword network taken during the month of April 2020.

2.2 Degrees

Definition 2.2 1. Given a graph G with vertex v, the *degree* of v, denoted by $\deg_G(v)$, is the number of edges incident with v. The subscript G may be omitted when there is no risk of confusion.

2. The *neighbor set* of v, denoted $N_G(v)$, is $\{w \in V(G) : vw \in E(G)\}$; any $w \in N_G(v)$ is called a *neighbor* of v. Notice that $\deg_G(v) = |N_G(v)|$.

3. The *closed neighbor set* of v, denoted $N_G[v]$, is $N_G(v) \cup \{v\}$.

We drop the subscripts from $N_G(v)$ and $N_G[v]$ if G is clear from context. See Figure 2.8 for an example.

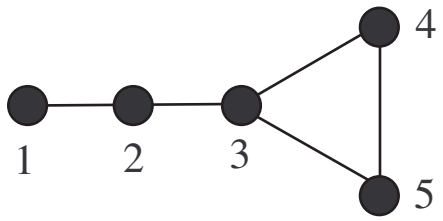


Figure 2.4: In the depicted graph, we have that $\deg(1) = 1, \deg(2) = 2, \deg(3) = 3, \deg(4) = 2, \deg(5) = 2$. We have that $N(3) = \{2, 4, 5\}$ and $N[2] = \{1, 2, 3\}$.

Definition 2.3 1. For a nonnegative integer m, if $\deg(v) = m$ for all $v \in V(G)$, then G is called *m-regular*.

2. The integer $\delta(G) = \min_{v \in V(G)} \deg(v)$ is the *minimum degree* of G, and the integer $\Delta(G) = \max_{v \in V(G)} \deg(v)$ is the *maximum degree* of G.

3. A vertex that has degree zero is called an *isolated vertex*, while a vertex adjacent to all others is called *universal*.

Example 2.1 In the graph in Figure 2.4, $\delta(G) = 1$ and $\Delta(G) = 3$.

We now introduce our first theorem, which provides an elementary but important re-

lationship between the degrees and the size of a graph. Note that the proof really is one line!

Theorem 2.1 (First Theorem of Graph Theory) If G is a graph, then

$$\sum_{u \in V(G)} \deg_G(u) = 2|E(G)|.$$

Proof. In the sum, each edge is counted exactly twice. □

A useful corollary of the First Theorem of Graph Theory is the following.

Theorem 2.2 In a graph, the number of vertices of odd degree is even.

Proof. From the First Theorem of Graph Theory, we know that $\sum_{u \in V(G)} \deg(u) = 2|E(G)|$. Let E be the sum of the degrees of vertices with even degrees, and let O be the sum of the degrees of vertices with odd degrees. We then have that

$$E + O = 2|E(G)|.$$

Since $E + O$ is even and we know E is even, it follows that O is even. This can only happen if there are an even number of odd degree vertices. □

This property puts restrictions on the possible degrees of a graph. For example, there cannot be a graph of order 19 that is 9-regular, as that would give an odd number of odd degree vertices.

2.3 Subgraphs and Connected Graphs

Definition 2.4 1. A *walk* in a graph G from vertex u to vertex v is a sequence $W = (u = v_0, v_1, \ldots, v_k = v)$ if $v_i v_{i+1} \in E(G)$ for $0 \leq i < k$. The *length* of a walk W is the number of vertices in W minus 1 (that is, the number of edges).

2. A walk is *closed* if $v_0 = v_k$.

3. A *path* is a walk without repeated vertices. The path of order n is denoted by P_n.

4. A *cycle* is a closed path of length at least 3. We use the notation C_n for a cycle of order n.

Figure 2.5: The path P_6.

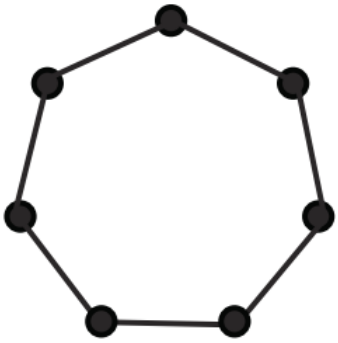


Figure 2.6: The cycle C_7.

Definition 2.5 1. The length of a shortest path in G between u and v is called the *distance* between u and v, denoted by $d_G(u, v)$. We drop the subscript G and write $d(u, v)$ if G is clear from context.

2. The *diameter* of G is

$$\operatorname{diam}(G) = \max\{d_G(v, w) : v, w \in V(G)\}.$$

See Figure 2.7. A shortest path between two vertices may not exist, in which case their distance is ∞.

Definition 2.6 1. A graph H is a *subgraph* of a graph G, written $H \subseteq G$, if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

2. The graph H is a *spanning subgraph* if $V(H) = V(G)$.

3. If $S \subseteq V(G)$, then the subgraph of G *induced* by S, denoted by $G[S]$, has vertices S and edges are those of G with endpoints in S.

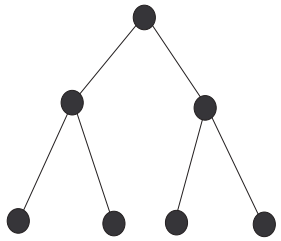


Figure 2.7: A graph of diameter 4.

4. The subgraph of G obtained by removing a subset S from V or E is denoted $G-S$. When S contains a single vertex or edge, say x, we write $G-x$.

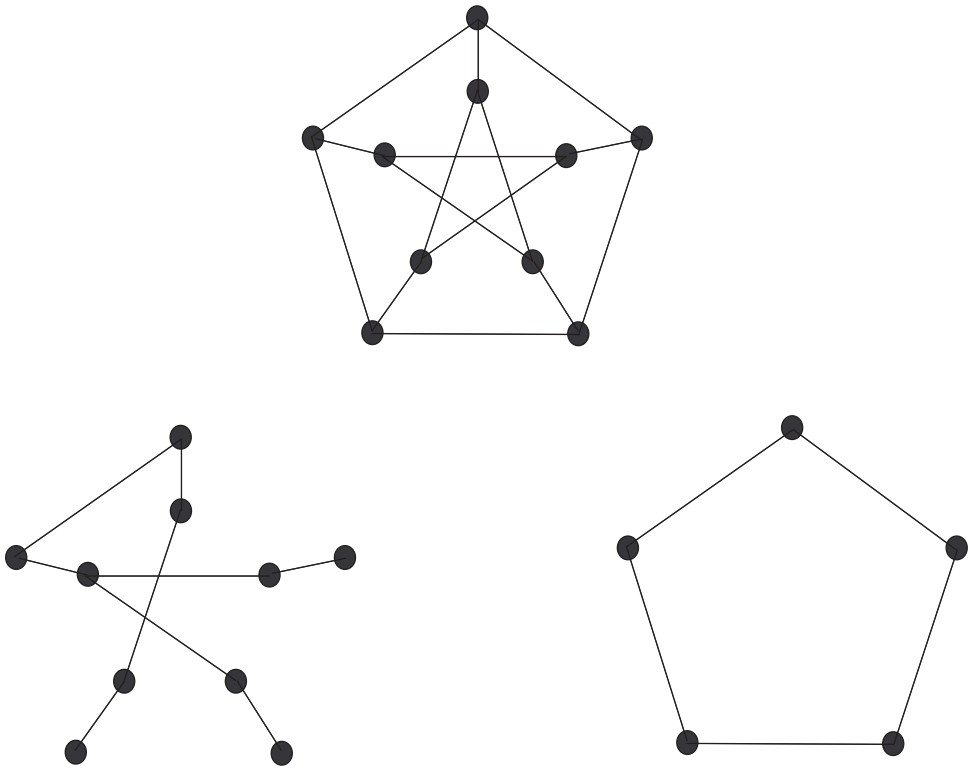


Figure 2.8: A graph and a spanning subgraph (bottom left) and induced subgraph (bottom right).

We consider some important examples of graphs.

Example 2.2 1. A *complete graph* of order n, written K_n, contains all edges between its vertices.

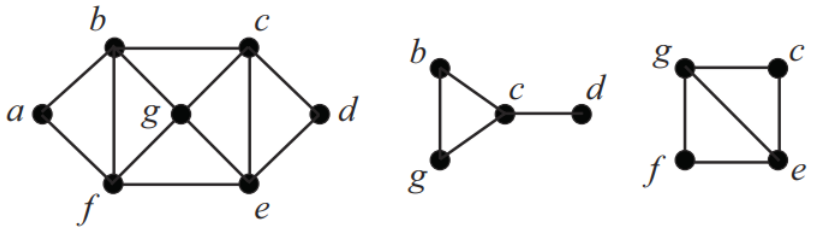


Figure 2.9: The graph G on the left and two of its induced subgraphs: $G[\{b, c, d, g\}]$ and $G[\{c, e, f, g\}]$.

2. The *complement* of a graph G, written $\overline{G}$, is the graph with vertices $V(G)$ and edges $\{xy : xy \notin E(G)\}$.

3. A *null graph* of order n, written $\overline{K_n}$, is the complement of K_n.

4. A set of vertices that is pairwise nonadjacent is an *independent set*.

5. For a positive integer k, a graph G is *k-partite* if $V(G)$ can be partitioned into k independent sets called *parts*.

   If $k = 2$, then we say G is *bipartite*; if all edges are present between the parts, then the graph is *complete bipartite*. For positive integers i and j, if the parts of a complete bipartite graph have cardinality i and j, then we write this graph as $K_{i,j}$.

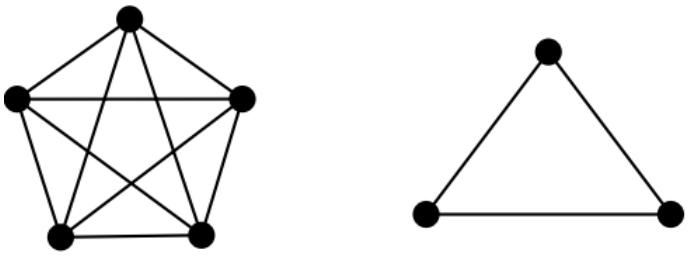


Figure 2.10: The complete graphs K_5 and K_3.

Definition 2.7 A graph is *connected* if every pair of distinct vertices is joined by a path, and *disconnected*, otherwise. The *components* of a graph G are the maximal connected induced subgraphs of G, with respect to set inclusion.

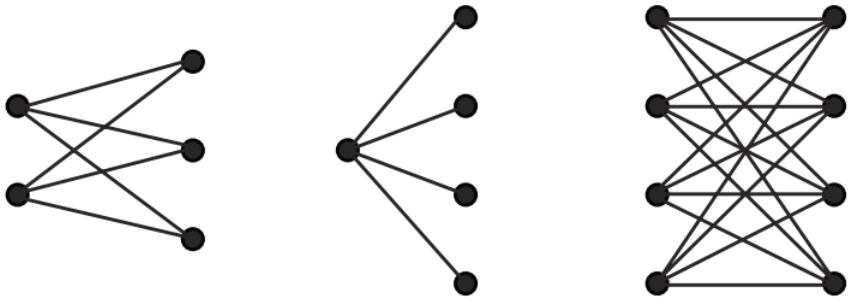


Figure 2.11: Complete bipartite graphs $K_{2,3}$, $K_{1,4}$, and $K_{4,4}$.

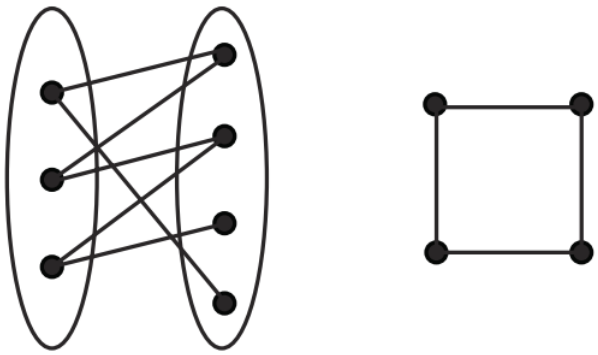


Figure 2.12: Two bipartite graphs. Note that the ovals on the left graph highlight the parts.

Example 2.3 For a positive integer n, an *n-bit binary string* is a sequence of length n consisting of zeros and ones. The n-dimensional *hypercube graph*, written Q_n, has vertices labeled by the n-bit binary strings, such that $xy \in E(Q_n)$ if and only if x and y differ by exactly one bit. We define Q_0 to be the graph with one vertex.

See Figure 2.13. We will show in the exercises that Q_n has 2^n vertices and is n-regular.

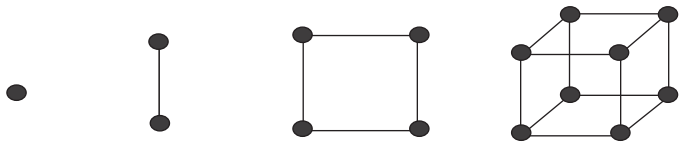


Figure 2.13: From left to right, the hypercube graphs Q_0, Q_1, Q_2, and Q_3.

2.4 Trees

Trees are a key graph family that is our next object of study.

Definition 2.8 A connected graph with no cycle is a *tree*. A *forest* is a graph with no cycle. Hence, a tree is a connected forest.

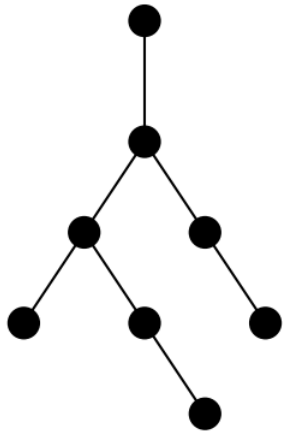


Figure 2.14: A tree.

Example 2.4 The graph P_n and an n-vertex *star* $K_{1,n-1}$ are trees.

Trees arise in many applications. For example, they appear as decision trees in machine learning; see Figure 2.15.

Definition 2.9 An *end-vertex* (or *leaf*) is a vertex of degree 1. A *spanning tree* is a spanning subgraph that is a tree.

We prove three theorems about trees.

Theorem 2.3 Trees have the property that any pair of distinct vertices are connected by a unique path.

Proof. Let G be a tree and let u, v be distinct vertices of G. If u and v are adjacent, then uv is the unique path connecting them. Suppose that u and v are not adjacent, and suppose for

Figure 2.15: A decision tree on what to do on a given day.

a contradiction that there are at least two paths P and Q connecting them. By joining P and Q together at u and v we obtain a cycle in G, which is a contradiction. □

Leaves play a special role when discussing trees.

Theorem 2.4 In a tree of order at least 2, there are at least two leaves.

Proof. Let G be a tree and let P be a longest path in G with endpoints u and v. We show that u is a leaf; the proof for v is similar.

Suppose that $\deg(u) \geq 2$. As P is a longest path, u cannot be adjacent to a vertex outside P, or else we found a longer path than P. Hence, u is adjacent to two vertices of P, which forms a cycle, which is a contradiction. Therefore, u is a leaf. □

Our final key fact about trees tells us their exact size in terms of their order.

Theorem 2.5 In a tree G, we have that $|E(G)| = |V(G)| - 1$.

We save the proof of Theorem 2.5 to Chapter 6, where we introduce induction.

Proof. We proceed by induction on $|V(G)|$. In the base case, where $|V(G)| = 1$, there are no edges, so $|E(G)| = 1 - 1 = 0$, as desired. Suppose the equality holds for trees of order n, for a fixed integer $n \geq 1$.

Let G be a tree of order $n+1$. We know that there are two leaves in G, as its order is at least 2. Let u be such a leaf. The graph $G-u$ is a tree: it is connected and no cycles are formed by deleting u. By the induction hypothesis,

$$|E(G-u)| = |V(G-u)| - 1 = (n+1) - 1 - 1 = n - 1.$$

If we add back u, then we add exactly one edge. Hence,

$$|E(G)| = n = |V(G)| - 1,$$

and the proof follows. □

2.5 Coloring and Domination

Definition 2.10

1. A *coloring* of a graph is an assignment of labels or *colors* to its vertices. A *proper coloring* is achieved when no two neighboring vertices have the same color.
2. The *chromatic number* of a graph G, denoted by $\chi(G)$, is the minimum number of colors required to achieve a proper coloring of G.
3. If G can be colored using at most k colors, then we say that G is *k-colorable*.

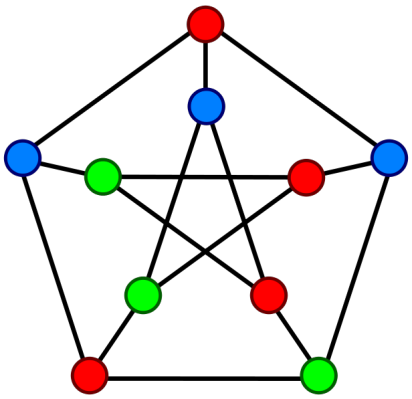


Figure 2.16: A proper coloring of a graph with three colors.

The chromatic number is monotone, in the sense that is described in the following theorem.

Theorem 2.6 If G is a graph with a subgraph H, then $\chi(H) \leq \chi(G)$.

Proof. If we proper color G, then use those same assignment of colors on H. As H is not adding any edges to those already in G, this is a proper coloring of H. □

Coloring also gives us a way to discuss bipartite graphs.

Theorem 2.7 A graph G is bipartite if and only if $\chi(G) \leq 2$.

Proof. If G is bipartite, then consider the independent sets X and Y that partitions $V(G)$. We assign distinct colors to each of X and Y. Note that one of X or Y (but not both) could be empty; hence, $\chi(G) \leq 2$.

If $\chi(G) \leq 2$, then label each vertex by one of the at most two colors. Each set of vertices of a single color must be independent, and so the graph G is bipartite. □

One way to bound the chromatic number from below is the presence of complete subgraphs.

Theorem 2.8 Suppose that H is a complete graph of order k that is a subgraph of G. We then have that $\chi(G) \geq k$.

Proof. A complete graph must have each of its vertices assigned distinct colors. Hence, $\chi(H) = k$. The proof now follows by Theorem 2.6. □

We can find a proper coloring by the *greedy algorithm*, as described in the proof of the following theorem.

Theorem 2.9 If G is a graph, then $\chi(G) \leq \Delta(G) + 1$.

Proof. We arrange the vertices of G in ascending order of their degree. Assign an arbitrary color c_1 to the lowest degree vertex. Repeat this process with each vertex in order, assigning the lowest ordered vertex an unused color. When any vertex v is to be colored, the number of colors already used cannot be any larger than its degree.

At the completion of the coloring, we see that the number of colors cannot be any larger than $\Delta(G)$ and thus, we might require at most one extra color. Thus, $\chi(G) \leq \Delta(G) + 1$. □

Definition 2.11 We call $S \subseteq V(G)$ a *dominating set* for G if for all $v \notin S$, there exists $w \in S$ such that $vw \in E(G)$. The minimum cardinality of a dominating set in G is denoted $\gamma(G)$, and is called the *domination number* of G.

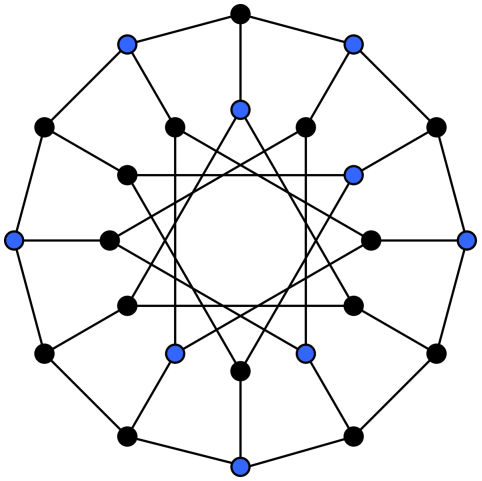


Figure 2.17: A graph with a dominating set in blue.

Note that each isolated vertex and vertex of degree 1 increases the domination number by 1. We will explore examples of domination numbers of graphs in the exercises.

Theorem 2.10 If G is a graph with no isolated vertices with a minimum cardinality dominating set S, then S^c is also a dominating set.

Proof. Suppose for a contradiction that S^c is not a dominating set. This implies that there is some vertex $u \in S$ such that there is no edge from u to any vertex in S^c. As there are no isolated vertices, u is not an isolated vertex, and so is adjacent to some vertex in $S \setminus \{u\}$. We then have that $S \setminus \{u\}$ is also a dominating set, which contradicts the minimality of S. Hence, S^c is a dominating set. □

We have the following bound on the domination number of graphs.

Theorem 2.11 If G is a graph with no isolated vertices, then $\gamma(G) \leq n/2$.

Proof. Let S be a minimum cardinality dominating set. For a contradiction, suppose that $\gamma(G) > n/2$, which implies that $|S| > n/2$. We then have by Theorem 2.10 that S^c is a

dominating set. Note that

$$|S^c| < n - n/2 < n/2,$$

which contradicts the fact that $\gamma(G) > n/2$. Hence, $\gamma(G) \leq n/2$, as desired. □

2.6 Directed Graphs

We may assign a direction to each edge of a graph.

Definition 2.12 A *directed graph* (or *digraph*) G is a pair consisting of a vertex set $V(G)$ and an edge set $E(G) \subseteq \{(x, y) : x, y \in V(G)\}$.

We may think of digraphs as binary relations, similar to graphs, but without the property of symmetry. We use the arrow notation to depict an edge pointing from vertex to vertex. We refer to (x, y) as *arcs*. See Figure 2.18.

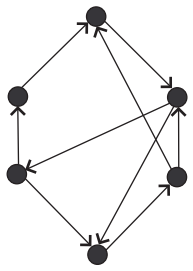


Figure 2.18: An example of a digraph.

Directed graphs are natural in many situations. For example, on Twitter, we have followers, where the social relationship flows in one direction (although it can be reciprocal). Another example is in the game show Survivor, where people vote each other off the show. Vertices are the players, and a directed edge from A to B means that A voted for B. See Figure 2.19 for the directed voter graph for the season Survivor: Heroes vs. Healers vs. Hustlers.

Definition 2.13 The *in-degree* of a vertex v, written $\deg^-(v)$, is the number of in-neighbors of v; that is,

$$\deg^-(v) = |\{u \in V : (u, v) \in E(G)\}|.$$

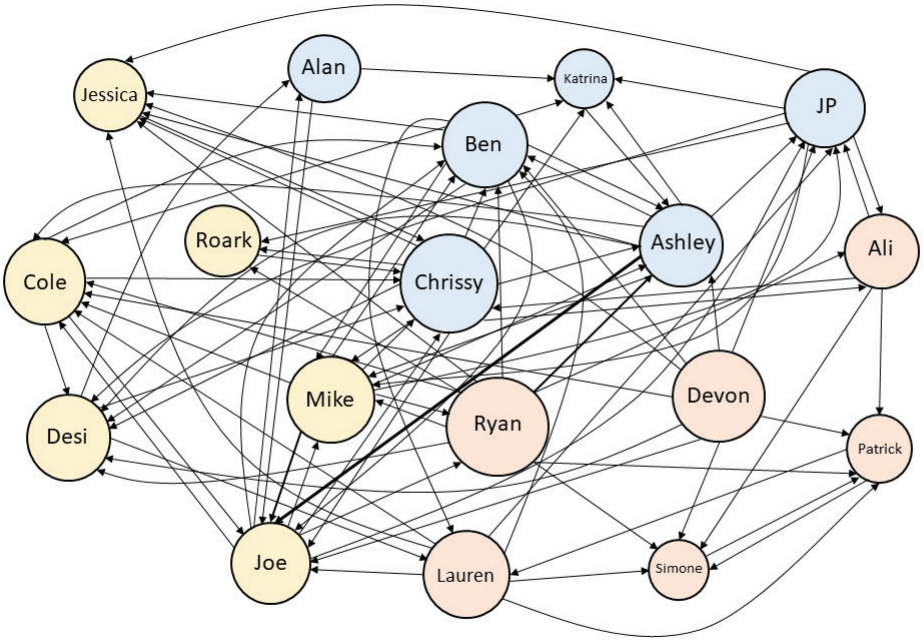


Figure 2.19: A directed voter graph of players in the social game show Survivor. Vertices are scaled by their prevalence throughout the game's season, and color-coded according to their original tribe. Thicker edges represent multiple votes.

Similarly, the *out-degree* of a vertex v, written $\deg^+(v)$, is the number of out-neighbors of v; that is,

$$\deg^+(v) = |\{u \in V : (v,u) \in E(G)\}|.$$

A directed graph is *oriented* if each pair of distinct vertices is in at most one arc.

Theorem 2.12 For a digraph G, we have that

$$\sum_{v \in V(G)} \deg^-(v) = \sum_{v \in V(G)} \deg^+(v).$$

Proof. For each directed edge (u,v), there is a contribution of exactly one to each of

$$\sum_{v \in V(G)} \deg^-(v)$$

and

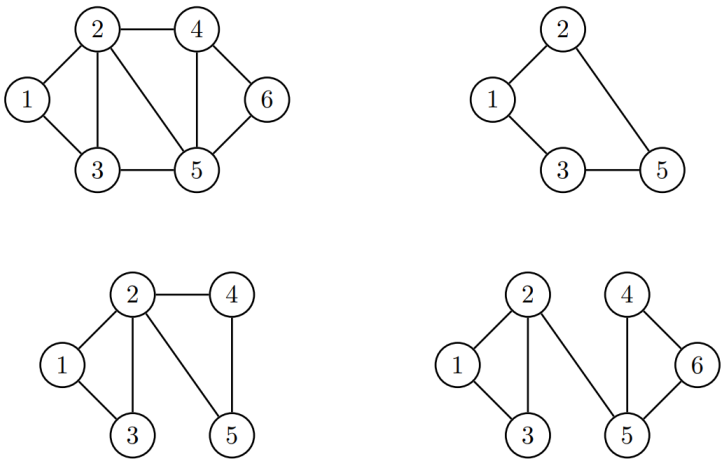
$$\sum_{v \in V(G)} \deg^+(v).$$

The proof follows. □

2.7 Exercises

An "(H)" at the beginning of an exercise denotes that it is more challenging than others.

(2.1) For the following four graphs, determine the order, size, and the degree of each vertex.



(2.2) For the graphs G in the previous exercise, determine the maximum degree $\Delta(G)$ and minimum degree $\delta(G)$. Also, list any isolated or universal vertices in G.

(2.3) Show that a graph with the given degrees cannot exist.

(a) 2, 3, 4, 5, 6, 7.

(b) 0, 0, 0, 1, 0.

(c) 1, 1, 1, 1, 1, 1, 2, 2, 3.

(d) 6, 6, 5, 4, 4, 3, 2, 2, 1.

(e) 1, 3, 3, 4, 5, 6.

(2.4) Verify that the sum of the degrees is twice the size in the two graphs G_1 and G_2 in Figure 2.20.

(2.5) A graph is *cubic* if each vertex has degree 3.

(a) Explain why a cubic graph must have an even number of vertices.

(b) Draw examples of cubic graphs of orders 4, 6, and 8.

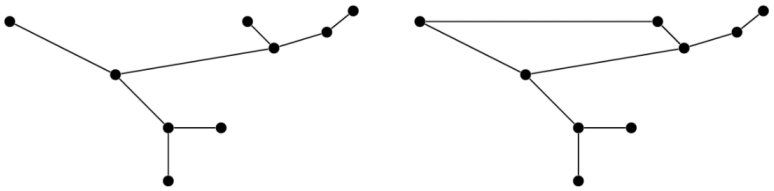


Figure 2.20: The graphs G_1 and G_2.

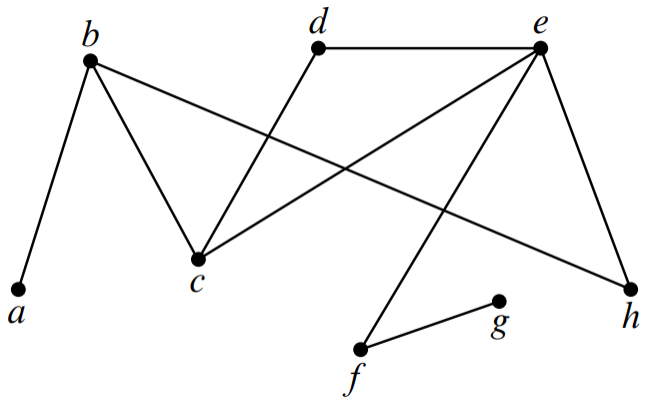


Figure 2.21: The graph G.

(2.6) Find the diameter of the graph G in Figure 2.21.

(2.7) Draw the complete graphs with orders 3, 4, 5, and 6.

(2.8) Explain why the following graphs are bipartite.

(a) A hypercube Q_n, where $n \geq 1$.

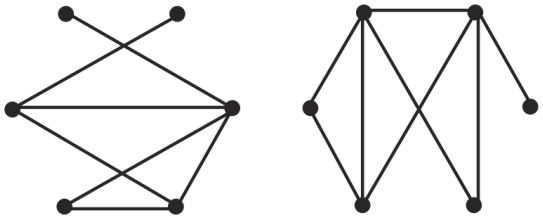
(b) A path P_n, where $n \geq 1$.

(c) A tree.

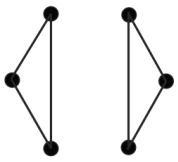
(2.9) Find all the independent sets in the hypercube Q_3.

(2.10) Suppose that G is a graph of order 7 with 15 edges. Find the number of edges in the complement $\overline{G}$.

(2.11) How many components do the following graphs G and H possess?



(a) The graph G.



(b) The graph H.

(2.12) For each of the following sets of vertices in the depicted graph G, draw the subgraph induced in G.

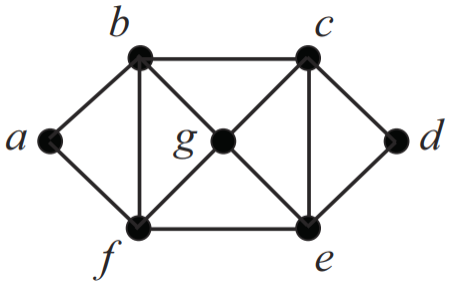


Figure 2.23: The graph G.

(a) $S_1 = \{a, b, c, d\}$.

(b) $S_2 = \{a, e, f, g\}$.

(c) $S_3 = \{b, f, g\}$.

(2.13) For each of the following graphs G, draw their complement $\overline{G}$.

(a) C_5.

(b) P_4.

(c) K_5.

(d) $K_{3,3}$.

(2.14) Explain why the hypercube graph Q_n has order 2^n and is n-regular. What is the size of Q_n?

(2.15) Let T be a tree with order n and size m.

(a) If $m = 10$, then what is n?

(b) If $n = 8$, then what is m?

(c) Suppose that $n = 6$. Can T have the following degrees? 1, 2, 2, 3, 3, 4.

(2.16) Give examples of trees with exactly k leaves, where $k \geq 0$ is an integer.

(2.17) Determine the chromatic number of the following graphs.

(a) A cycle of length n, where $n \geq 4$.

(b) A path of length n, where $n \geq 1$.

(c) A tree.

(d) The hypercube Q_n, where $n \geq 1$.

(e) The wheel W_n, which consists of a cycle C_n plus an additional universal vertex.

(2.18) Determine the domination number of the following graphs.

(a) A complete graph of order n.

(b) A null graph of order n.

(c) A path of length n, where $n \geq 1$.

(d) The hypercube Q_3.

(2.19) (H) Prove that if you color the edges of K_6 either red or blue, there must be triangle whose edges are all red or all blue.

(2.20) (a) Describe all the graphs with chromatic number 1.

(b) Describe all the graphs with domination number 1.

(2.21) Draw all the spanning trees of K_4.

(2.22) For each even integer $n \geq 2$, give examples of graphs G with $\gamma(G) = n/2$.

(2.23) Suppose that G is a connected graph on 6 vertices x_i, $1 \leq i \leq 6$. If the degrees of five of the vertices x_i are: 1, 2, 3, 4, and 5, then what must be the degree of the 6th vertex be?

(2.24) Determine the chromatic number of the Heawood graph depicted in Figure 2.24.

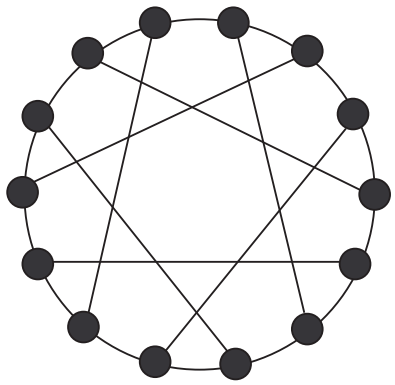


Figure 2.24: The Heawood graph.

(2.25) Prove that if a graph is bipartite, then it contains no cycles of odd length as subgraphs.

(2.26) (H) Let G be a graph with the property that every subgraph of G has a vertex of degree at most k, where k is fixed a positive integer. Show that $\chi(G) \leq k + 1$. (**Hint**: Use a greedy algorithm to color G.).

(2.27) (H) Show that in every graph with order at least two, there are at least two vertices of the same degree. (**Hint**: Consider cases when you have an isolated vertex or not.)

(2.28) In the following digraphs, determine the in-degree and out-degree of each vertex.

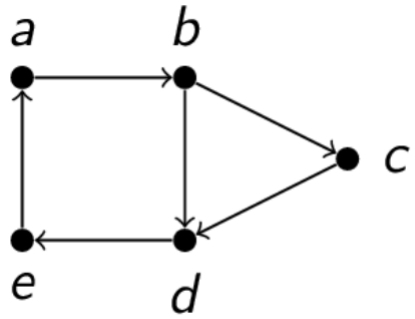


Figure 2.25: The digraph D_1.

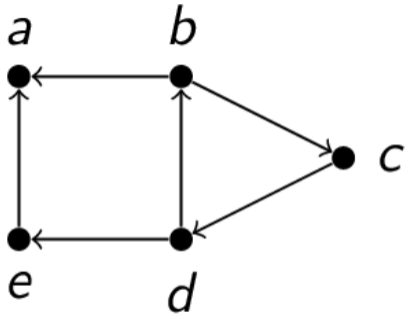


Figure 2.26: The digraph D_2.

(2.29) Draw all the directed graphs with 2 and 3 vertices.

(2.30) In a digraph, a vertex is a *source* if it has in-degree 0, and a *sink* if it has out-degree 0. Find the sources and sinks in the following digraphs.

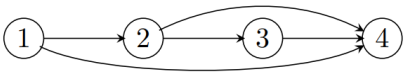


Figure 2.27: The digraph D.

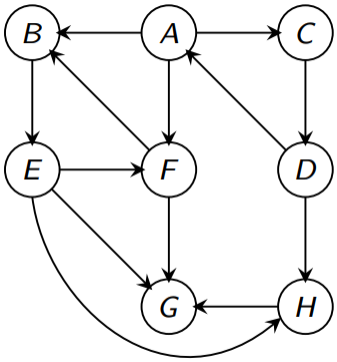


Figure 2.28: The digraph J.

2.8 Selected Answers and Hints

(2.3) (a) In a simple graph with order 6, no vertex can be degree 7. (b), (c), (d) There is an odd number of odd degree vertices. (e) In a simple graph with order 6, no vertex can be degree 6.

(2.5) (a) There must be an even number of odd degree vertices.

(2.6) 5

(2.8) (a) Consider the binary strings representing vertices. Color the ones with an even number of 1's by red, and the rest blue. (b), (c) Color an end vertex red, then alternate blue and red from there.

(2.10) The graph $\overline{G}$ has $\binom{7}{2} - 15 = 6$ edges.

(2.11) There are two components for each graph.

(2.14) By the First Theorem of Graph Theory, the size is $\frac{1}{2}n2^n$.

(2.15) (a) $n = 11$. (b) $m = 7$. (c) No, as there must be at least two leaves.

(2.16) The star graphs $K_{1,k}$ are examples of trees with $k \geq 0$ leaves.

(2.17) (a) If n is even, then $\chi(C_n) = 2$. Otherwise, it is 3. (b) 2. (c) 2. (d) 2. (e) If n is even, then $\chi(W_n) = 3$. Otherwise, it is 4.

(2.18) (a) 1. (b) n. (c) 2. (c) $\lceil n/3 \rceil$. (d) 2.

(2.19) Fix a vertex x in K_6. As $\deg(x) = 5$, there are at least 3 edges all one color, say red. Say the endpoints of those edges are a, b, c. If the edges between a, b, c are all blue, we are done. Otherwise, there is at least one red edge, say a, b. We then have that x, a, b, forms a red triangle.

(2.22) In the case $n = 2$, let $G = K_2$. If $n \geq 4$ and $n = 2m$, consider a *matching* graph, with m disjoint edges. We must dominate each edge with a single vertex, so the domination number is $m = n/2$.

(2.23) Vertex x_5 is universal, so x_1 is only adjacent to x_5. The vertex x_4 must be adjacent to every vertex except x_1, which means that x_2 is only adjacent to x_4, x_5. Hence, x_3 must be adjacent to x_4, x_5, x_6, and so $\deg(x_6) = 3$.

(2.24) 2.

(2.25) If G contains an odd cycle, then since an odd cycle has chromatic number 3, $\chi(G) \geq 3$.

(2.26) List the vertices as $x_1, x_2, \ldots, x_n$, so each x_i is adjacent to at most k vertices before it. Color x_1 by 1. Suppose that the first j vertices have been properly colored with at most $k+1$ colors, where $j \geq 1$ is fixed. The vertex x_{j+1} is adjacent to at most k vertices before it, and these vertices possess at most k colors. We are then free to properly color x_{j+1} with an unused color. This is the greedy algorithm. In this way, we may properly color each vertex from $x_1, \ldots, x_n$.

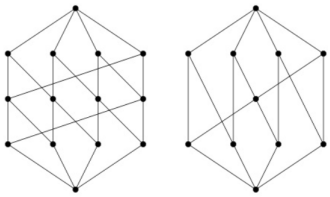
(2.27) Suppose G has order $n \geq 2$. If there is no isolated vertex, then the possible degrees are $1, 2, \ldots, n-1$. As there are n vertices and only $n-1$ possible degrees, some two vertices have the same degree; this is the Pigeonhole Principle that we will discuss in Chapter 3. If G contains an isolated vertex, then the possible degrees are $0, 1, 2, \ldots n-2$. Note that $n-1$ is not possible as there is an isolated vertex. The same argument with the Pigeonhole Principle holds in this case.

(2.28) In D_1, the in-degrees (from a to e): 1, 1, 1, 2, 1; out-degrees: 1, 2, 1, 1, 1. In D_2, the in-degrees: 2, 1, 1, 1, 1; out-degrees: 0, 2, 1, 2, 1.

(2.30) In D, the only source is 1, and the only sink is 4. In J, there are no sources, and G is the only sink.

Chapter 3

Relations and Functions



3.1 Introduction to Relations

Relations capture interactions between sets. This abstract notion underlies graphs, and also things like equivalence relations and partial orders. In this chapter, we will explore these topics, focusing mainly on binary relations. A special kind of binary relation is a function, which is a fundamental notion in mathematics.

Definition 3.1 For sets X and Y, a *binary relation* R from X to Y is a subset of $X \times Y$. Hence, R is a set of ordered pairs (x, y) with $x \in X$ and $y \in Y$. We write xRy if $(x, y) \in R$.
We say that R is a *binary relation on* X if $X = Y$; that is, $R \subseteq X \times X$.

Given a binary relation R from X to Y we can visualize it as an *arrow diagram*:

1. Draw X and Y as ovals, X on the left and Y on the right.
2. Put an arrow from $x \in X$ to $y \in Y$ if xRy.

For an example of an arrow diagram, see Figure 3.1. We may also visualize a relation R as a kind of directed graph, where there is a directed arrow from x to y if xRy. See Figure 3.2.

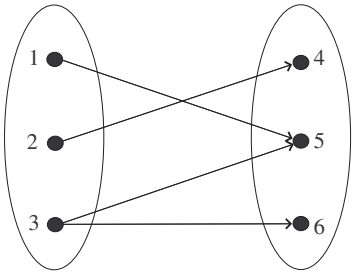


Figure 3.1: Arrow diagram of the relation $\{(1,5),(2,4),(3,5),(3,6)\}$.

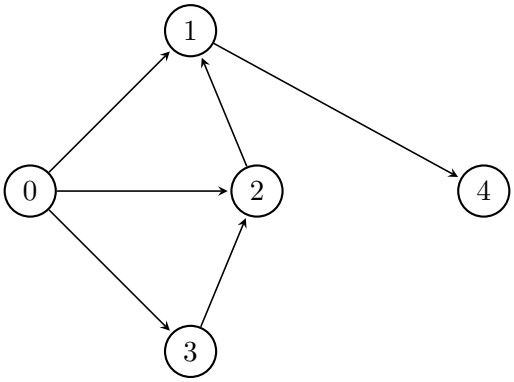


Figure 3.2: A relation as a directed graph with ordered pairs:

$$\{(0,1),(0,2),(0,3),(1,4),(2,1),(3,2)\}.$$

Graph theory was studied in the previous chapter, and we may think of graphs $G = (V, E)$ more formally as a kind of binary relation. In this case, the binary relation is the set of edges E, which has the *symmetry* property: for all $(x, y) \in E$, we have that $(y, x) \in E$. Symmetry and other properties of relations will be considered in the next section.

While our focus is on binary relations, we can generalize them as follows.

Definition 3.2 For sets X_i, where $1 \leq i \leq n$ define

$$\prod_{i=1}^{n} X_i = \{(x_1, x_2, \ldots, x_n) : \text{where } x_i \in X_i, 1 \leq i \leq n\}.$$

An n-ary *relation* R is a subset of $\prod_{i=1}^{n} X_i$.

Example 3.1 1. Consider the set $\mathbb{R}^n$, where the elements are n-dimensional n-tuples of real numbers. A relation S on $\mathbb{R}^n$ is given by

$$S = \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n : x_1 + x_2 + \ldots x_n = 0.\}$$

2. Let $X = \{a, b, c\}$, and let R be the 3-ary relation on $X \times X \times X$ defined by

$$\{(a, a, a), (a, a, b), (b, a, a), (c, a, a), (c, b, a)\}.$$

3.2 Properties of Relations

We study various properties that some, but not all, relations satisfy.

Definition 3.3 Let R be a binary relation on X.

1. The relation R is *reflexive* if for all $x \in X$, xRx.
2. The relation R is *symmetric* if for all $x, y \in X$, if xRy, then yRx.
3. The relation R is *transitive* if for all $x, y, z \in X$, if xRy and yRz, then xRz.

Note that not all relations have these properties. Further, any one of them is independent of the others, in the sense that there are relations that have one property but not the other two.

Example 3.2 1. Let $X = \{a, b, c\}$, and let $R = \{(b, b), (c, c), (a, b), (b, a)\}$. The relation R is neither reflexive or transitive, since (a, a) is not in R. However, it is symmetric.

2. Let X be the set of integers, and define the relation xSy if $y = kx$, for some integer k. We then have that the binary relation S is reflexive and transitive (do you see why?). However, it is not symmetric. For example, $2S4$, but $4S2$ is false.

3. Let X be the set of lines in the plane, and let P be the parallel relation: if L_1 and L_2 are lines, then $L_1 P L_2$ if L_1 and L_2 have the same slope (where vertical lines have infinite slope). We then have that P is reflexive, symmetric, and transitive.

In the case that all three properties hold, then we have a special kind of binary relation.

Definition 3.4 Let R be a binary relation on X. The relation R is an *equivalence relation* if it is reflexive, symmetric and transitive. We sometimes refer to the equivalence relation as (X, R).

Example 3.3

1. Let $X = \mathbb{R}$, and let R be equality: xRy if $x = y$. We then have that R is an equivalence relation.
2. The parallel relation on lines in the plane is an equivalence relation.
3. Let $m \geq 2$ be a fixed integer. For integers a, b, define $a \equiv b \pmod{m}$ if $a = b + km$, where $k \in \mathbb{Z}$. The relation $\equiv$ is an equivalence relation, as described in more detail in Chapter 5.

We next introduce an important concept stemming from equivalence relations.

Definition 3.5 Let R be an equivalence relation on X. For each $x \in X$, we denote the *equivalence class* of x, written $[x]$, by

$$[x] = \{y \in X : xRy\}.$$

Notice that an equivalence class is a set. We can interpret $[x]$ as all elements in a relation with x. Note that it may be that for distinct elements x and y that $[x] = [y]$.

Example 3.4

1. For the parallel relation on lines in the plane, the equivalence classes are lines with a given slope. Any two lines with the same slope give rise to the same equivalence class.
2. The equivalence classes of the $\equiv \pmod{2}$ relation correspond to the even and odd integers. For example, $[0] = [2] = [-8]$, while $[1] = [5] = [-17]$.

The following theorem describes the structure of equivalence classes.

Theorem 3.1 Let R be an equivalence relation on X, where we assume $X \neq \varnothing$.

1. For all $x \in X$, $[x] \neq \varnothing$.

2. If xRy, then $[x] = [y]$.

3. If $(x, y) \notin R$, then $[x] \cap [y] = \varnothing$.

Proof. For (1), note that $x \in [x]$.

For (2), let $a \in [x]$. We then have aRx. By transitivity with the fact that xRy, we have that aRy. Hence, $a \in [y]$, and so $[x] \subseteq [y]$. By an analogous argument, we have that $[y] \subseteq [x]$, and so $[x] = [y]$.

For (3), suppose that $(x, y) \notin R$, but $a \in [x] \cap [y]$. We then have that aRx and aRy. By symmetry, we have that xRa. By transitivity, we have that xRy. This contradiction finished the proof. □

The following theorem follows directly from Theorem 3.1.

Theorem 3.2 The equivalence classes of an equivalence relation R on a set X form a partition of X.

Hence, each equivalence relation naturally gives a partition. The converse is also true.

Definition 3.6 Let P be a partition of a set X. Define the binary relation R_P so that xRy if x and y are in the same part of the partition.

Example 3.5 Let $X = \{1, 2, 3\}$, and let $\{\{1, 2\}, \{3\}\}$ be a partition P of X. We then have that

$$R_P = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\},$$

which the reader may check is an equivalence relation. Note that the equivalence classes are $[1] = [2] = \{1, 2\}$ and $[3] = \{3\}$.

Every partition naturally gives rise to an equivalence relation. With this next result and Theorem 3.2, we have that equivalence relations and partitions are two ways of describing the same thing.

Theorem 3.3 If P is a partition of a set X, then R_P is an equivalence relation.

Because of Theorem 3.3, we call R_P the *equivalence relation induced by* P.

Proof of Theorem 3.3. Let $x, y, z \in X$. For reflexivity, note that x is in the part of P containing x. Hence, xR_Px.

For symmetry, if xR_Py, then x and y are in the same part of P. Hence, y and x are in the same part, and so yR_Px.

For transitivity, suppose that xR_Py and yR_Pz. We then have that x, y are in the same part and y, z are in the same part. It then follows that x, z are in the same part, and so xR_Pz.

As x, y, z were arbitrary, we have that R_P is an equivalence relation. □

3.3 Partial Orders

Partial orders provide one way of ranking objects. To define them, we define another property of relations.

Definition 3.7 Let R be a binary relation on a set X. We say that R is *antisymmetric* if xRy and yRx, then $x = y$.

The simplest example of an antisymmetric relation is $\leq$ on the real numbers. For real numbers x, y, if $x \leq y$ and $y \leq x$, then $x = y$.

Definition 3.8 A binary relation R on a set X is a *partial order* if R is reflexive, antisymmetric, and transitive. We call (X, R) a *partially ordered set* or a *poset*.

Example 3.6

1. Consider the relation $\leq$ on the natural numbers. The relation is reflexive, antisymmetric, and transitive. Hence, this is a partial order.
2. Let X be a nonempty set. The inclusion relation $\subseteq$ on the power set $\mathcal{P}(X)$ is a partial order.

Definition 3.9 In a poset (X, R), two elements x and y are *comparable* if either xRy or yRx. Otherwise, the elements are *incomparable*. A set of pairwise incomparable elements is called an *antichain*.

Definition 3.10 If (X, R) is a poset, and for all $x, y \in X$, xRy or yRx, then R is a *total order*, or *linear order*, or *chain*.

We now turn to graphical representations of posets. To form a *Hasse diagram* for a poset (X, R), we do the following.

1. Construct a digraph of the poset (X, R) so that all directed edges point up, except the loops.
2. Eliminate all loops.
3. Eliminate all directed edges that are redundant because of transitivity.
4. Eliminate the arrows on the directed edges.

Note that Hasse diagrams are distinct from drawings of graphs. Here are some examples of Hasse diagrams.

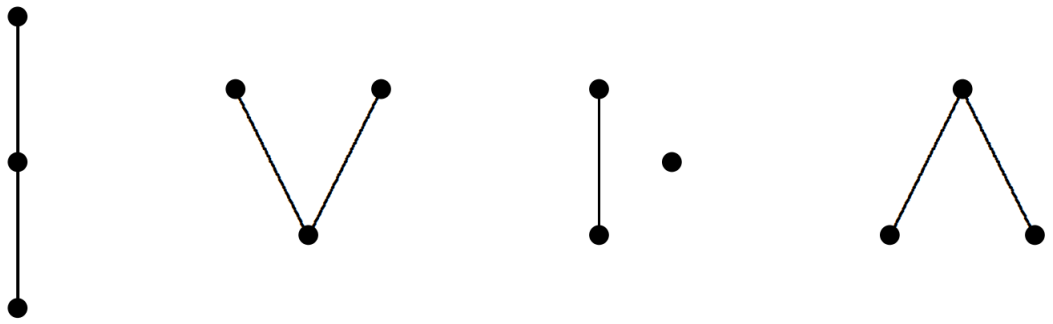


Figure 3.3: Four posets and their Hasse diagrams. The leftmost poset is a linear order with three elements. The remaining three posets have antichains with two elements.

We reference some *extremal* elements of posets.

Definition 3.11 Let R be a partial order on a set X.

1. An element u is a *least element* if for all $x \in X$, uRx.

2. An element v is a *greatest element* if for all $x \in X$, xRv.

3. An element u is a *minimal element* if there does not exist an element $x \in X \setminus \{u\}$ such that xRu.

4. An element v is a *maximal element* if there does not exist an element $x \in X \setminus \{v\}$ such that vRx.

Roughly put, a minimal element has nothing "below" it, while a maximal one has nothing "above" it. A least element is below every other element while a greatest element is above every other element.

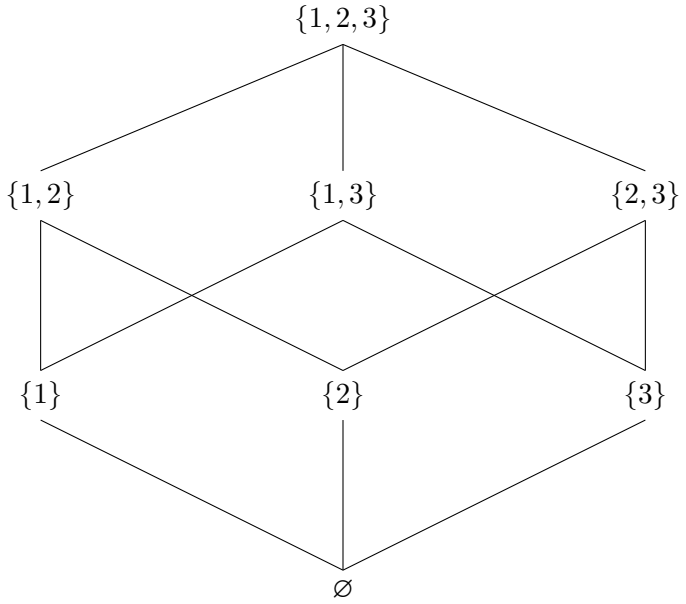


Figure 3.4: The Hasse diagram of the inclusion poset on subsets of $\{1, 2, 3\}$. The empty subset is the least element, and $\{1, 2, 3\}$ is the greatest element.

The following collects some facts about these extremal elements.

Theorem 3.4 Let R be a partial order on a set X.

1. If u is the least element of X, then u is a minimal element of X.

2. If v is the greatest element of X, then v is a maximal element of X.

3. Every least or greatest element of X is unique.

Proof. We prove (1) and leave the analogous proof of (2) to the reader. Suppose that there is an element $x \in X$, such that xRu. As u is a least element, we must have that $x = u$.

For (3), we show that a greatest element is unique; the proof for a least element is analogous. Suppose that v and v' are greatest elements. By definition, we have that vRv' and $v'Rv$. By antisymmetry, we have that $v = v'$. □

We finish the section with the following fact about finite posets.

Theorem 3.5 If (X, R) is a finite nonempty poset, then it has minimal and maximal elements.

Proof. We present the proof for minimal elements, with the analogous maximal proof omitted.

Suppose for a contradiction that there is no minimal element. Hence, for $x_1 \in X$, there is an $x_2 \neq x_1$ such that $x_2 R x_1$. As x_2 is not minimal, there is an $x_3 \neq x_2, x_1$ such that $x_3 R x_2$. Proceeding in this way, we find an infinite total order:

$$\ldots x_3 R x_2 R x_1.$$

This contradicts that (X, R) is finite. □

The finiteness condition is essential in Theorem 3.5. For example, consider the $\leq$ relation in $\mathbb{Z}$. There are no maximal or minimal elements in this poset.

3.4 Functions

Functions are a special kind of binary relation.

Definition 3.12 A *function* f is a binary relation on sets X and Y satisfying: for each $x \in X$, there is a unique $y \in Y$ so that xfy. We write $f(x) = y$ for xfy and say "f of x equals y."
We write $f : X \to Y$, and refer to X as the *domain* of f and Y as the *co-domain* of f.

Example 3.7 1. If $X = \{2, 3, 4\}$ and $Y = \{5, 6, 7\}$, then define the function $f(2) = 5$, $f(3) = 6$, and $f(4) = 7$. We may represent functions such as this by arrow diagrams, as in Figure 3.5. Note that the binary relation Figure 3.1 is not a function, as 3 is related to two elements.

2. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3 + 5$. This is an example of a cubic polynomial function defined on the real numbers.

3. Let $X = \mathcal{P}(\{a, b, c, d\})$ and $Y = \mathbb{N}$. Define $h(A) = |A|$. For example, $h(\varnothing) = 0$ and $h(\{a, c, d\}) = 3$.

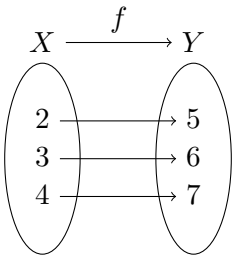


Figure 3.5: The arrow diagram for the function $f : X \to Y$ in Example 3.7 (1).

Definition 3.13 Let $f : X \to Y$ be a function. The *range* of f is

$$\{y \in Y : \text{ for some } x \in X, f(x) = y\}.$$

The range is a subset of the co-domain, which may be a proper subset.

Example 3.8 1. Let $f : [0, \infty) \to \mathbb{R}$ be defined by $f(x) = \sqrt{x}$. The range of f is then equal to the nonnegative real numbers.

2. If $X = \{1, 2, 3\}$ and $Y = \{5, 6, 7\}$, then define the function $g(1) = 6$, $g(2) = 6$, and $g(3) = 5$. The range of f equals $\{5, 6\}$.

As functions are so general, it is helpful to specify certain key properties about them.

Definition 3.14 Let X and Y be sets. We say a function $f : X \to Y$ is *injective* if for all $x, y \in X$, such that $x \neq y$, we have that $f(x) \neq f(y)$. Injective functions are also called *one-to-one* or *injections*.

By contraposition, a function f is injective if for all $x, y \in X$, if $f(x) = f(y)$, then $x = y$.

Example 3.9

1. Let $X = Y = \{1, 2, 3\}$ and $f : X \to X$ be defined by $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$. We then have that f is injective.
2. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3 + 5$. The function g is injective, since if $x^3 + 5 = y^3 + 5$, then $x = y$.
3. Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$. The function h is not injective, since $f(2) = f(-2)$.

Definition 3.15 Let X and Y be sets. We say a function $f : X \to Y$ is *surjective* if for all $y \in Y$, there exists $x \in X$ such that $f(x) = y$. Surjective functions are also called *onto* or *surjections*.

Recall that the range of a function is a subset of its co-domain. From the definition, a function is surjective if its range equals its co-domain.

Example 3.10

1. Let $X = Y = \{x, y, z\}$ and $f : X \to X$ be defined by $f(x) = x$, $f(y) = z$, and $f(z) = y$. We then have that f is surjective.
2. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^5 + 5$. The function g is surjective, since if $y = x^5 + 5$, we can solve for x as $x = (y - 5)^{1/5}$.
3. Let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = x^2$. The function h is not surjective, since -1 is not in the range of f.

The final definition in this section brings together the concepts of injective and bijective functions.

Definition 3.16 Let X and Y be sets. A function $f : X \to Y$ is *bijective* if it is both injective and surjective. Bijective functions are also called *bijections*. If $X = Y$, then we call this a *permutation*.

Example 3.11

1. Let $X = Y = \{1, 2, 3, 4, 5\}$ and $h : X \to X$ be defined by $h(1) = 1$, $h(2) = 3$, $h(3) = 5$, $h(4) = 2$, and $h(5) = 4$. We then have that h is bijective.

2. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^5$. The function g is an injective and surjective, and so it is a bijection.

3. The $h : [0, \infty) \to \mathbb{R}$ be defined by $h(x) = \sqrt{x}$ is not a bijection, as it is not surjective: the range of h does not equal $\mathbb{R}$.

Bijective functions are useful when discussing cardinality. An alternative approach to two sets X and Y having the same cardinality is that there is some bijection $f : X \to Y$.

3.5 Exercises

(3.1) Let $X = \{1, 2, 3, 4\}$. Draw the directed graphs of the following binary relations on X.

(a) $R = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$.

(b) $R = \{(2, 1), (1, 2), (1, 3), (3, 2), (4, 2), (4, 3), (4, 4)\}$.

(c) $R = \{(2, 2), (3, 2), (3, 3), (4, 2), (4, 3)\}$.

(3.2) Define the binary relation R on $\mathbb{N}$ by xSy if $x - y = 3k$ for some integer k. Describe the following sets.

(a) The set of all integers related by S to 0.

(b) The set of all integers related by S to 1.

(c) The set of all integers related by S to 2.

(3.3) Define the binary relation $|$ on $\mathbb{N}^+$ by $x|y$ if $y = xk$, for some integer k.

(a) Show that for all $x \in \mathbb{N}^+$, $x|x$.

(b) Show that for all $x, y \in \mathbb{N}^+$, $x|y$ and $y|x$, then $x = y$.

(c) Show that for all $x, y, z \in \mathbb{N}^+$, $x|y$ and $y|z$, then $x|z$.

(3.4) Let X be a set with n elements, where n is a positive integer. How many possible binary relations are there on X? (**Hint**: Count the subsets of $X \times X$.)

(3.5) If $X = \{1\}$, then describe the unique, nonempty binary relation defined on X.

(3.6) Give an example of a binary relation defined on $\{0, 1, 2\}$ that is transitive, but not reflexive and not symmetric.

(3.7) Give an example of a binary relation defined on $\{0, 1, 2, 3\}$ that is reflexive, but not symmetric and not transitive.

(3.8) Give an example of a binary relation defined on $\{0, 1, 2, 3, 4\}$ that is symmetric, but not reflexive and not transitive.

(3.9) Let X be a nonempty set. Explain why a binary relation defined on X containing a single ordered pair is always transitive.

(3.10) Let X be a set with at least two elements and $R = X \times X$. Show that R is an equivalence relation but not a partial order.

(3.11) Which of the following relations are equivalence relations on the given set X? If the relations are equivalence relations, then describe the equivalence classes.

(a) $\{(1,1),(2,2),(1,2)\}$ on $X = \{1,2\}$.

(b) $\{(1,1),(2,2),(1,2),(2,1)\}$ on $X = \{1,2\}$.

(c) $\{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3)\}$ on $X = \{1,2,3\}$.

(d) $\{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$ on $X = \{1,2,3\}$.

(3.12) Let $X = \{a, b, c, d, e, f, g\}$, and let $\{\{a, c, e\}, \{b\}, \{d, f, g\}\}$ be a partition P of X. Determine the equivalence relation induced by R_P.

(3.13) Let R be an equivalence relation. Prove that if $x, y \in X$ and $x \in [y]$, then $[x] = [y]$.

(3.14) Let X be the set of ordered pairs of positive integers, and let R be defined by $(x, y)R(u, v)$ if $x + v = u + y$.

(a) Show that (X, R) is an equivalence relation.

(b) What are the equivalence classes of R? Explain your work.

(3.15) Define the relation R on $X = \mathbb{R} \setminus \{0\}$ by xRy if $\frac{x}{y} \in \mathbb{Q}$. Explain why R is an equivalence relation.

(3.16) Define the relation R on $X = \mathbb{R} \setminus \{0\}$ by xRy if $x - y \in \mathbb{Z}$.

(a) Show that (X, R) is an equivalence relation.

(b) What are the equivalence classes of R? Explain your work.

(3.17) Define the relation R on $X = \mathbb{Q}$ by xRy is $3(x - y) \in \mathbb{Z}$.

(a) Show that (X, R) is an equivalence relation.

(b) What are the equivalence classes $[0]$ and $[\frac{1}{3}]$?

(3.18) Which of these relations on $\{1, 2, 3, 4\}$ are partial orderings?

(a) $\{(1,1),(2,2),(3,3),(4,4)\}$.

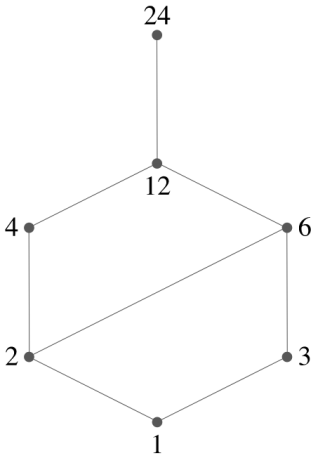
(b) $\{(1,1),(2,2),(3,1),(3,3),(3,4),(4,3),(4,4)\}$.

(c) $\{(1,2)\}$.

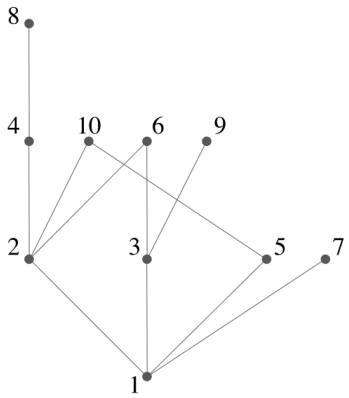
(d) $\{(1,1),(2,2),(3,3),(4,4),(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}$.

(3.19) Draw the Hasse diagram of the poset $(\{1,2,3,4,5,6,7,8,9,10,11\},R)$, where R is the divides relation $|$. What are the minimal and maximal elements?

(3.20) In the following Hasse diagrams, determine all extremal elements, if they exist: least, greatest, minimal, and maximal elements.



(a) The poset P.



(b) The poset Q.

(3.21) Draw the Hasse diagram for the poset $(\mathcal{P}(X),\subseteq)$, where $X=\{1,2,3,4\}$.

(3.22) Let X be a set of order n, where n is a positive integer. Find a partial order on X, where each element is both maximal and minimal.

(3.23) Let $X=\{a,b,c\}$. Describe all the partial orders on X where a is a greatest element and there is an antichain of cardinality two.

(3.24) Explain why each of the following functions is injective.

(a) $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=e^x$.

(b) $g:\mathbb{R}\to\mathbb{R}$ defined by $g(x)=x^3$.

(c) $h:\mathbb{R}\to\mathbb{R}$ defined by $h(x)=37x+14$.

(3.25) Explain why each of the following functions is **not** injective.

(a) $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=2x^2+12$.

(b) $g:\mathbb{R}\to\mathbb{R}$ defined by $g(x)=\sin(x)$.

(c) $h:\mathbb{R}\to\mathbb{R}$ defined by $h(x)=|x|$.

(3.26) Explain why each of the following functions is surjective.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \tan(x)$.

(b) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = 5x^3 + 7$.

(c) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = 5x + 4$.

(3.27) Explain why each of the following functions is **not** surjective.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$.

(b) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \sin(x)$.

(c) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = -|x|$.

(3.28) Explain why each of the following functions is bijective.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 10x + 7$.

(b) $g : \mathbb{R} \to \mathbb{R}^+$ defined by $g(x) = e^x$.

(c) $h : \mathbb{R}^+ \to \mathbb{R}$ defined by $h(x) = \log x$.

(3.29) Explain why each of the following functions is **not** bijective.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + x$.

(b) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \tan(x)$.

(c) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = e^x + 5$.

(3.30) Describe a bijection $f : \mathbb{N} \to \mathbb{Z}$. (**Hint**: Consider how to define f on odd and even nonnegative integers.)

3.6 Selected Answers and Hints

(3.2) For $i = 0, 1, 2$, the integers related by S to i are those that have remainder i when divided by 3.

(3.3) For (a), $x = 1x$. For (b), if $x = ky$ and $y = jx$, for integers j, k, then $kj = 1$, so $k = j = 1$ and $x = y$. For (c), if $y = kx$, and $z = jy$, then $z = (kj)x$. Hence, $x|z$.

(3.4) We have that $|X \times X| = n^2$. As a relation on X is a subset of $X \times X$, the number of binary relations on X is 2^{n^2}. Note that this includes the empty relation, with no ordered pairs.

(3.5) The only nonempty relation on $X = \{1\}$ is $\{(1, 1)\}$.

(3.6) There are many possible examples. One would be $\{(1, 2)\}$.

(3.7) One example would be $\{(0, 0), (1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\}$.

(3.8) One example would be $\{(1, 1), (2, 2), (3, 1), (1, 3)\}$.

(3.9) Suppose that R is the single pair $\{(a, b)\}$, for some a, b. As there is nothing to compare (a, b) with, the relation is transitive.

(3.10) As all pairs of elements of X are present, $X \times X$ is an equivalence relation. To see that this relation is not antisymmetric, suppose two distinct elements of X are a, b. We then have that $(a, b), (b, a) \in X \times X$, but $a \neq b$.

(3.11) The relations (b) and (d) are equivalence relations. In (b), the equivalence class is $[1] = [2] = \{1, 2\}$. In d), we have $[1] = [2] = [3] = \{1, 2, 3\}$.

(3.12) We have that $R_P = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (g, g), (a, c), (c, a), (a, e), (e, a), (c, e), (e, c), (d, f), (f, d), (d, g), (g, d), (f, g), (g, f)\}$.

(3.13) Let $u \in [x]$. We then have that uRx. As $x \in [y]$, we have that xRy. By transitivity, we have that uRy, so $u \in [y]$. Hence, $[x] \subseteq [y]$. The argument that $[y] \subseteq [x]$ is similar.

(3.14) (b) We have that $(x, y)R(u, v)$ if $x - y = u - v$. The equivalence class $[(x, y)]$ consists of all pairs (u, v) whose difference $u - v$ equals $x - y$.

(3.15) For transitivity, if xRy and yRz, then $\frac{x}{y}, \frac{y}{z}$ are rationals. We then have that $\frac{x}{y} \cdot \frac{y}{z} = \frac{x}{z}$ is rational.

(3.16) (a) For transitivity, if xRy and yRz, then $x-y, y-z \in \mathbb{Z}$. By adding, we have that $x-z \in \mathbb{Z}$. (b) For a nonzero real number x, we have that $[x]$ is the set of all nonzero real numbers whose decimal part equals the decimal part of x. For example, $3.1414 \in [17.1414]$.

(3.17) (a) For transitivity, if xRy and yRz, then $3(x-y), 3(y-z) \in \mathbb{Z}$. By adding, we have that $3(x - z) \in \mathbb{Z}$. (b) $[0] = \{x \in \mathbb{Q} : 3x \in \mathbb{Z}\}$, $[\frac{1}{3}] = \{x \in \mathbb{Q} : 3x - 1 \in \mathbb{Z}.\}$

(3.18) (a) and (d) are partial orders.

(3.19) The unique minimal element is 1. The maximal elements are 6, 7, 8, 9, 10, and 11.

(3.20) In P, the least and minimal element is 1 and the greatest and maximal element is 24. In Q, the least and minimal element is 1, and the maximal elements are 6, 7, 8, 9, and 10.

(3.22) Let the poset consist of the n distinct elements of X, with no pairs in the relation. This is then an n-element antichain, where each element is both minimal and maximal.

(3.23) There is only one such poset: $\{(a,a),(b,b),(c,c),(b,a),(c,a)\}$.

(3.24) Set the functions equal and solve. In (a), $f(x) = f(y)$ implies that $e^x = e^y$. By taking logarithms on both sides, derive that $x = y$.

(3.25) In each part, find one pair of distinct real numbers a, b such that function values on a and b are equal. Note that there are infinitely many counterexamples to show that each these three functions are not injective. (a) $f(1) = f(-1)$. (b) $g(0) = g(\pi)$. (c) $h(-1) = h(1)$.

(3.26) (b) Set $y = 5x^3 + 7$, and solve to give $x = (y-7)^{1/3}$.

(3.27) For each item, show the range is not the entire co-domain. For example, in (b), the range is $[-1, 1]$.

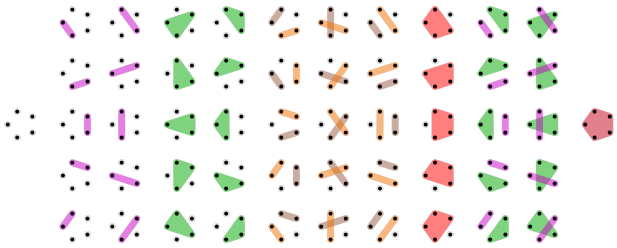
(3.28) For each item, show the given function is injective and surjective either directly or using previous exercises.

(3.29) (a) is neither injective nor surjective. (b) is not injective. (c) is not surjective.

(3.30) For $x \in \mathbb{N}$, we defined $f(x) = x/2$ if x is even, and $f(x) = -((x+1)/2)$ if x is odd.

Chapter 4

Combinatorics



4.1 Introduction

Counting is fundamental. We learn to count from an early age, so it comes like second nature. In our everyday lives, we count things such as coins in our pocket, votes on election night, or the number of likes on social media posts. Children count with their fingers, and as they mature, they learn to do so in more sophisticated ways.

In mathematics, counting takes on a life of its own through the field of *combinatorics*, which is the science and art of counting. Counting discrete structures brings many subtleties. We explore combinatorics in the present chapter, focusing on the sum and product rules of counting, the Pigeonhole Principle, and the Principle of Inclusion-Exclusion. We also discuss combinations and Pascal's triangle.

4.2 Sum Rule

We begin with a basic rule of counting.

Theorem 4.1 (Sum rule) Suppose that we are given disjoint sets X and Y. If $|X| = m$, and $|Y| = n$, then

$$|X \cup Y| = m + n.$$

The sum rule is an intuitive one: if X and Y do not intersect, then their number of elements is the sum of the number of elements from each set.

Example 4.1

1. There are 26 letters in the English alphabet and 10 digits. The sum rule tells us there are $26+10 = 36$ choices for a single letter or digit.
2. Suppose there are 13 pieces of white chalk and 8 pieces of red chalk. There are then $13 + 8 = 21$ total pieces of chalk.
3. Let S be the set of all alphanumeric strings (that is, strings whose entries are one of the letters of the English alphabet, or the digits 0, 1, 2, ..., 9) of length 2 that start with either 0 or J. We select the second element of the string in either case, so there are 36 possibilities in each case. The sum rule tells us there are $36 + 36 = 72$ strings in S.

The sum rule generalizes if we have more than two disjoint sets.

Theorem 4.2 (Generalized sum rule) If we are given pairwise disjoint sets X_i, where $1 \leq i \leq m$ so that $|X_i| = m_i$, then

$$\left|\bigcup_{i=1}^{m} X_i\right| = \sum_{i=1}^{m} |X_i|.$$

Example 4.2 If we have three each of apples, oranges, lemons, and cherries, then we have 12 pieces of fruit in total.

If the sets X and Y are not disjoint, then the sum rule does not apply.

Example 4.3 Let $X = \{1, 2, 3\}, Y = \{2, 3, 4\}$. If we form $X \cup Y$, then note that we count each part, where 2 and 3 are counted twice. However, the cardinality of the union is 4. We can think of this as $3 + 3 - 2$, where we are subtracting off 2 for the intersection of the sets.

Counting the union when the sets X_i are not disjoint becomes subtle. One simple but useful observation is the following.

Theorem 4.3 (Boole's inequality) For any sets A_i, we have that

$$\left|\bigcup_{i=1}^{m} A_i\right| \leq \sum_{i=1}^{m} |A_i|.$$

To give a precise count of the number of elements of the union, we need the following identity.

Theorem 4.4 (Principle of Inclusion-Exclusion) Let $X_1, X_2, \ldots, X_n$ be finite sets. We then have that

$$\begin{aligned}
\left|\bigcup_{1\leq i\leq n} X_i\right| &= |X_1 \cup X_2 \cup \cdots \cup X_n| \\
&= |X_1| + |X_2| + \cdots + |X_n| \\
&- |X_1 \cap X_2| - |X_1 \cap X_3| - \cdots - |X_{n-1} \cap X_n| \\
&+ |X_1 \cap X_2 \cap X_3| + |X_1 \cap X_2 \cap X_4| + \ldots \\
&+ |X_{n-2} \cap X_{n-1} \cap X_n| + (-1)^{n-1}|X_1 \cap X_2 \cap \cdots \cap X_n|.
\end{aligned}$$

The Principle of Inclusion-Exclusion may look daunting at first, but the expression has a simple structure that is straightforward to remember and apply. First, take the sum of the cardinalities of the sets, as you would in a disjoint union. We then subtract off the cardinalities of the pairwise intersections of the sets, then add the cardinalities of the triple intersections, and so on. The signs depend on the parity of the number of sets intersected: if there are i sets intersecting, then we add $(-1)^{i-1}$ to the sum of the cardinalities of the intersections. For example, if there is only one set in the intersection, then the sign is positive. If there are two, then it is negative. If there are 17, then the sign is positive.

Example 4.4 Suppose that 40 people own a car, 60 own a bike, and 50 take public transit. Suppose further that 25 own both a car and bike, 30 own a bike and take public transit, and 35 own a car and take public transit. There are 20 people who own a car and bike, and also take public transport. How many people have at least a car, bike, or take public transit?

We set X_1 to be the set of people with a car, X_2 to be the people with a bike, and X_3 be the people who take public transit. We are being asked for the cardinality of the

union of the sets X_1, X_2, and X_3. By the Principle of Inclusion-Exclusion, we have that $X_1 \cup X_2 \cup X_3$ equals

$$40 + 60 + 50 - 25 - 30 - 35 + 20 = 80.$$

Hence, the number of people who have at least a car, bike, or take public transport is 80.

4.3 Product Rule

The next counting principle is another basic counting principle.

Theorem 4.5 (Product rule) If a task X can be performed in m ways and a task Y can be performed in n ways, then we have that X and Y can be performed together in mn ways.

We may think of the product rule in terms of sets, where we count the Cartesian product $X \times Y$. In the setting of sets, the product rule says that

$$|X \times Y| = |X||Y|.$$

See Figure 4.1 for an example.

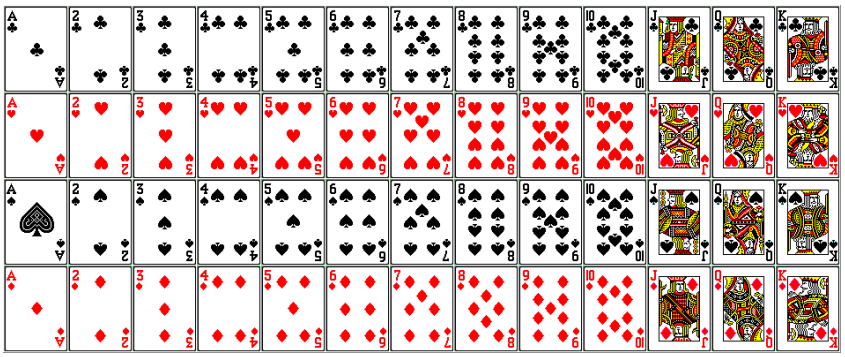


Figure 4.1: A standard deck of cards. There are four suits (clubs, diamonds, spades, and hearts), each with 13 cards. By the product rule there are $4 \times 13 = 52$ cards.

Example 4.5

1. The number of two digit numbers, including those that start with 0, is: $10 \cdot 10 = 100$, as there are 10 choices for each digit.

2. The number of three letter words (even the nonsense ones) that start with A is

$26 \cdot 26$, as there are 26 letters possible for each of the second and third letter.

3. If there are ten engineering students and each must take 6 elective courses, then there are $10 \cdot 6 = 60$ possibilities of matching students with courses.

The product rule applies to any number of tasks.

Theorem 4.6 (Generalized product rule) If tasks X_i can be performed in m_i ways, where $1 \leq i \leq n$, then we have

$$m_1 m_2 \cdot \cdots \cdot m_n$$

ways the tasks can be performed together.

Example 4.6

1. The number of 3-digit numbers not including 0 is 9^3.
2. The number of words (even nonsensical ones) of length 8 is 26^8.
3. Suppose we have a complete graph G of order 4 with vertices labeled 1, 2, 3, and 4. If we assign five colors to the vertices, then we can color the vertices in 5^4 distinct ways.

4.4 The Pigeonhole Principle

The Pigeonhole Principle is a simple but powerful tool when counting objects.

Theorem 4.7 (The Pigeonhole Principle) If n sets are assigned m colors, with $n > m$, then at least two of the sets have the same color.

The colors here can be any given property, so long as these are distinct. The name comes from the analogy of n pigeons occupying m holes. If there are more pigeons than holes, then there are at least two pigeons in some hole. See Figure 4.2. Note that the Pigeonhole Principle does not specify which sets have the same color, but just that some pair does. In that sense, it is an existential principle.

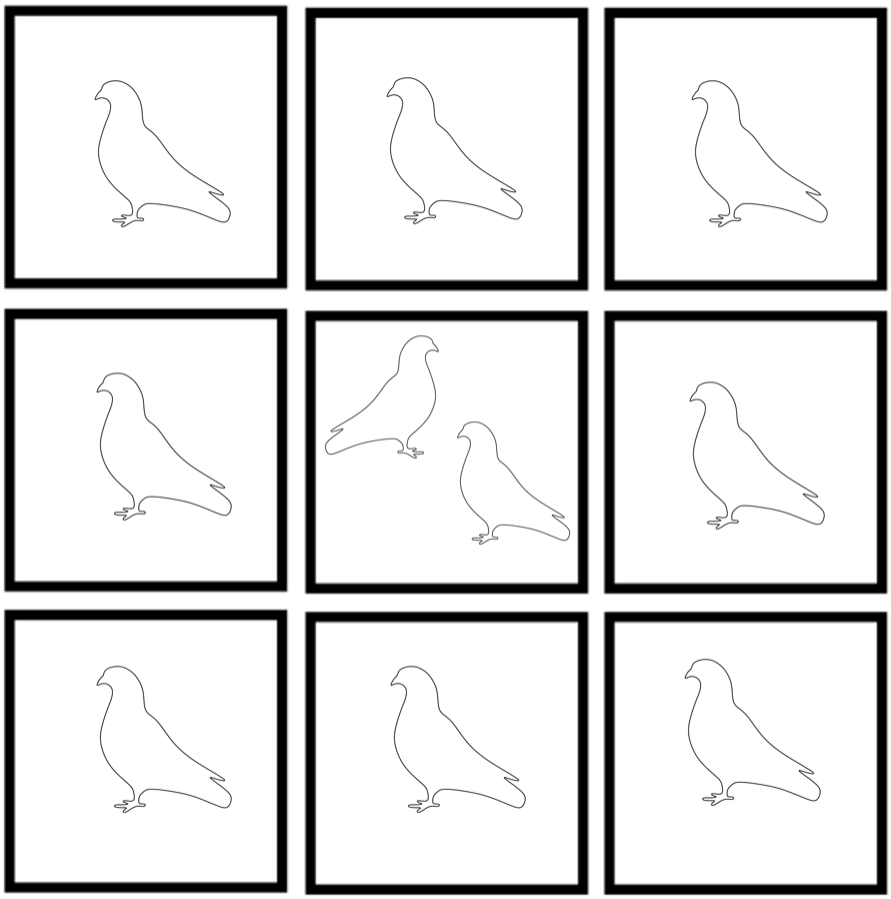


Figure 4.2: Ten pigeons in nine holes.

Example 4.7 1. If you choose a set of three nonnegative integers, then two of them are both even or both odd.

2. If you schedule 53 tasks in a calendar year, then there is a week with two of the tasks.

3. In a set of $2^n + 1$ binary strings of length n, two of them are equal.

Theorem 4.8 (General Pigeonhole Principle) If n sets are assigned with m colors with $n \geq m$, then at least $\lceil n/m \rceil$ sets have the same color.

Example 4.8 Consider 101 nonnegative integers. The General Pigeonhole Principle tells us that at least $\lceil 101/2 \rceil = 51$ are either even or odd. We think of even and odd as the two colors.

4.5 Permutations

Suppose that we choose an ordered sequence of r numbers from $\{1, 2, \ldots, n\}$ so each entry in the sequence is distinct. There are n choices for the first entry, then $n-1$ many choices for the second. Continuing in this way, we see that there are

$$n(n-1)(n-2)\cdots(n-r+1)$$

sequences of length r in which all elements are distinct. We call such a sequence a *permutation*.

Definition 4.1 For a positive integer n, we define n *factorial*, written $n!$, as

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

Definition 4.2 We denote the number of permutations of length r coming from $\{1, 2, \ldots, n\}$ by

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

Example 4.9

1. You must create a password with 8 letters and no repetitions of the letters. We then have there are $P(26, 8) = 26 \cdot 25 \cdot \cdots \cdot 19$ possible passwords.
2. A group of 1000 mathematicians must elect a president, a vice president, and an executive director to their society. We then have that there are $P(1000, 3)$ ways that the leadership positions can be filled.

4.6 Combinations

Definition 4.3 Let n and r be nonnegative integers, with $r \leq n$. We define the *combination*, written $\binom{n}{r}$, to be the number of subsets of a set of size n each with cardinality r. We say "n choose r."

Combinations are useful for counting ways of choosing a set of objects from within a larger set. For example, if we consider a complete graph K_n, each pair of distinct vertices is adjacent.

Hence, there are $\binom{n}{2}$-many edges in K_n.

Example 4.10

1. If we choose three apples from a set of four, then there are $\binom{4}{3} = 4$ choices.
2. If we choose one integer from a set of ten integers, then there are $\binom{10}{1} = 10$ choices.
3. If we choose 11 pens from a set of 11 pens, then there is only $\binom{11}{11} = 1$ choice of doing that task.

Note that $\binom{n}{r}r! = P(n,r)$. To see this, note that if we were trying to count $P(n,k)$ we could first choose the r elements to be in our permutation, then we could order them in $r!$ ways. This gives the important formula:

$$\begin{aligned}\binom{n}{r} &= \frac{n!}{(n-r)!r!} \\ &= \frac{(n)(n-1)(n-2)\cdots(n-r+1)}{r!}.\end{aligned}$$

There are special cases of combinations as captured in the following.

Theorem 4.9 (Basic properties of combinations) Let n be an integer.

1. $\binom{n}{0} = \binom{n}{n} = 1$.
2. $\binom{n}{1} = \binom{n}{n-1} = n$.
3. $\binom{n}{2} = \frac{n(n-1)}{2}$.

Proof. For (1), note that the only subset of cardinality 0 is the empty set; hence, $\binom{n}{0} = 1$. The only subset of cardinality n in an n-element set is itself, so $\binom{n}{n} = 1$.

For (2), there are exactly n singletons, and so $\binom{n}{1} = n$. If we take away exactly one element from an n-element set, then there are n ways to do this, and so $\binom{n}{n-1} = n$.

For (3), from the formula for combinations with $r = 2$, we have that

$$\binom{n}{2} = \frac{(n)(n-1)}{2} = \frac{n^2-n}{2},$$

as desired. □

Note that item (1) captures the special case of $\binom{0}{0} = 1$.

Combinations have a recursive quality that is captured in the following theorem.

Theorem 4.10 (Recursive property of combinations) For integers $n \geq 1$ and $r \leq n$, we have that

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

Proof. We give a *combinatorial proof*; that is, we count rather than expand the combinations as factorials. Let S be a set with n elements and fix $x \in S$. The number of subsets of cardinality r of S not including x is $\binom{n-1}{r}$. The number of subsets of cardinality r of S including x is $\binom{n-1}{r-1}$ as we have only $n-1$ elements to choose from, and x eliminates one element to choose, leaving $r-1$.

When choosing an r-element set X from S, the set X must either contain x or not, and both cases are disjoint. Hence, the sum rule tells us that there are $\binom{n-1}{r-1} + \binom{n-1}{r}$ choices for S, and so

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

as desired. □

Another important property of combinations is their symmetry.

Theorem 4.11 (Symmetry property of combinations) For integers $n \geq 0$ and $r \geq 0$, with $r \leq n$, we have that

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

Proof. We give a combinatorial proof. Suppose we choose an r-element subset X in an n-element set Y. That choice is equivalent to choosing X^c in Y. In other words, choosing a set is equivalent to choosing its complement. Hence, $\binom{n}{r} = \binom{n}{n-r}$. □

We also have the following identity.

Theorem 4.12 (Sum of squares of combinations) For $n \geq 0$, we have that

$$\sum_{r=0}^{n} \binom{n}{r}^2 = \binom{2n}{n}.$$

Proof. The binomial coefficient $\binom{2n}{n}$ counts the number of binary strings of length $2n$ with exactly n zeroes. We consider a different way of counting such strings.

If we consider a binary string of length $2n$ with exactly n zeroes, then it has r zeroes in the first n bits and $n-r$ in the second n bits. Therefore, we can count the binary strings of length $2n$ with exactly n zeroes in a different way, by partitioning them into how many such zeroes are in the first n bits. By the sum rule, the number of such strings is

$$\sum_{r=0}^{n} \binom{n}{r}\binom{n}{n-r}.$$

By the symmetry property of combinations, $\binom{n}{r} = \binom{n}{n-r}$, so this summation equals

$$\sum_{r=0}^{n} \binom{n}{r}^2,$$

and the proof follows. □

An important use of combinations is in expanding polynomial expressions.

Theorem 4.13 (Binomial Theorem) Let n be a nonnegative integers and let x, y be variables.

$$\begin{aligned}(x+y)^n &= \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r \\ &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}x \cdot y^n + \binom{n}{n}y^n.\end{aligned}$$

Example 4.11 We compute that $\binom{5}{0} = 1$, $\binom{5}{1} = 5$, and $\binom{5}{2} = 10$. Using this and the symmetry property of combinations, we find that

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

Example 4.12 1. If we set $x = y = 1$, in the Binomial Theorem, then we obtain the following formula:

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}.$$

We may see this identity combinatorially, as 2^n represents the number of subsets of an n-element set. By the sum rule, the right-side of the equation is the number of ways of choosing an r-element set, where r is an integer between 0 and n.

2. By choosing $x = 11, y = 1$ in the Binomial Theorem, we obtain the following formula that is not obvious otherwise:

$$12^n = \sum_{r=0}^{n} \binom{n}{r} 11^{n-r}.$$

4.7 Pascal's Triangle

We finish with *Pascal's triangle*, which is an arrangement of the combinations that makes them simple to remember. The rows of Pascal's triangle are indexed by nonnegative integers: $0, 1, 2, 3, \ldots$ In the nth row, we have each of $\binom{n}{r}$, where $1 \leq r \leq n$, where the values of r increase from left to right. We note that Pascal's triangle is also referred to as *Yanghui's triangle* or *Khayyam's triangle*.

The following are the first seven rows of Pascal's triangle.

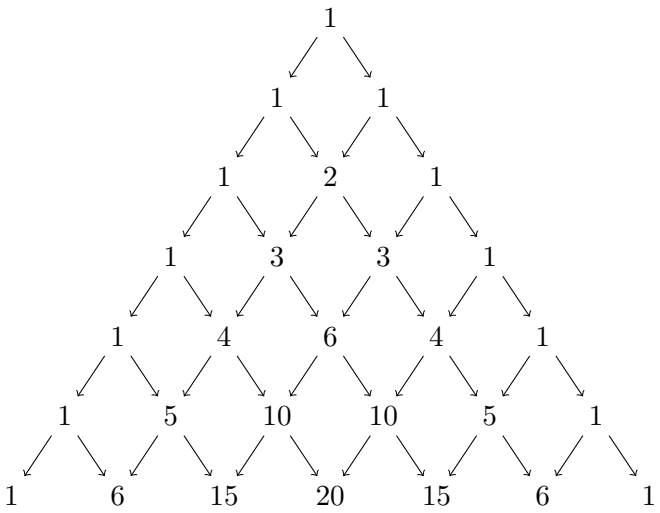
$$\begin{array}{ccccccccccccc}
 & & & & & \binom{0}{0} & & & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}$$

As integers, Pascal's triangle looks like the following, with the first seven rows shown. You

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

can see many patterns of how combinations are related in the triangle. Notice the symmetry of the combinations in a given row, forced by the symmetry property of combinations.

The identity $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ from the recursive property of combinations is seen by summing two entries in an upper row to give one entry in the next row between them. See the following diagram with arrows that capture this property.



4.8 Sequences

We finish the chapter with material on sequences, series, and products.

Definition 4.4 A *sequence* is an ordered list of numbers. A general sequence looks like

$$(a_n)_{n\geq 0} = a_0, a_1, a_2, a_3, \ldots$$

Notice that in our definition, a_n begins at $n = 0$. However, depending on the problem or example we are considering, the sequence can start at $n = 1$ or any fixed natural number.

Example 4.13 The following sequences are defined *recursively*, where the general term depends on the value of previous terms in the sequence. With recursive sequences, the first few values are given, such as those for $n = 0$ or $n = 1$.

1. $a_n = 2a_{n-1}$ for $n \geq 1$, with $a_0 = 2$.
2. $b_n = 3b_{n-1}$ for $n \geq 1$, with $b_0 = 14$.
3. $c_n = c_{n-1} + c_{n-2}$ for $n \geq 2$, with $a_0 = 0$ and $a_1 = 1$.

We focus on certain kinds of sequences that have a specified form.

Definition 4.5 Let a and r be real numbers.
A *geometric* sequence is of the form

$$a, ar, ar^2, ar^3, ar^4, \ldots,$$

where a is the *initial term* and r is the *common ratio*.
An *arithmetic* sequence is of the form

$$a, a + d, a + 2d, a + 3d, a + 4d, \ldots,$$

where a is the *initial term* and d is the *common difference*.

We consider examples of geometric and arithmetic sequences.

Example 4.14

1. $81, 27, 9, 3, 1, \frac{1}{3}, \ldots$ is a geometric sequence with initial term 81 and common ratio $\frac{1}{3}$.
2. $3, 8, 13, 18, 23, 28, 33, 38, \ldots$ is an arithmetic sequence, with initial term 3 and common difference 5.

Definition 4.6 Let $(a_n)_{n\geq 0}$ be a sequence. For $1 \leq m \leq n$, where m and n are integers, we define

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

We call k the *index of summation* and m and n the *limits* of the summation. We say m is the *lower limit* and n is the *upper limit*. Each a_k is a *term* of the sum.

The term $\sum_{k=m}^{n} a_k$ is sometimes called a *series*.

Example 4.15 We have that

$$\sum_{k=1}^{7} k^2 = 1 + 4 + 9 + 16 + 25 + 36 + 49 = 140.$$

We collect together some important sums of integers, their squares, and their cubes.

Theorem 4.14 (Sums of integers) Let n be a positive integer. We then have the following:

$$\begin{aligned}
\sum_{k=1}^{n} k &= \frac{n(n+1)}{2}, \\
\sum_{k=1}^{n} k^2 &= \frac{n(n+1)(2n+1)}{6}, \\
\sum_{k=1}^{n} k^3 &= \frac{n^2(n+1)^2}{4}.
\end{aligned}$$

We may also consider *infinite* sums, of the form $\sum_{k=m}^{\infty} a_k$, where the summation has no end.

Theorem 4.15 (Sum of a geometric series) Let $x \neq 1$ be a real number and let a be real number. We then have that

$$\sum_{k=0}^{n} ax^k = a\left(\frac{1-x^{n+1}}{1-x}\right).$$

If $|x| < 1$, then

$$\sum_{k=0}^{\infty} ax^k = \frac{a}{1-x}.$$

Example 4.16 1.

$$\sum_{k=0}^{10} 3 \cdot (-2)^k = 3\left(\frac{1-(-2)^{11}}{1-(-2)}\right) = 2049$$

is a geometric series with initial term 3 and common ratio -2.

2. The infinite series

$$27 + 18 + 12 + 8 + \cdots$$

equals

$$\frac{27}{1-(2/3)}.$$

Notice that we factor out 27 before using the formula for geometric series.

Similar to sums, we can form general products of numbers.

Definition 4.7 If $(a_n)_{n\geq 0}$ is a sequence, then for $1 \leq m \leq n$, where m and n are integers, we define

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

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

Example 4.17 1. For a positive integer n,

$$\prod_{k=1}^{n} k = n!$$

2. For a positive integer n,

$$\prod_{k=1}^{n} 2 = 2^n.$$

4.9 Exercises

(4.1) (a) If you have 10 apples, 5 oranges, and 6 bananas, then how many pieces of fruit do you have?

(b) If there are 26 quarters and 12 dimes, then how many coins do you have?

(4.2) Suppose that we are given disjoint sets X_i with $|X_i| = i^2$, where $1 \leq i \leq 5$. Determine

$$|X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5|.$$

(4.3) If X, Y, Z are sets with $|X| = 5$, $|Y| = 6$, and $|Z| = 8$, then what is the maximum cardinality of $X \cup Y \cup Z$?

(4.4) (a) How many binary strings (that is, strings consisting of only 0's and 1's) are there of length 6?

(b) How many binary strings are there of length 6 beginning with 010?

(c) How many binary strings are there of length 6 beginning and ending with 1?

(4.5) How many words (even nonsensical ones) are there of length 5 that begin with the letter A?

(4.6) Each edge of a complete graph K_6 is colored either red or blue. How many distinct ways can we color the edges of K_6? You may assume each edge is distinguishable from the others.

(4.7) Recall that an integer k is a *divisor* of an integer n if $k|n$.

(a) Determine the number of distinct divisors of $2^2 3^3$.

(b) Determine the number of distinct divisors of $2^4 3^5 7^5$.

(c) Determine the number of distinct divisors of $2^5 3^4 7^6 11^2$.

(4.8) Let X, Y, Z be sets. Calculate $|(X \cup Y \cup Z)|$ if $|X| = 60$, $|Y| = 100$, $|Z| = 81$, $|X \cap Y| = 11$, $|X \cap Z| = 12$, $|Y \cap Z| = 18$, and $|X \cap Y \cap Z| = 7$.

(4.9) Using the Principle of Inclusion-Exclusion, determine the number of binary strings of length ten that start with 101 or end with 00.

(4.10) Using the Principle of Inclusion-Exclusion, determine the number of binary strings of length ten that start with 101, or end with 00, or have 11 at positions 5 and 6.

(4.11) In a simple graph with 10 vertices and no isolated vertices, explain why some pair of vertices have the same degree.

(4.12) (a) In room with 14 people, why do at least two of them have birthdays in the same month?

(b) In a graph with 10 vertices and 6 edges, show that there is a vertex of degree at least 2.

(c) Choose five distinct integers from 1 to 8. Show that two of them sum to 9.

(4.13) Show that if a set contains 151 nonnegative integers, then at least 76 are either even or odd.

(4.14) Compute $P(3,2)$, $P(5,2)$, and $P(10,8)$.

(4.15) (a) A password has 5 letters with no repetitions of letters. How many possible passwords are there?

(b) Suppose we have a five distinct coins. How many ways can we place them in order in a row?

(c) In a graph G of order 10 with vertices labeled $1, 2, \ldots, 10$, if each vertex receives one of 10 colors without repetition, how many distinct colorings of G are there?

(4.16) Compute $\binom{10}{2}$, $\binom{10}{3}$, and $\binom{10}{7}$.

(4.17) By expanding the combinations with factorials, prove the symmetry property of combinations: For integers $n \geq 0$ and $r \geq 0$, with $r \leq n$, we have that

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

(4.18) Express

$$\sum_{r=0}^{25} \binom{25}{r}^2$$

as a single combination.

(4.19) How many pairs of distinct integers chosen from $\{1, 2, \ldots, 101\}$ have an even sum?

(4.20) Find

$$\sum_{r=0}^{n} \binom{n}{r} 25^r.$$

(4.21) Expand the following expressions using the Binomial Theorem.

(a) $(2x + 3y)^4$.

(b) $(1 + 2/x)^3$.

(c) $(-1/x - 5x^2)^5$.

(4.22) In the expansion of

$$(2x^2 - 1/x)^{10},$$

find the coefficient in front of the term $1/x$.

(4.23) Write out the 9th row of Pascal's triangle.

(4.24) (H) Prove the following identity:

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

(**Hint**: Do a combinatorial proof. If we choose a, b, c with $a < b < c$ from $1, 2, \ldots n$, then consider cases for a.)

(4.25) Explain why the sequence

$$b_n = 3n - 1,$$

where $n \geq 1$, is an arithmetic sequence, and determine the 19th term in the sequence.

(4.26) Explain why the sequence

$$c_n = \frac{1}{4 \cdot 3^{n-1}},$$

where $n \geq 1$, is a geometric sequence, and determine the 11th sum of the sequence.

(4.27) Determine

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

(4.28) Compute

$$\sum_{k=0}^{\infty} (-0.3)^k.$$

(4.29) (H) Show that

$$\sum_{n=1}^{14} \frac{1}{n(n+1)} = \frac{14}{15}.$$

(**Hint**: Use the fact that $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$.)

(4.30) (H) Show that

$$\prod_{n=2}^{25} \left(1 - \frac{1}{n^2}\right) = \frac{26}{50}.$$

(**Hint**: Use the fact that $1 - \frac{1}{n^2} = \frac{(n-1)(n+1)}{n^2} = \frac{n-1}{n}\frac{n+1}{n}$.)

4.10 Selected Answers and Hints

(4.1) (a) 21. (b) 38.

(4.2) $1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$.

(4.3) 19.

(4.4) (a) $2^6 = 64$. (b) $2^3 = 8$. (c) $2^4 = 16$.

(4.5) 26^4.

(4.6) There are $\binom{6}{2} = 15$ edges, and so there are 2^{15} distinct colorings of the edges of K_6.

(4.7) (a) The divisors of 2^2 are $1, 2, 2^2$. The divisors of 3^3 are $1, 3, 3^2, 3^3$. The divisors of $2^3 3^3$ are divisors of 2 and 3, so there are $3 \cdot 4 = 12$ divisors. (b) $5 \cdot 6 \cdot 6 = 180$. (c) $6 \cdot 5 \cdot 7 \cdot 3 = 630$.

(4.8) By the Principle of Inclusion-Exclusion, $|X \cup Y \cup Z| = 60 + 100 + 81 - 11 - 12 - 18 + 7$.

(4.9) $2^7 + 2^8 - 2^5 = 352$.

(4.10) $2^7 + 2^8 + 2^8 - 2^5 - 2^5 - 2^6 + 2^3 = 514$.

(4.11) The possible degrees are $1, 2, \ldots 9$. As there are 10 vertices, by the Pigeonhole Principle, some two vertices have the same degree.

(4.12) (a) Apply the Pigeonhole Principle. (b) If each vertex has degree at most 1, then there are at most 5 pairs of adjacent vertices. As there is 6 edges, by the Pigeonhole Principle, one of these vertices receives an additional edge, giving a vertex of degree at least two, which is a contradiction. (c) The ways two numbers from 1 to 8 could sum to 9 are $1+8, 2+7, 3+6, 4+5$. If we choose 5 distinct integers, then, by the Pigeonhole Principle, some two of them equal one of the four pairs $1+8, 2+7, 3+6, 4+5$.

(4.13) If even is red and odd is blue, then there is at least one $\lceil 151/2 \rceil = 76$ of one color.

(4.14) $P(3,2) = 6, P(5,2) = 20, P(10,8) = 1,814,400$.

(4.15) (a) $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22$. (b) 5! (c) 10!.

(4.16) $\binom{10}{2} = 45, \binom{10}{3} = \binom{10}{7} = 120$.

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

(4.18) $\binom{50}{25}$.

(4.19) $\binom{50}{2} + \binom{51}{2}$.

(4.20) 26^n.

(4.21) (a) $16x^4 + 96x^3y + 216x^2y^2 + 216xy^3 + 81y^4$. (b) $\frac{8}{x^3} + \frac{12}{x^2} + \frac{6}{x} + 1$. (c) $-3125x^{10} - 3125x^7 - \frac{1}{x^5} - 1250x^4 - \frac{25}{x^2} - 250x$.

(4.22) -960. Use the binomial theorem to expand the expression and think about which term has exponent -1.

(4.23) 1, 8, 28, 56, 70, 56, 28, 8, 1.

(4.24) The number of ways of choosing three distinct integers a, b, c from $1, 2, \ldots, n$ integers is $\binom{n}{3}$. Suppose without loss of generality that $a < b < c$. If $a = 1$, then there are $\binom{n-1}{2}$ choices for b, c. If $a = 2$, there are $\binom{n-2}{2}$ choices for b, c, and so on. By the sum rule, the identity holds.

(4.25) $b_n = 3n - 1$ is of the form $2 + 3k$, where $k \geq 0$. If $n = 19$, then $b_{19} = 56$.

(4.26) $c_n = \frac{1}{4 \cdot 3^{n-1}}$ has $a = 1/4$ and $r = \frac{1}{3^{n-1}}$. The 11th term is $\frac{1}{4 \cdot 3^{10}}$.

(4.27) $3 \cdot \frac{5^2 6^2}{4} + 4 \cdot \frac{4 \cdot 5 \cdot 9}{6}$.

(4.28) $\frac{1}{1.3}$.

(4.29) Use the fact that $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$. The sum then equals

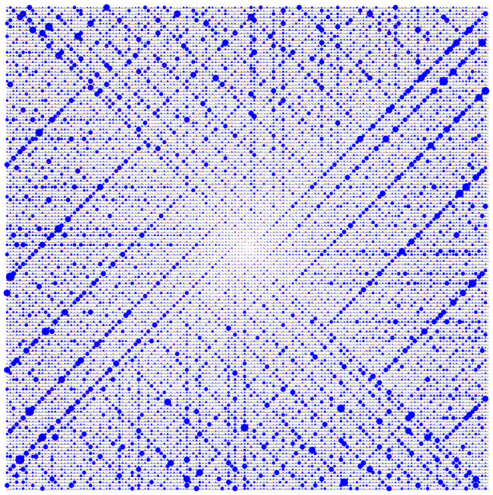
$$1 + \left(-\frac{1}{2} + \frac{1}{2}\right) + \left(-\frac{1}{3} + \frac{1}{3}\right) + \cdots + \left(-\frac{1}{14} + \frac{1}{14}\right) - \frac{1}{15} = 1 - \frac{1}{15} = \frac{14}{15}.$$

(4.30) Use the fact that $1 - \frac{1}{n^2} = \frac{(n-1)(n+1)}{n^2} = \frac{n-1}{n}\frac{n+1}{n}$. The product then equals

$$\left(\frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \ldots \cdot \frac{25-1}{25}\right) \cdot \left(\frac{3}{2} \cdot \frac{4}{3} \cdot \frac{5}{4} \cdot \ldots \cdot \frac{26}{25}\right) = \frac{26}{50}.$$

Chapter 5

Number Theory



5.1 Introduction to Number Theory

We learn about numbers from an early age, but few of us delve more deeply into their mathematical properties. Number theory focuses on mathematical properties of numbers, and important topics in the area are divisibility, primes, Diophantine equations, and congruences.

One basic but useful topic is *parity*, where we consider properties of even and odd numbers.

Definition 5.1 (Parity) An integer x is *even* if $x = 2a$, for some integer a. An integer x is *odd* if $x = 2b + 1$, for some integer b.

The following collects key facts on parity.

Theorem 5.1 (Properties of parity) Let x and y be integers.

1. If x and y are both even, then so are $x + y$ and xy.
2. If x is even and y is odd, then $x + y$ is odd.
3. If x is odd and y is odd, then $x + y$ is even.
4. We have that x is even if and only if x^2 is even.

Proof. We prove (1) and (4), leaving (2) and (3) to the reader.

For (1), if $x = 2a$ and $y = 2b$ for integers a, b, we have that

$$x + y = 2a + 2b = 2(a + b)$$

and

$$xy = (2a)(2b) = 2(2ab),$$

and so are both even.

For (4), note that (1) shows that if x is even, then so is x^2, by letting $y = x$. Now suppose that x is odd, so $x = 2a + 1$. Hence,

$$x^2 = 4a^2 + 4a + 1 = 2(a^2 + 2a) + 1,$$

and so x^2 is odd. By contraposition, this shows that x^2 even implies that x is even. □

These key facts on parity help us prove something about *irrational* numbers; that is, number which are not rational.

Theorem 5.2 The real number $\sqrt{2}$ is irrational.

Proof. Suppose for contradiction that $\sqrt{2}$ is rational, and is a fraction $\frac{p}{q}$ with $p, q \in \mathbb{Z}$. Suppose further that p and q share no common factor, as otherwise, we may eliminate common factors. We then have that $2q^2 = p^2$. Hence, p^2 is even and so p is even by our key facts on parity. Write $p = 2k$ for some integer k.

It follows that

$$2q^2 = p^2 = (2k)^2 = 4k^2,$$

and canceling 2 derives that

$$q^2 = 2k^2.$$

Hence, we find that q^2 is even and hence, q is even. But then we have that p and q share a common factor, which contradicts our assumption. Thus, $\sqrt{2}$ is irrational, as desired. □

Many other real numbers are known to be irrational, such as $\sqrt{3}$, $\sqrt{5}$, and $\sqrt{6}$. We explore these proofs in the exercises.

5.2 Divisors

Divisors play a central role in number theory, as they help us define prime numbers and the Euclidean algorithm.

Definition 5.2

1. We say that a *divides* b, denoted $a|b$, if $b = na$, for some integer n.
2. If a divides b, then b is said to be *divisible* by a.
3. The number a is called a *divisor* or *factor* of b, and b is called a *multiple* of a.

Example 5.1 We have that

$$11 \times 7 = 77,$$

and so $11|77$ and $7|77$. The divisors of 77 are

$$\{-1, 1, -7, 7, -11, 11, -77, 77\}.$$

Note every integer divides 0, since $0 = 0a$ for any integer a.

Definition 5.3 The *greatest common divisor* of nonzero integers a and b is the largest integer that divides both a and b. We write $\gcd(a, b)$ for the greatest common divisor of a and b.

Since 1 divides all integers, the greatest common divisor of two numbers is always defined.

Example 5.2 We have the following examples:

$$\gcd(11, 17) = 1, \gcd(24, 16) = 8, \gcd(0, 11) = 11.$$

We may allow one of a or b to be zero; note that $\gcd(0, a) = a$ for any nonzero integer a.

Definition 5.4 A number $p > 1$ is *prime* if its only positive factors are 1 and p. Otherwise, it is *composite*.

We use the following critical fact without proof.

Theorem 5.3 (Fundamental Theorem of Arithmetic) Every number equals a product of primes, which is unique up to the ordering of factors.

The Fundamental Theorem of Arithmetic allows us to view each number as made up of building blocks of prime numbers.

Example 5.3 The prime factorization of 112 is

$$2 \times 2 \times 2 \times 2 \times 7,$$

which is written more compactly as

$$2^4 \times 7,$$

or

$$2^4 7.$$

Theorem 5.4 (Euclid's theorem) There are infinitely many primes.

Proof. Suppose for a contradiction that there are only finitely many primes, $p_1, p_2, \ldots, p_m$. Form the integer

$$N = p_1 \cdot p_2 \cdot \cdots \cdot p_m + 1.$$

Note that none of the p_i equals N, since $N > p_i$ for all $1 \leq i \leq m$.

When dividing N by p_i, the remainder is 1. Hence, $p_i \nmid N$ for all $1 \leq i \leq m$. This then contradicts the Fundamental Theorem of Arithmetic, as every number is a product of primes, and so has some prime divisor. The contradiction implies that our assumption that there are only finitely many primes is false. □

We consider some visual representations of prime factorizations. First, we can represent prime factorizations by a tree, as in Figure 5.1. To read this, start at the top, and keep dividing by the least prime factor as long as possible, and then repeat with larger prime factors. The prime factorization is the product of the leaves, which are circled.

For a second visualization of prime factorization, we consider a Hasse diagram and partial

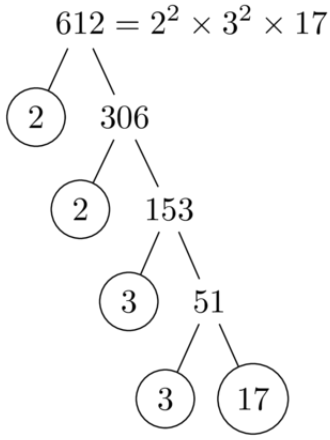


Figure 5.1: A prime factorization of 612 represented as a tree.

order of factors; for more background on partial orders, see Chapter 3. We have $a \leq b$ if $a|b$. The number 1 is the least element and 60 is the largest. Note that the primes are incomparable.

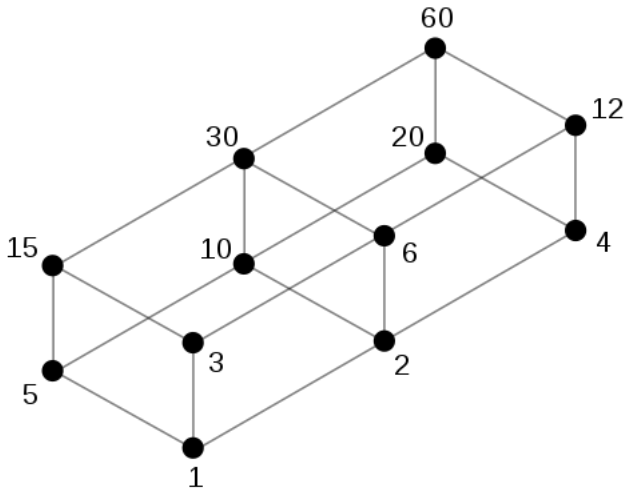


Figure 5.2: The Hasse diagram of the factors of 60.

The following theorem is helpful when dealing with greatest common divisors. We state it without proof.

Theorem 5.5 (Bézout's Theorem) Let a and b be nonzero integers, and let $d = \gcd(a, b)$. We then have that there exist integers m and n such that

$$ma + nb = d.$$

We can use Bézout's identity to prove the following.

Theorem 5.6 (Euclid's lemma) If p is prime and $p|ab$, then either $p \mid a$ or $p \mid b$.

Proof. Suppose that $p|ab$ and $p \nmid a$. We must prove that $p \mid b$.

Since $p \nmid a$ and p is prime, the greatest common divisor of p and a must be 1. Therefore, by Bézout's identity, there exist integers m and n such that

$$ma + np = 1.$$

Multiplying through by b gives

$$mab + npb = b.$$

Since $p|ab$, the left side of this equation is divisible by p, and hence, we have that $p|b$. □

5.3 The Euclidean Algorithm

The Euclidean algorithm is a method for deriving the greatest common divisor of two positive integers. The algorithm is based on the following simple observation:

Theorem 5.7 (Reducing gcds) If a and b are integers that are not both zero, then

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

Proof. Any common divisor of a and b is also a divisor of $a-b$. Furthermore, since $b = a+(b-a)$, any common divisor of a and $b - a$ is also a divisor of b.

We conclude that the pairs (a, b) and $(a, b - a)$ have precisely the same common divisors, and thus, have the same greatest common divisor. □

The Euclidean algorithm consists of repeatedly applying this theorem until the greatest common divisor becomes apparent.

Example 5.4 We find the greatest common divisor of 90 and 126. For this, since $126 - 90 = 36$, the lemma tells us that

$$\gcd(90, 126) = \gcd(90, 36).$$

Next we subtract 36 from 90 to reduce the problem further:

$$\gcd(90, 36) = \gcd(54, 36).$$

Since 36 is still the smaller number, we subtract it again:

$$\gcd(54, 36) = \gcd(18, 36).$$

Subtracting the 18 gives

$$\gcd(18, 36) = \gcd(18, 18) = 18.$$

We conclude that $\gcd(90, 126) = 18$.

Here is an example of computing the gcd with larger integers.

Example 5.5 We calculate $\gcd(67620, 66234)$. For this, we write

$$67620 = 66234 \cdot 1 + 1386.$$

Therefore, we have that $\gcd(67620, 66234) = \gcd(66234, 1386)$. We now repeat this process until we end up with a remainder of 0:

$$66234 = 1386 \cdot 47 + 1092$$

$$1386 = 1092 \cdot 1 + 294$$

$$1092 = 294 \cdot 3 + 210$$

$$294 = 210 \cdot 1 + 84$$

$$210 = 84 \cdot 2 + 42$$

$$84 = 42 \cdot 2 + 0.$$

It follows that $\gcd(67620, 66234) = \gcd(42, 0) = 42$.

5.4 Linear Diophantine Equations

We focus on equations with integer coefficients and integer solutions.

Definition 5.5 An equation of the form $ax + by = c$, where $a, b, c, x, y \in \mathbb{Z}$ is called a *linear Diophantine equation* or *LDE*.

Determining if an LDE has a solution depends on the greatest common divisor of its coefficients.

Theorem 5.8 (Checking if an LDE has a solution) Let $d = \gcd(a, b)$. The LDE

$$ax + by = c$$

has a solution if and only if $d|c$.

Proof. Suppose that $ax + by = c$ has an integer solution, say $x_0, y_0 \in \mathbb{Z}$. Since $d|a$ and $d|b$, we have that $d \mid (ax_0 + by_0) = c$.

Next assume that $d|c$. There then exists an integer k such that $dk = c$. By Bézout's Lemma, there exist integers u and v such that $au + bv = \gcd(a, b) = d$. Multiplying by k gives

$$a(uk) + b(vk) = dk = c$$

Therefore, a solution is given by $x = uk$ and $y = vk$. □

Example 5.6 We find one solution to the LDE $20x + 35y = 5$. Notice that we can simplify the LDE by dividing by 5 first to give

$$4x + 7y = 1.$$

It is straightforward to check that one solution is given by $x = 2$ and $y = -1$.

Theorem 5.9 (Solutions of an LDE) Let $d = \gcd(a, b)$ where $a \neq 0$ and $b \neq 0$. If $(x, y) = (x_0, y_0)$ is a solution to the LDE

$$ax + by = c,$$

then all solutions are given by

$$x = x_0 + \frac{b}{d}t \qquad y = y_0 - \frac{a}{d}t$$

for all $t \in \mathbb{Z}$. We may write the solution set as

$$\{(x_0 + \tfrac{b}{d}t, y_0 - \tfrac{a}{d}t) : t \in \mathbb{Z}\}.$$

Example 5.7 We find all integer solutions to $5x - 8y = 3$ where x and y are integers. By inspection, $x_0 = -1$ and $y_0 = -1$ is a solution. Since $\gcd(5, -8) = 1$, we have that the complete solution set is given by

$$x = -1 + (-8)t = -1 - 8t$$
$$y = -1 - 5t$$

for all $t \in \mathbb{Z}$.

Example 5.8 We solve the Diophantine equation $858x + 253y = 33$.
First we find $\gcd(858, 253)$ by using the Euclidean algorithm:

$$\begin{aligned} 858 &= 3 \cdot 253 + 99 \\ 253 &= 2 \cdot 99 + 55 \\ 99 &= 1 \cdot 55 + 44 \\ 55 &= 1 \cdot 44 + 11 \\ 44 &= 4 \cdot 11 + 0. \end{aligned} \tag{5.1}$$

Therefore the $\gcd(858, 253) = 11$. Since $33 = 3 \cdot 11$, our equation has solutions. By using backward substitutions we find that:

$$\begin{aligned}11 &= 55 + (-1)\cdot 44\\ &= 55 + (-1)\cdot(99 + (-1)\cdot 55) = 2\cdot 55 + (-1)\cdot 99\\ &= 2\cdot(253 + (-2)\cdot 99) + (-1)\cdot 99 = 2\cdot 253 + (-5)\cdot 99\\ &= 2\cdot 253 + (-5)\cdot(858 + (-3)\cdot 253) = (-5)\cdot 858 + 17\cdot 253.\end{aligned}$$

Thus, $858\cdot(-5) + 253\cdot 17 = 11$, and $(x_0, y_0) = (3\cdot(-5), 3\cdot 17) = (-15, 51)$ is a particular solution of $858x + 253y = 33$, and the general solution of the equation is

$$\{(x,y) \,:\, x = -15 + \frac{253}{11}t = -15 + 23t,\ y = 51 - \frac{858}{11}t = 51 - 78t,\ t \in \mathbb{Z}\}.$$

5.5 Congruences

A congruence in number theory is nothing more than a statement about divisibility.

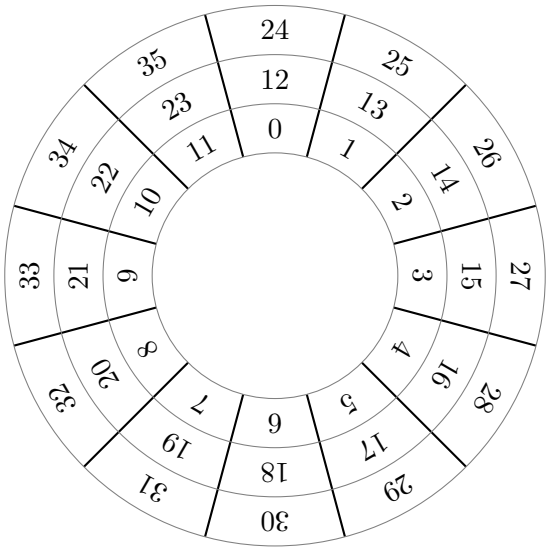
Definition 5.6 Let m be a positive integer. We say that a is *congruent to b modulo m* if $m|(a-b)$, where a and b are integers. If a is congruent to b modulo m, then we write $a \equiv b \pmod{n}$.

Note that if $a \equiv b \pmod{m}$ then $a = b + km$, where $k \in \mathbb{Z}$.

Example 5.9

1. $25 \equiv 1 \pmod{4}$ since $4|24 = 25 - 1$.
2. $1 \equiv -3 \pmod{4}$ since $4|4 = 1 - (-3)$.
3. $19 \equiv 5 \pmod{7}$.
4. $1001 \equiv 1 \pmod{5}$.
5. $2k + 1 \equiv 1 \pmod{2}$, which implies every odd number is congruent to 1 modulo 2. The numbers congruent to 0 modulo 2 are exactly the even integers.

We may visualize modular arithmetic using a clock. In the case $m = 12$, every integer is congruent to exactly one of $0, 1, 2, \ldots, 11$, and these are arranged in concentric circles around the innermost one representing the hours (with 0 representing 12).



There are many common properties between equations and congruences. Some properties are listed in the following.

Theorem 5.10 (Key properties of congruences) Let a, b, c and d denote integers. Let m be a positive integer. We then have the following, which we include without proof.

1. $a \equiv a \pmod{m}$.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
4. If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$.
5. If $a \equiv b \pmod{m}$, then $a - c \equiv b - c \pmod{m}$.
6. If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.
7. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
8. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$.
9. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Note that the first three items in the theorem show that congruences are equivalence relations.

We finish with an introduction to congruence classes, which are the equivalence classes of

the congruence binary relation.

Definition 5.7 Let $a, b \in \mathbb{Z}$ with $n > 0$. We define the *congruence class of a modulo n* to be

$$[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}.$$

Note that

$$[a]_n = \{b \in \mathbb{Z} : b = a + kn \text{ for } k \in \mathbb{Z}\}.$$

If it is understood, then we will drop the subscript n and write $[a]$. We may also say $[a]$ modulo n.

Example 5.10 We compute $[4]$ modulo 3.

$$\begin{aligned}[4]_3 &= \{b \in \mathbb{Z} : b = 4 + 3k \text{ for } k \in \mathbb{Z}\} \\ &= \{4, 4 \pm 3, 4 \pm 3 \cdot 2, 4 \pm 3 \cdot 3, \ldots\} \\ &= \{4, 1, 7, -2, 10, 13, -5, \ldots\}.\end{aligned}$$

Theorem 5.11 **(Equality of congruence classes)** Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We then have that $a \equiv b \pmod{n}$ if and only if $[a]_n = [b]_n$.

The theorem gives that for $n \geq 2$, the distinct congruence classes are $[0], [1], \ldots, [n-1]$.

Example 5.11 We find $2^{644} \pmod{645}$. The number 2^{644} is so large, you cannot simply enter it into a calculator. Instead, we first divide 644 by powers of 2 to give:

$$644 = 2^9 + 2^7 + 2^2.$$

We then find that:

$$\begin{aligned}
2^2 &= 2 \cdot 2 = 4 \equiv 4 \pmod{645} \\
2^4 &\equiv 4 \cdot 4 = 16 \equiv 16 \pmod{645} \\
2^8 &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\
2^{16} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\
2^{32} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\
2^{64} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645} \\
2^{128} &\equiv 256 \cdot 256 = 65,536 \equiv 391 \pmod{645} \\
2^{256} &\equiv 391 \cdot 391 = 152,881 \equiv 16 \pmod{645} \\
2^{512} &\equiv 16 \cdot 16 = 256 \equiv 256 \pmod{645}.
\end{aligned}$$

As $2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4$, we have that

$$2^{644} \equiv 256 \cdot 391 \cdot 16 \pmod{645}.$$

Hence,

$$256 \cdot 391 = 100099 \equiv 121 \pmod{645},$$

and

$$121 \cdot 16 = 1936 \equiv 1 \pmod{645}.$$

Thus, $2^{644} \equiv 1 \pmod{645}$.

5.6 Exercises

(5.1) Find all the divisors of the following three integers: 6, 12, and 42.

(5.2) Identify all the numbers up to and including 31 as prime or composite.

(5.3) Find the prime factorizations of the following numbers.

(a) 25.

(b) 66.

(c) 131.

(d) 1000.

(5.4) For each of your answers in the previous exercise, represent the prime factorization as a tree, like the one in Figure 5.1.

(5.5) (a) Prove that $2^{1/3}$ is irrational. (**Hint**: Mimic the proof by contradiction used for $\sqrt{2}$.)

(b) Prove that $\sqrt{3}$ is irrational.

(c) Prove that $\sqrt{5}$ is irrational.

(5.6) Define the positive-integer valued function $\phi(n)$ to be the number of positive integers m such that $m \leq n$ and $\gcd(m, n) = 1$.

(a) Find $\phi(1)$.

(b) Find $\phi(7)$.

(c) Find $\phi(9)$.

(d) Prove that for a prime p that $\phi(p) = p - 1$.

(e) (H) Prove that for a prime p and positive integer n that $\phi(p^n) = p^n - p^{n-1}$.

(5.7) Find the smallest nonnegative integer x satisfying the following congruence equations.

(a) $491 \equiv x \pmod{17}$.

(b) $55 \equiv x \pmod{4}$.

(c) $-1999 \equiv x \pmod{10}$.

(d) $-177 \equiv x \pmod{3}$.

(5.8) A *partition* of a positive integer n is a way of writing n as a sum of positive integers. Two sums that differ only in the order of their summands are considered the same partition. For example, 4 has partitions

$$4,$$

$$1 + 3,$$

$$2 + 2,$$

$$2 + 1 + 1,$$

and

$$1 + 1 + 1 + 1.$$

The partition function $p(n)$ represents the number of possible partitions of a nonnegative integer n. From our example, $p(4) = 5$.

(a) Find $p(3)$.

(b) Find $p(5)$.

(c) Find $p(6)$.

(5.9) Find the least nonnegative integer satisfying the following congruence equation:

$$4^{60} \equiv x \pmod{69}.$$

(5.10) Find the least nonnegative integer x such that $17^{213} \equiv x \pmod 5$. (**Hint**: Use the fact that $17^2 \equiv 4 \equiv -1 \pmod 5$.)

(5.11) Prove that if n is a nonnegative integer whose decimal representation ends in 0, then $5|n$.

(5.12) Show that for all nonnegative integers n that $n^2 + n$ is always even.

(5.13) Show that for integers a, b, c, if $c|a$, and $c|b$, then

$$c|(3a + 5b).$$

(5.14) *Casting out nines.*

(a) Show that modulo 9, each nonnegative integer is the sum of its digits.

(b) Explain why a positive integer is divisible by 9 exactly when the sum of its digits is divisible by 9.

(c) Using (b), explain why $999,182,754$ is divisible by 9 without using a calculator.

(d) Find the least nonnegative integer x such that $988,394,343,4x11$ is divisible by 9.

(5.15) Prove that if n is an odd integer, then $5n^2 + 7$ is even.

(5.16) Find $\gcd(2^3 5^3 7^3, 2^3 7^3 11^2)$.

(5.17) Find $\gcd(11^2 13^7 19^3, 2^{16} 11^{14} 19^2)$.

(5.18) Using the Euclidean algorithm, find the following gcds.

(a) $\gcd(15, 24)$

(b) $\gcd(101, 107)$.

(c) $\gcd(1000, 888)$.

(d) $\gcd(4567, 91837)$.

(5.19) Prove that for every prime p that $\gcd(p, p + 1) = 1$.

(5.20) Solve the linear Diophantine equation:

$$7x - 9y = 3.$$

(5.21) Find all integers x and y such that:

$$2173x + 2491y = 53.$$

(5.22) Find all integers x and y such that:

$$2173x + 2491y = 159.$$

(5.23) Show there is no integers solution to:

$$2173x + 2491y = 210.$$

(5.24) Solve the linear Diophantine equation:

$$858x + 253y = 33.$$

(5.25) Find all integer solutions to:

$$258x + 147y = 369.$$

(5.26) Show there are no integers solution to:

$$155x + 45y = 7.$$

(5.27) Solve the linear Diophantine equation:

$$60x + 33y = 9.$$

(5.28) For $n \geq 2$, suppose that $1 \leq a \leq n-1$. We say that x is an *inverse* of $a \pmod{n}$ if

$$ax \equiv 1 \pmod{n}.$$

(a) Explain why a has no inverse modulo n if $\gcd(a, n) > 1$.

(b) Show that 5 has no inverse modulo 25.

(c) Find the inverse of $8 \pmod{11}$. (**Hint**: Express the $\gcd(8, 11)$ as a linear combination of 8 and 11.)

(5.29) An ordered sequence of integers (a, b, c) satisfying

$$a^2 + b^2 = c^2$$

are called a *Pythagorean triple*.

(a) Show that $(3, 4, 5)$ is a Pythagorean triple.

(b) Show that $(5, 12, 13)$ is a Pythagorean triple.

(c) Show that $(8, 15, 17)$ is a Pythagorean triple.

(d) Explain why if (a, b, c) is a Pythagorean triple and n is a positive integer, then (an, bn, cn) is a Pythagorean triple.

(e) Using (d) show that there are infinitely many Pythagorean triples.

(5.30) A positive integer n is *perfect* if it is the sum of its positive divisors, excluding itself.

(a) Show that 6 is perfect.

(b) Show that 28 is perfect.

(c) (H) Show that 496 is perfect.

Surprisingly, no one knows if there are infinitely many perfect numbers.

5.7 Selected Answers and Hints

(5.1) The integer 6 has divisors: 1, 2, 3, 6. The integer 12 has divisors 1, 2, 3, 4, 6, 12. The integer 42 has divisors: 1, 2, 3, 6, 7, 14, 21, 42.

(5.2) The primes up to and including 31 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and the rest are composite.

(5.3) (a) 5^2. (b) $2 \cdot 3 \cdot 11$. (c) 131. (d) $2^3 5^3$.

(5.5) (a) For a contradiction, suppose that $2^{1/3} = p/q$, where p and q are integers with no common factors. We then have that $p^3 = 2q^3$, so p^3 is even, which implies that p is even. If $p = 2k$ for some integer k, then $q^3 = 4k^3$, and so q is also even, which is a contradiction.

For (b) and (c), employ similar proofs by contradiction, using Euclid's Lemma to show that if a prime $p|n^2$, then $p|n$.

(5.6) (a) $\phi(1) = 1$. (b) $\phi(7) = 6$. (c) $\phi(9) = 6$.

For (d), notice that p satisfies $\gcd(p, m) = 1$, for all positive integers $m < p$.

For (e), the total number of positive integers $m \leq p^n$ is p^n. The positive integers $m \leq p^n$ satisfying $\gcd(p^n, m) > 1$, are $p, p^2, \ldots, p^{n-1}p = p^n$, and there are p^{n-1} of those. Taking the difference of p^n and p^{n-1} gives the desired answer.

(5.7) (a) 15. (b) 3. (c) 1. (d) 0.

(5.8) (a) 3. (b) 7. (d) 11.

(5.9) 58.

(5.10) $17^{213} = 17 \cdot 17^4 \cdot 17^{16} \cdot 17^{64} \cdot 17^{128} \equiv 2 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \equiv 2 \pmod 5$.

(5.11) Note that $10 \equiv 0 \pmod 5$. Hence, an integer is divisible by 5 if and only if its decimal representation ends in 0 or 5.

(5.12) Consider cases for n even and n odd.

(5.13) We have that $a = ck$ and $b = cj$, for k and j integers. Hence, $3a + 5b = c(3k + 5j)$.

(5.14) (a), (b) Use the fact that $10 \equiv 1 \pmod 9$. (c) $9 + 9 + 9 + 1 + 8 + 2 + 7 + 5 + 4 = 54$. (d) 6.

(5.15) Show that $5n^2$ is odd.

(5.16) $2^3 7^3$.

(5.17) $11^2 19^2$.

(5.18) (a) 3. (b) 1. (c) 8. (d) 1.

(5.19) If m divides p and $p + 1$, then m divides $(p + 1) - p = 1$, and so $m = 1$.

(5.20) $x = 3 - 9t, y = 2 - 7t$, where t is an integer. The particular solution was found by inspection.

(5.21) $x = -8 + 47t, y = 7 - 41t$, where t is an integer.

(5.22) $x = -24 + 47t, y = 21 - 41t$, where t is an integer.

(5.23) As $\gcd(2173, 2491) = 53$, and since 53 does not divide 210, there is no integer solution to the LDE.

(5.24) $x = -15 + 23t, y = 51 - 78t$, where t is an integer.

(5.25) $x = 492 + 49t, y = -861 - 86t$, where t is an integer.

(5.26) As $\gcd(155, 45) = 5$, and as 5 does not divide 7, the equation has no integer solution to the LDE.

(5.27) $x = 15 + 11t, y = -27 - 20t$, where t is an integer.

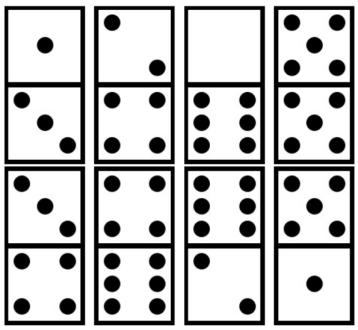
(5.28) (a) If $ax \equiv 1 \pmod{n}$, then $ax + kn = 1$, for some integer k. Hence, $\gcd(a, n)=1$. (b) $\gcd(5, 25) = 5$. (c) 7.

(5.29) (a) $3^2+4^2 = 5^2$. (b) $5^2+12^2 = 13^2$. (c) $8^2+15^2 = 17^2$. (d) $(an)^2+(bn)^2 = n^2(a^2+b^2) = (cn)^2$. (e) Use (d) and let $n \geq 2$ be an integer.

(5.30) (a) $6 = 1+2+3$. (b) $28 = 1+2+4+7+14$. (d) $496 = 1+2+4+8+16+31+62+124+248$.

Chapter 6

Induction



6.1 Introducing Induction

Induction is a proof technique for properties and statements about the natural numbers. One such property is the following.

Example 6.1 For a positive integer n,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{6.1}$$

Note that (6.1) holds for infinitely many different choices of n, so you cannot prove it by checking it for each positive integer. The formula (6.1) holds if $n = 1$, as the left side in that case is 1 and the right side is $\frac{1(2)}{2} = 1$.

To prove the statement using induction, we make the assumption that it is true for a fixed n. We know this is true for $n = 1$ as described above, but we are assuming there that we have checked every case up to and including n.

What happens for the value $n + 1$? We have that

$$1 + 2 + \cdots + n + n + 1 = (1 + 2 + \cdot + n) + n + 1.$$

The bracketed expression satisfies (6.1) by our assumption, so replace it with $\frac{n(n+1)}{2}$ to

give:

$$\frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}.$$

We derived the right side by finding a common denominator and collecting the terms. What we established is that if (6.1) holds for a given n, then it also holds for $n+1$. As (6.1) holds for $n = 1$, by what we have shown it holds $n = 2$, then $n = 3$, and so on.

We now give the formal definition of induction.

Definition 6.1 Let $P(n)$ be a property of the integer $n \geq 0$. Suppose that the following items hold.

1. $P(0)$ holds.
2. For an integer $n \geq 0$, assuming $P(n)$ holds, then $P(n+1)$ holds.

We then have that $P(n)$ holds for every integer $n \geq 0$.

We make a few comments about Definition 6.2. First, $P(n)$ is a *property* so it can be many things. For example, it could be an equality like in (6.1), or it could be an inequality, or it could be a property of graphs of order n. Another point is that item (1) may require that $P(1)$ holds or even $P(k)$ holds for some integer $k > 1$. In those cases, the conclusion is that $P(n)$ holds for all $n \geq k$.

Item (1) is called the *base case* of the induction. The assumption that $P(n)$ holds is the *induction hypothesis*. Verifying that $P(n+1)$ holds is the *inductive step*. Every inductive proof always has these three parts, completed in order.

Induction holds because of the properties of integers, which start at 0 and increment by 1. You can reach any integer by such incrementation. We can visualize induction therefore, as a toppling of dominoes, where 0 or k is the first domino toppled, and the inductive step applied repeatedly pushes over the next one, the one after that, and so on.

We now give a full proof by induction to further illustrate the concept. More examples using induction from various topics in the book appear in the next section.

Theorem 6.1 If n is a positive integer, then $23^n - 1$ is divisible by 11.

Proof. . We first verify the base case, which is for $n = 1$. In this case, $23^1 - 1 = 22$, which is

$2 \cdot 11$. The base case holds and the induction begins.

Assume for our inductive hypothesis that for a fixed positive integer, $23^n - 1$ is divisible by 11. For the inductive step, consider $23^{n+1} - 1$. We then have that

$$\begin{aligned} 23^{n+1} - 1 &= 23 \cdot 23^n - 1 \\ &= (22 + 1) \cdot 23^n - 1 \\ &= 2 \cdot 11 \cdot 23^n + (23^n - 1). \end{aligned}$$

The term $2 \cdot 11 \cdot 23^n$ is divisible by 11, and together with the induction hypothesis, we may conclude that $23^{n+1} - 1$ is divisible by 11. The inductive step follows, and the desired property holds for all positive integers by induction. □

6.2 Examples of induction

As induction applies to general properties of integers, we present several diverse examples of it in this section, ranging from summation formulas, to theorems in number theory and graph theory. We begin with a two identities on sums of integers.

Theorem 6.2 If n is a positive integer, then

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

Proof. We proceed by induction on $n \geq 1$. For the base case with $n = 1$, the fraction $\frac{n(n+1)(2n+1)}{6}$ equals $\frac{2 \cdot 3}{6} = 1$.

For the induction hypothesis, suppose the equality holds for a fixed $n \geq 1$. We then have

for the inductive step that

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \text{ (by induction hypothesis)} \\
&= (n+1)\cdot\left(\frac{n(2n+1)+6n+6}{6}\right) \\
&= \frac{(n+1)(n+2)(2n+3)}{6} \\
&= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.
\end{aligned}$$

Hence, the equality holds for all $n \geq 1$ by induction. □

Our next equality is on the sum of the first odd integers.

Theorem 6.3 If n is a nonnegative integer, then

$$\sum_{i=0}^{n}(2n+1) = (n+1)^2.$$

Proof. We proceed by induction on $n \geq 1$. The base case with $n = 1$ follows since both sides of the equation equal 1.

For the induction hypothesis, suppose the equality holds for a fixed $n \geq 1$. We then have for the inductive step that

$$\begin{aligned}
\sum_{i=0}^{n+1} 2i+1 &= \sum_{i=1}^{n}(2i+1) + 2n + 3 \\
&= (n+1)^2 + 2n + 3 \text{ (by induction hypothesis)} \\
&= n^2 + 4n + 4 \\
&= (n+2)^2 \\
&= ((n+1)+1)^2.
\end{aligned}$$

Hence, the equality holds for all $n \geq 0$ by induction. □

We next consider two inequalities with proofs by induction.

Theorem 6.4 If $n \geq 4$ is an integer, then $2^n < n!$.

Proof. We proceed by induction on $n \geq 1$. For the base case with $n = 4$ we have that $2^n = 16$, while $n! = 24$.

For the induction hypothesis, suppose the inequality holds for a fixed $n \geq 4$. We then have for the inductive step that

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &< 2n! \text{ (by induction hypothesis)} \\ &< (n+1)n! \\ &= (n+1)!, \end{aligned}$$

where the last inequality holds since $2 < n + 1$. Hence, the equality holds for all $n \geq 4$ by induction. □

Theorem 6.5 If $n \geq 1$ is an integer and $-1 < a$, then

$$1 + na \leq (1 + a)^n.$$

Proof. We proceed by induction on $n \geq 1$. For the base case with $n = 1$ both sides of the equality equal $1 + a$.

For the induction hypothesis, suppose the inequality holds for a fixed $n \geq 1$. We then have for the inductive step that

$$\begin{aligned} 1 + (n+1)a &\leq 1 + na + a + na^2 \\ &= (1 + na)(1 + a) \\ &\leq (1 + a)^n(1 + a) \text{ (by induction hypothesis)} \\ &= (1 + a)^{n+1}, \end{aligned}$$

where the first inequality holds since $0 \leq na^2$. Hence, the equality holds for all $n \geq 1$ by induction. □

Recall that a *tree* is a graph that is connected and with no cycles. We prove Theorem 2.5 giving the exact size of trees in terms of their order.

Theorem 6.6 In a tree G, we have that $|E(G)| = |V(G)| - 1$.

Proof. We proceed by induction on $|V(G)| = n \geq 1$. In the base case, where $n = |V(G)| = 1$, there are no edges, so $|E(G)| = 1 - 1 = 0$, as desired.

Suppose the equality holds for trees of order n, for a fixed integer $n \geq 1$. Let G be a tree of order $n+1$. We know that there are two leaves in G, as its order is at least 2. Let u be such a leaf. The graph $G - u$ is a tree: it is connected and no cycles are formed by deleting u. By the induction hypothesis, we have that

$$|E(G-u)| = |V(G-u)| - 1 = (n+1) - 1 - 1 = n - 1.$$

If we add back u, then we add exactly one edge. Hence,

$$|E(G)| = n = |V(G)| - 1,$$

and the proof follows. □

We give a proof of the binomial theorem using induction.

Theorem 6.7 (Binomial Theorem) Let n be a nonnegative integers and let x, y be variables.

$$\begin{aligned}(x+y)^n &= \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r \\ &= \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x \cdot y^n + \binom{n}{n} y^n.\end{aligned}$$

Proof. We prove the theorem by induction on $n \geq 1$. In the case $n = 1$, the left side and right side both equal $x + y$, so the base case holds.

Assume the equation holds for a fixed $n \geq 1$. For the induction step, we need the following recurrence property of combinations, which was Theorem 4.10: for integers $n \geq 1$ and $r \leq n$, we have that

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

Now consider the expansion:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\left(\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}x\cdot y^n + \binom{n}{n}y^n\right) \\
&= \binom{n}{0}x^{n+1} + \left(\binom{n}{0} + \binom{n}{1}\right)x^n y + \left(\binom{n}{1} + \binom{n}{2}\right)x^{n-1}y^2 + \\
&\quad \cdots + \left(\binom{n}{n-1} + \binom{n}{n}\right)xy^n + \binom{n}{n}y^{n+1} \\
&= \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y + \binom{n+1}{2}x^{n-1}y^2 + \cdots + \binom{n+1}{n}xy^n + \binom{n+1}{n+1}y^{n+1},
\end{aligned}$$

where we use the recurrence property of combinations in the fourth equality, and the fact that $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ in the final equality. Hence, the proof follows by induction. □

We finish with an application of induction to divisibility.

Theorem 6.8 For an integer $n \geq 1$, the number $n^3 + 2n$ is divisible by 3.

Proof. For the base case with $n = 1$, the number $n^3 + 2n = 3$, which is divisible by 3.

Suppose that $n^3 + 2n$ is divisible by 3 for a fixed $n \geq 1$. For the inductive step, note that

$$\begin{aligned}
(n+1)^3 + 2(n+1) &= (n^3 + 3n^2 + 3n + 1) + (2n + 2) \\
&= (n^3 + 2n) + (3n^2 + 3n + 3).
\end{aligned}$$

The final expression is divisible by 3, since $n^3 + 2n$ is by induction hypothesis, and $3n^2 + 3n + 3 = 3(n^2 + n + 1)$. The proof follows by induction. □

6.3 Strong induction

In the induction hypothesis, we assumed that our desired property holds for a fixed nonnegative integer n. However, we may assume that the property holds for all values up to an including n without any loss of generality. As in our dominoes analogy, if the 99th domino falls, then that means the first 98 fell before it. We refer to this as *strong induction* and it is defined more precisely as follows.

Definition 6.2 Let $P(n)$ be a property of the integer $n \geq 0$. Suppose that the following items hold.

1. $P(0)$ holds.
2. For an integer $n \geq 0$, assuming $P(k)$ holds for all $0 \leq k \leq n$, then $P(n+1)$ holds.

We then have that $P(n)$ holds for every integer $n \geq 0$.

Notice that the only difference between the definition of strong and the normal induction is in the inductive hypothesis, as stated in (2). Strong induction is effective especially in situations where you to use multiple previously established cases to prove your induction step.

As an illustration of strong induction, we prove the following theorem, which is a big part of the Fundamental Theorem of Arithmetic, which was Theorem 5.3 in Chapter 5.

Theorem 6.9 Every integer $n \geq 2$ is a product of primes.

Proof. We use strong induction on n. The base case is $n = 2$, which is prime. Suppose that for a fixed integer $n \geq 2$, the conclusion holds for all integers k such that $2 \leq k \leq n$.

Next, consider $n+1$. If $n+1$ is prime, then the inductive step holds. Suppose that $n+1$ is composite, so $n+1 = ab$, where a and b are positive integers at least 2.

Note that $2 \leq a, b \leq n$. By induction hypothesis, there are primes $n_1, n_2, \ldots, n_j$ and $m_1, m_2, \ldots, m_k$ such that

$$\begin{aligned} n+1 &= ab \\ &= n_1 \cdot n_2 \cdots n_j \cdot m_1 \cdot m_2 \cdots m_k. \end{aligned}$$

We then have that $n+1$ is a product of primes, and induction step follows. □

Another application of strong induction is to inductively defined sequences, or recurrences. We will study these in more detail in the next section

Theorem 6.10 Let a_n be a sequence of positive integers defined by $a_1 = 1$, $a_2 = 8$, and for $n \geq 3$,

$$a_n = a_{n-1} + 2a_{n-2}.$$

We then have that for all integers $n \geq 1$,

$$a_n = 3 \cdot 2^{n-1} + 2(-1)^n.$$

Proof. In the case $n = 1$, we are given that $a_1 = 1$. The right side of the formula is $3 \cdot 2^0 + 2(-1)^1 = 1$, so this case follows. Similarly, $a_2 = 8$ and the formula in this case gives $3 \cdot 2^1 + 2(-1)^2 = 8$.

Now for a fixed $n \geq 2$, suppose the result hold for all integers k such that $1 \leq k \leq n$. We then have that

$$\begin{aligned} a_{n+1} &= a_n + 2a_{n-1} \\ &= 3 \cdot 2^{n-1} + 2(-1)^n + 2(3 \cdot 2^{n-2} + 2(-1)^{n-1}) \\ &= 3 \cdot (2^{n-1} + 2^{n-1}) + 2((-1)^n + 2(-1)^{n-1}) \\ &= 3 \cdot 2^n + 2(-1)^{n+1}, \end{aligned}$$

where the first equality holds by the definition of the sequence and the second equality holds by induction hypothesis. In the final equality, we use the fact that $(-1)^{n+1} = (-1)^n + 2(-1)^{n-1}$, which can be seen by checking the equality in the cases when n is even or odd. Hence, the desired form for a_n holds for all integers $n \geq 1$ by strong induction. □

Consider the sequence of integers whose general term is the sum of the two previous terms. We set $a_0 = 0$, $a_1 = 1$, and then define $a_{n+1} = a_n + a_{n-1}$, where $n \geq 1$. This is the famous *Fibonacci sequence* and the first terms in the sequence are: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89. These are called *Fibonacci numbers* and they appear in many different settings, from patterns in flowers and plants, to fractals, and to the Platonic solids.

We prove the following inequality about terms in the Fibonacci sequence.

Theorem 6.11 If a_n is the nth term in the Fibonacci sequence, then for all $n \geq 1$ we have that

$$a_n \geq \left(\frac{3}{2}\right)^{n-2}.$$

Proof. In the base case $n = 1$, we have that $a_1 = 1 \geq \frac{2}{3} = \left(\frac{3}{2}\right)^{1-2}$, as desired.

Suppose that the inequality holds for all $k \leq n$, where $n \geq 1$ is a fixed integer. For the induction step, we have that:

$$\begin{aligned} a_{n+1} &= a_n + a_{n-1} \\ &\geq \left(\frac{3}{2}\right)^{n-2} + \left(\frac{3}{2}\right)^{n-3} \\ &\geq \left(\frac{3}{2} + 1\right)\left(\frac{3}{2}\right)^{n-3} \\ &\geq \left(\frac{5}{2}\right)\left(\frac{3}{2}\right)^{n-3} \\ &\geq \left(\frac{3}{2}\right)^{2}\left(\frac{3}{2}\right)^{n-3} \\ &= \left(\frac{3}{2}\right)^{(n+1)-2}, \end{aligned}$$

where the first inequality follows by the induction hypothesis, and the fourth inequality follows since $\frac{5}{2} \geq \frac{9}{4} = \left(\frac{3}{2}\right)^2$. □

6.4 Recurrence relations

We finish the chapter by focusing on inductively defined sequences.

Definition 6.3 A *recurrence relation* is a sequence $(a_n)_{n\geq 0}$ of real numbers so that for some fixed $n \geq 1$, the term a_n is defined by the previous terms in the sequence.

The term a_n may be defined by one or more than one such terms. As recurrence relations form such a broad topic, we consider a particular kind with a nice structure.

Definition 6.4 Suppose that the recurrence relation $(a_n)_{n\geq 0}$ satisfies

$$a_n = Aa_{n-1} + Ba_{n-2},$$

where A, B are non-zero real numbers. We refer to this sequence as a *second-order linear homogeneous recurrence relation.*

Note that second-order linear homogeneous recurrence relations have general terms that

depend on the previous two terms in the sequence. Although not part of the definition, we are usually given a few values of such sequences in their definition, such as the terms a_0 and a_1.

Example 6.2 The following are both examples of second-order linear homogeneous recurrence relations.

1. The *Fibonacci sequence* is defined by the recurrence relation

$$a_{n+1} = a_n + a_{n-1},$$

   where $n \geq 1$ with $a_0 = 0$, $a_1 = 1$. In this example, $A = B = 1$.

2. Suppose that $a_0 = 1, a_1 = 4$, and let $a_n = 6a_{n-1} - 9a_{n-2}$, for all $n \geq 2$. In this case, $A = 6$ and $B = -9$.

3. The recurrence relation $a_n = a_{n-1} + 2a_{n-2} + 3a_{n-3}$, where $n \geq 3$ is not a second-order linear homogeneous recurrence relation, as it depends on three previous terms not two.

We derive a closed form expression for the general term of second-order linear homogeneous recurrence relations. For this, we need the following definition.

Definition 6.5 Suppose that we are given the recurrence relation $(a_n)_{n\geq 0}$ defined by

$$a_n = Aa_{n-1} + Ba_{n-2},$$

where A, B are non-zero real numbers. The quadratic polynomial

$$x^2 - Ax - B = 0$$

is the *characteristic equation* of the recurrence relation.

As a quadratic equation, the characteristic equation has equal or distinct roots. These roots may be complex numbers, although we only focus on the cases when they are real numbers in this text. The main theorem of this section is the following, whose proof is omitted.

Theorem 6.12 Suppose that the recurrence relation $(a_n)_{n\geq 0}$ satisfies

$$a_n = Aa_{n-1} + Ba_{n-2},$$

where A, B are non-zero real numbers.

1. If the characteristic equation has two distinct roots r_1 and r_2, then

   $$a_n = C{r_1}^n + D{r_2}^n,$$

   where C and D are real numbers determined by the terms a_0 and a_1.

2. If the characteristic equation has a single root r, then

   $$a_n = Cr^n + Dnr^n,$$

   where C and D are real numbers determined by the terms a_0 and other known terms in the sequence.

Notice there are two general forms to the solution of a second-order linear homogeneous recurrence relation depending on whether the roots of the characteristic equation are equal or not.

To illustrate how we may apply Theorem 6.12, we now return to our examples and give closed-form expressions for the general terms of the sequences.

Example 6.3 1. The Fibonacci sequence is defined by the recurrence relation

$$a_{n+1} = a_n + a_{n-1},$$

where $n \geq 1$ with $a_0 = 0$, $a_1 = 1$. We have the characteristic equation:

$$x^2 - x - 1 = 0,$$

which has roots

$$r_1 = \frac{1+\sqrt{5}}{2}, r_2 = \frac{1-\sqrt{5}}{2}.$$

Hence, by Theorem 6.12, we have that for all $n \geq 0$

$$a_n = C\left(\frac{1+\sqrt{5}}{2}\right)^n + D\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

From the case $n = 0$, we have that the equation $C + D = 1$. From the case $n = 1$, we have the equation

$$C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

Using the fact that $C = D - 1$, we may solve these two linear equations in C and D to give that

$$C = \frac{1+\sqrt{5}}{2\sqrt{5}}, D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

We find after simplification that for all $n \geq 0$ that

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

Even though the irrational numbers $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$ appear in the solution, note that all of the terms are integers. The irrational number $\frac{1+\sqrt{5}}{2}$ is called the *golden ratio*.

2. For the recurrence relation $a_0 = 1, a_1 = 4$, and let $a_n = 6a_{n-1} - 9a_{n-2}$, for all $n \geq 2$, the characteristic equation is:

$$x^2 - 6x + 9 = 0,$$

which has a unique root $r = 3$. By Theorem 6.12, we have that for all $n \geq 0$, $a_n = C3^n + Dn3^n$. From the case $n = 0$, we derive that $C = 1$, and from $n = 1$, we have that $3C + 3D = 4$, and so $D = \frac{1}{3}$. Hence, for all $n \geq 0$,

$$a_n = 3^n + \frac{1}{3}n3^n.$$

6.5 Exercises

(6.1) Let X be a set with n elements, where $n \geq 1$ is an integer. Prove that the number of subsets of X is 2^n.

(6.2) Prove that for integers $n \geq 1$ that

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

(6.3) Prove that for an integer $n \geq 1$ that

$$\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2.$$

(6.4) Prove that for all integers $n \geq 1$, $2^n < 3^n$.

(6.5) Show that for all integers $n \geq 1$, $7^{2n} - 48n - 1$ is divisible by 2304.

(6.6) Show that for integers $n \geq 2$ that

$$\prod_{k=2}^{n} \left(1 - \frac{1}{k^2}\right) = \frac{n+1}{2n}.$$

(6.7) Show that for integers $n \geq 1$ that

$$\prod_{k=1}^{n} \left(1 + \frac{1}{k^2}\right) \leq n + 1.$$

(6.8) Use induction to prove that the number of edges in a complete graph K_n is $\frac{n(n-1)}{2}$, where $n \geq 1$ is an integer.

(6.9) Show that for all integers $n \geq 5$ that $n^2 < 2^n$.

(6.10) Show that for all integers $n \geq 4$ that $2^n < n!$.

(6.11) Prove that

$$\frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \cdots + \frac{n}{n \times (n+1)} = \frac{n}{n+1}.$$

(6.12) Prove that $n^3 + 2n$ is divisible by 3 for all integers $n \geq 0$.

(6.13) Show that $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ is an even integer for all integers $n \geq 1$. (*Hint*: Use strong induction.)

(6.14) If a graph G of order n contains no triangle K_3, then it contains at most $\frac{n^2}{4}$ edges. (*Hint*: Use strong induction on n. In the induction step, remove a pair of adjacent vertices.)

(6.15) Show that every graph $G = (V, E)$ has at least $|V| - |E|$ components.

(6.16) Let (X, R) be a finite poset. Use induction to prove that (X, R) contains a minimal element.

(6.17) Let (X, R) be a finite total order with $|X| = n$. We say that a function $f : \{1, 2, \ldots, n\} \to X$ is *order preserving on* (X, R) if for all $1 \leq i, j \leq n$, if $i < j$ then $f(i)Rf(j)$. Prove that there is a unique order-preserving bijection on (X, R). (*Hint:* Use induction on $|X|$ and

use the fact that any order-preserving bijection f must satisfy $f(z) = z$, where z is the greatest element of (X, R).)

(6.18) Show that $\binom{2n}{n} < 2^{2n-2}$ for all integers $n \geq 5$.

(6.19) Prove that each integer $n \geq 12$ is a sum of 4's and 5's. (*Hint*: Verify this for $n = 12, 13, 14, 15$ and then use strong induction on $n \geq 16$.)

(6.20) Assuming that $\sin x \neq 0$ for a real number x, prove that for an integer $n \geq 1$ that

$$\cos x \cdot \cos 2x \cdot \cdots \cdot \cos 2^{n-1}x = \frac{\sin 2^n x}{2^n \cdot \sin x}.$$

(6.21) Let $i^2 = -1$. Prove *De Moivre's formula*: for an integer $n \geq 1$ and x a real number, we have that

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx.$$

(6.22) Let $x \neq 1$ be a real number and let a be real number. For an integer $n \geq 1$, prove that

$$\sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x}.$$

(6.23) Prove for an integer $n \geq 1$ that

$$\sum_{k=1}^{n} \frac{1}{k^2} < 2 - \frac{1}{n}.$$

(6.24) Let $a_0 = 1$ and $a_1 = 8$. Define $a_n = 2a_{n-1} + 2a_{n-2}$ for all integers $n \geq 2$. Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.25) Suppose that $a_0 = 1$ and $a_1 = 3$ and for integer $n \geq 2$ that

$$a_n = 4a_{n-1} - 4a_{n-2}.$$

Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.26) Suppose that $a_0 = 1$ and $a_1 = -1$ and for integer $n \geq 2$ that

$$a_n = 4a_{n-2}$$

Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.27) Suppose that $a_0 = 1$ and $a_1 = 8$ and for integer $n \geq 2$ that

$$a_n = a_{n-1} + 2a_{n-2}.$$

Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.28) Suppose that $a_0 = 2$ and $a_1 = 3$ and for integer $n \geq 2$ that

$$a_n = 3a_{n-1} + 4a_{n-2}.$$

Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.29) Suppose that $a_0 = 5$ and $a_1 = 8$ and for integer $n \geq 2$ that

$$a_n = 3a_{n-1} + 4a_{n-2}.$$

Find a closed-form expression for the general term a_n, where $n \geq 0$.

(6.30) Suppose that $a_0 = 9$ and $a_1 = 20$ and for integer $n \geq 2$ that

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

Find a closed-form expression for the general term a_n, where $n \geq 0$.

6.6 Selected Answers and Hints

(6.1) In the induction step, fix an element $u \in X$ and consider the subsets containing u and those not containing u.

(6.2) Use the fact that $\frac{(-1)^n n(n+1)}{2} + (-1)^{n+1}(n+1)^2 = \frac{(-1)^n(n+1)}{2}(-n-2)$.

(6.3) Use the fact that $\frac{1}{4}n^2(n+1)^2 + (n+1)^3 = \frac{1}{4}(n+1)^2(n+1+1)^2$.

(6.4) Use the fact that $2^{n+1} = 2 \cdot 2^{n+1}$.

(6.5) Let $f(n) = 7^{2n} - 48n - 1$. Show that $f(n+1) = 49 \cdot f(n) + 2304n$.

(6.8) In the inductive, step, if we remove a vertex from the complete graph K_{n+1}, then we remove n edges.

(6.9) Use the fact that $2^{n+1} = 2 \cdot 2^n > 2n^2 > (n+1)^2$.

(6.10) Apply the induction hypothesis to give $(n+1)2^n < (n+1)n!$.

(6.12) Use the fact that $(n+1)^3 + 2(n+1) = n^3 + 2n + 3(n^2+n+1)$.

(6.15) Use induction on the number of edges of the graph. In the induction step, consider what happens when you remove an edge.

(6.16) Use induction on $|X|$.

(6.18) Use the fact that $\binom{2n+2}{n+1} = \binom{2n}{n}\frac{(2n+2)(2n+1)}{(n+1)(n+1)}$.

(6.20) Use the identity $\sin 2y = 2\sin y \cos y$.

(6.21) Use the addition formulas $\sin x + y = \sin x \cos y + \sin y \cos x$ and $\cos x + y = \cos x \cos y - \sin x \sin y$.

(6.22) Use the fact that $(x-1)x^{n+1} + x^{n+1} - 1 = x^{n+2} - 1$.

(6.23) In the induction step, use the fact that $2 - \frac{n^2+n+1}{n(n+1)^2} < 2 - \frac{n(n+1)}{n(n+1)^2} = 2 - \frac{1}{n+1}$.

(6.24) $a_n = \frac{1}{6}((3-7\sqrt{3})(1-\sqrt{3})^n + (3+7\sqrt{3})(1+\sqrt{3})^n)$.

(6.25) $a_n = 2^{n-1} + 2 \cdot 2^{n-1}$.

(6.26) $a_n = 2^{n-2}(3(-1)^n + 1)$.

(6.27) $a_n = 3 \cdot 2^n - 2(-1)^n$.

(6.28) $a_n = (-1)^n + 4^n$.

(6.29) $a_n = \frac{1}{5}(12 \cdot (-1)^n + 13 \cdot 4^n.)$

(6.30) $a_n = 7 \cdot 2^n + 2 \cdot 3^n$.

Index

$G[V(H)]$, 38
$K_{i,j}$, 39
$N_G(v)$, 35
$N_G[v]$, 35
$P(n,r)$, 79
Q_n, 40
$X \cap Y$, 12
$X \cup Y$, 12
$X \setminus Y$, 12
$X \times Y$, 17
$X \triangle Y$, 13
X^c, 12
$\Delta(G)$, 35
$\chi(G)$, 43
$\deg_G(v)$, 35
$\delta(G)$, 35
$\operatorname{diam}(G)$, 37
$\exists$, 24
$\forall$, 24
$\gamma(G)$, 45
$\gcd(a,b)$, 95
$\mathbb{N}$, 11
$\mathbb{Q}$, 12
$\mathbb{R}$, 12
$\mathbb{Z}$, 12
$\mathcal{P}(X)$, 17
$\overline{G}$, 39
$\subseteq$, 10
$\varnothing$, 10
$a \equiv b \pmod{n}$, 102
$d_G(u,v)$, 37

antisymmetric, 61
arithmetic sequence, 85

base case, 113
biconditional, 21
bijective function, 66
binary relation, 56
Binomial Theorem, 82, 117

cardinality, 10
chain, 62
characteristic equation, 122
closed neighbor set, 35
co-domain, 64
combination, 79
comparable, 62
components, 39
composite number, 95
congruence, 102
conjunction, 21
contradiction, 23
contrapositive, 23
converse, 23
countable set, 18
cycle, 37

De Moivre's formula, 126
disjoint sets, 13
disjunction, 21
divisor, 95

domain, 64
dominating set, 45
domination number, 43, 45

edge set, 32
end-vertex, 41
equivalence class, 59
equivalence relation, 59
Euclid's theorem, 96
existential quantifier, 24

factorial, 79
Fibonacci sequence, 120
First Theorem of Graph Theory, 36
function, 64
Fundamental Theorem of Arithmetic, 96, 119

General Pigeonhole Principle, 78
Generalized product rule, 77
Generalized sum rule, 74
geometric sequence, 85
graph, 32
  bipartite, 39
  complement, 39
  complete, 38
  complete bipartite, 39
  connected, 39
  directed, 46
  disconnected, 39
  forest, 41
  hyercube, 40
  null, 39
  order, 32
  size, 32
  star, 41
  tree, 41
greatest common divisor, 95
greatest element, 63

Hasse diagram, 62

implication, 21
in-degree, 46
incomparable, 62
independent set, 39
induction hypothesis, 113
induction step, 113
injective function, 65

least element, 62
linear Diophantine equation, 100

maximal element, 63
maximum degree, 35
minimal element, 63
minimum degree, 35

negation, 21
neighbor, 35
neighbor set, 35

ordered pair, 11
out-degree, 47

parity, 93
partial order, 61
Pascal's triangle, 83
path, 37
permutation, 79
power set, 17
predicate, 24
prime number, 95
Principle of Inclusion-Exclusion, 75
Product rule, 76

recurrence relation, 121
reflexive, 58

second-order linear homogeneous recurrence relation, 121
sequence, 85
singleton, 11
spanning subgraph, 37

statement, 20
strong induction, 119
subgraph, 37
    induced, 37
subset, 10
Sum rule, 74
surjective function, 66
symmetric, 58

tautology, 23
The Pigeonhole Principle, 77
total order, 62
transitive, 58
tree
    spanning, 41

uncountable set, 19
universal quantifier, 24
unordered pair, 11

vertex
    isolated, 35
    universal, 35
vertex set, 32

walk, 36