21-127 Lecture Notes
Fall 2025

Gregory Johnson

December 3, 2025

Department of Mathematics
Carnegie Mellon University

Contents

Part I.

Sets and Logic

1. August 25

1.1. Introduction to Concepts

Concepts of Mathematics may feel like a fundamental shift from the math courses you've taken before. While you may be comfortable with challenging problems and computations from calculus or beyond, this course emphasizes something different: rigorous abstraction and formal proof. This transition can seem intimidating at first, since it asks you to move from working with concrete formulas to reasoning about formal definitions and general objects—a skill that lies at the heart of advanced mathematics and computer science. The good news is that this skill can be learned with steady practice, and our goal is to help you develop it step by step. With guidance and persistence, you will gradually reshape the way you approach problems and prepare yourself for the demands of higher-level study.

Caution: Some students in this course may have seen related ideas in previous math or computer science classes, or may even be taking *Concepts* for a second time. It is important, however, not to assume results or anticipate concepts that have not yet been formally introduced in lecture. We will proceed carefully and deliberately, building our understanding one step at a time. The only prerequisite for this course is a solid grasp of algebraic principles and arithmetic operations.

1.1.1. Mathematical Statements

In mathematics, our primary focus is on *mathematical statements* (or *propositions*). These are combinations of mathematical symbols and English words that can be definitively classified as either true or false, with no ambiguity.

Definition. A *mathematical statement*, also known as a *proposition*, is a declarative sentence (or string of sentences) that can be definitively classified as either true or false, meaning it possesses a determinable truth value.

Examples 1.1.1.

- $1 + 1 = 2$

  This is a `True` proposition.

- If n is a nonnegative integer then $n^2 + n + 41$ is a prime number.

  This is a `False` proposition. The first counterexample occurs at $n = 40$.

- There are infinitely many prime numbers of the form $2^n - 1$, where n is an integer.

  It is not known whether this is `True` or `False`, but it is still a valid proposition. It has a truth value, even if we have not determined which one yet.

Non-Examples 1.1.2.

- $x^2 \geq 8$

  By itself this is not a proposition. Without knowing what x represents, we cannot verify whether the statement is `True` or `False`. Later we will see that this is an example of what we call a *variable proposition* (also known as an *open sentence* or *predicate* in logic).

- $1 + = 2$

  This is a nonsensical string of symbols and has no meaning.

- This statement is false.

  Although this is a declarative sentence, it does not have a truth value. If the statement were `True` then it would also be `False`, and if it were `False` then it would also be `True`. Our definition of a mathematical statement excludes paradoxes like this.

(A course devoted specifically to symbolic logic would offer a more formal definition of a mathematical statement, but this explanation is sufficient for our purposes.)

Special Names for Proven Statements

When reading a mathematics textbook or paper, you might encounter established results labeled as *theorem*, *corollary*, *lemma*, or simply *proposition*. These labels help convey the role and importance of a given result.

- **Theorem**: An important result.
- **Corollary**: A result that follows from a theorem with little extra work. For instance, applying a general theorem to a special case.
- **Lemma**: A smaller result that is useful in proving more significant results later.
- **Proposition**: A general term that can apply to any result. It is often used for results that are not substantial enough to be called theorems.

1.1.2. Formal Definitions

In mathematics, a definition fixes the exact meaning of a term so that everyone is using it consistently. These definitions often arise from recurring mathematical concepts. For example, consider the following definition of an isosceles triangle.

Definition. A triangle is called *isosceles* if and only if two of its sides have equal length.

A few things to note here.

- The phrase "if and only if" is often abbreviated as "iff". It indicates that the statement is biconditional: any triangle called "isosceles" has two sides of equal length, **and** any triangle with two sides of equal length is classified as "isosceles". All definitions are biconditional, even if the author phrases them differently.
- Definitions must be unambiguous. We may not infer anything about the term other than what is stated in the definition. Given the definition above, any triangle with either two or three sides of equal length satisfies the definition of being "isosceles". If the intention were to describe only triangles with exactly two sides of equal length, that restriction would need to be explicitly stated.
- We may need to appeal to other formal definitions to fully understand this one. For instance, what is a "triangle", a "side" of a triangle, or the "length" of a side? You may think of definitions as abbreviations for much longer mathematical statements or concepts. For example, it is easier to say "isosceles triangle" than "a polygon with exactly three sides in which at least two of them are equal in length", especially if the concept comes up frequently.

Formal definitions play a crucial role in crafting rigorous mathematical proofs. Relying on precise definitions is essential for moving from vague, intuitive reasoning to mathematically correct and formally articulated arguments.

1.1.3. Proofs

In your previous math courses, you have likely encountered proofs for different theorems. But what exactly is a proof? How do we determine the truth of a proposition? Unlike in law, where terms such as "preponderance of evidence" and "beyond a reasonable doubt" are used, mathematicians do not rely on weight of evidence. Instead, we seek certainty. Consider the following example.

Proposition: For any positive integer n, the greatest common divisor of $n^{17} + 9$ and $(n+1)^{17} + 9$ is 1.

You could have a computer plug in values for n for a lifetime and never find a counterexample. You might then begin to suspect that the proposition is true. Such a statement is called a *conjecture*, meaning a claim believed to be true but not yet proven. However,

in this case the conjecture is false. The first counterexample occurs at

$$n = 8424432925592889329288197322308900672459420460792433$$

If a proposition is true, we clearly need more than computational checks. So what is a proof?

Definition. A *proof* is a logical argument that establishes the truth of a mathematical statement beyond any doubt.

Important Criteria for Proofs

- **Precision**: Every statement should be true and unambiguous.
- **Logic**: Each step must follow from previous steps with proper motivation and explanation.
- **Organization**: The argument should proceed in a clear order, starting from assumptions and ending with the desired result.
- **Clarity**: Steps should be connected with enough explanation for the reader to follow. Write your proofs with the audience of a typical student in this course in mind, including enough detail for them to understand.

It will take time to grow comfortable with writing proofs. Look at examples in the lecture notes and textbook to see how proofs are typically structured. Practice by working on worksheet problems and unassigned exercises before consulting solutions. Re-read your own proofs and make revisions. Pay close attention to feedback you receive.

Later, when we reach the logic section, we will begin studying proof-writing strategies based on the structure of statements. First, however, we will need to establish some of the basic vocabulary related to sets and logic.

1.2. Exploring Statements and Proofs

Exercise 1.2.1. Which of the following are *mathematical statements*? Justify your answer.

(a) Pittsburgh has the most bridges of any city in the world.

(b) Pittsburgh is the best city in the world.

(c) Where is Pittsburgh?

(d) 2 is a prime number.

(e) n is a prime number.

(f) All positive integers are prime.

(g) If n is an even integer greater than 3 then n can be written as the sum of 2 primes.

(h) $5^2 = 25$.

(i) $x^3 + 1 = 28$.

(j) If $x^3 + 1 = 28$ then $x = 3$.

Exercise 1.2.2. Consider the following theorem and proof:

Theorem: If m and $m + n$ are both even integers then n is an even integer.

Proof: Let $m = 2a$ and $n = 2b$, where a and b are integers. Then $m + n = 2a + 2b$. Subtracting m from both sides we get

$$n = 2a + 2b - m = 2a + 2b - 2a = 2b$$

Therefore we have shown n is even. □

(a) Is this theorem true?

(b) Is the proof valid and well written? Explain your reasoning.

(c) If your answer to (a) is yes and (b) is no, try to fix the proof. What are the basic assumptions of this proposition? If your answer to (a) is no, try to fix the proposition to make it true and then prove it.

Exercise 1.2.3.

1. Consider the following proposition and the proposed proof given by a student:

   Proposition: $\sqrt{xy} \leq \frac{x+y}{2}$

   Proof:

$$\begin{aligned} 0 \leq (x-y)^2 &\implies 0 \leq x^2 - 2xy + y^2 \\ &\implies 4xy \leq x^2 + 2xy + y^2 \\ &\implies xy \leq \frac{(x+y)^2}{4} \\ &\implies \sqrt{xy} \leq \frac{x+y}{2} \end{aligned}$$

   □

   a) Is the proposition true? Are the assumptions stated clearly?

   b) Is the proof valid and well written? Explain your reasoning.

   c) If the proposition is true but the proof is not fully correct, try to fix the proof. If the proposition is false, propose a corrected statement and prove it.

2. Let x, y, z be nonnegative real numbers such that $y + z \geq 2$. Using what you have learned from the previous problems:

   a) Write a proposition stating that under these conditions $(x+y+z)^2 \geq 4x+4yz$.

   b) Prove your proposition. (*Hint: For any real numbers a and b, $a^2+b^2 \geq 2ab$.*)

Exercise 1.2.4. A father, mother, and son were dining when another family (also a father, mother, and son) noticed their resemblance. The second father asked, "How old are you? We must be around the same age." The first father, a mathematician, replied cryptically: "Our ages sum to 72, I am six times as old as my son, and when I am twice his age later in life, our combined ages will double our current total."

Set up a system of equations based on this information and determine the ages of the three family members.

Exercise 1.2.5.

(a) Solve the following system of equations for (x, y, z):

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 8 \\ x - 2y - z &= -2 \end{aligned}$$

(b) Solve the similar system for (x, y, z):

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 9 \\ x - 2y - z &= -2 \end{aligned}$$

(c) Solve one more similar system:

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 9 \\ x - 2y - z &= -1 \end{aligned}$$

(d) Compare the results:

   (i) From part (a) to part (b), find the magnitude of the change in each variable:

$$|\Delta x|, \quad |\Delta y|, \quad |\Delta z|.$$

   Repeat for the change from part (b) to part (c).

   (ii) Which variable's value is most affected by these small changes in the equations? Which is least affected?

(iii) How do the ratios of the largest to smallest changes compare between the two transitions (from (a)→(b) and (b)→(c))?

(iv) Based on your results, what can you say about how the solution responds when you slightly change the constants on the right-hand sides?

2. August 27

2.1. Basic Set Theory

A set is a foundational concept in mathematics, and much of mathematics can be expressed in terms of set theory. In formal set theory, a set is treated as an undefined primitive, with its properties and behavior described by axioms. This level of rigor goes beyond the scope of this course. Instead, we will adopt a naive, intuitive understanding of sets that is sufficient for our purposes.

Definition. A *set* is a well-defined collection of objects, considered as a single object in its own right. The objects in a set are called *elements* (or *members*). A set is *well-defined* if, given any object, we can unambiguously decide whether it belongs to the set.

For example, we may define P as the set of all prime numbers, or S as the set of all students currently enrolled in 21-127.

Notation. We commonly use capital letters to denote sets and lowercase letters to denote elements of sets. We write $x \in X$ to indicate that "x is an element of X," and $x \notin X$ to indicate that "x is not an element of X."

2.1.1. How to Define a Set

In mathematics, defining a set using a description, such as "Let P be the set of prime numbers," can sometimes be acceptable for informal discussions. However, such definitions are often unclear or ambiguous and can lead to misunderstandings or inaccuracies. Precise and unambiguous definitions are crucial for rigorous mathematical reasoning and proofs.

To avoid these issues, mathematicians use formal methods to define sets. Two common methods are *roster notation* and *set-builder notation.*

Roster Notation

Roster notation lists all the elements of a set explicitly. For example, the set of the first five prime numbers can be written as $P = \{2, 3, 5, 7, 11\}$. This method is straightforward

but only practical for sets with a small number of elements.

When dealing with sets that have a clear and recognizable pattern, we may sometimes use an informal "implied list" notation with ellipses, such as

$$E = \{0, 2, 4, 6, 8, 10, \ldots\}$$

In these cases, it is important to include a clarifying setence to specify the pattern: "Here E represents the set of nonnegative, even integers." Although this method is informal, it sometimes can be the easiest way to convey the idea to the reader.

Set-Builder Notation

Set-Builder Notation provides a more flexible and precise way to define sets, especially those with infinitely many elements. It describes the properties that characterize the elements of the set. For instance, we can define $P(x)$ to be the predicate "$x^2 \geq 8$". As we discussed before, this is not a proposition because x is not defined, but when a real number is substituted for x, it becomes a proposition.

If $P(x)$ is a predicate, then the set S of all elements x from a larger set A which satisfy $P(x)$ is denoted as

$$S = \{x \in A \mid P(x)\} \quad \text{or} \quad S = \{x \in A : P(x)\}$$

On the left side of the vertical line (or colon), we indicate which set our elements are coming from, and on the right side of the vertical line, we indicate which properties must hold of them.

Example 2.1.1. Let S be the set of students in 21-127. We may define a new set F as

$$F = \{x \in S \mid x \text{ is a freshman}\}$$

Then F is the set of all freshmen in 21-127.

Example 2.1.2. Let $\mathbb{R}$ be the set of all real numbers. We may define a new set S as

$$S = \{x \in \mathbb{R} \mid x^2 - x - 2 > 0\}$$

This is the set of all real numbers satisfying the inequality $x^2 - x - 2 > 0$.

2.1.2. Set Equality and Subsets

The defining characteristics of sets stem from the definition of set equality.

Definition. Let A and B be sets. We say that A and B are *equal*, denoted $A = B$, iff the following two properties hold:

1. Every element from A is also an element of B.
2. Every element from B is also an element of A.

Note. From the definition of set equality, we see that order, repetition, and set presentation do not matter when determining if two sets are the same. For example, if we define sets A, B, and C as

$$A = \{1, -1\}, \quad B = \{1, -1, 1\}, \quad C = \{x \in \mathbb{R} \mid x^2 = 1\}$$

then $A = B = C$.

Definition. We say a set A is a *subset* of a set B, denoted $A \subseteq B$, iff every element of A is also an element of B.

Note. We can now rephrase the definition of set equality in terms of subsets:

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

The $\subseteq$ relation has a property known as *transitivity*, which we will discuss in more detail in the future. Below, we will see how transitivity is an immediate consequence of our formal definition above.

Theorem 2.1.3 (Transitivity of the Subset Relation)**.** *For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

(We will feel our way through our first proof.)

Proof. Assume that A, B, and C are arbitrary sets with the property that $A \subseteq B$ and $B \subseteq C$. Our goal is to show that $A \subseteq C$.

We start by taking an arbitrary element $a \in A$. Since we are given that $A \subseteq B$, by the definition of a subset, every element of A is also an element of B. Therefore, we have $a \in B$.

Next, we use the fact that $B \subseteq C$. By the definition of a subset, every element of B is also an element of C. Since we have already established that $a \in B$, it follows that $a \in C$.

Since a was chosen arbitrarily from A, this reasoning applies to all elements of A. Thus, every element of A is also an element of C, which means $A \subseteq C$ by definition of a subset.

Therefore, we have shown that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. □

Notation.

- $A \not\subseteq B$ means "A is not a subset of B". By our definition of a subset, this means that there exists an element $a \in A$ such that $a \notin B$.
- $A \subsetneq B$ or $A \subset B$ means "A is a proper subset of B". That is, $A \subseteq B$ but $A \neq B$.

Exercise 2.1.4. Define sets A, B, and C as follows:

$$A = \{1, 2, 3, 4, 5, 6\}$$
$$B = \{1, 2, 3, 4, 5, 6, \{1, 2\}, \{3\}, \{5\}\}$$
$$C = \{x \in A \mid x^2 > 4\}$$

Determine whether the following statements are true or false.

(a) $3 \in A$

(b) $\{3\} \in B$

(c) $\{1, 2\} \subseteq A$

(d) $A \in B$

(e) $\{1, 2\} \in B$

(f) $4 \in C$

(g) $\{x \in B \mid x \notin A\} = \{\{1, 2\}, \{3\}, \{5\}\}$

(h) $\{6\} \in A$

(i) $C \subseteq A$

(j) $\{1, 2\} \subseteq B$

(k) $3 \in B$

(l) $\{3\} \in A$

(m) $\{4\} \subsetneq C$

(n) $B \subseteq A$

(o) $\{\{3\}\} \subseteq B$

(p) $A \subseteq B$

(q) $5 \subseteq B$

(r) $\{x \in B \mid x \notin A\} = \{1, 2, 3, 5\}$

(s) $\{x \in B \mid x \notin A\} = \{\}$

(t) $D \subseteq C$ where
$D = \{x \in A \mid x \text{ is even}\}$

(u) $\{\{1, 2\}, \{3\}\} \subseteq B$

2.1.3. Number Sets

Several sets of numbers are so commonly referred to that they get fixed notation. For now, several properties of these sets from elementary algebra will be taken for granted.

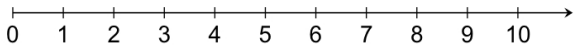
The Natural Numbers

$\mathbb{N}$ is used to denote the set of natural numbers. That is,

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

$\mathbb{N}$ is defined to be the smallest set containing 0 and closed under the successor function (the $+1$ function). Informally, the natural numbers are the points on a number line that

can be obtained by starting at 0 and moving right by a unit of length any number of times. (Our standard counting numbers.)



Properties of $\mathbb{N}$ we may assume:

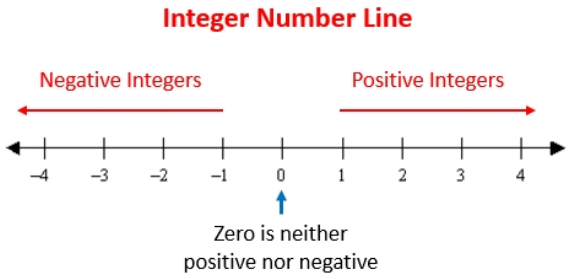
- There is no largest natural number.
- 0 is the smallest natural number.
- The sum of two natural numbers is a natural number.
- The product of two natural numbers is a natural number.

The Integers

$\mathbb{Z}$ is used to denote the set of all integers. That is,

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

The integers are the set of natural numbers along with their additive inverses (their negatives). We can think of $\mathbb{Z}$ as the set of points on a number line that can be obtained by moving either left or right by a unit length at a time. (Later, we will formally construct this set from $\mathbb{N}$.)



Note. We will often use $\mathbb{Z}^+$ to denote the set of positive integers. That is,

$$\mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$$

Properties of $\mathbb{Z}$ we may assume:

- There is neither a largest nor a smallest integer.
- The sum, difference, or product of two integers is an integer.

We will explore the properties of the integers in more depth in the number theory section of the course, but we will discuss a few basic properties here.

Definition (Integer Divisibility)**.** For $a, b \in \mathbb{Z}$, we say that a *divides* b, denoted $a \mid b$, if and only if there exists an integer c such that $b = ac$.

Example 2.1.5.

- $2 \mid 6$ because $6 = 2 \cdot 3$.
- $3 \nmid 7$ because $7 \neq 3c$ for any $c \in \mathbb{Z}$.
- $0 \mid 0$ because $0 = 0 \cdot k$ for any integer k.
- $2 \mid 0$ because $0 = 2 \cdot 0$.

From the definition of the integer divisibility, we can prove properties of this relation.

Theorem 2.1.6 (Transitivity of Divisibility)**.** *For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Assume that $a, b, c \in \mathbb{Z}$ such that $a \mid b$ and $b \mid c$. Then, by definition of integer divisibility, there exists $m, n \in \mathbb{Z}$ such that $b = ma$ and $c = nb$. We then have the following chain of equalities, using the associativity of multiplication.

$$c = nb = n(ma) = (nm)a$$

Since $nm \in \mathbb{Z}$, it follows that $a \mid c$. □

Exercise 2.1.7. Write the following sets out in formal set-builder notation.

(a) A is the set of integers that can be expressed as the difference of two perfect squares.

(b) $B = \{1, 8, 27, 64, \ldots\}$ *(Assume the pattern continues indefinitely.)*

(c) C is the set of all positive divisors of 36.

Exercise 2.1.8. Determine if the following statements are True or False. Justify your answer.

(a) $0 \mid 5$

(b) $5 \mid 0$

(c) For $a, b \in \mathbb{Z}$, if $a \mid b$ then $a \leq b$.

(d) For $a, b \in \mathbb{N}$, if $a \mid b$ then $a \leq b$.

(e) The remainder, r, when an integer a is divided by a nonzero integer b is always nonnegative.

Exercise 2.1.9.

(a) Provide an example of $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ and $ab \mid c$

(b) Provide an example of $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ but $ab \nmid c$

3. August 29

3.1. Basic Set Theory

3.1.1. Number Sets

The Integers continued

Using integer divisibility, we define what it means for an integer to be even or odd.

Definition (Even/Odd)**.** An integer n is called *even* if and only if $2 \mid n$. An integer n is called *odd* if and only if n is not even, i.e., $2 \nmid n$.

Note. By our definition, every integer is either even or odd, but not both.

The following theorem formalizes our basic idea of "division with remainder" from grade school. We will state it without proof for now, but we will prove it in the next couple of weeks, and we will use this theorem heavily in the number theory section.

Theorem 3.1.1 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < |b|$. Here, q is called the quotient and r is referred to as the remainder.*

For example, if $a = 44$ and $b = 7$, the only way to write $44 = 7q + r$ with $0 \leq r < 7$ is

$$44 = 7 \cdot 6 + 2$$

If $a = -44$ and $b = 7$, the only way to write $-44 = 7q + r$ with $0 \leq r < 7$ is

$$-44 = 7 \cdot (-7) + 5$$

And if $a = 44$ and $b = -7$, the only way to write $44 = (-7)q + r$ with $0 \leq r < 7$ is

$$44 = (-7) \cdot (-6) + 2$$

Corollary 3.1.2 (Equivalent Definition of Even/Odd)**.** *For any $n \in \mathbb{Z}$:*

- *n is even if and only if $n = 2m$ for some $m \in \mathbb{Z}$.*
- *n is odd if and only if $n = 2m + 1$ for some $m \in \mathbb{Z}$.*

Exercise 3.1.3. For each pair (a, b), find the unique integers q (quotient) and r (remainder) guaranteed by the Division Algorithm.

(a) $a = 17$, $b = 5$

(b) $a = -17$, $b = 5$

(c) $a = 84$, $b = -12$

(d) $a = 7$, $b = 9$

Exercise 3.1.4. Prove the following statement: For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Scaffolding: Let $a, b, c \in \mathbb{Z}$ be arbitrary and fixed integers such that $a \mid b$ and $a \mid c$.

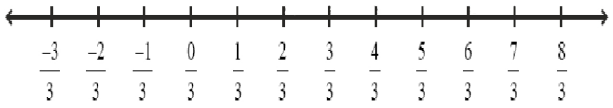
- Write down the formal definition of $a \mid b$.
- Write down the formal definition of $a \mid c$.
- Add the two equations from Step 1 and Step 2 together.
- Factor the resulting sum on the right-hand side.
- Explain why the result of Step 4 satisfies the definition of $a \mid (b + c)$.

The Rational Numbers

$\mathbb{Q}$ is used to denote the "set of all rational numbers". That is

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$$

On a number line, $\mathbb{Q}$ represents the set of points obtained by dividing any unit segment into an equal number of parts. For example, dividing each unit into 3 equal parts gives a subset of the rational numbers, as illustrated below.



Recall that addition, subtraction, multiplication, and division of rational numbers are defined in terms of addition and multiplication of integers:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Thus, many properties of the rational numbers can be derived from our assumed properties of the integers.

Proposition 3.1.5. *The following properties hold for rational numbers:*

1. *The sum (or difference) of two rational numbers is a rational number.*
2. *The product of two rational numbers is a rational number.*
3. *The quotient of two rational numbers, where the divisor is nonzero, is a rational number.*

We will prove property 1 below. The other properties follow similarly and are left as exercises for the reader.

Proof. Let $x, y \in \mathbb{Q}$. By definition of the rational numbers, there exist integers $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$ such that $x = \frac{a}{b}$ and $y = \frac{c}{d}$. Then,

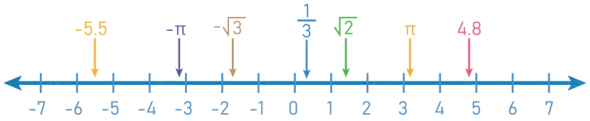
$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{Z}$ with $bd \neq 0$, we conclude that $x + y \in \mathbb{Q}$. □

Note. In addition to these properties, you may also assume that there is neither a largest nor a smallest rational number.

The Real Numbers

$\mathbb{R}$ denotes the set of real numbers. This set includes all the rational numbers $\mathbb{Q}$, as well as all irrational numbers. In other words, $\mathbb{R}$ is the completion of the rationals, filling in all the "holes" on the number line.



Properties of $\mathbb{R}$ we may assume:

- There is neither a largest nor a smallest real number.
- The sum, difference, and product of two real numbers are real numbers.
- A real number divided by a nonzero real number is still a real number.
- The product of two nonzero real numbers is nonzero.

Recall that *intervals* of real numbers are subsets of $\mathbb{R}$ satisfying specific inequalities, as denoted below using set-builder notation. Assume $a, b \in \mathbb{R}$ with $a < b$:

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\} \qquad (-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$$
$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\} \qquad (-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$$
$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\} \qquad (a, \infty) = \{x \in \mathbb{R} \mid a < x\}$$
$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \qquad [a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$$

Another important subset of the reals to define is the set of *irrational numbers*. These are real numbers that cannot be expressed as a ratio of two integers. Examples include $\sqrt{2}$ and π. Formally, the set of irrational numbers is:

$$\{\text{irrational numbers}\} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$$

The Empty Set

$\varnothing$ denotes the *empty set*, which is the unique set with no elements. Formally, we write:

$$\varnothing = \{\,\}$$

The First n-many Positive Integers

For any natural number $n \in \mathbb{N}$, we use the notation $[n]$ to denote the set of the first n positive integers. Specifically:

$$[n] = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$$

For example:

$$\begin{aligned} [0] &= \varnothing \\ [1] &= \{1\} \\ [2] &= \{1, 2\} \\ [3] &= \{1, 2, 3\} \\ &\vdots \end{aligned}$$

Note. The notation $[n]$ is used to refer to the set of the first n positive integers, where $[0]$ is the empty set, and $[n]$ for $n \geq 1$ includes all positive integers up to n.

Exercise 3.1.6.

(a) Write the following set in roster notation:

$$A = \left\{ n \in \mathbb{Z} \mid \text{there exists } r \in \mathbb{Q} \text{ s.t. } n = r + \frac{1}{r} \right\}$$

(b) Describe the following set in formal set-builder notation. You may assume that the pattern continues indefinitely.

$$C = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots \right\}$$

(c) Define the sets A and B as follows:

$$A = \{x \in \mathbb{R} \mid x^2 - 4 \geq 0\}$$
$$B = \{y \in \mathbb{R} \mid y \geq 2\}$$

Does $A = B$? Why or why not?

Exercise 3.1.7.

(a) Provide an example of a rational number q and an irrational number x such that qx is irrational.

(b) Provide an example of a rational number q and an irrational number x such that qx is rational.

3.2. Logic

We are in the process of learning a new language. We start with the basic words and terminology to make precise, unambiguous mathematical statements and study the structure of propositions. Understanding the structure of propositions will help us determine how to prove or disprove statements.

3.2.1. Propositional Logic

The most elementary logic we can study is called *propositional logic*. In propositional logic, we examine the logical relationships between various mathematical statements based on their sentence structure.

To study the structure of propositions, we must have a starting point–our atoms for propositional logic.

Definition. An *atomic proposition* (or *atom*) is a proposition whose truth value is independent of the truth value of any other proposition. In particular, an atomic proposition cannot be broken down into simpler propositions.

In propositional logic, we use *propositional variables* such as P, Q, R, etc., to denote atomic propositions. We can think of these in the same way we think of variables in algebra; any proposition may be substituted for these propositional variables. For example, we may define the atomic propositions P and Q as:

$P :=$ "It will rain today."
$Q :=$ "Every prime number greater than 2 is odd."

From here, we will build compound statements using logical connectives. The logical connectives for propositional logic are:

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

With these, we can create more complicated propositions such as the following:

$$\neg(P \rightarrow (\neg Q \wedge R))$$

We will define each of these logical connectives one at a time. To aid in this process, we will use a *truth table*. A truth table is a table used to describe the truth value of a compound proposition under all possible truth values of the atomic propositions within it. If n different atomic propositions appear in the compound statement, then the truth table requires 2^n rows. Truth tables are useful for defining logical connectives and proving logical equivalences of various propositions.

We now proceed to define each of our connectives.

Conjunction

Any two propositions can be combined to form a new proposition called the *conjunction* of the original propositions. A conjunction is translated as "and" and is denoted with the $\wedge$ symbol. For propositions P and Q, we define the truth value of the compound proposition $P \wedge Q$ as:

$P \wedge Q$ is true if and only if both P and Q are true.

We can summarize this with a truth table:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

We can also combine two propositions to form a new proposition called the *disjunction* of the original propositions. A disjunction is translated as "or" and is denoted with the $\vee$ symbol. For propositions P and Q, we define the truth value of the compound proposition $P \vee Q$ as:

$P \vee Q$ is true if and only if either P is true or Q is true or both.

Again, we summarize this with a truth table:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Negation

Given a single proposition, we can form a new proposition called its *logical negation*. A negation is translated as "not" and denoted $\neg$. If P is a proposition, then we define the truth value of $\neg P$ as:

$\neg P$ is true if and only if P is false.

We present this as a truth table below:

P	$\neg P$
T	F
F	T

Logical Implication

Given two propositions P and Q, we can form the compound proposition "if P then Q", denoted $P \to Q$, known as an *implication*. We define $P \to Q$ to be true **unless** P is true and Q is false. This is best presented as a truth table:

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

This is the hardest to understand of the logical connectives but also the most important. To understand the truth table above, it is helpful to view implication as an obligation or contract. For example, suppose the professor were to say:

> "If you get 100% on the final exam, then you will get an A for the course."

Under what conditions would this statement be false? That is, what would need to happen for the professor to be considered a liar? Hopefully, we can see that the above statement would be a lie only if a student received 100% on the final exam but the professor did not give them an A for the course.

Caution: Do not mistake logical implication for causality. While we often read $P \to Q$ as "P implies Q" in logic, it does not mean that Q can be deduced from P, as we typically mean when we write proofs. There are many logical implications that are true but are not useful and would not be used in ordinary English. For example, the following proposition is always true:

> If you are a student at Carnegie Mellon University, then 2 is a prime number.

Both P and Q are true, making $P \to Q$ true, but there is no causality. Even if you are not a student at Carnegie Mellon University and are reading this statement, it is still true. This brings us to another important point about implications: anytime P is false, $P \to Q$ is true. It is often said that a false proposition implies any proposition.

There is a famous interaction between logician Bertrand Russell and one of his students when first presented with this idea:

> **Student**: "In that case, given that $1 = 0$, prove that you are the Pope."
> **Russell**: "Add 1 to both sides of the equation: then we have $2 = 1$. The set containing just me and the Pope has 2 members. But $2 = 1$, so it has only 1 member; therefore, I am the Pope."

Note that the statement "If $1 = 0$, then I am the pope." would be true regardless of who said it, even the pope.

Terminology for $P \to Q$: P is called the *antecedent*, *hypothesis*, or *supposition*. Q is called the *consequent* or *conclusion*.

Note. If $P \to Q$ is true and P is true, then we can deduce that Q must also be true. This rule of inference is known as *Modus Ponens* and is an essential concept in proof writing.

Below we present some additional terminology for variants of $P \to Q$.

Definition. Let P and Q be atomic propositions.

- The *converse* of $P \to Q$ is $Q \to P$.
- The *contrapositive* of $P \to Q$ is $\neg Q \to \neg P$.
- The *inverse* of $P \to Q$ is $\neg P \to \neg Q$.

The Biconditional Connective

Given two propositions P and Q, we can form the compound proposition "P if and only if Q", denoted $P \leftrightarrow Q$, known as a biconditional statement. We define $P \leftrightarrow Q$ to be true iff P and Q have the same truth values. This is shown in the truth table below:

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Definition. If P and Q are propositional formulas and $P \leftrightarrow Q$ is true for all possible truth values of the atomic propositions, then we say that P and Q are *logically equivalent*, denoted $P \equiv Q$.

Exercise 3.2.1. In propositional logic, a *tautology* is a propositional formula which is always true, regardless of the truth values of the propositional variables. Use a truth table to determine whether or not the following statement is a tautology.

$$((P \to Q) \wedge \neg Q) \to \neg P$$

Exercise 3.2.2. Define the propositions P, Q, and R as follows:

$$\begin{aligned} P :=&\ \text{“It is raining.”} \\ Q :=&\ \text{“There are bears in the area.”} \\ R :=&\ \text{“It is not safe outside.”} \end{aligned}$$

Write each of the following statements symbolically:

(a) It is raining, but there are no bears in the area.

(b) It is unsafe outside whenever bears are in the area and it is raining.

(c) It is not safe outside even though there is neither rain nor bears in the area.

(d) For it to be safe outside, it is necessary but not sufficient that there are no bears in the area.

4. September 3

4.1. Logic

4.1.1. Propositional Logic

Logical Equivalences

Logical equivalences between various proposition structures allow us to understand, simplify, negate, and prove various propositions. We take a look at a few important logical equivalences.

Theorem 4.1.1 (De Morgan's Laws for Connectives)**.** *For all propositions P and Q, the following logical equivalences hold true:*

1. $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$
2. $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

In propositional logic, we can prove logical equivalences using a truth table.

Proof. Let P and Q be arbitrary and fixed propositions. The following truth table verifies that $\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$
T	T	T	F	F	F	F	T
T	F	F	T	F	T	T	T
F	T	F	T	T	F	T	T
F	F	F	T	T	T	T	T

□

Note. As we've seen a little bit already, we can nest compound propositions as deeply as we like. We use parentheses to disambiguate propositions.

We list a few more important logical equivalences. These will be useful for understanding the logical negation of a proposition as well as developing proof techniques for our

propositions. All of these theorems are proven via simple truth tables. We'll state most of them without proof.

Theorem 4.1.2 (Distributive Law for Connectives)**.** *For all propositions P, Q, and R, the following logical equivalences hold:*

1. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
2. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

Theorem 4.1.3 (Law of Double Negation)**.** *For any proposition P, $\neg\neg P \equiv P$.*

Theorem 4.1.4 (Commutative Law)**.** *For any propositions P and Q, the following are true:*

1. $P \wedge Q \equiv Q \wedge P$
2. $P \vee Q \equiv Q \vee P$

Theorem 4.1.5 (Associative Law)**.** *For any propositions P, Q, and R, the following are true:*

1. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
2. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$

The associative law allows us to drop some parentheses in our statement without losing unique readability. If the connectives are all $\wedge$'s or $\vee$'s, then the parentheses are not necessary. Since $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$, we do not need to disambiguate between these two propositions. We may simply write $P \wedge Q \wedge R$. Similarly, we may write $P \vee Q \vee R$ in place of $(P \vee Q) \vee R$ or $P \vee (Q \vee R)$.

Note. When the connectives are a mix of $\wedge$'s and $\vee$'s, we still need parentheses. As we can see from Theorem 4.1.2, $P \wedge (Q \vee R) \not\equiv (P \wedge Q) \vee R$. Simply writing "$P \wedge Q \vee R$" is ambiguous and not considered a well-formed proposition.

Theorem 4.1.6 (Biconditional Equivalence)**.** *For any propositions P and Q,*

$$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P).$$

Theorem 4.1.7 (Disjunctive Form of Implication)**.** *For any propositions P and Q,*

$$P \rightarrow Q \equiv \neg P \vee Q.$$

Recall that $\neg Q \to \neg P$ is called the *contrapositive* of $P \to Q$. It is an important fact in mathematics that these two sentence structures are always logically equivalent. Later, when we discuss proof writing, this logical equivalence will give us an important proof technique known as a *proof by contraposition*.

Theorem 4.1.8 (Contraposition)**.** *For any propositions P and Q,*

$$P \to Q \equiv \neg Q \to \neg P.$$

Proof. Let P and Q be arbitrary and fixed propositions. The following truth table demonstrates the logical equivalence between $P \to Q$ and $\neg Q \to \neg P$.

P	Q	$P \to Q$	$\neg P$	$\neg Q$	$\neg Q \to \neg P$	$(P \to Q) \leftrightarrow (\neg Q \to \neg P)$
T	T	T	F	F	T	T
T	F	F	F	T	F	T
F	T	T	T	F	T	T
F	F	T	T	T	T	T

□

Exercise 4.1.9. Use truth tables to determine whether or not the given propositional formulae σ_1 and σ_2 are logically equivalent.

$$\sigma_1 = (P \vee Q) \to R$$
$$\sigma_2 = (P \to R) \wedge (Q \to R)$$

Exercise 4.1.10. Write the contrapositive of the following statements in natural, idiomatic English.

(a) If I do my assignments, I will get a good grade in the course.

(b) I will not be late unless there is traffic.

4.1.2. Predicate Logic

Propositional logic has some severe limitations. For instance, how could we express propositions such as "The square of every real number is nonnegative" or "There exists a negative real number" in propositional logic? To handle statements of this form, we introduce predicate logic.

Recall: A *predicate* or *variable proposition* is a statement involving free (unbound) variables. A predicate itself does not have a truth value, but it takes on a truth value once its variables are specified.

Example 4.1.11.

1. $P(x) := x^2 \geq 8$ defined on $x \in \mathbb{R}$ is a predicate. From this predicate, we can form propositions by either specifying the value of x, stating that $P(x)$ is sometimes true, or stating that $P(x)$ is always true. The following are all examples of propositions formed from $P(x)$:
   - If $x = 3$ then $x^2 \geq 8$.
   - For all $x \in \mathbb{R}$, $x^2 \geq 8$.
   - There exists $x \in \mathbb{R}$ such that $x^2 \geq 8$.
2. $Q(n) :=$ "n is prime" defined on $n \in \mathbb{N}$ is a predicate. The following are all propositions:
   - $Q(0)$, $Q(1)$, $Q(2)$, etc.
   - There exists $n \in \mathbb{N}$ such that $Q(n)$ holds.
   - For all $n \in \mathbb{N}$, $Q(n)$ holds.

In the above examples, one way to turn a predicate into a proposition is to specify how often the predicate holds true. In this case, we say that we have *quantified the variables*. We now introduce two mathematical symbols, called *quantifiers*, denoting the English quantifiers "there exists" and "for all."

The Universal Quantifier

The symbol $\forall$ is called the *universal quantifier* and translates as "for all." If S is a set and $P(x)$ is a predicate defined on $x \in S$, then $\forall x \in S, P(x)$ means "For every $x \in S$, $P(x)$ holds true."

Example 4.1.12. We can express the proposition "The square of any real number is nonnegative" symbolically as:

$$\forall x \in \mathbb{R}, x^2 \geq 0$$

The predicate here was $P(x) := x^2 \geq 0$. Combining this with the universal quantifier turned it into a proposition.

Example 4.1.13. Let S be the set of all integers that are not perfect squares (integers that are not the square of another integer). Using the universal quantifier, we can formally define this set as follows:

$$S = \{n \in \mathbb{Z} \mid \forall m \in \mathbb{Z}, n \neq m^2\}$$

Note that $Q(n) := \forall m \in \mathbb{Z}, n \neq m^2$ is still a predicate because n is unbound. Remember that when we use set-builder notation, the right-hand side must be a predicate.

The Existential Quantifier

The symbol $\exists$ is called the *existential quantifier* and translates as "there exists." If S is a set and $P(x)$ is a predicate defined on $x \in S$, then $\exists x \in S, P(x)$ means "There exists an $x \in S$ such that $P(x)$ holds true."

Example 4.1.14. We can formally express the proposition "The polynomial $2x^3 - x^2 - 4x + 2$ has a rational root" as:

$$\exists x \in \mathbb{Q}, (2x^3 - x^2 - 4x + 2 = 0)$$

Example 4.1.15. If we wish to define $\mathcal{E}$ to be the set of even integers, we can express this in set-builder notation using the existential quantifier:

$$\mathcal{E} = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, (n = 2m)\}$$

Notes about Predicate Logic

- Once the free variables are bound, a predicate becomes a proposition. This means that the logical equivalences from propositional logic still apply. For instance, by the logical equivalence of contraposition we have:

  $$\forall x \in S, \exists y \in S, (P(x) \to Q(y)) \equiv \forall x \in S, \exists y \in S, (\neg Q(y) \to \neg P(x))$$

- If two adjacent quantifiers of the same type bind variables, then the order of quantification does not matter. For example:

  $$\forall x \in S, \forall y \in S, P(x, y) \equiv \forall y \in S, \forall x \in S, P(x, y)$$

  Because the order does not matter, we may write this in shorthand as:

  $$\forall x, y \in S, P(x, y)$$

- If the adjacent quantifiers are different, then you cannot change their order without changing the meaning of the proposition.

  Example 4.1.16. Consider the proposition:

  $$\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, (x < y)$$

  This translates to English as "For every integer x, there exists a larger integer y" (a true statement). On the other hand, the proposition

  $$\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, (x < y)$$

  translates to English as "There exists an integer y that is greater than all integers" (a false statement).

- Many statements in mathematics concern the existence of a unique element with a special property. If $P(x)$ is a predicate defined on $x \in S$ and we wish to say that there is one and only one element in S making $P(x)$ true, we can express this formally as:

$$(\exists x \in S, P(x)) \wedge (\forall a, b \in S, (P(a) \wedge P(b)) \rightarrow a = b)$$

This states: "There exists an x in S satisfying $P(x)$, and any two elements that satisfy $P(x)$ must be equal." Because we so often want to express existence and uniqueness in mathematics, we commonly use the shorthand notation $\exists!$. That is, the proposition

$$\exists!\, x \in S, P(x)$$

translates to "There exists a unique x in S such that $P(x)$ holds."

Example 4.1.17. We can restate the Division Algorithm using this shorthand notation:

$$\forall a, b \in \mathbb{Z}, (b \neq 0 \rightarrow \exists!\, q, r \in \mathbb{Z}, (a = bq + r \wedge 0 \leq r < |b|))$$

Exercise 4.1.18. Consider the following propositions involving sets A, B, and C:

$$\sigma_1 := \ \forall x \in A, \exists y \in B, (x + y \in C)$$
$$\sigma_2 := \ \exists y \in B, \forall x \in A, (x + y \in C)$$

(a) Provide an example of sets A, B, and C where σ_1 is true and σ_2 is false. If no such example exists, explain why.

(b) Provide an example of sets A, B, and C where σ_1 is false and σ_2 is true. If no such example exists, explain why.

Exercise 4.1.19. Using the standard number sets ($\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$) and logical symbols ($\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$), along with basic arithmetic symbols ($+$, $-$, $\cdot$, $<$, $>$, $=$, $\neq$) and constants (0, 1, -1, etc.), write the following statements in symbolic form:

(a) The product of two nonpositive real numbers is always nonnegative.

(b) The only integers that have a multiplicative inverse in the set of integers are 1 and -1.

(c) For any integer n, n is odd if and only if $n^2 - 1$ is divisible by 8.

5. September 5

5.1. Logic

5.1.1. Predicate Logic

Maximally Negating Propositions

When proving propositions, it is often helpful to understand the logical negation of a statement, particularly when using proof by contradiction. While $\neg P$ is technically the negation of P, simply saying "not P is true" is not very useful to work with. Instead, we would like to find a proposition Q that is logically equivalent to $\neg P$, where only the atomic formulas in Q are negated. Such a proposition is called a *maximally negated* proposition.

From our established logical equivalences, we already have most of the tools necessary to maximally negate propositions. The one remaining piece is to determine how to negate quantified statements.

Example 5.1.1. Consider the proposition

$$P := \ \forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ (xy = 1).$$

In words, P states: "Every real number has a multiplicative inverse." Which of the following is logically equivalent to $\neg P$?

(a) No real number has a multiplicative inverse.

(b) There is a real number that has a multiplicative inverse.

(c) There is a real number that does not have a multiplicative inverse.

The correct answer is (c). The statement P claims that every real number has a multiplicative inverse, so it fails if even a single real number lacks one. Symbolically, (c) can be written as

$$\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ (xy \neq 1).$$

Comparing this negation to the original statement, notice that both quantifiers are switched and the innermost formula is negated. This illustrates the general pattern for negating quantified statements.

Theorem 5.1.2 (DeMorgan's Laws for Quantifiers)**.** *For any set S and predicate $P(x)$:*

1. $\neg\, \forall x \in S, P(x) \;\equiv\; \exists x \in S, \neg P(x)$
2. $\neg\, \exists x \in S, P(x) \;\equiv\; \forall x \in S, \neg P(x)$

Since these statements involve quantifiers, truth tables cannot be used to establish the equivalences. We prove part (1) directly by showing that each side implies the other.

Proof.

- Assume $\neg\, \forall x \in S, P(x)$ holds. Then it is not the case that every $x \in S$ satisfies $P(x)$. Therefore, there must exist some $x \in S$ for which $P(x)$ does not hold, i.e. $\exists x \in S, \neg P(x)$.
- Conversely, assume $\exists x \in S, \neg P(x)$ holds. Then for some $a \in S$, we have $\neg P(a)$. This means not every element of S satisfies $P(x)$, so $\forall x \in S, P(x)$ is false. Hence $\neg\, \forall x \in S, P(x)$ is true.

□

Now we have all the tools we need to maximally negate any proposition that we may encounter. Below, we present an example demonstrating a systematic method for finding the maximally negated form of a proposition. In general, you do not need to show these intermediate steps, but we include them here to illustrate the process.

Example 5.1.3. Let $P(x)$, $Q(y)$, and $R(x, y, z)$ be variable propositions. Consider the sentence σ given below

$$\forall x \in S, \exists y \in S, \forall z \in S, ((P(x) \wedge Q(y)) \to R(x, y, z))$$

We will write $\neg\sigma$ in maximally negated form.

$$\begin{aligned}
\neg\sigma &\equiv \neg\forall x \in S, \exists y \in S, \forall z \in S, ((P(x) \wedge Q(y)) \to R(x, y, z)) \\
&\equiv \exists x \in S, \neg\exists y \in S, \forall z \in S, ((P(x) \wedge Q(y)) \to R(x, y, z)) \\
&\equiv \exists x \in S, \forall y \in S, \neg\forall z \in S, ((P(x) \wedge Q(y)) \to R(x, y, z)) \\
&\equiv \exists x \in S, \forall y \in S, \exists z \in S, \neg((P(x) \wedge Q(y)) \to R(x, y, z)) \\
&\equiv \exists x \in S, \forall y \in S, \exists z \in S, \neg(\neg(P(x) \wedge Q(y)) \vee R(x, y, z)) \\
&\equiv \exists x \in S, \forall y \in S, \exists z \in S, (\neg\neg(P(x) \wedge Q(y)) \wedge \neg R(x, y, z)) \\
&\equiv \exists x \in S, \forall y \in S, \exists z \in S, ((P(x) \wedge Q(y)) \wedge \neg R(x, y, z))
\end{aligned}$$

Finally, using the associative law for conjunctions, we can simplify the expression by removing unnecessary parentheses without ambiguity. Thus, the maximally negated form of $\neg\sigma$ is

$$\neg\sigma \equiv \exists x \in S, \forall y \in S, \exists z \in S, (P(x) \wedge Q(y) \wedge \neg R(x, y, z))$$

Recipe for Finding a Maximally Negated Form

1. **Move negations inward.** Start with the outermost negation and apply the rules for negating quantifiers:

$$\neg\forall x \in S, P(x) \;\equiv\; \exists x \in S, \neg P(x), \qquad \neg\exists x \in S, P(x) \;\equiv\; \forall x \in S, \neg P(x).$$

2. **Push negations through connectives.** Use DeMorgan's Laws and double-negation elimination:

$$\neg(A \wedge B) \equiv (\neg A \vee \neg B), \qquad \neg(A \vee B) \equiv (\neg A \wedge \neg B), \qquad \neg\neg A \equiv A.$$

3. **Rewrite implications.** Replace $A \to B$ with $\neg A \vee B$ before pushing negations inside.

4. **Repeat until only atomic formulas are negated.** Continue applying the rules until no quantifiers or connectives have a negation directly in front of them.

At the end of this process, you will have a *maximally negated* form of the original proposition.

Exercise 5.1.4. Write the logical negation of the following statements in maximally negated form. Next, determine whether the original statement or its negation is true, and briefly explain your reasoning. No formal proof is required.

(a) $\forall x \in \mathbb{R}, \big(-1 < x < 1 \to \exists y \in \mathbb{R}, \big(-1 < y < 1 \wedge y^2 = x^3\big)\big)$

(b) $\forall x, y \in \mathbb{R}, (x = y \leftrightarrow \forall \varepsilon \in \mathbb{R}, (\varepsilon > 0 \to |x - y| < \varepsilon))$

5.2. Proof Writing

Now that we have studied the structure of propositions and their negations, we are ready to discuss strategies for proving or disproving mathematical statements. We will break this discussion into steps, beginning with quantifiers and then moving on to implications and biconditionals.

For each type of claim, we will examine both *direct proofs* and *indirect proofs*. A direct proof attempts to establish the truth of the statement as written. An indirect proof instead establishes the truth of a logically equivalent statement (for example, a contrapositive or the negation of the negation).

5.2.1. Universal Statements

A *universal statement* is a proposition of the form $\forall x \in S, P(x)$.

Direct Proofs

Direct Proof Strategy

Let $x \in S$ be arbitrary but fixed. Demonstrate that $P(x)$ is true. Since $x \in S$ was chosen arbitrarily, we may conclude that $\forall x \in S, P(x)$ is true.

As a common and important case, recall that for two sets A and B, we say $A \subseteq B$ if and only if $\forall a \in A, (a \in B)$. To prove $A \subseteq B$, we let $a \in A$ be arbitrary and then show that $a \in B$. Proofs of this form are often called *containment proofs*, because we are showing that the set B "contains" all elements of A.

Example 5.2.1. Let

$$A = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z},\ n = 10m - 15\} \quad \text{and} \quad B = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z},\ n = 5m\}.$$

Prove that $A \subseteq B$.

Proof. Let $a \in A$ be an *arbitrary and fixed* element. By definition of A, there exists $m \in \mathbb{Z}$ such that $a = 10m - 15$. Fix such an m. Factoring out a 5, we obtain

$$a = 10m - 15 = 5(2m - 3).$$

Since $2m - 3 \in \mathbb{Z}$, it follows that $a = 5k$ for some integer k (namely $k = 2m - 3$). Hence $a \in B$. Because a was arbitrary, we conclude that $A \subseteq B$. □

Note. In early proofs, it is important to explicitly emphasize that an element chosen from a set is both *arbitrary and fixed*. This reminds us that we are not working with a special example, but with a general placeholder element. Later, once this point has been internalized, we will typically write simply "Let $a \in A$," with the arbitrariness and fixedness of a understood from context.

Indirect Proofs

By Theorem 5.1.2, we know that

$$\neg\forall x \in S, P(x) \quad \equiv \quad \exists x \in S, \neg P(x).$$

Indirect Proof Strategy

To prove $\forall x \in S, P(x)$ indirectly, assume for the sake of contradiction (AFSOC) that $\exists x \in S, \neg P(x)$ holds. Fix such an x and proceed through a chain of logical deductions until you arrive at a contradiction. Conclude that $\forall x \in S, P(x)$ must be true.

Example 5.2.2. Prove that $\forall x, y \in \mathbb{Z}, x^2 - 4y^2 \neq 2$.

Proof. Assume for the sake of contradiction that there exist integers $x, y \in \mathbb{Z}$ such that

$$x^2 - 4y^2 = 2.$$

Fix such an x and y. Since x is an integer, it is either even or odd. We consider both cases.

- Case 1: Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Fix such a k. Substituting into the equation gives

  $$(2k)^2 - 4y^2 = 2 \quad \Longrightarrow \quad 4k^2 - 4y^2 = 2.$$

  Thus $4(k^2 - y^2) = 2$, which implies $4 \mid 2$, a contradiction.

- Case 2: Suppose x is odd. Then, by the division algorithm, $x = 2\ell + 1$ for some $\ell \in \mathbb{Z}$. Fix such an ℓ. Substituting into the equation gives

  $$(2\ell + 1)^2 - 4y^2 = 2 \quad \Longrightarrow \quad 4\ell^2 + 4\ell + 1 - 4y^2 = 2.$$

  Rearranging,

  $$4(\ell^2 + \ell - y^2) = 1.$$

  Since $\ell^2 + \ell - y^2 \in \mathbb{Z}$, this would imply $4 \mid 1$, a contradiction.

Since both cases lead to contradictions, our assumption was false. Therefore,

$$\forall x, y \in \mathbb{Z}, \quad x^2 - 4y^2 \neq 2.$$

□

Exercise 5.2.3. Prove that there are no integer solutions to the equation $m^2 = 3n + 2$.

Exercise 5.2.4. Let $A = \{x \in \mathbb{R} \mid x^2 - 6x + 5 > 0\}$ and $B = (-\infty, 1)$. Prove that $B \subseteq A$.

5.2.2. Existential Statements

An *existential statement* is a proposition of the form $\exists x \in S, P(x)$.

Direct Proofs

Direct Proof Strategy

Demonstrate that there exists $x \in S$ such that $P(x)$ holds.

The most common approach is a *proof by demonstration*, where we provide a concrete example of an element $x \in S$ that satisfies $P(x)$.

Example 5.2.5. Prove $\exists x \in \mathbb{Q}, (2x^3 - x^2 - 4x + 2 = 0)$.

Proof. Let $f(x) = 2x^3 - x^2 - 4x + 2$. Note that we can factor $f(x)$ as follows:

$$2x^3 - x^2 - 4x + 2 = (2x - 1)(x^2 - 2)$$

Now, consider $x = \frac{1}{2} \in \mathbb{Q}$. Then

$$f\left(\tfrac{1}{2}\right) = (1 - 1)\left(\tfrac{1}{4} - 2\right) = 0$$

Therefore, there exists $x \in \mathbb{Q}$ such that $f(x) = 0$, as desired. □

A proof by demonstration is also commonly used to *disprove* a universal statement by providing a *counterexample*. Specifically, to prove $\neg\forall x \in S, P(x)$, it suffices to demonstrate that $\exists x \in S, \neg P(x)$.

Example 5.2.6. Recall in Example 5.2.1 we proved that $A \subseteq B$ where

$$A = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, n = 10m - 15\} \quad \text{and} \quad B = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, n = 5m\}$$

Now, prove that $B \not\subseteq A$.

To disprove the universal statement $\forall b \in B, (b \in A)$, we need to find a counterexample showing $\exists b \in B, (b \notin A)$.

Counterexample. Consider $b = 0$. We see that $0 \in B$ because $0 = 5 \cdot 0$ and $0 \in \mathbb{Z}$. However, $0 \notin A$ because $0 = 10m - 15$ if and only if $m = \frac{3}{2}$, which is not an integer. Therefore, $B \not\subseteq A$. □

6. September 8

6.1. Proof Writing

6.1.1. Existential Statements

Direct Proofs

In addition to constructive proofs, we may also encounter *non-constructive direct proofs*. These establish the existence of certain elements without explicitly identifying them. The following is a classic example.

Example 6.1.1. Claim: There exist two irrational numbers a and b such that $a^b \in \mathbb{Q}$.

We will demonstrate that such a and b exist without explicitly identifying them. For the purposes of this proof, assume that $\sqrt{2}$ is irrational (a fact we will soon prove).

Proof. Consider $\sqrt{2}^{\sqrt{2}}$. This number is either rational or irrational. We consider both cases.

- Case 1: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$. Then $a = \sqrt{2}$ and $b = \sqrt{2}$ satisfy the claim.
- Case 2: $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. Then $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ satisfy the claim because

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}.$$

Since one of these two cases must hold, we conclude that there exist irrational numbers a and b such that $a^b \in \mathbb{Q}$. □

Many other common examples of non-constructive direct proofs exist. For instance, numerous proofs invoking the Mean Value Theorem or the Intermediate Value Theorem are non-constructive, since these theorems assert the existence of certain points but do not provide a way to find them explicitly.

Indirect Proofs

By Theorem 5.1.2, we know that

$$\neg\exists x \in S, P(x) \equiv \forall x \in S, \neg P(x).$$

Indirect Proof Strategy

Assume for the sake of contradiction that $\forall x \in S, \neg P(x)$ holds. Derive a contradiction from this assumption. Conclude that $\exists x \in S, P(x)$ must be true.

A famous example of an indirect proof of an existential statement is the *Pigeonhole Principle*. Before stating and proving this theorem, we first need to define the *floor* and *ceiling* functions.

Definition. Let $x \in \mathbb{R}$.

- The *floor* of x, denoted $\lfloor x \rfloor$, is the greatest integer n such that $n \leq x$. Equivalently, $\lfloor x \rfloor$ is the unique integer $n \in \mathbb{Z}$ such that $n \leq x < n+1$.
- The *ceiling* of x, denoted $\lceil x \rceil$, is the least integer n such that $x \leq n$. Equivalently, $\lceil x \rceil$ is the unique integer $n \in \mathbb{Z}$ such that $n - 1 < x \leq n$.

Theorem 6.1.2 (Pigeonhole Principle)**.** *Let $n, k \in \mathbb{Z}^+$. If n objects are placed into k boxes, then there exists a box containing at least $\left\lceil \frac{n}{k} \right\rceil$ objects.*

We will state this theorem more formally after our discussion of cardinality.

Colloquially, the Pigeonhole Principle is often stated as: *"If many pigeons fly into not very many pigeonholes, then at least one pigeonhole must contain multiple pigeons."*

Proof. Suppose objects $a_1, a_2, \ldots, a_n$ are placed into boxes $A_1, A_2, \ldots, A_k$. Assume for the sake of contradiction that

$$\forall i \in [k], \quad A_i \text{ contains fewer than } \left\lceil \frac{n}{k} \right\rceil \text{ objects.}$$

Since each A_i contains an integer number of objects, this means

$$\forall i \in [k], \quad A_i \text{ contains at most } \left\lceil \frac{n}{k} \right\rceil - 1 \text{ objects.}$$

By definition of the ceiling function we have

$$\left\lceil \frac{n}{k} \right\rceil - 1 < \frac{n}{k} \leq \left\lceil \frac{n}{k} \right\rceil$$

Therefore, the total number of objects in all k boxes is at most

$$k \cdot \left(\left\lceil \frac{n}{k} \right\rceil - 1 \right) < k \cdot \frac{n}{k} = n,$$

contradicting the fact that exactly n objects were placed into the boxes.

Hence, there must exist some $i \in [k]$ such that A_i contains at least $\left\lceil \frac{n}{k} \right\rceil$ objects. □

Exercise 6.1.3. Returning to exercise 5.2.4, let $A = \{x \in \mathbb{R} \mid x^2 - 6x + 5 > 0\}$ and $B = (-\infty, 1)$. Prove that $A \not\subseteq B$.

Exercise 6.1.4. Prove the following propositions:

(a) $\exists x \in \mathbb{R}, |x^3| < x^2$

(b) For $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_{n+1} \in [0, 1]$, it is the case that:

$$\exists\, i < j \in [n+1], |x_i - x_j| \leq \frac{1}{n}.$$

6.1.2. Conditional Statements

Conditional statements are those of the form $P \to Q$. Proofs of conditional statements are the most common type of proofs in mathematics. We now build on what we established with universal and existential statements to include this connective.

Direct Proofs

Direct Proof Strategy

Assume P is true. Show that Q must also be true.

We previously saw an example of this proof method when we proved Theorem 2.1.6 about the transitivity of divisibility. Symbolically, we can express this theorem as:

$$\forall a, b, c \in \mathbb{Z}\, ((a \mid b \wedge b \mid c) \to a \mid c)$$

To prove this, we let a, b, and c be arbitrary integers such that $a \mid b$ and $b \mid c$. We then demonstrated, using the definition of divisibility, that $a \mid c$.

Let's look at another example of this proof technique.

Example 6.1.5.

Claim: For all integers n, if n is even then n^2 is even.

Symbolically, we can express this statement as

$$\forall n \in \mathbb{Z},\ \Big((\exists m \in \mathbb{Z},\, n = 2m) \to (\exists \ell \in \mathbb{Z},\, n^2 = 2\ell) \Big).$$

Proof. Let $n \in \mathbb{Z}$ be arbitrary and fixed. Suppose that n is even. Then there exists $m \in \mathbb{Z}$ such that $n = 2m$. Fix such an m. Squaring both sides of the equation gives

$$n^2 = (2m)^2 = 4m^2 = 2(2m^2).$$

Let $\ell = 2m^2 \in \mathbb{Z}$. Then $n^2 = 2\ell$, which shows that n^2 is even, as desired. □

Indirect Proofs

There are two types of indirect proofs for conditional statements that are often very similar: proof by contraposition and proof by contradiction.

(1) (Proof by Contraposition) Recall the contrapositive logical equivalence from Theorem 4.1.8:

$$P \to Q \equiv \neg Q \to \neg P.$$

Contrapositive Proof Strategy

Assume $\neg Q$ is true. Show that $\neg P$ must also be true.

(2) (Proof by Contradiction) From Theorem 4.1.7 (the disjunctive form of implication) and Theorem 4.1.1 (De Morgan's laws) we have

$$\neg(P \to Q) \equiv P \wedge \neg Q.$$

Contradiction Proof Strategy

Assume for the sake of contradiction that $P \wedge \neg Q$ holds. Find a contradiction based on this assumption. Conclude that $P \to Q$ must hold.

To see an example of the former, let's look at the converse of Example 6.1.5.

Example 6.1.6.

Claim: For all integers n, if n^2 is even then n is even.

Symbolically, we can express this proposition as

$$\forall n \in \mathbb{Z},\ ((\exists k \in \mathbb{Z}, n^2 = 2k) \to (\exists \ell \in \mathbb{Z}, n = 2\ell)).$$

By Contraposition. Let $n \in \mathbb{Z}$ (be arbitrary and fixed). It suffices to show that if n is not even, then n^2 is also not even. Assume that n is not even, i.e., n is odd. Then there exists $\ell \in \mathbb{Z}$ such that $n = 2\ell + 1$. Fix such an ℓ. Then

$$n^2 = (2\ell + 1)^2 = 4\ell^2 + 4\ell + 1 = 2(2\ell^2 + 2\ell) + 1.$$

Since $2\ell^2 + 2\ell \in \mathbb{Z}$, we have $n^2 = 2k + 1$ for some $k \in \mathbb{Z}$. Hence n^2 is odd, and therefore n^2 is not even, as desired. □

We now look at a proof by contradiction.

Example 6.1.7. Using the definition of the rational numbers and the properties of the integers, prove that for any real numbers x and y, if x is rational and y is irrational then $x + y$ is irrational.

Symbolically, we can express this proposition as

$$\forall x, y \in \mathbb{R},\ ((x \in \mathbb{Q} \wedge y \notin \mathbb{Q}) \to x + y \notin \mathbb{Q}).$$

By Contradiction. Let $x, y \in \mathbb{R}$ such that $x \in \mathbb{Q}$ and $y \notin \mathbb{Q}$. Assume for the sake of contradiction that $x + y \in \mathbb{Q}$. Since $x, x + y \in \mathbb{Q}$, there exist $m, n, p, q \in \mathbb{Z}$ with $n, q \neq 0$ such that

$$x = \frac{m}{n} \quad \text{and} \quad x + y = \frac{p}{q}.$$

Fix m, n, p, q. Then

$$y = (x + y) - x = \frac{p}{q} - \frac{m}{n} = \frac{np - mq}{nq}.$$

Since $np - mq, nq \in \mathbb{Z}$ with $nq \neq 0$ (because $n \neq 0$ and $q \neq 0$), this implies that $y \in \mathbb{Q}$, contradicting our assumption that $y \notin \mathbb{Q}$. Therefore $x + y \notin \mathbb{Q}$, and the claim holds. □

Exercise 6.1.8. Consider the following proposition:

$$\forall n \in \mathbb{Z}, \big(\exists m \in \mathbb{Z}, \big(2n^2 + 3 = 5m\big) \to \forall k \in \mathbb{Z}, (n \neq 5k)\big)$$

(a) Write the logical negation of this proposition in maximally negated form.

(b) Prove or disprove the original proposition. Clearly state any assumptions, provide justifications for your steps, and write a formal proof using only the properties of integers in an organized manner.

Exercise 6.1.9. Prove or disprove the following proposition. Clearly state any assumptions, provide detailed justifications for your steps, and write a formal proof using only the definitions of even and odd integers and the assumed properties of integer arithmetic.

Proposition: If n is an integer then $n^2 + n - 41$ is an odd number.

Exercise 6.1.10. Prove the following proposition:

$$\forall x, y \in \mathbb{R}, (x + y \geq 0 \to x^3 + y^3 \geq x^2 y + x y^2)$$

7. September 10

7.1. Proof Writing

7.1.1. Biconditional Statements

Biconditional statements are propositions of the form $P \leftrightarrow Q$ (read: "P if and only if Q," or simply "P iff Q"). There are two common techniques for proving biconditional statements.

(1) **Standard Method**: Prove both $P \to Q$ and $Q \to P$ separately, using any of the techniques from the previous section. These proofs together establish the biconditional.

(2) **Intermediary Method**: Construct a chain of logical equivalences. Prove

$$P \Leftrightarrow A \Leftrightarrow B \Leftrightarrow \cdots \Leftrightarrow Q$$

for some number of intermediate propositions $A, B, \ldots$. Each step must be reversible when using this method.

Standard Method

Standard Method

Prove both directions separately:

- Assume P and show Q.
- Assume Q and show P.

Observe that if we combine our proofs from Examples 6.1.5 and 6.1.6, we have shown that for any integer n, n is even **if and only if** n^2 is even. We state this as a proposition.

Proposition 7.1.1. *For all $n \in \mathbb{Z}$, n is even iff n^2 is even.*

We now prove a more general version of this result.

Theorem 7.1.2. *For all $m, n \in \mathbb{Z}$, mn is even iff m is even or n is even.*

Proof. Let $m, n \in \mathbb{Z}$ be arbitrary and fixed.

($\Rightarrow$) We prove the contrapositive. Suppose neither m nor n is even, so both are odd. Then there exist $r, s \in \mathbb{Z}$ such that $m = 2r + 1$ and $n = 2s + 1$. Fix r and s. Then

$$mn = (2r + 1)(2s + 1) = 2(2rs + r + s) + 1.$$

Since $2rs + r + s \in \mathbb{Z}$, we see that mn is odd. Thus, if mn is even, then at least one of m or n must be even.

($\Leftarrow$) Suppose either m is even or n is even. We consider two cases.

- Case 1: m is even. Then $m = 2k$ for some $k \in \mathbb{Z}$, so

$$mn = (2k)n = 2(kn).$$

  Since $kn \in \mathbb{Z}$, mn is even.

- Case 2: n is even. Then $n = 2\ell$ for some $\ell \in \mathbb{Z}$, so

$$mn = m(2\ell) = 2(m\ell).$$

  Since $m\ell \in \mathbb{Z}$, mn is even.

In either case, mn is even.

□

Note. In the backward direction, Cases 1 and 2 were identical except for the distinction of which integer we labeled as "m" and which we labeled as "n". In such situations we may simplify the proof by assuming just one case holds "without loss of generality" (abbreviated WLOG). "Without loss of generality" means we can assume a specific case because it represents all possible cases without limiting the general argument.

Example 7.1.3. Here is a streamlined proof of the backward direction of Theorem 7.1.2 using WLOG.

Proof. ($\Leftarrow$): Suppose either m or n is even. Without loss of generality, assume m is even. Then $m = 2r$ for some $r \in \mathbb{Z}$. Fix r. Then

$$mn = (2r)n = 2(rn).$$

Since $rn \in \mathbb{Z}$, mn is even, as required. □

Notes about Disjunctions

(1) To prove $(P \vee Q) \to R$ directly, break into cases:

- Case 1: Assume P holds. Prove R holds.
- Case 2: Assume Q holds. Prove R holds.

If the two cases are symmetrical, we may use "without loss of generality" (WLOG).

(2) To prove $P \to (Q \vee R)$:

- (Direct Proof) Assume P and $\neg Q$. Prove R.
- (Indirect Proof) Use contraposition: assume $\neg Q$ and $\neg R$, and prove $\neg P$.

Example 7.1.4. In the forward direction of Theorem 7.1.2, we previously used contraposition. Below we rewrite the proof using a direct method.

Proof. ($\Rightarrow$): Let $m, n \in \mathbb{Z}$ such that mn is even. Then $mn = 2k$ for some $k \in \mathbb{Z}$. Fix k. We want to show that either m is even or n is even.

If m is even, the proof is complete. Otherwise, m is odd, so $m = 2\ell + 1$ for some $\ell \in \mathbb{Z}$. Fix ℓ. Then

$$2k = mn = (2\ell + 1)n = 2\ell n + n.$$

Rearranging yields

$$n = 2k - 2\ell n = 2(k - \ell n).$$

Since $k - \ell n \in \mathbb{Z}$, it follows that n is even. Thus, either m or n is even, as required. □

The Intermediary Method

Intermediary Method

Construct a sequence of reversible logical steps:

$$P \Leftrightarrow A \Leftrightarrow B \Leftrightarrow \cdots \Leftrightarrow Q.$$

Creating a chain of logical equivalences in which each step is reversible can be challenging. Proofs by equivalence chains are most effective for simple propositions where each step is justified by a definition, algebraic manipulation, or a previously proven biconditional statement. We will see more examples of this when we return to set theory. Below is a straightforward illustration.

Example 7.1.5.

Claim: For all $x, y \in \mathbb{R}$, $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$.

Proof. Let $x, y \in \mathbb{R}$ be arbitrary and fixed. We construct the following chain of logical equivalences:

$$\begin{aligned} x^3 + x^2y = y^2 + xy &\Leftrightarrow x^3 + x^2y - y^2 - xy = 0 \\ &\Leftrightarrow (x^2 - y)(x + y) = 0 \\ &\Leftrightarrow (x^2 - y = 0) \text{ or } (x + y = 0) \\ &\Leftrightarrow y = x^2 \text{ or } y = -x. \end{aligned}$$

Each step follows by reversible algebraic manipulation, so the equivalences are valid in both directions. Therefore, the original biconditional statement holds. □

Note. When using the Intermediary Method, every step must be a *reversible* logical equivalence. If even one step only works in one direction, the entire chain fails to justify the biconditional. This contrasts with direct proofs, where one-way implications are often sufficient. Always double-check that each transformation can be undone.

Exercise 7.1.6. Using just the definition of divisibility and the properties of the integers, prove that for all integers n, $3 \mid n^2 - 1$ if and only if $3 \nmid n$.

Exercise 7.1.7. Prove the following proposition:

$$\forall x, y \in \mathbb{R}, \big(x \neq y \to \big((x+1)^2 = (y+1)^2 \leftrightarrow x + y = -2\big)\big)$$

7.1.2. Existence and Uniqueness Proofs

Propositions of the form $\exists! \, x \in S \, P(x)$ ("there exists a unique $x \in S$ such that $P(x)$ holds") require a two-part proof:

Proving Existence and Uniqueness

1. **Existence**: Prove the existential statement $\exists x \in S, P(x)$ using established methods.
2. **Uniqueness**: Let $x, y \in S$ such that $P(x)$ and $P(y)$ both hold. Show that $x = y$.

Recall that when we introduced the integers, we stated the Division Algorithm in Theorem 3.1.1. We restate it here in the case where $b > 0$.

Theorem 7.1.8 (Division Algorithm)**.** *For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \quad \textit{with} \quad 0 \leq r < b.$$

To prove this theorem, we must show both the existence of such q and r, and that they are the *only* integers satisfying $a = bq + r$ with $0 \leq r < b$. We will prove the existence portion later, when we study induction. For now, we prove the uniqueness portion.

Uniqueness. Let $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ satisfy

$$a = bq_1 + r_1 = bq_2 + r_2, \qquad 0 \leq r_1 < b, \quad 0 \leq r_2 < b.$$

From the inequalities, we obtain $-b < -r_2 \leq 0$. Adding this to $0 \leq r_1 < b$ gives

$$-b < r_1 - r_2 < b.$$

Since $bq_1 + r_1 = bq_2 + r_2$, it follows that

$$r_1 - r_2 = b(q_2 - q_1).$$

Thus $r_1 - r_2$ is a multiple of b. Dividing the inequality $-b < r_1 - r_2 < b$ by b yields

$$-1 < q_2 - q_1 < 1.$$

Because $q_2 - q_1 \in \mathbb{Z}$, we must have $q_2 - q_1 = 0$, so $q_1 = q_2$. Substituting back gives

$$r_1 - r_2 = b(q_2 - q_1) = 0,$$

hence $r_1 = r_2$. Therefore, the quotient and remainder are unique. □

Exercise 7.1.9. Consider the following proposition:

$$\exists!\, y \in \mathbb{R}, \forall x \in \mathbb{R}, (x + y = x)$$

(a) What does this statement say in natural, idiomatic English?

(b) Write the logical negation of this statement in maximally negated form.

(c) Prove the original statement.

7.1.3. Proof-Writing Tips

Writing Proofs

- **State Your Hypotheses**. Clearly state any assumptions or conditions needed for your proof. For example, if you assume that a function is continuous or that a set is non-empty, make sure to state this explicitly at the beginning of the proof.

- **Check Your Proof's Structure**. Ensure that your proof has a clear structure with a defined start, body, and conclusion. The proof should lead logically from the hypotheses to the conclusion, and each part of the proof should contribute to this progression.
- **Include All Steps**. Don't skip steps when writing your proofs. It is important for your reader to follow your work. Even if a step seems obvious to you, include it. Your intended audience should be able to completely understand and verify your proof.
- **Explain Why Steps Are Valid**. Each step should be correct and clearly justified. If a step relies on a theorem or lemma, briefly mention this and explain why the application is valid.
- **Define New Variables or Notation**. When introducing new variables or notation, be clear. For example, instead of writing "Since n is even, $n = 2m$," write "Since n is even, there exists an integer m such that $n = 2m$."
- **Use First Person Plural**. Proofs should be written in the first person plural using the pronoun "we." For instance, "We then have..." or "We now see that..."
- **Use Complete Sentences**. Good mathematical writing uses complete sentences. Your proof should be a short work of mathematical prose, with correct grammar, sentence structure, and punctuation.

  Students writing proofs for the first time often feel like they're not allowed to use words because they're "not math." A page full of just a series of mathematical symbols might look impressive, but it usually makes your argument harder to follow. Words (and even diagrams) are often necessary to explain your arguments. Notation should be used in moderation to improve readability and precision.
- **Indicate Directions in Biconditional Proofs**. When proving biconditional claims, clearly indicate which direction of the proposition you are proving. For instance, if you are proving $P \leftrightarrow Q$, your proof should have two parts:

  ($\Rightarrow$): Prove $P \to Q$

  ($\Leftarrow$): Prove $Q \to P$
- **Use Appropriate Notation**. Use the appropriate notation for the context. For example, instead of writing "Let $a \in X$," it is better to write "Let $x \in X$" or "Let $a \in A$." Avoid confusing notations like "Let $X \in A \times B$." Instead, write "Let $(a, b) \in A \times B$."
- **Revise and Refine**. After completing a proof, review it to check for clarity and accuracy. Look for any parts that might be confusing or ambiguous and revise them. Rewriting parts of the proof in simpler terms can also help clarify your arguments.

Coming Up With Proofs

- **Determine Hypotheses**. Identify your hypotheses clearly. The proposition is likely not true without these hypotheses.
- **Clarify the Goal**. Determine exactly what you are trying to show.
- **Use Scratch Work**. The order in which we come up with a proof is often not the order in which we write it. Do some scratch work first. Work both forward from the assumptions and backward from the desired conclusion. Ideally, find a place in between where they meet.
- **Look for Similar Proofs**. Consider how the proof of the proposition may be similar to previous proofs you have seen. Look through example problems from the text, lecture notes, unassigned problems, or worksheets. Are there ideas from any of these proofs that you can apply to your current problem?
- **Check Definitions**. When stuck, review your definitions. For instance, if you have assumed that $5 \mid n$, how can you rewrite n from the definition of divisibility?
- **Use Concrete Examples**. Try finding a concrete example that meets the hypotheses. Can you see how the conclusion follows from the hypotheses for this specific example?
- **Search for Counterexamples**. Try finding a counterexample. If the proposition is true, you'll fail, but you may see what obstacles are causing you to fail. This should aid you in determining why the proposition is true.
- **Proceed by Contradiction**. If you want to prove $P \to Q$, consider what goes wrong if $P \wedge \neg Q$ is true. With this added knowledge, you may be able to rewrite your proof as a direct proof or a proof by contrapositive.

Common Mistakes

- **Avoid Variable Duplication**. Avoid using the same variable for multiple purposes. For instance, instead of writing "Since m and n are even, $m = 2k$ and $n = 2k$ for some $k \in \mathbb{Z}$," write "Since m and n are even, $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$."
- **Understand Definitions**. Common errors often result from misunderstanding definitions. Formal definitions are essential for mathematics. Any math course consists of many new definitions, and it is important to learn these. Students often don't know how to proceed with a proof because they don't understand the definition of the object they are working with.

General Advice

- **Practice Regularly**. To write proofs, you need to be able to think abstractly and lay out a mathematical argument appropriately. Thinking abstractly and laying out a mathematical argument takes practice. Be patient. It comes with time.
- **Incorporate Feedback**. If you are working in a collaborative setting or if you have access to mentors or peers, seek feedback on your proofs. They might offer insights or highlight areas where the proof can be improved.
- **Work on Proof Readability**. Aim for readability and coherence in your proofs. Avoid overly complex sentences or convoluted reasoning. The goal is not just to prove something but to make it understandable for others.
- **Understand Presented Proofs**. Make sure to understand the proofs presented in lectures and recitations. This can help you understand the type of reasoning involved in a proof. Often, rewriting proofs by hand in your own words can help solidify your understanding of the ideas within the proof.
- **Don't Rely Solely on Posted Solutions**. You will gain very little by simply reading posted solutions. For instance, if you're trying to prove a proposition for practice and get stumped, don't just immediately look up the proof. Sleep on it. Process it in your subconscious for a while. Experiment with a few ideas. Talk it over with a classmate, a TA, or the professor. Then, if necessary, look up the proof. When you finally see the techniques used, they will be more meaningful and more likely to stick. This will aid in your proof-writing intuition (or "mathematical maturity"). Over time, your collection of proof-writing tricks and techniques will grow.

8. September 12

8.1. Sets Part 2

We return now to set theory to discuss set proofs and operations.

8.1.1. Containment and Double Containment Proofs

Given two sets A and B, recall that to prove $A \subseteq B$, we must establish the proposition

$$\forall a \in A,\ (a \in B).$$

To do so, we take an arbitrary element $a \in A$ and show that $a \in B$. This is known as a *containment proof*.

Containment Proofs

To prove $A \subseteq B$:

- Let $a \in A$ be arbitrary.
- Show that $a \in B$.

Further, recall that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Therefore, to prove set equality, we typically write a two-part proof: we prove both that $A \subseteq B$ and that $B \subseteq A$. This is known as a *double containment proof*.

Double Containment Proofs

To prove $A = B$:

($\subseteq$) Let $a \in A$. Show that $a \in B$.

($\supseteq$) Let $b \in B$. Show that $b \in A$.

We begin with a basic example of a double containment proof. More examples will appear as we introduce set operations.

Example 8.1.1. Let $A = \{x \in \mathbb{R} \mid x^2 - x - 12 < 0\}$ and $B = (-3, 4)$ (the open interval of real numbers between -3 and 4). Prove that $A = B$.

Proof. We proceed by double containment.

($\subseteq$) Let $a \in A$. Then $a \in \mathbb{R}$ and $a^2 - a - 12 < 0$. Factoring gives

$$(a-4)(a+3) < 0.$$

For the product to be negative, one of the factors must be positive and the other must be negative. Thus, either:

- $a - 4 > 0$ and $a + 3 < 0$, which implies $a > 4$ and $a < -3$, an impossibility;
- or $a - 4 < 0$ and $a + 3 > 0$, which implies $-3 < a < 4$.

Therefore, $a \in (-3, 4) = B$, showing that $A \subseteq B$.

($\supseteq$) Let $b \in B$. Then $b \in \mathbb{R}$ and $-3 < b < 4$. Rearranging, we have $b + 3 > 0$ and $b - 4 < 0$. Hence,

$$(b-4)(b+3) < 0.$$

Hence, $b^2 - b - 12 < 0$, which means $b \in A$. Therefore, $B \subseteq A$.

By double containment, we conclude that $A = B$. □

8.1.2. Power Sets

A fundamental concept in set theory is the *power set*. Given any set A, the power set of A, denoted by $\mathcal{P}(A)$, is the set of all subsets of A. This includes every possible subset, ranging from the empty set to the set A itself. In other words, the power set collects all the different ways elements of A can be grouped into subsets, providing a comprehensive view of the structure of A.

Understanding power sets is important because they play a significant role in many areas of mathematics, including combinatorics, probability, and logic. Power sets are also central to discussions about cardinality, since the size of $\mathcal{P}(A)$ is always strictly larger than the size of A. We will return to this point when we discuss Cantor's theorem and the idea of different sizes of infinity.

Definition. Let A be a set. The *power set* of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. That is,

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Example 8.1.2. Let $A = \{a, b\}$. Then the distinct subsets of A are

$$\varnothing,\ \{a\},\ \{b\},\ A.$$

Therefore,

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

(*A set of sets!*)

The following theorem is immediate from the definition.

Theorem 8.1.3. *For any set A, $\varnothing \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$.*

Example 8.1.4. Consider the set $\varnothing$. Write $\varnothing$, $\mathcal{P}(\varnothing)$, $\mathcal{P}(\mathcal{P}(\varnothing))$, and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$ in roster notation.

- $\varnothing = \{\ \}$
- $\mathcal{P}(\varnothing) = \{\varnothing\}$

  Note that $\varnothing \neq \{\varnothing\}$. If we view a set as a "bag," then $\varnothing$ is a bag with nothing in it, while $\{\varnothing\}$ is a bag containing an empty bag.
- $\mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \mathcal{P}(\varnothing)\} = \{\varnothing, \{\varnothing\}\}$
- $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$

Exercise 8.1.5. Let $A = \{0, 1, 2, \{1\}\}$. Determine whether the following statements are True or False.

1. $\varnothing \in \mathcal{P}(A)$
2. $\varnothing \subseteq \mathcal{P}(A)$
3. $\{\varnothing\} \in \mathcal{P}(A)$
4. $\{\varnothing\} \subseteq \mathcal{P}(A)$
5. $1 \in \mathcal{P}(A)$
6. $\{1\} \in \mathcal{P}(A)$
7. $\{1\} \subseteq \mathcal{P}(A)$
8. $\{\{1\}\} \in \mathcal{P}(A)$
9. $\{\{1\}\} \subseteq \mathcal{P}(A)$
10. $\{0, 2\} \in \mathcal{P}(A)$
11. $\{0, 2\} \subseteq \mathcal{P}(A)$

8.1.3. Fundamental Set Operations

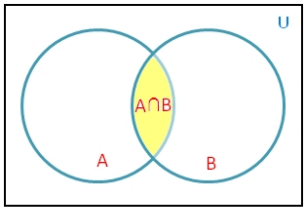
Let A and B be arbitrary sets, and let U be a set (called a *universal set*) such that $A \subseteq U$ and $B \subseteq U$.

Pairwise Intersection

The *intersection* of sets A and B, denoted $A \cap B$, is the set of all elements that A and B have in common.

$$A \cap B = \{x \in U \mid x \in A \wedge x \in B\}$$

Below is the standard Venn diagram representing the intersection of two sets.



A ∩ B

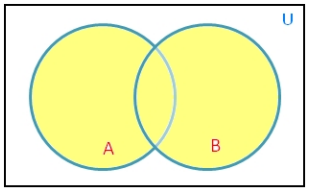
If $A \cap B = \varnothing$, then A and B are said to be *disjoint*.

Pairwise Union

The *union* of A and B, denoted $A \cup B$, is the set of all elements that are members of either A or B (or both).

$$A \cup B = \{x \in U \mid x \in A \vee x \in B\}$$

Below is the standard Venn diagram representing the union of two sets.



A ∪ B

The following are some basic properties of intersections and unions.

Theorem 8.1.6. *Let A and B be arbitrary sets. Then*

1. $A \cap B = B \cap A$
2. $A \cup B = B \cup A$
3. $A \cap B \subseteq A$
4. $A \subseteq A \cup B$
5. $A \subseteq B$ *iff* $A \cap B = A$

Properties (1) and (2) follow from the symmetry of "and" and "or" in logic ($P \wedge Q \equiv Q \wedge P$, $P \vee Q \equiv Q \vee P$). We now prove the remaining properties.

Proof.

3. Let $x \in A \cap B$. By definition of intersection, $x \in A$ and $x \in B$. Hence $x \in A$. Since x was arbitrary, we conclude $A \cap B \subseteq A$.

4. Let $a \in A$. Then, by the definition of union, $a \in A \cup B$. Therefore, $A \subseteq A \cup B$.

5. ($\Rightarrow$) Suppose $A \subseteq B$. We want to show that $A \cap B = A$. From property (3), we already know $A \cap B \subseteq A$. It remains to show $A \subseteq A \cap B$.

   Let $a \in A$. Since $A \subseteq B$, we also have $a \in B$. Thus $a \in A \cap B$ by definition of intersection. Therefore $A \subseteq A \cap B$, and hence $A = A \cap B$.

   ($\Leftarrow$) Suppose $A = A \cap B$. Let $a \in A$. Then $a \in A \cap B$, so $a \in B$ by definition of intersection. Therefore $A \subseteq B$.

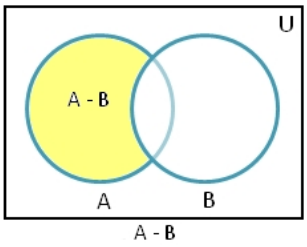
□

Set Difference

The *set difference* between sets A and B, denoted $A \setminus B$, is the set of all elements which are in A but not in B.

$$A \setminus B = \{x \in U \mid x \in A \wedge x \notin B\}$$

Below is the standard Venn diagram representing the set difference $A \setminus B$.



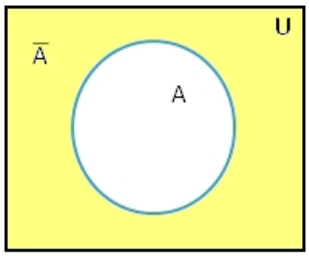
Complement

The *complement* of a set A, denoted $\overline{A}$ or A^c, is the set of all elements in U that are not in A.

$$\overline{A} = \{x \in U \mid x \notin A\} = U \setminus A$$

Note that the definition of $\overline{A}$ depends on the choice of U. Often, the universal set U is not explicitly stated but is understood from context.

Below is the standard Venn diagram for this definition.



Summary

Operation	Notation / Definition	Description
Intersection	$A \cap B = \{x \in U \mid x \in A \wedge x \in B\}$	Elements in both A and B
Union	$A \cup B = \{x \in U \mid x \in A \vee x \in B\}$	Elements in A, or in B, or in both
Difference	$A \setminus B = \{x \in U \mid x \in A \wedge x \notin B\}$	Elements in A but not in B
Complement	$\overline{A} = U \setminus A = \{x \in U \mid x \notin A\}$	Elements in U not in A

Exercise 8.1.7. Let $A = [10]$, $B = \{0, 1, 2\}$, and $C = \{0, 1, 9, 10, 11\}$. Write the following sets in roster notation.

1. $(A \setminus B) \cap C$
2. $(A \cup C) \setminus (B \cup C)$
3. $(A \setminus B) \cup (A \setminus C)$
4. $(A \setminus B) \cap (A \setminus C)$
5. $(A \cap C) \setminus B$
6. $A \setminus (B \cap C)$

Indexed Unions and Intersections

Indexing sets is useful when we want to define or reference a large (possibly infinite) number of sets without listing each one explicitly.

Definition. Let I be a set. A *family of sets indexed by* I, or simply an *indexed family of sets*, is a collection where each element of I corresponds to a set A_i. The set I is called an *index set*. We typically denote the indexed family of sets as either $\{A_i \mid i \in I\}$ or $\{A_i\}_{i \in I}$.

Example 8.1.8. For each $i \in \mathbb{N}$, define

$$A_i = [2i + 1] \setminus [i].$$

Then $\mathcal{F} = \{A_i \mid i \in \mathbb{N}\}$ is a family of sets indexed by $\mathbb{N}$. Each set A_i has an explicit definition in terms of i (this is common). For instance:

$$\begin{aligned} A_0 &= [1] \setminus [0] = \{1\}, \\ A_1 &= [3] \setminus [1] = \{2, 3\}, \\ A_2 &= [5] \setminus [2] = \{3, 4, 5\}, \\ A_3 &= [7] \setminus [3] = \{4, 5, 6, 7\}. \end{aligned}$$

Definition. Let $\{A_i\}_{i \in I}$ be an indexed family of sets. We define:

- **Indexed Intersection:**

$$\bigcap_{i \in I} A_i = \{x \in U \mid \forall i \in I,\, x \in A_i\}.$$

- **Indexed Union:**

$$\bigcup_{i \in I} A_i = \{x \in U \mid \exists i \in I,\, x \in A_i\}.$$

Example 8.1.9. Consider the family of sets from Example 8.1.8. We determine its indexed intersection and union.

Claim 1. $\bigcap\limits_{i \in \mathbb{N}} A_i = \varnothing$.

Proof. Assume for the sake of contradiction that there exists $x \in \bigcap\limits_{i \in \mathbb{N}} A_i$. Then, by definition of an indexed intersection, $x \in A_i$ for all $i \in \mathbb{N}$. Therefore, $x \in A_0$ and $x \in A_1$, and hence $x \in A_0 \cap A_1$. However,

$$A_0 \cap A_1 = \{1\} \cap \{2, 3\} = \varnothing,$$

a contradiction. Hence $\bigcap\limits_{i \in \mathbb{N}} A_i = \varnothing$. □

Claim 2: $\bigcup\limits_{i \in \mathbb{N}} A_i = \mathbb{Z}^+$

Proof. ($\subseteq$) Let $x \in \bigcup\limits_{i \in \mathbb{N}} A_i$. By definition of an indexed union, $x \in A_i$ for some $i \in \mathbb{N}$. Fix such an i. From the definition of A_i, we have $x \in [2i + 1] \setminus [i]$ and hence $x \in [2i + 1]$ by the definition of a set difference. Since $x \in [2i + 1]$, it follows that $x \in \mathbb{Z}^+$. Therefore, $\bigcup\limits_{i \in \mathbb{N}} A_i \subseteq \mathbb{Z}^+$.

($\supseteq$) Let $x \in \mathbb{Z}^+$ be arbitrary and fixed. Consider

$$A_{x-1} = [2x-1] \setminus [x-1].$$

Since $x \geq 1$, we have $x - 1 \geq 0$ and $2x - 1 \geq x$. Thus $x \in [2x-1]$. Moreover, since $x > x - 1$, we have $x \notin [x-1]$. Hence $x \in A_{x-1}$ by definition of set difference. Therefore $x \in \bigcup_{i \in \mathbb{N}} A_i$ by definition of an indexed union. Since x was arbitrary, we conclude that $\mathbb{Z}^+ \subseteq \bigcup_{i \in \mathbb{N}} A_i$.

By double containment, $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{Z}^+$. □

Exercise 8.1.10. Write the following sets in either interval notation or roster notation.

(a) $\bigcap_{n \in \mathbb{N}} \left[\frac{1}{n+1}, n+1\right]$

(b) $\bigcup_{n \in \mathbb{N}} \left[\frac{1}{n+1}, n+1\right]$

(c) $\bigcap_{n \in \mathbb{N}} \left(\frac{1}{n+1}, n+1\right)$

(d) $\bigcup_{n \in \mathbb{N}} \left(\frac{1}{n+1}, n+1\right)$

9. September 15

9.1. Sets Part 2

9.1.1. De Morgan's Laws for Sets

In propositional logic, De Morgan's Laws describe how negation interacts with conjunctions and disjunctions. These laws have direct analogs in set theory, where they describe the relationship between set complements, unions, and intersections. Understanding these laws helps us manipulate and simplify expressions involving sets, just as in logic.

Theorem 9.1.1 (DeMorgan's Laws)**.** *If A, X, Y are sets, then*

1. $A \setminus (X \cup Y) = (A \setminus X) \cap (A \setminus Y)$
2. $A \setminus (X \cap Y) = (A \setminus X) \cup (A \setminus Y)$

Additionally, let $\{X_i \mid i \in I\}$ be an indexed family of sets. Then

3. $A \setminus \bigcup_{i \in I} X_i = \bigcap_{i \in I} (A \setminus X_i)$
4. $A \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I} (A \setminus X_i)$

We will prove the fourth statement. The remaining cases follow in a similar way.

Proof of (4). Let A be a set and $\{X_i \mid i \in I\}$ an indexed family of sets. We prove that

$$A \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I} (A \setminus X_i)$$

by double containment.

($\subseteq$) Suppose $a \in A \setminus \bigcap_{i \in I} X_i$. Then $a \in A$ and $a \notin \bigcap_{i \in I} X_i$, by definition of set difference. By the definition of an indexed intersection, there exists some $j \in I$ such that $a \notin X_j$. Fix such a j.

Since $a \in A$ and $a \notin X_j$, we have that $a \in A \setminus X_i$. By the definition of an indexed union, it follows that $a \in \bigcup_{i \in I} (A \setminus X_i)$. Therefore, $A \setminus \bigcap_{i \in I} X_i \subseteq \bigcup_{i \in I} (A \setminus X_i)$.

($\supseteq$) Let $a \in \bigcup_{i \in I}(A \setminus X_i)$. By the definition of an indexed union, there exists some $j \in I$ such that $a \in A \setminus X_j$. Fix such a j.

By the definition of set difference, $a \in A$ and $a \notin X_j$. Since $a \notin X_j$, it follows that $a \notin \bigcap_{i \in I} X_i$. Therefore, $a \in A \setminus \bigcap_{i \in I} X_i$. Thus $\bigcup_{i \in I}(A \setminus X_i) \subseteq A \setminus \bigcap_{i \in I} X_i$.

By double containment, we conclude that

$$A \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I}(A \setminus X_i).$$

□

Corollary 9.1.2. *Let A and B be subsets of a universal set U. Then*

1. $\overline{A \cap B} = \overline{A} \cup \overline{B}$
2. $\overline{A \cup B} = \overline{A} \cap \overline{B}$

9.1.2. Cartesian Products

In set theory, the Cartesian product of two sets provides a way to pair each element of one set with each element of another set. This operation is fundamental in many areas of mathematics, allowing us to construct ordered pairs and define relations and functions. The Cartesian product helps us explore the relationships between different sets in a structured manner.

Definition. Let A and B be sets. The *Cartesian product* of A and B, denoted $A \times B$ is defined as follows:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

where the elements $(a, b) \in A \times B$ are *ordered pairs.*

The defining property of an ordered pair is that for $a, c \in A$ and $b, d \in B$

$$(a, b) = (c, d) \quad \text{if and only if} \quad a = c \text{ and } b = d.$$

Note. To be precise, in formal set theory, an object having the same properties as an ordered pair can be defined using the Kuratowski definition:

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

Using this construction, the Cartesian product $A \times B$ is the set of all such ordered pairs where the first element is from A and the second element is from B. This formalism

ensures that the order of the elements in the pair is maintained, which is crucial for distinguishing between (a, b) and (b, a) when $a \neq b$.

Example 9.1.3.

$$\mathbb{N} \times \mathbb{Z} = \{(m, n) \mid m \in \mathbb{N} \text{ and } n \in \mathbb{Z}\}$$
$$\mathbb{Z} \times \mathbb{N} = \{(m, n) \mid m \in \mathbb{Z} \text{ and } n \in \mathbb{N}\}$$

Notice that Cartesian products are not commutative. $\mathbb{N} \times \mathbb{Z} \neq \mathbb{Z} \times \mathbb{N}$. For instance, $(0, -1) \in \mathbb{N} \times \mathbb{Z}$ but $(0, -1) \notin \mathbb{Z} \times \mathbb{N}$ because $-1 \notin \mathbb{N}$. In fact, the only time $A \times B = B \times A$ is when A and B are the same set, or when one of them is empty.

Example 9.1.4. In the case where A and B are the same set, it is common to use exponential notation to represent the Cartesian product of the set with itself. This is seen most often in algebra and calculus when we talk about the Cartesian plane:

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

The Cartesian plane is simply the set of all possible ordered pairs of real numbers.

Example 9.1.5. For any set A, we have

$$A \times \varnothing = \varnothing \times A = \varnothing.$$

Repeated Cartesian Products

If we wanted to take a Cartesian product of three sets, there are a couple of ways we may do this:

$$(A \times B) \times C = \{((a, b), c) \mid a \in A,\ b \in B,\ c \in C\}$$
$$A \times (B \times C) = \{(a, (b, c)) \mid a \in A,\ b \in B,\ c \in C\}$$

Although these sets are technically different, they are essentially the same in practice. There is a natural way to associate elements of $(A \times B) \times C$ with elements of $A \times (B \times C)$. Specifically, we can identify $((a, b), c)$ in $(A \times B) \times C$ with $(a, (b, c))$ in $A \times (B \times C)$. Therefore, the distinction in parentheses does not add meaningful information.

To simplify notation, we typically drop the parentheses when dealing with repeated Cartesian products. We define an *ordered triple* (a, b, c) in the same way as an ordered pair, and extend the Cartesian product to three sets as follows:

$$A \times B \times C = \{(a, b, c) \mid a \in A,\ b \in B,\ c \in C\}$$

If you have taken Calculus 3, you have likely worked extensively with ordered triples already. Just as the Cartesian plane is represented by $\mathbb{R}^2$, the three-dimensional Cartesian coordinate system is given by

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

More generally, if $n \in \mathbb{Z}^+$ and $A_1, A_2, \ldots, A_n$ are sets, then

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$$

where $(a_1, a_2, \ldots, a_n)$ is called an *n-tuple*.

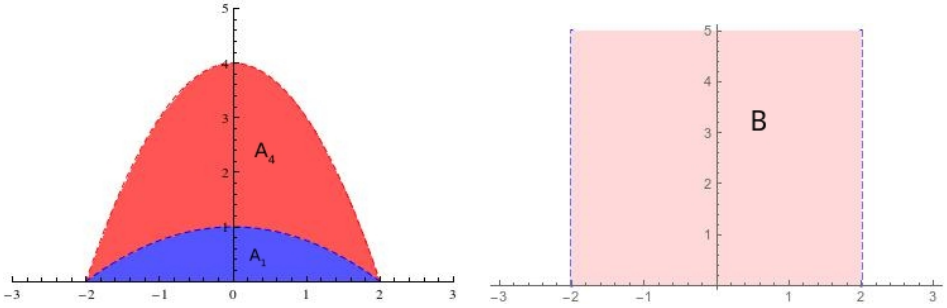
Example 9.1.6. Let $\mathbb{R}^+ = (0, \infty)$, the set of positive real numbers. For each $r \in \mathbb{R}^+$, define

$$A_r = \{(x, y) \in \mathbb{R}^2 \mid 0 < y < -\frac{r}{4}x^2 + r\}.$$

Also define

$$B = \{(x, y) \in \mathbb{R}^2 \mid -2 < x < 2 \text{ and } y > 0\}.$$

1. Provide a graphical representation of A_1, A_4, and B.



2. Prove that $\bigcup_{r \in \mathbb{R}^+} A_r = B$.

   Proof. We proceed by double containment.

   ($\subseteq$) Let $(x, y) \in \bigcup_{r \in \mathbb{R}^+} A_r$ be arbitrary and fixed. By definition of an indexed union we have $(x, y) \in A_r$ for some $r \in \mathbb{R}^+$. Fix such an r. By definition of A_r we have

   $$0 < y < -\frac{r}{4}x^2 + r.$$

   Factoring gives

   $$-\frac{r}{4}x^2 + r = -\frac{r}{4}(x^2 - 4) = -\frac{r}{4}(x - 2)(x + 2).$$

   Since $y > 0$, the right-hand side must also be positive, which forces $(x - 2)(x + 2) < 0$. This implies that $(x - 2)$ and $(x + 2)$ have opposite signs. Since $x + 2 > x - 2$ it must be the case that $x + 2 > 0$ and $x - 2 < 0$, which gives us that $-2 < x < 2$. Combining this with $y > 0$, we conclude $(x, y) \in B$, as desired.

($\supseteq$) Let $(x, y) \in B$ be arbitrary and fixed. Then $y > 0$ and $-2 < x < 2$, so $(x-2)(x+2) < 0$. We want $r > 0$ such that

$$y < -\frac{r}{4}(x-2)(x+2).$$

Scratch Work:

$$y < -\frac{r}{4}(x-2)(x+2) \iff -\frac{4y}{(x-2)(x+2)} < r$$

We know there must exist a positive real number greater than $-\dfrac{4y}{(x-2)(x+2)}$. We use this to continue the proof.

Fix any $r > -\dfrac{4y}{(x-2)(x+2)}$. We observe that since $y > 0$, $(x-2)(x+2) < 0$, and $-\dfrac{4y}{(x-2)(x+2)} < r$ it must be the case that $y < -\dfrac{r}{4}(x-2)(x+2)$. Thus we have $(x, y) \in \mathbb{R}^2$ and $0 < y < -\dfrac{r}{4}(x-2)(x+2)$, and therefore $(x, y) \in A_r$. By definition of an indexed union, $(x, y) \in \bigcup_{r \in \mathbb{R}^+} A_r$, as desired.

Since we have shown both containments, it follows that

$$\bigcup_{r \in \mathbb{R}^+} A_r = B.$$

□

Exercise 9.1.7. Consider the following sets and determine whether the statements in (a)-(n) are `True` or `False`.

$$\begin{aligned} A &= \{z \in \mathbb{Z} \mid -3 \leq z \leq 3\}, \\ B &= \{y \in \mathbb{Z} \mid -5 < y < 6\}, \\ C &= \{x \in \mathbb{R} \mid x^2 \geq 9\}, \\ D &= \{x \in \mathbb{R} \mid x < -3\}, \\ E &= \{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(n = 2k)\}. \end{aligned}$$

(a) $A \subseteq B$

(b) $C \cap D = \varnothing$

(c) $4 \in E \cap B$

(d) $\{4\} \subseteq A \cap E$

(e) $10 \in C \setminus D$

(f) $A \cup B \supseteq C$

(g) $3 \in A \cap C$

(h) $0 \in (A \setminus B) \cup D$

(i) $E \cap C \subseteq \mathbb{Z}$

(j) $0 \notin B \setminus C$

(k) $(0,0) \in A \times E$

(l) $(0,0) \in \mathcal{P}(A \times E)$

(m) $D \in \mathcal{P}(C)$

(n) $(A \times B) \setminus (C \times D) = (A \setminus C) \times (B \setminus D)$

Exercise 9.1.8. Prove that for all sets A and B, $A \times B = B \times A$ if and only if $A = \varnothing$ or $B = \varnothing$ or $A = B$.

Exercise 9.1.9. For any sets A and B, the *symmetric difference* of A and B, denoted $A \triangle B$, is defined as:

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

(a) Prove, via double containment, that for any sets A and B, $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

(b) Prove that $A \triangle B = \varnothing$ if and only if $A = B$.

Exercise 9.1.10. For each of the following, either prove the statement using a set containment proof or disprove it by constructing a counterexample.

(a) Prove or disprove: For any sets A, B, and C,

$$(A \cup B) \setminus C \subseteq (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)).$$

(b) Prove or disprove: For any sets A, B, and C,

$$(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \subseteq (A \cup B) \setminus C.$$

9.1.3. Set Equality via Logical Equivalences

Set equality can always be viewed as a biconditional statement, which is why double containment proofs and biconditional proofs share a similar structure. Let U be a universal set containing two sets A and B. Then the statement $A = B$ can be written symbolically as

$$\forall x \in U,\ (x \in A \leftrightarrow x \in B).$$

Recall that one way to prove a biconditional statement is by constructing a chain of logical equivalences. This method can also be applied to sets. It is particularly useful when the proof relies on definitions, algebraic manipulations, or previously established biconditional results. However, it is important to recognize that this approach may not be suitable for all proofs, especially those that require more nuanced or intricate reasoning beyond straightforward equivalences.

Before we do an example, we first need a lemma that will serve as a useful intermediary result.

Lemma 9.1.11. *For any sets A, B, and C, we have*

$$C \subseteq A \cap B \quad \textit{if and only if} \quad C \subseteq A \textit{ and } C \subseteq B.$$

Proof. Let A, B, and C be sets.

($\Rightarrow$) Assume $C \subseteq A \cap B$. To show $C \subseteq A$ and $C \subseteq B$, let $c \in C$. Since $C \subseteq A \cap B$, we have $c \in A \cap B$. By the definition of intersection, $c \in A$ and $c \in B$. Thus $C \subseteq A$ and $C \subseteq B$.

($\Leftarrow$) Assume $C \subseteq A$ and $C \subseteq B$. To show $C \subseteq A \cap B$, let $c \in C$. Then $c \in A$ and $c \in B$, so by the definition of intersection, $c \in A \cap B$. Hence $C \subseteq A \cap B$.

□

With this lemma established, we can now prove the following proposition using a chain of logical equivalences.

Proposition 9.1.12. *For all sets A and B,*

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B).$$

Proof. Let A and B be sets, and let U be a universal set containing $\mathcal{P}(A)$ and $\mathcal{P}(B)$. Fix an arbitrary $X \in U$. Then:

$$\begin{array}{lcll} X \in \mathcal{P}(A) \cap \mathcal{P}(B) & \Leftrightarrow & X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) & \text{(Defn of Intersection)} \\ & \Leftrightarrow & X \subseteq A \wedge X \subseteq B & \text{(Defn of Power Set)} \\ & \Leftrightarrow & X \subseteq A \cap B & \text{(Lemma 9.1.11)} \\ & \Leftrightarrow & X \in \mathcal{P}(A \cap B) & \text{(Defn of Power Set)} \end{array}$$

Since this chain of equivalences holds for all $X \in U$, it follows by the definition of set equality that

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B).$$

□

Proving Set Equality via Logical Equivalences

To prove $A = B$:

1. Let U be a universal set containing both A and B.
2. Translate the statement $A = B$ into logical form:
$$\forall x \in U,\ (x \in A \leftrightarrow x \in B).$$
3. Fix an arbitrary element x in the universal set under consideration.
4. Build a chain of equivalences, starting from $x \in A$ and step by step transforming it into $x \in B$, using only definitions, algebraic manipulations, and previously proven biconditionals.
5. Conclude that $x \in A \leftrightarrow x \in B$ holds for all x, and therefore $A = B$.

Exercise 9.1.13. Let A and B be subsets of a universal set U. Prove that $\overline{A \setminus B} = \overline{A} \cup B$.

9.2. End Exam 1 Material

Part II.

Induction

10. September 17

10.1. Principle of Mathematical Induction

Previously, we discussed proving universal statements by showing that a proposition holds for an arbitrary element of the set in question. However, for universal statements of the form

$$\textit{For every integer } n \geq M,\ P(n) \textit{ is true,}$$

there is another technique known as the *principle of mathematical induction* that is often more effective.

To introduce this principle, we first recall our working definition of $\mathbb{N}$. This definition captures the essential structure of the natural numbers without going into the deeper foundations of set theory.

Definition (Working Definition)**.** The set of natural numbers $\mathbb{N}$ is the "smallest" set I such that

$$0 \in I \quad \text{and} \quad (\forall k \in I,\ k+1 \in I).$$

That is, let I be any set such that $0 \in I$ and whenever $k \in I$, then also $k+1 \in I$. Define

$$\mathcal{F} = \{X \subseteq I \mid 0 \in X \ \wedge\ \forall k \in I, (k \in X \to k+1 \in X)\}.$$

Then

$$\mathbb{N} = \bigcap_{X \in \mathcal{F}} X.$$

Remark. Other, more formal approaches to defining the natural numbers exist. The *Peano axioms* characterize $\mathbb{N}$ through logical rules, while in set theory (ZFC) one can construct $\mathbb{N}$ explicitly from the axioms. We will not use these approaches in this course, but a brief sketch of the set-theoretic construction is provided in Appendix A.

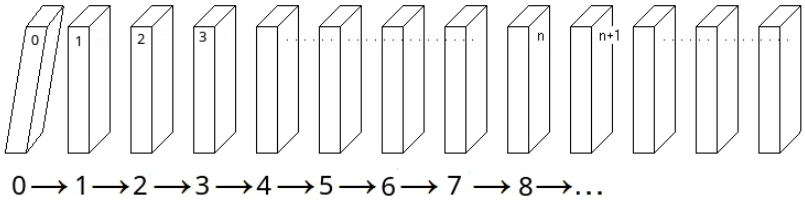
From this working definition of $\mathbb{N}$, we immediately obtain the following result, which justifies the method of proof by induction.

Theorem 10.1.1 (Principle of Mathematical Induction)**.** *Let $P(n)$ be a statement about $n \in \mathbb{N}$. If*

1. *$P(0)$ is true, and*
2. *for all $k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is true,*

then $P(n)$ is true for all $n \in \mathbb{N}$.

As an analogy, consider an infinite line of equally spaced dominoes representing the natural numbers, as shown below.



The assumptions of the Principle of Mathematical Induction can be interpreted as follows:

1. The first domino falls over.
2. If one domino falls over, then the next domino will fall over.

From this, we can conclude that any given domino will eventually fall over. That is, if we let $P(n)$ be the predicate "The nth domino falls over," then we can conclude $\forall n \in \mathbb{N}, P(n)$ holds true.

Note. Both conditions are essential in order to conclude that an arbitrary domino will eventually fall over.

We will now prove the Principle of Mathematical Induction from the definition of $\mathbb{N}$.

Proof. Let $P(n)$ be a predicate defined on $n \in \mathbb{N}$ such that:

1. $P(0)$ holds, and
2. $\forall k \in \mathbb{N}, (P(k) \to P(k+1))$ holds.

Define a set $S \subseteq \mathbb{N}$ as follows:

$$S = \{n \in \mathbb{N} \mid P(n)\}.$$

We wish to show that $S = \mathbb{N}$. Since $S \subseteq \mathbb{N}$ by definition, it suffices to show that $\mathbb{N} \subseteq S$.

By assumption (1), $P(0)$ holds, so $0 \in S$. By assumption (2), S is closed under the successor function: for all $k \in \mathbb{N}$, if $k \in S$, then $k + 1 \in S$. Thus, S contains 0 and is

closed under successors. By the definition of $\mathbb{N}$ as the smallest set with these properties, it follows that $\mathbb{N} \subseteq S$.

Therefore, $S = \mathbb{N}$ by double containment. Hence, $P(n)$ holds for all $n \in \mathbb{N}$. □

While this proof appears to require induction starting at $n = 0$, the following corollary shows that we may begin at any integer M.

Corollary 10.1.2 (Corollary to PMI)**.** *Let $M \in \mathbb{Z}$ and $S = \{z \in \mathbb{Z} \mid z \geq M\}$. Further, let $P(n)$ be a predicate defined on S such that*

1. *$P(M)$ holds*
2. *$\forall k \in S, (P(k) \to P(k+1))$ holds*

Then $\forall n \in S, P(n)$ holds.

Proof. Let $P(n)$ be as above, and define a new predicate $Q(n)$ on $n \in \mathbb{N}$ by

$$Q(n) \Leftrightarrow P(n + M)$$

From (1), $P(M)$ holds, so $Q(0)$ holds.

Now assume $Q(k)$ holds for some $k \in \mathbb{N}$. Then $P(k + M)$ holds. Since $k + M \in S$, assumption (2) implies $P(k + M + 1)$ holds, hence $Q(k + 1)$ holds. Thus, $Q(n)$ satisfies the two conditions of induction. By PMI, $Q(n)$ holds for all $n \in \mathbb{N}$.

Finally, let $n \in S$ be arbitrary. Then $n - M \in \mathbb{N}$, so $Q(n - M)$ holds. By definition of Q, this means $P(n)$ holds. Since $n \in S$ was arbitrary, we conclude $\forall n \in S, P(n)$ holds. □

PMI Template

Let $M \in \mathbb{Z}$ and $S = \{n \in \mathbb{Z} \mid n \geq M\}$.

Claim: $\forall n \in S, P(n)$ is true.

Proof: We proceed by induction on $n \in S$.

- **Base Case**: $n = M$. Prove that $P(M)$ holds.
- **Inductive Hypothesis**: Assume $n \in S$ and $P(n)$ holds.
- **Inductive Step**: Use the assumption that $P(n)$ holds to prove that $P(n+1)$ holds.

By the principle of mathematical induction, $\forall n \in S, P(n)$ holds. □

Before we move on to our first example, let us make a couple of notes on summations and products. Statements involving summations and products are often proved by induction, since both are defined recursively.

- For $n \in \mathbb{Z}^+$, the sum of real numbers $a_1, a_2, \ldots, a_n$, denoted $\sum_{i=1}^{n} a_i$, is defined recursively as follows:
  - $\sum_{i=1}^{0} a_i = 0$
  - $\sum_{i=1}^{n+1} a_i = \left(\sum_{i=1}^{n} a_i\right) + a_{n+1}$

  For example:

$$\sum_{i=1}^{4}(i^2+1) = (1^2+1)+(2^2+1)+(3^2+1)+(4^2+1) = 34$$

- For $n \in \mathbb{Z}^+$, the product of real numbers $a_1, a_2, \ldots, a_n$, denoted $\prod_{i=1}^{n} a_i$, is defined recursively as follows:
  - $\prod_{i=1}^{0} a_i = 1$
  - $\prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) \cdot a_{n+1}$

  For example:

$$\prod_{i=1}^{4}(i^2+1) = (1^2+1)\cdot(2^2+1)\cdot(3^2+1)\cdot(4^2+1) = 1700$$

10.1.1. Examples

We are now ready to begin working through examples.

Example 10.1.3. For $n \in \mathbb{Z}^+$, the nth *triangular number*, T_n, is defined as the sum of the first n consecutive positive integers. That is,

$$T_n = \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n.$$

We would like to find a closed-form expression for T_n.

First, let us compute a few examples to look for a pattern:

- $T_1 = 1$
- $T_2 = 1 + 2 = 3$
- $T_3 = 1 + 2 + 3 = 6 = 4 + 2$

- $T_4 = 1+2+3+4 = 10 = 5+5$
- $T_5 = 1+2+3+4+5 = 15 = 6+6+3$
- $T_6 = 1+2+3+4+5+6 = 21 = 7+7+7$
- $T_{100} = 1+2+3+\cdots+100 = \underbrace{101+\cdots+101}_{50 \text{ times}}$
- $T_{101} = 1+2+3+\cdots+101 = \underbrace{102+\cdots+102}_{50 \text{ times}} + 51$

These suggest the following observations:

- If n is even, we can pair terms so that each pair sums to $n+1$. Since there are $\frac{n}{2}$ such pairs,
$$\sum_{i=1}^{n} i = (n+1)\left(\frac{n}{2}\right) = \frac{n(n+1)}{2}.$$
- If n is odd, we can again pair terms so that each pair sums to $n+1$, leaving the middle term $\frac{n+1}{2}$ unpaired. Therefore,
$$\sum_{i=1}^{n} i = (n+1)\left(\frac{n-1}{2}\right) + \frac{n+1}{2} = \frac{n(n+1)}{2}.$$

In both cases, we obtain the same closed-form expression. This motivates the following proposition.

Claim: For all $n \in \mathbb{Z}^+$,
$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Proof. We proceed by induction on $n \in \mathbb{Z}^+$.

- **Base Case**: For $n = 1$,
$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$
Thus the base case holds.
- **Inductive Step**: Assume for some $k \in \mathbb{Z}^+$ that
$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}.$$
(This is the *inductive hypothesis.*)

We must show

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}.$$

Observe the following chain of equalities:

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \quad \text{(by the inductive hypothesis)} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}.
\end{aligned}$$

By the Principle of Mathematical Induction, it follows that

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

for all $n \in \mathbb{Z}^+$. □

Exercise 10.1.4. Prove that for every $n \in \mathbb{Z}^+$, the following holds:

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Exercise 10.1.5. For each part below, determine the set of natural numbers for which the property holds true, and prove your claim.

(a) $2^n \geq (n+1)^2$

(b) $3^{n+1} > n^4$

(c) $n^3 + (n+1)^3 > (n+2)^3$

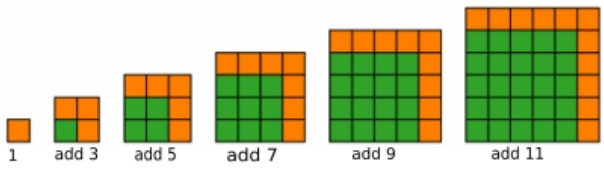
(d) $3^n \geq 2^{n+1}$

11. September 19

11.1. Principle of Mathematical Induction

11.1.1. Examples

Example 11.1.1. We will consider the sum of consecutive *odd* integers. Let's draw some pictures and make some observations.



If we keep adding consecutive odd numbers, will we always get a square? It sure looks like it, but a preponderance of evidence is not sufficient justification. It's possible that this pattern falls apart for some larger values of n. However, from our geometric description, we can see that using our observation that 1 block makes a 1×1 square, we showed that $1+3$ blocks make a 2×2 square. From there, we were able to show that $1+3+5$ blocks can form a 3×3 square. Since we used the previous case being true to show that the next case is true, this seems to lend itself to induction.

Claim: For all $n \in \mathbb{Z}^+$, $\sum_{i=1}^{n}(2i-1) = n^2$.

Proof. We proceed by induction on $n \in \mathbb{Z}^+$.

- **Base Case**: If $n = 1$, then

$$\sum_{i=1}^{1}(2i-1) = 1 = 1^2,$$

  as desired.

- **Inductive Step**: Let $k \in \mathbb{Z}^+$ and assume $\sum_{i=1}^{k}(2i-1) = k^2$ (*this is our Inductive Hypothesis*). Then we have the following chain of equalities:

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \left(\sum_{i=1}^{k}(2i-1)\right) + (2(k+1)-1)\\ &= \left(\sum_{i=1}^{k}(2i-1)\right) + (2k+1)\\ &= k^2 + 2k + 1 \quad \text{(by the Inductive Hypothesis)}\\ &= (k+1)^2.\end{aligned}$$

Hence, $\sum_{i=1}^{k+1}(2i-1) = (k+1)^2$, as desired.

By the principle of mathematical induction, we conclude that $\sum_{i=1}^{n}(2i-1) = n^2$ for all $n \in \mathbb{Z}^+$. □

11.1.2. Sequences

Definition. A *sequence of real numbers* is an enumerated collection of reals in which repetition and order matter. For now, we focus on sequences of real numbers, typically enumerated by either $\mathbb{N}$ or $\mathbb{Z}^+$.

Notation: $\langle a_n \rangle_{n\in\mathbb{N}}$ represents the sequence

$$\langle a_n \rangle_{n\in\mathbb{N}} = \langle a_0, a_1, a_2, a_3, \ldots \rangle,$$

where each a_i is a real number. a_0 is the 0th term, a_1 is the 1st term, etc. Similarly,

$$\langle a_n \rangle_{n\in\mathbb{Z}^+} = \langle a_1, a_2, a_3, \ldots \rangle.$$

More formally, a sequence can be thought of as a function $f : \mathbb{N} \to \mathbb{R}$. We have not yet studied functions formally, so for now we treat this as an intuition.

Often, sequences are defined recursively, which makes them particularly well-suited for proofs by induction. For example, recall the *triangular numbers*, $\langle T_n \rangle_{n\in\mathbb{Z}^+}$, defined by

$$T_n = 1 + 2 + 3 + \cdots + n.$$

We can also define this sequence recursively by specifying the initial term (the base case) and how each subsequent term is derived from the previous one (the recurrence relation):

$$\begin{aligned}T_1 &= 1,\\ T_{n+1} &= T_n + (n+1).\end{aligned}$$

In this section, we will introduce two important sequences.

The Factorial Sequence

Definition. For $n \in \mathbb{N}$, we define $n!$, read "n factorial," by

$$n! = \prod_{i=1}^{n} i.$$

Since product notation is itself defined recursively, this definition can also be rewritten as follows:

$$0! = 1$$
$$(n+1)! = (n+1) \cdot n!$$

For example,

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120.$$

Now let us look at an induction proof involving the factorial sequence.

Example 11.1.2. For which values of $n \in \mathbb{N}$ does the inequality $n! > 2^n$ hold?

To answer this, we first examine small values of n:

n	2^n	$n!$
0	1	1
1	2	1
2	4	2
3	8	6
4	16	24
5	32	120
6	64	720

From this table, we see that at $n = 4$, $n!$ first exceeds 2^n. Moreover, it appears that $n!$ continues to grow faster than 2^n thereafter. This suggests the following conjecture.

Claim: For all integers $n \geq 4$, we have $n! > 2^n$.

Proof. We proceed by induction on $n \in \mathbb{N}$ with $n \geq 4$.

- **Base Case**: When $n = 4$, we compute

  $$4! = 24 > 16 = 2^4,$$

  as required.

- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 4$ and assume $k! > 2^k$. We want to show $(k+1)! > 2^{k+1}$. Using the recursive definition of factorial, we compute:

$$\begin{aligned}(k+1)! &= (k+1) \cdot k! \quad \text{(By Definition)} \\ &> (k+1) \cdot 2^k \quad \text{(By the Inductive Hypothesis)} \\ &> 2 \cdot 2^k \quad \text{(Since } k \geq 4\text{)} \\ &= 2^{k+1}.\end{aligned}$$

  Thus, $(k+1)! > 2^{k+1}$, as desired.

By the principle of mathematical induction, we conclude that $n! > 2^n$ for all integers $n \geq 4$. □

Note. Notice that our proof did not address the values $n = 0, 1, 2, 3$, since the claim only concerned $n \geq 4$. To check what happens at those smaller values, we had to verify them directly using the table. The induction proof neither proves nor disproves the inequality for $n < 4$; it simply establishes the result for all $n \geq 4$.

Exercise 11.1.3. Prove that for all positive integers n,

$$\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$$

The Fibonacci Sequence

Definition. For $n \in \mathbb{N}$, we define the nth Fibonacci number, f_n, recursively by

$$f_n = \begin{cases} 0 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ f_{n-1} + f_{n-2} & \text{if } n \geq 2. \end{cases}$$

The first several Fibonacci numbers are:

$$\langle f_n \rangle_{n \in \mathbb{N}} = \langle 0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8, \ldots \rangle.$$

Example 11.1.4. Prove that $f_n < 2^n$ for all $n \in \mathbb{N}$.

Problem: In order to prove that the claim holds for f_{n+1}, we will need to refer not only to f_n but also to f_{n-1}. How can we handle this situation using the principle of mathematical induction?

11.1.3. Strong Induction

Theorem 11.1.5 (Strong Principle of Mathematical Induction)**.** *Let $P(n)$ be a predicate defined for all $n \in \mathbb{N}$. Suppose:*

1. *$P(0)$ holds.*
2. *$\forall k \in \mathbb{N}, ((\forall i \in [k] \cup \{0\}, P(i)) \to P(k+1))$ holds.*

Then $P(n)$ holds for all $n \in \mathbb{N}$.

In other words, if $P(0)$ is true and whenever $P(0), P(1), \ldots, P(n)$ are all true this implies $P(n+1)$ is true, then $P(n)$ is true for all $n \in \mathbb{N}$.

We will now prove the Strong Principle of Mathematical Induction using the ordinary Principle of Mathematical Induction.

Proof. Let $P(n)$ be a predicate defined for all $n \in \mathbb{N}$, satisfying conditions (1) and (2) of the theorem. Define a new proposition $Q(n)$ for $n \in \mathbb{N}$ by

$$Q(n) := \forall i \in [n] \cup \{0\}, P(i).$$

We proceed by induction on $n \in \mathbb{N}$ to show that $Q(n)$ holds for all $n \in \mathbb{N}$.

- **Base Case**: $n = 0$. By assumption (1), $P(0)$ holds. By the definition of $Q(n)$, we have $Q(0) \equiv P(0)$. Thus $Q(0)$ holds.
- **Inductive Step**: Let $k \in \mathbb{N}$ and assume $Q(k)$ holds (*this is the inductive hypothesis*). From the definition of $Q(k)$, this means $\forall i \in [k] \cup \{0\}, P(i)$ holds.

  By condition (2), it follows that $P(k+1)$ holds. Therefore, $\forall i \in [k+1] \cup \{0\}, P(i)$ holds, so $Q(k+1)$ holds.

By the principle of mathematical induction, $Q(n)$ holds for all $n \in \mathbb{N}$.

Finally, to see that this implies $\forall n \in \mathbb{N}, P(n)$: let $n \in \mathbb{N}$. Since $Q(n)$ holds, we have $\forall i \in [n] \cup \{0\}, P(i)$. Because $n \in [n] \cup \{0\}$, it follows that $P(n)$ holds. Since n was arbitrary, $\forall n \in \mathbb{N}, P(n)$ holds. □

Exercise 11.1.6. Let $P(n)$ be a predicate defined on $n \in \mathbb{Z}$. For each case below, identify which instances of the proposition you could **necessarily** deduce.

(a) **Base Case:** $P(-3)$. **Implication:** $\forall n \in \mathbb{Z}, (P(n) \to P(n+1))$.

(b) **Base Case:** $P(1)$. **Implication:** $\forall n \in \mathbb{N}, (P(n) \to P(2n))$.

(c) **Base Case:** $P(0)$. **Implication:** $\forall n \in \mathbb{Z}, (P(n) \to (P(n-1) \wedge P(n+1)))$.

(d) **Base Cases:** $P(-1) \wedge P(0)$. **Implication:** $\forall n \in \mathbb{Z}^+, (P(n) \to P(n+2))$.

(e) **Base Case:** $P(0)$. **Implications:** $\forall n \in \mathbb{Z}, ((P(n) \to P(n+6)) \wedge (P(2n) \to P(n)))$.

Template for Induction Proofs Using SPMI

Let $M \in \mathbb{Z}$ and define $S = \{n \in \mathbb{Z} \mid n \geq M\}$.

Claim: $\forall n \in S, P(n)$.

Proof: We proceed by strong induction on $n \in S$.

Base Case: Show $P(M)$ holds because ...

There may be more base cases if necessary.

Inductive Step: Let $k \in S$ such that $P(i)$ holds for all $i \in S$ with $M \leq i \leq k$. Show $P(k+1)$ holds.

If there are ℓ many base cases, assume $k \geq M + \ell$.

By the strong principle of mathematical induction, we conclude that $\forall n \in S, P(n)$ holds.

Notice that in the template we allow for multiple base cases, even though the theorem itself does not explicitly mention this. Multiple base cases arise when the truth of

$$P(k+1)$$

is completely independent of the truth of

$$P(0), P(1), \ldots, P(k),$$

so there is no causality linking these earlier terms to $P(k+1)$. In such situations, we must verify the first several values directly. Eventually, however, the sequence becomes causal, meaning that each term depends on previous ones, at which point strong induction can be applied.

Before returning to Example 11.1.4, we will first examine the historically significant induction problem that necessitated the use of the strong inductive hypothesis. To do so, we first need to formally define a prime number.

Definition.

- A natural number n is called *prime* if and only if $n > 1$ and its only positive divisors are 1 and n.
- A natural number n is called *composite* if and only if $n > 1$ and n is not prime.

  That is, there exists $a, b \in \mathbb{N}$ with $1 < a \leq b < n$ such that $n = ab$.

For instance, the first 10 prime numbers are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29$$

In the chapter on number theory, we will discuss prime numbers in much more depth. For now, the important idea is that prime numbers are the basic building blocks of the natural numbers (and, in fact, the integers as well).

Our first strong induction proof is the first half of an important result in number theory, the *Fundamental Theorem of Arithmetic*.

Theorem 11.1.7 (Fundamental Theorem of Arithmetic, Part 1)**.** *For all $n \in \mathbb{N}$ with $n > 1$, n is either prime or a product of primes.*

Proof. We proceed by strong induction on the integers $n \geq 2$. Define $P(n)$ to be the proposition that "n is either prime or a product of primes."

- **Base Case**: $n = 2$. The number 2 is prime since the only possible positive divisors are 1 and 2, which both divide 2. Thus, $P(2)$ holds.
- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 2$ and assume $P(i)$ holds for all $i \in \mathbb{N}$ with $2 \leq i \leq k$. Consider $n = k + 1$. We break this into two cases:
  - Case 1: If $k + 1$ is prime, then $P(k + 1)$ holds, as desired.
  - Case 2: If $k + 1$ is not prime, then there exist $p, q \in \mathbb{N}$ with $2 \leq p \leq q \leq k$ such that $k + 1 = pq$. Fix such p and q. By the inductive hypothesis, both p and q are either prime or a product of primes. Thus, for some $a, b \in \mathbb{Z}^+$,

    $$p = \prod_{i=1}^{a} p_i, \quad q = \prod_{j=1}^{b} q_j$$

    where the p_i's and q_j's are primes. Therefore,

    $$k + 1 = \left(\prod_{i=1}^{a} p_i\right)\left(\prod_{j=1}^{b} q_j\right),$$

    which shows that $k + 1$ is a product of primes. Hence $P(k + 1)$ holds.

By the strong principle of mathematical induction, $P(n)$ holds for all integers $n \geq 2$. □

12. September 24

12.1. Principle of Mathematical Induction

12.1.1. Strong Induction

To see another variety of a strong induction proof, let us now revisit Example 11.1.4.

Example 12.1.1.

Claim: For all $n \in \mathbb{N}$, $f_n < 2^n$.

We will have two base cases for this proof for two reasons. First, f_0 and f_1 are defined independently of the previous terms, so the truth value of $f_n < 2^n$ will need to be manually verified for these terms. Secondly, since f_n is defined in terms of the previous **two** terms for $n \geq 2$, we will need to know that the inequality holds for two consecutive terms in order to apply the (strong) inductive hypothesis.

Proof. We proceed by strong induction on $n \in \mathbb{N}$.

- **Base Cases**: We verify that the inequality holds for $n = 0$ and $n = 1$.
  - $n = 0$. $f_0 = 0 < 1 = 2^0$, as desired.
  - $n = 1$. $f_1 = 1 < 2 = 2^1$, as desired.
- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 1$, and assume that $f_i < 2^i$ for all $i \in \mathbb{Z}$ with $0 \leq i \leq k$. We want to show $f_{k+1} < 2^{k+1}$.

$$\begin{aligned} f_{k+1} &= f_k + f_{k-1} && \text{(by definition, since } k+1 \geq 2\text{)} \\ &< 2^k + 2^{k-1} && \text{(by IH)} \\ &= 2^{k-1}(2+1) \\ &= 2^{k-1} \cdot 3 \\ &< 2^{k-1} \cdot 2^2 \\ &= 2^{k+1} \end{aligned}$$

  Therefore, $f_{k+1} < 2^{k+1}$, as desired.

By the strong principle of mathematical induction, we conclude that $f_n < 2^n$ for all $n \in \mathbb{N}$. □

Note. In our first strong induction example, it was necessary to assume that $P(i)$ held for all $2 \leq i \leq k$ in order to conclude that $P(k+1)$ holds. In this example, however, it was enough to assume that $P(k-1)$ and $P(k)$ hold in order to prove $P(k+1)$. The standard strong induction hypothesis is sufficient here, but you could alternatively rephrase the inductive hypothesis to match the specific assumptions actually used in the proof. For instance:

> Let $k \in \mathbb{N}$ with $k \geq 1$ such that $f_k < 2^k$ and $f_{k-1} < 2^{k-1}$. We want to show that $f_{k+1} < 2^{k+1}$.

Notice that, thanks to our two base cases, this hypothesis is valid when $k = 1$. From there, we can conclude that $P(2)$ holds, then $P(3)$ holds, and so on.

SPMI With Multiple Base Cases

Let $M \in \mathbb{Z}$ and define $S = \{n \in \mathbb{Z} \mid n \geq M\}$.

Claim: $\forall n \in S, P(n)$.

Proof: We proceed by strong induction on $n \in S$.

Base Cases: Prove $P(M), P(M+1), \ldots, P(M+s)$ hold.

Inductive Step: Let $k \in \mathbb{Z}$ with $k \geq M+s$ and assume $P(i)$ holds for all $i \in \mathbb{Z}$ with $M \leq i \leq k$. Show $P(k+1)$ holds.

By the strong principle of mathematical induction, we conclude that $\forall n \in S, P(n)$ holds.

Exercise 12.1.2. Define a sequence recursively as follows.

$$a_n = \begin{cases} 2 & \text{if } n = 0 \\ 2 & \text{if } n = 1 \\ 2a_{n-1} + 8a_{n-2} & \text{if } n \geq 2 \end{cases}$$

Prove that $a_n = 4^n + (-2)^n$ for all $n \in \mathbb{N}$.

Exercise 12.1.3. Define the sequence $\langle a_n \rangle_{n \in \mathbb{Z}^+}$ recursively as follows:

$$a_n = \begin{cases} 2 & \text{if } n = 1 \\ 3 & \text{if } n = 2 \\ 4 & \text{if } n = 3 \\ a_{n-1} + 3a_{n-3} + 2 & \text{if } n \geq 4 \end{cases}$$

Prove that $a_n \leq 2^n$ for all $n \in \mathbb{Z}^+$.

Exercise 12.1.4. Let f_n denote the n^{th} Fibonacci number. Prove that for all $n \in \mathbb{N}$, the following equality holds.

$$\sum_{k=1}^{n} f_{2k} = f_{2n+1} - 1$$

There is one more important consequence of the Principle of Mathematical Induction (actually logically equivalent to PMI) which we will discuss.

12.1.2. Well-Ordered Sets

Definition. Let X be a set ordered by $<$. X is called *well-ordered* if and only if every nonempty subset has a least element.

In future lectures, we will discuss how to construct other orderings of sets, but for now, we will be referring just to our standard $<$ ordering on $\mathbb{R}$ and its subsets.

Examples 12.1.5. Some examples of well-ordered sets (ordered by $<$):

1. $\mathbb{N}$
2. $\{x \in \mathbb{Z} \mid x \geq -100\}$
3. $\left\{\frac{n}{2} \mid n \in \mathbb{N}\right\}$
4. $\{2^n \mid n \in \mathbb{N}\}$

Non-Examples 12.1.6. Plenty of sets are not well-ordered under the standard $<$ ordering. If there exists a nonempty subset with no least element, then the set is not well-ordered. For instance,

1. $\mathbb{Z}$
2. $\mathbb{R}$
3. $[0, 1)$
4. $\{2^n \mid n \in \mathbb{Z}\}$

Well-ordered sets are important with regard to mathematical induction. Every set that we have inducted on so far has been a well-ordered subset of $\mathbb{Z}$, although we haven't proven that yet. This is a consequence of the following theorem, which also will give us a new variation on mathematical induction.

Theorem 12.1.7 (Well-Ordering Property)**.** $\mathbb{N}$ *is well-ordered by* $<$.

Proof. Let $P(n)$ be the predicate "every subset of $\mathbb{N}$ containing n has a least element." We will prove $P(n)$ holds for all $n \in \mathbb{N}$ by strong induction.

> **Base Case**: $n = 0$. Since 0 is the least natural number, any subset of $\mathbb{N}$ containing 0 has a least element. Thus $P(0)$ holds.

Inductive Step: Let $k \in \mathbb{N}$ and assume $P(i)$ holds for all natural numbers i with $0 \leq i \leq k$. Now consider $n = k + 1$, and let $S \subseteq \mathbb{N}$ with $k + 1 \in S$.

- If S has no element less than $k + 1$, then $k + 1$ is the least element in S.
- If S contains an element $i \leq k$, then by inductive hypothesis, we know $P(i)$ holds. Hence S has a least element.

Since these are the only two possibilities, $P(k + 1)$ holds.

By the strong principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$.

Since any nonempty subset $S \subseteq \mathbb{N}$ must contain some $n \in \mathbb{N}$, we conclude that $\mathbb{N}$ is well-ordered. □

There was nothing special about starting at 0 in $\mathbb{N}$. We therefore have the following corollary.

Corollary 12.1.8. *For $M \in \mathbb{Z}$, if $S = \{x \in \mathbb{Z} \mid x \geq M\}$, then S is well-ordered.*

We'll see two main uses for the Well-Ordering Property.

WOP as Part of a Larger Proof

In number theory and other fields of discrete mathematics, it is common to use the Well-Ordering Property (the existence of a least element satisfying the proposition) as a step in a larger proof. We'll use it here to finally complete the proof of the Division Algorithm.

Theorem 12.1.9 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$.*

We have already shown that if such q and r exist, then they are unique (see the proof of Theorem 3.1.1). It remains to show that q and r always exist.

Existence. Define $S \subseteq \mathbb{N}$ as follows:

$$S = \{n \in \mathbb{N} \mid \exists k \in \mathbb{Z}, (n = a - bk)\}.$$

For any integer $k \leq \frac{a}{b}$, we have $a - bk \geq 0$, so $S \neq \varnothing$. By the Well-Ordering Property, there exists a least element $r \in S$. Fix r. Then, by definition of S, we have $r = a - bq$ for some $q \in \mathbb{Z}$. Fix q as well. We want to show that these are our desired values of q and r from the statement of the theorem.

Since $r \in S \subseteq \mathbb{N}$, we know $r \geq 0$. It remains to show that $r < b$.

Assume, for the sake of contradiction, that $r \geq b$. Then $r - b \geq 0$. Substituting $r = a - bq$, we compute:

$$r - b = a - bq - b = a - b(q + 1) \geq 0.$$

This implies that $r - b \in S$, contradicting our assumption that r was the least element of S. Hence, $a = bq + r$ with $0 \leq r < b$.

Therefore, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$, as desired. $\square$

13. September 26

13.1. Principle of Mathematical Induction

13.1.1. Well-Ordered Sets

Proof by Infinite Descent

The other major application of the Well-Ordering Property is a variant of induction known as a *proof by infinite descent*.

One consequence of the Well-Ordering Property is that there is no infinite descending sequence of natural numbers. In a proof by infinite descent, we assume, for the sake of contradiction, that the claim fails for some $n \in \mathbb{N}$. We then show that it must also fail for a smaller value $m \in \mathbb{N}$. Iterating this process would yield an infinite descending sequence of natural numbers, contradicting the Well-Ordering Property.

There are many different ways of phrasing infinite descent arguments, but below we present one outline of how such a proof may proceed.

Template for Infinite Descent Proofs

Claim: $\forall n \in \mathbb{N}, P(n)$

Proof: Assume for the sake of contradiction (AFSOC) that $\exists n \in \mathbb{N}$ such that $\neg P(n)$ holds. Let $n \in \mathbb{N}$ be the least natural number such that $\neg P(n)$ holds (which exists by the WOP).

Show that $\exists k \in \mathbb{N}$ with $k < n$ such that $\neg P(k)$ holds. This contradicts our assumption.

Therefore, by the Well-Ordering Property, $\forall n \in \mathbb{N}, P(n)$ holds.

Example 13.1.1. Claim: $\sqrt{2}$ is irrational.

Proof. To prove that $\sqrt{2}$ is irrational, it suffices to show that

$$\sqrt{2} \neq \frac{m}{n} \quad \text{for all } m, n \in \mathbb{Z}^+.$$

Define the predicate $P(n)$ on $n \in \mathbb{Z}^+$ by

$$P(n) := \forall m \in \mathbb{Z}^+, (\sqrt{2} \neq \frac{m}{n}).$$

Our goal is to show that $\forall n \in \mathbb{Z}^+, P(n)$ holds.

Assume, for the sake of contradiction, that $\exists n \in \mathbb{Z}^+$ such that $\neg P(n)$ holds. Fix $n \in \mathbb{Z}^+$ as the least such that $\neg P(n)$ holds, which exists by the Well-Ordering Property. Since $\neg P(n)$ holds, there exists $m \in \mathbb{Z}^+$ such that $\sqrt{2} = \frac{m}{n}$. Fix such an m. Squaring both sides of the equation and rearranging gives

$$2n^2 = m^2.$$

Thus m^2 is even. By Proposition 7.1.1, m is even, so $m = 2m'$ for some $m' \in \mathbb{Z}^+$. Fix m'. Substituting back, we obtain

$$2n^2 = 4(m')^2 \quad \Rightarrow \quad n^2 = 2(m')^2.$$

This implies n^2 is even, and hence n is even. Therefore $n = 2n'$ for some $n' \in \mathbb{Z}^+$. Fix n'. Since $n = 2n'$ and $n' < n$, we have found a smaller denominator. Substituting back, we get

$$\sqrt{2} = \frac{m}{n} = \frac{2m'}{2n'} = \frac{m'}{n'}.$$

Thus $\neg P(n')$ holds, contradicting the minimality of n.

Therefore, our assumption was false, and $P(n)$ holds for all $n \in \mathbb{Z}^+$. Hence $\sqrt{2}$ is irrational. □

Exercise 13.1.2. Prove that $\sqrt[3]{3}$ must be irrational.

Part III.

Functions and Relations

14. September 26

14.1. Binary Relations

In this section, we will explore the concept of a *binary relation* between two sets (often just called a *relation*). The idea of a relation between two sets is already familiar to you. A binary relation allows us to compare or link elements from two sets. For instance, when we say $2 < 3$, we are comparing two elements from $\mathbb{Z}$. Similarly, when we say "Bill takes a class with Professor Johnson," we are linking an element from the set of students with an element from the set of professors.

We formalize this idea by defining a binary relation as a subset of the Cartesian product of the two sets being linked.

Definition. Let S and T be sets.

- If $R \subseteq S \times T$, then R is called a *binary relation between* S and T. If $(a, b) \in R$, we say that "a is in relation to b," sometimes denoted aRb.
- S is called the *domain* of R, and T is called the *codomain* of R.

Many of the common relations in mathematics (and in other contexts) are relations where both elements belong to the same set (i.e., $S = T$). In that case, we simply say that R *is a relation on* S, meaning that $R \subseteq S \times S$.

We begin by examining examples of binary relations, some linking elements of different sets, and others connecting elements of the same set.

Examples 14.1.1.

1. Let S be the set of students at CMU and T be the set of professors at CMU. We define a relation $R \subseteq S \times T$ such that $(s, t) \in R$ if and only if s has taken a class with t. That is,

   $$R = \{(s, t) \in S \times T \mid s \text{ has taken a class with } t\}.$$

   For any given pair (s, t) of student and professor, we can determine whether s has taken a class with t by checking if $(s, t) \in R$.

2. The standard ordering relation $<$ is a relation on sets such as $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$. We can express this comparison as a set of ordered pairs. For instance, for $x, y \in \mathbb{R}$, we have
$$x < y \text{ iff } (x, y) \in \{(a, b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R}^+, (a + c = b)\}.$$

3. The divisibility relation on the integers is another common example. Recall that for $m, n \in \mathbb{Z}$, we say that $m \mid n$ if and only if there exists $k \in \mathbb{Z}$ such that $m \cdot k = n$. This relation can be viewed as the set of ordered pairs R_d:
$$R_d = \{(m, n) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}, (m \cdot k = n)\}.$$

4. The subset relation $\subseteq$ is another familiar example. Let S be a set. We define the binary relation of $\subseteq$ on $\mathcal{P}(S)$ (the power set of S) such that for any $A, B \in \mathcal{P}(S)$, the following holds:
$$A \subseteq B \text{ iff } \forall x \in S, (x \in A \to x \in B).$$
We can also express this relation as the set of ordered pairs, R_s:
$$R_s = \{(A, B) \in \mathcal{P}(S) \times \mathcal{P}(S) \mid \forall x \in S, (x \in A \to x \in B)\}.$$

5. Functions are another important type of binary relation. For instance, the function $f(x) = x^2$, defined for $x \in \mathbb{R}$, is a relation that links elements of $\mathbb{R}$ with other elements of $\mathbb{R}$. The function f can be represented as the set of ordered pairs in $\mathbb{R}^2$ that satisfy the condition $y = x^2$. In other words, the function f is given by:
$$f = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}.$$
This set is commonly referred to as the *graph* of f.

6. Equality is perhaps the most common binary relation on any set. For any set S, equality can be expressed as the set of ordered pairs for which the first and second components are identical:
$$R_e = \{(a, a) \in S \times S \mid a \in S\}.$$

Exercise 14.1.2. Let $S = \{1, 2, 3\}$.

(a) How many different binary relations on S exist?

(b) What is the binary relation on S with the fewest number of elements?

(c) What is the binary relation on S with the most number of elements?

14.2. Functions

Recall how a function was first introduced to you in earlier courses. Was it presented as a "rule" mapping elements from one set to another? Was it defined as a curve in $\mathbb{R}^2$ that passes the vertical line test? What if there is no explicit rule for defining the mapping? Must a function be something that we can graph in $\mathbb{R}^2$? Formally, a function is a relation that is more general than these definitions.

Definition. Let A and B be sets, and let f be a binary relation between A and B. We say that f is a *function from A to B*, denoted $f : A \to B$, if and only if for each $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

Notation: We write $f(a) = b$ to mean that $(a, b) \in f$.

Recall that for any relation $R \subseteq A \times B$, we say that A is the *domain* of R and B is the *codomain* of R. This terminology is most commonly used when f is a function. If $f : A \to B$ is a function, then A is the domain of f and B is the codomain of f.

Examples 14.2.1.

1. Let S be any set. We define the *identity function on S*, denoted Id_S or simply Id if the domain is clear from context, by

   $$\mathrm{Id}_S : S \to S \text{ such that for all } x \in S,\ \mathrm{Id}_S(x) = x.$$

   That is, the identity function maps each element to itself. Equivalently, we can write Id_S as the set of ordered pairs:

   $$\mathrm{Id}_S = \{(x, x) \mid x \in S\}.$$

2. Define the function $f : \mathbb{R}^+ \to \mathbb{R}$ by $f(x) = \sqrt{x}$ for any $x \in \mathbb{R}^+$. Then f is a function and can be expressed formally as:

   $$f = \{(a, b) \in \mathbb{R}^+ \times \mathbb{R} \mid a = b^2 \wedge b > 0\}.$$

3. Let $A = \{x, y, z\}$. Define $g : A \to \mathbb{N}$ by:

   $$g = \{(x, 1), (y, 10), (z, 42)\}.$$

   Note that there is no requirement for a specific pattern in the mapping, even if the domain is infinite. We do not need to explicitly write a rule defining the mapping for it to be a function. We simply need to ensure that for each $a \in A$, there is a unique $b \in B$ such that $(a, b) \in g$.

Non-Examples 14.2.2. The following proposed "functions" are *ill-defined*:

1. Suppose you define a mapping $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \frac{1}{x}$.

   f is not defined over the entire domain. In particular, $f(0)$ is undefined.

2. Suppose you define a mapping $g : \mathbb{N} \to \mathbb{N}$ by $g(n) = \sqrt{n}$.

   While $g(n)$ is defined for each $n \in \mathbb{N}$, the output does not always belong to the codomain $\mathbb{N}$. For example, $g(2) = \sqrt{2} \notin \mathbb{N}$.

3. Suppose you define a mapping $h : \mathbb{Q} \to \mathbb{Z}$ by $h\left(\frac{p}{q}\right) = p + q$.

   h is not well-defined because it fails to satisfy the uniqueness condition. For instance, $\frac{1}{2} = \frac{2}{4}$, but $h\left(\frac{1}{2}\right) = 3$ while $h\left(\frac{2}{4}\right) = 6$.

15. September 29

15.1. Functions

As seen in the previous non-examples, we can be given a rule for a mapping $f : A \to B$, and it may not be clear whether or not it is a function. For this reason, we introduce the terminology of a *well-defined function*. A well-defined function is simply a binary relation that satisfies the definition of a function. However, it is worth emphasizing this point, as we are often given "rules" for mappings rather than explicit sets of ordered pairs.

Definition. A mapping $f : A \to B$ is a *well-defined function* iff f satisfies the following conditions:

1. **(Totality)** For all $a \in A$, $f(a)$ is defined. (That is, A is the domain of f.)
2. **(Existence)** For all $a \in A$, $f(a) \in B$. (That is, f maps each element of A to an element of B, so B is the codomain.)
3. **(Uniqueness)** For all $a \in A$, $f(a)$ must be uniquely defined. (That is, for each $a \in A$, there is a unique element in B corresponding to a.)

Condition 3 may seem obvious, but it becomes important in cases where the domain consists of multiple representations of the same element (such as $\frac{1}{2}$ and $\frac{2}{4}$), or when the mapping is defined piecewise.

Exercise 15.1.1. Determine which of the following maps are well-defined functions.

(a) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f\left(\frac{m}{n}\right) = \frac{m+n}{n^2}$

(b) $g : \mathbb{Q} \to \mathbb{Q}$ defined by $g\left(\frac{m}{n}\right) = \frac{2m+n}{2n}$

(c) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \frac{x^2-1}{x^2+1}$

(d) $j : \mathbb{R} \to \mathbb{R}$ defined by $j(x) = \frac{x^2+1}{x^2-1}$

(e) $k : \mathbb{N} \to \mathbb{N}$ defined by $k(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n}{3} & \text{if } 3 \mid n \\ n & \text{otherwise} \end{cases}$

(f) $\ell : \mathbb{N} \to \mathbb{N}$ defined by $\ell(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } 4 \mid n \\ n & \text{otherwise} \end{cases}$

Because a function is simply a set of ordered pairs, the equality of two functions follows directly from the definition of equality for sets.

Theorem 15.1.2 (Function Equality)**.** *Let A and B be sets, and let $f : A \to B$ and $g : A \to B$ be functions. Then $f = g$ if and only if $\forall a \in A$, $f(a) = g(a)$.*

Exercise 15.1.3. Prove the above theorem.

The important point is that two functions are considered equal not based on how they are defined, but on their behavior: they must yield the same output for every element in the domain, regardless of how their rules are expressed.

Example 15.1.4. Let $A = \{1, 2, 3\}$. Define $f : A \to \mathbb{Z}$ by $f(x) = x^3 - x^2 - 6$ and $g : A \to \mathbb{Z}$ by $g(x) = 5x^2 - 11x$.

At first glance, f and g seem to be different functions because they have different defining expressions. However, since A has only three elements, we can manually verify that f and g give the same output for every element in A:

$$f = \{(1, -6), (2, -2), (3, 12)\} = g$$

Therefore, f and g are indeed equal despite their differing rules.

You may have noticed that we have not used the word "range" when discussing functions. This is because the term "range" can be ambiguous: some use it to mean the *codomain* (the set of potential outputs), while others use it to mean the set of actual outputs. To avoid this ambiguity, we will not use the term "range." Instead, we use the term *image* when referring to the set of actual outputs, as defined below.

15.1.1. Images and Preimages

Definition. Let A and B be sets, and let $f : A \to B$ be a function. For any subset $X \subseteq A$, the *image of X under f*, denoted by $\mathrm{Im}_f(X)$, is defined as:

$$\mathrm{Im}_f(X) = \{b \in B \mid \exists a \in X, (f(a) = b)\}.$$

If $X = A$, we refer to this as the *image of f*.

Note. The image of any subset $X \subseteq A$ under f is always a subset of the codomain B. That is, for any $X \subseteq A$, we have $\text{Im}_f(X) \subseteq B$.

Example 15.1.5. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Then:

$$\text{Im}_f(\mathbb{R}) = [0, \infty),$$
$$\text{Im}_f(\{-2, 1, 2\}) = \{1, 4\}.$$

Let's now see how to use the definition of images in a proof.

Proposition 15.1.6. *Let A and B be sets, and let $f : A \to B$ be a function. For any $S, T \in \mathcal{P}(A)$, we have*

$$Im_f(S \cap T) \subseteq Im_f(S) \cap Im_f(T)$$

Proof. Let $y \in \text{Im}_f(S \cap T)$ be arbitrary. By the definition of the image, there exists some $x \in S \cap T$ such that $f(x) = y$. Fix such an x. By the definition of intersection, we have $x \in S$ and $x \in T$. Since $y = f(x)$ and $x \in S$, it follows that $y \in \text{Im}_f(S)$. Similarly, since $x \in T$, we also have $y \in \text{Im}_f(T)$. Thus, $y \in \text{Im}_f(S) \cap \text{Im}_f(T)$, as desired.

Since y was arbitrary, we conclude that $\text{Im}_f(S \cap T) \subseteq \text{Im}_f(S) \cap \text{Im}_f(T)$. □

Exercise 15.1.7. Show that the reverse containment does not always hold.

Similar to the definition of an image, we have the concept of a *preimage* (also called the *inverse image*). The image of a set is the set of outputs corresponding to inputs from the original set. Similarly, the preimage of a subset of the codomain is the set of inputs that yield those outputs (if any). We formalize this idea below.

Definition. Let A and B be sets, and let $f : A \to B$ be a function. For any subset $Y \subseteq B$, the *preimage of Y under f*, denoted $\text{PreIm}_f(Y)$, is defined as:

$$\text{PreIm}_f(Y) = \{a \in A \mid f(a) \in Y\}$$

Note. Since A is the domain of f, it always holds that $\text{PreIm}_f(B) = A$.

Example 15.1.8. Consider again the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. Then:

$$\text{PreIm}_f(\mathbb{R}) = \mathbb{R},$$
$$\text{PreIm}_f([0, \infty)) = \mathbb{R},$$
$$\text{PreIm}_f(\{1, 4\}) = \{\pm 1, \pm 2\},$$
$$\text{PreIm}_f(\{1, -4\}) = \{\pm 1\},$$
$$\text{PreIm}_f([-1, 4]) = [-2, 2].$$

Proposition 15.1.9. *Let A and B be sets, and let $f : A \to B$ be a function. For any $S, T \in \mathcal{P}(B)$, we have*

$$PreIm_f(S \cap T) = PreIm_f(S) \cap PreIm_f(T)$$

Proof. Let $S, T \in \mathcal{P}(B)$ and $a \in A$ be arbitrary. Then

$$\begin{aligned}
a \in \mathrm{PreIm}_f(S \cap T) &\iff f(a) \in S \cap T && \text{(definition of preimage)} \\
&\iff f(a) \in S \ \wedge \ f(a) \in T && \text{(definition of intersection)} \\
&\iff a \in \mathrm{PreIm}_f(S) \ \wedge \ a \in \mathrm{PreIm}_f(T) && \text{(definition of preimage)} \\
&\iff a \in \mathrm{PreIm}_f(S) \cap \mathrm{PreIm}_f(T) && \text{(definition of intersection).}
\end{aligned}$$

Since $a \in A$ was arbitrary, we conclude that $\mathrm{PreIm}_f(S \cap T) = \mathrm{PreIm}_f(S) \cap \mathrm{PreIm}_f(T)$. □

Exercise 15.1.10. Define a function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \sqrt{1 + x^2}$. Determine the following sets.

(a) $\mathrm{Im}(f)$.

(b) $\mathrm{Im}_f([-5, 5])$

(c) $\mathrm{PreIm}_f([0, 1])$

(d) $\mathrm{PreIm}_f((3, 5))$

Exercise 15.1.11. Let A and B be nonempty sets and $f : A \to B$ be a function. Prove that the following equality holds for all $Y_1, Y_2 \in \mathcal{P}(B)$.

$$\mathrm{PreIm}_f(Y_1 \setminus Y_2) = \mathrm{PreIm}_f(Y_1) \setminus \mathrm{PreIm}_f(Y_2)$$

15.1.2. Jections

We now introduce a few special (and important!) types of functions: surjections, injections, and bijections.

Injections

Definition. Let A and B be sets, and let $f : A \to B$ be a function. We say that f is *injective* (or *one-to-one*) if and only if for all $x, y \in A$, if $f(x) = f(y)$, then $x = y$.

Standard Injectivity Proof Outline

- Let $x, y \in A$ such that $f(x) = f(y)$.
- Use the definition of f and other assumptions to show that $x = y$.
- Conclude that f is injective.

Let's begin with a simple example to illustrate this concept.

Example 15.1.12. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 5x + 6$. Prove that f is an injection.

Proof. Let $x, y \in \mathbb{R}$ such that $f(x) = f(y)$. Then:

$$5x + 6 = 5y + 6.$$

Subtracting 6 from both sides, we get

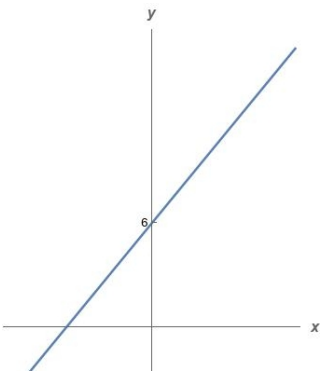
$$5x = 5y.$$

Dividing both sides by 5 gives:

$$x = y.$$

Therefore, f is injective. □

In early algebra courses, we often say that a function $f : \mathbb{R} \to \mathbb{R}$ is injective if and only if it "passes the horizontal line test." This means that any horizontal line drawn in the Cartesian plane will intersect the graph of the function at most once. In the case of the function $f(x) = 5x + 6$, the graph passes the horizontal line test, as shown on the right.



A function fails the horizontal line test if there are two distinct values of x that correspond to the same value of y.

16. October 1

16.1. Functions

16.1.1. Jections

Injections

We now look at a function where the definition splits into two cases depending on whether the input is positive or not.

Example 16.1.1. Define a function $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n - 1 & \text{if } n > 0, \\ -2n & \text{if } n \leq 0. \end{cases}$$

Claim: f is injective.

Proof. Let $x, y \in \mathbb{Z}$ such that $f(x) = f(y)$.

We will consider three cases: (1) both x and y are positive, (2) both x and y are non-positive, and (3) one is positive and the other is non-positive.

- Case 1: Suppose $x, y > 0$. In this case, $f(x) = f(y)$ implies $2x - 1 = 2y - 1$. By adding 1 to both sides, we get $2x = 2y$, and dividing by 2, we obtain $x = y$.
- Case 2: Suppose $x, y \leq 0$. Here, $f(x) = f(y)$ implies $-2x = -2y$. Dividing both sides by -2, we get $x = y$.
- Case 3: Without loss of generality, assume $x > 0$ and $y \leq 0$. Then, $f(x) = f(y)$ implies $2x - 1 = -2y$. Rearranging this, we have $2x + 2y = 1$, or equivalently, $x + y = \frac{1}{2}$. However, $x + y \in \mathbb{Z}$, while $\frac{1}{2} \notin \mathbb{Z}$, a contradiction. Hence, this case is not possible.

Since in all cases we either have $x = y$ or a contradiction, we conclude that $f(x) = f(y)$ implies $x = y$ for all $x, y \in \mathbb{Z}$. Therefore, f is injective. □

Remark. It is important not to forget the third case where one input is positive and the other is non-positive. Although it might feel like the first two cases should cover

everything, the mixed case is precisely where we need to argue that no equality is possible. Without this check, the proof would be incomplete.

Disproving Injectivity

To show that a function $f : A \to B$ is not injective, it is enough to find distinct elements $x, y \in A$ such that $f(x) = f(y)$. This kind of argument is usually a simple proof by demonstration.

Example 16.1.2. As a contrast, let us examine a function that fails to be injective.

Define $f : \mathbb{Z}^2 \to \mathbb{Z}$ by $f(x, y) = x + y$.

Claim: f is not an injection.

Proof. Consider $(0, 0), (1, -1) \in \mathbb{Z}^2$. Since $(0, 0) \neq (1, -1)$ but $f(0, 0) = 0 = f(1, -1)$, we have found two distinct inputs with the same output. Therefore f is not an injection. □

Exercise 16.1.3. Determine whether or not the following functions are injections.

(a) $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(x, y) = (3x + 4y, 2x + y)$.

(b) $g : \mathbb{R}^3 \to \mathbb{R}^2$ such that $f(x, y, z) = (xz, yz)$.

(c) $h : \mathbb{R} \to \mathbb{R}$ such that

$$h(x) = \begin{cases} x^3 + 3x^2 + 3x & \text{if } x \leq 0 \\ 5 - 2x & \text{if } x > 0 \end{cases}$$

(d) $j : \mathbb{N}^2 \to \mathbb{Z}$ such that

$$j(a, b) = \begin{cases} b & \text{if } a = 0 \\ -2^{a-1}(2b + 1) & \text{if } a > 0 \end{cases}$$

Recall the result from recitation that every positive integer can be expressed uniquely as a power of 2 times an odd number.

Surjections

Definition. Let A and B be sets, and let $f : A \to B$ be a function. We say f is *surjective* (or *onto*) if and only if $\text{Im}_f(A) = B$. That is,

$$\forall b \in B,\ \exists a \in A \text{ such that } f(a) = b.$$

Standard Surjectivity Proof Outline

- Let $b \in B$ be arbitrary and fixed.
- Show that there exists $a \in A$ such that $f(a) = b$. (This is often done by explicitly constructing such an a.)
- Conclude that f is surjective.

Notice that surjectivity focuses on whether every element of the codomain is "hit" by the function. As a first illustration, let's revisit the function from Example 16.1.2. Although it failed to be injective, we will see that it *is* surjective.

Example 16.1.4. Define $f : \mathbb{Z}^2 \to \mathbb{Z}$ by $f(m, n) = m + n$.

Claim: f is a surjection.

Proof. Let $y \in \mathbb{Z}$ be arbitrary. We want to show that there exists $(m, n) \in \mathbb{Z}^2$ such that $f(m, n) = y$.

Consider $(y, 0) \in \mathbb{Z}^2$. Then

$$f(y, 0) = y + 0 = y.$$

Since y was arbitrary, this proves that f is surjective. □

Example 16.1.5. Let $f : \mathbb{Q} \to \mathbb{Q}$ be defined by $f(x) = 1 + 2x$.

Claim: f is a surjection.

Proof. Let $y \in \mathbb{Q}$. Then $y = \dfrac{m}{n}$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. Fix such m and n.

To find x such that $f(x) = y$, we need to solve

$$1 + 2x = \frac{m}{n}.$$

Rearranging the equation, we get $x = \dfrac{m - n}{2n}$. Since m and n are integers with $n \neq 0$, it follows that $x = \dfrac{m - n}{2n} \in \mathbb{Q}$. Then

$$f\left(\frac{m - n}{2n}\right) = 1 + 2 \cdot \frac{m - n}{2n} = 1 + \frac{m - n}{n} = \frac{n + (m - n)}{n} = \frac{m}{n} = y.$$

Since $y \in \mathbb{Q}$ was arbitrary, we conclude that f is surjective. □

Next, let us revisit the function from Example 16.1.1. Earlier we showed it was injective; here we will prove that it is also surjective. This means the function actually turns out to be a bijection, though we will make that terminology precise later.

Example 16.1.6. Define a function $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n - 1 & \text{if } n > 0, \\ -2n & \text{if } n \leq 0. \end{cases}$$

Claim: f is a surjection.

Proof. Let $y \in \mathbb{N}$ be arbitrary. We consider two cases: when y is even and when y is odd.

- Case 1: Suppose y is even. Then $y = 2k$ for some $k \in \mathbb{N}$. Consider $x = -k$. Since $-k \leq 0$, we have
$$f(x) = f(-k) = -2(-k) = 2k = y.$$
- Case 2: Suppose y is odd. Then $y = 2k+1$ for some $k \in \mathbb{N}$. Consider $x = k+1 \in \mathbb{Z}$. Since $k + 1 > 0$, we have
$$f(x) = f(k + 1) = 2(k + 1) - 1 = 2k + 1 = y.$$

Since we have addressed both possibilities, we conclude that f is surjective. □

Disproving Surjectivity

A function $f : A \to B$ is not surjective if and only if there exists an element $b \in B$ such that $f(a) \neq b$ for all $a \in A$.

In other words, to disprove surjectivity it suffices to find a single element in the codomain that is not in the image of f.

Example 16.1.7. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \frac{x+|x|}{2}$.

Claim: f is not a surjection.

Proof. Consider $y = -1 \in \mathbb{R}$. Assume for the sake of contradiction that there exists $x \in \mathbb{R}$ such that $f(x) = -1$. Then:

$$\frac{x + |x|}{2} = -1.$$

We consider two cases based on the value of x:

- Case 1: Suppose $x \geq 0$. Then $|x| = x$, and the equation becomes
$$\frac{x + x}{2} = -1 \implies \frac{2x}{2} = -1 \implies x = -1.$$
But this contradicts our assumption that $x \geq 0$.

- Case 2: Suppose $x < 0$. Then $|x| = -x$, and the equation becomes

$$\frac{x - x}{2} = -1 \implies \frac{0}{2} = -1 \implies 0 = -1,$$

which is a contradiction.

Since both cases lead to a contradiction, there is no $x \in \mathbb{R}$ such that $f(x) = -1$. Thus, -1 is not in the image of f, and f is not surjective. □

Exercise 16.1.8. Determine whether or not the following functions are surjections.

(a) $f : \mathbb{N}^2 \to \mathbb{Z}$ such that $f(a, b) = 2^a - 3^b$.

(b) $g : \mathbb{R}^3 \to \mathbb{R}^2$ such that $g(x, y, z) = (xz, yz)$.

(c) $h : \mathbb{R} \to \mathbb{R}$ such that

$$h(x) = \begin{cases} x^3 + 3x^2 + 3x & \text{if } x \leq 0 \\ 5 - 2x & \text{if } x > 0 \end{cases}$$

(d) $j : \mathbb{N}^2 \to \mathbb{Z}$ such that

$$j(a, b) = \begin{cases} b & \text{if } a = 0 \\ -2^{a-1}(2b + 1) & \text{if } a > 0 \end{cases}$$

Recall the result from recitation that every positive integer can be expressed uniquely as a power of 2 times an odd number.

Bijections

Definition. Let A and B be sets, and let $f : A \to B$ be a function. We say that f is a *bijection* if and only if f is both an injection and a surjection.

We have already encountered some examples of bijections, though we did not explicitly call them that at the time.

Example 16.1.9. Define $f : \mathbb{Z} \to \mathbb{N}$ by

$$f(n) = \begin{cases} 2n - 1 & \text{if } n > 0, \\ -2n & \text{if } n \leq 0. \end{cases}$$

Recall from Example 16.1.1 that we proved f is injective, and from Example 16.1.6 that f is surjective. Therefore, f is a bijection.

Example 16.1.10. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 5x + 6$. In Example 15.1.12, we showed that f is injective. It remains to verify that f is surjective.

Proof. Let $y \in \mathbb{R}$ be arbitrary. Consider $x = \dfrac{y-6}{5} \in \mathbb{R}$. Then

$$f\left(\frac{y-6}{5}\right) = 5\left(\frac{y-6}{5}\right) + 6 = y.$$

Therefore, f maps onto all of $\mathbb{R}$, proving that f is surjective. Since f is both injective and surjective, it follows that f is a bijection. □

In both examples, we established bijectivity by separately proving injectivity and surjectivity. This two-part process is the standard way to show that a function is a bijection. We now formalize it into a general strategy.

Proving Bijectivity – Method 1

To prove that a function $f : X \to Y$ is a bijection, you need to:

- Prove that f is an injection (i.e., for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$).
- Prove that f is a surjection (i.e., for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$).

Example 16.1.11. Define $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \begin{cases} \dfrac{1}{x-1}, & \text{if } x < 1, \\ \sqrt{x-1}, & \text{if } x \geq 1. \end{cases}$$

Claim: f is a bijection.

Proof. We will prove that f is both injective and surjective.

- **Injectivity**: Let $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$. We consider three cases:

  Case 1: Assume $x_1, x_2 < 1$. Then

  $$\frac{1}{x_1 - 1} = \frac{1}{x_2 - 1}.$$

  Rearranging gives $x_1 - 1 = x_2 - 1$, so $x_1 = x_2$, as required.

  Case 2: Assume $x_1, x_2 \geq 1$. Then

  $$\sqrt{x_1 - 1} = \sqrt{x_2 - 1}.$$

  Squaring both sides yields $x_1 - 1 = x_2 - 1$, so $x_1 = x_2$.

Case 3: Without loss of generality, assume $x_1 < 1$ and $x_2 \geq 1$. Then

$$f(x_1) = \frac{1}{x_1 - 1} < 0, \qquad f(x_2) = \sqrt{x_2 - 1} \geq 0.$$

Since a negative number cannot equal a nonnegative number, this contradicts the assumption that $f(x_1) = f(x_2)$.

Since all cases either forced $x_1 = x_2$ or led to a contradiction, we conclude that f is injective.

- **Surjectivity**: Let $y \in \mathbb{R}$. We want to show there exists $x \in \mathbb{R}$ such that $f(x) = y$. We split into two cases:

  Case 1: Suppose $y < 0$. Define $x = \frac{1}{y} + 1$. Since $y \neq 0$ and $y < 0$, it follows that $x < 1$. Then

  $$f(x) = f\left(\frac{1}{y} + 1\right) = \frac{1}{\frac{1}{y} + 1 - 1} = \frac{1}{\frac{1}{y}} = y.$$

  Case 2: Suppose $y \geq 0$. Define $x = y^2 + 1$. Since $y^2 \geq 0$, we have $x \geq 1$. Then

  $$f(x) = f(y^2 + 1) = \sqrt{y^2 + 1 - 1} = \sqrt{y^2} = |y| = y,$$

  where the last equality holds because $y \geq 0$.

  In both cases, we have found an $x \in \mathbb{R}$ such that $f(x) = y$. Therefore, f is surjective.

Since f is both injective and surjective, we conclude that f is a bijection. □

Because $f : \mathbb{R} \to \mathbb{R}$ is a bijection, this is also visible in its graph: every horizontal line intersects the graph at exactly one point, confirming both injectivity and surjectivity.

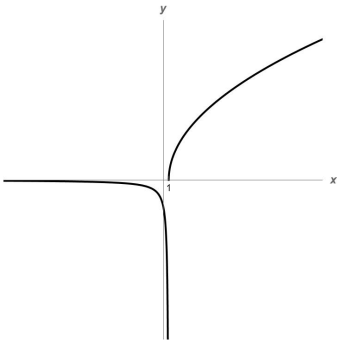


Figure 16.1.: The graph of the bijection

Exercise 16.1.12. Below are two functions from $\mathbb{R} \to (0, \infty)$. For each function, prove or disprove that it is a bijection.

(a) $f(x) = \begin{cases} e^x & \text{if } x \leq 0 \\ 2 - e^{-x} & \text{if } x > 0 \end{cases}$

(b) $g(x) = \begin{cases} -2x + 1 & \text{if } x \leq 0 \\ \dfrac{1}{2x+1} & \text{if } x > 0 \end{cases}$

16.1.2. Composition and Inverses of Functions

Before introducing a second method for proving bijectivity, we first need to define the operation of composing functions.

Definition. Let A, B, and C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. The *composition of g and f* is the function $h : A \to C$ defined by

$$h(a) = g(f(a)) \quad \text{for all } a \in A.$$

We denote this by $h = g \circ f$.

An important property of function composition is that it is *associative*.

Theorem 16.1.13 (Associativity of Composition)**.** *Let A, B, C, and D be sets, and let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be functions. Then*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Proof. Let $a \in A$. Then

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a).$$

Since $a \in A$ was arbitrary, we conclude that $h \circ (g \circ f) = (h \circ g) \circ f$. □

Note. Let $f : A \to B$. Then

$$\mathrm{Id}_B \circ f = f \quad \text{and} \quad f \circ \mathrm{Id}_A = f.$$

In particular, if $f : A \to A$, then

$$\mathrm{Id}_A \circ f = f \circ \mathrm{Id}_A = f.$$

This shows that the identity function is the identity element under the binary operation of composition.

17. October 3

17.1. Functions

17.1.1. Composition and Inverses of Functions

The following theorem summarizes key properties of function composition with respect to injections, surjections, and bijections.

Theorem 17.1.1. *Let A, B, and C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Then the following properties hold:*

1. *If f and g are injections, then $g \circ f : A \to C$ is also an injection.*
2. *If f and g are surjections, then $g \circ f : A \to C$ is also a surjection.*
3. *If f and g are bijections, then $g \circ f : A \to C$ is also a bijection.*

Proof.

1. Assume that $f : A \to B$ and $g : B \to C$ are injections. We will show that $g \circ f : A \to C$ is injective.

   Let $a_1, a_2 \in A$ such that $(g \circ f)(a_1) = (g \circ f)(a_2)$. By the definition of composition, this gives:

   $$g(f(a_1)) = g(f(a_2)).$$

   Since g is injective, we conclude:

   $$f(a_1) = f(a_2).$$

   And since f is injective, it follows that $a_1 = a_2$. Therefore, $g \circ f$ is injective.

2. The proof that $g \circ f$ is surjective is left as an exercise for recitation.

3. Since $g \circ f$ is both injective (by 1) and surjective (by 2), it is bijective.

□

Inverses

Now that we have defined function composition, we can introduce the concept of inverse functions and prove an important result about bijections.

Definition. Let A and B be sets, and let $f : A \to B$ and $g : B \to A$ be functions.

- g is called a *left inverse* of f if and only if $g \circ f = \mathrm{Id}_A$.
- g is called a *right inverse* of f if and only if $f \circ g = \mathrm{Id}_B$.
- g is called a *(two-sided) inverse* of f if and only if g is both a left and a right inverse.
- f is *invertible* if and only if f has a two-sided inverse.

Notation: If f is invertible, we denote its inverse function by f^{-1}.

While not every function is invertible, an important property of inverses is that if they exist, they are unique.

Theorem 17.1.2 (Uniqueness of Inverses)**.** *Let A and B be sets, and let $f : A \to B$ be a function. If f is invertible, then its inverse function f^{-1} is unique.*

Proof. Let $f : A \to B$ be invertible. Suppose $g : B \to A$ and $g' : B \to A$ are both inverses of f. We want to show that $g = g'$.

Since g and g' are inverses of f, we know:

$$f \circ g = \mathrm{Id}_B, \quad g \circ f = \mathrm{Id}_A, \quad f \circ g' = \mathrm{Id}_B, \quad g' \circ f = \mathrm{Id}_A.$$

Let $b \in B$ be arbitrary. Then

$$g(b) = (g \circ \mathrm{Id}_B)(b) = (g \circ (f \circ g'))(b) = ((g \circ f) \circ g')(b) = (\mathrm{Id}_A \circ g')(b) = g'(b).$$

Thus, $g(b) = g'(b)$ for all $b \in B$, which shows $g = g'$. Therefore, the inverse of f is unique. □

We now establish our major result for this section.

Theorem 17.1.3. *Let A and B be sets, and let $f : A \to B$ be a function. Then f is invertible if and only if f is a bijection.*

Proof.

($\Rightarrow$): Suppose f is invertible. Then there exists a function $g : B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. We show that f is a bijection.

- *Injective:* Let $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$. Applying g to both sides gives

$$g(f(a_1)) = g(f(a_2)).$$

  Since $g \circ f = \mathrm{Id}_A$, it follows that

$$id_A(a_1) = \mathrm{Id}_A(a_2) \quad \Longrightarrow \quad a_1 = a_2.$$

  Hence f is injective.

- *Surjective:* Let $b \in B$ be arbitrary. Define $a = g(b) \in A$. Since f and g are inverses, we have

$$f(a) = f(g(b)) = \mathrm{Id}_B(b) = b.$$

  Hence f is surjective.

Thus f is both injective and surjective, so f is a bijection.

($\Leftarrow$): Suppose f is a bijection (i.e., injective and surjective). Define the relation

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

We show g is a function from B to A.

Let $b \in B$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$, so $(b, a) \in g$. To show uniqueness, suppose $(b, a), (b, a') \in g$. Then $f(a) = b = f(a')$. Since f is injective, $a = a'$. Thus each $b \in B$ corresponds to a unique $a \in A$, so g is a function.

By construction, $f \circ g = \mathrm{Id}_B$ and $g \circ f = \mathrm{Id}_A$. Hence g is the inverse of f, so f is invertible.

□

From this theorem, we obtain a second method for proving bijectivity.

Proving Bijectivity – Method 2

To prove that $f : A \to B$ is a bijection, it suffices to show that f is invertible.

- Construct the inverse function $g : B \to A$ and prove that it is well-defined.
- Prove that $f \circ g = \mathrm{Id}_B$.
- Prove that $g \circ f = \mathrm{Id}_A$.
- Conclude that $g = f^{-1}$ and hence f is a bijection.

Note. This method is best suited to functions defined by simple rules (where one can easily solve for x in terms of $f(x)$). For more complicated functions (especially piecewise ones), it is typically clearer to prove injectivity and surjectivity directly.

Example 17.1.4. Let $S = \mathbb{R} \setminus \{3\}$ and $T = \mathbb{R} \setminus \{1\}$. Define $f : S \to T$ by

$$f(x) = \frac{x-2}{x-3}.$$

Prove that f is a bijection.

Scratch work:

$$y = \frac{x-2}{x-3} \implies xy - 3y = x - 2 \implies x(y-1) = 3y - 2 \implies x = \frac{3y-2}{y-1}.$$

Proof. Define $g : T \to S$ by

$$g(x) = \frac{3x-2}{x-1}.$$

We will show that g is the inverse of f.

- **Well-Definedness**: Since $x \neq 1$ for all $x \in T$, the expression $\dfrac{3x-2}{x-1}$ is defined. If $x_1 = x_2$, then clearly
$$\frac{3x_1 - 2}{x_1 - 1} = \frac{3x_2 - 2}{x_2 - 1},$$
so $g(x_1) = g(x_2)$. To check that $g(x) \in S$, we verify that $g(x) \neq 3$ for all $x \in T$:
$$g(x) = 3 \iff \frac{3x-2}{x-1} = 3 \iff 3x - 2 = 3x - 3 \iff -2 = -3,$$
a contradiction. Hence $g(x) \in S$ for all $x \in T$, and g is well-defined.

- **Computation of $g \circ f$**: Let $x \in S$. Then
$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g\left(\frac{x-2}{x-3}\right) \\ &= \frac{3\left(\frac{x-2}{x-3}\right) - 2}{\left(\frac{x-2}{x-3}\right) - 1} \\ &= \frac{3(x-2) - 2(x-3)}{(x-2) - (x-3)} \\ &= \frac{x}{1} \\ &= x.\end{aligned}$$
Therefore $g \circ f = \mathrm{Id}_S$.

- **Computation of $f \circ g$**: Let $x \in T$. Then

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f\left(\frac{3x-2}{x-1}\right) \\ &= \frac{\left(\frac{3x-2}{x-1}\right) - 2}{\left(\frac{3x-2}{x-1}\right) - 3} \\ &= \frac{(3x-2) - 2(x-1)}{(3x-2) - 3(x-1)} \\ &= \frac{x}{1} \\ &= x.\end{aligned}$$

  Therefore $f \circ g = \mathrm{Id}_T$.

Since $g = f^{-1}$, we conclude that f is invertible, and hence f is a bijection. □

Exercise 17.1.5. Prove that the following functions are bijections by explicitly constructing an inverse function and proving that it is in the inverse function.

(a) $f : \mathbb{R} \setminus \{-2\} \to \mathbb{R} \setminus \{4\}$ such that $f(x) = \frac{4x+5}{x+2}$.

(b) $g : \mathbb{R}^2 \to \mathbb{R}^2$ such that $g(x, y) = (3x + 4y, 2x + y)$.

Exercise 17.1.6. Let A and B be nonempty sets and $f : A \to B$ be a function. Prove that f has a left inverse if and only if f is injective.

18. October 6

18.1. Homogeneous Relations

Now that we've explored functions as a special type of binary relation, we turn our attention to relations where the domain and codomain are the same set. These are called *homogeneous relations*. Such relations are especially important because many of the most familiar mathematical structures, such as orderings and equivalence relations, are defined in terms of simple properties like reflexivity, symmetry, and transitivity. By studying these properties in isolation, we will see how they combine to give rise to these richer and more structured types of relations.

Definition. Let R be a binary relation on a set S. Then R is called:

- *Reflexive* iff $\forall x \in S, (x, x) \in R$ (i.e., every element is related to itself).
- *Irreflexive* iff $\forall x \in S, (x, x) \notin R$ (i.e., no element is related to itself).
- *Symmetric* iff $\forall x, y \in S, ((x, y) \in R \to (y, x) \in R)$.
- *Antisymmetric* iff $\forall x, y \in S, (((x, y) \in R \land (y, x) \in R) \to x = y)$.
- *Transitive* iff $\forall x, y, z \in S, (((x, y) \in R \land (y, z) \in R) \to (x, z) \in R)$.
- *Total* iff $\forall x, y \in S, (x \neq y \to ((x, y) \in R \lor (y, x) \in R))$ (i.e., any two distinct elements are comparable).

Notes.

- **Irreflexivity vs. Reflexivity:** Irreflexivity is not the opposite of reflexivity. Both are universal statements. The only time a relation can be both reflexive and irreflexive is when the set S is empty. However, many relations are neither reflexive nor irreflexive.
- **Symmetry vs. Antisymmetry:** Antisymmetry is not the opposite of symmetry. These properties are not logical negations of one another. The only relations that are both symmetric and antisymmetric are subsets of the equality relation. However, many relations are neither symmetric nor antisymmetric.
- **Contrapositive in Antisymmetry:** In some cases, the hypothesis of antisymmetry (both (x, y) and (y, x) being in R) may never hold. In such cases, it is useful

to consider the contrapositive: if $x \neq y$, then either $(x, y) \notin R$ or $(y, x) \notin R$.

Below we examine several common binary relations and determine whether they satisfy these properties.

Set	Relation	Refl.	Irrefl.	Symm.	Antisymm.	Trans.	Total
$\mathbb{R}$	$<$	No	Yes	No	Yes	Yes	Yes
$\mathbb{R}$	$\leq$	Yes	No	No	Yes	Yes	Yes
$\mathbb{R}$	$x \sim y$ iff $x - y \in \mathbb{Z}$	Yes	No	Yes	No	Yes	No
$\mathcal{P}(S)$	$\subseteq$	Yes	No	No	Yes	Yes	No
$S \neq \varnothing$	$=$	Yes	No	Yes	Yes	Yes	No
$\mathbb{Z}$	$\mid$	Yes	No	No	No	Yes	No
[2]	$R = \{(1, 1), (1, 2)\}$	No	No	No	Yes	Yes	Yes

Exercise 18.1.1. Let $S = [6]$.

(a) If possible, construct a relation R on S that is reflexive and symmetric but not transitive. If not possible, write "Not Possible." Briefly explain your reasoning.

(b) If possible, construct a relation R' on S that is symmetric and transitive but not reflexive. If not possible, write "Not Possible." Briefly explain your reasoning.

Exercise 18.1.2. Let $S = [5]$ and define $R \subseteq S^2$ as follows:

$$R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3), (4, 4), (5, 5)\}$$

Determine whether or not R satisfies the following properties. Provide brief justifications.

(a) Reflexivity

(b) Irreflexivity

(c) Symmetry

(d) Antisymmetry

(e) Transitivity

(f) Totality

At this point, we turn our attention to two special types of relations on sets—equivalence relations and order relations.

18.1.1. Equivalence Relations

In previous math courses, you may have encountered situations where objects that are distinct in one context are considered equivalent in another. For example, angles such as $0°$, $360°$, and $720°$ differ numerically, but they represent the same direction when drawn on a circle. Similarly, in geometry, two similar triangles are often treated as equivalent because they share the same angles, even if their side lengths differ. These examples highlight how, depending on the context, certain differences are ignored and objects are regarded as "essentially the same."

Definition. A relation R on a set S is called an *equivalence relation* if and only if R is reflexive, symmetric, and transitive.

Equivalence relations arise in many mathematical contexts. Here are some common examples:

1. Equality on any set.
2. Similarity of triangles: $\triangle A \sim \triangle B$ if and only if they have the same interior angles.
3. Rounding real numbers to the nearest integer: two real numbers x and y are equivalent if they round to the same nearest integer.

$$x \sim y \iff \exists n \in \mathbb{Z} \text{ such that } x, y \in \left[n - \frac{1}{2}, n + \frac{1}{2}\right).$$

4. Logical equivalence in propositional logic.
5. Parity on $\mathbb{Z}$: two integers a and b are equivalent if and only if they have the same parity (i.e., both are even or both are odd).

One of the most commonly used equivalence relations in mathematics and computer science is *congruence modulo* m on the integers. We now give the formal definition of this relation.

Definition. Let $m \in \mathbb{Z}^+$. For any $a, b \in \mathbb{Z}$, we say that a *is congruent to* b *modulo* m, denoted $a \equiv b \pmod{m}$, if and only if $m \mid (a - b)$.

Theorem 18.1.3. *For any $m \in \mathbb{Z}^+$, congruence modulo m is an equivalence relation on $\mathbb{Z}$.*

Proof. Let $m \in \mathbb{Z}^+$. We will show that congruence modulo m is reflexive, symmetric, and transitive.

- (Reflexivity): Let $a \in \mathbb{Z}$. We want to show that $a \equiv a \pmod{m}$.

  Since $a - a = 0 = m \cdot 0$, we have $m \mid (a - a)$, and thus $a \equiv a \pmod{m}$, as desired.

- (Symmetry): Let $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{m}$. We want to show that $b \equiv a \pmod{m}$.

  Since $a \equiv b \pmod{m}$, we have $m \mid (a - b)$, meaning $a - b = mk$ for some $k \in \mathbb{Z}$. It follows that $b - a = m(-k)$, which implies $m \mid (b - a)$ because $-k \in \mathbb{Z}$. Therefore, $b \equiv a \pmod{m}$, as desired.

- (Transitivity): Let $a, b, c \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. We want to show that $a \equiv c \pmod{m}$.

  From $a \equiv b \pmod{m}$, we have $a - b = mk$ for some $k \in \mathbb{Z}$. From $b \equiv c \pmod{m}$, we have $b - c = m\ell$ for some $\ell \in \mathbb{Z}$. Summing these equations gives:

  $$a - c = (a - b) + (b - c) = mk + m\ell = m(k + \ell)$$

  Thus $m \mid (a - c)$, and therefore $a \equiv c \pmod{m}$.

Since congruence modulo m is reflexive, symmetric, and transitive, it follows that it is an equivalence relation on $\mathbb{Z}$. □

Congruence modulo m is often used to describe sets with cyclic structure. Even if you have not encountered the terminology before, you have almost certainly used the idea. Here are some familiar examples:

- **Days of the week:** The days repeat every 7 days. For instance, if 25 days ago was a Monday, then today is a Friday because $25 \equiv 4 \pmod{7}$, meaning it is 4 days past a Monday.
- **Clocks:** Converting between 24-hour and 12-hour time uses congruence modulo 12. For example, $16 : 00$ satisfies $16 \equiv 4 \pmod{12}$, so the time is 4:00 PM in 12-hour notation.
- **Parity:** Odd and even integers can be described using congruence modulo 2. We have $a \equiv b \pmod{2}$ if and only if $a - b$ is even, meaning a and b have the same parity.
- **Angles:** Angles measured in degrees can be treated using congruence modulo 360. For example, $375 \equiv 15 \pmod{360}$, so 375° and 15° are coterminal.

To get a handle on this equivalence relation, let's consider the case of $m = 3$. A few quick observations about which integers are or are not congruent to one another:

- $26 \equiv 2 \pmod{3}$ because $3 \mid (26 - 2)$
- $0 \equiv 3 \pmod{3}$ because $3 \mid (0 - 3)$
- $7 \not\equiv 21 \pmod{3}$ because $3 \nmid (7 - 21)$

19. October 8

19.1. Homogeneous Relations

19.1.1. Equivalence Classes

The purpose of defining an equivalence relation is to identify the underlying structure of equality in order to generalize it to other contexts. Since an equivalence relation defines a new notion of two elements being *the same*, it is useful to discuss sets of elements that are all considered *the same* as each other. Below, we make precise this idea of being *the same*.

Definition. Let R be an equivalence relation on a set S. For every $x \in S$, we define the *equivalence class of x under R*, denoted $[x]_R$, by

$$[x]_R = \{y \in S \mid (x, y) \in R\}$$

That is, $[x]_R$ is the collection of all elements that are equivalent to x, under the specific notion of equivalence being discussed.

The set of all equivalence classes is referred to as the *quotient set*, denoted S/R, read "S modulo R". That is

$$S/R = \{[x]_R \mid x \in S\}$$

Because congruence modulo m is a commonly used equivalence relation, the set of equivalence classes (commonly called *congruence classes* in this context) has a special notation.

Special Notation

For $m \in \mathbb{Z}^+$, the set S/R of congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$. This set contains m equivalence classes:

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

We often write integers as if they were their equivalence classes, viewing $\mathbb{Z}/m\mathbb{Z}$ as a cycle of m distinct classes.

Example 19.1.1. Consider congruence modulo 3 on $\mathbb{Z}$. What do the equivalence classes look like?

$$[0]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-0)\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, (x = 3k)\} = \{\ldots, -3, 0, 3, 6, 9, 12, \ldots\}$$
$$[1]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-1)\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, (x = 3k+1)\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-2)\} = \{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, (x = 3k+2)\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$
$$[3]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-3)\} = \{x \in \mathbb{Z} \mid 3 \mid x\} = [0]_3$$
$$[4]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-4)\} = \{x \in \mathbb{Z} \mid 3 \mid (x-1)\} = [1]_3$$
$$[5]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x-5)\} = \{x \in \mathbb{Z} \mid 3 \mid (x-2)\} = [2]_3$$

We should also look at some equivalence classes for negative integers:

$$[-1]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x+1)\} = \{x \in \mathbb{Z} \mid 3 \mid (x-2)\} = [2]_3$$
$$[-2]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x+2)\} = \{x \in \mathbb{Z} \mid 3 \mid (x-1)\} = [1]_3$$
$$[-3]_3 = \{x \in \mathbb{Z} \mid 3 \mid (x+3)\} = \{x \in \mathbb{Z} \mid 3 \mid x\} = [0]_3$$

Let's make a few observations about these equivalence classes and how they relate to our original set, $\mathbb{Z}$.

- There are 3 distinct equivalence classes: $[0]_3$, $[1]_3$, and $[2]_3$.
- Each equivalence class is an infinite set of integers.
- The union of the equivalence classes gives the entire set: $[0]_3 \cup [1]_3 \cup [2]_3 = \mathbb{Z}$.
- The equivalence classes are pairwise disjoint.
- We have $S/R = \mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$.

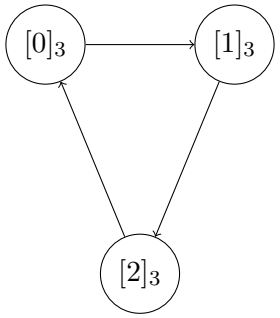


Figure 19.1.: The equivalence classes of $\mathbb{Z}/3\mathbb{Z}$ arranged in a cycle.

Exercise 19.1.2. For each of the following, prove that the given relation is an equivalence relation and describe the different equivalence classes.

(a) Suppose $f : A \to B$ is a function. Define the relation $\sim$ on B by

$$x \sim y \quad \iff \quad \mathrm{PreIm}_f(\{x\}) = \mathrm{PreIm}_f(\{y\})$$

(b) Define $\simeq$ on $\mathbb{Z}$ by

$$x \simeq y \iff |x| = |y|$$

(c) Define $\cong$ on $\mathbb{Z}$ by

$$x \cong y \iff 11 \mid 4x + 7y$$

(d) Define $\doteq$ on $\mathbb{Q} \setminus \{0\}$ by

$$x \doteq y \iff \exists k \in \mathbb{Z},\ \frac{x}{y} = 2^k$$

(e) Define $\approx$ on $\mathbb{Z}$ by

$$x \approx y \iff \cos(x)\cos(y) > 0$$

19.1.2. The Fundamental Theorem of Equivalence Relations

In the previous example of $\mathbb{Z}/3\mathbb{Z}$, the congruence classes modulo 3 formed what we call a *partition* of $\mathbb{Z}$.

Definition. Let S be a set, I be an index set, and $A_i \subseteq S$ for each $i \in I$. Then $\{A_i \mid i \in I\}$ is called a *partition* of S if and only if:

1. For each $i \in I$, $A_i \neq \varnothing$.
2. For each $i, j \in I$, either $A_i = A_j$ or $A_i \cap A_j = \varnothing$.
3. $\bigcup_{i \in I} A_i = S$.

That is, $\{A_i \mid i \in I\}$ is a partition of S if and only if the A_i's divide S into nonempty, non-overlapping pieces.

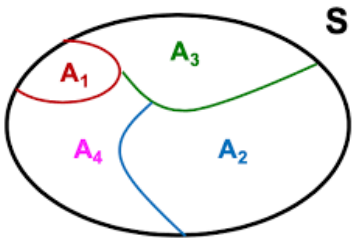


Figure 19.2.: An illustration of a partition of a set.

Returning to Example 19.1.1, we see that $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$ satisfies the three properties of a partition:

1. Each congruence class in $\mathbb{Z}/3\mathbb{Z}$ is a nonempty subset of the integers.

2. Any two congruence classes in $\mathbb{Z}/3\mathbb{Z}$ are either equal to each other or disjoint from each other.
3. The union of the three distinct congruence classes in $\mathbb{Z}/3\mathbb{Z}$ is all of $\mathbb{Z}$.

It is not a coincidence that $\mathbb{Z}/3\mathbb{Z}$ is a partition of $\mathbb{Z}$. In fact, this phenomenon holds for all equivalence relations (and conversely), as the following theorem states.

Theorem 19.1.3 (Fundamental Theorem of Equivalence Relations)**.** *Let S be a nonempty set. Then the following hold:*

1. *If R is an equivalence relation on S, then S/R is a partition of S.*
2. *If $\mathcal{F}$ is a partition of S, then there exists an equivalence relation R on S such that $S/R = \mathcal{F}$.*

Before proving this theorem (or at least one direction of it—we'll leave the other for homework), let's look at a concrete example of the reverse direction. We've already seen how an equivalence relation produces a partition; now we'll see how a partition gives rise to an equivalence relation.

Example 19.1.4. Let $S = [6]$ and $\mathcal{F} = \{\{1\}, \{2, 5, 6\}, \{3, 4\}\}$ be a partition of S. We want to find an equivalence relation R on S such that $S/R = \mathcal{F}$.

Define $R \subseteq S \times S$ by declaring two elements related if they belong to the same block of the partition. Explicitly,

$$R = \{(1,1), (2,2), (2,5), (2,6), (3,3), (3,4), (4,3), (4,4), (5,2), (5,5), (5,6), (6,2), (6,5), (6,6)\}.$$

We can manually check that R is an equivalence relation on S.

- (R): Is $(x, x) \in R$ for each $x \in [6]$? ✓
- (S): For each $(x, y) \in R$, is $(y, x) \in R$ also? ✓
- (T): For each $(x, y), (y, z) \in R$, is $(x, z) \in R$ also? ✓

So, R is an equivalence relation on S, and S/R has 3 distinct equivalence classes.

$$\begin{aligned} [1]_R &= \{1\}, \\ [2]_R = [5]_R = [6]_R &= \{2, 5, 6\}, \\ [3]_R = [4]_R &= \{3, 4\}. \end{aligned}$$

Thus, the set of equivalence classes is exactly the given partition:

$$S/R = \{[1]_R, [2]_R, [3]_R\} = \mathcal{F}.$$

We now proceed to prove the theorem.

Proof.

1. Homework
2. Let $\mathcal{F} = \{S_i\}_{i \in I}$ be a partition of S. Define a relation R on S by

$$R = \{(x, y) \in S \mid \exists i \in I, (x \in S_i \wedge y \in S_i)\}.$$

We want to show that R is an equivalence relation and that $S/R = \mathcal{F}$. First, we check reflexivity, symmetry, and transitivity.

- (R): Let $x \in S$. Since $\mathcal{F}$ is a partition of S, we have $\bigcup_{i \in I} S_i = S$. Hence, $x \in S_i$ for some $i \in I$, by the definition of an indexed union. Fix such an i. Then $x \in S_i$ implies that $(x, x) \in R$, as desired.
- (S): Let $x, y \in S$ such that $(x, y) \in R$. Then, by definition of R, we have $x \in S_i \wedge y \in S_i$ for some $i \in I$. Fix such an i. Since conjunction is commutative, this implies $y \in S_i \wedge x \in S_i$. Hence $(y, x) \in R$, as desired.
- (T): Let $x, y, z \in S$ such that $(x, y), (y, z) \in R$. Then, by definition of R, there exists $i \in I$ such that $x \in S_i \wedge y \in S_i$, and there exists $j \in I$ such that $y \in S_j \wedge z \in S_j$. Fix such i and j. Since $\mathcal{F}$ is a partition of S and $y \in S_i$ and $y \in S_j$, it must be the case that $S_i = S_j$ (the pieces of a partition are either equal or disjoint). Thus, $x \in S_i \wedge z \in S_i$, implying that $(x, z) \in R$, as desired.

Therefore, R is an equivalence relation on S. It remains to show $S/R = \mathcal{F}$. We proceed by double containment.

- ($\subseteq$): Let $A \in S/R$. Then, by definition, $A = [x]_R$ for some $x \in S$. Since $\mathcal{F}$ is a partition, x belongs to exactly one block $S_i \in \mathcal{F}$. Then

$$A = [x]_R = \{y \in S \mid y \in S_i\} = S_i.$$

Therefore, $A \in \mathcal{F}$, as desired.

- ($\supseteq$): Let $S_i \in \mathcal{F}$. Since $\mathcal{F}$ is a partition, $S_i \neq \varnothing$. Fix $x \in S_i$. By uniqueness of the partition blocks, S_i is the only block of $\mathcal{F}$ containing x. Thus

$$[x]_R = \{y \in S \mid y \in S_i\} = S_i,$$

so $S_i \in S/R$.

By double containment, we conclude that $S/R = \mathcal{F}$.

□

The utility of equivalence relations extends beyond classification: they provide the foundation for many mathematical structures, such as quotient groups in group theory and partitions in topology. Recognizing and applying these concepts will deepen your understanding of advanced mathematics and the connections between its different areas.

19.1.3. (Optional) Formal Constructions of $\mathbb{Z}$ and $\mathbb{Q}$

Previously, we discussed how to construct the natural numbers (or a structure having the same properties as $\mathbb{N}$) from the axioms of set theory. Now, with the power of equivalence relations, we can formally construct the integers and rational numbers. This approach allows us to define addition and multiplication on these sets in a way that is consistent with the operations we already take for granted.

Constructing the Integers

The natural numbers do not include additive inverses, so subtraction is not always possible within $\mathbb{N}$. To address this, we will construct the integers by introducing formal differences. The guiding idea is that an ordered pair $(a, b) \in \mathbb{N}^2$ represents the "formal difference" $a - b$.

However, we must be careful: since subtraction is not defined in $\mathbb{N}$, we cannot simply say $(a, b) = (c, d)$ whenever $a - b = c - d$. Instead, we use the following property of $\mathbb{N}$:

$$\text{Cancellation Law: If } k + m = n + m \text{ then } k = n.$$

This motivates the following definition.

Theorem 19.1.5. *Define a relation $\sim$ on $\mathbb{N}^2$ by*

$$(a, b) \sim (c, d) \quad \iff \quad a + d = b + c.$$

Then $\sim$ is an equivalence relation on $\mathbb{N}^2$.

Proof. To be completed in recitation. □

The quotient set $\mathbb{N}^2/\!\sim$ will represent our set of integers. Each equivalence class $[(a, b)]_\sim$ under this relation represents the integer corresponding to the formal difference $a - b$. For example,

$$[(3, 1)]_\sim \quad \text{represents } 3 - 1 = 2, \qquad [(2, 5)]_\sim \quad \text{represents } 2 - 5 = -3.$$

We now want to define addition and multiplication on $\mathbb{N}^2/\!\sim$ in a way that matches how these operations behave in $\mathbb{Z}$. For instance, we want

$$2 + (-3) \quad \text{to correspond to} \quad [(3, 1)]_\sim + [(2, 5)]_\sim,$$

and the result should represent -1. Similarly,

$$2 \cdot (-3) \quad \text{should correspond to} \quad [(3, 1)]_\sim \cdot [(2, 5)]_\sim,$$

and the result should represent -6.

Motivated by these examples, we define our operations as follows.

Definition. We define addition on $\mathbb{N}^2/\sim$ by

$$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c, b+d)]_\sim,$$

and multiplication by

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd,\, ad+bc)]_\sim.$$

Recall that equivalence classes can be represented by multiple ordered pairs. For example,

$$[(2,0)]_\sim = [(3,1)]_\sim = [(4,2)]_\sim = \cdots$$

Our definitions above used specific representatives, so we must verify that the operations are *well-defined*. That is, the result does not depend on the choice of representative.

Theorem 19.1.6. *The operations defined above are well-defined. In particular, if* $(a,b) \sim (a',b')$ *and* $(c,d) \sim (c',d')$*, then:*

1. $(a+c, b+d) \sim (a'+c', b'+d')$,
2. $(ac+bd, ad+bc) \sim (a'c'+b'd',\, a'd'+b'c')$.

Equivalently, if $[(a,b)]_\sim = [(a',b')]_\sim$ and $[(c,d)]_\sim = [(c',d')]_\sim$, then

$$[(a,b)]_\sim + [(c,d)]_\sim = [(a',b')]_\sim + [(c',d')]_\sim \quad \text{and} \quad [(a,b)]_\sim \cdot [(c,d)]_\sim = [(a',b')]_\sim \cdot [(c',d')]_\sim.$$

Before proving this theorem, let's explore an example.

Example 19.1.7. Suppose we want to represent the sum $2+3$. Using our definition of addition, we could write:

$$[(2,0)]_\sim + [(3,0)]_\sim = [(2+3, 0+0)]_\sim = [(5,0)]_\sim,$$

which represents the number 5, as expected. But we could also represent 2 and 3 differently:

$$[(3,1)]_\sim + [(10,7)]_\sim = [(3+10, 1+7)]_\sim = [(13,8)]_\sim,$$

which also represents the number 5. Our theorem states that no matter which representatives of 2 and 3 we choose, the sum will always represent 5.

Similarly, for the product $2 \cdot 3 = 6$:

$$[(2,0)]_\sim \cdot [(3,0)]_\sim = [(6+0, 0+0)]_\sim = [(6,0)]_\sim$$

represents 6, while

$$[(3,1)]_\sim \cdot [(10,7)]_\sim = [(30+7,\ 21+10)]_\sim = [(37,31)]_\sim$$

also represents 6. This illustrates that multiplication, too, should be independent of the choice of representatives.

We now proceed to prove the theorem.

Proof. Let $(a,b),(a',b'),(c,d),(c',d') \in \mathbb{N}^2$ such that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$.

1. We want to show that $(a+c, b+d) \sim (a'+c', b'+d')$.

   By assumption,
   $$a+b' = b+a' \quad \text{and} \quad c+d' = d+c'.$$
   Adding these two equalities gives
   $$a+c+b'+d' = b+d+a'+c',$$
   which shows $(a+c, b+d) \sim (a'+c', b'+d')$.

   Thus, addition is well-defined on $\mathbb{Z}$.

2. We want to show that $(ac+bd, ad+bc) \sim (a'c'+b'd', a'd'+b'c')$.

   As in the previous case, from our assumptions we have
   $$a+b' = b+a' \quad \text{and} \quad c+d' = d+c'.$$

   Multiplying the first equality by c and d, and the second by a' and b', we obtain
   $$c(a+b') = c(b+a'), \quad d(a+b') = d(b+a'),$$
   and
   $$a'(c+d') = a'(d+c'), \quad b'(c+d') = b'(d+c').$$

   Adding these four equalities together yields

   $$c(a+b')+d(a+b')+a'(c+d')+b'(c+d') = c(b+a')+d(b+a')+a'(d+c')+b'(d+c').$$

   Expanding both sides gives

   $$ac+bd+a'd'+b'c'+b'c+a'd+a'c+b'd = ad+bc+a'c'+b'd'+a'c+b'd+a'd+b'c.$$

   Cancelling the common terms on both sides, we are left with
   $$ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'.$$

This is exactly the condition that

$$(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c'),$$

as desired.

Therefore multiplication is well-defined on $\mathbb{Z}$.

□

Remark. With these definitions of addition and multiplication, the set $\mathbb{Z}$ inherits many of the familiar properties we expect integers to satisfy: associativity, commutativity, distributivity, and the existence of additive identities and inverses. These follow from the corresponding properties in $\mathbb{N}$, but require careful checking in this new framework.

Exercise 19.1.8. Prove the following properties of $\mathbb{Z}$ using the equivalence class construction:

(a) Show that the element $[(a, a)]_\sim$ serves as the additive identity in $\mathbb{Z}$.

(b) Prove that for each $[(a, b)]_\sim \in \mathbb{Z}$, the element $[(b, a)]_\sim$ is its additive inverse.

(c) Show that $[(1, 0)]_\sim$ is the multiplicative identity in $\mathbb{Z}$.

(d) Verify that addition and multiplication in $\mathbb{Z}$ are commutative.

(e) Prove that multiplication distributes over addition.

(f) Prove that $\mathbb{Z}$ has no zero divisors. That is, if $[(a, b)]_\sim \cdot [(c, d)]_\sim = [(0, 0)]_\sim$ then $[(a, b)]_\sim = [(0, 0)]_\sim$ or $[(c, d)]_\sim = [(0, 0)]_\sim$.

Constructing the Rationals

Now that we have a formal definition of the integers, we can follow a similar path to construct the rational numbers. The integers do not always include multiplicative inverses, so we cannot define division in $\mathbb{Z}$. Let $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. We will define a relation on $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$ that matches how we informally think of equality of fractions, $\frac{a}{b} = \frac{c}{d}$, but avoids direct use of division.

We rely on the fact that the integers have no zero divisors:

$$a \cdot b = 0 \iff a = 0 \text{ or } b = 0.$$

This motivates our definition.

Theorem 19.1.9. *Define a relation $\simeq$ on $\mathbb{Z} \times \mathbb{Z}^*$ by*

$$(a, b) \simeq (c, d) \quad \iff \quad ad = bc.$$

Then $\simeq$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.

Proof. Homework 6. □

The quotient set $\mathbb{Z} \times \mathbb{Z}^*/\simeq$ will represent our set of rational numbers. Each equivalence class $[(a, b)]_\simeq$ under this relation represents the rational number corresponding to the quotient $\frac{a}{b}$. For example,

$$[(-1, 2)]_\simeq \quad \text{represents } -\frac{1}{2}, \qquad [(8, 4)]_\simeq \quad \text{represents } \frac{8}{4} = 2.$$

We now define addition and multiplication on $\mathbb{Z} \times \mathbb{Z}^*/\simeq$ in a way consistent with how these operations behave in $\mathbb{Q}$. For instance, we want

$$-\frac{1}{2} + 2 \quad \text{to correspond to} \quad [(-1, 2)]_\simeq + [(8, 4)]_\simeq,$$

and the result should represent $\frac{3}{2}$. Similarly,

$$-\frac{1}{2} \cdot 2 \quad \text{should correspond to} \quad [(-1, 2)]_\simeq \cdot [(8, 4)]_\simeq,$$

and the result should represent -1.

Motivated by these examples, we define our operations as follows.

Definition. We define addition on $\mathbb{Z} \times \mathbb{Z}^*/\simeq$ by

$$[(a, b)]_\simeq + [(c, d)]_\simeq = [(ad + bc,\ bd)]_\simeq,$$

and multiplication by

$$[(a, b)]_\simeq \cdot [(c, d)]_\simeq = [(ac,\ bd)]_\simeq.$$

Let's revisit our previous example.

Example 19.1.10. Suppose we want to take the sum and product of $-\frac{1}{2}$ and 2. Using the representatives from before and our formal definition of addition and multiplication,

we have

$$[(-1,2)]_\simeq + [(8,4)]_\simeq = [(-4+16,8)]_\simeq = [(12,8)]_\simeq = \frac{12}{8} = \frac{3}{2},$$
$$[(-1,2)]_\simeq \cdot [(8,4)]_\simeq = [(-8,8)]_\simeq = \frac{-8}{8} = -1.$$

If instead we had chosen $[(2,-4)]_\simeq$ to represent $-\frac{1}{2}$ and $[(2,1)]_\simeq$ to represent 2, we should still get the same answers:

$$[(2,-4)]_\simeq + [(2,1)]_\simeq = [(2-8,-4)]_\simeq = [(-6,-4)]_\simeq = \frac{-6}{-4} = \frac{3}{2},$$
$$[(2,-4)]_\simeq \cdot [(2,1)]_\simeq = [(4,-4)]_\simeq = \frac{4}{-4} = -1.$$

An example alone is not a proof, but it does indicate that these operations are probably well-defined, as this theorem confirms.

Theorem 19.1.11. *The operations defined above are well-defined. In particular, if* $(a,b) \simeq (a',b')$ *and* $(c,d) \simeq (c',d')$*, then*

1. $(ad+bc, bd) \simeq (a'd'+b'c', b'd')$,
2. $(ac, bd) \simeq (a'c', b'd')$.

The proof of this theorem is similar to the analogous theorem for the integers. We leave this as an exercise.

Exercise 19.1.12. Prove the previous theorem.

Be sure to use only properties of the integers when working with these expressions.

We now have formal constructions of the integers and rationals, together with precise definitions of their arithmetic operations. Along the way we proved many basic properties that are often taken for granted. This illustrates the broader mathematical principle that rigorous proofs and deeper theory require precise, formal definitions from the ground up.

20. October 10

20.1. Homogeneous Relations

20.1.1. Order Relations

An **order relation** is a relation that ranks elements of a set against one another. Order relations generalize the familiar concepts of $<$, $\leq$, and $\subseteq$.

Definition.

- A relation R on a set S is called a *partial order* if and only if R is reflexive, antisymmetric, and transitive.
- If R is a partial order on S, then (S, R) is called a *partially ordered set* (or *poset*). For example, $(\mathcal{P}(S), \subseteq)$ (for any set S) and $(\mathbb{R}, \leq)$ are posets.
- A relation R is called a *strict partial order* if and only if R is irreflexive, antisymmetric, and transitive. For example, $(\mathcal{P}(S), \subsetneq)$ and $(\mathbb{R}, <)$ are strict partial orders.
- A relation R is called a *total order* (or *linear order*) if and only if it is a partial order in which every pair of elements of S is comparable under R.

As mentioned above, $(\mathcal{P}(S), \subseteq)$ and $(\mathbb{R}, \leq)$ are two of the most common partial orders. The definition of a partial order can thus be viewed as a generalization of these familiar examples.

Let's begin by proving that $\subseteq$ is a partial order on a power set.

Example 20.1.1. Consider the relation $\subseteq$ on $\mathcal{P}(\mathbb{N})$. We will prove that $\subseteq$ is a partial order on $\mathcal{P}(\mathbb{N})$.

Proof. We must show that $\subseteq$ is reflexive, antisymmetric, and transitive.

- (R): Let $X \in \mathcal{P}(\mathbb{N})$. For every $n \in \mathbb{N}$, if $n \in X$, then $n \in X$, trivially. Thus $X \subseteq X$.
- (AS): Let $X, Y \in \mathcal{P}(\mathbb{N})$ such that $X \subseteq Y$ and $Y \subseteq X$. y the definition of set equality, this implies $X = Y$.

- (T): Let $X, Y, Z \in \mathcal{P}(\mathbb{N})$ such that $X \subseteq Y$ and $Y \subseteq Z$. Let $x \in X$. Since $X \subseteq Y$, we have $x \in Y$; and since $Y \subseteq Z$, we have $x \in Z$. Therefore $X \subseteq Z$.

Hence, $(\mathcal{P}(\mathbb{N}), \subseteq)$ is a poset. □

The relation $\subseteq$ also motivates the term *partial* order: it provides a partial ranking of elements in $\mathcal{P}(\mathbb{N})$, but not all elements are comparable. For instance, $\{1\} \not\subseteq \{2\}$ and $\{2\} \not\subseteq \{1\}$. A partial order in which all pairs of elements are comparable is called a *total order* (or *linear order*).

A standard example of a total order is $(\mathbb{R}, \leq)$, and a standard example of a strict total order is $(\mathbb{R}, <)$. By contrast, $\subseteq$ serves as the canonical example of a partial order that is not total.

Example 20.1.2. Consider the set $\mathbb{N}^2$. How can we linearly order the elements of this set?

A natural first attempt might be to define

$$(a, b) \prec (c, d) \quad \text{iff} \quad a < c \text{ and } b < d.$$

However, while this defines a strict partial order, it fails to satisfy totality. For instance, $(1, 2) \not\prec (2, 1)$ and $(2, 1) \not\prec (1, 2)$.

Instead, we can order the elements of $\mathbb{N}^2$ in the same way we alphabetize words: by comparing the first components and, if they are equal, comparing the second components. This is known as the *lexicographic ordering* of $\mathbb{N}^2$.

$$(a, b) \prec (c, d) \quad \text{iff} \quad (a < c) \vee ((a = c) \wedge (b < d)).$$

Claim. The relation $\prec$ is a strict total order on $\mathbb{N}^2$.

Proof. We show that $\prec$ is irreflexive, antisymmetric, transitive, and total.

- (IR): Let $(a, b) \in \mathbb{N}^2$. Since neither $a < a$ nor $b < b$ holds, we have $(a, b) \not\prec (a, b)$.
- (AS): We will prove the contrapositive of the definition of antisymmetry. Let $(a, b), (c, d) \in \mathbb{N}^2$ such that $(a, b) \neq (c, d)$. We want to show $(a, b) \not\prec (c, d)$ or $(c, d) \not\prec (a, b)$.

  Since $(a, b) \neq (c, d)$, either $a \neq c$ or $b \neq d$. We consider the cases of $a = c$ and $a \neq c$.

  - Case 1: $a \neq c$. Without loss of generality, we may assume that $a < c$. Then $(c, d) \not\prec (a, b)$ since $c \not< a$.
  - Case 2: $a = c$. Since $(a, b) \neq (c, d)$ and $a = c$, it must be the case that $b \neq d$. Without loss of generality, we may assume that $b < d$. Then $(c, d) \not\prec (a, b)$ since $c = a$ but $d \not< b$.

Since these are the only two cases, we conclude that $\prec$ is antisymmetric.

- (TR): Let $(a,b),(c,d),(e,f) \in \mathbb{N}^2$ such that $(a,b) \prec (c,d)$ and $(c,d) \prec (e,f)$. We must show that $(a,b) \prec (e,f)$.

  From $(a,b) \prec (c,d)$, we have $a < c$ or $(a = c \wedge b < d)$; from $(c,d) \prec (e,f)$, we have $c < e$ or $(c = e \wedge d < f)$. Consider cases:

  - Case 1: $a < e$. Then $(a,b) \prec (e,f)$ by definition.
  - Case 2: $a = e$. Then it must be the case that $a = c = e$. Since $(a,b) \prec (c,d)$ and $a = c$, we have $b < d$. Similarly, since $(c,d) \prec (e,f)$ and $c = e$, we have $d < f$. Therefore, since $b < d$ and $d < f$, we have $b < f$. Thus, $(a,b) \prec (e,f)$, as desired.

  Therefore $\prec$ is transitive.

- (TO): Let $(a,b),(c,d) \in \mathbb{N}^2$ with $(a,b) \neq (c,d)$. Then either $a \neq c$ or $b \neq d$.

  - If $a \neq c$, then either $a < c$ or $c < a$. In the first case $(a,b) \prec (c,d)$, and in the second $(c,d) \prec (a,b)$.
  - If $a = c$ and $b \neq d$, then either $b < d$ or $d < b$. In the first case $(a,b) \prec (c,d)$, and in the second $(c,d) \prec (a,b)$.

  Hence every pair is comparable, so $\prec$ is total.

Therefore, $(\mathbb{N}^2, \prec)$ is a strict total order. □

Exercise 20.1.3. Define a relation $\preceq$ on $\mathbb{N}$ by

$$m \preceq n \quad \text{iff} \quad m \mid n.$$

(a) Prove that $\preceq$ is a partial order on $\mathbb{N}$.

(b) Prove that $\preceq$ is not a total order on $\mathbb{N}$.

(c) An element $n \in \mathbb{N}$ is called a *minimal element* if there is no $m \in \mathbb{N}$ such that $m \preceq n$, other than n itself. Find all minimal elements of $\mathbb{N}$ under this ordering.

(d) An element $n \in \mathbb{N}$ is called a *maximal element* if there is no $m \in \mathbb{N}$ such that $n \preceq m$, other than n itself. Find all maximal elements of $\mathbb{N}$ under this ordering.

Exercise 20.1.4. Define a relation $\preceq$ on $\mathbb{Q}^+$ (the set of positive rational numbers) by

$$a \preceq b \quad \text{iff} \quad \exists m \in \mathbb{Z}^+, a = bm$$

Determine whether or not $\preceq$ is a partial order on $\mathbb{Q}^+$. If so, determine whether it is also a total order. If not, identify a property that it fails to satisfy.

Exercise 20.1.5. A relation R on a set U is called *asymmetric* if and only if for all $x, y \in U$, if $(x, y) \in R$ then $(y, x) \notin R$. Prove that a relation R on a set U is asymmetric if and only if R is both anti-symmetric and irreflexive.

20.2. End Exam 2 Material

Part IV.

Cardinality

21. October 20

21.1. Introduction

Informally, the *cardinality* of a set S, denoted $|S|$, is the number of elements in the set. For finite sets, this definition is straightforward. However, for infinite sets, it is not immediately clear how we can define the notion of two infinite sets having the same cardinality. Below are some initial questions we might consider:

(1) How should we compare the sizes of sets?

(2) What does it mean for two sets to have the same size?

(3) Should all infinite sets be considered the same size?

To motivate our exploration of Questions (1) and (2), let's begin with a simpler case.

Simpler Question: How can we determine whether two *finite* sets have the same size?

One possible answer is to count the elements in each set. However, this approach breaks down when the sets are infinite. A more flexible method is to *pair* the elements of the two sets. If we can match each element of set A with exactly one element of set B, with no elements left unmatched in either set, then the two sets must contain the same number of elements.

Example 21.1.1. Let $A = \{w, x, y, z\}$ and $B = \{\heartsuit, \diamondsuit, \clubsuit, \spadesuit\}$.

w	$\leftrightarrow$	$\heartsuit$
x	$\leftrightarrow$	$\diamondsuit$
y	$\leftrightarrow$	$\clubsuit$
z	$\leftrightarrow$	$\spadesuit$

What we are actually doing here is defining a *bijection* $f : A \to B$.

This idea extends naturally to sets of any size and leads to our formal definition of "having the same cardinality."

Definition. Two sets A and B are said to have the *same cardinality*, or to be *equinumerous*, denoted $|A| = |B|$, if and only if there exists a bijection $f : A \to B$.

To better understand this definition, let's look at some examples.

Example 21.1.2. Let $A = \{a, b, c\}$ and $B = \{d\}$. Since A has three elements while B has only one, it is clear that $|A| \neq |B|$. This can also be seen from the definition: any function $f : A \to B$ must map every element of A to d, which makes f non-injective. Therefore, no bijection can exist between A and B.

Example 21.1.3. Let E be the set of even integers. The function $f : \mathbb{Z} \to E$ defined by $f(n) = 2n$ is a bijection. Hence, the set of even integers has the same cardinality as the set of all integers: $|E| = |\mathbb{Z}|$.

Example 21.1.4. Recall from Example 16.1.9 the function $f : \mathbb{Z} \to \mathbb{N}$ given by

$$f(n) = \begin{cases} 2n - 1, & \text{if } n > 0, \\ -2n, & \text{if } n \leq 0. \end{cases}$$

This function is a bijection, showing that $|\mathbb{Z}| = |\mathbb{N}|$. In other words, the integers and natural numbers have the same cardinality.

Example 21.1.5. The function $f : (0, 1) \to (0, 2)$ defined by $f(x) = 2x$ is a bijection. Thus, the number of real numbers in the interval $(0, 1)$ is equal to the number in $(0, 2)$; that is, $|(0, 1)| = |(0, 2)|$.

Example 21.1.6. The function $f : (0, 1) \to \mathbb{R}$, defined by $f(x) = \ln\left(\frac{1-x}{x}\right)$, provides a bijection from $(0, 1)$ to the entire real line. Therefore, $|(0, 1)| = |\mathbb{R}|$: there are just as many real numbers in $(0, 1)$ as there are in all of $\mathbb{R}$.

With these examples in mind, we will next focus on finite sets. Our goal will be to show that this formal definition of cardinality agrees with our intuitive understanding of "counting" elements.

21.2. Finite Sets

We begin by formally defining what it means for a set to be finite or infinite.

Definitions.

- A set X is said to be *finite* iff there exists some $n \in \mathbb{N}$ and a bijection $f : [n] \to X$. In this case, we define the *cardinality* of X to be $|X| = n$.
- A set X is said to be *infinite* iff it is not finite. That is, if no bijection exists between $[n]$ and X for any $n \in \mathbb{N}$.

Let's look at a simple example to see how this definition corresponds with our everyday understanding of counting.

Example 21.2.1. Consider the set

$$A = \{\text{Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}\}.$$

By counting the days, we find that $|A| = 7$. This process of counting, or *enumerating* the elements, can be viewed as constructing a bijection $f : [7] \to A$. For instance, if we list the days from left to right, we define

$$f(1) = \text{Su}, \quad f(2) = \text{Mo}, \quad f(3) = \text{Tu}, \quad f(4) = \text{We}, \quad f(5) = \text{Th}, \quad f(6) = \text{Fr}, \quad f(7) = \text{Sa}.$$

Alternatively, if we list the days in reverse order, we obtain another bijection $g : [7] \to A$ defined by

$$g(1) = \text{Sa}, \quad g(2) = \text{Fr}, \quad g(3) = \text{Th}, \quad g(4) = \text{We}, \quad g(5) = \text{Tu}, \quad g(6) = \text{Mo}, \quad g(7) = \text{Su}.$$

Both functions confirm that A is a finite set with cardinality 7.

While the notation $|X| = n$ suggests that this value of n is unique, we need to establish that rigorously. Specifically, we will show that there cannot be two distinct natural numbers m and n such that $|X| = m$ and $|X| = n$.

Theorem 21.2.2 (Injection Criterion for Finite Sets)**.** *For all $m, n \in \mathbb{N}$, there exists an injection $f : [m] \to [n]$ if and only if $m \leq n$.*

Proof. Let $m, n \in \mathbb{N}$.

($\Leftarrow$): Suppose $m \leq n$. Define $f : [m] \to [n]$ by $f(x) = x$. This function is well-defined since $[m] \subseteq [n]$, and it is clearly injective because distinct elements of $[m]$ have distinct images under f.

($\Rightarrow$): We prove the contrapositive. Assume $m > n$, and let $f : [m] \to [n]$ be any function. For each $i \in [n]$, define

$$A_i = \text{PreIm}_f(\{i\}).$$

Each element of $[m]$ belongs to exactly one of the sets $A_1, A_2, \ldots, A_n$, and different A_i's have no elements in common. Since $m > n$, the pigeonhole principle implies that at least one of these sets, say A_i, contains two distinct elements $m_1 \neq m_2$. Then $f(m_1) = f(m_2) = i$, so f is not injective.

□

This theorem confirms that if a set X is finite, its cardinality is uniquely determined. Thus, the formal definition of finite cardinality agrees perfectly with our usual, intuitive notion of "counting" elements.

Corollary 21.2.3. *If X is a finite set, then there exists a unique $n \in \mathbb{N}$ such that $|X| = n$.*

Proof. Let X be a finite set. Suppose, for contradiction, that there exist distinct $m, n \in \mathbb{N}$ such that $|X| = m$ and $|X| = n$. Then there are bijections $f : [n] \to X$ and $g : [m] \to X$. Without loss of generality, assume $m > n$.

Consider the composition

$$f^{-1} \circ g : [m] \to [n].$$

This map is a bijection, since it is the composition of two bijections. In particular, it is an injection from the larger set $[m]$ into the smaller set $[n]$, contradicting the injection criterion established above.

Therefore, it is impossible for two different values m and n to satisfy $|X| = m = n$. Hence, the value of $n \in \mathbb{N}$ such that $|X| = n$ is unique. □

A few additional corollaries are worth noting.

Corollaries 21.2.4.

1. *For all $n \in \mathbb{N}$, every subset of $[n]$ is finite.*
2. *If $f : A \to B$ is an injection and B is finite, then $|A| \leq |B|$. In particular, if $A \subseteq B$, then $|A| \leq |B|$.*
3. *If $g : A \to B$ is a surjection and A is finite, then $|A| \geq |B|$.*
4. *If A is finite and B is any set, then $|A \cap B| \leq |A|$ and $|A \setminus B| \leq |A|$.*

Next, we mention two additional results concerning finite cardinality. The first pertains to the cardinality of Cartesian products, for which we will provide a formal proof in recitation.

Theorem 21.2.5. *If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.*

Proof. In recitation. □

The second result concerns the cardinality of unions. Before presenting the general theorem for determining $|A \cup B|$, we first need a lemma that addresses the case where the sets are disjoint.

Lemma 21.2.6. *If A and B are finite and disjoint sets, then $|A \cup B| = |A| + |B|$.*

Proof. Let A and B be finite and disjoint sets, and let $|A| = m$ and $|B| = n$. Fix bijections $f : [m] \to A$ and $g : [n] \to B$. Construct a function $h : [m+n] \to A \cup B$ by

$$h(k) = \begin{cases} f(k), & \text{if } 1 \leq k \leq m, \\ g(k-m), & \text{if } m+1 \leq k \leq m+n. \end{cases}$$

We will show that h is a bijection.

- **Injectivity**. Let $k_1, k_2 \in [m+n]$ and suppose $h(k_1) = h(k_2)$.
  - If both $k_1, k_2 \leq m$ or both $k_1, k_2 > m$, then $k_1 = k_2$ since f and g are injective.
  - If $k_1 \leq m$ and $k_2 > m$ (or vice versa), then $h(k_1) \in A$ and $h(k_2) \in B$, and hence
    $$h(k_1) = h(k_2) \in A \cap B$$
    contradicting the assumption that A and B are disjoint.

  Hence h is injective.
- **Surjectivity**: Let $y \in A \cup B$.
  - Case 1: If $y \in A$, then since f is surjective, there exists $k \in [m]$ such that $f(k) = y$. Thus $h(k) = f(k) = y$.
  - Case 2: If $y \in B$, then since g is surjective, there exists $\ell \in [n]$ such that $g(\ell) = y$. Then $h(m+\ell) = g(\ell) = y$.

  Therefore, h is surjective.

Since h is both injective and surjective, it is a bijection. Hence $|A \cup B| = m + n = |A| + |B|$. □

The following theorem is a special case of a more general result we will discuss later in the combinatorics section, known as the *Principle of Inclusion–Exclusion (PIE)*.

Theorem 21.2.7 (PIE version 1)**.** *If A and B are finite sets, then*

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

Proof. Let A and B be finite sets. Observe that $A \cup B = A \cup (B \setminus A)$ and that $A \cap (B \setminus A) = \varnothing$. By Lemma 21.2.6,

$$|A \cup B| = |A| + |B \setminus A|.$$

Furthermore, since $B = (B \setminus A) \cup (B \cap A)$ and the two sets are disjoint, Lemma 21.2.6 also gives

$$|B| = |B \setminus A| + |B \cap A|.$$

Rearranging, we have $|B \setminus A| = |B| - |B \cap A|$. Substituting into the earlier expression yields

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

□

Exercise 21.2.8. Let X and Y be non-empty sets with $|X| = m$ and $|Y| = n$. Prove that the number of functions $f : X \to Y$ is n^m.

Exercise 21.2.9. Define a relation $\cong$ on $\mathcal{P}(\mathbb{Z})$ by

$$A \cong B \quad \text{if and only if} \quad A \triangle B \text{ is finite}$$

(a) Prove that $\cong$ is an equivalence relation on $\mathcal{P}(\mathbb{Z})$.

(b) Describe the elements in $[\varnothing]_{\cong}$. List 3 distinct elements from this set.

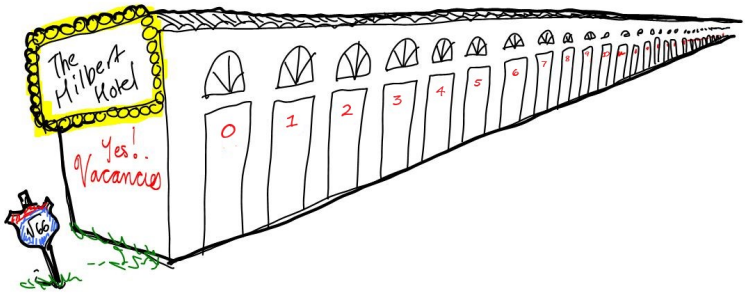
(c) Describe the elements in $[\mathbb{N}]_{\cong}$. List 3 distinct elements from this set.

21.3. Basic Cardinality Comparisons

There are various cardinalities of infinite sets, some of which may appear different in size but actually have the same cardinality. To illustrate this phenomenon, mathematician David Hilbert proposed the famous thought experiment known as *Hilbert's Hotel*.

21.3.1. Hilbert's Hotel

Imagine a hotel with infinitely many rooms, enumerated by the natural numbers:



Suppose all the rooms at Hilbert's Hotel are currently occupied. Let's explore how the hotel can still accommodate additional guests under various scenarios.

1. *Suppose 1 new guest arrives. Can we find them a room?*

   Even though all rooms are occupied, we can still accommodate the new guest. Instruct each current guest in room n to move to room $n+1$. This frees up room 0, which can now be given to the new guest.

   This scenario demonstrates that

   $$|\mathbb{N} \cup \{-1\}| = |\mathbb{N}|.$$

2. *Suppose an infinite number of new guests arrive, enumerated by* $\mathbb{N}$*. Can we find rooms for them?*

   Despite all rooms being occupied and an infinite number of new guests arriving, it is still possible to find rooms for everyone. Move each current guest in room n to room $2n$. This leaves all odd-numbered rooms vacant, which can be assigned to the new guests. Specifically, place new guest m in room $2m+1$.

   This scenario illustrates that

   $$|\{0,1\} \times \mathbb{N}| = |\mathbb{N}|.$$

3. *Suppose an infinite number of buses (enumerated by* $\mathbb{N}$*), each containing an infinite number of guests (also enumerated by* $\mathbb{N}$*), arrive. Can we find rooms for them?*

   This situation is more challenging, since we now have infinitely many groups of infinitely many guests arriving while all rooms are still occupied. Surprisingly, we can still accommodate everyone by utilizing the fact that there are infinitely many prime numbers, and that for distinct primes p and q and integers k and ℓ,

   $$p^k \neq q^\ell.$$

   Here's how we proceed:

- Move the current guest in room n to room 2^{n+1}. Now, only rooms of the form 2^k (for some $k \in \mathbb{Z}^+$) are occupied, leaving all other rooms vacant.
- For bus 0, assign new guest n to room 3^{n+1}.
- For bus 1, assign new guest n to room 5^{n+1}.
- In general, for bus m, assign new guest n to room p_{m+2}^{n+1}, where p_{m+2} denotes the $(m+2)$-nd prime number.
- At this point, every guest has a room, and some rooms remain empty (e.g., rooms 1 and 6). Any room not of the form p^k for some prime p and positive integer k is vacant.

This scenario shows that

$$|\mathbb{N}^2| \leq |\mathbb{N}|,$$

since the room assignment defines an injection rather than a bijection.

Recall: We previously constructed a bijection $f : \mathbb{N}^2 \to \mathbb{N}$, confirming that

$$|\mathbb{N}^2| = |\mathbb{N}|.$$

22. October 24

22.1. Basic Cardinality Comparisons

22.1.1. Countable vs. Uncountable Sets

The main distinction among infinite sets that we will discuss is whether they can be placed in bijective correspondence with $\mathbb{N}$.

Definitions. A set X is called:

- *countably infinite* if there exists a bijection $f : \mathbb{N} \to X$. In this case, we denote its cardinality by $|X| = \aleph_0$.
- *countable* (also called *listable* or *denumerable*) if X is either finite or countably infinite.
- *uncountable* if X is infinite but not countably infinite.

Up to this point, every set we have encountered is countable. To justify the existence of uncountable sets, we first need to understand why $\aleph_0$ represents the "smallest" infinite cardinality.

To do this, we must establish two facts:

1. $\mathbb{N}$ is not finite, and
2. if X is an infinite set, then there exists an injection $f : \mathbb{N} \to X$.

We begin by showing that $\mathbb{N}$ is infinite. Specifically, we will prove that there is no bijection $f : [n] \to \mathbb{N}$ for any $n \in \mathbb{N}$. The key ingredient is the following lemma.

Lemma 22.1.1. *If $A \subseteq \mathbb{N}$ is finite and non-empty, then A has a maximum element.*

Proof. We proceed by induction on $n = |A|$.

- **Base Case**: $n = 1$. Let $A = \{a_1\}$ for some $a_1 \in \mathbb{N}$. Then $a_1 = \max(A)$.
- **Inductive Step**: Let $n \in \mathbb{Z}^+$ and assume any non-empty finite subset of $\mathbb{N}$ with cardinality n has a maximum element. Let $A \subseteq \mathbb{N}$ with $|A| = n+1$, and enumerate

A as:

$$A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}.$$

Consider $B = A \setminus \{a_{n+1}\}$. Then $|B| = n$, so by the inductive hypothesis, B has a maximum element. Let $a_k = \max(B)$ for some $k \in [n]$.

We consider two cases:

- Case 1: $a_k < a_{n+1}$. Then for all $i \in [n+1]$, $a_i \leq a_{n+1}$, so $a_{n+1} = \max(A)$.
- Case 2: $a_k > a_{n+1}$. Then $a_k \geq a_i$ for all $i \in [n+1]$, so $a_k = \max(A)$.

In either case, A has a maximum element.

By the principle of mathematical induction, the lemma follows. □

Theorem 22.1.2. *The set $\mathbb{N}$ is infinite.*

Proof. Assume, for contradiction, that $\mathbb{N}$ is finite. Since $\mathbb{N} \neq \varnothing$, there exists $n \in \mathbb{Z}^+$ and a bijection $f : [n] \to \mathbb{N}$. Then we may write

$$\mathbb{N} = \{f(1), f(2), \ldots, f(n)\}.$$

By Lemma 22.1.1, $\mathbb{N}$ has a maximum element, say $f(k)$. However, $f(k) + 1 \in \mathbb{N}$, contradicting that $f(k)$ is maximal. Hence $\mathbb{N}$ is infinite. □

We have already shown that infinite sets exist, with $\mathbb{N}$ serving as one example. To establish that $\mathbb{N}$ is the "smallest" infinite set, we will show that it can be injected into any infinite set.

Theorem 22.1.3. *For any set A, either A is finite or there exists an injection $f : \mathbb{N} \to A$.*

Note. This proof relies on the *Axiom of Countable Choice* (ACC), which permits making an infinite sequence of choices. We present a simplified overview below.

Proof. Let A be a set. If A is finite, there is nothing to prove. Otherwise, assume A is infinite. We will construct an injection $f : \mathbb{N} \to A$ inductively.

For each $n \in \mathbb{N}$, define $\mathbb{N}_n = \{0, 1, \ldots, n\}$. Choose an arbitrary element $a_0 \in A$ and set $f(0) = a_0$.

Now let $n \in \mathbb{N}$ and assume distinct elements $f(k) \in A$ have been chosen for all $k \leq n$. Since A is infinite, the set $A \setminus \{f(k) \mid k \in \mathbb{N}_n\}$ is nonempty. By the ACC, select an element $a_{n+1} \in A \setminus \{f(k) \mid k \in \mathbb{N}_n\}$ and define $f(n+1) = a_{n+1}$.

Proceeding in this manner defines a function $f : \mathbb{N} \to A$. By construction, $f(n+1) \notin \{f(k) \mid k \in \mathbb{N}_n\}$, so $f(m) \neq f(n)$ whenever $m \neq n$. Hence, f is injective. □

This theorem supports the claim that $\aleph_0$ is the smallest infinite cardinality, since every infinite set has at least this cardinality.

A few immediate corollaries follow from this theorem.

Corollaries 22.1.4.

1. *A set A is infinite if and only if there exists a subset $B \subseteq A$ such that $|B| = \aleph_0$.*
2. *Every subset $A \subseteq \mathbb{N}$ is either finite or has cardinality $|A| = \aleph_0$.*
3. *If $f : A \to \mathbb{N}$ is an injection, then A is countable.*

22.1.2. Linear Ordering of Cardinalities

We can define a linear ordering of cardinalities on the class of all sets based on two important set-theoretic theorems.

Definition. Let S and T be sets. We define:

1. $|S| \leq |T|$ if and only if there exists an injection $f : S \to T$.
2. $|S| \geq |T|$ if and only if there exists a surjection $g : S \to T$.

The definition of $|S| \leq |T|$ is motivated by the Cantor–Bernstein–Schröder theorem, which we will explore below.

Note. If A and B are finite sets and there exist injections $f : A \to B$ and $g : B \to A$, then both f and g must be bijections. In particular, if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Question: Does this result extend to infinite sets?

Answer: Not directly.

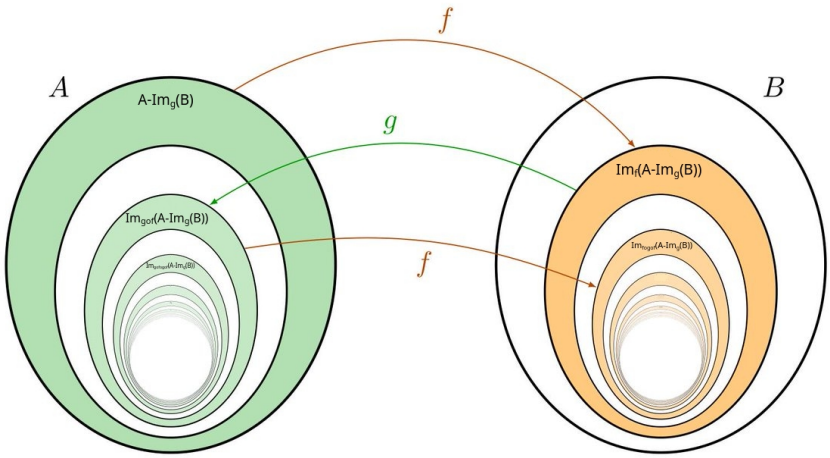
Example 22.1.5. Consider the sets $\mathbb{N}$ and $2\mathbb{N} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N}, x = 2y\}$. Define functions $f : \mathbb{N} \to 2\mathbb{N}$ by $f(n) = 4n$ and $g : 2\mathbb{N} \to \mathbb{N}$ by $g(n) = n$. Both f and g are injections, but neither is a bijection.

Although having injections in both directions does not imply that the injections themselves are bijections, it does imply that *some* bijection must exist between the two sets. This result is known as the Cantor–Bernstein–Schröder Theorem (CBS Theorem).

Theorem 22.1.6 (Cantor–Bernstein–Schröder (CBS) Theorem)**.** *Let A and B be sets. If there exist injections $f : A \to B$ and $g : B \to A$, then there exists a bijection $h : A \to B$.*

Proof. Assume that injections f and g exist. If $\mathrm{Im}_g(B) = A$, then g is a bijection, and we are done. Otherwise, assume $\mathrm{Im}_g(B) \subsetneq A$. Define the set $S \subseteq A$ as

$$S = (A \setminus \mathrm{Im}_g(B)) \cup \left(\bigcup_{n \in \mathbb{Z}^+} \mathrm{Im}_{(g \circ f)^n}(A \setminus \mathrm{Im}_g(B)) \right).$$



Note that $A \setminus S \subseteq \mathrm{Im}_g(B)$. Let g^{-1} denote the inverse of g on the domain $\mathrm{Im}_g(B)$. Define the function $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in S, \\ g^{-1}(x) & \text{if } x \notin S. \end{cases}$$

We claim that h is the desired bijection.

- **Injectivity**: Suppose $h(x) = h(y)$ for some $x, y \in A$. We consider three cases:
  - Case 1: If $x, y \in S$, then $f(x) = f(y)$ implies $x = y$ since f is injective.
  - Case 2: If $x, y \notin S$, then $g^{-1}(x) = g^{-1}(y)$ implies $x = y$ since g^{-1} is injective.
  - Case 3: Assume without loss of generality that $x \in S$ and $y \notin S$. Then $f(x) = g^{-1}(y)$ implies $(g \circ f)(x) = y$. Since $x \in S$, we have $x \in \mathrm{Im}_{(g \circ f)^k}(A \setminus \mathrm{Im}_g(B))$ for some $k \in \mathbb{N}$, and thus $y \in \mathrm{Im}_{(g \circ f)^{k+1}}(A \setminus \mathrm{Im}_g(B)) \subseteq S$, contradicting the assumption that $y \notin S$. Hence, this case cannot occur.

Therefore, h is injective.

- **Surjectivity**: Let $y \in B$ be arbitrary. We consider two cases:
  - Case 1: If $g(y) \notin S$, let $x = g(y)$. Then $h(x) = g^{-1}(x) = y$, as required.
  - Case 2: If $g(y) \in S$, then there exists some $k \in \mathbb{N}$ such that $g(y) = (g \circ f)^k(x)$ for some $x \in A \setminus \mathrm{Im}_g(B)$. Since $k > 0$, we can write $g(y) = (g \circ f)(z) = g(f(z))$ for $z = (g \circ f)^{k-1}(x)$. Thus, $y = f(z)$ and $h(z) = f(z) = y$.

  Therefore, h is surjective.

Since h is both injective and surjective, we conclude that $h : A \to B$ is a bijection, and hence $|A| = |B|$. □

The CBS Theorem justifies our definition of $|A| \leq |B|$ when there exists an injection $f : A \to B$. To establish $|A| = |B|$, it is often easier to show that there exist injections $f : A \to B$ and $g : B \to A$ than to construct an explicit bijection $h : A \to B$. The CBS Theorem guarantees that if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$, providing the antisymmetry needed for a linear ordering.

In practice, the CBS Theorem is used to confirm the existence of **some bijection** $h : A \to B$ without requiring the specific bijection constructed in its proof. To illustrate this, let us revisit Example 22.1.5.

Example 22.1.7. Recall from Example 22.1.5 that we defined injections $f : \mathbb{N} \to 2\mathbb{N}$ by $f(x) = 4x$ and $g : 2\mathbb{N} \to \mathbb{N}$ by $g(x) = x$. Both f and g are injections, but neither is a bijection.

To construct a bijection between $\mathbb{N}$ and $2\mathbb{N}$ using the Cantor–Bernstein–Schröder (CBS) Theorem, we begin by finding the complement of the image of g. Since $\mathrm{Im}_g(2\mathbb{N}) = 2\mathbb{N}$, it follows that $A \setminus \mathrm{Im}_g(B)$ is the set of odd natural numbers. Define

$$\begin{aligned} S &= (A \setminus \mathrm{Im}_g(B)) \cup \mathrm{Im}_{g\circ f}(A \setminus \mathrm{Im}_g(B)) \cup \mathrm{Im}_{g\circ f\circ g\circ f}(A \setminus \mathrm{Im}_g(B)) \cup \cdots \\ &= \{\text{odd naturals}\} \cup \{4 \cdot \text{odd naturals}\} \cup \{16 \cdot \text{odd naturals}\} \cup \cdots \\ &= \{4^m(2n+1) \mid m, n \in \mathbb{N}\}. \end{aligned}$$

The set S consists of numbers of the form $4^m(2n+1)$ for all $m, n \in \mathbb{N}$, capturing every element covered by the iterative application of f and g.

Next, we construct the bijection $h : \mathbb{N} \to 2\mathbb{N}$:

$$h(x) = \begin{cases} 4x & \text{if } x = 4^m(2n+1) \text{ for some } m, n \in \mathbb{N}, \\ x & \text{otherwise.} \end{cases}$$

This mapping sends each element of S to $4x$, pairing it with a unique element of $2\mathbb{N}$, while leaving elements outside of S unchanged.

To visualize this mapping, consider its action on the first few natural numbers:

x	$h(x)$	x	$h(x)$
1	4	7	28
2	2	8	8
3	12	9	36
4	16	10	10
5	20	11	44
6	6	12	48

The table illustrates how h maps elements from $\mathbb{N}$ to $2\mathbb{N}$. You should verify for yourself that this mapping is indeed injective and surjective, confirming h as a bijection.

Note, however, that while the CBS theorem ensures the existence of such a bijection, it does not necessarily yield the simplest one. A much simpler bijection is $j : \mathbb{N} \to 2\mathbb{N}$ defined by $j(x) = 2x$, which is more direct but does not arise from the CBS theorem's construction.

Finally, our definition of $\geq$ is motivated by the following theorem, which tells us that the existence of an injection one way is equivalent to the existence of a surjection the other way. The proof is an elegant application of the Axiom of Choice, which we are assuming throughout.

Theorem 22.1.8 (Partition Principle)**.** *Let A be a nonempty set and B any set. There exists an injection $f : A \to B$ if and only if there exists a surjection $g : B \to A$.*

Proof sketch.

($\Rightarrow$): Suppose $f : A \to B$ is injective. We define a surjection $g : B \to A$ as follows: for $b \in \text{Im}(f)$, set $g(b) = f^{-1}(b)$ (well-defined since f is injective). For $b \notin \text{Im}(f)$, map b to an arbitrary fixed $a_0 \in A$. This covers all $a \in A$ since $g(f(a)) = a$.

($\Leftarrow$): Suppose $f : B \to A$ is surjective. Then for each $a \in A$, $\text{PreIm}_f(\{a\})$ is nonempty. By the Axiom of Choice, there exists a function $g : A \to B$ such that $g(a) \in \text{PreIm}_f(\{a\})$ for all $a \in A$. (i.e., We select one element from $\text{PreIm}_f(\{a\})$ for each $a \in A$.) This function g is injective: if $g(a_1) = g(a_2)$, then applying f gives $a_1 = f(g(a_1)) = f(g(a_2)) = a_2$.

□

Exercise 22.1.9. This problem explores the existence of bijections between the open interval $(0, 1)$ and the closed interval $[0, 1]$.

Consider the inclusion map $f : (0, 1) \to [0, 1]$ defined by $f(x) = x$ and the function $g : [0, 1] \to (0, 1)$ defined by $g(x) = \frac{2x+1}{4}$.

(a) Briefly justify that f and g are injections, verifying the hypothesis of the CBS Theorem.

(b) The CBS Theorem implies that a bijection $h : (0, 1) \to [0, 1]$ exists. Give an explicit formula for the bijection h constructed by the proof of the theorem using these specific functions f and g.

(c) Find another bijection $j : (0, 1) \to [0, 1]$ (or vice versa) without using the CBS Theorem.

Exercise 22.1.10. Let $S = \{n \in \mathbb{Z} \mid n \not\equiv 0 \pmod 7\}$. Use the CBS Theorem to show that there exists a bijection between S and $\mathbb{N}$.

23. October 27

23.1. Countable Sets

Recall that a countably infinite set is a set S that has the same cardinality as $\mathbb{N}$. This represents the smallest size of an infinite set, making it a natural starting point for exploring results about the sizes of infinite sets, which often defy intuition.

For instance, we have already shown that there exists a bijection $f : \mathbb{N} \to 2\mathbb{N}$. This implies that $|2\mathbb{N}| = |\mathbb{N}|$, even though $2\mathbb{N} \subsetneq \mathbb{N}$. In other words, there are just as many natural numbers as there are even natural numbers.

We have also previously encountered bijections $g : \mathbb{N} \to \mathbb{Z}$ and $h : \mathbb{N} \to \mathbb{N}^2$. Thus, we can conclude that

$$|2\mathbb{N}| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{N}^2|.$$

Next, we will prove some important results about countable sets, beginning with a classic example. We will present two different proofs of this result: the traditional "snaking proof" and an alternative argument using the Cantor–Bernstein–Schröder (CBS) Theorem.

23.1.1. Countability of the Rationals

Theorem 23.1.1. *The set of rational numbers $\mathbb{Q}$ is countably infinite.*

Proof. We aim to demonstrate the existence of a bijection $f : \mathbb{N} \to \mathbb{Q}$. In other words, we seek an explicit way to enumerate all rational numbers so that every rational number appears at a finite position in the list.

To do so, we arrange all rational numbers of the form $\frac{a}{b}$ in a two-dimensional array, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Each entry of this array represents one rational number.

We then traverse this array diagonally to ensure that every rational number is encountered within a finite number of steps. Since each diagonal contains only finitely many entries, this process covers the entire array. Beginning at 0, we "snake" our way through the diagonals, skipping any fractions that are not in lowest terms, as illustrated below.

This traversal defines a function $f : \mathbb{N} \to \mathbb{Q}$ recursively, assigning to each natural number the corresponding rational number in the sequence. The beginning of this enumeration may be represented as follows:

x	0	1	2	3	4	5	6	7	8	$\cdots$
$f(x)$	0	1	$\frac{1}{2}$	-1	2	$-\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$-\frac{1}{3}$	$\cdots$

Every rational number appears exactly once in this list, and each appears at a finite index, establishing a bijection $f : \mathbb{N} \to \mathbb{Q}$. Hence, $\mathbb{Q}$ is countably infinite. □

We now present an alternative proof that $\mathbb{Q}$ is countably infinite, this time using the Cantor–Bernstein–Schröder (CBS) Theorem. For this proof, we assume the Fundamental Theorem of Arithmetic, which we have partially established.

Theorem 23.1.2 (Fundamental Theorem of Arithmetic (FTOA))**.** *Every integer greater than* 1 *can be written uniquely as a product of prime numbers.*

We have already shown that every integer greater than 1 can be expressed as a product of primes. In a later section on number theory, we will prove the uniqueness of this factorization. For the purposes of this proof, we assume the full validity of the Fundamental Theorem of Arithmetic.

Theorem 23.1.3. *The set $\mathbb{Q}$ is countably infinite.*

Proof. We will construct injections $f : \mathbb{N} \to \mathbb{Q}$ and $g : \mathbb{Q} \to \mathbb{N}$. By the CBS Theorem, this will imply $|\mathbb{N}| = |\mathbb{Q}|$.

- Define $f : \mathbb{N} \to \mathbb{Q}$ by $f(n) = \frac{n}{1}$. If $f(m) = f(n)$ for $m, n \in \mathbb{N}$, then $m = n$, so f is injective. Hence $|\mathbb{N}| \leq |\mathbb{Q}|$.
- To construct an injection $g : \mathbb{Q} \to \mathbb{N}$, note that every rational number can be written uniquely in reduced form as $\frac{a}{b}$, where $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, and $\gcd(a, b) = 1$.

  Define $g : \mathbb{Q} \to \mathbb{N}$ by

$$g\left(\frac{a}{b}\right) = \begin{cases} 2^a \cdot 5^b & \text{if } a \geq 0, \\ 3^{-a} \cdot 5^b & \text{if } a < 0 \end{cases}$$

  where $\frac{a}{b} \in \mathbb{Q}$ is in reduced form.

  We now verify that g is injective. Suppose $g(x) = g(y)$, where $x = \frac{a_1}{b_1}$ and $y = \frac{a_2}{b_2}$, with $a_i \in \mathbb{Z}$, $b_i \in \mathbb{Z}^+$, and $\gcd(a_i, b_i) = 1$ for $i = 1, 2$. We consider three cases:

  - **Case 1**: $a_1, a_2 \geq 0$. Then $g(x) = g(y)$ implies $2^{a_1}5^{b_1} = 2^{a_2}5^{b_2}$. By the FTOA, we have $a_1 = a_2$ and $b_1 = b_2$.
  - **Case 2**: $a_1, a_2 < 0$. Then $g(x) = g(y)$ implies $3^{-a_1}5^{b_1} = 3^{-a_2}5^{b_2}$, and again the FTOA gives $a_1 = a_2$ and $b_1 = b_2$.
  - **Case 3**: Without loss of generality, suppose $a_1 \geq 0$ and $a_2 < 0$. Then $2^{a_1}5^{b_1} = 3^{-a_2}5^{b_2}$. By the FTOA, this forces $a_1 = a_2 = 0$, contradicting $a_2 < 0$.

  Therefore, g is injective, and $|\mathbb{Q}| \leq |\mathbb{N}|$.

By the Cantor–Bernstein–Schröder Theorem, we conclude that $|\mathbb{N}| = |\mathbb{Q}|$, so $\mathbb{Q}$ is countably infinite. □

We have already seen that several familiar sets are countable. We now establish some general results that allow us to construct new countable sets from previously known ones.

23.1.2. Properties of Countable Sets

Recall that $|\mathbb{N}^2| = |\mathbb{N}|$. Using this fact, together with induction, we can prove the following result.

Theorem 23.1.4. *For any $n \in \mathbb{Z}^+$, $|\mathbb{N}^n| = \aleph_0$.*

Proof. Recall that $|\mathbb{N}^2| = |\mathbb{N}|$, and let $f : \mathbb{N}^2 \to \mathbb{N}$ be a bijection.

We proceed by induction on $n \in \mathbb{Z}^+$.

- **Base Case**: For $n = 1$, we have $|\mathbb{N}^1| = |\mathbb{N}| = \aleph_0$, which holds by definition.

- **Inductive Step**: Suppose that for some $n \in \mathbb{Z}^+$, we have $|\mathbb{N}^n| = \aleph_0$. Then there exists a bijection $g : \mathbb{N}^n \to \mathbb{N}$. Define a function $h : \mathbb{N}^{n+1} \to \mathbb{N}^2$ by

$$h((a_1, a_2, \ldots, a_n), a_{n+1}) = (g(a_1, a_2, \ldots, a_n), a_{n+1}).$$

  We show that h is a bijection.

  - **Injectivity**: Suppose

$$h((a_1, \ldots, a_n), a_{n+1}) = h((b_1, \ldots, b_n), b_{n+1}).$$

    Then, by definition of h,

$$(g(a_1, \ldots, a_n), a_{n+1}) = (g(b_1, \ldots, b_n), b_{n+1}),$$

    which implies that

$$g(a_1, \ldots, a_n) = g(b_1, \ldots, b_n) \quad \text{and} \quad a_{n+1} = b_{n+1}.$$

    Since g is injective, it follows that $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$, and hence $a_i = b_i$ for all $i \in [n+1]$. Thus, h is injective.

  - **Surjectivity**: Let $(x, y) \in \mathbb{N}^2$ be arbitrary. Since g is surjective, there exists $(a_1, \ldots, a_n) \in \mathbb{N}^n$ such that $g(a_1, \ldots, a_n) = x$. Then for $((a_1, \ldots, a_n), y) \in \mathbb{N}^{n+1}$,

$$h((a_1, \ldots, a_n), y) = (g(a_1, \ldots, a_n), y) = (x, y).$$

    Hence h is surjective.

  Since h is both injective and surjective, it is a bijection.

  Finally, the composition $f \circ h : \mathbb{N}^{n+1} \to \mathbb{N}$ is a bijection, since it is the composition of two bijections. Therefore, $|\mathbb{N}^{n+1}| = |\mathbb{N}| = \aleph_0$.

By the principle of mathematical induction, we conclude that $|\mathbb{N}^n| = \aleph_0$ for all $n \in \mathbb{Z}^+$. □

Combining this result with the properties of finite Cartesian products, we obtain the following theorem.

Theorem 23.1.5 (Finite Product of Countable Sets is Countable)**.** *If $n \in \mathbb{Z}^+$ and $X_1, \ldots, X_n$ are nonempty countable sets, then*

$$\prod_{i=1}^{n} X_i = X_1 \times X_2 \times \cdots \times X_n$$

is countable. Moreover, if at least one X_i is infinite, then $\prod_{i=1}^{n} X_i$ is countably infinite.

We've seen that we can take finite Cartesian products of countable sets and remain countable. For unions of sets, we can do even better. The following result shows that a countably infinite union of countably infinite sets is still countably infinite.

Theorem 23.1.6. *Suppose $\{A_n\}_{n\in\mathbb{N}}$ is a family of countably infinite sets. Then*

$$\bigcup_{n\in\mathbb{N}} A_n$$

is countably infinite.

Proof. Let $A = \bigcup_{n\in\mathbb{N}} A_n$. We will show that $\aleph_0 \leq |A|$ and $\aleph_0 \geq |A|$.

- Since A_0 is countably infinite, there exists a bijection $f_0 : \mathbb{N} \to A_0$. Define $g : \mathbb{N} \to A$ by $g(n) = f_0(n)$. Because f_0 is injective, g is also injective. Hence $\aleph_0 = |\mathbb{N}| \leq |A|$.
- For each $n \in \mathbb{N}$, let $f_n : \mathbb{N} \to A_n$ be a bijection (which exists because $|A_n| = \aleph_0$ by assumption). Define $h : \mathbb{N}^2 \to A$ by $h(n, m) = f_n(m)$. We will show that h is surjective.

  Let $a \in A$ be arbitrary. Then $a \in A_n$ for some $n \in \mathbb{N}$. Fix such an n. Since f_n is surjective, there exists $m \in \mathbb{N}$ such that $f_n(m) = a$. Thus $h(n, m) = f_n(m) = a$. Because $a \in A$ was arbitrary, h is surjective. Therefore $\aleph_0 = |\mathbb{N}^2| \geq |A|$.

By the Cantor–Bernstein–Schröder Theorem and the partition principle, it follows that $|A| = \aleph_0$, as desired. □

Since a countably infinite union of countably infinite sets is countably infinite, it follows that when we take either fewer unions or smaller sets, the union remains countable.

Corollaries 23.1.7 (A Countable Union of Countable Sets is Countable)**.**

1. *If $|A| = \aleph_0$ and $|B| \leq \aleph_0$, then $|A \cup B| = \aleph_0$.*
2. *If $\{A_i\}_{i\in\mathbb{N}}$ is a family of countable sets, then $A = \bigcup_{i\in\mathbb{N}} A_i$ is countable.*
3. *If $\{A_i\}_{i\in[n]}$ (for some $n \in \mathbb{Z}^+$) is a finite family of countable sets, then $A = \bigcup_{i\in[n]} A_i$ is countable. Moreover:*
   a) *If $|A_i| = \aleph_0$ for at least one $i \in [n]$, then $|A| = \aleph_0$.*
   b) *If each A_i is finite, then A is finite with $|A| \geq \max\{|A_i|\}_{i\in[n]}$.*

Note. Regarding part (3b) in the previous corollary, we will discuss a formula for determining $|A|$ in the combinatorics section later in the semester.

Exercise 23.1.8. Show that the following sets are countably infinite.

(a) $A = \{f : \{0, 1\} \to \mathbb{N} \mid f \text{ is a function}\}$

(b) $B =$ the set of circles in $\mathbb{R}^2$ whose centers have integer coordinates and whose radii have rational lengths.

(c) $C = \{f : \mathbb{N} \to \mathbb{N} \mid \forall x \in \mathbb{N}, f(x + 1) = f(x) + 1\}$

(d) $D =$ the set of all "words", where a "word" is a finite string of letters from the English alphabet.

23.2. Uncountable Sets

So far, we have shown that many different infinite sets share the same size as $\mathbb{N}$. This might naturally lead to the question: do *uncountably infinite* sets even exist? In this section, we will not only demonstrate that uncountably infinite sets do exist, but also establish that there are multiple distinct sizes (cardinalities) among uncountably infinite sets. Our main proof technique will be a powerful method known as *diagonalization*.

23.2.1. Uncountability of the Real Numbers

To show that the real numbers are uncountable, we need to establish that there is no possible way to enumerate them. How can we prove that such an enumeration cannot exist? As is often done in mathematics, we will proceed by *contradiction*.

To make this argument concrete, we will describe real numbers using their decimal expansions and apply a diagonalization argument.

A real number $x \in \mathbb{R}$ can be represented in its decimal form as

$$x = x_0.x_1x_2x_3\cdots,$$

where $x_0 \in \mathbb{Z}$ is the integer part, and $x_i \in \mathbb{N}$ with $0 \leq x_i \leq 9$ for $i \in \mathbb{Z}^+$ represent the decimal digits. For example,

$$\frac{5}{6} = 0.83333\cdots = 0.8\overline{3}.$$

Technical Note: Decimal representations are not always unique. In particular, a decimal that ends with an infinite sequence of 9's is equal to the corresponding decimal that ends with an infinite sequence of 0's. (This is usually proved in Calculus 2 using geometric series.) For example,

$$0.499999\cdots = 0.50000\cdots.$$

To avoid this ambiguity, we adopt the following convention: a decimal representation of $x \in \mathbb{R}$ is said to be in *normalized form* if it does not end with an infinite string of 9's.

Exercise 23.2.1. (*For those who have taken Calculus 2*)

Suppose that $x \in [0, 1)$ has two distinct decimal expansions:

$$x = 0.a_1a_2a_3\cdots,$$
$$x = 0.b_1b_2b_3\cdots,$$

where $a_i, b_i \in \{0, 1, \ldots, 9\}$ for all i. Let M be the smallest positive integer such that $a_M \neq b_M$ and assume that $a_M > b_M$. Prove that:

- $a_i = b_i$ for all $1 \leq i < M$,
- $a_M = b_M + 1$,
- $a_i = 0$ and $b_i = 9$ for all $i > M$.

With this convention in place, we can now use diagonalization to prove that there are uncountably many real numbers in the interval $(0, 1)$.

24. October 29

24.1. Uncountable Sets

24.1.1. Uncountability of the Real Numbers

Theorem 24.1.1. *The open interval* $(0,1)$ *is uncountable.*

Proof. Let $f : \mathbb{Z}^+ \to (0,1)$ be an arbitrary function. We aim to show that f is not surjective.

For each $n \in \mathbb{Z}^+$, write $f(n)$ in normalized decimal form as

$$\begin{aligned} f(1) &= 0.c_{1,1}c_{1,2}c_{1,3}\cdots \\ f(2) &= 0.c_{2,1}c_{2,2}c_{2,3}\cdots \\ f(3) &= 0.c_{3,1}c_{3,2}c_{3,3}\cdots \\ f(4) &= 0.c_{4,1}c_{4,2}c_{4,3}\cdots \\ &\vdots \quad \vdots \end{aligned}$$

We will construct a number $x \in (0,1)$ such that $x \notin \mathrm{Im}(f)$. Define x by specifying its nth digit x_n as

$$x_n = \begin{cases} 1, & \text{if } c_{n,n} \neq 1, \\ 2, & \text{if } c_{n,n} = 1. \end{cases}$$

By construction, $x_n \neq c_{n,n}$ for all $n \in \mathbb{Z}^+$. Thus x differs from $f(n)$ in the nth decimal place for every n, meaning $x \neq f(n)$ for all $n \in \mathbb{Z}^+$. Since $x \in (0,1)$ and $x \notin \mathrm{Im}(f)$, it follows that f is not surjective.

Because $f : \mathbb{Z}^+ \to (0,1)$ was chosen arbitrarily, this shows that $\aleph_0 = |\mathbb{Z}^+| < |(0,1)|$. Therefore, the interval $(0,1)$ is uncountable. □

Note. The proof above illustrates the general idea behind *diagonalization*: given any attempt to list all elements of a certain set (for example, $f(1), f(2), f(3), \ldots$), we construct a new element that systematically differs from each listed one in at least one place.

More precisely, the diagonalization strategy involves the following pattern:

1. Assume, for contradiction, that an enumeration of the set exists.

2. Represent each element in a way that exposes infinitely many "coordinates" or distinguishable components (for example, digits of a real number, or values of a sequence).
3. Construct a new element by changing the nth coordinate (or component) of the nth listed element in a deliberate way.
4. Conclude that this new element differs from every element in the list, contradicting the assumption of a complete enumeration.

The key feature of diagonalization is that the new element disagrees with the nth listed element in the nth component, ensuring that it is distinct from every item in the list.

This strategy generalizes beyond decimal expansions. In each case, the heart of the argument is the same: no enumeration can capture every possible object once we can systematically construct one that escapes the list.

Corollary 24.1.2. *$\mathbb{R}$ is uncountable, and $|\mathbb{R}| = |(0,1)|$.*

Proof. Define $f : (0,1) \to \mathbb{R}$ by

$$f(x) = \ln\left(\frac{1-x}{x}\right).$$

Proving that f is a bijection was left as an exercise earlier. Since $(0,1)$ is uncountable and f is a bijection, it follows that $\mathbb{R}$ is also uncountable. □

Corollary 24.1.3. *For any $a, b \in \mathbb{R}$ with $a < b$, each of the following sets is uncountable:*

- (a,b)
- $[a,b)$
- $(-\infty, b)$
- (a, ∞)
- $(a,b]$
- $[a,b]$
- $(-\infty, b]$
- $[a, \infty)$

24.1.2. Cantor's Theorem

Our diagonalization argument for the real numbers revealed that $(0,1)$ cannot be enumerated by the natural numbers. Cantor's Theorem extends this idea even further: for *any* set S, the collection of all its subsets—its power set—is strictly larger than S itself.

Theorem 24.1.4 (Cantor's Theorem)**.** *For any set S, we have $|S| < |\mathcal{P}(S)|$.*

Notes.

- If S is finite, Cantor's Theorem can be verified directly. In Homework 7, we proved that $|\mathcal{P}([n])|= 2^n$ for all $n \in \mathbb{N}$, and it can be proven by induction that $n < 2^n$ for all $n \in \mathbb{N}$.
- For infinite sets S, the theorem implies an infinite hierarchy of distinct infinite cardinalities, obtained by repeatedly taking power sets. For example:

$$|\mathbb{N}|< |\mathcal{P}(\mathbb{N})|< |\mathcal{P}(\mathcal{P}(\mathbb{N}))|< |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|< \cdots$$

Proof. Let S be an arbitrary set, and suppose $g : S \to \mathcal{P}(S)$ is any function. Define a set $T \in \mathcal{P}(S)$ by

$$T = \{x \in S \mid x \notin g(x)\}.$$

We will show that $T \neq g(x)$ for any $x \in S$. Let $x \in S$ be arbitrary.

- Case 1: Suppose $x \in T$. Then, by definition of T, we have $x \notin g(x)$. Hence $x \in T$ but $x \notin g(x)$, so $T \neq g(x)$.
- Case 2: Suppose $x \notin T$. Then, by definition of T, we have $x \in g(x)$. Hence $x \notin T$ but $x \in g(x)$, so again $T \neq g(x)$.

Thus $T \neq g(x)$ for every $x \in S$, meaning T is not in the image of g. Therefore g is not surjective. Since $g : S \to \mathcal{P}(S)$ was arbitrary, no surjection from S onto $\mathcal{P}(S)$ exists, and hence $|S|< |\mathcal{P}(S)|$. □

The construction in the proof is another example of *diagonalization*, where we created a new set T that disagrees with each $g(x)$ regarding the membership of x.

Example 24.1.5. To illustrate Cantor's Theorem for the case $S = \mathbb{N}$, we will show that no surjection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ can exist. Let $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ be an arbitrary function, and define

$$T = \{n \in \mathbb{N} \mid n \notin f(n)\}.$$

We claim that T is not equal to $f(n)$ for any $n \in \mathbb{N}$.

To get some intuition, let us look at a few examples.

- Suppose $f(0) = \{0, 3\}$. Then $0 \notin T$ because $0 \in f(0)$, so $T \neq f(0)$.
- Suppose $f(1) = \{5\}$. Then $1 \in T$ because $1 \notin f(1)$, so $T \neq f(1)$.
- Suppose $f(2) = \mathbb{N}$. Then $2 \notin T$ because $2 \in f(2)$, so $T \neq f(2)$.
- Suppose $f(3) = \{1, 2, 4\}$. Then $3 \in T$ because $3 \notin f(3)$, so $T \neq f(3)$.

In each case, T differs from $f(n)$ at the element n itself.

More generally, for any $n \in \mathbb{N}$, we have two cases:

- Case 1: If $n \in f(n)$, then $n \notin T$, so $T \neq f(n)$.
- Case 2: If $n \notin f(n)$, then $n \in T$, so $T \neq f(n)$.

Thus, for every $n \in \mathbb{N}$, the set T differs from $f(n)$ in at least one element—specifically, at the "diagonal position" n. This pattern of constructing a new object that disagrees with the n-th object at the n-th coordinate is the essence of the diagonalization method.

Since $T \in \mathcal{P}(\mathbb{N})$ and $T \neq f(n)$ for all $n \in \mathbb{N}$, we conclude that f is not a surjection. Therefore,

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|.$$

Diagonalization thus provides a systematic way to construct an element not listed in any proposed enumeration.

24.1.3. Infinite Binary Sequences

The technique used in Cantor's Theorem also applies to other sets with infinite structure. One important example is the set of all infinite binary sequences. Although this result was proven in recitation, we restate it here to highlight its connection with Cantor's argument.

Theorem 24.1.6. *Define $\{0,1\}^{\mathbb{N}}$ as the set of all infinite sequences consisting of 0s and 1s. That is,*

$$\{0,1\}^{\mathbb{N}} = \{\langle a_i \rangle_{i \in \mathbb{N}} \mid \forall i \in \mathbb{N},\, a_i \in \{0,1\}\}\,.$$

Then $\{0,1\}^{\mathbb{N}}$ is uncountably infinite.

Cantor's diagonal argument can be adapted to this setting by assuming we have an enumeration of all infinite binary sequences and then constructing a new sequence that differs from the n-th sequence at its n-th position. The resulting sequence cannot appear in the list, proving that no enumeration can include every element of $\{0,1\}^{\mathbb{N}}$.

Conceptually, this result is equivalent to Cantor's Theorem for $\mathcal{P}(\mathbb{N})$: each infinite binary sequence can be viewed as the characteristic function of a subset of $\mathbb{N}$. Thus, $\{0,1\}^{\mathbb{N}}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality, providing another example of how diagonalization exposes uncountable structures.

Exercise 24.1.7. Show that the following sets are uncountable.

(a) $A = \{f : \mathbb{N} \to \{0,1\} \mid f \text{ is a function}\}$

(b) $B = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a function}\}$

(c) $C = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a bijection}\}$

(d) $D =$ the set of infinite sequences of integers.

(e) $E = \mathbb{R} \setminus \mathbb{Q}[\sqrt{2}]$ where

$$\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Q}, x = a + b\sqrt{2}\}$$

Part V.

Number Theory

25. October 29

25.1. Introduction

Number theory is possibly the oldest field of mathematics, and much of modern mathematics has its roots in it. The simplest description of number theory is *the study of arithmetic*. Number theorists investigate the fundamental properties of the integers, exploring their structure and relationships. At the heart of this field lies the study of prime numbers, which play a central role. Many of the most famous unsolved problems in mathematics are found in number theory, often characterized by their simplicity to state but difficulty to solve.

Examples of Number Theoretic Results and Conjectures

1. There are infinitely many ordered triples of positive integers (x, y, z) such that $x^2 + y^2 = z^2$.
2. *Fermat's Last Theorem*: There are no ordered triples of positive integers (x, y, z) such that $x^n + y^n = z^n$ for any $n \geq 3$.
3. *Lagrange's Four-Square Theorem*: Every nonnegative integer can be expressed as the sum of four perfect squares. For example, $35 = 5^2 + 3^2 + 1^2 + 0^2$.
4. *Goldbach's Conjecture*: Every even integer greater than 2 can be written as the sum of two prime numbers. For example, $14 = 3 + 11$ (or $14 = 7 + 7$).
5. *Twin Prime Conjecture*: There are infinitely many pairs of prime numbers of the form $(p, p + 2)$.

To begin our study of number theory, we will first review some relevant definitions and results from earlier sections.

- A natural number $n > 1$ is called *prime* if its only divisors are 1 and itself. In other words, if n is prime and $n = ab$ for $a, b \in \mathbb{N}$, then either $a = 1$ or $b = 1$ (Lecture 11).
- A natural number $n > 1$ is called *composite* if there exist $a, b \in \mathbb{N}$ such that $1 < a \leq b < n$ and $n = ab$. In other words, $n > 1$ and is not prime.
- The natural number $n = 1$ is called a *unit*.

- Every natural number $n > 1$ is either prime or can be expressed as a product of prime numbers (Theorem 11.1.7).

We now state a useful result that was proved in class on September 8, and repeat the proof here for reference:

Theorem 25.1.1. *Let $m, n \in \mathbb{Z}$ be nonzero integers. If $m \mid n$, then $|m| \leq |n|$.*

Proof. Let $m, n \in \mathbb{Z} \setminus \{0\}$ such that $m \mid n$. Then there exists an integer $a \in \mathbb{Z}$ such that $n = ma$. Since the absolute value function is multiplicative, we have $|n| = |m| \cdot |a|$. Because m and n are nonzero, $a \neq 0$, which implies $|a| \geq 1$. Therefore, $|n| = |m| \cdot |a| \geq |m| \cdot 1 = |m|$. □

The following corollary is an immediate consequence of the theorem.

Corollary 25.1.2. *Let $m, n \in \mathbb{Z}$. If $m \mid n$ and $n \mid m$, then $m = \pm n$.*

From the definitions and results above, we know that every composite integer n has a prime factor $p < n$. In fact, we can say more: every composite integer n has a prime factor $p \leq \sqrt{n}$. This observation provides a straightforward (though inefficient) method for checking whether a natural number n is prime.

Theorem 25.1.3. *If $n \in \mathbb{N}$ is composite, then n has a prime factor p such that $p \leq \sqrt{n}$.*

Proof. Let $n \in \mathbb{N}$ be composite, and express n as $n = ab$ for some $a, b \in \mathbb{N}$ with $1 < a \leq b < n$. We first show that $a \leq \sqrt{n}$.

Assume, for the sake of contradiction, that $a > \sqrt{n}$. Then

$$n = (\sqrt{n})^2 < a^2 \leq ab = n,$$

which yields the contradiction $n < n$. Therefore, $a \leq \sqrt{n}$.

Let p be any prime divisor of a (possibly a itself, if a is prime). Then $p \leq a \leq \sqrt{n}$ and, since $p \mid a$ and $a \mid n$, it follows by transitivity that $p \mid n$. □

Example 25.1.4. Use the previous theorem to determine whether 91 or 97 is prime.

Observe that $\sqrt{91} < \sqrt{97} < 10$, and the only prime numbers less than 10 are 2, 3, 5, and 7. To determine whether 91 or 97 is prime, we need to check if they are divisible by 2, 3, 5, or 7.

- It is clear that $2 \nmid 91$ (since 91 is odd) and $5 \nmid 91$ (since 91 does not end in 0 or 5). We also find that $3 \nmid 91$, but we notice that $7 \mid 91$ and $91 = 7 \cdot 13$. Thus, 91 is $\boxed{\text{composite}}$.
- Similarly, $2 \nmid 97$ and $5 \nmid 97$. Checking for divisibility by 3 and 7, we find that $3 \nmid 97$ and $7 \nmid 97$. Therefore, 97 is $\boxed{\text{prime}}$.

Exercise 25.1.5. Determine which of the following integers are primes.

(a) 201
(b) 203
(c) 207
(d) 211
(e) 213
(f) 221

26. October 31

26.1. GCDs, LCMs, and Linear Combinations

By Theorem 25.1.1, if n is a nonzero integer, then n can have only finitely many divisors, since $m \mid n$ implies $|m| \leq |n|$. Because any two nonzero integers each have finitely many divisors, it is natural to define the *greatest* divisor common to both. In fact, we can relax this requirement so that only one of the integers must be nonzero.

Definition. For $a, b \in \mathbb{Z}$, not both zero, an integer d is called a *common divisor* of a and b if $d \mid a$ and $d \mid b$. Furthermore, d is called the *greatest common divisor* of a and b, denoted $\gcd(a, b)$, if d is the largest of their common divisors.

Examples 26.1.1.

1. Consider $m = 54$ and $n = 42$.

$$\begin{aligned} \text{Set of divisors of } 54 &= \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18, \pm 27, \pm 54\}, \\ \text{Set of divisors of } 42 &= \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}, \\ \text{Set of common divisors} &= \{\pm 1, \pm 2, \pm 3, \pm 6\}. \end{aligned}$$

   Therefore, $\gcd(54, 42) = 6$, the largest element from the set of common divisors.

2. $\gcd(-6, -15) = 3$. Even though both integers are negative, the greatest common divisor is always taken to be positive.

3. $\gcd(0, 44) = 44$. Since every integer divides 0, we have $\gcd(0, n) = |n|$ for any integer $n \neq 0$. (The value $\gcd(0, 0)$ is undefined.)

Since the divisors of $-m$ are the same as those of m, it follows that $\gcd(m, n) = \gcd(|m|, |n|)$. Therefore, we often restrict our attention to pairs of nonnegative integers.

Definition. Let $a, b \in \mathbb{Z}$, not both zero. Then a and b are called *relatively prime* (or *coprime*) if $\gcd(a, b) = 1$.

The following theorem states that if we divide a and b by their greatest common divisor, then the resulting integers have no common divisors other than ± 1. This simple but powerful result is foundational in the study of arithmetic.

Theorem 26.1.2. *Let $a, b \in \mathbb{Z}$, not both zero. If $\gcd(a, b) = d$, then*

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof. Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Suppose $n \in \mathbb{Z}^+$ divides both $\frac{a}{d}$ and $\frac{b}{d}$. Then there exist integers $k, \ell \in \mathbb{Z}$ such that

$$\frac{a}{d} = nk \quad \text{and} \quad \frac{b}{d} = n\ell,$$

which implies $a = nkd$ and $b = n\ell d$. Hence, nd is a common divisor of a and b. Since $d = \gcd(a, b)$, we must have $nd \leq d$, and therefore $n = 1$ because $n, d \in \mathbb{Z}^+$. Thus,

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \quad \square$$

Exercise 26.1.3. Find the greatest common divisor of each of the following pairs of integers.

(a) 5,15

(b) 0, 111

(c) $-27, -45$

(d) -90, 100

(e) 100, 121

(f) 1001, 289

26.1.1. The Euclidean Algorithm

The *Euclidean Algorithm* is a well-known and efficient method for computing the greatest common divisor (GCD) of two integers. Its foundation rests on the following lemma.

Theorem 26.1.4 (EA Theorem)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. For any $k \in \mathbb{Z}$,*

$$\gcd(a, b) = \gcd(b,\ a - bk).$$

Proof. We will show that a and b have the same set of common divisors as b and $a - bk$, using a double-containment argument.

- Suppose $c \in \mathbb{Z}$ is a common divisor of a and b, i.e., $c \mid a$ and $c \mid b$. Then there exist $x, y \in \mathbb{Z}$ such that $a = cx$ and $b = cy$. It follows that

  $$a - bk = c(x - yk),$$

  so $c \mid (a - bk)$. Thus, c is a common divisor of b and $a - bk$.

- Conversely, suppose $c \in \mathbb{Z}$ is a common divisor of b and $a - bk$, i.e., $c \mid b$ and $c \mid (a - bk)$. Then there exist $x, y \in \mathbb{Z}$ such that $b = cx$ and $a - bk = cy$. Hence,

$$a = (a - bk) + bk = cy + cxk = c(y + xk),$$

  and therefore $c \mid a$. Thus, c is a common divisor of a and b.

Since the two pairs share the same common divisors, it follows that $\gcd(a, b) = \gcd(b, a - bk)$. □

Given that $\gcd(a, b) = \gcd(|a|, |b|)$ and $\gcd(a, 0) = |a|$ (for $a \neq 0$), the Euclidean Algorithm is used to find the GCD of two *positive integers*.

Strategy: The Euclidean Algorithm

Let $a, b \in \mathbb{Z}$ with $a > b > 0$.

- Set $r_0 = a$ and $r_1 = b$.
- For $j \geq 2$, apply the Division Algorithm to divide r_{j-2} by r_{j-1}, yielding

$$r_{j-2} = q_{j-1} r_{j-1} + r_j,$$

  where $0 \leq r_j < r_{j-1}$.
- Terminate the process when $r_n = 0$.
- The last nonzero remainder, r_{n-1}, is equal to $\gcd(a, b)$.

The Idea. The algorithm produces a strictly decreasing sequence of nonnegative remainders:

$$r_0 > r_1 > r_2 > \cdots > r_{n-1} > r_n = 0.$$

By the well-ordering property of the natural numbers, this sequence must eventually terminate with a remainder of 0. Applying Theorem 26.1.4 repeatedly gives

$$\begin{aligned} \gcd(a, b) &= \gcd(r_0, r_1) \\ &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) \\ &\vdots \\ &= \gcd(r_{n-1}, 0) \\ &= r_{n-1}. \end{aligned}$$

This procedure will be clarified through a concrete example.

Example 26.1.5. Find $\gcd(148, 40)$.

Solution. Here, $r_0 = 148$ and $r_1 = 40$. We repeatedly apply the Division Algorithm until the remainder becomes 0:

$$\begin{aligned} 148 &= 40 \cdot 3 + 28, \\ 40 &= 28 \cdot 1 + 12, \\ 28 &= 12 \cdot 2 + 4, \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

The greatest common divisor of 148 and 40 is the last nonzero remainder. Therefore, $\gcd(148, 40) = 4$.

Exercise 26.1.6. Without a calculator, use the Euclidean Algorithm to compute the GCD of the following pairs of integers.

(a) 171 and 33

(b) 1872 and 300

(c) 325299 and 325

(d) $n^7 - 1$ and $n^5 - 1$ where $n > 1$

Exercise 26.1.7. Prove that for any $n \in \mathbb{N}$, $5n + 3$ and $3n + 2$ are coprime.

26.1.2. Linear Combinations

The Euclidean Algorithm can be used to find integers x and y such that $ax + by = \gcd(a, b)$.

Example 26.1.8. Performing the Euclidean Algorithm on 148 and 40, we have:

$$\begin{aligned} 148 &= 40 \cdot 3 + 28, \\ 40 &= 28 \cdot 1 + 12, \\ 28 &= 12 \cdot 2 + 4, \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

Thus, $\gcd(148, 40) = 4$. To express 4 as a linear combination of 148 and 40, we solve for the remainders in the first three equations:

$$\begin{aligned} 28 &= 148 - 3 \cdot 40, \\ 12 &= 40 - 1 \cdot 28, \\ 4 &= 28 - 2 \cdot 12. \end{aligned}$$

Substituting the second equation into the expression for 4 gives:

$$4 = 28 - 2 \cdot (40 - 28) = 3 \cdot 28 - 2 \cdot 40.$$

Next, substituting the expression for 28 yields:

$$4 = 3 \cdot (148 - 3 \cdot 40) - 2 \cdot 40 = 3 \cdot 148 - 11 \cdot 40.$$

Therefore, $\gcd(148, 40) = 3 \cdot 148 - 11 \cdot 40$.

The values $x = 3$ and $y = -11$ found in the previous example are not unique. In fact, there are infinitely many integer pairs (x, y) satisfying $148x + 40y = 4$. However, $\gcd(148, 40)$ is the *smallest* positive integer that can be written in the form $148x + 40y$. The following theorem establishes this general result.

Theorem 26.1.9 (Bézout's Lemma)**.** *Let $a, b \in \mathbb{Z}$, not both zero. Then:*

1. *There exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.*
2. *If $x, y \in \mathbb{Z}$ satisfy $ax + by > 0$, then $ax + by \geq \gcd(a, b)$.*

Proof. We will prove both statements simultaneously. Define the set $S \subseteq \mathbb{Z}^+$ by

$$S = \{c \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z},\ (ax + by = c)\}.$$

Since $|a|+|b| \in S$, the set S is non-empty. By the Well-Ordering Property, S has a least element. Let $d = ma + nb$, where $m, n \in \mathbb{Z}$, be the smallest element of S. To establish both conditions, we need to show that $d = \gcd(a, b)$.

To show that $d \mid a$, let $q, r \in \mathbb{Z}$ be such that $0 \leq r < d$ and $a = dq + r$, as guaranteed by the Division Algorithm. Solving for r and substituting $d = ma + nb$, we get:

$$r = a - dq = a - (ma + nb)q = (1 - qm)a + (-qn)b.$$

Thus, r can be written in the form $ax + by$, but since $r < d$, it must be that $r \notin S$, implying $r = 0$. Hence, $d \mid a$. An identical argument shows that $d \mid b$, making d a common divisor of a and b.

To show that d is the *greatest* common divisor, let $t \in \mathbb{Z}^+$ be a common divisor of a and b. Then there exist $k, \ell \in \mathbb{Z}$ such that $a = tk$ and $b = t\ell$. Substituting these into $d = ma + nb$, we obtain:

$$d = mtk + nt\ell = t(mk + n\ell).$$

Thus, $t \mid d$. Since both t and d are positive, we conclude $t \leq d$, establishing that $d = \gcd(a, b)$. □

Several useful consequences follow immediately from Bézout's Lemma. We will discuss many of these in recitation, but you are encouraged to try proving them on your own. One is left as an exercise below.

Corollaries 26.1.10. *Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$.*

1. *If $t \mid a$ and $t \mid b$, then $t \mid d$.*

   (Every common divisor divides the greatest common divisor.)

2. *For all $c \in \mathbb{Z}$, there exist $m, n \in \mathbb{Z}$ such that $am + bn = c$ if and only if $d \mid c$.*

3. *a and b are coprime if and only if there exist $m, n \in \mathbb{Z}$ such that $am + bn = 1$.*

4. *For all $m \in \mathbb{Z}^+$, $\gcd(ma, mb) = m \cdot \gcd(a, b) = md$.*

Exercise 26.1.11.

(a) Use the Euclidean Algorithm to find $\gcd(1819, 3587)$.

(b) Find a pair $(x, y) \in \mathbb{Z}^2$ such that $1819x + 3587y = \gcd(1819, 3587)$.

Exercise 26.1.12. Let $a, b \in \mathbb{Z}$, not both 0, and $m \in \mathbb{Z}^+$. Prove that $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Exercise 26.1.13. Prove that if a and b are relatively prime integers then $\gcd(a+b, a-b) = 1$ or 2, with $\gcd(a + b, a - b) = 2$ if and only if a and b have the same parity.

27. November 3

27.1. GCDs, LCMs, and Linear Combinations

27.1.1. Linear Diophantine Equations

A *Diophantine equation* is a polynomial equation with integer coefficients, typically involving multiple variables, in which the goal is to find integer (or sometimes rational) solutions. The study of such equations forms a central area of research in Number Theory, with applications ranging from cryptography to mathematical puzzles. Diophantine equations come in many forms, varying greatly in difficulty and complexity.

In this course, we will focus on a specific type of Diophantine equation called *linear Diophantine equations*, which involve polynomials of degree one. To motivate our exploration, let's look at a few examples that illustrate the variety and challenges of Diophantine problems:

Examples 27.1.1.

1. Find all $(x, y) \in \mathbb{Z}^2$ such that $y^2 = x^3 + 16$.

   This is an example of a Mordell equation, a type of cubic Diophantine equation. These equations often have only a few integer solutions or none at all. For this particular equation, the only integer solutions are $(0, 4)$ *and* $(0, -4)$.

2. Find all $n \in \mathbb{Z}$ that can be expressed as the sum of three cubes, i.e.,

   $$\exists x, y, z \in \mathbb{Z},\ n = x^3 + y^3 + z^3.$$

   This is an example of a longstanding open problem in number theory. While some values of n *have been resolved, finding solutions for all* n *remains an unsolved challenge.*

3. Find all $(x, y) \in \mathbb{Z}^2$ such that $6x + 9y = 27$.

   This is a linear Diophantine equation, which we will study in detail. Unlike the previous examples, linear Diophantine equations can often be solved systematically, and we will develop techniques to find all solutions.

A Diophantine equation of the form $ax + by = c$, where $a, b, c \in \mathbb{Z}$, is called a *linear Diophantine equation in two variables.*

We know from Bézout's lemma that $\exists x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$. If a solution exists, we can find one such solution using the Reverse Euclidean Algorithm, as illustrated in Example 26.1.8. First, find $x', y' \in \mathbb{Z}$ such that $ax' + by' = \gcd(a, b)$. For instance, in Example 26.1.8, we found that

$$\gcd(148, 40) = 4 = 148(3) + 40(-11).$$

Since $\gcd(a, b) \mid c$, we can find one solution to $ax + by = c$ by multiplying the equation $ax' + by' = \gcd(a, b)$ by $\frac{c}{\gcd(a,b)}$. For instance, if $c = 36$, then multiplying the previous equation by 9 gives

$$36 = 148(27) + 40(-99).$$

Now that we know how to find one solution to $ax + by = c$, how do we find all solutions? Are there others? And if so, how many? Let's first get a basic idea of how we can use one solution to find all solutions through the following example.

Example 27.1.2. Find all integral solutions to $6x + 9y = 21$.

$x, y \in \mathbb{Z}$ satisfy $6x + 9y = 21$ if and only if $2x + 3y = 7$ (dividing through by $\gcd(6, 9)$). Thus, it suffices to find all solutions to $2x + 3y = 7$. Since the numbers are small, we can guess a solution:

$$2(2) + 3(1) = 7.$$

Thus, $(2, 1)$ is one solution to the equation. Now, suppose $(x, y) \in \mathbb{Z}^2$ is **any** solution to $2x + 3y = 7$. We then have

$$2x + 3y = 7 = 2(2) + 3(1).$$

This equation holds if and only if

$$2(x - 2) = 3(1 - y).$$

Let $m = x - 2$ and $n = 1 - y$, so our equation becomes $2m = 3n$. Since $2m$ is even (and $2 \nmid 3$), it must be the case that $2 \mid n$, hence $n = 2k$ for some $k \in \mathbb{Z}$. Substituting this into our previous equation gives

$$2m = 6k \implies m = 3k.$$

Using $m = x - 2$ and $n = 1 - y$, we find

$$x = 2 + 3k \quad \text{and} \quad y = 1 - 2k.$$

Thus, any solution must be of the form $(2 + 3k, 1 - 2k)$ for some $k \in \mathbb{Z}$. Furthermore, we can verify that any ordered pair of this form satisfies the Diophantine equation:

$$2(2 + 3k) + 3(1 - 2k) = 4 + 6k + 3 - 6k = 7.$$

Hence, the solution set is $\{(2 + 3k, 1 - 2k) \mid k \in \mathbb{Z}\}$.

We summarize the result below. The proof, which generalizes the previous example, is left for homework.

Theorem 27.1.3. *Let $a, b, c \in \mathbb{Z}$ with a and b not both zero. If $\gcd(a, b) \mid c$, then there are infinitely many integer solutions to $ax + by = c$. Moreover, if (x_0, y_0) is one solution, then all solutions are given by*

$$\{(x_0 + m(b/d), y_0 - m(a/d)) \mid m \in \mathbb{Z},\ d = \gcd(a, b)\}.$$

Proof. Homework. □

Exercise 27.1.4. Find all integer solutions to the following linear Diophantine equations, or state why none exist.

(a) $123x + 45y = 17$

(b) $123x + 45y = 18$

27.1.2. Least Common Multiples

We now discuss the concept of the least common multiple, which serves as a natural counterpart to the greatest common divisor.

Definition. Let $a, b, c \in \mathbb{Z} \setminus \{0\}$. We say that c is a *common multiple* of a and b if $a \mid c$ and $b \mid c$. Furthermore, c is called the *least common multiple of a and b*, denoted $\operatorname{lcm}[a, b]$, if $c > 0$ and c is the smallest of all positive common multiples of a and b.

The following theorem establishes a key property of the least common multiple.

Theorem 27.1.5. *Let $a, b \in \mathbb{Z}$, not both zero. For any $n \in \mathbb{Z}$, we have*

$$\operatorname{lcm}[a, b] \mid n \quad \textit{if and only if} \quad a \mid n \textit{ and } b \mid n.$$

Proof.

($\Rightarrow$): Suppose $\operatorname{lcm}[a, b] \mid n$. Since $a \mid \operatorname{lcm}[a, b]$ and $b \mid \operatorname{lcm}[a, b]$, the transitivity of divisibility implies that $a \mid n$ and $b \mid n$. Thus, n is a common multiple of a and b.

($\Leftarrow$): Suppose $a \mid n$ and $b \mid n$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $0 \leq r < \operatorname{lcm}[a, b]$ such that $n = q \cdot \operatorname{lcm}[a, b] + r$. Since $a \mid n$ and $a \mid \operatorname{lcm}[a, b]$, we have $a \mid (n - q \cdot \operatorname{lcm}[a, b])$, implying $a \mid r$ by the properties of divisibility. A similar argument shows that $b \mid r$.

Since $0 \leq r < \text{lcm}[a, b]$ and r is a common multiple of a and b, it follows that $r = 0$. Hence, $\text{lcm}[a, b] \mid n$.

□

The following corollaries capture additional useful properties of the least common multiple. Their proofs are left as exercises.

Corollaries 27.1.6. *Let $a, b \in \mathbb{Z}$, not both zero. Then:*

1. $\text{lcm}[a, b] = |b|$ *if and only if* $a \mid b$.
2. *For any* $m \in \mathbb{Z}^+$, $\text{lcm}[ma, mb] = m \cdot \text{lcm}[a, b]$.

Exercise 27.1.7. Prove the previous corollaries.

The next theorem establishes a fundamental relationship between the greatest common divisor and the least common multiple.

Theorem 27.1.8 (GCD-LCM Theorem)**.** *For any positive integers a and b, we have*

$$\gcd(a, b) \cdot \text{lcm}[a, b] = ab.$$

Proof. Homework □

Note. To compute the least common multiple of two integers, no new algorithm is required. Once the greatest common divisor is known, the least common multiple can be determined directly using the GCD-LCM relationship.

27.2. Prime Factorizations

Prime numbers are often referred to as the building blocks of the integers. One of the most significant properties of integers is that every positive integer greater than 1 can be expressed as a product of prime numbers in exactly one way, up to the order of the factors. This result is known as the Fundamental Theorem of Arithmetic. The decomposition of integers into their prime factors is a powerful tool in mathematics, with applications ranging from simplifying fractions to enabling secure encryption methods. The key result needed to establish this theorem is derived from Bézout's Lemma.

Theorem 27.2.1 (Euclid's Lemma)**.** *Let $a, b, c \in \mathbb{Z}$. If a and b are relatively prime (i.e., $\gcd(a, b) = 1$) and $a \mid bc$, then $a \mid c$.*

Proof. Let $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a \mid bc$. Since $\gcd(a, b) = 1$, Bézout's Lemma guarantees the existence of integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Fix such values of m and n. Since $a \mid bc$, there exists some $k \in \mathbb{Z}$ such that $bc = ak$. Multiplying both sides of $am + bn = 1$ by c gives

$$amc + bnc = c.$$

Substituting $bc = ak$ into the equation, we get

$$c = amc + akn = a(mc + kn).$$

Thus, $a \mid c$, as required. □

The following corollary is a special case of Euclid's Lemma when a is a prime number.

Corollary 27.2.2. *Let $p, b, c \in \mathbb{Z}$ with p prime. If $p \mid bc$, then $p \mid b$ or $p \mid c$.*

28. November 5

28.1. Prime Factorizations

We now have the necessary tools to establish the Fundamental Theorem of Arithmetic.

Theorem 28.1.1 (Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be uniquely written as a product of prime numbers, up to the order of the prime factors.*

In other words, if

$$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$$

for prime numbers p_i and q_j such that $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$ and $p_i = q_i$ for each $i \in [r]$.

Proof.
Existence – This has already been established in Theorem 11.1.7.

Uniqueness – Suppose, for the sake of contradiction, that there exists a positive integer n such that $n > 1$ and n has two distinct prime factorizations. Let n_0 be the smallest such integer, according to the well-ordering property. Then, there exist positive integers $k, \ell \in \mathbb{Z}^+$ and prime numbers p_i and q_j for $1 \leq i \leq k$ and $1 \leq j \leq \ell$ such that

$$n_0 = \prod_{i=1}^{k} p_i = \prod_{j=1}^{\ell} q_j.$$

We consider two cases:

- Case 1: $k = 1$ or $\ell = 1$. Without loss of generality, assume $k = 1$. Then

  $$n_0 = p_1 = \prod_{j=1}^{\ell} q_j.$$

  Since p_1 is prime, it must be that $\ell = 1$ and hence $n_0 = p_1 = q_1$. This contradicts the assumption that the prime factorizations were distinct.

- Case 2: $k, \ell \geq 2$. Since $p_1 \mid n_0$, it follows that $p_1 \mid \prod_{j=1}^{\ell} q_j$. Because p_1 is prime, the corollary to Euclid's Lemma implies that there exists some $j \in [\ell]$ such that $p_1 \mid q_j$. By relabeling the q_j's if necessary, we may assume that $p_1 \mid q_1$. This implies that $q_1 = p_1$ since q_1 is prime. Then $\frac{n_0}{p_1}$ is an integer greater than 1, and

$$\frac{n_0}{p_1} = \prod_{i=2}^{k} p_i = \prod_{j=2}^{\ell} q_j.$$

  Since $k, \ell \geq 2$, this shows that $\frac{n_0}{p_1}$ has two distinct prime factorizations. But $\frac{n_0}{p_1} < n_0$, contradicting the assumption that n_0 was the smallest integer greater than 1 with two distinct prime factorizations.

Since these are the only two cases and they both lead to contradictions, we conclude that every integer $n > 1$ can be written *uniquely* as a product of primes. □

Examples 28.1.2.

1. $240 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^4 \cdot 3 \cdot 5$.

   Moreover, this is the only way to factor 240 into a product of prime numbers. Viewing the prime numbers as the building blocks, we see that 240 is composed of 4 copies of 2, 1 copy of 3, and 1 copy of 5.

2. $289 = 17 \cdot 17 = 17^2$

3. $1001 = 7 \cdot 11 \cdot 13$

Our next result establishes a fact that we have been assuming implicitly for some time.

Corollary 28.1.3 (Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Proof. Assume, for the sake of contradiction, that there are only finitely many prime numbers, say n primes for some $n \in \mathbb{Z}^+$. List these primes as

$$p_1, p_2, \ldots, p_n.$$

Define $P \in \mathbb{N}$ to be one more than the product of these primes, i.e.,

$$P = \left(\prod_{i=1}^{n} p_i \right) + 1 = p_1 p_2 \cdots p_n + 1.$$

Since $P > 1$, the Fundamental Theorem of Arithmetic implies that P has at least one prime divisor. Given that there are only finitely many primes, it follows that $p_j \mid P$ for some $j \in \{1, 2, \ldots, n\}$. Thus, we can write $P = p_j k$ for some $k \in \mathbb{Z}$.

However, p_j also divides $\prod_{i=1}^{n} p_i$ (as p_j is one of the factors in the product), so we can express $\prod_{i=1}^{n} p_i = p_j \ell$ for some $\ell \in \mathbb{Z}$. Consequently, we have

$$1 = P - \prod_{i=1}^{n} p_i = p_j(k - \ell),$$

which implies $p_j \mid 1$. This is a contradiction, as no prime number divides 1. Therefore, our original assumption must be false, and there are indeed infinitely many prime numbers. □

Note. This proof shows that if $p_1, \ldots, p_n$ are the first n prime numbers, then the next prime could be as large as

$$P = \left(\prod_{i=1}^{n} p_i \right) + 1.$$

However, this is a significant overestimate. For example, this method would imply that $p_{10} \leq 223092871$, while in reality, $p_{10} = 29$.

28.1.1. Divisors

Let $\mathbb{P}$ be the set of prime numbers. For each $p \in \mathbb{P}$ and $n \in \mathbb{Z}^+$, define

$$v_p(n) = \max\{a \in \mathbb{N} \mid p^a \text{ divides } n\}$$

as the largest power of p dividing n. If a, b, and n are positive integers such that $n = ab$, then for all $p \in \mathbb{P}$, we have $v_p(n) = v_p(a) + v_p(b)$. Hence, $v_p(a) \leq v_p(n)$. This implies that if n has a prime factorization

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$

then we can express a as

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

for some a_i where $0 \leq a_i \leq n_i$ for each $1 \leq i \leq k$. (Note that we allow $a_i = 0$ for any or all values of i.) Since any positive divisor must be of this form, and any integer of this form is indeed a divisor of n, we have now classified all divisors of n. This allows us to count the number of divisors of n.

- For an arbitrary divisor a of n, there are $n_i + 1$ possible values for $v_{p_i}(a)$.
- Since there are k distinct primes in the prime factorization of n, the total number of divisors of n is given by $\prod_{i=1}^{k} (n_i + 1)$.

GCDs and LCMs Revisited

We can use the above ideas to provide an alternative characterization of GCDs and LCMs.

Theorem 28.1.4. *Let $a, b \in \mathbb{Z}$ be greater than 1. Further, let $\{p_1, \ldots, p_n\}$ be the set of all prime factors of either a or b. Then we can express a and b as*

$$a = \prod_{i=1}^{n} p_i^{a_i} \quad \text{and} \quad b = \prod_{i=1}^{n} p_i^{b_i},$$

where $a_i \geq 0$ and $b_i \geq 0$ for $1 \leq i \leq n$. Then

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}},$$
$$\operatorname{lcm}[a, b] = \prod_{i=1}^{n} p_i^{\max\{a_i, b_i\}}.$$

Proof. Let $d = \gcd(a, b)$. For each $1 \leq i \leq n$, we have $v_{p_i}(d) \leq a_i$ and $v_{p_i}(d) \leq b_i$. Thus,

$$v_{p_i}(d) \leq \min\{a_i, b_i\}.$$

Moreover, $\prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$ divides a, as seen from

$$a = \left(\prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}} \right) \left(\prod_{i=1}^{n} p_i^{a_i - \min\{a_i, b_i\}} \right).$$

Similarly, $\prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$ divides b. Since d is the greatest common divisor of a and b, we must have $v_{p_i}(d) = \min\{a_i, b_i\}$ for all i. Therefore, $d = \prod_{i=1}^{n} p_i^{\min\{a_i, b_i\}}$.

A similar argument establishes the result for the least common multiple. □

Example 28.1.5. Consider the integers 720 and 700. We have

$$720 = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^0,$$
$$700 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1,$$
$$\gcd(720, 700) = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0,$$
$$\operatorname{lcm}[720, 700] = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^1.$$

Hence, $\gcd(720, 700) = 20$ and $\operatorname{lcm}(720, 700) = 25200$.

The GCD-LCM Theorem 27.1.8 follows immediately from the previous theorem.

Corollary 28.1.6 (GCD-LCM Theorem)**.** *For all $a, b \in \mathbb{Z}^+$, we have*

$$ab = \gcd(a, b) \cdot \operatorname{lcm}[a, b].$$

Exercise 28.1.7.

(a) Prove that a positive integer n is a perfect square if and only if the exponent of each prime factor of n is even.

(b) Prove that if a and b are coprime positive integers and their product is a perfect square, then a and b are themselves perfect squares.

(c) Prove that if a and b are positive integers and ab is a perfect square, then $a = dm^2$ and $b = dn^2$ where $d = \gcd(a, b)$, for some coprime integers m and n.

(d) Reprove the irrationality of $\sqrt{2}$ in the following way:

- Assume for the sake of contradiction that $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ are coprime. Use part (a) to arrive at a contradiction.

Exercise 28.1.8. Use the fundamental theorem of arithmetic to prove that $17^{1/3}$ is irrational.

28.2. Modular Arithmetic

Recall: For $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$, we say that a *is congruent to* b *modulo* m, denoted $a \equiv b \pmod{m}$, if and only if $m \mid (a-b)$. We proved in Theorem 18.1.3 that congruence modulo m is an equivalence relation. The set of equivalence classes (often called *congruence classes* in this context) is denoted by

$$\mathbb{Z}/m\mathbb{Z} = \{[a]_m \mid a \in \mathbb{Z}\}.$$

In computer science, "mod" is often treated as an operation that takes an integer a as input and returns the remainder r when a is divided by m. As a relation, this means $a \equiv r \pmod{m}$ (equivalently, $[a]_m = [r]_m$). This interpretation can be justified by the following theorem.

Theorem 28.2.1. *For all $a, b \in \mathbb{Z}$ and all $m \in \mathbb{Z}^+$, we have*

$$a \equiv b \pmod{m} \iff a \text{ and } b \text{ have the same remainder when divided by } m.$$

Proof. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. By the Division Algorithm, there exist unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that

$$a = mq_1 + r_1 \quad \text{and} \quad b = mq_2 + r_2,$$

where $0 \leq r_1 < m$ and $0 \leq r_2 < m$. We will show that $a \equiv b \pmod{m}$ if and only if $r_1 = r_2$.

($\Rightarrow$): Suppose $a \equiv b \pmod{m}$. Then $m \mid (a - b)$, so there exists $k \in \mathbb{Z}$ such that $a - b = mk$. Substituting our expressions for a and b, we get

$$mk = m(q_1 - q_2) + (r_1 - r_2).$$

Solving for $r_1 - r_2$ gives

$$r_1 - r_2 = m(k - (q_1 - q_2)),$$

which shows that $m \mid (r_1 - r_2)$. Since $0 \leq r_1, r_2 < m$, we have $-m < r_1 - r_2 < m$, and the only multiple of m in this range is 0. Hence $r_1 - r_2 = 0$, so $r_1 = r_2$.

($\Leftarrow$): Suppose $r_1 = r_2$. Then

$$a - b = m(q_1 - q_2),$$

which implies $m \mid (a - b)$, and therefore $a \equiv b \pmod{m}$.

□

The following corollary is immediate.

Corollary 28.2.2. *Let $m \in \mathbb{Z}^+$. Every integer is congruent to exactly one element of the set $\{0, 1, \ldots, m-1\}$ modulo m. Equivalently,*

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

The set $\{0, 1, \ldots, m-1\}$ is an example of what we call a *complete set of residues* modulo m.

Definition. For $m \in \mathbb{Z}^+$, a set $\{a_1, \ldots, a_m\} \subset \mathbb{Z}$ is called a *complete set of residues modulo m* if every integer is congruent to exactly one element of $\{a_1, \ldots, a_m\}$ modulo m.

Examples 28.2.3. There are infinitely many complete sets of residues modulo m, but some are more commonly used than others.

- **Least Nonnegative Residues modulo** m: $\{0, 1, \ldots, m-1\}$.
- **Least Positive Residues modulo** m: $\{1, 2, \ldots, m\}$.
- **Least Absolute Residues modulo** m:
  - If m is odd: $\{0, 1, -1, 2, -2, \ldots, \frac{m-1}{2}, -\frac{m-1}{2}\}$.
  - If m is even: $\{0, 1, -1, 2, -2, \ldots, \frac{m-2}{2}, -\frac{m-2}{2}, \frac{m}{2}\}$.

Example 28.2.4. The sets $\{0, 1, 2, 3, 4\}$ and $\{0, 1, -1, 2, -2\}$ both form complete sets of residues modulo 5.

Exercise 28.2.5. For each part below, determine whether the given set of integers S forms a complete set of residues modulo m.

(a) $S = \{4, 21, 104\}$, $m = 3$

(b) $S = \{-33, -5, -2, 2, 5, 12, 41\}$, $m = 8$

(c) $S = \{-25, -15, -5, 0, 10, 20\}$, $m = 6$

(d) $S = \{-68, -14, -6, 4, 40, 63, 83\}$, $m = 7$

29. November 7

29.1. Modular Arithmetic

The main advantage of working with congruences is that it simplifies arithmetic involving remainders, as the standard rules for addition, subtraction, and multiplication still apply. Division, however, requires special consideration, which we will address later.

Theorem 29.1.1 (Modular Arithmetic Lemma)**.** *Let $m \in \mathbb{Z}^+$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:*

1. $a \pm c \equiv b \pm d \pmod{m}$
2. $ac \equiv bd \pmod{m}$

Proof. Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $m \mid (a - b)$ and $m \mid (c - d)$, so there exist integers $k, \ell \in \mathbb{Z}$ such that $a - b = mk$ and $c - d = m\ell$. We now verify each claim.

1. Using $a - b = mk$ and $c - d = m\ell$, we find

$$(a \pm c) - (b \pm d) = (a - b) \pm (c - d) = mk \pm m\ell = m(k \pm \ell).$$

   Hence $m \mid (a \pm c - (b \pm d))$, so $a \pm c \equiv b \pm d \pmod{m}$.

2. Substituting $a = b + mk$ and $c = d + m\ell$, we have

$$\begin{aligned} ac &= (b + mk)(d + m\ell) \\ &= bd + m(kd + \ell b + mk\ell). \end{aligned}$$

   Thus $m \mid (ac - bd)$, so $ac \equiv bd \pmod{m}$.

□

Remark. Another way to interpret Theorem 29.1.1 is that we have defined addition and multiplication on $\mathbb{Z}/m\mathbb{Z}$ by

$$\begin{aligned} [a]_m + [b]_m &= [a + b]_m, \\ [a]_m \cdot [b]_m &= [ab]_m. \end{aligned}$$

The Modular Arithmetic Lemma guarantees that these operations are *well-defined*: the results do not depend on the choice of representatives for the equivalence classes. Consequently, $\mathbb{Z}/m\mathbb{Z}$ carries a natural algebraic structure.

Let us now explore some examples illustrating what we can and cannot do as a result of the Modular Arithmetic Lemma.

Examples 29.1.2.

- For $x \in \mathbb{Z}$, $x + 10 \equiv x + 3 \pmod 7$ since $10 \equiv 3 \pmod 7$. This shows that we can reduce the constants appearing in a sum modulo 7.
- For $x, y \in \mathbb{Z}$, if $x \equiv y \pmod 7$, then $x+3 \equiv y+3 \pmod 7$. This demonstrates that we can add the same number to both sides of a congruence, just as with ordinary equations, and the equivalence remains valid.
- For $x, y \in \mathbb{Z}$, if $x + 3 \equiv y \pmod 7$, then $x \equiv y - 3 \pmod 7$. We can therefore subtract the same number from both sides of a congruence and maintain the equivalence. Moreover, since $-3 \equiv 4 \pmod 7$, we could also write $x \equiv y + 4 \pmod 7$.
- For $x \in \mathbb{Z}$, if $x \equiv 3 \pmod 7$, then $2x \equiv 6 \pmod 7$. This shows that we can multiply both sides of a congruence by 2 without breaking equivalence. Since $6 \equiv -1 \pmod 7$, this can also be written as $2x \equiv -1 \pmod 7$.

The following corollary follows from a straightforward induction argument, which we leave to the reader.

Corollary 29.1.3. *Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. If $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$ for all $n \in \mathbb{Z}^+$.*

Exercise 29.1.4. Prove that $4^n \equiv 1 + 3n \pmod 9$ for all $n \in \mathbb{N}$.

29.1.1. The Problem with Division

We have established that addition, subtraction, and multiplication are well-defined operations modulo m, but division remains problematic. The following examples illustrate why:

- If $2x \equiv 1 \pmod m$, we **cannot** conclude that $x \equiv \frac{1}{2} \pmod m$, since $\frac{1}{2} \notin \mathbb{Z}$, and congruences modulo m are defined only over integers. (Recall that it is an equivalence relation on $\mathbb{Z}$.)
- If $6x \equiv 21 \pmod m$, we **cannot** divide both sides by 3 directly. For example, $6 \equiv 21 \pmod{15}$, but $2 \not\equiv 7 \pmod{15}$. However, we do have $2 \equiv 7 \pmod{\frac{15}{3}}$.

The next theorem clarifies how certain forms of division can still be managed within modular arithmetic.

Theorem 29.1.5 (Cancellation Law)**.** *For $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, if $d = \gcd(c, m)$ and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{\frac{m}{d}}$.*

Proof. Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Assume $ac \equiv bc \pmod{m}$, which implies that $m \mid (ac - bc)$, or equivalently, $c(a-b) = mk$ for some $k \in \mathbb{Z}$. Let $d = \gcd(c, m)$. Dividing both sides of the equation by d, we obtain

$$\left(\frac{c}{d}\right)(a-b) = \left(\frac{m}{d}\right)k.$$

Thus, $\frac{m}{d} \mid \left(\frac{c}{d}\right)(a-b)$. By Theorem 26.1.2, we know that $\gcd\left(\frac{c}{d}, \frac{m}{d}\right) = 1$, so by Euclid's Lemma it follows that $\frac{m}{d} \mid (a-b)$. Hence, $a \equiv b \pmod{\frac{m}{d}}$. □

Example 29.1.6.

- Consider the congruence $24x \equiv 18y \pmod{45}$. We wish to divide both sides by 6 to simplify. Since $\gcd(6, 45) = 3$, the modulus reduces by this factor, yielding

$$4x \equiv 3y \pmod{15}.$$

- For $24x \equiv 18y \pmod{46}$, we have $\gcd(6, 46) = 2$, so dividing by 6 gives

$$4x \equiv 3y \pmod{23}.$$

- Finally, if $24x \equiv 18y \pmod{47}$, then $\gcd(6, 47) = 1$ (since 47 is prime). In this case, the modulus remains unchanged:

$$4x \equiv 3y \pmod{47}.$$

Exercise 29.1.7. Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $\gcd(a, m) = 1$.

(a) Prove that for all $k, \ell \in \mathbb{Z}$, $k \equiv \ell \pmod{m}$ if and only if $ak \equiv a\ell \pmod{m}$.

(b) Prove that the following set forms a complete set of residues modulo m.

$$\{n \in \mathbb{Z} \mid \exists k \in [m], n = ak + b\}$$

29.1.2. Multiplicative Inverses

There is another analogue of division in modular arithmetic that applies when the divisor has certain properties. Recall that for a nonzero real number x, dividing by x is equivalent to multiplying by its *multiplicative inverse* $y = \frac{1}{x}$, where $xy = 1$. The number

y is called the *multiplicative inverse* of x because their product equals one. We now wish to generalize this idea to congruences modulo m.

We investigate multiplicative inverses in $\mathbb{Z}/m\mathbb{Z}$. Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. We ask: under what conditions does $[a]_m$ have a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$? Equivalently, for which integers a does there exist an integer b such that $ab \equiv 1 \pmod{m}$? If such a b exists, we denote it by $b \equiv a^{-1} \pmod{m}$.

Note that a^{-1} does *not* represent the rational number $\frac{1}{a}$ (which may not be an integer); instead, it denotes the multiplicative inverse of a modulo m. This notation parallels that used for inverses of bijections.

Theorem 29.1.8 (MIRP Theorem)**.** *Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Then a and m are relatively prime if and only if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$.*

Equivalently, $\gcd(a, m) = 1$ if and only if $[a]_m$ has a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$.

Before proving the theorem, let us consider a few examples.

Examples 29.1.9.

- There is no solution to $6x \equiv 1 \pmod{21}$ because $\gcd(6, 21) = 3 \neq 1$.
- There is a solution to $5x \equiv 1 \pmod{21}$ since $\gcd(5, 21) = 1$. Indeed,

  $$5 \cdot 17 = 85 \equiv 1 \pmod{21}.$$

  Thus, $5^{-1} \equiv 17 \pmod{21}$. By the Modular Arithmetic Lemma (Theorem 29.1.1), the congruence $5x \equiv 1 \pmod{21}$ holds for all $x \in [17]_{21}$.

  Alternatively, we can express this multiplicative inverse in $\mathbb{Z}/21\mathbb{Z}$ as

  $$[5]_{21} \cdot [17]_{21} = [1]_{21}.$$

We now proceed with the proof of the MIRP Theorem.

Proof. Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.

($\Rightarrow$): Suppose $\gcd(a, m) = 1$. By Bézout's Lemma, there exist integers k, ℓ such that $ak + m\ell = 1$. Fix such k, ℓ. Then $ak + m\ell \equiv ak \pmod{m}$, so $ak \equiv 1 \pmod{m}$. Hence, a has a multiplicative inverse modulo m.

($\Leftarrow$): Conversely, assume there exists $k \in \mathbb{Z}$ such that $ak \equiv 1 \pmod{m}$. Then $m \mid (ak - 1)$, so $ak - 1 = m\ell$ for some $\ell \in \mathbb{Z}$. Rearranging gives $ak + m(-\ell) = 1$, which implies $\gcd(a, m) = 1$ by Bézout's Lemma, since 1 is a linear combination of a and m.

□

The following corollary states that if a multiplicative inverse exists, it is unique modulo m.

Corollary 29.1.10. *Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. If $k, \ell \in \mathbb{Z}$ satisfy $ak \equiv 1 \pmod{m}$ and $a\ell \equiv 1 \pmod{m}$, then $k \equiv \ell \pmod{m}$.*

Example 29.1.11. Find all $x \in \mathbb{Z}$ such that $4x \equiv 5 \pmod{7}$.

First, note that 4 is invertible modulo 7 since $\gcd(4, 7) = 1$. We find that $4^{-1} \equiv 2 \pmod{7}$ because $4 \cdot 2 = 8 \equiv 1 \pmod{7}$.

Now, let $x \in \mathbb{Z}$ satisfy $4x \equiv 5 \pmod{7}$. Multiplying both sides by 2 gives

$$2 \cdot 4x \equiv 2 \cdot 5 \pmod{7}.$$

Simplifying, we obtain

$$x \equiv 3 \pmod{7}.$$

Therefore, the set of solutions is

$$\{x \in \mathbb{Z} \mid 4x \equiv 5 \pmod{7}\} = [3]_7.$$

The following corollary characterizes when a linear congruence modulo m has a solution.

Corollary 29.1.12. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$.*

Proof. You will work through this proof in recitation. □

Finding Multiplicative Inverses

Question: Given $\gcd(a, m) = 1$, how do we find a multiplicative inverse of a modulo m?

Answer: There are several ways to do this.

1. **Mental Math**.

   If m is small, the most efficient method may be to solve mentally or use guess-and-check, since there are only a few possible residues.

Example 29.1.13. Find $x \in \mathbb{Z}$ such that $7x \equiv 1 \pmod{15}$.

Considering the set of least positive residues modulo 15, the only possible inverses of 7 modulo 15 are the integers between 1 and 15 that are relatively prime to 15:

$$\{1, 2, 4, 7, 8, 11, 13, 14\}.$$

We can rule out 1 and 14, since

$$\begin{aligned} 7 \cdot 1 &\equiv 7 \pmod{15}, \\ 7 \cdot 14 \equiv 7(-1) &\equiv -7 \pmod{15}. \end{aligned}$$

Additionally, we observe that

$$7 \cdot 2 = 14 \equiv -1 \pmod{15}.$$

From this, we deduce that

$$7 \cdot (-2) = -14 \equiv 1 \pmod{15}.$$

Thus,

$$7^{-1} \equiv -2 \equiv 13 \pmod{15}.$$

Example 29.1.14. Find $x \in \mathbb{Z}$ such that $7x \equiv 1 \pmod{31}$.

We want to find x such that $7x = 31\ell + 1$ for some $\ell \in \mathbb{Z}$.

We can see that $7 \nmid (31 \cdot 1 + 1)$ but $7 \mid (31 \cdot 2 + 1)$. Hence,

$$7 \cdot 9 = 63 \equiv 1 \pmod{31}.$$

This implies that $7^{-1} \equiv 9 \pmod{31}$.

Exercise 29.1.15. Use mental math or guess-and-check to find the multiplicative inverse of a modulo m for each of the following pairs (a, m).

(a) $a = 4$, $m = 9$ (b) $a = 5$, $m = 22$ (c) $a = 9$, $m = 41$

To handle larger values of m, there are two primary options we will consider:

(2) **Use the Euclidean Algorithm.**

Find $x, y \in \mathbb{Z}$ such that $ax + my = 1$. This implies $ax \equiv 1 \pmod{m}$, and hence $a^{-1} \equiv x \pmod{m}$.

Example 29.1.16. Find an inverse of 65 modulo 101.

First, perform the Euclidean algorithm:

$$\begin{aligned} 101 &= 65(1) + 36, \\ 65 &= 36(1) + 29, \\ 36 &= 29(1) + 7, \\ 29 &= 7(4) + 1, \\ 7 &= 1(7) + 0. \end{aligned}$$

Thus, $\gcd(65, 101) = 1$. Back-substituting, we find:

$$\begin{aligned} 1 &= 29 + 7(-4) \\ &= 29 + (36 - 29)(-4) \\ &= 36(-4) + 29(5) \\ &= 36(-4) + (65 - 36)(5) \\ &= 65(5) + 36(-9) \\ &= 65(5) + (101 - 65)(-9) \\ &= 101(-9) + 65(14). \end{aligned}$$

Hence,

$$1 = 101(-9) + 65(14),$$

which implies $65 \cdot 14 \equiv 1 \pmod{101}$, and therefore

$$65^{-1} \equiv 14 \pmod{101}.$$

Exercise 29.1.17. Use the Euclidean algorithm to find a multiplicative inverse of a modulo m for each of the following pairs (a, m).

(a) $a = 37$, $m = 101$ (b) $a = 123$, $m = 256$

Exercise 29.1.18.

(a) Use the Euclidean algorithm to determine $\gcd(999, 102)$.

(b) Find all $x, y \in \mathbb{Z}$ such that $999x + 102y = \gcd(999, 102)$.

(c) Find all integer solutions, if any, to the congruence $102x+20 \equiv 461 \pmod{999}$.

③ **Use the *order* of an integer modulo m.**

This will be our next topic of discussion.

30. November 10

30.1. Modular Arithmetic

30.1.1. Order of an Element Modulo m

In this section, we introduce the *order* of an element modulo m and some key related theorems: Fermat's Little Theorem and Euler's Theorem.

We begin with an important existence result.

Theorem 30.1.1. *Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ be relatively prime to m. Then there exists a positive integer n such that $a^n \equiv 1 \pmod{m}$.*

Proof. Consider the following $m+1$ integers:

$$a^1,\ a^2,\ a^3,\ \ldots,\ a^m,\ a^{m+1}.$$

Since $|\mathbb{Z}/m\mathbb{Z}| = m$, the Pigeonhole Principle implies that there exist distinct integers k, ℓ with $a^k \equiv a^\ell \pmod{m}$. Without loss of generality, assume $k > \ell$. Multiplying both sides by $(a^{-1})^\ell$ gives

$$a^{k-\ell} \equiv 1 \pmod{m}.$$

Hence, $n = k - \ell \in \mathbb{Z}^+$ satisfies the desired property. □

Once such an integer n is found satisfying $a^n \equiv 1 \pmod{m}$, we can immediately determine a multiplicative inverse of a modulo m.

Corollary 30.1.2. *Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ be relatively prime to m. If $n \in \mathbb{Z}^+$ satisfies $a^n \equiv 1 \pmod{m}$, then $a^{-1} \equiv a^{n-1} \pmod{m}$.*

The theorem guarantees that whenever a is relatively prime to m, there exists some positive integer n for which $a^n \equiv 1 \pmod{m}$. We now define the smallest such n.

Definition. Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ be relatively prime to m. The *order of a modulo m*, denoted $\text{ord}_m(a)$, is the smallest positive integer n such that

$$a^n \equiv 1 \pmod{m}.$$

Example 30.1.3. To determine $\text{ord}_5(2)$, compute successive powers of 2 modulo 5:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{5}, \\ 2^2 &\equiv 4 \equiv -1 \pmod{5}, \\ 2^3 &\equiv 8 \equiv 3 \pmod{5}, \\ 2^4 &\equiv 16 \equiv 1 \pmod{5}. \end{aligned}$$

Since 4 is the smallest positive integer such that $2^n \equiv 1 \pmod{5}$, we conclude that

$$\text{ord}_5(2) = 4.$$

There are infinitely many other values of n such that $2^n \equiv 1 \pmod{5}$:

$$2^8 \equiv 1 \pmod{5}, \quad 2^{12} \equiv 1 \pmod{5},$$

$$\text{and in general, } 2^{4k} \equiv 1 \pmod{5} \text{ for all } k \geq 1.$$

Fermat's Little Theorem

When the modulus is prime, any integer not divisible by it is coprime to the modulus, giving the following result.

Theorem 30.1.4 (Fermat's Little Theorem)**.** *If p is a prime number and $a \in \mathbb{Z}$ is coprime to p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let p be a prime and $a \in \mathbb{Z}$ be coprime to p. For any $i, j \in \{0, 1, 2, \ldots, p-1\}$, we have $ai \equiv aj \pmod{p}$ if and only if $i \equiv j \pmod{p}$ by the Cancellation Law, since $\gcd(a, p) = 1$. Thus, $\{0, 1, 2, \ldots, p-1\}$ and the set

$$\{0, a, 2a, \ldots, (p-1)a\}$$

form a complete residue system modulo p.

Removing 0 from each set, we have that the sets $\{1, 2, \ldots, p-1\}$ and $\{a, 2a, \ldots, (p-1)a\}$ represent the same set of residues modulo p, possibly in a different order. This yields the following congruence

$$a \cdot (2a) \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

which can be rewritten as

$$a^{p-1}(1 \cdot 2 \cdots (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Since p is prime, $\gcd(i, p) = 1$ for each $i \not\equiv 0 \pmod{p}$, and we can cancel these terms from both sides to conclude that

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Corollary 30.1.5. *Let p be a prime and $a \in \mathbb{Z}$.*

1. *If $\gcd(a, p) = 1$, then $ord_p(a) \mid p - 1$.*
2. *$a^p \equiv a \pmod{p}$ (even if a is not coprime to p).*

Exercise 30.1.6. Use Fermat's little theorem to find the least nonnegative residue of a modulo m for each of the following:

(a) $a = 5^{100}$, $m = 7$

(b) $a = 6^{2000}$, $m = 11$

(c) $a = 3^{999999999}$, $m = 7$

(d) $a = 2^{1000001}$, $m = 17$

Exercise 30.1.7.

(a) Determine the order of 4 modulo 19.

(b) Use your answer from part (a) to find 4^{-1} modulo 19. Give your answer as the least nonnegative residue.

(c) Solve the congruence equation:

$$4x \equiv 11 \pmod{19}$$

Give your final answer in the form $x \equiv b \pmod{19}$, where b is the least nonnegative residue.

Exercise 30.1.8. Prove that if $n \in \mathbb{Z}$ is odd and $3 \nmid n$ then $n^2 \equiv 1 \pmod{24}$.

Exercise 30.1.9. Prove that $30 \mid n^9 - n$ for all $n \in \mathbb{Z}$.

Euler's Theorem

What if the modulus is not prime? To handle this case, we introduce *Euler's totient function*.

Definition. *Euler's totient function* $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as

$$\begin{aligned}\phi(n) &= |\{k \in [n] \mid \gcd(k, n) = 1\}| \\ &= \text{The number of integers } 1 \leq k \leq n \text{ coprime to } n \\ &= \text{The number of elements in } \mathbb{Z}/n\mathbb{Z} \text{ with multiplicative inverses.}\end{aligned}$$

Examples 30.1.10.

$$\begin{aligned}\phi(3) &= |\{k \in [3] \mid \gcd(k, 3) = 1\}| = |\{1, 2\}| = 2, \\ \phi(4) &= |\{k \in [4] \mid \gcd(k, 4) = 1\}| = |\{1, 3\}| = 2, \\ \phi(5) &= |\{k \in [5] \mid \gcd(k, 5) = 1\}| = |\{1, 2, 3, 4\}| = 4, \\ \phi(6) &= |\{k \in [6] \mid \gcd(k, 6) = 1\}| = |\{1, 5\}| = 2, \\ \phi(7) &= |\{k \in [7] \mid \gcd(k, 7) = 1\}| = |\{1, 2, 3, 4, 5, 6\}| = 6.\end{aligned}$$

If the prime factorization of n is known, there is a useful formula for computing $\phi(n)$. This formula follows from the two lemmas below.

Lemma 30.1.11. *If p is a prime number and $a \in \mathbb{Z}^+$, then $\phi(p^a) = p^a - p^{a-1}$.*

Proof. Let $p, a \in \mathbb{Z}^+$ with p prime. Since the only prime factor of p^a is p, for any $n \in \mathbb{Z}$, $\gcd(n, p^a) \neq 1$ if and only if $p \mid n$. We use this observation in the following chain of equalities.

$$\begin{aligned}\phi(p^a) &= |\{m \in \mathbb{Z} \mid 1 \leq m \leq p^a \wedge \gcd(m, p^a) = 1\}| \\ &= p^a - |\{m \in \mathbb{Z} \mid 1 \leq m \leq p^a \wedge p \mid m\}| \\ &= p^a - |\{kp \mid 1 \leq k \leq p^{a-1}\}| \\ &= p^a - p^{a-1}.\end{aligned}$$

□

Lemma 30.1.12. *If $a, b \in \mathbb{Z}^+$ are coprime, then $\phi(ab) = \phi(a)\phi(b)$.*

Proof. You will prove this in your homework. □

Combining Lemmas 30.1.11 and 30.1.12, we get a formula for computing $\phi(n)$ for any positive integer n.

Euler's Totient Formula

Let $n \in \mathbb{Z}^+$ have canonical prime factorization $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Then

$$\begin{aligned}
\phi(n) &= \phi(p_1^{n_1})\phi(p_2^{n_2}) \cdots \phi(p_k^{n_k}) \\
&= \left(p_1^{n_1} - p_1^{n_1-1}\right)\left(p_2^{n_2} - p_2^{n_2-1}\right) \cdots \left(p_k^{n_k} - p_k^{n_k-1}\right) \\
&= \prod_{i=1}^{k} \left(p_i^{n_i} - p_i^{n_i-1}\right) \\
&= n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

Example 30.1.13. Consider $360 = 2^3 \cdot 3^2 \cdot 5^1$. Then

$$\phi(360) = \phi(2^3)\phi(3^2)\phi(5^1) = (8-4)(9-3)(5-1) = \boxed{96}$$

Exercise 30.1.14. Find the value of the $\phi(n)$ for each of the following values of n.

(a) 100

(b) 256

(c) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

(d) 20!

Exercise 30.1.15. Find all $n \in \mathbb{Z}^+$ such that $\phi(n) = 12$. Be sure to prove that you found all solutions.

Exercise 30.1.16. Show that there is no positive integer n such that $\phi(n) = 14$.

31. November 12

31.1. Modular Arithmetic

31.1.1. Order of an Element Modulo m

Euler's Theorem

Now that we have Euler's totient function, we can state and prove the analogue to Fermat's Little Theorem.

Theorem 31.1.1 (Euler's Theorem)**.** *If $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ is coprime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$.*

The proof follows similarly to the proof of Fermat's Little Theorem.

Proof. Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a set of distinct residues coprime to m, called a *reduced residue system* modulo m. Since $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$ for each $1 \leq i \leq \phi(m)$, we have $\gcd(ar_i, m) = 1$ for each $1 \leq i \leq \phi(m)$. Then, by the Cancellation Law and the fact that the r_i's are distinct modulo m, we have

$$ar_i \equiv ar_j \pmod{m} \iff r_i \equiv r_j \pmod{m} \iff i = j.$$

Therefore, $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is also a reduced residue system modulo m. Thus,

$$\prod_{i=1}^{\phi(m)} ar_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

Applying the Cancellation Law to each r_i in the product yields

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

as desired. □

Definition. For $m \in \mathbb{Z}^+$, a *reduced residue system* modulo m is a set of $\phi(m)$-many integers such that each element is relatively prime to m, and no two different elements of the set are congruent modulo m.

We have corollaries similar to those from Fermat's Little Theorem.

Corollaries 31.1.2. *Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.*

1. *If $\gcd(a, m) = 1$, then $ord_m(a) \mid \phi(m)$.*
2. *If $\gcd(a, m) = 1$, then $a^{-1} \equiv a^{\phi(m)-1} \pmod{m}$.*

Example 31.1.3. Consider $m = 18 = 2 \cdot 3^2$. Then $\phi(18) = \phi(2)\phi(3^2) = (2-1)\cdot(9-3) = 6$. Thus, there are 6 values of n with $0 \leq n \leq 17$ that are coprime to 18. These values form a *reduced residue system*:

$$\{1, 5, 7, 11, 13, 17\}.$$

Each of these elements has an order (since they are coprime to 18), and their orders must divide 6. We proceed to find each of their orders:

$$\begin{aligned} \text{ord}_{18}(1) &= 1, \\ \text{ord}_{18}(5) &= 6, \\ \text{ord}_{18}(7) &= 3, \\ \text{ord}_{18}(11) &= 6, \\ \text{ord}_{18}(13) &= 3, \\ \text{ord}_{18}(17) &= 2. \end{aligned}$$

Exercise 31.1.4.

(a) Calculate $\phi(14)$ and list all elements in $[14]$ which are coprime to 14.

(b) Determine the multiplicative inverse of each integer from part (a).

(c) Find the least nonnegative residue of 9^{999999} modulo 14.

Exercise 31.1.5.

(a) Calculate $\phi(35)$ and list all elements in $[35]$ which are coprime to 35.

(b) Determine $\text{ord}_{35}(3)$, the order of 3 modulo 35.

(c) Find the least nonnegative residue of 3^{-1} modulo 35.

(d) Find the least nonnegative residue of 3^{100000} modulo 35.

Exercise 31.1.6.

(a) Calculate $\phi(50)$

(b) Determine $\text{ord}_{50}(7)$.

(c) Find the least nonnegative residue of 7^{-1} modulo 50.

(d) Find all integer solutions to the congruence $7x + 27 \equiv 4 \pmod{50}$.

Exercise 31.1.7. Let $m \in \mathbb{Z}$ with $m > 2$, and let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. Prove that $\sum_{i=1}^{\phi(m)} r_i \equiv 0 \pmod{m}$.

Exercise 31.1.8. Use Euler's theorem to prove that $51 \mid \left(10^{32n+9} - 7\right)$ for all $n \in \mathbb{N}$.

Exercise 31.1.9. Find all solutions, if any, to the following congruence equations.

(a) $3x \equiv 5 \pmod{7}$

(b) $100x - 2 \equiv 24 \pmod{12}$

(c) $15x \equiv 7 \pmod{32}$

(d) $22x \equiv 3 \pmod{40}$

(e) $39x \equiv 52 \pmod{130}$

(f) $80x \equiv 51 \pmod{171}$

Exercise 31.1.10. Find the least nonnegative residue of each of the following

(a) 100 modulo 13

(b) 99 modulo 28

(c) 103^{2025} modulo 48

(d) 3^{341} modulo 124

(e) $\sum_{k=1}^{100} k!$ modulo 7

(f) $\sum_{k=1}^{100} k!$ modulo 12

31.1.2. The Chinese Remainder Theorem

The Chinese Remainder Theorem is one of the most celebrated and widely applicable results in number theory. In its simplest form, it addresses how to find integers that satisfy multiple congruence conditions with different moduli. Beyond its theoretical importance, it has applications across many areas of mathematics and computer science, and it admits numerous generalizations.

Versions of this theorem were known in China as early as the 3rd century CE, where it was used to solve calendar and remainder problems, hence the name.

Examples 31.1.11.

1. Find all $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{3}$, and $x \equiv 1 \pmod{2}$.
2. Find all $x \in \mathbb{Z}$ such that $x^2 \equiv 1 \pmod{21}$.

Theorem 31.1.12 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}^+$ be pairwise relatively prime. Let $a_1, a_2, \ldots, a_r \in \mathbb{Z}$. The system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \cdots m_r$.

There are several ways to prove this theorem, but an inductive argument is both natural and illustrative of how we actually solve systems of congruences in practice.

Proof. We proceed by induction on the integer $r \geq 2$.

- **Base case:** $r = 2$. Let $a_1, a_2 \in \mathbb{Z}$ and $m_1, m_2 \in \mathbb{Z}^+$ with $\gcd(m_1, m_2) = 1$. Consider the system of congruences

  $$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

  Let $x \in \mathbb{Z}$ satisfy $x \equiv a_1 \pmod{m_1}$. This is equivalent to the existence of some integer y_1 such that $x = m_1 y_1 + a_1$. Fix y_1. We now seek conditions on x that ensure $x \equiv a_2 \pmod{m_2}$.

  Since $\gcd(m_1, m_2) = 1$, there exists $n_1 \in \mathbb{Z}$ such that $m_1 n_1 \equiv 1 \pmod{m_2}$ by the MIRP Theorem (29.1.8). Fix such an n_1. We then have the following logical equivalences:

  $$\begin{aligned} x \equiv a_2 \pmod{m_2} &\Leftrightarrow m_1 y_1 + a_1 \equiv a_2 \pmod{m_2} \\ &\Leftrightarrow m_1 y_1 \equiv a_2 - a_1 \pmod{m_2} \\ &\Leftrightarrow y_1 \equiv n_1(a_2 - a_1) \pmod{m_2} \\ &\Leftrightarrow y_1 = n_1(a_2 - a_1) + m_2 y_2 \text{ for some } y_2 \in \mathbb{Z} \\ &\Leftrightarrow x = m_1 n_1 (a_2 - a_1) + m_1 m_2 y_2 + a_1 \text{ for some } y_2 \in \mathbb{Z} \\ &\Leftrightarrow x \equiv m_1 n_1 (a_2 - a_1) + a_1 \pmod{m_1 m_2} \end{aligned}$$

  Thus, $x = m_1 n_1 (a_2 - a_1) + a_1$ is a solution to the system of congruences, and any solution must be congruent to this expression modulo $m_1 m_2$. Therefore, the system of congruences has a unique solution modulo $m_1 m_2$, as required.

It is worth checking that $x = m_1 n_1 (a_2 - a_1) + a_1$ actually solves this system. When working modulo m_1, we have

$$x = m_1 n_1 (a_2 - a_1) + a_1 \equiv 0 + a_1 \equiv a_1 \pmod{m_1}$$

Working modulo m_2, using $m_1 n_1 \equiv 1 \pmod{m_2}$, we have

$$x = m_1 n_1 (a_2 - a_1) + a_1 \equiv 1 \cdot (a_2 - a_1) + a_1 \equiv a_2 \pmod{m_2}$$

- **Inductive step:** Let $r \geq 2$ and assume the Chinese Remainder Theorem holds for any system of r congruences with pairwise relatively prime moduli. Let $a_1, \ldots, a_r, a_{r+1} \in \mathbb{Z}$ and $m_1, \ldots, m_r, m_{r+1} \in \mathbb{Z}^+$ with the m_i's pairwise relatively prime. Consider the following system of $(r+1)$ congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \\ x &\equiv a_{r+1} \pmod{m_{r+1}} \end{aligned}$$

  By the inductive hypothesis, there exists a unique solution $s \in \mathbb{Z}$ to the first r congruences modulo $\prod_{i=1}^{r} m_i$. Our system now reduces to

$$\begin{aligned} x &\equiv s \pmod{\prod_{i=1}^{r} m_i} \\ x &\equiv a_{r+1} \pmod{m_{r+1}} \end{aligned}$$

  Since $\gcd\left(\prod_{i=1}^{r} m_i, m_{r+1}\right) = 1$, the moduli in this reduced system are relatively prime. By the base case, there is a unique solution modulo $M = \prod_{i=1}^{r+1} m_i$, completing the proof.

By the Principle of Mathematical Induction, the Chinese Remainder Theorem holds for any integer $r \geq 2$. □

Example 31.1.13. Find all integers x which satisfy the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

By the Chinese Remainder Theorem, there is a unique solution modulo $30 = 2 \cdot 3 \cdot 5$.

Suppose x is a solution to the system. We start with the largest modulus and work down to find x up to congruence modulo 30.

- Since $x \equiv 3 \pmod 5$, we have $x = 5k + 3$ for some $k \in \mathbb{Z}$.
- Since $x \equiv 2 \pmod 3$, we substitute to get $5k + 3 \equiv 2 \pmod 3$, which implies $2k \equiv 2 \pmod 3$. Thus, $k \equiv 1 \pmod 3$, so $k = 3\ell + 1$ for some $\ell \in \mathbb{Z}$. Plugging this in, we get $x = 5(3\ell + 1) + 3 = 15\ell + 8$.
- Since $x \equiv 1 \pmod 2$, we substitute to get $15\ell + 8 \equiv 1 \pmod 2$, so $x = 30m + 23$ for $m \in \mathbb{Z}$.

Thus, $x \equiv 23 \pmod{30}$ is the unique solution modulo 30.

Example 31.1.14. Find all $x \in \mathbb{Z}$ such that $x^2 \equiv 1 \pmod{21}$.

Solution. Since $21 = 3 \cdot 7$ and $\gcd(3, 7) = 1$, we can use the Chinese Remainder Theorem. The original congruence is equivalent to the system of congruences:

$$x^2 \equiv 1 \pmod 3 \quad \text{and} \quad x^2 \equiv 1 \pmod 7$$

For any prime p, Euclid's lemma implies the following:

$$x^2 \equiv 1 \pmod p \iff p \mid (x-1)(x+1) \iff p \mid (x-1) \vee p \mid x+1 \iff x \equiv \pm 1 \pmod p$$

Therefore, $x^2 \equiv 1 \pmod 3$ iff $x \equiv \pm 1 \pmod 3$, and $x^2 \equiv 1 \pmod 7$ iff $x \equiv \pm 1 \pmod 7$.

We now have 4 independent systems to solve. For each one, the Chinese Remainder Theorem guarantees a unique solution modulo 21.

- Case 1: $x \equiv 1 \pmod 3$ and $x \equiv 1 \pmod 7$. Then $x \equiv 1 \pmod{21}$ is a solution to this system, so must be unique modulo 21.
- Case 2: $x \equiv -1 \pmod 3$ and $x \equiv -1 \pmod 7$. Then $x \equiv -1 \equiv 20 \pmod{21}$ is a solution to this system, so must be unique modulo 21.
- Case 3: $x \equiv 1 \pmod 3$ and $x \equiv -1 \pmod 7$. Let $x = 7k - 1$ for some $k \in \mathbb{Z}$. Substituting into the other congruence, we have:

  $$7k - 1 \equiv 1 \pmod 3 \implies k \equiv 2 \pmod 3$$

  so $k = 3\ell + 2$ for some $\ell \in \mathbb{Z}$. Thus,

  $$x = 7k - 1 = 7(3\ell + 2) - 1 = 21\ell + 13$$

  Hence, $x \equiv 13 \pmod{21}$.
- Case 4: $x \equiv -1 \pmod 3$ and $x \equiv 1 \pmod 7$. Let $x = 7k + 1$ for some $k \in \mathbb{Z}$. Substitute into the other congruence to get:

  $$7k + 1 \equiv -1 \pmod 3 \implies k \equiv -2 \equiv 1 \pmod 3$$

  so $k = 3\ell + 1$ for some $\ell \in \mathbb{Z}$. Thus,

  $$x = 7k + 1 = 7(3\ell + 1) + 1 = 21\ell + 8$$

  Hence, $x \equiv 8 \pmod{21}$.

Therefore, the set of all integers x satisfying $x^2 \equiv 1 \pmod{21}$ is:

$$\boxed{\{x \in \mathbb{Z} \mid x \equiv \pm 1 \text{ or } \pm 8 \pmod{21}\}}$$

Exercise 31.1.15. For each part below, find all solutions to the given system of congruences.

(a) $\begin{aligned} x &\equiv 5 \pmod 7 \\ x &\equiv 3 \pmod 8 \\ x &\equiv 1 \pmod 9 \end{aligned}$ (b) $\begin{aligned} 2x &\equiv 1 \pmod{23} \\ 9x &\equiv 12 \pmod{31} \end{aligned}$ (c) $\begin{aligned} 3x + 1 &\equiv 2 \pmod{11} \\ x &\equiv 3 \pmod{17} \\ 5x &\equiv 12 \pmod{18} \end{aligned}$

Exercise 31.1.16. Three roommates Adam, Bill, and Carol eat pizza on a regular basis. Adam eats pizza once every 3 days, Bill eats pizza once every 5 days, and Carol eats pizza once every 7 days. In 2025, Adam ate pizza on January 1, Bill ate pizza on January 2, and Carol ate pizza on January 3. What was the first date in 2025 that they all ate pizza on the same day?

31.1.3. Linear Diophantine Equations with Modular Arithmetic

Recall Theorem 27.1.3.

Theorem 31.1.17. *Let $a, b, c \in \mathbb{Z}$ with a and b not both zero. If $\gcd(a, b) \mid c$, then there are infinitely many integer solutions to $ax + by = c$. Moreover, if (x_0, y_0) is one solution, then all solutions are given by*

$$\{(x_0 + m(b/d), y_0 - m(a/d)) \mid m \in \mathbb{Z},\ d = \gcd(a, b)\}.$$

Memorizing formulas can be tedious. Now that we have a grasp of modular arithmetic, we can solve linear Diophantine equations without relying on memorization. This approach is demonstrated in the example below.

Example 31.1.18. Find all integer solutions to the equation $9x + 15y = 6$.

Solution: Let $x \in \mathbb{Z}$ be arbitrary. Then,

$$\begin{aligned} \exists y \in \mathbb{Z} \text{ such that } 9x + 15y = 6 &\Leftrightarrow 9x \equiv 6 \pmod{15} \\ &\Leftrightarrow 3x \equiv 2 \pmod 5 \\ &\Leftrightarrow x \equiv 4 \pmod 5 \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } x = 4 + 5k. \end{aligned}$$

So we have $x = 4 + 5k$ for some $k \in \mathbb{Z}$. Fix any such k. Let $y \in \mathbb{Z}$ satisfy $9x + 15y = 6$, substitute $x = 4 + 5k$ into the equation, and solve for y:

$$9(4 + 5k) + 15y = 6 \Leftrightarrow 15y = -30 - 45k \Leftrightarrow y = -2 - 3k.$$

Thus, the solution set to this Diophantine equation is

$$\{(4 + 5k, -2 - 3k) \mid k \in \mathbb{Z}\}.$$

Exercise 31.1.19. Use modular arithmetic to find all solutions to the following linear Diophantiune equations.

(a) $15x + 24y = 57$

(b) $63x + 17y = 5$

31.2. End Exam 3 Material

Part VI.

Combinatorics

32. November 14

32.1. Introduction

Combinatorics, often called *enumerative combinatorics* in its simplest form, is the study of counting finite sets. While counting might sound straightforward, answering questions such as "How many elements have property X?" can quickly become complex and requires precise techniques.

Historically, combinatorics originated in recreational mathematics and games-for example, in questions like "In how many ways can one deal a full house in poker?" Today, however, it is a foundational area of mathematics with applications across pure and applied mathematics, computer science, the natural sciences, and the social sciences. Its principles are especially useful in computer science for algorithm analysis and optimization, and in probability theory for computing event likelihoods.

Combinatorics provides tools not only for counting and arranging objects but also for analyzing the structure and relationships among sets. The field has evolved to include a wide range of methods, from elementary counting techniques to more advanced approaches involving algebra and geometry, leading to insights across many areas of study.

32.2. Basic Counting Principles

We begin by formalizing a few basic counting principles that may feel intuitive but are essential for a rigorous approach to combinatorics. Although these properties may seem obvious, stating them precisely will establish a foundation for more advanced counting techniques.

32.2.1. The Rule of Sum (Addition Principle)

To state this theorem, we first define a slightly relaxed notion of a partition for finite sets (specific to combinatorics) that allows parts to be empty.

Definition. Let A be a finite set. A collection of subsets $\{A_i\}_{i\in I}$ is called a *partition* of A if and only if

$$\bigcup_{i\in I} A_i = A \quad \text{and} \quad A_i \cap A_j = \varnothing \text{ for all } i \neq j.$$

Theorem 32.2.1 (Rule of Sum)**.** *If A is a finite set and $\mathcal{F} = \{A_1, \ldots, A_m\}$ is a finite partition of A, then*

$$|A| = \sum_{i=1}^{m} |A_i| = |A_1| + |A_2| + \cdots + |A_m|.$$

This rule is intuitive, as illustrated by the following example.

Example 32.2.2. Let A be the set of possible entrées at a restaurant. We can partition A into subsets A_1 and A_2, where

$$\begin{aligned} A_1 &= \text{ the set of entrees marked as spicy} \\ A_2 &= \text{ the set of entrees not marked as spicy} \end{aligned}$$

If $|A_1| = 13$ and $|A_2| = 20$ then $|A| = 33$ by the Rule of Sum.

The proof of this theorem follows immediately from Lemma 21.2.6 in the section on Cardinality.

Exercise 32.2.3. Let A be a finite subset and $A_1 \subseteq A$. Use the Rule of Sum to prove that $|A \setminus A_1| = |A| - |A_1|$.

The previous exercise leads to the following corollary.

Corollary 32.2.4 (Rule of Difference)**.** *If A is a finite set and $A_1 \subseteq A$, then*

$$|A \setminus A_1| = |A| - |A_1|.$$

Before our next corollary, we first define an n-to-1 surjection.

Definition. A function $f : A \to B$ is called an *n-to-1 surjection* if and only if f is surjective and each $b \in B$ has exactly n preimages in A; that is,

$$|\mathrm{PreIm}_f(\{b\})| = n.$$

In other words, every element of the codomain is mapped to by exactly n elements of the domain.

Corollary 32.2.5 (Rule of Division)**.** *Let A and B be finite sets, and let $f : A \to B$ be an n-to-1 surjection. Then*

$$|B| = \frac{|A|}{n}.$$

> "To count the number of cows in a field, first count the number of legs and then divide by 4."

Proof. Let $B = \{b_1, b_2, \ldots, b_k\}$. Then

$$A = \mathrm{PreIm}_f(\{b_1\}) \cup \mathrm{PreIm}_f(\{b_2\}) \cup \cdots \cup \mathrm{PreIm}_f(\{b_k\})$$

where $|\mathrm{PreIm}_f(\{b_i\})| = n$ for each i. Then, the Rule of Sum implies

$$|A| = \underbrace{n + n + \cdots + n}_{k \text{ times}} = nk = n|B|.$$

□

32.2.2. The Rule of Product (Multiplication Principle)

Theorem 32.2.6 (Rule of Product)**.** *Let $n \in \mathbb{Z}^+$ and let A_i be a finite set for each $i \in [n]$. If*

$$A = A_1 \times A_2 \times \cdots \times A_n,$$

then

$$|A| = \prod_{i=1}^{n} |A_i|.$$

This principle is intuitive, as illustrated by the following example.

Example 32.2.7. Let A be the set of all possible meals that can be ordered at a restaurant where each meal consists of one appetizer, one entrée, and one dessert. Define

$$A_1 = \text{the set of possible appetizers},$$
$$A_2 = \text{the set of possible entrées},$$
$$A_3 = \text{the set of possible desserts}.$$

We can view A as $A = A_1 \times A_2 \times A_3$. If $|A_1| = 5$, $|A_2| = 10$, and $|A_3| = 6$, then by the Rule of Product,

$$|A| = 5 \cdot 10 \cdot 6 = 300.$$

To formally prove this theorem, we can rely on results already discussed in the section on cardinality.

Sketch of Proof. If $A_i = \varnothing$ for any i, then $|A| = 0$ and $\prod_{i=1}^{n} |A_i| = 0$. Otherwise, assume each A_i is nonempty and proceed by induction on $n \in \mathbb{Z}^+$. The base case $n = 1$ is trivial, and for $n = 2$, we have shown that if $|A_1| = k$ and $|A_2| = \ell$, then $|A_1 \times A_2| = k\ell$. The general inductive step follows in a similar manner. □

The following restatement aligns more closely with how the Rule of Product is applied in practice.

Theorem 32.2.8 (Rule of Product, Reformulated)**.** *Suppose that the elements of a set are constructed by making a sequence of k choices such that:*

(i) The i-th choice can be made in r_i ways, independently of previous choices.

(ii) Each element in the set is uniquely determined by this sequence of choices.

Then the total number of elements in the set is given by $\prod_{i=1}^{k} r_i$.

Returning to our restaurant example, each possible meal results from a sequence of three independent choices: there are 5 choices for an appetizer, 10 choices for an entrée (regardless of the appetizer), and 6 choices for a dessert (regardless of prior selections). Thus, there are $5 \cdot 10 \cdot 6 = 300$ possible meals, each uniquely determined by one sequence of choices.

A Combined Example Using Rules of Sum and Product

Example 32.2.9. How many strings of lowercase English letters are there of length 4 or less (including the empty string)?

Let A be the set of all such strings. We can partition A by length:

$$\{A_0, A_1, A_2, A_3, A_4\},$$

where

$$\begin{aligned} A_0 &= \text{the set of strings of length 0,} \\ A_1 &= \text{the set of strings of length 1,} \\ A_2 &= \text{the set of strings of length 2,} \\ A_3 &= \text{the set of strings of length 3,} \\ A_4 &= \text{the set of strings of length 4.} \end{aligned}$$

By the Rule of Sum,

$$|A| = |A_0| + |A_1| + |A_2| + |A_3| + |A_4|.$$

Let S be the set of lowercase English letters, so $|S| = 26$. Applying the Rule of Product, we find

$$\begin{aligned} |A_0| &= 1, \\ |A_1| &= 26, \\ |A_2| &= 26^2, \\ |A_3| &= 26^3, \\ |A_4| &= 26^4. \end{aligned}$$

Therefore,

$$|A| = 1 + 26 + 26^2 + 26^3 + 26^4 = 475{,}255.$$

A Combined Example Using Rules of Product and Division

Example 32.2.10. How many 2-card hands can be dealt from a standard deck of 52 playing cards?

Solution. Consider the following 2-step process for constructing a 2-card hand:

- Select the first card from the deck: 52 choices.
- Select the second card from the remaining 51 cards: 51 choices.

By the Rule of Product, there are $52 \cdot 51$ ways to select an *ordered* pair of cards. However, the order of the cards in a hand does not matter, so each unordered 2-card hand is counted twice in this process. By the Rule of Division, we divide by 2 to account for this overcounting, yielding

$$\frac{52 \cdot 51}{2} = 1,326$$

distinct 2-card hands.

We will revisit similar counting problems when we discuss binomial coefficients.

Exercise 32.2.11. A student is choosing a two-course meal from a menu that has 4 appetizers, 6 main courses, and 3 desserts. How many meals are possible if the student can choose to have:

(a) An appetizer and a main course?

(b) A main course and a dessert?

(c) An appetizer and a dessert?

(d) Any two distinct courses? (Meaning: an appetizer and a main, OR a main and a dessert, OR an appetizer and a dessert).

Exercise 32.2.12. A car model comes in 4 colors, with 3 interior options, and 2 transmission types. Additionally, there is an optional sunroof that can be added only if the car is either red or blue. How many distinct car configurations are possible?

Exercise 32.2.13. How many even 4-digit numbers are there with distinct digits?

Exercise 32.2.14. In how many ways can 5 people sit around a circular table? (Two arrangements are considered the same if one can be rotated to obtain the other).

Exercise 32.2.15. How many binary strings of length 8 start with `1` or end with `00`?

32.2.3. The Pigeonhole Principle

Recall that we introduced the Pigeonhole Principle (Theorem 6.1.2) informally earlier in the semester. Below is a more formal statement, along with a proof.

Theorem 32.2.16 (Pigeonhole Principle)**.** *Let A be a finite set partitioned into parts $A_1, \ldots, A_k$ for some $k \in \mathbb{Z}^+$. If $|A| = n$, then there exists $i \in [k]$ such that*

$$|A_i| \geq \left\lceil \frac{n}{k} \right\rceil.$$

In particular, if $n > k$, then there exists $i \in [k]$ such that $|A_i| > 1$.

> "If many pigeons are placed into too few pigeonholes, at least one pigeonhole will contain multiple pigeons."

Proof. Let A be partitioned into the sets $\{A_1, \ldots, A_k\}$. Assume, for contradiction, that $|A_i| < \frac{n}{k}$ for each $i \in [k]$. Then, by the Rule of Sum,

$$|A| = \sum_{i=1}^{k} |A_i| < \sum_{i=1}^{k} \frac{n}{k} = n,$$

which contradicts the assumption that $|A| = n$. Therefore, there must exist some $i \in [k]$ such that $|A_i| \geq \left\lceil \frac{n}{k} \right\rceil$. □

Example 32.2.17. Suppose 75 students attended lecture today. The Pigeonhole Principle implies that there must be at least

$$\left\lceil \frac{75}{12} \right\rceil = 7$$

students who share the same birth month.

Why? If each month contained at most 6 students' birthdays, then the total number of students would be $6 \cdot 12 = 72$, contradicting the assumption of 75 students.

Example 32.2.18. A standard deck of 52 playing cards has 4 distinct suits (spades, clubs, hearts, diamonds) and 13 ranks for each suit (2,3,4,5,6,7,8,9,10,J,Q,K,A). How many cards must be selected to guarantee at least 3 cards of a single suit?

The Pigeonhole Principle tells us to find the smallest integer n such that

$$\left\lceil \frac{n}{4} \right\rceil = 3.$$

Thus, $n = 2 \cdot 4 + 1 = 9$, so we must select at least $\boxed{9 \text{ cards}}$ to guarantee at least 3 cards of a single suit.

The Pigeonhole Principle is one of the simplest yet most powerful theorems in mathematics and often yields surprising results.

Example 32.2.19 (Friends and Strangers Theorem)**.** Suppose a party has six people. Consider any two of them: they are either meeting for the first time (mutual strangers) or already know each other (mutual acquaintances). The theorem states:

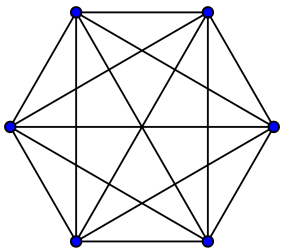
> "In any party of six people, at least three of them are (pairwise) mutual strangers or mutual acquaintances."

Proof. Label the six people as $\{a, b, c, d, e, f\}$. Consider person a and let A be the set of acquaintances of a, and S be the set of strangers to a. Then $\{A, S\}$ partitions $\{b, c, d, e, f\}$. Since $|A|+|S|= 5$, the Pigeonhole Principle implies that at least one of A or S has at least 3 people.

- Case 1: $|A| \geq 3$. All people in A are acquaintances with a. If any two in A are acquainted, they form a group of 3 mutual acquaintances with a. Otherwise, if no two people in A know each other, then A is a group of 3 mutual strangers.
- Case 2: $|S| \geq 3$. All people in S are strangers to a. If any two in S are strangers to each other, they form a group of 3 mutual strangers with a. Otherwise, if all people in S know each other, then S is a group of 3 mutual acquaintances. □

□

This theorem can also be interpreted using a complete graph with 6 vertices:



It states that if all edges are colored either red or blue, a monochromatic triangle is guaranteed. (Try it!)

Exercise 32.2.20. A drawer contains 10 black socks and 10 white socks. What is the minimum number of socks you must take out (without looking) to guarantee a pair of the same color?

Exercise 32.2.21. Prove that among any 6 integers, there are two whose difference is divisible by 5.

Exercise 32.2.22. How many distinct numbers must be chosen from the set [30] to ensure that at least one pair sums to 31?

Exercise 32.2.23. Given 5 points placed on a line segment of length 1, prove that two of them are within distance $\frac{1}{4}$ of each other.

Exercise 32.2.24. Suppose there are 5 teaching track professors in the math department. Each year, 2 are chosen to teach Concepts of Mathematics. How many years can the department go without repeating the same selection of 2 professors? Prove this is optimal by exhibiting such a sequence of that length, as well as invoking the Pigeonhole Principle to show that any longer sequence necessarily uses a pairing more than once.

Exercise 32.2.25. Let $n \in \mathbb{Z}^+$ and $A \in \mathcal{P}(\mathbb{Z})$ with $|A| = n$. Prove that there exists a nonempty $X \in \mathcal{P}(A)$ such that

$$\sum_{x \in X} x \equiv 0 \pmod{n}$$

Exercise 32.2.26. Show that among any 13 real numbers, there are two numbers whose difference is within $\frac{1}{12}$ of an integer.

Exercise 32.2.27. Let $S = [2n]$ for some $n \in \mathbb{Z}^+$, and let $T \in \mathcal{P}(S)$ such that $|T| = n+1$. Prove that there must exist $x, y \in T$ such that x and y are coprime.

33. November 17

33.1. Basic Counting Principles

33.1.1. The Principle of Double Counting

If we count the size of a set in two different ways, then both expressions for the cardinality of the set must be equal. This principle, known as *double counting*, often reveals interesting combinatorial identities.

Example 33.1.1 (The Handshake Lemma)**.** Suppose there are n people at a party, and everyone shakes hands with everyone else exactly once. How many handshakes occur in total?

- Method 1: Each of the n people shakes hands with $n-1$ others. Counting all handshakes in this way gives $n(n-1)$, but each handshake is counted twice (once for each participant). Thus, we divide by 2 to obtain the total number of unique handshakes:
$$\frac{n(n-1)}{2}.$$
- Method 2: Number the n people from 1 to n. To avoid double counting, consider only the handshakes each person makes with those numbered lower than themselves. Let A_i denote the set of handshakes made by person i with people numbered below i. Since person i has $i-1$ such handshakes, we find
$$|A| = \sum_{i=1}^{n} |A_i| = \sum_{i=1}^{n} (i-1) = \sum_{j=1}^{n-1} j.$$

Since both expressions describe the total number of handshakes, they must be equal. Therefore,
$$\frac{n(n-1)}{2} = \sum_{j=1}^{n-1} j.$$
This equality coincides with the formula for the sum of the first $n-1$ positive integers, which we previously proved by induction.

The argument above illustrates a *counting in two ways* proof. We will encounter additional examples of this technique throughout the remainder of these notes.

We now wish to discuss some additional combinatorial methods. Most counting problems that we encounter fall into one of four categories: arrangements without repetition, arrangements with repetition, selections without repetition, and selections with repetition.

33.2. Arrangements and Selections

33.2.1. Ordered Arrangements/Permutations

Definition. Let $n, k \in \mathbb{N}$ with $n \geq k$, and let X be a set with $|X| = n$. A *k-arrangement of X* is an injection $f : [k] \to X$.

Arrangements appear frequently in combinatorics, and several equivalent descriptions are used in practice.

For example, a *string* of distinct letters is an arrangement: the positions in the string form the domain, and the chosen letters form the codomain.

$\underline{\text{M}}\,\underline{\text{A}}\,\underline{\text{T}}\,\underline{\text{H}}$ is a 4-arrangement of the alphabet (a string of length 4 with no repeated letters).

Similarly, a *finite sequence* or *ordered n-tuple* with no repeated entries is an arrangement.

The 5-tuple $(1, 2, 3, 5, 8)$ is a 5-arrangement.

Counting the number of k-arrangements of a set of size n is a straightforward application of the Rule of Product.

Theorem 33.2.1. *Let $n, k \in \mathbb{Z}^+$ with $n \geq k$, and let X be a set with $|X| = n$. Then the number of k-arrangements from X is given by*

$$n \cdot (n-1) \cdots (n-k+1) = \prod_{i=0}^{k-1} (n-i) = \frac{n!}{(n-k)!}.$$

Proof. Without loss of generality, we may assume $X = [n]$. Let $P(n, k)$ denote the set of k-arrangements of $[n]$. We construct an arbitrary $f \in P(n, k)$ through the following k-step procedure:

- Choose $f(1)$: there are n options.
- Choose $f(2)$, distinct from $f(1)$: there are $n - 1$ options.
- In general, at step i, there are $n - (i - 1)$ options for $f(i)$.

After step k, the function f is completely determined. Each arrangement is produced by exactly one such sequence of choices, so by the Rule of Product,

$$|P(n,k)| = \prod_{i=1}^{k}(n-(i-1)) = \prod_{i=0}^{k-1}(n-i) = \frac{n!}{(n-k)!}.$$

□

We illustrate with a simple example.

Example 33.2.2. Out of a group of 20 contestants, we must select first, second, and third place. How many possible outcomes are there?

Let X be the set of contestants. This is equivalent to counting the number of injections $f : [3] \hookrightarrow X$, since the three places must be assigned to three distinct contestants. Alternatively, we can view this as filling three ordered positions:

$$\underline{\quad}_{\text{1st}} \quad \underline{\quad}_{\text{2nd}} \quad \underline{\quad}_{\text{3rd}}$$

By the Rule of Product, there are

$$20 \text{ choices for 1st}, \quad 19 \text{ choices for 2nd}, \quad 18 \text{ choices for 3rd}.$$

$$\underset{\text{1st}}{\underline{20}} \quad \underset{\text{2nd}}{\underline{19}} \quad \underset{\text{3rd}}{\underline{18}}$$

Thus the total number of possible outcomes is

$$20 \cdot 19 \cdot 18 = \frac{20!}{17!} = \boxed{6840}.$$

The most important special case is when $k = n$, which yields the notion of a *permutation*.

Definition. Let $n \in \mathbb{Z}^+$ and let X be a finite set with $|X| = n$. A *permutation* of X is a bijection $f : [n] \to X$. Equivalently, a permutation is a string or ordered n-tuple containing each element of X exactly once.

Notation: Given a set X, we denote the set of permutations of X by $\mathrm{Sym}(X)$. When $X = [n]$, we write S_n.

Example 33.2.3. Let $S = \{a, b, c\}$.

- Examples of permutations of S: (a, b, c), (b, a, c), (c, b, a).
- Non-examples: (b, b, a) (repetition), (a, c) (not all elements used).

The permutation (b, a, c) can equivalently be viewed as the bijection $f : [3] \to S$ defined by $f(1) = b$, $f(2) = a$, and $f(3) = c$.

Since a permutation is simply an n-arrangement of an n-element set, the previous theorem immediately yields the following corollary.

Corollary 33.2.4. *Let $n \in \mathbb{Z}^+$ and let X be a set with $|X| = n$. Then there are $n!$ permutations on X.*

We next consider arrangements where repetition is allowed.

Definition. Let $n, k \in \mathbb{Z}^+$ and let X be a set with $|X| = n$. A *k-arrangement with repetition* from X is a function $f : [k] \to X$. Equivalently, it is an ordered k-tuple whose entries lie in X, and repetitions are permitted.

Let $T(n, k)$ denote the set of k-arrangements with repetition from $[n]$. Since each of the k positions has n independent choices, the Rule of Product gives

$$|T(n, k)| = |[n]^k| = n^k.$$

We record this as a theorem for convenience.

Theorem 33.2.5. *For any $n, k \in \mathbb{Z}^+$, the number of k-arrangements with repetition from a set of size n is n^k.*

Example 33.2.6. Determine the number of binary strings of length 10.

A binary string of length 10 is a 10-arrangement with repetition from $\{0, 1\}$. Thus the number of such strings is $|T(2, 10)| = 2^{10} = 1024$.

33.2.2. Selections/Combinations

Selections are similar to arrangements, except order does not matter.

Definition. Let $n, k \in \mathbb{N}$ with $k \leq n$, and let X be a set with $|X| = n$. A k-selection from X is a subset of X of size k.

Notation: We write $\binom{n}{k}$ for the number of k-selections from $[n]$. This is called the *binomial coefficient* and is read as "n choose k."

If $k < 0$ or $k > n$, we define $\binom{n}{k} = 0$. For $0 \leq k \leq n$, the following theorem provides a formula to compute $\binom{n}{k}$.

Theorem 33.2.7. *Let $n, k \in \mathbb{N}$ with $k \leq n$. Then $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.*

Proof. Let $P(n, k)$ be the set of all k-arrangements from $[n]$. We count $|P(n, k)|$ in two different ways.

1. By our previous result, we know that $|P(n, k)| = \frac{n!}{(n-k)!}$.
2. Alternatively, we can build a k-arrangement in two steps:
   - First choose the underlying k elements. There are $\binom{n}{k}$ ways to choose a k-subset of $[n]$.
   - Then arrange these k elements in order, which can be done in $k!$ ways.

   By the Rule of Product, we conclude that $|P(n, k)| = k! \binom{n}{k}$.

Equating the two expressions for $|P(n, k)|$ gives

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

Solving for $\binom{n}{k}$ completes the proof:

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

□

Corollary 33.2.8. *For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$,*

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

Example 33.2.9. How many different poker hands (5-card hands) can be dealt from a standard deck of 52 playing cards?

Solution: Since only the set of cards matters (order is irrelevant), the number of possible hands is

$$\boxed{\binom{52}{5} = 2,598,960}.$$

The binomial coefficient gets its name from its role in the binomial theorem, which you may have encountered before.

Theorem 33.2.10 (The Binomial Theorem)**.** *Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. Then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

This theorem can be proven in several ways. You will see a combinatorial proof of this result in recitation.

Exercise 33.2.11. Foundational Exercises

(a) In how many ways can you arrange 7 distinct books on a bookshelf?

(b) A pizza place offers 12 distinct toppings. How many pizzas are possible with 3 distinct toppings?

(c) A class has 20 students. How many ways are there to choose a committee of 4 students?

(d) 8 runners compete in a race. In how many different orders can the first, second, and third place finishers be decided?

(e) How many different 5-digit binary sequences are there?

(f) How many anagrams of the word `ORANGE` are there?
As mathematicians, we consider an anagram to be any rearrangement of the letters, even if it doesn't make an actual word.

Exercise 33.2.12. Standard Applications

(a) How many ways can 4 boys and 3 girls stand in a line if the girls must stand together?

(b) From a club of 8 men and 7 women, how many ways are there to form a committee of 5 people if the committee must have at least 2 women?

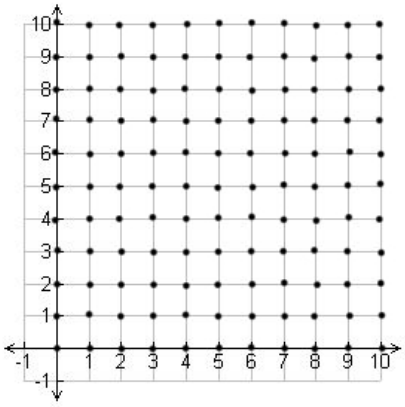
(c) How many triangles can be formed by connecting vertices of a regular octagon?

(d) A password must be 6 characters long. The first 3 characters must be distinct letters from the English alphabet (not case sensitive), and the last 3 characters must be distinct digits from 0-9. How many such passwords are possible?

(e) How many (distinct) anagrams of the word `BANANA` are there?

(f) A company has 10 engineers and 7 salespeople. How many ways can a team of 5 be selected to go to a conference if the team must have at least one engineer and at least one salesperson?

Exercise 33.2.13. Consider $\mathbb{N}^2$ represented visually on a plane.



The grid of dots on the plane is known as a *lattice*. Define a *lattice path* to be a path from $(0, 0)$ to a particular point that is only allowed to move rightwards or upwards at any step.

(a) Given $(a, b) \in \mathbb{N}^2$, how many distinct lattice paths are there to (a, b)?

(b) Let $n \in \mathbb{N}$. How many lattice paths from $(0, 0)$ to $(2n, 2n)$ pass through the point (n, n)?

Exercise 33.2.14. From a group of 7 mathematicians and 4 physicists, how many ways are there to form a committee of 5 that has more mathematicians than physicists and has a designated chairperson who must be a mathematician?

Exercise 33.2.15. In how many ways can 5 married couples be seated around a circular table if each couple must sit together?

34. November 21

34.1. Counting Arguments

Before developing more theory, we will pause to look at some examples that apply the counting principles we have established so far.

34.1.1. Poker Hands

A common example in introductory combinatorics or discrete probability is counting poker hands. We will use a standard deck of 52 playing cards (4 suits, each with 13 ranks), but no prior knowledge of poker is required; any poker-specific details will be provided as needed.

Example 34.1.1. How many 5-card poker hands are *One Pair* hands? A *One Pair* hand consists of 2 cards of one rank and 3 additional cards, each of distinct ranks different from the pair and different from one another (so the hand is neither a three-of-a-kind nor a two-pair).

We can use a multi-step Rule of Product approach to ensure that each one-pair hand is constructed in exactly one way and that no invalid hands are counted.

Rule of Product procedure:

- Choose the rank of the pair: $\binom{13}{1} = 13$ choices.
- From that rank, choose 2 suits: $\binom{4}{2}$ choices.
- Choose 3 additional ranks (all distinct and all different from the paired rank): $\binom{12}{3}$ choices.
- For each of these 3 ranks, choose a suit: $\binom{4}{1}^3 = 4^3$ choices.

By the Rule of Product, the total number of one-pair hands is:

$$\text{Total} = \binom{13}{1} \cdot \binom{4}{2} \cdot \binom{12}{3} \cdot 4^3 = 1,098,240$$

Answer: 1,098,240 one-pair hands.

If you used a different Rule-of-Product approach, that is perfectly fine. The final count will be the same, though there are several valid ways to construct the set. Here is one alternative method:

Alternative procedure:

- Select 4 distinct ranks to appear in the hand: $\binom{13}{4}$ choices.
- From these 4 ranks, choose 1 to be the rank of the pair: $\binom{4}{1}$ choices.
- For this rank, choose 2 suits: $\binom{4}{2}$ choices.
- For each of the 3 remaining ranks, choose a suit: $\binom{4}{1}^3 = 4^3$ choices.

Applying the Rule of Product again yields

$$\text{Total} = \binom{13}{4} \cdot \binom{4}{1} \cdot \binom{4}{2} \cdot 4^3 = 1,098,240$$

Answer: 1,098,240 one-pair hands.

Let us try another example involving poker hands.

Example 34.1.2. A 5-card poker hand is called a *Full House* if it consists of 3 cards of one rank and 2 cards of another rank (that is, a three-of-a-kind together with a pair). How many distinct Full House hands are possible?

Rule of Product procedure:

- Choose the two ranks that will appear in the hand: $\binom{13}{2}$ choices.
- From these two ranks, choose the rank of the three-of-a-kind: $\binom{2}{1} = 2$ choices.
- For that rank, choose 3 suits: $\binom{4}{3}$ choices.
- For the remaining rank, choose 2 suits: $\binom{4}{2}$ choices.

Thus, by the Rule of Product, the number of Full House hands is

$$\text{Total} = \binom{13}{2} \cdot \binom{2}{1} \cdot \binom{4}{3} \cdot \binom{4}{2} = 3{,}744.$$

Answer: 3,744 Full House hands.

Exercise 34.1.3. A *Three-of-a-Kind* is a 5-card hand that contains 3 cards of one rank, with the remaining 2 cards each of different ranks, distinct from the three-of-a-kind and from each other (that is, not a Full House and not a Four-of-a-Kind). How many distinct Three-of-a-Kind hands are possible?

34.1.2. Binary n-tuples

A common example in combinatorics involves counting subsets of binary n-tuples. Many combinatorial arguments can be phrased in terms of binary n-tuples (as you may have seen in recitation). We will find these useful for our discussion of selections with repetition.

Example 34.1.4. For $n \in \mathbb{Z}^+$, recall that $\{0,1\}^n$ denotes the set of binary n-tuples.

Let $n \geq 3$. How many binary n-tuples are there that contain *at least* three 1's?

In many counting problems, it is easier to determine the size of the complement of a set rather than counting the set directly. Here, instead of counting all binary n-tuples with exactly three 1's, four 1's, ..., up to n 1's, it is simpler to count the number with zero, one, or two 1's and subtract this from the total number of binary n-tuples.

Define $S = \{0,1\}^n$. First, note that $|S| = 2^n$ since each component has two choices, 0 or 1. We now calculate the number of binary n-tuples with fewer than three 1's. For each $i \in \{0,1,2\}$, let A_i denote the subset of binary n-tuples that contain exactly i many 1's.

- $|A_0| = \binom{n}{0} = 1$, because a binary n-tuple with no 1's must be the tuple $(0,0,\ldots,0)$.
- $|A_1| = \binom{n}{1} = n$. Here we choose which one of the n components is 1; all remaining components are 0.
- $|A_2| = \binom{n}{2} = \frac{n(n-1)}{2}$. We select two of the n components to be 1's; all remaining components are 0.

Since the sets A_0, A_1, A_2 are pairwise disjoint, the Rule of Difference gives

$$|S \setminus (A_0 \cup A_1 \cup A_2)| = 2^n - \binom{n}{0} - \binom{n}{1} - \binom{n}{2}$$

Thus, there are $\boxed{2^n - \binom{n}{0} - \binom{n}{1} - \binom{n}{2}}$ binary n-tuples with at least three 1's.

Later, when we introduce the Principle of Inclusion–Exclusion, we will see how to handle complements when the relevant sets are not disjoint.

This example motivates the following proposition.

Proposition 34.1.5. *For all $n \in \mathbb{N}$, $2^n = \sum_{i=0}^{n} \binom{n}{i}$.*

Below we present another example of a *counting in two ways* argument, using the Principle of Double Counting.

Proof. Let $n \in \mathbb{N}$, and consider the set $S = \{0,1\}^n$ of binary n-tuples. If $n = 0$, the only element of S is the empty string, so $|S| = 2^0 = 1$. For $n \geq 1$, $|S| = 2^n$ by the arrangements-with-repetition formula, since each of the n components has two choices.

Alternatively, we can count $|S|$ by partitioning S as $\{S_i \mid 0 \leq i \leq n\}$, where S_i is the set of binary n-tuples with exactly i components equal to 1.

Observe that if $i \neq j$, then $S_i \cap S_j = \varnothing$, because no binary n-tuple can have both i and j components equal to 1. Furthermore,

$$\bigcup_{i=0}^{n} S_i = S,$$

since every binary n-tuple has between 0 and n entries equal to 1. Thus, $\{S_i \mid 0 \leq i \leq n\}$ is a partition of S.

For each $i \in \{0, 1, \ldots, n\}$, we have $|S_i| = \binom{n}{i}$, since forming such a tuple amounts to choosing which i of the n components are 1's.

Using the Rule of Sum,

$$|S| = \sum_{i=0}^{n} |S_i| = \sum_{i=0}^{n} \binom{n}{i}.$$

Equating the two expressions for $|S|$ yields

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

□

Exercise 34.1.6. Let $n \in \mathbb{Z}^+$ and S be the set of all binary strings of length n. Each of the following expressions is the size of some subset of S. For each one, identify such a subset and explain why it works.

(a) 2^{n-2}

(b) $2^n - \binom{n}{n} - \binom{n}{n-1} - \binom{n}{n-2} - \binom{n}{n-3}$

(c) $\binom{n}{2} - \binom{n-1}{1}$

(d) $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k}$

Exercise 34.1.7. Consider finding the number of 4-tuples from the set $\{1, 2, 3\}$ that include one of each number. In both parts (a) and (b) a student proposes a "Proof" for the number of such 4-tuples. Explain why their reasoning is incorrect by exhibiting an object in the set that has been counted twice.

(a) Pick one of the 4 spots in the tuple for the 1, then pick a spot for the 2, then pick a spot for the 3. Then pick one of the three numbers to appear in the 4th empty spot.

$$\binom{4}{1}\binom{3}{1}\binom{2}{1}\binom{3}{1} = 72$$

(b) Pick 3 of the 4 spots to be filled by the numbers 1,2,3. Permute those elements in those chosen spots. Pick a number for the 4th empty spot.

$$\binom{4}{3} \cdot 3! \cdot 3 = 72$$

(c) Provide a correct counting argument for the number of possible 4-tuples.

35. November 24

35.1. Counting in Two Ways Proofs

We have now seen several examples of proofs using the principle of double counting. This proof technique has several advantages. First, it is sometimes difficult to establish an equality algebraically, while a combinatorial proof may be far more transparent. Second, even when an identity *can* be proved algebraically or by induction, those methods may obscure the underlying combinatorial idea. Counting in two ways often reveals why the equality is true by highlighting the processes being counted.

Below is a basic template for a "counting in two ways" proof.

Counting in Two Ways Proof Template

1. Motivated by the expressions on both sides of the equation, define a set S whose cardinality you will compute in two ways. **Make sure the definition of your set is clear.**
2. Give a counting argument for $|S|$ that yields the expression on the left-hand side of the equation.
3. Give a counting argument for $|S|$ that yields the expression on the right-hand side of the equation.
4. Conclude that since both expressions count $|S|$, they must be equal.

We now look at some standard examples of counting in two ways.

35.1.1. Pascal's Triangle

Many high school algebra courses introduce Pascal's triangle as a tool for expanding binomials. If you have seen it before, you may recall that the entries on the sides are 1's, and each entry inside the triangle is the sum of the two entries directly above it. Rows 0 through 5 are shown below.

Although this is Pascal's triangle, we can formally define it using binomial coefficients. Each entry is equal to $\binom{n}{k}$, where n is the row number and k is the position within the row. Both n and k start at 0, with $0 \leq k \leq n$.

$n=0$:						1					
$n=1$:					1		1				
$n=2$:				1		2		1			
$n=3$:			1		3		3		1		
$n=4$:		1		4		6		4		1	
$n=5$:	1		5		10		10		5		1

Table 35.1.: Pascal's Triangle

Using this notation, Pascal's triangle may be rewritten as in Table 35.2.

					$\binom{0}{0}$						
				$\binom{1}{0}$		$\binom{1}{1}$					
			$\binom{2}{0}$		$\binom{2}{1}$		$\binom{2}{2}$				
		$\binom{3}{0}$		$\binom{3}{1}$		$\binom{3}{2}$		$\binom{3}{3}$			
	$\binom{4}{0}$		$\binom{4}{1}$		$\binom{4}{2}$		$\binom{4}{3}$		$\binom{4}{4}$		
$\binom{5}{0}$		$\binom{5}{1}$		$\binom{5}{2}$		$\binom{5}{3}$		$\binom{5}{4}$		$\binom{5}{5}$	

Table 35.2.: Pascal's Triangle

We now show that this binomial coefficient description is equivalent to the recursive version in Table 35.1. In particular, we prove the following.

Theorem 35.1.1 (Pascal's Formula)**.** *For all $n, k \in \mathbb{Z}^+$ with $k \leq n$, it holds that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.*

This identity states that each binomial coefficient equals the sum of the two entries directly above it. We prove it using a counting in two ways argument.

Proof. Motivated by the left-hand side, define

$$S = \{T \in \mathcal{P}([n]) \mid |T| = k\},$$

the set of all k-element subsets of $[n]$. We compute $|S|$ in two ways.

- **Left-hand side (LHS):** By definition, $|S| = \binom{n}{k}$, since $\binom{n}{k}$ represents the number of k-element subsets of a set with n-many elements.
- **Right-hand side (RHS):** We partition S into subsets A and B defined as follows:

$$A = \{T \in S \mid 1 \in T\},$$
$$B = \{T \in S \mid 1 \notin T\}.$$

  Notice that $S = A \cup B$ and $A \cap B = \varnothing$, so $\{A, B\}$ forms a partition of S.

  We count $|A|$ and $|B|$ separately:

  - $|A| = \binom{n-1}{k-1}$, since each subset in A includes the element 1, leaving $k-1$ elements to be chosen from the remaining $n-1$ elements.
  - $|B| = \binom{n-1}{k}$, since each subset in B is formed by choosing all k-elements from the set $\{2, 3, \ldots, n\}$.

  By the Rule of Sum, we have

$$|S| = |A| + |B| = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Equating our two expressions for $|S|$ yields $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. □

There are many interesting patterns in Pascal's triangle. For example, consider what happens when we sum the entries along a diagonal.

				1						
			1		1					
		1		2		1				
	1		3		3		1			
1		4		6		4		1		
	5		10		10		5		1	
1		6		15		20		15		6		1

Table 35.3.: Summation Identity

Summing the red entries along the diagonal produces the boxed red entry one row below and one position to the right. The same holds for the blue diagonal. This pattern persists throughout Pascal's triangle. We now generalize this observation.

Proposition 35.1.2 (Summation Identity)**.** *For all $k, n \in \mathbb{N}$, we have:*

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

Proof. Let $k, n \in \mathbb{N}$, and let $S = \{T \in \mathcal{P}([n+1]) \mid |T| = k+1\}$. We will compute $|S|$ in two different ways.

- **Right-hand side:** By definition, $|S| = \binom{n+1}{k+1}$.
- **Left-hand side:** Partition S into subsets S_i for $i \in [n] \cup \{0\}$ where

  $$S_i = \{T \in S \mid (i+1 \in T) \wedge \forall j \in T,\, j \leq i+1\}.$$

  Here, S_i consists of all subsets $T \in S$ where the largest element is $i+1$. Clearly, $S_i \cap S_j = \varnothing$ for $i \neq j$, and since any $T \in S$ has a largest element between 1 and $n+1$, we have $\bigcup_{i=0}^{n} S_i = S$. Thus, $\{S_i\}$ is indeed a partition of S.

  For each $0 \leq i \leq n$, $|S_i| = \binom{i}{k}$, since there are $\binom{i}{k}$ ways to select the remaining k elements of a subset of size $k+1$ with $i+1$ as the largest element. By the Rule of Sum, $|S| = \sum_{i=0}^{n} |S_i| = \sum_{i=0}^{n} \binom{i}{k}$.

Therefore, $\binom{n+1}{k+1} = \sum_{i=0}^{n} \binom{i}{k}$. □

35.1.2. The Binomial Theorem

Before moving on to more examples of counting in two ways arguments, we record an important identity involving binomial coefficients. You will prove this theorem in recitation, but we state it here for later reference.

Theorem 35.1.3 (Binomial Theorem)**.** *For all $n \in \mathbb{N}$ and all real numbers x, y, we have*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

The coefficients in this expansion are exactly the entries that appear in Pascal's triangle. In fact, if you list the coefficients of $(x+y)^n$ in order, you obtain the entire nth row of the triangle. This connection is one of the main reasons binomial coefficients play such a central role in counting.

Examples 35.1.4.

1. Expanding a small power:
$$(x+y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

2. Using the theorem to obtain coefficients:
$$(2-t)^4 = \sum_{k=0}^{4}\binom{4}{k}2^{4-k}(-t)^k = 16 - 32t + 24t^2 - 8t^3 + t^4.$$

3. Since the coefficients match Pascal's triangle, we have
$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

You will prove the Binomial Theorem in recitation by giving a combinatorial counting argument for the coefficient $\binom{n}{k}$ of $x^{n-k}y^k$.

Exercise 35.1.5. Use the Binomial Theorem to show the following identities.

(a) $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$

(b) $3^n = \sum_{k=0}^{n}\binom{n}{k}2^k = \sum_{k=0}^{n}\binom{n}{k}2^{n-k}$

(c) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}2^{n-k} = 1$

(d) $(1+x)^{2n} = \sum_{k=0}^{2n}\left(\sum_{j=0}^{k}\binom{n}{j}\binom{n}{k-j}\right)x^k$

Hint: Use the Binomial Theorem twice.

So far, we have been describing our sets as purely mathematical objects (e.g., the set of subsets of $[n]$ of size k). As we begin to work with more complicated sets, a purely set-theoretic description can become difficult for the reader to follow. To address this, we introduce a helpful strategy for describing subsets and their elements in a more intuitive and accessible way.

35.1.3. New Strategy: Committees and Leaders

This strategy is widely used in combinatorial proofs. For example, instead of referring directly to the set of subsets of $[n]$ of size k, we can think of this set as the collection of all committees of size k chosen from n distinct people. By reducing the technical mathematical language, this approach helps highlight the underlying counting ideas.

Example 35.1.6. Prove that for all $k, n \in \mathbb{Z}^+$,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Proof. Let $k, n \in \mathbb{Z}^+$, and let S be the set of all k-person committees with a designated chairperson, formed from a group of n people. We will compute $|S|$ in two different ways.

- **(LHS):** Construct an element of S by the following procedure:
  - Choose a k-person committee from the n people. There are $\binom{n}{k}$ ways to do this.
  - From the k committee members, select one person to serve as chair. There are k choices.

  By the Rule of Product, $|S| = k\binom{n}{k}$.
- **(RHS):** Alternatively, construct an element of S as follows:
  - Choose the chairperson from among the n people. There are n choices.
  - From the remaining $n-1$ people, select $k-1$ additional committee members. There are $\binom{n-1}{k-1}$ ways to do this.

  Again by the Rule of Product, $|S| = n\binom{n-1}{k-1}$.

Since both procedures count the same set S, the two expressions for $|S|$ must be equal. Therefore,

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

□

Remark. The set S used in the proof above can also be described formally as

$$S = \{(T, t) \in \mathcal{P}([n]) \times [n] : t \in T,\ |T| = k\}.$$

Here, $[n]$ represents the set of n people, T represents the committee, and t is the designated chairperson (a distinguished element of T).

While this formal description is precise, describing the elements of S as "committees with leaders" often makes the combinatorial structure more transparent.

The next exercise continues this idea with a small twist. Try to solve it on your own before reading further.

Exercise 35.1.7. Let $n \in \mathbb{Z}^+$. Prove that

$$n \cdot 2^{n-1} = \sum_{k=1}^{n} k \binom{n}{k}.$$

36. December 1

36.1. Counting in Two Ways Proofs

We now modify the previous example to explore another useful counting argument. The twist here is that we must keep track of two roles on each committee, and an important distinction will arise.

Example 36.1.1. Prove that for all $n \in \mathbb{Z}^+$,

$$\sum_{k=1}^{n} k^2 \binom{n}{k} = n \cdot 2^{n-1} + n(n-1) \cdot 2^{n-2}.$$

Proof. Let $n \in \mathbb{Z}^+$, and let S be the set of all nonempty committees formed from n people, where each committee has both a leader and a planner. The leader and planner may be the same person or two different people.

Important note. When describing a set such as S, we must specify whether the two roles must be filled by distinct individuals. The counting changes significantly depending on whether overlap is allowed.

A precise description of S is:

$$S = \{(T, k, \ell) \in \mathcal{P}([n]) \times [n] \times [n] : k \in T,\ \ell \in T\},$$

where T is the committee, k is the leader, and ℓ is the planner. We now count $|S|$ in two ways.

- **(LHS): Counting by committee size.**

  Partition S into the subsets S_k, where S_k consists of committees of size k. To construct an element of S_k:

  - Choose the k-person committee: $\binom{n}{k}$ choices.
  - Choose the leader from among the k committee members.
  - Choose the planner from among the k committee members.

  By the Rule of Product, $|S_k| = k^2 \binom{n}{k}$. Summing over all valid committee sizes gives

  $$|S| = \sum_{k=1}^{n} k^2 \binom{n}{k}.$$

- **(RHS): Counting by role assignments.**

  Partition S into two subsets:

  $$A = \text{committees where the leader and planner are the same person,}$$
  $$B = \text{committees where the leader and planner are distinct people.}$$

  Counting A:

  - Choose the person who serves as both leader and planner: n choices.
  - Choose any (possibly empty) subset of the remaining $n-1$ people to complete the committee: 2^{n-1} choices.

  By the rule of product, $|A| = n \cdot 2^{n-1}$.

  Counting B:

  - Choose the leader: n choices.
  - Choose the planner from the remaining $n-1$ people: $n-1$ choices.
  - From the remaining $n-2$ people, choose a (possibly empty) subset to complete the committee: 2^{n-2} choices.

  By the rule of product, $|B| = n(n-1) \cdot 2^{n-2}$.

  By the Rule of Sum,

  $$|S| = |A| + |B| = n \cdot 2^{n-1} + n(n-1) \cdot 2^{n-2}.$$

Finally, equating our two expressions for $|S|$ gives the desired identity:

$$\sum_{k=1}^{n} k^2 \binom{n}{k} = n \cdot 2^{n-1} + n(n-1) \cdot 2^{n-2}.$$

□

Exercise 36.1.2. Prove the following identities via a "counting in two ways" argument. Use the exact form given. Do not simplify algebraically.

(a) Let $a, b, k \in \mathbb{Z}^+$ with $a + b \geq k$.

$$\binom{a+b}{k} = \sum_{i=0}^{k} \binom{a}{i} \binom{b}{k-i}$$

(b) Let $n \in \mathbb{Z}^+$.

$$3^n - 2^n = \sum_{k=1}^{n} 2^{k-1} \cdot 3^{n-k}$$

(c) Let $m, n \in \mathbb{Z}^+$ with $n \geq m$.

$$\binom{n}{m} \cdot 2^{n-m} \cdot m = \sum_{k=m}^{n} k \binom{n}{k} \binom{k-1}{m-1}$$

(d) Let $n \in \mathbb{N}$ with $n \geq 4$.

$$\binom{\binom{n}{2}}{2} = 3 \cdot \binom{n}{4} + 3 \cdot \binom{n}{3}$$

36.2. Selections with Repetition

In this section, we address the question: *With repetition allowed, how many ways are there to select n objects from k types of objects?* To build intuition, we first examine a concrete example.

Example 36.2.1. A donut shop sells 10 different flavors of donuts. You want to buy 12 donuts from the shop. How many distinct ways can you order these dozen donuts?

This is a selection problem because the order in which the donuts are chosen does not matter. For example, selecting a glazed donut followed by a powdered donut is the same as selecting a powdered donut followed by a glazed donut. However, this is not a simple selection problem because choosing 2 glazed donuts is different from choosing 1 glazed donut in your box of 12.

To visualize the situation, imagine organizing the 12 donuts by flavor:

OO	OOO	·····	O
Flavor 1	Flavor 2	·····	Flavor 10

Place an `O` above Flavor n (for $1 \leq n \leq 10$) for each donut of that flavor. To separate the flavors, insert dividers between groups. In total, the diagram contains 12 O's (one for each donut) and 9 dividers (one fewer than the number of flavors).

This arrangement corresponds to a binary string of length $12+10-1 = 21$, consisting of 12 `0`'s (donuts) and 9 `1`'s (dividers). The number of possible arrangements is the number of ways to choose 12 positions for the `0`'s (or equivalently, 9 positions for the `1`'s):

$$\binom{21}{12} = \binom{21}{9} = 293,930.$$

Thus, there are 293,930 distinct ways to buy a dozen donuts.

This correspondence between selections with repetition and binary strings leads directly to the following general theorem.

Theorem 36.2.2 (Stars and Bars)**.** *With repetition allowed, there are* $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$ *ways to select* n *objects from* k *types.*

Equivalently, this is the number of nonnegative integer solutions to the equation

$$x_1 + x_2 + \cdots + x_k = n, \quad \text{for } k, n \in \mathbb{N}.$$

Note. This result is often referred to as the *stars and bars* theorem, a name derived from a visual mnemonic. The "stars" represent the objects being selected (e.g., donuts), while the "bars" divide the stars into k groups corresponding to the different object types. This terminology is widely used in combinatorics and can be helpful when recalling or visualizing the theorem.

Example 36.2.3. Suppose we roll n indistinguishable six-sided dice.

(a) **How many different outcomes are possible?**

Since the dice are indistinguishable and each die shows a number from 1 to 6, this is a selection-with-repetition problem. For example, one outcome could be rolling three 2's, two 3's, and one 6, which we can represent as:

	OOO	OO			O
1	2	3	4	5	6

Here, the total number of outcomes is the number of ways to distribute n rolls among the six possible results:

$$\binom{n+5}{5}.$$

(b) **Assume** $n \geq 12$**. How many outcomes are possible if at least 2 dice show each number?**

Begin by assigning 2 dice to each of the six faces, using up 12 rolls. The remaining $n - 12$ rolls can be distributed arbitrarily among the six outcomes. By stars and bars, the total number of outcomes is:

$$\binom{(n-12)+5}{5}.$$

Alternatively, we can frame this in terms of integer equations. We wish to count the number of solutions to

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = n, \qquad x_i \geq 2.$$

Letting $y_i = x_i - 2$, we rewrite the equation as

$$y_1 + y_2 + y_3 + y_4 + y_5 + y_6 = n - 12, \quad \text{where } y_i \geq 0.$$

The number of nonnegative integer solutions is again

$$\binom{(n-12)+5}{5}.$$

(c) **In how many ways can we roll 20 dice with at most three 6's?**

We present two different correct answers below:

- **Answer 1**: Find the complement. How many ways can we roll the 20 dice with *at least* four 6's?
  - Begin by assigning four dice to 6.
  - The remaining 16 dice can be assigned arbitrarily.

  By the Stars-and-Bars theorem, there are $\binom{21}{5}$ ways to roll the dice with at least four 6's. Since there are $\binom{25}{5}$ outcomes possible with no restriction, we apply the Rule of Subtraction to get the number of outcomes with *at most* three 6's:

$$\binom{25}{5} - \binom{21}{5} \quad \text{possible outcomes}$$

- **Answer 2**: Find the number of solutions that satisfy $x_6 = k$ for $0 \leq k \leq 3$. For each k, assign exactly k dice to x_6. The remaining $20 - k$ dice can be distributed arbitrarily among x_1 through x_5. Applying stars-and-bars, this can be done in

$$\binom{(20-k)+(5-1)}{5-1} = \binom{24-k}{4} \quad \text{ways}$$

  Applying the Rule of Sum we have

$$\sum_{k=0}^{3} \binom{24-k}{4} = \binom{24}{4} + \binom{23}{4} + \binom{22}{4} + \binom{21}{4}$$

  possible outcomes.

Note that the second answer could be rewritten as

$$\sum_{k=0}^{24} \binom{k}{24} - \sum_{k=0}^{20} \binom{k}{4},$$

and, by the Summation Identity, this equals $\binom{25}{5} - \binom{21}{5}$, the first answer we arrived at.

37. December 3

37.1. Selections with Repetition

Example 37.1.1. Suppose we have 10 pirates who must divvy up 100 pieces of gold. Suppose further that Captains Redbeard and Blackbeard are among the 10 pirates.

(a) **How many ways are there to divvy up the 100 pieces of gold among the 10 pirates?**

We are distributing 100 objects (pieces of gold) among 10 types (individual pirates). Using the selections-with-repetition formula, this can be done in

$$\binom{100+10-1}{10-1} = \boxed{\binom{109}{9} = 4,263,421,511,271}$$

different ways.

(b) **How many ways are there to divvy up the gold if exactly 2 pirates receive no gold?**

We can construct a division of gold with this property via a 3-step rule of product:

- Determine which 2 pirates receive no gold. There are $\binom{10}{2}$ options.
- Give one piece of gold to each of the remaining 8 pirates. This can be done in 1 way.
- Distribute the remaining 92 pieces of gold among the 8 pirates. Using the selections-with-repetition formula, this can be done in

$$\binom{92+8-1}{8-1} = \binom{99}{7}$$

different ways.

By the Rule of Product, there are

$$\boxed{\binom{10}{2}\binom{99}{7} = 669,916,419,480}$$

distributions in which exactly 2 pirates receive no gold.

(c) **Suppose Redbeard must get at least 5 pieces of gold and Blackbeard must get at most 5 pieces of gold. How many ways are there to divvy up the gold with these restrictions?**

First, there are

$$\binom{95+10-1}{10-1} = \binom{104}{9}$$

ways to distribute the gold so that Redbeard gets at least 5 pieces. This is determined by first giving Redbeard 5 pieces, then distributing the remaining 95 pieces among all 10 pirates using the selections-with-repetition formula.

Next, there are

$$\binom{89+10-1}{10-1} = \binom{98}{9}$$

ways to distribute the gold so that Redbeard gets at least 5 pieces **and** Blackbeard gets more than 5 pieces (at least 6). This is done by first giving Redbeard 5 pieces, Blackbeard 6 pieces, and then distributing the remaining 89 pieces among all 10 pirates.

Finally, by the Rule of Subtraction, the number of distributions in which Redbeard gets at least 5 pieces and Blackbeard gets at most 5 pieces is

$$\boxed{\binom{104}{9} - \binom{98}{9} = 1{,}173{,}807{,}751{,}480.}$$

(d) **How many ways are there to divvy up the gold if Redbeard gets at least 10 pieces of gold, but Blackbeard gets somewhere between 5 and 15 (inclusive) pieces of gold?**

First, there are

$$\binom{85+10-1}{10-1} = \binom{94}{9}$$

ways to distribute the gold so that Redbeard gets at least 10 pieces and Blackbeard gets at least 5 pieces. This is done by first giving Redbeard 10 pieces and Blackbeard 5 pieces, then distributing the remaining 85 pieces among all 10 pirates.

Next, there are

$$\binom{74+9}{9} = \binom{83}{9}$$

ways to distribute the gold so that Redbeard gets at least 10 pieces and Blackbeard gets more than 15 pieces (at least 16).

By the Rule of Subtraction, the number of distributions in which Redbeard gets at least 10 pieces and Blackbeard gets between 5 and 15 pieces (inclusive) is

$$\boxed{\binom{94}{9} - \binom{83}{9} = 734{,}983{,}717{,}468.}$$

(e) **How many ways are there to divvy up the gold so that Redbeard gets somewhere between 0 and 10 (inclusive) pieces of gold and Blackbeard gets somewhere between 10 and 20 (inclusive) pieces of gold?**

There are

$$\binom{90+10-1}{10-1} = \binom{99}{9}$$

ways to divvy up the gold so that Blackbeard gets at least 10 pieces. We will use the version 1 of the Principle of Inclusion–Exclusion (Theorem refPIE1) to determine how many of these ways result in Redbeard getting at most 10 pieces and Blackbeard getting at most 20 pieces.

- There are $\binom{88}{9}$ ways to distribute the gold so that Blackbeard gets at least 10 pieces and Redbeard gets more than 10 (at least 11) pieces.
- There are $\binom{88}{9}$ ways to distribute the gold so that Blackbeard gets more than 20 (at least 21) pieces.
- There are $\binom{77}{9}$ ways to distribute the gold so that Blackbeard gets more than 20 pieces **and** Redbeard gets more than 10 pieces.

By the Principle of Inclusion–Exclusion, the number of valid distributions is

$$\boxed{\binom{99}{9} - 2\binom{88}{9} + \binom{77}{9} = 749{,}652{,}784{,}639.}$$

Thus, there are 749,652,784,639 ways to divvy up the gold so that Redbeard gets at most 10 pieces and Blackbeard gets between 10 and 20 (inclusive) pieces.

Exercise 37.1.2. Consider the Diophantine equation $a + b + c + d = 25$.

(a) How many nonnegative integer solutions are there?

(b) How many positive integer solutions are there?

(c) How many nonnegative integer solutions are there with $a \geq 3$ and $b \geq 2$?

(d) How many integer solutions are there with $a \geq 3$, $b \geq 2$, $c \geq 0$, and $d \geq -3$?

(e) How many nonnegative integer solutions are there with $a \leq 9$ and $b \leq 8$?

Exercise 37.1.3. A baker has 48 cupcakes to distribute among 4 distinct serving tables.

(a) In how many ways can the baker distribute the cupcakes if all 48 cupcakes are distinct?

(b) In how many ways can this be done if all 48 cupcakes are identical?

(c) Suppose there are 6 flavors of cupcakes, with 8 identical cupcakes of each flavor. How many distributions are possible?

(d) How many distributions are possible if the cupcakes are identical and no table is left empty?

(e) Suppose the baker faces the following constraints: Tables 1 and 2 may not receive more than 10 cupcakes each, and Tables 3 and 4 must not be empty. If all cupcakes are identical, how many valid distributions are possible?

Exercise 37.1.4. Your bank requires you to create a 4-digit ATM PIN code (digits 0–9). How many PIN codes are possible if the digits form a *non-decreasing* sequence? (That is, $d_1 \leq d_2 \leq d_3 \leq d_4$.)

37.2. Principle of Inclusion-Exclusion

Recall from Theorem 21.2.7 that if A_1 and A_2 are finite sets, then:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Here, $|A_1| + |A_2|$ counts all elements in A_1 and A_2, but elements in $A_1 \cap A_2$ are counted twice. To correct this, we subtract $|A_1 \cap A_2|$.

We now extend this idea. Consider three finite sets A_1, A_2, and A_3. Then:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

As before, terms like $|A_1 \cap A_2|$ are subtracted to account for double-counting, and $|A_1 \cap A_2 \cap A_3|$ is added to correct over-subtraction of elements common to all three sets.

We now state and prove the general case.

Theorem 37.2.1 (Principle of Inclusion-Exclusion)**.** *Let $m \in \mathbb{Z}^+$, S be a finite set, and $A_1, A_2, \ldots, A_m \subseteq S$. Then:*

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{i=1}^{m} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k|$$

$$- \cdots + (-1)^{m+1} \left| \bigcap_{i=1}^{m} A_i \right|.$$

Equivalently:

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{\varnothing \neq X \subseteq [m]} (-1)^{|X|+1} \left| \bigcap_{i \in X} A_i \right|.$$

Proof. Define the characteristic function $f_i : S \to \{0, 1\}$ by:

$$f_i(x) = \begin{cases} 1 & \text{if } x \in A_i, \\ 0 & \text{if } x \notin A_i. \end{cases}$$

Now define $F : S \to \{0, 1\}$ by:

$$F(x) = 1 - \prod_{i=1}^{m} (1 - f_i(x)).$$

This function is 1 if $x \in \bigcup_{i=1}^{m} A_i$ and 0 otherwise. Therefore:

$$\sum_{x \in S} F(x) = |A_1 \cup A_2 \cup \cdots \cup A_m|.$$

Expanding $F(x)$ using the Binomial Theorem, we have:

$$F(x) = 1 - \prod_{i=1}^{m} (1 - f_i(x)) = \sum_{\varnothing \neq X \subseteq [m]} (-1)^{|X|+1} \prod_{i \in X} f_i(x).$$

By summing over $x \in S$, we obtain:

$$\sum_{x \in S} F(x) = \sum_{\varnothing \neq X \subseteq [m]} (-1)^{|X|+1} \left| \bigcap_{i \in X} A_i \right|.$$

Equating this with $|A_1 \cup A_2 \cup \cdots \cup A_m|$, we derive the desired result. □

Example 37.2.2. How many integers from 1 to 1000 are divisible by 5, 7, or 11?

Solution. Define the sets $A_5, A_7, A_{11} \subseteq [1000]$, where:

- A_5 is the set of integers divisible by 5,
- A_7 is the set of integers divisible by 7, and
- A_{11} is the set of integers divisible by 11.

We aim to find $|A_5 \cup A_7 \cup A_{11}|$. First, observe:

$$\begin{aligned} |A_5| &= \left\lfloor \frac{1000}{5} \right\rfloor = 200, \\ |A_7| &= \left\lfloor \frac{1000}{7} \right\rfloor = 142, \\ |A_{11}| &= \left\lfloor \frac{1000}{11} \right\rfloor = 90. \end{aligned}$$

Recall that an integer is divisible by both a and b if and only if $\text{lcm}[a, b]$ divides that integer. Using this fact, and the fact that 5, 7, and 11 are pairwise coprime, we can compute the cardinalities of the pairwise intersections:

$$\begin{aligned} |A_5 \cap A_7| &= \left\lfloor \frac{1000}{\text{lcm}[5,7]} \right\rfloor = \left\lfloor \frac{1000}{35} \right\rfloor = 28, \\ |A_5 \cap A_{11}| &= \left\lfloor \frac{1000}{\text{lcm}[5,11]} \right\rfloor = \left\lfloor \frac{1000}{55} \right\rfloor = 18, \\ |A_7 \cap A_{11}| &= \left\lfloor \frac{1000}{\text{lcm}[7,11]} \right\rfloor = \left\lfloor \frac{1000}{77} \right\rfloor = 12. \end{aligned}$$

Similarly, for the triple intersection, we have:

$$|A_5 \cap A_7 \cap A_{11}| = \left\lfloor \frac{1000}{\text{lcm}[5,7,11]} \right\rfloor = \left\lfloor \frac{1000}{385} \right\rfloor = 2.$$

By the Principle of Inclusion-Exclusion, we have:

$$|A_5 \cup A_7 \cup A_{11}| = |A_5| + |A_7| + |A_{11}| - |A_5 \cap A_7| - |A_5 \cap A_{11}| - |A_7 \cap A_{11}| + |A_5 \cap A_7 \cap A_{11}|,$$

Substituting the values, we get:

$$\begin{aligned} |A_5 \cup A_7 \cup A_{11}| &= 200 + 142 + 90 - 28 - 18 - 12 + 2 \\ &= \boxed{376}. \end{aligned}$$

Thus, there are 376 integers from 1 to 1000 that are divisible by 5, 7, or 11.

Often, the cardinality $|\bigcap_{i\in X} A_i|$ does not depend on the specific subsets A_i, but only on $|X|$ – the number of subsets in the intersection. In such cases, the Principle of Inclusion-Exclusion can be expressed in a simpler form.

Corollary 37.2.3. *Let $m \in \mathbb{N}$, S be a finite set, and $A_1, A_2, \ldots, A_m \in \mathcal{P}(S)$. Further, assume that for each $X \subseteq [m]$, the cardinality $|\bigcap_{i\in X} A_i|$ depends only on $|X|$. Then,*

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = \sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k} \left| \bigcap_{i=1}^{k} A_i \right|.$$

Example 37.2.4. How many integers between 0 and 99,999 have, among their digits, at least one occurrence of 2, 5, and 8?

Let S be the set of integers between 0 and 99,999. Then $|S| = 10^5$. Define:

$$A_2 = \{x \in S \mid \text{none of the digits of } x \text{ are } 2\},$$

$$A_5 = \{x \in S \mid \text{none of the digits of } x \text{ are } 5\},$$

$$A_8 = \{x \in S \mid \text{none of the digits of } x \text{ are } 8\}.$$

We wish to find $|\overline{A}_2 \cap \overline{A}_5 \cap \overline{A}_8|$, the number of integers that include at least one of the digits 2, 5, and 8. Using De Morgan's laws:

$$|\overline{A}_2 \cap \overline{A}_5 \cap \overline{A}_8| = |S| - |A_2 \cup A_5 \cup A_8|.$$

To compute $|A_2 \cup A_5 \cup A_8|$, we use PIE. Note:

- $|A_i| = 9^5$ for each $i \in \{2, 5, 8\}$, as these are integers with 5 digits, excluding one specific digit (9 choices per digit).
- $|A_i \cap A_j| = 8^5$ for all $i \neq j \in \{2, 5, 8\}$, since these are integers excluding two specific digits (8 choices per digit).
- $|A_2 \cap A_5 \cap A_8| = 7^5$, as these are integers excluding all three digits (7 choices per digit).

Applying PIE:

$$|A_2 \cup A_5 \cup A_8| = \binom{3}{1} 9^5 - \binom{3}{2} 8^5 + \binom{3}{3} 7^5.$$

Therefore,

$$|\overline{A}_2 \cap \overline{A}_5 \cap \overline{A}_8| = |S| - |A_2 \cup A_5 \cup A_8| = \boxed{10^5 - 3 \cdot 9^5 + 3 \cdot 8^5 - 7^5}$$

We conclude our discussion of the Principle of Inclusion-Exclusion with one final example.

Example 37.2.5. Find the number of nonnegative integer solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 34$$

such that $0 \leq x_i \leq 10$ for each $i \in \{1, 2, 3, 4\}$.

First, let S be the set of nonnegative integer solutions to the equation without the restriction $0 \leq x_i \leq 10$. Using the stars-and-bars formula, the total number of solutions is

$$|S| = \binom{34 + 4 - 1}{4 - 1} = \binom{37}{3}.$$

For each $i \in [4]$, let A_i be the set of nonnegative integer solutions where $x_i \geq 11$. We wish to compute $|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3 \cap \overline{A}_4|$, the number of solutions satisfying $0 \leq x_i \leq 10$ for all i.

For each $i \in [4]$, the condition $x_i \geq 11$ can be reduced by setting $x_i' = x_i - 11$. Substituting into the equation, this corresponds to finding nonnegative integer solutions to

$$x_1 + x_2 + x_3 + x_4 = 23.$$

Thus,

$$|A_i| = \binom{23 + 4 - 1}{4 - 1} = \binom{26}{3}.$$

For $i \neq j \in [4]$, the condition $x_i \geq 11$ and $x_j \geq 11$ similarly reduces the equation to

$$x_1 + x_2 + x_3 + x_4 = 12,$$

so

$$|A_i \cap A_j| = \binom{12 + 4 - 1}{4 - 1} = \binom{15}{3}.$$

For $i \neq j \neq k \in [4]$, the condition $x_i \geq 11$, $x_j \geq 11$, and $x_k \geq 11$ reduces the equation to

$$x_1 + x_2 + x_3 + x_4 = 1,$$

giving

$$|A_i \cap A_j \cap A_k| = \binom{1 + 4 - 1}{4 - 1} = \binom{4}{3}.$$

Finally, if $x_i \geq 11$ for all $i \in [4]$, then

$$x_1 + x_2 + x_3 + x_4 \geq 44,$$

which is impossible since the original equation sums to 34. Hence,

$$|A_1 \cap A_2 \cap A_3 \cap A_4| = 0.$$

Using the Principle of Inclusion-Exclusion, we compute:

$$|\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3 \cap \overline{A}_4| = \binom{37}{3} - \binom{4}{1}\binom{26}{3} + \binom{4}{2}\binom{15}{3} - \binom{4}{3}\binom{4}{3} + 0 = \boxed{750}.$$

Exercise 37.2.6. In a group of 100 students, 45 study mathematics, 38 study physics, 42 study chemistry, 15 study both mathematics and physics, 18 study both mathematics and chemistry, 16 study both physics and chemistry, and 7 study all three. How many students study none of these subjects?

Exercise 37.2.7. Use the Principle of Inclusion–Exclusion to find the number of integers between 1 and 2500 that are not divisible by 4, 5, or 6.

Exercise 37.2.8. How many orderings of the eight letters $\{a, b, c, d, e, f, g, h\}$ contain none of the consecutive patterns ab, cd, ef, or gh?

Exercise 37.2.9. How many permutations of [7] contain at least one of the consecutive increasing patterns 123, 345, or 567?

Exercise 37.2.10. Determine the number of nonnegative integer solutions to

$$x_1 + x_2 + x_3 + x_4 = 20$$

satisfying $x_1 \leq 7$, $x_2 \leq 5$, $x_3 \leq 6$, and $x_4 \leq 4$.

Exercise 37.2.11. Eight people sit in a row. How many seatings avoid all three of the following adjacency restrictions?

- Alice cannot sit next to Bob
- Claire cannot sit next to Diana
- Evan cannot sit next to Fiona

Exercise 37.2.12. How many lattice paths from $(0, 0)$ to $(10, 10)$ using only steps $(1, 0)$ and $(0, 1)$ avoid all three points $(3, 3)$, $(5, 6)$, and $(7, 5)$?

Part VII.

Appendix

A. Constructing the Naturals

In this course, we take the natural numbers for granted, but it is possible to construct them formally inside modern set theory. The most commonly used foundation is *Zermelo–Fraenkel set theory with the Axiom of Choice* (ZFC).

A.1. The ZFC Axioms (Informal List)

ZFC is a collection of axioms that govern the behavior of sets.

- **Extensionality:** Two sets are equal if and only if they have the same elements.
- **Empty Set:** There exists a set, denoted $\varnothing$, with no elements.
- **Pairing:** For any sets a and b, there exists a set $\{a, b\}$.
- **Union:** For any set A, there exists a set $\bigcup A$ whose elements are exactly those belonging to members of A.
- **Power Set:** For any set A, there exists a set $\mathcal{P}(A)$ whose elements are all subsets of A.
- **Specification (Subset Axiom Scheme):** Given any set A and any property $P(x)$ (expressible in the language of set theory), there exists a set $\{x \in A \mid P(x)\}$.
- **Replacement (Axiom Scheme):** The image of any set under any definable function is itself a set.
- **Infinity:** There exists an *inductive set* I such that $\varnothing \in I$ and for all $x \in I$, the successor $x \cup \{x\}$ is also in I.
- **Foundation (Regularity):** Every non-empty set A contains an element a that is disjoint from A (i.e., $a \cap A = \varnothing$).
- **Choice:** For any collection of nonempty sets, there is a function that chooses one element from each set.

The *Axiom of Infinity* is crucial here: it guarantees the existence of at least one inductive set from which we can build the natural numbers. (The Axiom of Choice is not needed for $\mathbb{N}$ itself, but is included in ZFC for broader mathematics.)

A.2. The Successor Function

Define the *successor* of a set x as

$$S(x) := x \cup \{x\}.$$

This ensures $x \in S(x)$ and $x \subsetneq S(x)$, mimicking the intuitive "add one" operation.

A.3. Defining $\mathbb{N}$

The Axiom of Infinity provides an inductive set I. However, I may contain extra elements. To obtain the *smallest* inductive set, we apply the Axiom of Specification to define:

$$\mathbb{N} := \bigcap \{X \subseteq I : \varnothing \in X \text{ and } \forall x \in X,\ S(x) \in X\}.$$

This set $\mathbb{N}$ is the intersection of all inductive subsets of I. It is itself inductive and is the unique minimal inductive set.

A.4. The von Neumann Ordinals

With this construction, each natural number is identified with a specific set:

$$\begin{aligned}
0 &:= \varnothing, \\
1 &:= S(0) = \{\varnothing\} = \{0\}, \\
2 &:= S(1) = \{\varnothing, \{\varnothing\}\} = \{0, 1\}, \\
3 &:= S(2) = \{0, 1, 2\}, \\
&\vdots \\
n &:= \{0, 1, 2, \ldots, n-1\}.
\end{aligned}$$

In other words, each n is the set of all smaller natural numbers. This construction also defines the usual ordering: $m < n$ if and only if $m \in n$.

A.5. Arithmetic on $\mathbb{N}$

Addition and multiplication can be defined recursively using the successor function. For example, addition is defined by:

$$\begin{aligned}
m + 0 &:= m, \\
m + S(n) &:= S(m + n).
\end{aligned}$$

From these definitions, all familiar properties of arithmetic (commutativity, associativity, distributivity, etc.) can be derived using induction. This development is rigorous but lengthy, and is typically studied in more advanced logic or set theory courses.

A.6. Induction as a Theorem

Since $\mathbb{N}$ is defined as the smallest inductive set, the Principle of Mathematical Induction follows as a theorem in ZFC.

Theorem A.6.1 (Principle of Mathematical Induction)**.** *Let $X \subseteq \mathbb{N}$. If:*

1. $0 \in X$*, and*
2. $\forall n \in \mathbb{N},\ (n \in X \implies S(n) \in X)$*,*

then $X = \mathbb{N}$.

Proof Sketch. The assumptions say that X is inductive. Since $\mathbb{N}$ is defined as the intersection of all inductive sets contained in some inductive I, it follows that $\mathbb{N} \subseteq X$. The reverse inclusion $X \subseteq \mathbb{N}$ is immediate from the definition of X as a subset of $\mathbb{N}$. Hence $X = \mathbb{N}$. □

This theorem directly implies the familiar induction principle for statements: if a property $P(n)$ holds for $n = 0$ and $P(n)$ implies $P(n + 1)$ for all n, then $P(n)$ holds for all $n \in \mathbb{N}$ (by considering the set $X = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$).

Solutions/Hints for Exercises

Solutions and Hints

1. August 25

Exercise 1.2.1

Which of the following are *mathematical statements*? Justify your answer.

(a) Pittsburgh has the most bridges of any city in the world.

Solution. This is a mathematical statement.

(b) Pittsburgh is the best city in the world.

Solution. Maybe. We would need a formal definition of "best" in order for this to be a statement.

(c) Where is Pittsburgh?

Solution. This is not a statement.

(d) 2 is a prime number.

Solution. This is a statement.

(e) n is a prime number.

Solution. This is not a statement. (n is a free variable.)

(f) All positive integers are prime.

Solution. This is a statement.

(g) If n is an even integer greater than 3 then n can be written as the sum of 2 primes.

Solution. This is a statement.

(h) $5^2 = 25$.

Solution. This is a statement.

(i) $x^3 + 1 = 28$.

Solution. This is not a statement. (x is a free variable.)

(j) If $x^3 + 1 = 28$ then $x = 3$.

Solution. This is not a statement. (x is still a free variable.)

Exercise 1.2.2

Consider the following theorem and proof:

Theorem: If m and $m + n$ are both even integers then n is an even integer.

Proof: Let $m = 2a$ and $n = 2b$, where a and b are integers. Then $m + n = 2a + 2b$. Subtracting m from both sides we get

$$n = 2a + 2b - m = 2a + 2b - 2a = 2b$$

Therefore we have shown n is even. □

(a) Is this theorem true?

Solution. Yes. This is a true statement.

(b) Is the proof valid and well written? Explain your reasoning.

Solution. The proof is invalid, but not poorly written. In the theorem, the assumptions were that m and $m + n$ were both even, but in the proof the author assumed m and n were even. In particular, the author used cyclic reasoning by assuming n was even in order to prove that n was even.

(c) If your answer to (a) is yes and (b) is no, try to fix the proof. What are the basic assumptions of this proposition? If your answer to (a) is no, try to fix the proposition to make it true and then prove it.

Proof. Let m and n be integers such that m and $m+n$ are both even. Then there exists integers a and b such that $m = 2a$ and $m + n = 2b$. Then

$$\begin{aligned} n &= (m + n) - m \\ &= 2b - 2a \\ &= 2(b - a) \end{aligned}$$

Since $b - a$ is an integer, we have shown that n is even. □

Exercise 1.2.3

1. Consider the following proposition and the proposed proof given by a student:

   Proposition: $\sqrt{xy} \leq \frac{x+y}{2}$

Proof:

$$\begin{aligned} 0 \leq (x-y)^2 &\implies 0 \leq x^2 - 2xy + y^2 \\ &\implies 4xy \leq x^2 + 2xy + y^2 \\ &\implies xy \leq \frac{(x+y)^2}{4} \\ &\implies \sqrt{xy} \leq \frac{x+y}{2} \end{aligned}$$

□

a) Is the proposition true? Are the assumptions stated clearly?

Solution. The proposition is false and poorly written. Without declaring the variables, the "proposition" itself is not a mathematical statement. Moreover, this statement isn't true if x or y is allowed to be negative. Consider $x = y = -1$. Then the LHS is positive while the RHS is negative, making the proposition false. Additionally, if x is positive and y is negative (or vice versa) then the statement doesn't make any sense, even extending to the complex numbers.

b) Is the proof valid and well written? Explain your reasoning.

Solution. The proof can't be valid since the statement is false if x and y are allowed to be arbitrary real numbers. In particular, the proof is invalid in the last step when taking the square root. For one, $\sqrt{xy}$ may not be defined in the reals. For another, $\sqrt{\frac{(x+y)^2}{4}} = \frac{|x+y|}{2}$, which is not necessarily equal to $\frac{x+y}{2}$.

c) If the proposition is true but the proof is not fully correct, try to fix the proof. If the proposition is false, propose a corrected statement and prove it.

New Proposition: For any nonnegative real numbers x and y, $\sqrt{xy} \leq \frac{x+y}{2}$.

Proof. Let x and y be arbitrary nonnegative real numbers. Since $x \geq 0$ and $y \geq 0$, the square roots $\sqrt{x}$ and $\sqrt{y}$ are defined (as real numbers). Furthermore, the square of any real number is nonnegative. Therefore:

$$\begin{aligned} 0 &\leq (\sqrt{x} - \sqrt{y})^2 \\ &= x - 2\sqrt{xy} + y. \end{aligned}$$

Adding $2\sqrt{xy}$ to both sides of the inequality yields:

$$2\sqrt{xy} \leq x + y.$$

Dividing both sides by 2 gives the desired result:

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

□

2. Let x, y, z be nonnegative real numbers such that $y + z \geq 2$. Using what you have learned from the previous problems:

   a) Write a proposition stating that under these conditions $(x+y+z)^2 \geq 4x+4yz$.

   Proposition. For all nonnegative real numbers x, y, z, if $y + z \geq 2$ then $(x + y + z)^2 \geq 4x + 4yz$.

   b) Prove your proposition.

   Proof. Let x, y, z be nonnegative real numbers such that $y+z \geq 2$. Recall that for any real numbers a and b, $a^2 + b^2 \geq 2ab$, which follows from $(a - b)^2 \geq 0$. We proceed with the following derivation:

$$\begin{aligned}(x + y + z)^2 &= x^2 + 2x(y + z) + (y + z)^2 \\ &\geq 0 + 2x(2) + (y^2 + z^2 + 2yz) && \text{(since } x^2 \geq 0 \text{ and } y + z \geq 2\text{)} \\ &\geq 4x + (2yz + 2yz) && \text{(since } y^2 + z^2 \geq 2yz\text{)} \\ &= 4x + 4yz.\end{aligned}$$

   This establishes the desired inequality. □

Exercise 1.2.4

A father, mother, and son were dining when another family (also a father, mother, and son) noticed their resemblance. The second father asked, "How old are you? We must be around the same age." The first father, a mathematician, replied cryptically: "Our ages sum to 72, I am six times as old as my son, and when I am twice his age later in life, our combined ages will double our current total."

Set up a system of equations based on this information and determine the ages of the three family members.

Solution. Let f denote the father's age, m denote the mother's age, and s denote the son's age. Then we have the following system of equations:

(1) $f + m + s = 72$ (Ages sum to 72)

(2) $f = 6s$ (Father is six times as old as his son)

(3) Let t be the number of years from now until the father is twice his son's age. At that time:

$$\begin{aligned}f + t &= 2(s + t) && \text{(Father is twice as old as son)} \\ (f + t) + (m + t) + (s + t) &= 2 \cdot 72 && \text{(Combined ages double)}\end{aligned}$$

The ages are: $\boxed{f = 36,\ m = 30, \text{ and } s = 6}$

Exercise 1.2.5

(a) Solve the following system of equations for (x, y, z):

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 8 \\ x - 2y - z &= -2 \end{aligned}$$

Solution. $\boxed{(x, y, z) = (11, 9, -5)}$

(b) Solve the similar system for (x, y, z):

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 9 \\ x - 2y - z &= -2 \end{aligned}$$

Solution. $\boxed{(x, y, z) = \left(\frac{32}{3}, \frac{25}{3}, -4\right)}$

(c) Solve one more similar system:

$$\begin{aligned} x + y + z &= 15 \\ 2x - y + z &= 9 \\ x - 2y - z &= -1 \end{aligned}$$

Solution. $\boxed{(x, y, z) = \left(\frac{34}{3}, \frac{26}{3}, -5\right)}$

(d) Compare the results:

(i) From part (a) to part (b), find the magnitude of the change in each variable:

$$|\Delta x|, \quad |\Delta y|, \quad |\Delta z|.$$

Repeat for the change from part (b) to part (c).

Solution.

- From (a) to (b): $|\Delta x| = \frac{1}{3}$, $|\Delta y| = \frac{2}{3}$, $|\Delta z| = 1$
- From (b) to (c): $|\Delta x| = \frac{2}{3}$, $|\Delta y| = \frac{1}{3}$, $|\Delta z| = 1$

(ii) Which variable's value is most affected by these small changes in the equations? Which is least affected?

Solution. In each case, z changed the most. From (a) $\to$ (b), x changed the least, while from (b) $\to$ (c), y changed the least.

(iii) How do the ratios of the largest to smallest changes compare between the two transitions (from (a)$\to$(b) and (b)$\to$(c))?

Solution. The ratio of the largest change to the smallest change is $3:1$ in both transitions.

(iv) Based on your results, what can you say about how the solution responds when you slightly change the constants on the right-hand sides?

Solution. It appears that the ratio of the largest change to the smallest change in the variables remains constant at $3:1$ as the constants on the right-hand side are changed, even though different variables may change the most or least in each case. This reflects a consistent, linear relationship between the changes in the equations and the changes in the solution.

2. August 27

Exercise 2.1.4

Define sets A, B, and C as follows:

$$A = \{1, 2, 3, 4, 5, 6\}$$
$$B = \{1, 2, 3, 4, 5, 6, \{1, 2\}, \{3\}, \{5\}\}$$
$$C = \{x \in A \mid x^2 > 4\}$$

Determine whether the following statements are true or false.

(a) $3 \in A$ — True

(b) $\{3\} \in B$ — True

(c) $\{1, 2\} \subseteq A$ — True

(d) $A \in B$ — False

(e) $\{1, 2\} \in B$ — True

(f) $4 \in C$ — True

(g) $\{x \in B \mid x \notin A\} = \{\{1,2\},\{3\},\{5\}\}$ True

(h) $\{6\} \in A$ False

(i) $C \subseteq A$ True

(j) $\{1,2\} \subseteq B$ True

(k) $3 \in B$ True

(l) $\{3\} \in A$ False

(m) $\{4\} \subsetneq C$ True

(n) $B \subseteq A$ False

(o) $\{\{3\}\} \subseteq B$ True

(p) $A \subseteq B$ True

(q) $5 \subseteq B$ False

(r) $\{x \in B \mid x \notin A\} = \{1,2,3,5\}$ False

(s) $\{x \in B \mid x \notin A\} = \{\}$ False

(t) $D \subseteq C$ where $D = \{x \in A \mid x \text{ is even}\}$ False

(u) $\{\{1,2\},\{3\}\} \subseteq B$ True

Exercise 2.1.7

Write the following sets out in formal set-builder notation.

(a) A is the set of integers that can be expressed as the difference of two perfect squares.

Solution. $\boxed{A = \{n \in \mathbb{Z} \mid \text{there exists } a, b \in \mathbb{Z} \text{ such that } n = a^2 - b^2\}}$

(b) $B = \{1, 8, 27, 64, \ldots\}$ *(Assume the pattern continues indefinitely.)*

Solution. $\boxed{B = \{n \in \mathbb{N} \mid n > 0 \text{ and there exists } a \in \mathbb{N} \text{ such that } n = a^3\}}$

(c) C is the set of all positive divisors of 36.

Solution. $\boxed{C = \{n \in \mathbb{N} \ : \ n \mid 36\}}$

Exercise 2.1.8

Determine if the following statements are True or False. Justify your answer.

(a) $0 \mid 5$

Solution. $\boxed{\text{False}}$. For any $m \in \mathbb{Z}$, $0 \cdot m = 0 \neq 5$.

(b) $5 \mid 0$

Solution. $\boxed{\text{True}}$. $0 = 5 \cdot 0$.

(c) For $a, b \in \mathbb{Z}$, if $a \mid b$ then $a \leq b$.

Solution. $\boxed{\text{False}}$. $2 \mid -4$ but $2 \not\leq -4$

(d) For $a, b \in \mathbb{N}$, if $a \mid b$ then $a \leq b$.

Solution. $\boxed{\text{False}}$. $5 \mid 0$ but $5 \not\leq 0$.

(e) The remainder, r, when an integer a is divided by a nonzero integer b is always nonnegative.

Solution. $\boxed{\text{True}}$. $0 \leq r < |b|$.

Exercise 2.1.9

(a) Provide an example of $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ and $ab \mid c$

Possible Solution. $a = 2$, $b = 3$, $c = 6$

(b) Provide an example of $a, b, c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$ but $ab \nmid c$

Possible Solution. $a = 3$, $b = 3$, $c = 6$

3. August 29

Exercise 3.1.3

For each pair (a, b), find the unique integers q (quotient) and r (remainder) guaranteed by the Division Algorithm.

(a) $a = 17$, $b = 5$

Solution. $17 = 5(3) + 2$. $\boxed{q = 3,\ r = 2}$

(b) $a = -17$, $b = 5$

Solution. $-17 = 5(-4) + 3$. $\boxed{q = -4,\ r = 3}$

(c) $a = 84$, $b = -12$

Solution. $84 = -12(-7) + 0$. $\boxed{q = -7,\ r = 0}$

(d) $a = 7$, $b = 9$

Solution. $7 = 9(0) + 7$. $\boxed{q = 0,\ r = 7}$

Exercise 3.1.4

Prove the following statement: For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Scaffolding: Let $a, b, c \in \mathbb{Z}$ be arbitrary and fixed integers such that $a \mid b$ and $a \mid c$.

- Write down the formal definition of $a \mid b$.

  Answer. $a \mid b$ implies $b = am$ for some $m \in \mathbb{Z}$.

- Write down the formal definition of $a \mid c$.

  Answer. $a \mid c$ implies $c = an$ for some $n \in \mathbb{Z}$.

- Add the two equations from Step 1 and Step 2 together.

  Answer. $b + c = am + an$

- Factor the resulting sum on the right-hand side.

  Answer. $b + c = a(m + n)$.

- Explain why the result of Step 4 satisfies the definition of $a \mid (b + c)$.

  Answer. Let $k = m + n$. Then, by Step 4, we have $b + c = ak$. Moreover, $k \in \mathbb{Z}$ since the integers are closed under addition and $m, n \in \mathbb{Z}$. Therefore, $a \mid (b + c)$.

Exercise 3.1.6

(a) Write the following set in roster notation:

$$A = \left\{ n \in \mathbb{Z} \mid \text{there exists } r \in \mathbb{Q} \text{ s.t. } n = r + \frac{1}{r} \right\}$$

Solution. $\boxed{A = \{-2, 2\}}$

(b) Describe the following set in formal set-builder notation. You may assume that the pattern continues indefinitely.

$$C = \left\{ \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots \right\}$$

Solution. $\boxed{C = \left\{ x \in \mathbb{Q} \mid \text{there exists } n \in \mathbb{Z}^+ \text{ s.t. } x = \frac{n}{n+1} \right\}}$

(c) Define the sets A and B as follows:

$$A = \{x \in \mathbb{R} \mid x^2 - 4 \geq 0\}$$
$$B = \{y \in \mathbb{R} \mid y \geq 2\}$$

Does $A = B$? Why or why not?

Solution. $\boxed{A \neq B}$. While $B \subseteq A$, $A \not\subseteq B$. There exists elements $a \in A$ such that $a \notin B$. For instance, $-3 \in A$ but $-3 \notin B$.

Exercise 3.1.7

(a) Provide an example of a rational number q and an irrational number x such that qx is irrational.

Possible Solution. $q = 1$, $x = \sqrt{2}$

(b) Provide an example of a rational number q and an irrational number x such that qx is rational.

Possible Solution. $q = 0$, $x = \sqrt{2}$

Exercise 3.2.1

In propositional logic, a *tautology* is a propositional formula which is always true, regardless of the truth values of the propositional variables. Use a truth table to determine whether or not the following statement is a tautology.

$$((P \to Q) \wedge \neg Q) \to \neg P$$

Solution.

P	Q	$P \to Q$	$(P \to Q) \wedge \neg Q$	$((P \to Q) \wedge \neg Q) \to \neg P$
T	T	T	F	T
T	F	F	F	T
F	T	T	F	T
F	F	T	T	T

$((P \to Q) \wedge \neg Q) \to \neg P$ $\boxed{\text{is a tautology}}$.

Exercise 3.2.2

Define the propositions P, Q, and R as follows:

$$\begin{aligned} P &:= \text{“It is raining.”} \\ Q &:= \text{“There are bears in the area.”} \\ R &:= \text{“It is not safe outside.”} \end{aligned}$$

Write each of the following statements symbolically:

(a) It is raining, but there are no bears in the area.

(b) It is unsafe outside whenever bears are in the area and it is raining.

(c) It is not safe outside even though there is neither rain nor bears in the area.

(d) For it to be safe outside, it is necessary but not sufficient that there are no bears in the area.

Solutions.

(a) $P \wedge (\neg Q)$

(b) $(Q \wedge P) \to R$ or $(Q \to R) \wedge P$, depending on interpretation.

(c) $R \wedge (\neg Q \wedge \neg P)$

(d) $(\neg R) \to (\neg Q)$

4. September 3

Exercise 4.1.9

Use truth tables to determine whether or not the given propositional formulae σ_1 and σ_2 are logically equivalent.

$$\begin{aligned} \sigma_1 &= (P \vee Q) \to R \\ \sigma_2 &= (P \to R) \wedge (Q \to R) \end{aligned}$$

Solution. $\boxed{\sigma_1 \equiv \sigma_2}$

P	Q	R	$P \vee Q$	σ_1	$P \to R$	$Q \to R$	σ_2
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Exercise 4.1.10

Write the contrapositive of the following statements in natural, idiomatic English.

(a) If I do my assignments, I will get a good grade in the course.

(b) I will not be late unless there is traffic.

Solution.

(a) "If I get a bad grade in this course, then I didn't do my assignments."

(b) "If I am late then there was traffic."

Exercise 4.1.18

Consider the following propositions involving sets A, B, and C:

$$\sigma_1 := \forall x \in A, \exists y \in B, (x + y \in C)$$
$$\sigma_2 := \exists y \in B, \forall x \in A, (x + y \in C)$$

(a) Provide an example of sets A, B, and C where σ_1 is true and σ_2 is false. If no such example exists, explain why.

(b) Provide an example of sets A, B, and C where σ_1 is false and σ_2 is true. If no such example exists, explain why.

Solution.

(a) Consider $A = B = \{1, 2\}$ and $C = \{3\}$.

- For σ_1: We must check whether, for each $x \in A$, there exists a corresponding $y \in B$ such that $x + y \in C$.

- When $x = 1$, choosing $y = 2$ gives $1 + 2 = 3$, which is in C.
- When $x = 2$, choosing $y = 1$ gives $2 + 1 = 3$, which is also in C.

Therefore, σ_1 is true.

- For σ_2: We must check if there exists a single $y \in B$ such that for all $x \in A$, $x + y \in C$.
  - If $y = 1$, then for $x = 1$, $1 + 1 = 2$, which is not in C.
  - If $y = 2$, then for $x = 2$, $2 + 2 = 4$, which is also not in C.

  Thus, σ_2 is false.

(b) This is not possible. Suppose that σ_2 is true, i.e., there exists a $y \in B$ such that for all $x \in A$, $x + y \in C$. Fix this y. Then, for each $x \in A$, we know $x + y \in C$ for this specific value of y. This satisfies the condition of σ_1, which asserts that for every $x \in A$, there exists a $y \in B$ such that $x + y \in C$. Hence, σ_1 must also be true. Therefore, it is not possible for σ_1 to be false while σ_2 is true.

Exercise 4.1.19

Using the standard number sets ($\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$) and logical symbols ($\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$), along with basic arithmetic symbols ($+$, $-$, $\cdot$, $<$, $>$, $=$, $\neq$) and constants (0, 1, -1, etc.), write the following statements in symbolic form:

(a) The product of two nonpositive real numbers is always nonnegative.

(b) The only integers that have a multiplicative inverse in the set of integers are 1 and -1.

(c) For any integer n, n is odd if and only if $n^2 - 1$ is divisible by 8.

Solution.

(a) $\forall x, y \in \mathbb{R}, ((x \leq 0 \wedge y \leq 0) \rightarrow (0 \leq xy))$

(b) $\forall n \in \mathbb{Z}, ((\exists m \in \mathbb{Z}, mn = 1) \leftrightarrow (n = 1 \vee n = -1))$

(c) $\forall n \in \mathbb{Z}, ((\exists m \in \mathbb{Z}, n = 2m + 1) \leftrightarrow (\exists k \in \mathbb{Z}, n^2 - 1 = 8k))$

5. September 5

Exercise 5.1.4

Write the logical negation of the following statements in maximally negated form. Next, determine whether the original statement or its negation is true, and briefly explain your

reasoning. No formal proof is required.

(a) $\forall x \in \mathbb{R}, \big(-1 < x < 1 \to \exists y \in \mathbb{R}, \big(-1 < y < 1 \wedge y^2 = x^3\big)\big)$

Solution.

$$\exists x \in \mathbb{R}, \Big(-1 < x < 1 \wedge \forall y \in \mathbb{R}, (y \leq -1 \vee y \geq 1 \vee y^2 \neq x^3)\Big)$$

The negation of the original proposition is true. Consider $x = -\frac{1}{2}$. Then $x^3 = -\frac{1}{8}$, which does not have a real square root, let alone one between -1 and 1. Therefore, there is some x in the interval $(-1, 1)$ for which no such y exists, proving the negation to be true.

(b) $\forall x, y \in \mathbb{R}, (x = y \leftrightarrow \forall \varepsilon \in \mathbb{R}, (\varepsilon > 0 \to |x - y| < \varepsilon)\,)$

Solution.

$$\exists x, y \in \mathbb{R}, \Big((x = y \wedge \exists \varepsilon \in \mathbb{R}, (\varepsilon > 0 \wedge |x-y| \geq \varepsilon)) \vee (x \neq y \wedge \forall \varepsilon \in \mathbb{R}, (\varepsilon > 0 \to |x-y| < \varepsilon))\Big)$$

The original proposition is true. Two real numbers x and y are equal if and only if their difference is zero, which happens if and only if their difference is less than every positive real number. The forward and reverse implications match the conditions of equality, confirming that the original statement is true.

Exercise 5.2.3

Prove that there are no integer solutions to the equation $m^2 = 3n + 2$.

Proof. Assume for the sake of contradiction that there exist $m, n \in \mathbb{Z}$ with $m^2 = 3n+2$. By the Division Algorithm, we can uniquely write $m = 3q + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. We consider the possible values of r:

- Case 1: $r = 0$. Then $m = 3q$, so $m^2 = 9q^2 = 3(3q^2)$. Thus m^2 is divisible by 3, so its remainder upon division by 3 is 0. But $3n + 2$ has remainder 2, so equality is impossible.
- Case 2: $r = 1$. Then $m = 3q + 1$, so
$$m^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1.$$
Thus m^2 has remainder 1 upon division by 3, which again cannot equal $3n + 2$.
- Case 3: $r = 2$. Then $m = 3q + 2$, so
$$m^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1.$$
Thus m^2 also has remainder 1 upon division by 3, so equality is impossible here as well.

Since these are the only possible cases for m, and each leads to a contradiction, we conclude that there are no integers m, n satisfying $m^2 = 3n + 2$. □

Exercise 5.2.4

Let $A = \{x \in \mathbb{R} \mid x^2 - 6x + 5 > 0\}$ and $B = (-\infty, 1)$. Prove that $B \subseteq A$.

Proof. Let $x \in B$ be arbitrary but fixed. Then $x \in \mathbb{R}$ with $x < 1$. Factor

$$x^2 - 6x + 5 = (x - 1)(x - 5).$$

Because $x < 1$, we have $x - 1 < 0$, and since $x < 1 < 5$, we also have $x - 5 < 0$. The product of two negative numbers is positive, so

$$x^2 - 6x + 5 = (x - 1)(x - 5) > 0.$$

Therefore $x \in A$. Since $x \in B$ was arbitrary, we conclude $B \subseteq A$. □

6. September 8

Exercise 6.1.3

Returning to exercise 5.2.4, let $A = \{x \in \mathbb{R} \mid x^2 - 6x + 5 > 0\}$ and $B = (-\infty, 1)$. Prove that $A \not\subseteq B$.

Proof. Consider $x = 6 \in \mathbb{R}$. Then $x \in A$ because

$$x^2 - 6x + 5 = 36 - 36 + 5 = 5 > 0.$$

However, $x \notin B$ because $x \not< 1$. Since there exists an element $x \in A$ such that $x \notin B$, we conclude that $A \not\subseteq B$.

Exercise 6.1.4

Prove the following propositions:

(a) $\exists x \in \mathbb{R}, |x^3| < x^2$

Proof. Consider $x = \frac{1}{2} \in \mathbb{R}$. Then

$$|x^3| = \frac{1}{8} < \frac{1}{4} = x^2.$$

Therefore, there exists $x \in \mathbb{R}$ such that $|x^3| < x^2$. □

(b) For $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_{n+1} \in [0, 1]$, it is the case that:

$$\exists\, i < j \in [n+1], |x_i - x_j| \leq \frac{1}{n}.$$

Proof. Break the interval $[0,1]$ up into the n subintervals

$$I_k = \begin{cases} [\,\frac{k-1}{n}, \frac{k}{n}\,) & \text{for } k = 1, 2, \ldots, n-1, \\ [\,\frac{n-1}{n}, 1\,] & \text{for } k = n. \end{cases}$$

Each I_k has length $\frac{1}{n}$, and the family $\{I_1, \ldots, I_n\}$ covers $[0,1]$.

Place the $n+1$ points $x_1, \ldots, x_{n+1}$ into these n intervals. By the Pigeonhole Principle (Theorem 6.1.2), some interval I_k must contain at least two of the points, say x_i and x_j with $i \neq j$. Since both x_i and x_j lie in the same interval I_k of length $\frac{1}{n}$, their distance satisfies

$$|x_i - x_j| \leq \frac{1}{n}.$$

If desired, we may reorder indices so that $i < j$, and the claim follows. □

Exercise 6.1.8

Consider the following proposition:

$$\forall n \in \mathbb{Z}, \big(\exists m \in \mathbb{Z}, \big(2n^2 + 3 = 5m\big) \to \forall k \in \mathbb{Z}, (n \neq 5k)\big)$$

(a) Write the logical negation of this proposition in maximally negated form.

Solution.

$$\exists n \in \mathbb{Z}, ((\exists m \in \mathbb{Z}, 2n^2 + 3 = 5m) \wedge (\exists k \in \mathbb{Z}, n = 5k))$$

(b) Prove or disprove the original proposition. Clearly state any assumptions, provide justifications for your steps, and write a formal proof using only the properties of integers in an organized manner.

Proof of Original Proposition.

We prove the proposition by contraposition. Let $n \in \mathbb{Z}$ be a multiple of 5, so there exists $k \in \mathbb{Z}$ with $n = 5k$. Then

$$\begin{aligned} 2n^2 + 3 &= 2(5k)^2 + 3 \\ &= 50k^2 + 3 \\ &= 5(10k^2) + 3. \end{aligned}$$

By the Division Algorithm, this shows that when $2n^2 + 3$ is divided by 5, the quotient is $10k^2$ and the remainder is 3. In particular, the remainder is not 0. Therefore, $2n^2 + 3$ cannot equal $5m$ for any $m \in \mathbb{Z}$.

This establishes that if n is divisible by 5, then there does not exist $m \in \mathbb{Z}$ such that $2n^2 + 3 = 5m$. By contraposition, the original proposition holds. □

We'll be able to write up this proof more nicely once we've discussed the modular congruence relation and modular arithmetic.

Exercise 6.1.9

Prove or disprove the following proposition. Clearly state any assumptions, provide detailed justifications for your steps, and write a formal proof using only the definitions of even and odd integers and the assumed properties of integer arithmetic.

Proposition: If n is an integer then $n^2 + n - 41$ is an odd number.

Proof. Let $n \in \mathbb{Z}$ (be arbitrary and fixed). Since n is an integer, n is either even or odd. We will consider both cases.

- Case 1: n is even. Then $n = 2m$ for some $m \in \mathbb{Z}$. Thus,

$$\begin{aligned} n^2 + n - 41 &= (2m)^2 + (2m) - 41 \\ &= 4m^2 + 2m - 41. \end{aligned}$$

  Factoring out 2:

$$n^2 + n - 41 = 2(2m^2 + m - 21) + 1.$$

  Since $2m^2 + m - 21 \in \mathbb{Z}$, $n^2 + n - 41$ is odd, as desired.

- Case 2: n is odd. Then $n = 2m + 1$ for some $m \in \mathbb{Z}$. Thus,

$$\begin{aligned} n^2 + n - 41 &= (2m + 1)^2 + (2m + 1) - 41 \\ &= (4m^2 + 4m + 1) + (2m + 1) - 41 \\ &= 4m^2 + 6m - 39. \end{aligned}$$

  Factoring out 2:

$$n^2 + n - 41 = 2(2m^2 + 3m - 20) + 1.$$

  Since $2m^2 + 3m - 20 \in \mathbb{Z}$, $n^2 + n - 41$ is odd, as desired.

Since these are the only possible cases for n, we conclude that $n^2 + n - 41$ is odd for all integers n. □

Exercise 6.1.10

Prove the following proposition:

$$\forall x, y \in \mathbb{R}, (x + y \geq 0 \to x^3 + y^3 \geq x^2 y + x y^2)$$

Proof. Let $x, y \in \mathbb{R}$ with $x + y \geq 0$. We want to show that

$$x^3 + y^3 \geq x^2y + xy^2.$$

Consider $(x - y)^2$. Since the square of any real number is nonnegative,

$$(x - y)^2 \geq 0.$$

Multiplying both sides by $x + y \geq 0$ gives

$$(x + y)(x - y)^2 \geq 0.$$

Expanding the left-hand side,

$$(x + y)(x - y)^2 = (x + y)(x^2 - 2xy + y^2) = x^3 + y^3 - x^2y - xy^2.$$

Thus,

$$x^3 + y^3 - (x^2y + xy^2) \geq 0,$$

which is equivalent to

$$x^3 + y^3 \geq x^2y + xy^2.$$

Therefore, $x + y \geq 0$ implies $x^3 + y^3 \geq x^2y + xy^2$, as desired. □

7. September 10

Exercise 7.1.6

Using just the definition of divisibility and the properties of the integers, prove that for all integers n, $3 \mid n^2 - 1$ if and only if $3 \nmid n$.

Below we demonstrate 2 valid methods for proving this statement.

Proof 1 (Contrapositive/Direct Approach). Let $n \in \mathbb{Z}$.

- ($\Rightarrow$): We prove the contrapositive. Assume $3 \mid n$. Then, by definition of divisibility, $n = 3k$ for some $k \in \mathbb{Z}$, so

  $$n^2 - 1 = (3k)^2 - 1 = 9k^2 - 1 = 3(3k^2) - 1 = 3(3k^2 - 1) + 2.$$

  Since $3k^2 - 1 \in \mathbb{Z}$, we have that $n^2 - 1$ has a remainder of 2 when divided by 3, and hence is not divisible by 3. Thus,

  $$3 \mid n^2 - 1 \Longrightarrow 3 \nmid n.$$

- ($\Leftarrow$): Assume $3 \nmid n$. By the division algorithm write $n = 3q + r$ with $q \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. Since $3 \nmid n$ we must have $r \in \{1, 2\}$.

- If $r = 1$, then $n = 3q + 1$ and

$$n^2 - 1 = (3q + 1)^2 - 1 = 9q^2 + 6q = 3(3q^2 + 2q).$$

  Since $3q^2 + 2q \in \mathbb{Z}$, $3 \mid n^2 - 1$.

- If $r = 2$, then $n = 3q + 2$ and

$$n^2 - 1 = (3q + 2)^2 - 1 = 9q^2 + 12q + 3 = 3(3q^2 + 4q + 1).$$

  $3q^2 + 4q + 1 \in \mathbb{Z}$, so again $3 \mid n^2 - 1$.

In both cases we have $3 \mid n^2 - 1$. Thus,

$$3 \nmid n \implies 3 \mid n^2 - 1.$$

Combining the two implications proves the desired equivalence. □

Proof 2 (Exhaustive Case Analysis). By the division algorithm, for any $n \in \mathbb{Z}$ there exist unique integers q and r with $0 \leq r \leq 2$ such that $n = 3q + r$. We consider the three cases.

- **Case $r = 0$.** Then $n = 3q$ and

$$n^2 - 1 = (3q)^2 - 1 = 9q^2 - 1 = 3(3q^2) - 1 = 3(3q^2 - 1) + 2,$$

  so $3 \nmid n^2 - 1$. Hence in this case $3 \nmid n^2 - 1$ and $3 \mid n$.

- **Case $r = 1$.** Then $n = 3q + 1$ and

$$n^2 - 1 = (3q + 1)^2 - 1 = 9q^2 + 6q = 3(3q^2 + 2q),$$

  so $3 \mid n^2 - 1$ and $3 \nmid n$.

- **Case $r = 2$.** Then $n = 3q + 2$ and

$$n^2 - 1 = (3q + 2)^2 - 1 = 9q^2 + 12q + 3 = 3(3q^2 + 4q + 1),$$

  so $3 \mid n^2 - 1$ and $3 \nmid n$.

Thus $3 \mid n^2 - 1$ exactly in the cases $r = 1, 2$, i.e. precisely when $3 \nmid n$, proving the equivalence. □

Exercise 7.1.7

Prove the following proposition:

$$\forall x, y \in \mathbb{R}, \big(x \neq y \to \big((x + 1)^2 = (y + 1)^2 \leftrightarrow x + y = -2\big)\big)$$

Proof. Let $x, y \in \mathbb{R}$ such that $x \neq y$.

($\Rightarrow$) Suppose that $(x+1)^2 = (y+1)^2$. Taking square roots of both sides, we get:

$$|x+1| = |y+1|.$$

This equation implies two possibilities:

$$x+1 = y+1 \quad \text{or} \quad x+1 = -(y+1).$$

- In the first case, $x+1 = y+1$, subtracting 1 from both sides yields $x = y$, which contradicts our assumption that $x \neq y$. Therefore, this case cannot occur.
- In the second case, $x+1 = -(y+1)$. Simplifying this gives:

$$x+1 = -y-1$$

which can be rearranged to:

$$x+y = -2$$

Hence, if $(x+1)^2 = (y+1)^2$, then $x+y = -2$, as required.

($\Leftarrow$) Now, suppose that $x+y = -2$. We can rearrange this as:

$$x+1 = -y-1$$

Squaring both sides of this equation, we obtain:

$$(x+1)^2 = (-y-1)^2$$

Since squaring removes the negative sign, we have:

$$(x+1)^2 = (y+1)^2$$

which is the desired result.

Thus, we have shown that $(x+1)^2 = (y+1)^2$ if and only if $x+y = -2$, provided $x \neq y$. □

Exercise 7.1.9

Consider the following proposition:

$$\exists!\, y \in \mathbb{R}, \forall x \in \mathbb{R}, (x+y = x)$$

(a) What does this statement say in natural, idiomatic English?

Solution. There is a unique additive identity in the reals.

(b) Write the logical negation of this statement in maximally negated form.

Solution.

$$\Big(\forall y \in \mathbb{R}, \exists x \in \mathbb{R},\ x{+}y \neq x\Big) \vee \Big(\exists a, b \in \mathbb{R},\ (a \neq b \wedge \forall x \in \mathbb{R},\ (x{+}a = x \wedge x{+}b = x))\Big)$$

(c) Prove the original statement.

Proof.

- (Existence): Consider $y = 0 \in \mathbb{R}$. For any $x \in \mathbb{R}$, we have $x + 0 = x$, so existence is satisfied.
- (Uniqueness): Suppose $y, z \in \mathbb{R}$ such that for any $x \in \mathbb{R}$, $x + y = x$ and $x + z = x$. Fix an arbitrary $x \in \mathbb{R}$. Then, by assumption,

$$x + y = x + z$$

subtracting x from both sides yields $y = z$, as desired.

Therefore, there is a unique additive identity in the real number system. □

8. September 12

Exercise 8.1.5

1. True. For any set A, $\varnothing \subseteq A$ so $\varnothing \in \mathcal{P}(A)$, regardless of our set A.
2. True. $\varnothing$ is a subset of all sets.
3. False. $\varnothing \notin A$, so $\{\varnothing\} \not\subseteq A$ and thus $\{\varnothing\} \notin \mathcal{P}(A)$.
4. True. Since $\varnothing \in \mathcal{P}(A)$ we have $\{\varnothing\} \subseteq \mathcal{P}(A)$.
5. False. 1 is not a set, so it can't be a subset of A.
6. True. Since $1 \in A$ we have $\{1\} \in \mathcal{P}(A)$.
7. False. $1 \notin \mathcal{P}(A)$ since $1 \not\subseteq A$. Thus $\{1\} \not\subseteq \mathcal{P}(A)$.
8. True. Since $\{1\} \in A$ we have $\{\{1\}\} \in \mathcal{P}(A)$.
9. True. Since $1 \in A$ we have $\{1\} \in \mathcal{P}(A)$ and thus $\{\{1\}\} \subseteq \mathcal{P}(A)$.
10. True. Since $0, 2 \in A$ we have $\{0, 2\} \in \mathcal{P}(A)$.
11. False. $0, 2 \notin \mathcal{P}(A)$ and thus $\{0, 2\} \not\subseteq \mathcal{P}(A)$.

Exercise 8.1.7

$A = [10]$, $B = \{0, 1, 2\}$, and $C = \{0, 1, 9, 10, 11\}$.

1. $(A \setminus B) \cap C = \{9, 10\}$
2. $(A \cup C) \setminus (B \cup C) = \{3, 4, 5, 6, 7, 8\}$
3. $(A \setminus B) \cup (A \setminus C) = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$
4. $(A \setminus B) \cap (A \setminus C) = \{3, 4, 5, 6, 7, 8\}$
5. $(A \cap C) \setminus B = \{9, 10\}$
6. $A \setminus (B \cap C) = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Exercise 8.1.10

(a) $\displaystyle\bigcap_{n\in\mathbb{N}} \left[\frac{1}{n+1}, n+1\right] = \boxed{\{1\}}$

(b) $\displaystyle\bigcup_{n\in\mathbb{N}} \left[\frac{1}{n+1}, n+1\right] = \boxed{(0, \infty)}$

(c) $\displaystyle\bigcap_{n\in\mathbb{N}} \left(\frac{1}{n+1}, n+1\right) = \boxed{\varnothing}$

(d) $\displaystyle\bigcup_{n\in\mathbb{N}} \left(\frac{1}{n+1}, n+1\right) = \boxed{(0, \infty)}$

9. September 15

Exercise 9.1.7

Consider the following sets and determine whether the statements in (a)-(n) are `True` or `False`.

$$
\begin{aligned}
A &= \{z \in \mathbb{Z} \mid -3 \leq z \leq 3\},\\
B &= \{y \in \mathbb{Z} \mid -5 < y < 6\},\\
C &= \{x \in \mathbb{R} \mid x^2 \geq 9\},\\
D &= \{x \in \mathbb{R} \mid x < -3\},\\
E &= \{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(n = 2k)\}.
\end{aligned}
$$

(a) $A \subseteq B$

(b) $C \cap D = \varnothing$

(c) $4 \in E \cap B$

(d) $\{4\} \subseteq A \cap E$

(e) $10 \in C \setminus D$

(f) $A \cup B \supseteq C$

(g) $3 \in A \cap C$

(h) $0 \in (A \setminus B) \cup D$

(i) $E \cap C \subseteq \mathbb{Z}$

(j) $0 \notin B \setminus C$

(k) $(0, 0) \in A \times E$

(l) $(0, 0) \in \mathcal{P}(A \times E)$

(m) $D \in \mathcal{P}(C)$

(n) $(A \times B) \setminus (C \times D) = (A \setminus C) \times (B \setminus D)$

Solutions.

(a) True. If $z \in A$, then $z \in \mathbb{Z}$ and $-3 \leq z \leq 3$. This implies $-5 < z < 6$, so $z \in B$. Hence, $A \subseteq B$.

(b) False. Counterexample: $-4 \in C \cap D$. Since $(-4)^2 = 16 \geq 9$, we have $-4 \in C$, and because $-4 < -3$, we have $-4 \in D$. Therefore, $C \cap D \neq \varnothing$.

(c) True. We know $4 \in \mathbb{N}$, and $4 = 2 \cdot 2$, so $4 \in E$. Additionally, $4 \in \mathbb{Z}$ and $-5 < 4 < 6$, so $4 \in B$. Hence, $4 \in E \cap B$.

(d) False. We know $4 \notin A$, so $4 \notin A \cap E$. Thus, $\{4\} \not\subseteq A \cap E$.

(e) True. We know $10 \in C$ because $10^2 = 100 \geq 9$. Also, $10 \notin D$ because $10 \not< -3$. Therefore, $10 \in C \setminus D$.

(f) False. Counterexample: $\pi \in C$ because $\pi^2 \geq 9$, but $\pi \notin A$ (since $A \subseteq \mathbb{Z}$) and $\pi \notin B$. Therefore, $\pi \notin A \cup B$, so $A \cup B \not\supseteq C$.

(g) True. We know $3 \in \mathbb{Z}$, and $-3 \leq 3 \leq 3$, so $3 \in A$. Additionally, $3 \in \mathbb{R}$ and $3^2 = 9 \geq 9$, so $3 \in C$. Therefore, $3 \in A \cap C$.

(h) False. Since $A \setminus B = \varnothing$ by (a), we have $0 \notin A \setminus B$. Also, $0 \notin D$ because $0 \not< -3$. Therefore, $0 \notin (A \setminus B) \cup D$.

(i) True. We know $E \cap C \subseteq E$, and since $E \subseteq \mathbb{N} \subseteq \mathbb{Z}$, we have $E \cap C \subseteq \mathbb{Z}$.

(j) False. We know $0 \in B$ because $-5 < 0 < 6$, and $0 \notin C$ because $0^2 = 0 \not\geq 9$. Therefore, $0 \in B \setminus C$, contradicting the statement.

(k) True. Since $0 \in A$ and $0 \in E$, we have $(0, 0) \in A \times E$.

(l) False. The ordered pair $(0, 0)$ is not a subset of $A \times E$. Therefore, it cannot be an element of $\mathcal{P}(A \times E)$, which contains subsets of $A \times E$, not individual elements.

(m) True. Since $D \subseteq C$, we have $D \in \mathcal{P}(C)$.

(n) False. Counterexample: Consider $(0, -4)$. We know $0 \in A$ and $-4 \in B$, so $(0, -4) \in A \times B$. However, $(0, -4) \notin C \times D$ because $0 \notin C$. Therefore, $(0, -4) \in (A \times B) \setminus (C \times D)$.

However, $(0, -4) \notin (A \setminus C) \times (B \setminus D)$ because $-4 \notin B \setminus D$. This shows the sets are not equal.

Exercise 9.1.8

Prove that for all sets A and B, $A \times B = B \times A$ if and only if $A = \varnothing$ or $B = \varnothing$ or $A = B$.

Proof. Let A and B be arbitrary sets.

($\Rightarrow$) Suppose $A \times B = B \times A$. We will show that $A = \varnothing$ or $B = \varnothing$ or $A = B$. This is logically equivalent to proving that if $A \neq \varnothing$ and $B \neq \varnothing$, then $A = B$.

Assume $A \neq \varnothing$ and $B \neq \varnothing$. Let $a \in A$ and $b \in B$ be arbitrary and fixed. Then $(a, b) \in A \times B$ by the definition of a Cartesian product. Since $A \times B = B \times A$, it follows that $(a, b) \in A \times B$ implies $(a, b) \in B \times A$. By the definition of the Cartesian product, this implies $a \in B$ and $b \in A$. Since $a \in A$ and $b \in B$ were arbitrary choices, we conclude that $A \subseteq B$ and $B \subseteq A$. Therefore, by double containment, $A = B$, as required.

($\Leftarrow$) Suppose that $A = \varnothing$, $B = \varnothing$, or $A = B$. If $A = \varnothing$, then $A \times B = B \times A = \varnothing$, as desired. Similarly, if $B = \varnothing$, the equality holds trivially.

Now suppose $A = B \neq \varnothing$. Let $(a, b) \in A \times B$ be arbitrary and fixed. Then $a \in A$ and $b \in B$, and since $A = B$, we have $a \in B$ and $b \in A$, implying $(a, b) \in B \times A$. Thus, $A \times B \subseteq B \times A$. A similar argument shows $B \times A \subseteq A \times B$. Therefore, $A \times B = B \times A$, completing the proof. □

Exercise 9.1.9

For any sets A and B, the *symmetric difference* of A and B, denoted $A \triangle B$, is defined as:

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

(a) Prove, via double containment, that for any sets A and B, $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Proof.

($\subseteq$) Let $x \in (A \cup B) \setminus (A \cap B)$. By the definition of set difference, $x \in A \cup B$ and $x \notin A \cap B$. Since $x \in A \cup B$, it must be that $x \in A$ or $x \in B$.

Suppose $x \in A$. Since $x \notin A \cap B$ and $x \in A$, it must be that $x \notin B$ (otherwise x would be in $A \cap B$). Thus, $x \in A \setminus B$.

Similarly, if $x \in B$, since $x \notin A \cap B$, it must be that $x \notin A$. Thus, $x \in B \setminus A$.

Therefore, $x \in (A \setminus B) \cup (B \setminus A)$. This shows that $(A \cup B) \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A)$.

($\supseteq$) Let $x \in (A \setminus B) \cup (B \setminus A)$. By the definition of union, $x \in A \setminus B$ or $x \in B \setminus A$.

If $x \in A \setminus B$, then $x \in A$ and $x \notin B$. Hence, $x \in A \cup B$ and $x \notin A \cap B$ because $x \notin B$. Therefore, $x \in (A \cup B) \setminus (A \cap B)$.

Similarly, if $x \in B \setminus A$, then $x \in B$ and $x \notin A$. Thus, $x \in A \cup B$ and $x \notin A \cap B$ because $x \notin A$. Therefore, $x \in (A \cup B) \setminus (A \cap B)$.

Therefore, $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$.

By double containment, $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$, as desired. $\square$

(b) Prove that $A \triangle B = \varnothing$ if and only if $A = B$.

Proof.

($\Rightarrow$) Suppose $A \triangle B = \varnothing$. We want to show that $A = B$.

Take any element $a \in A$. If $a \notin B$, then $a \in A \setminus B$ by the definition of set difference. Since $A \triangle B = (A \cup B) \setminus (A \cap B)$, and we have $A \triangle B = \varnothing$, it follows that $a \notin A \triangle B$. This contradicts our assumption that $a \in A \setminus B$ if $a \notin B$. Therefore, $a \in B$.

Similarly, take any element $b \in B$. If $b \notin A$, then $b \in B \setminus A$. Again, since $A \triangle B = \varnothing$, $b \notin A \triangle B$, which contradicts the assumption that $b \in B \setminus A$. Thus, $b \in A$.

Therefore, $A \subseteq B$ and $B \subseteq A$, which implies $A = B$.

($\Leftarrow$) Suppose $A = B$. Then $A \setminus B = \varnothing$ and $B \setminus A = \varnothing$ by the definition of set difference. Hence, from part (a), we have

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = \varnothing \cup \varnothing = \varnothing.$$

Thus, $A \triangle B = \varnothing$, as desired.

Therefore, $A \triangle B = \varnothing$ if and only if $A = B$. $\square$

Exercise 9.1.10

For each of the following, either prove the statement using a set containment proof or disprove it by constructing a counterexample.

(a) Prove or disprove: For any sets A, B, and C,

$$(A \cup B) \setminus C \subseteq (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)).$$

Counterexample. Consider $A = \{1, 2\}$, $B = \{2, 3\}$, and $C = \{1, 3\}$. Then:

$$(A \cup B) \setminus C = \{1, 2, 3\} \setminus \{1, 3\} = \{2\}.$$

However,

$$(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) = (\{1, 2\} \setminus \{1, 2, 3\}) \cup (\{2, 3\} \setminus \{1, 2, 3\}) = \varnothing \cup \varnothing = \varnothing.$$

Thus, $(A \cup B) \setminus C \not\subseteq (A \setminus (B \cup C)) \cup (B \setminus (A \cup C))$. □

(b) Prove or disprove: For any sets A, B, and C,

$$(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \subseteq (A \cup B) \setminus C.$$

Proof. Let A, B, and C be arbitrary and fixed sets. Further, let $x \in (A \setminus (B \cup C)) \cup (B \setminus (A \cup C))$. By the definition of a union, we have that either $x \in A \setminus (B \cup C)$ or $x \in B \setminus (A \cup C)$. Without loss of generality, assume that $x \in A \setminus (B \cup C)$.

This implies that $x \in A$ and $x \notin B \cup C$ by the definition of set difference. From $x \notin B \cup C$, we conclude that $x \notin B$ and $x \notin C$. Since $x \in A$, the definition of a union implies that $x \in A \cup B$.

Thus, $x \in A \cup B$ and $x \notin C$, which implies that $x \in (A \cup B) \setminus C$, again by the definition of set difference.

Since $x \in (A \setminus (B \cup C)) \cup (B \setminus (A \cup C))$ was arbitrary, we conclude that:

$$(A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \subseteq (A \cup B) \setminus C.$$

□

Exercise 9.1.13

Let A and B be subsets of a universal set U. Prove that $\overline{A \setminus B} = \overline{A} \cup B$.

Proof. Let $x \in U$ be arbitrary. Then

$$\begin{aligned} x \in \overline{A \smallsetminus B} &\iff x \notin A \smallsetminus B && \text{(Defn of complement)} \\ &\iff x \notin A \ \vee \ x \in B && \text{(Defn of set difference)} \\ &\iff x \in \overline{A} \ \vee \ x \in B && \text{(Defn of complement)} \\ &\iff x \in \overline{A} \cup B && \text{(Defn of union).} \end{aligned}$$

Since $x \in U$ was arbitrary, we conclude

$$\overline{A \smallsetminus B} = \overline{A} \cup B.$$

□

10. September 17

Exercise 10.1.4

Prove that for every $n \in \mathbb{Z}^+$, the following holds:

$$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Proof. We proceed by induction on $n \in \mathbb{Z}^+$.

- **Base Case:** $n = 1$. We have

  $$\sum_{i=1}^{1} i^3 = 1^3 = 1 = (1)^2 = \left(\frac{1 \cdot 2}{2} \right)^2,$$

  so the base case holds.

- **Inductive Step:** Let $n \in \mathbb{Z}^+$ such that

  $$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

  We want to show that

  $$\sum_{i=1}^{n+1} i^3 = \left(\frac{(n+1)(n+2)}{2} \right)^2.$$

We demonstrate this with the following chain of equalities:

$$\begin{aligned}
\sum_{i=1}^{n+1} i^3 &= (n+1)^3 + \sum_{i=1}^{n} i^3 \\
&= (n+1)^3 + \left(\frac{n(n+1)}{2}\right)^2 && \text{(By inductive hypothesis)} \\
&= (n+1)^2\left((n+1) + \frac{n^2}{4}\right) && \text{(Factoring)} \\
&= (n+1)^2\left(\frac{n^2+4n+4}{4}\right) \\
&= \frac{(n+1)^2(n+2)^2}{4} \\
&= \left(\frac{(n+1)(n+2)}{2}\right)^2,
\end{aligned}$$

as desired.

By the principle of mathematical induction, we conclude that $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$ for all $n \in \mathbb{Z}^+$. □

Exercise 10.1.5

For each part below, determine the set of natural numbers for which the property holds true, and prove your claim.

(a) **Claim**: $2^n \geq (n+1)^2$ for $n = 0$ and $n \geq 6$.

Proof. We manually verify the claim for $n < 6$.

- $n = 0$: $2^0 = 1 \geq 1 = (0+1)^2$.
- $n = 1$: $2^1 = 2 < 4 = (1+1)^2$.
- $n = 2$: $2^2 = 4 < 9 = (2+1)^2$.
- $n = 3$: $2^3 = 8 < 16 = (3+1)^2$.
- $n = 4$: $2^4 = 16 < 25 = (4+1)^2$.
- $n = 5$: $2^5 = 32 < 36 = (5+1)^2$.

We now proceed by induction on integers $n \geq 6$.

- **Base Case**: For $n = 6$, we have $2^6 = 64 \geq 49 = (6+1)^2$, so the base case holds.
- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 6$ and assume $2^k \geq (k+1)^2$. We will show that $2^{k+1} \geq (k+2)^2$.

Using the inductive hypothesis, we have:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &\geq 2 \cdot (k+1)^2 \quad \text{(by inductive hypothesis)} \\ &= 2(k^2 + 2k + 1) \\ &= 2k^2 + 4k + 2 \\ &\geq k^2 + 4k + 4 \quad \text{(since } k^2 \geq 2 \text{ for } k \geq 6) \\ &= (k+2)^2. \end{aligned}$$

Therefore, $2^{k+1} \geq (k+2)^2$, completing the inductive step.

By the principle of mathematical induction, we conclude that $2^n \geq (n+1)^2$ for $n = 0$ and all integers $n \geq 6$. □

(b) **Claim**: $3^{n+1} > n^4$ for $n = 0$, $n = 1$, $n = 2$, and for all integers $n \geq 5$.

Proof: We manually verify that the inequality holds for $n = 0$, $n = 1$, $n = 2$ and fails for $n = 3$ and $n = 4$:

- $n = 0$: $3^{0+1} = 3 > 0 = 0^4$.
- $n = 1$: $3^{1+1} = 9 > 1 = 1^4$.
- $n = 2$: $3^{2+1} = 27 > 16 = 2^4$.
- $n = 3$: $3^{3+1} = 81 = 81 = 3^4$.
- $n = 4$: $3^{4+1} = 243 < 256 = 4^4$.

To prove the inequality holds for all integers $n \geq 5$, we proceed by induction.

- **Base Case**: $n = 5$. We check that

$$3^{5+1} = 729 > 625 = 5^4.$$

  Thus, the base case holds.

- **Inductive Step**: Let $k \in \mathbb{Z}$ with $k \geq 5$ and assume $3^{k+1} > k^4$. We want to show that $3^{k+2} > (k+1)^4$. Then we have:

$$
\begin{aligned}
3^{k+2} &= 3 \cdot 3^{k+1} \\
&> 3k^4 \quad \text{(by IH)} \\
&= k^4 + k^4 + k^4 \\
&\geq k^4 + 5k^3 + 5k^3 \quad (\text{since } k \geq 5 \Rightarrow k^4 \geq 5k^3) \\
&= k^4 + 4k^3 + 6k^3 \quad \text{(rearranging terms)} \\
&\geq k^4 + 4k^3 + 30k^2 \quad (\text{since } k \geq 5 \Rightarrow k^3 \geq 5k^2) \\
&= k^4 + 4k^3 + 6k^2 + 24k^2 \quad \text{(rearranging terms)} \\
&\geq k^4 + 4k^3 + 6k^2 + 120k \quad (\text{since } k \geq 5 \Rightarrow k^2 \geq 5k) \\
&= k^4 + 4k^3 + 6k^2 + 4k + 116k \quad \text{(rearranging terms)} \\
&> k^4 + 4k^3 + 6k^2 + 4k + 1 \quad (\text{since } 116k > 1 \text{ for } k \geq 5) \\
&= (k+1)^4.
\end{aligned}
$$

Therefore, for integers $k \geq 5$, the inequality holds. This completes the inductive step.

Thus, by the principle of mathematical induction, we conclude that $3^{n+1} > n^4$ for $n = 0$, $n = 1$, $n = 2$, and for all integers $n \geq 5$. □

(c) **Claim**: $n^3 + (n+1)^3 > (n+2)^2$ for all natural numbers $n \geq 2$.

Proof. First, observe that this claim does not hold for $n = 0$ and $n = 1$:

- $0^3 + (0+1)^3 = 1 < 8 = (0+2)^3$
- $1^3 + (1+1)^3 = 9 < 27 = (1+2)^3$

We proceed by induction on the natural numbers $n \geq 2$.

- **Base Case:** Let $n = 2$. We compute:

$$2^3 + (2+1)^3 = 36 > 16 = (2+2)^2,$$

so the claim holds for $n = 2$.

- **Inductive Step:** Let $k \in \mathbb{N}$ with $k \geq 2$ and assume that

$$k^3 + (k+1)^3 > (k+2)^2.$$

We want to prove that $(k+1)^3 + (k+2)^3 > (k+3)^2$. Starting from the

left-hand side, we have:

$$\begin{aligned}(k+1)^3+(k+2)^3 &= k^3+(k+1)^3+6k^2+12k+8\\ &> (k+2)^2+6k^2+12k+8 \quad \text{(by the inductive hypothesis)}\\ &= 7k^2+16k+12\\ &> k^2+6k+9 \quad (\text{since } 7k^2>k^2, 16k>6k, \text{ and } 12>9)\\ &= (k+3)^2.\end{aligned}$$

Thus, $(k+1)^3+(k+2)^3>(k+3)^2$, as required.

By the principle of mathematical induction, we conclude that $n^3+(n+1)^3>(n+2)^2$ for all natural numbers $n \geq 2$. □

(d) **Claim**: $3^n \geq 2^{n+1}$ for all natural numbers $n \geq 2$.

Proof. First, observe that the claim does not hold for $n=0$ and $n=1$:

- $3^0 = 1 < 2 = 2^{0+1}$
- $3^1 = 3 < 4 = 2^{1+1}$

We now proceed by induction on $n \in \mathbb{N}$ with $n \geq 2$.

- **Base Case**: Let $n=2$. We compute:

$$3^2 = 9 \geq 2^3 = 8,$$

as desired.

- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 2$ and assume $3^k \geq 2^{k+1}$. We want to show that $3^{k+1} \geq 2^{k+2}$. Using the inductive hypothesis (IH), we have the following chain of equalities and inequalities:

$$\begin{aligned}3^{k+1} &= 3^k \cdot 3\\ &\geq 2^{k+1} \cdot 3 \quad \text{(by IH)}\\ &\geq 2^{k+1} \cdot 2\\ &= 2^{k+2}.\end{aligned}$$

Thus, by the principle of mathematical induction, we conclude that $3^n \geq 2^{n+1}$ for all natural numbers $n \geq 2$. □

11. September 19

Exercise 11.1.3

Prove that for all positive integers n,

$$\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$$

Proof. We proceed by induction on $n \in \mathbb{Z}^+$.

- (Base Case): $n = 1$. We have

  $$\sum_{k=1}^{1} \frac{k}{(k+1)!} = \frac{1}{2} = 1 - \frac{1}{2!},$$

  as desired. So the base case holds.

- (Inductive Step): Let $n \in \mathbb{Z}^+$ such that

  $$\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$$

  We want to show that

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

  To see this, observe the following chain of equalities:

  $$\begin{aligned}
  \sum_{k=1}^{n+1} \frac{k}{(k+1)!} &= \sum_{k=1}^{n} \frac{k}{(k+1)!} + \frac{n+1}{(n+2)!} \\
  &= \left(1 - \frac{1}{(n+1)!}\right) + \frac{n+1}{(n+2)!} \quad \text{(By IH)} \\
  &= 1 - \frac{n+2}{(n+2)!} + \frac{n+1}{(n+2)!} \\
  &= 1 - \frac{1}{(n+2)!},
  \end{aligned}$$

  as desired.

By the principle of mathematical induction, we conclude that

$$\sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$$

for all positive integers n. □

Exercise 11.1.6

Let $P(n)$ be a predicate defined on $n \in \mathbb{Z}$. For each case below, identify which instances of the proposition you could **necessarily** deduce.

(a) **Base Case:** $P(-3)$. **Implication:** $\forall n \in \mathbb{Z}, (P(n) \to P(n+1))$.

Solution: We can deduce that $P(n)$ holds for the set

$$S = \{n \in \mathbb{Z} \mid n \geq -3\}.$$

Since $P(-3)$ holds and the implication states that if $P(n)$ holds, then so does $P(n+1)$, we can conclude $P(-3)$, $P(-2)$, $P(-1)$, and so on for all integers greater than or equal to -3.

(b) **Base Case:** $P(1)$. **Implication:** $\forall n \in \mathbb{N}, (P(n) \to P(2n))$.

Solution: We can deduce that $P(n)$ holds for the set

$$S = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, n = 2^k\}.$$

The base case tells us that $P(2^0) = P(1)$ holds. The implication shows that if $P(n)$ holds, then so does $P(2n)$. Therefore, we can conclude that $P(n)$ holds for all powers of 2.

(c) **Base Case:** $P(0)$. **Implication:** $\forall n \in \mathbb{Z}, (P(n) \to (P(n-1) \wedge P(n+1)))$.

Solution: We can deduce that $P(n)$ holds for all integers n. Knowing $P(0)$ holds and that if $P(n)$ holds, then both $P(n-1)$ and $P(n+1)$ hold, we can propagate this implication in both directions. For example, from $P(0)$, we can deduce $P(-1)$ and $P(1)$, and from there, we can deduce $P(-2)$, $P(2)$, and so on. Thus, $P(n)$ holds for all $n \in \mathbb{Z}$.

(d) **Base Cases:** $P(-1) \wedge P(0)$. **Implication:** $\forall n \in \mathbb{Z}^+, (P(n) \to P(n+2))$.

Solution: We can only conclude that $P(-1)$ and $P(0)$ hold. The implication only applies to positive integers, and since neither -1 nor 0 is a positive integer, the implication does not apply in this case. Thus, no further conclusions can be drawn about positive integers.

(e) **Base Case:** $P(0)$. **Implications:** $\forall n \in \mathbb{Z}, ((P(n) \to P(n+6)) \wedge (P(2n) \to P(n)))$.

Solution: We can deduce that $P(n)$ holds for the set

$$S = \{n \in \mathbb{N} \mid \exists k \in \mathbb{Z}, n = 3k\}.$$

From $P(0)$ and the first implication, we can conclude that $P(n)$ holds for all nonnegative multiples of 6. From the second implication, we deduce that if $P(n)$ holds for an even number, then $P(n/2)$ holds as well. Combining this with the result from the first implication, we conclude that $P(n)$ holds for all nonnegative multiples of 3.

12. September 24

Exercise 12.1.2

Define a sequence recursively as follows.

$$a_n = \begin{cases} 2 & \text{if } n = 0 \\ 2 & \text{if } n = 1 \\ 2a_{n-1} + 8a_{n-2} & \text{if } n \geq 2 \end{cases}$$

Prove that $a_n = 4^n + (-2)^n$ for all $n \in \mathbb{N}$.

Proof. We proceed by strong induction on $n \in \mathbb{N}$.

- **Base Cases**:
  - $n = 0$: We have $4^0 + (-2)^0 = 1 + 1 = 2 = a_0$.
  - $n = 1$: We have $4^1 + (-2)^1 = 4 - 2 = 2 = a_1$.
- **Inductive Step**: Let $k \in \mathbb{N}$ with $k \geq 1$ and assume for $i \in \mathbb{N}$ with $0 \leq i \leq k$ we have $a_i = 4^i + (-2)^i$. We aim to show that $a_{k+1} = 4^{k+1} + (-2)^{k+1}$.

  By the recursive definition of a_n, for $k + 1 \geq 2$:

$$\begin{aligned} a_{k+1} &= 2a_k + 8a_{k-1} \quad \text{(by definition)} \\ &= 2\left(4^k + (-2)^k\right) + 8\left(4^{k-1} + (-2)^{k-1}\right) \quad \text{(by IH)} \\ &= 2 \cdot 4^k + 2 \cdot (-2)^k + 8 \cdot 4^{k-1} + 8 \cdot (-2)^{k-1} \\ &= 4^{k+1} - (-2)^{k+1} + 2 \cdot (-2)^{k+1} \\ &= 4^{k+1} + (-2)^{k+1}. \end{aligned}$$

Thus, by the principle of strong induction, $a_n = 4^n + (-2)^n$ for all $n \in \mathbb{N}$. □

Exercise 12.1.3

Define the sequence $\langle a_n \rangle_{n \in \mathbb{Z}^+}$ recursively as follows.

$$a_n = \begin{cases} 2 & \text{if } n = 1 \\ 3 & \text{if } n = 2 \\ 4 & \text{if } n = 3 \\ a_{n-1} + 3a_{n-3} + 2 & \text{if } n \geq 4 \end{cases}$$

Prove that $a_n \leq 2^n$ for all $n \in \mathbb{Z}^+$.

Proof: We proceed by strong induction on $n \in \mathbb{Z}^+$.

- **Base Cases**: We manually verify the claim for $n = 1$, $n = 2$, and $n = 3$:
  - $n = 1$: $a_1 = 2 \leq 2^1$.
  - $n = 2$: $a_2 = 3 \leq 2^2$.
  - $n = 3$: $a_3 = 4 \leq 2^3$.
- **Inductive Step**: Let $k \in \mathbb{Z}^+$ with $k \geq 3$ such that $a_k \leq 2^k$, $a_{k-1} \leq 2^{k-1}$, and $a_{k-2} \leq 2^{k-2}$. We want to show that $a_{k+1} \leq 2^{k+1}$. Then:

$$\begin{aligned} a_{k+1} &= a_k + 3a_{k-2} + 2 \quad \text{(By definition because } k \geq 3\text{)} \\ &\leq 2^k + 3 \cdot 2^{k-2} + 2 \quad \text{(By IH)} \\ &\leq 2^k + 4 \cdot 2^{k-2} \quad \text{(Because } k - 2 \geq 1\text{)} \\ &= 2^k + 2^k \\ &= 2^{k+1} \end{aligned}$$

  Therefore, $a_{k+1} \leq 2^{k+1}$, as desired.

By strong induction, $a_n \leq 2^n$ for all positive integers n. □

Exercise 12.1.4

Let f_n denote the n^{th} Fibonacci number. Prove that for all $n \in \mathbb{N}$, the following equality holds.

$$\sum_{k=1}^{n} f_{2k} = f_{2n+1} - 1$$

Proof. We proceed by induction on $n \in \mathbb{N}$.

- **Base Case**: $n = 0$. Observe that $\sum_{k=1}^{0} f_{2k} = 0 = 1 - 1 = f_1 - 1 = f_{2(0)+1} - 1$, as desired
- **Inductive Step**: Let $m \in \mathbb{N}$ such that

$$\sum_{k=1}^{m} f_{2k} = f_{2m+1} - 1.$$

  We need to show that

$$\sum_{k=1}^{m+1} f_{2k} = f_{2(m+1)+1} - 1.$$

We calculate:

$$\begin{aligned}\sum_{k=1}^{m+1} f_{2k} &= f_{2m+2} + \sum_{k=1}^{m} f_{2k} \\ &= f_{2m+2} + f_{2m+1} - 1 \quad \text{(by IH)} \\ &= f_{2m+3} - 1 \quad \text{(by the Fibonacci recurrence, } f_{n+2} = f_{n+1} + f_n) \\ &= f_{2(m+1)+1} - 1.\end{aligned}$$

Hence, $\sum_{k=1}^{m+1} f_{2k} = f_{2(m+1)+1} - 1$, as desired.

Therefore, by PMI, $\sum_{k=1}^{n} f_{2k} = f_{2n+1} - 1$ for all $n \in \mathbb{N}$. □

13. September 26

Exercise 13.1.2

Prove that $\sqrt[3]{3}$ must be irrational.

Proof. To prove that $\sqrt[3]{3}$ is irrational, it suffices to show that

$$\sqrt[3]{3} \neq \frac{m}{n} \quad \text{for all } m, n \in \mathbb{Z}^+.$$

Define the predicate $P(n)$ on $n \in \mathbb{Z}^+$ by

$$P(n) := \forall m \in \mathbb{Z}^+, \ \left(\sqrt[3]{3} \neq \frac{m}{n}\right).$$

Our goal is to show $\forall n \in \mathbb{Z}^+$, $P(n)$ holds.

Assume, for the sake of contradiction, that there exists $n \in \mathbb{Z}^+$ such that $\neg P(n)$ holds. By the Well-Ordering Property choose the least such n. Since $\neg P(n)$ holds, there exists $m \in \mathbb{Z}^+$ with

$$\sqrt[3]{3} = \frac{m}{n}.$$

Fix such an m. Cubing both sides gives

$$3n^3 = m^3.$$

Hence 3 divides m^3. Consider the integer

$$m^3 - m = m(m^2 - 1) = m(m-1)(m+1).$$

The three integers $m-1, m, m+1$ are consecutive, so one of them is a multiple of 3. Therefore the product $m(m-1)(m+1)$ is a multiple of 3, and hence 3 divides $m^3 - m$. Since 3 divides m^3 as well, it follows that 3 divides the difference

$$m = m^3 - (m^3 - m),$$

so 3 divides m. Thus we may write $m = 3m'$ for some $m' \in \mathbb{Z}^+$. Substituting back into $3n^3 = m^3$ yields

$$3n^3 = (3m')^3 = 27(m')^3 \quad \Longrightarrow \quad n^3 = 9(m')^3.$$

Therefore 3 divides n^3, and by the same argument applied to n we conclude 3 divides n. Write $n = 3n'$ for some $n' \in \mathbb{Z}^+$. Since $n' = \frac{n}{3} < n$, we have produced a strictly smaller denominator. Moreover,

$$\sqrt[3]{3} = \frac{m}{n} = \frac{3m'}{3n'} = \frac{m'}{n'},$$

so $\neg P(n')$ holds, contradicting the minimality of n.

Thus our assumption was false, and $P(n)$ holds for all $n \in \mathbb{Z}^+$. Hence $\sqrt[3]{3}$ is irrational. □

Exercise 14.1.2

Let $S = \{1, 2, 3\}$.

(a) How many different binary relations on S exist?

Solution. The set $S \times S$ has exactly 9 elements, so there are exactly $2^9 = 512$ subsets of $S \times S$, and every subset is a relation on S. Therefore, there are $\boxed{512}$ binary relations on S.

(b) Which binary relation on S contains the fewest ordered pairs?

Solution. The empty relation, $\boxed{\varnothing}$, which contains no ordered pairs.

(c) Which binary relation on S contains the most ordered pairs?

Solution. The universal relation, $\boxed{S \times S}$, which contains all ordered pairs.

Exercise 15.1.1

Determine which of the following maps are well-defined functions.

(a) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f\left(\frac{m}{n}\right) = \frac{m+n}{n^2}$

Solution. $\boxed{\text{Ill-defined}}$. Does not satisfy uniqueness.

(b) $g : \mathbb{Q} \to \mathbb{Q}$ defined by $g\left(\frac{m}{n}\right) = \frac{2m+n}{2n}$

Solution. Well-defined. The definition of g could be rewritten as $g(x) = x + \frac{1}{2}$.

(c) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \frac{x^2-1}{x^2+1}$

Solution. Well-defined.

(d) $j : \mathbb{R} \to \mathbb{R}$ defined by $j(x) = \frac{x^2+1}{x^2-1}$

Solution. Ill-defined. Does not satisfy totality. $j(1)$ and $j(-1)$ are undefined.

(e) $k : \mathbb{N} \to \mathbb{N}$ defined by $k(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n}{3} & \text{if } 3 \mid n \\ n & \text{otherwise} \end{cases}$

Solution. Ill-defined. Does not satisfy uniqueness. Consider $n = 6$.

(f) $\ell : \mathbb{N} \to \mathbb{N}$ defined by $\ell(n) = \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } 4 \mid n \\ n & \text{otherwise} \end{cases}$

Solution. Well-defined.

14. September 29

Exercise 15.1.3

Let A and B be sets, and let $f : A \to B$ and $g : A \to B$ be functions. Then $f = g$ if and only if $\forall a \in A$, $f(a) = g(a)$.

Proof Sketch.

($\Rightarrow$): Assume $f = g$, as sets. Let $a \in A$ be arbitrary. Then $\exists! \, b \in B$ such that $(a, b) \in f$ and hence $(a, b) \in g$. Therefore $f(a) = b = g(a)$.

($\Leftarrow$): Assume $f(a) = g(a)$ for all $a \in A$. Let $(x, y) \in f$ be arbitrary. Then $y = f(x)$ and hence $y = g(x)$, by assumption. Therefore, $(x, y) \in g$, proving $f \subseteq g$. A symmetric argument shows that $g \subseteq f$, so $f = g$, as desired. □

Exercise 15.1.7

Prove that there exists sets A and B, a function $f : A \to B$, and subsets $S, T \in \mathcal{P}(A)$ such that

$$\text{Im}_f(S) \cap \text{Im}_f(T) \not\subseteq \text{Im}_f(S \cap T)$$

Proof. Define $f : [3] \to [3]$ such that $f(1) = 1$, $f(2) = 1$, and $f(3) = 3$. Consider the sets $S = \{1, 3\}$ and $T = \{2, 3\}$, so $S \cap T = \{3\}$. Then $\text{Im}_f(S) = \{1, 3\}$, $\text{Im}_f(T) = \{1, 3\}$ and $\text{Im}_f(S \cap T) = \{3\}$. We can see that, in this case, $\text{Im}_f(S \cap T) \subsetneq \text{Im}_f(S) \cap \text{Im}_f(T)$. $\square$

Exercise 15.1.10

Define a function $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \sqrt{1 + x^2}$. Determine the following sets.

(a) $\text{Im}(f)$.

Solution: $\boxed{[1, \infty)}$

(b) $\text{Im}_f([-5, 5])$

Solution: $\boxed{[1, \sqrt{26}]}$

(c) $\text{PreIm}_f([0, 1])$

Solution: $\boxed{\{0\}}$

(d) $\text{PreIm}_f((3, 5))$

Solution: $\boxed{(-2\sqrt{6}, -2\sqrt{2}) \cup (2\sqrt{2}, 2\sqrt{6})}$

Exercise 15.1.11

Let A and B be nonempty sets and $f : A \to B$ be a function. Prove that the following equality holds for all $Y_1, Y_2 \in \mathcal{P}(B)$.

$$\text{PreIm}_f(Y_1 \setminus Y_2) = \text{PreIm}_f(Y_1) \setminus \text{PreIm}_f(Y_2)$$

Proof. Let $Y_1, Y_2 \in \mathcal{P}(B)$ and let $a \in A$ be arbitrary.

$$\begin{aligned}
a \in \text{PreIm}_f(Y_1 \setminus Y_2) &\Leftrightarrow f(a) \in Y_1 \setminus Y_2 && \text{(Definition of Preimage)} \\
&\Leftrightarrow f(a) \in Y_1 \wedge f(a) \notin Y_2 && \text{(Definition of Set Difference)} \\
&\Leftrightarrow a \in \text{PreIm}_f(Y_1) \wedge a \notin \text{PreIm}_f(Y_2) && \text{(Definition of Preimage)} \\
&\Leftrightarrow a \in \text{PreIm}_f(Y_1) \setminus \text{PreIm}_f(Y_2) && \text{(Definition of Set Difference)}
\end{aligned}$$

Since $a \in A$ was arbitrary, we have shown that $\text{PreIm}_f(Y_1 \setminus Y_2) = \text{PreIm}_f(Y_1) \setminus \text{PreIm}_f(Y_2)$, as required. □

15. October 1

Exercise 16.1.3

Determine whether or not the following functions are injections.

(a) $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(x, y) = (3x + 4y, 2x + y)$.

Claim. f is an injection.

Proof. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ such that $f(x_1, y_1) = f(x_2, y_2)$. Expanding by the definition of f and equality of ordered pairs:

$$\begin{aligned} 3x_1 + 4y_1 &= 3x_2 + 4y_2 \\ 2x_1 + y_1 &= 2x_2 + y_2 \end{aligned}$$

Rearranging these equations:

$$\begin{aligned} 3(x_1 - x_2) &= 4(y_2 - y_1) \\ 2(x_1 - x_2) &= y_2 - y_1 \end{aligned}$$

Substituting the expression for $y_2 - y_1$ from the second into equation into the first equation:

$$\begin{aligned} 3(x_1 - x_2) = 8(x_1 - x_2) &\implies 5(x_1 - x_2) = 0 \\ &\implies x_1 = x_2, \end{aligned}$$

so the x-coordinates are the same. From the previous equations, it immediately follows that the y-coordinates are also the same:

$$y_2 - y_1 = 0 \quad \implies \quad y_1 = y_2$$

Therefore, $(x_1, y_1) = (x_2, y_2)$, and hence f is injective. □

(b) $g : \mathbb{R}^3 \to \mathbb{R}^2$ such that $f(x, y, z) = (xz, yz)$.

Claim. g is not an injection.

Counterexample. Consider $(2, 2, 1), (1, 1, 2) \in \mathbb{R}^3$. Clearly $(2, 2, 1) \neq (1, 1, 2)$ but

$$g(2, 2, 1) = (2, 2) = g(1, 1, 2).$$

Therefore g is not injective. □

(c) $h : \mathbb{R} \to \mathbb{R}$ such that

$$h(x) = \begin{cases} x^3 + 3x^2 + 3x & \text{if } x \leq 0 \\ 5 - 2x & \text{if } x > 0 \end{cases}$$

Claim. h is not an injection.

Counterexample. Consider $\frac{5}{2}, 0 \in \mathbb{R}$. Clearly $\frac{5}{2} \neq 0$, but from the definition of h we have

$$h\left(\frac{5}{2}\right) = 5 - 2\left(\frac{5}{2}\right) = 0 = 0^3 + 3(0^2) + 3(0) = h(0)$$

Therefore, h is not injective. □

(d) $j : \mathbb{N}^2 \to \mathbb{Z}$ such that

$$j(a, b) = \begin{cases} b & \text{if } a = 0 \\ -2^{a-1}(2b + 1) & \text{if } a > 0 \end{cases}$$

Claim. j is an injection.

Proof. Let $(a_1, b_1), (a_2, b_2) \in \mathbb{N}^2$ such that $j(a_1, b_1) = j(a_2, b_2)$. We consider three cases:

- Case 1: If $a_1 = a_2 = 0$, then $j(a_1, b_1) = j(a_2, b_2)$ implies $b_1 = b_2$, so $(a_1, b_1) = (a_2, b_2)$, as desired.
- Case 2: If $a_1 > 0$ and $a_2 > 0$, then $j(a_1, b_1) = j(a_2, b_2)$ implies

  $$-2^{a_1 - 1}(2b_1 + 1) = -2^{a_2 - 1}(2b_2 + 1).$$

  By the uniqueness of the power of 2 and odd number factorization, we have $a_1 - 1 = a_2 - 1$ and $2b_1 + 1 = 2b_2 + 1$. From this, we conclude $a_1 = a_2$ and $b_1 = b_2$. Thus, $(a_1, b_1) = (a_2, b_2)$, as desired.
- Case 3: Without loss of generality, assume $a_1 = 0$ and $a_2 > 0$. Then $j(a_1, b_1) = j(a_2, b_2)$ implies $b_1 = -2^{a_2 - 1}(2b_2 + 1)$. However, $b_1 \geq 0$ and $-2^{a_2 - 1}(2b_2 + 1) < 0$, which is a contradiction. Hence, this case cannot occur.

Since these are the only three cases, we conclude that j is injective. □

Exercise 16.1.8

Determine whether or not the following functions are surjections.

(a) $f : \mathbb{N}^2 \to \mathbb{Z}$ such that $f(a, b) = 2^a - 3^b$.

Claim. f is not a surjection.

Counterexample. Consider $n = 2 \in \mathbb{Z}$. Assume for the sake of contradiction that there exists $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = 2$, and fix such an ordered pair. Then

$$2^a - 3^b = 2 \quad \Rightarrow \quad 3^b = 2^a - 2$$

If $a \neq 0$, this implies that $3^b = 2\left(2^{a-1} - 1\right)$ is even, a contradiction. And if $a = 0$ then we have $3^b = -1$, which is also impossible. Therefore, $2 \notin \text{Im}(f)$ and hence f is not a surjection. □

(b) $g : \mathbb{R}^3 \to \mathbb{R}^2$ such that $g(x, y, z) = (xz, yz)$.

Claim. g is a surjection.

Proof. Let $(x, y) \in \mathbb{R}^2$ be arbitrary. Then

$$(x, y, 1) \in \mathbb{R}^3 \text{ and } g(x, y, 1) = (x \cdot 1, y \cdot 1) = (x, y).$$

Since $(x, y) \in \mathbb{R}^2$ was arbitrary, we conclude that g is a surjection. □

(c) $h : \mathbb{R} \to \mathbb{R}$ such that

$$h(x) = \begin{cases} x^3 + 3x^2 + 3x & \text{if } x \leq 0 \\ 5 - 2x & \text{if } x > 0 \end{cases}$$

Claim. h is not a surjection.

Counterexample. Consider $y = 6 \in \mathbb{R}$. We claim that for all $x \in \mathbb{R}$, $h(x) \neq 6$. To see this, let $x \in \mathbb{R}$ and case on whether or not $x \leq 0$.

- Case 1: $x \leq 0$. Then $h(x) = x^3 + 3x^2 + 3x = (x + 1)^3 - 1$. We see that

$$h(x) = 6 \iff (x + 1)^3 - 1 = 6 \iff x = -1 + \sqrt[3]{7}$$

  But $x \leq 0$ and $-1 + \sqrt[3]{7} > 0$, so $h(x) \neq 6$.

- Case 2: $x > 0$. Then $h(x) = 5 - 2x$ and we see that

$$h(x) = 6 \iff 5 - 2x = 6 \iff x = -\frac{1}{2}$$

  But $x > 0$ and $-\frac{1}{2} \leq 0$, so $h(x) \neq 6$.

Since these are the only possible cases, we have $\forall x \in \mathbb{R}, h(x) \neq 6$ and hence h is not surjective. □

(d) $j : \mathbb{N}^2 \to \mathbb{Z}$ such that

$$j(a,b) = \begin{cases} b & \text{if } a = 0 \\ -2^{a-1}(2b+1) & \text{if } a > 0 \end{cases}$$

Recall the result from recitation that every positive integer can be expressed uniquely as a power of 2 times an odd number.

Claim. j is a surjection.

Proof. Let $x \in \mathbb{Z}$ be arbitrary. We consider two cases.

- If $x \geq 0$, then $(0, x) \in \mathbb{N}^2$ and $j(0, x) = x$.
- If $x < 0$, then $|x| \in \mathbb{Z}^+$ and we can uniquely write $|x| = 2^r \cdot s$ where $r \in \mathbb{N}$ and $s \in \mathbb{N}$ is odd. Thus, x can be uniquely written as $x = -2^r \cdot s$ for the same r and s. Since s is odd and $r \geq 0$, we have $(r+1, \frac{s-1}{2}) \in \mathbb{N}^2$ with $r + 1 \geq 1$. Then
$$j\left(r+1, \frac{s-1}{2}\right) = -2^r \cdot s = x,$$
as desired.

Since x was arbitrary, we conclude that j is surjective.

Exercise 16.1.12

Below are two functions from $\mathbb{R} \to (0, \infty)$. For each function, prove or disprove that it is a bijection.

(a) $f(x) = \begin{cases} e^x & \text{if } x \leq 0 \\ 2 - e^{-x} & \text{if } x > 0 \end{cases}$

Claim. f is not a bijection.

Proof. It suffices to show that f is not a surjection. Consider $y = 3 \in (0, \infty)$ and assume for the sake of contradiction that there exists $x \in \mathbb{R}$ such that $f(x) = 3$. We consider 2 cases:

- Case 1: $x \leq 0$. Then $f(x) = 3$ implies that $e^x = 3$ which implies that $x = \ln 3 > 0$, contradicting our assumption. Therefore this case can't happen.
- Case 2: $x > 0$. Then $f(x) = 3$ implies that
$$2 - e^{-x} = 3 \quad \Longrightarrow \quad e^{-x} = -1$$

which is not possible, because $e^{-x} > 0$ for all x. Therefore, this case can't happen either.

Since both cases led to a contradiction, we conclude that $3 \notin \text{Im}(f)$ and thus f is not a surjection (and hence not a bijection). □

(b) $g(x) = \begin{cases} -2x+1 & \text{if } x \leq 0 \\ \dfrac{1}{2x+1} & \text{if } x > 0 \end{cases}$

Claim. g is a bijection.

Proof. We proceed to prove that g is injective and surjective.

- *Injectivity.* Let $x_1, x_2 \in \mathbb{R}$ such that $g(x_1) = g(x_2)$. We consider 3 cases:
  - ▸ Case 1. $x_1, x_2 \leq 0$. Since $g(x_1) = g(x_2)$ we have
  $$-2x_1 + 1 = -2x_2 + 1 \quad \Longrightarrow \quad x_1 = x_2,$$
  as desired.
  - ▸ Case 2. $x_1, x_2 > 0$. Since $g(x_1) = g(x_2)$ we have
  $$\frac{1}{2x_1+1} = \frac{1}{2x_2+1} \quad \Longrightarrow \quad 2x_1 + 1 = 2x_2 + 1 \quad \Longrightarrow \quad x_1 = x_2,$$
  as desired.
  - ▸ Case 3. One is positive and the other is nonpositive. Without loss of generality, assume $x_1 \leq 0$ and $x_2 > 0$.
    - ◇ For $x_1 \leq 0$, $g(x_1) = -2x_1 + 1$. Since $x_1 \leq 0$, we have that $-2x_1 \geq 0$ and hence $g(x_1) \geq 1$.
    - ◇ For $x_2 > 0$, $g(x_2) = \frac{1}{2x_2+1}$. Since $x_2 > 0$, we have $2x_2 + 1 > 1$, so $0 < g(x_2) < 1$.

  Since $g(x_1) \geq 1$ and $g(x_2) < 1$, it is impossible to have $g(x_1) = g(x_2)$. Thus, this case cannot occur.

  Since in all possible cases where $g(x_1) = g(x_2)$, we have $x_1 = x_2$, the function g is injective.
- *Surjectivity.* Let $y \in (0, \infty)$ be arbitrary. We want to show there exists $x \in \mathbb{R}$ such that $g(x) = y$. We consider 2 cases:
  - ▸ Case 1: $0 < y < 1$. Set $x = \frac{1-y}{2y}$. Since $y > 0$, $x > 0$. Then $g(x) = \frac{1}{2\left(\frac{1-y}{2y}\right)+1} = \frac{1}{\frac{1-y}{y}+1} = \frac{1}{\frac{1}{y}} = y$.

- Case 2: $y \geq 1$. Set $x = \frac{1-y}{2}$. Since $y \geq 1$, $x \leq 0$. Then $g(x) = -2\left(\frac{1-y}{2}\right) + 1 = y$.

Since for every $y \in (0, \infty)$ we have found an $x \in \mathbb{R}$ such that $g(x) = y$, the function g is surjective.

Therefore, g is a bijection. □

16. October 3

Exercise 17.1.5

Prove that the following functions are bijections by explicitly constructing an inverse function and proving that it is in the inverse function.

(a) $f : \mathbb{R} \setminus \{-2\} \to \mathbb{R} \setminus \{4\}$ such that $f(x) = \frac{4x+5}{x+2}$.

Proof. Define $g : \mathbb{R} \setminus \{4\} \to \mathbb{R} \setminus \{-2\}$ by

$$g(x) = \frac{2x-5}{4-x}.$$

We will show that g is the inverse of f.

- **Well-Definedness**: Since $x \neq 4$ for all $x \in \mathbb{R} \setminus \{4\}$, the expression $\dfrac{2x-5}{4-x}$ is defined. If $x_1 = x_2$, then clearly

$$\frac{2x_1 - 5}{4 - x_1} = \frac{2x_2 - 5}{4 - x_2},$$

so $g(x_1) = g(x_2)$. To check that $g(x) \in \mathbb{R} \setminus \{-2\}$, we verify that $g(x) \neq -2$ for all $x \in \mathbb{R} \setminus \{4\}$:

$$g(x) = -2 \iff \frac{2x-5}{4-x} = -2 \iff 2x - 5 = 2x + 8 \iff -5 = 8,$$

a contradiction. Hence, $g(x) \neq -2$ for all x in the domain, so g is well-defined.

- **Computation of $g \circ f$**: Let $x \in \mathbb{R} \setminus \{-2\}$. Then

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g\left(\frac{4x+5}{x+2}\right) \\ &= \frac{2\left(\frac{4x+5}{x+2}\right) - 5}{4 - \left(\frac{4x+5}{x+2}\right)} \\ &= \frac{2(4x+5) - 5(x+2)}{4(x+2) - (4x+5)} \\ &= \frac{3x}{3} \\ &= x.\end{aligned}$$

  Therefore $g \circ f = \mathrm{Id}$.

- **Computation of $f \circ g$**: Let $x \in \mathbb{R} \setminus \{4\}$. Then

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f\left(\frac{2x-5}{4-x}\right) \\ &= \frac{4\left(\frac{2x-5}{4-x}\right) + 5}{\left(\frac{2x-5}{4-x}\right) + 2} \\ &= \frac{4(2x-5) + 5(4-x)}{(2x-5) + 2(4-x)} \\ &= \frac{3}{3} \\ &= x.\end{aligned}$$

  Therefore $f \circ g = \mathrm{Id}$.

Since $g = f^{-1}$, we conclude that f is invertible, and hence f is a bijection. □

(b) $g : \mathbb{R}^2 \to \mathbb{R}^2$ such that $g(x, y) = (3x + 4y, 2x + y)$.

Proof. Define $h : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$h(x, y) = \left(-\frac{1}{5}x + \frac{4}{5}y,\ \frac{2}{5}x - \frac{3}{5}y\right)$$

Note that for all $(x, y) \in \mathbb{R}^2$, $h(x, y)$ exists, is unique, and is an element of $\mathbb{R}^2$. It remains to show that $h = g^{-1}$.

To see that $h \circ g = \mathrm{Id}_{\mathbb{R}^2}$, let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{aligned}(h \circ g)(x, y) &= \left(-\frac{1}{5}(3x + 4y) + \frac{4}{5}(2x + y),\ \frac{2}{5}(3x + 4y) - \frac{3}{5}(2x + y)\right) \\ &= \left(-\frac{3}{5}x - \frac{4}{5}y + \frac{8}{5}x + \frac{4}{5}y,\ \frac{6}{5}x + \frac{8}{5}y - \frac{6}{5}x - \frac{3}{5}y\right) \\ &= (x, y)\end{aligned}$$

And to see that $g \circ h = \mathrm{Id}_{\mathbb{R}^2}$, again let $(x, y) \in \mathbb{R}^2$. Then

$$\begin{aligned}(g \circ h)(x, y) &= \left(3\left(-\frac{1}{5}x + \frac{4}{5}y\right) + 4\left(\frac{2}{5}x - \frac{3}{5}y\right),\ 2\left(-\frac{1}{5}x + \frac{4}{5}y\right) + \left(\frac{2}{5}x - \frac{3}{5}y\right)\right) \\ &= \left(-\frac{3}{5}x + \frac{12}{5}y + \frac{8}{5}x - \frac{12}{5}y,\ -\frac{2}{5}x + \frac{8}{5}y + \frac{2}{5}x - \frac{3}{5}y\right) \\ &= (x, y)\end{aligned}$$

Since $g \circ h = \mathrm{Id}_{\mathbb{R}^2}$ and $h \circ g = \mathrm{Id}_{\mathbb{R}^2}$ we conclude that g is a bijection. □

Exericse 17.1.6

Let A and B be nonempty sets and $f : A \to B$ be a function. Prove that f has a left inverse if and only if f is injective.

Proof. Assume A and B are non-empty sets and $f : A \to B$ is a function.

($\Rightarrow$) Let $g : B \to A$ be a left inverse of f. Then $g \circ f = \mathrm{Id}_A$ by definition of a left inverse. To see that f is injective, let $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$. Since these values are equal, and elements of B, we must have $g(f(a_1)) = g(f(a_2))$. But then, by assumption $g \circ f = \mathrm{Id}_A$, so we have $\mathrm{Id}_A(a_1) = \mathrm{Id}_A(a_2)$. Finally, by definition of the identity function, we get that $a_1 = a_2$, as desired. Therefore f is an injection.

($\Leftarrow$) Assume f is injective. Since $A \neq \varnothing$, fix a value $a_0 \in A$. Note that since f is injective, if $b \in \mathrm{Im}(f)$ then $\exists!\, a \in A$ such that $f(a) = b$. Define $g : B \to A$ as follows:

$$g(b) = \begin{cases} a & \text{if } b \in \mathrm{Im}(f) \wedge f(a) = b \\ a_0 & \text{if } b \notin \mathrm{Im}(f) \end{cases}$$

From the observations that a is unique if it exists, we have that g is well-defined. Moreover, let $a \in A$ be arbitrary, and let $b = f(a)$. Then

$$(g \circ f)(a) = g(f(a)) = g(b) = a$$

Hence, $g \circ f = \mathrm{Id}_A$, and we conclude that g is a left-inverse. □

17. October 6

Exercise 18.1.1

Let $S = [6]$.

(a) If possible, construct a relation R on S that is reflexive and symmetric but not transitive. If not possible, write "Not Possible." Briefly explain your reasoning.

Possible Solution: Define R as follows.

$$R = \{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3),(4,4),(5,5),(6,6)\}$$

R is reflexive since $(a,a) \in R$ for each $a \in [6]$. R is symmetric since whenever $(a,b) \in R$ we also have $(b,a) \in R$. But R is not transitive since $(1,2),(2,3) \in R$ but $(1,3) \notin R$.

(b) If possible, construct a relation R' on S that is symmetric and transitive but not reflexive. If not possible, write "Not Possible." Briefly explain your reasoning.

Possible Solution: We could define R' as simply as $R' = \{(1,1)\}$ to satisfy these conditions. We observe that R' is symmetric since for any $(a,b) \in R'$ we also have $(b,a) \in R'$ (there's only 1 element to check). R' is also transitive since whenever $(a,b),(b,c) \in R'$ we have $(a,c) \in R'$. Again, there's only 1 element, so the only possibility is that $(a,b) = (b,c) = (1,1)$. In which case $(a,c) = (1,1) \in R'$. However, R' is not reflexive since $(2,2) \notin R'$.

Exercise 18.1.2

Let $S = [5]$ and define $R \subseteq S^2$ as follows:

$$R = \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3),(4,4),(5,5)\}$$

Determine whether or not R satisfies the following properties. Provide brief justifications.

(a) Reflexivity

Answer: Yes. $(a,a) \in R$ for each $a \in [5]$.

(b) Irreflexivity

Answer: No. $(1,1) \in R$ so R is not irreflexive.

(c) Symmetry

Answer: No. $(1,2) \in R$ but $(2,1) \notin R$.

(d) Antisymmetry

Answer: Yes. For any $a \neq b \in S$ either $(a, b) \notin R$ or $(b, a) \notin R$.

(e) Transitivity

Answer: Yes. For any $a, b, c \in S$ if $(a, b), (b, c) \in R$ then $(a, c) \in R$.

(f) Totality

Answer: No. $1, 4 \in S$ with $1 \neq 4$, but $(1, 4) \notin R$ and $(4, 1) \notin R$.

18. October 8

Exercise 19.1.2

For each of the following, prove that the given relation is an equivalence relation and describe the different equivalence classes.

(a) Suppose $f : A \to B$ is a function. Define the relation $\sim$ on B by

$$x \sim y \quad \iff \quad \text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{y\})$$

(b) Define $\simeq$ on $\mathbb{Z}$ by

$$x \simeq y \quad \iff \quad |x| = |y|$$

(c) Define $\cong$ on $\mathbb{Z}$ by

$$x \cong y \quad \iff \quad 11 \mid 4x + 7y$$

(d) Define $\doteq$ on $\mathbb{Q} \setminus \{0\}$ by

$$x \doteq y \quad \iff \quad \exists k \in \mathbb{Z},\ \frac{x}{y} = 2^k$$

(e) Define $\approx$ on $\mathbb{Z}$ by

$$x \approx y \quad \iff \quad \cos(x)\cos(y) > 0$$

Proof Outlines.

(a) Reflivity/symmetry/transitivity follows from equality of sets.

- (R): $\text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{x\})$.
- (S): If $\text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{y\})$ then equality is symmetric.
- (T) If $\text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{y\})$ and $\text{PreIm}_f(\{y\}) = \text{PreIm}_f(\{z\})$ then $\text{PreIm}_f(\{x\}) = \text{PreIm}_f(\{z\})$.

Equivalence classes. Each element in $\mathrm{Im}(f)$ is in its own equivalence class consisting of just itself, and there is one additional equivalence class consisting of all elements of $B \setminus \mathrm{Im}(f)$.

(b) Reflivity/symmetry/transitivity follows from properties of equalities.

- (R): $|x| = |x|$.
- (S): $|x| = |y| \Rightarrow |y| = |x|$.
- (T): $|x| = |y|$ and $|y| = |z|$ imply $|x| = |z|$.

Equivalence classes. For $n \in \mathbb{N}$,

$$[0]_{\simeq} = \{0\}, \qquad [n] = \{n, -n\} \text{ for } n \geq 1.$$

(c)

- (R): $4x + 7x = 11x$ is divisible by 11.
- (S): We know $11 \mid 11x + 11y$. If $11 \mid 4x + 7y$ then $11 \mid (11x + 11y) - (4x + 7y)$.
- (T): $11 \mid 4x + 7y$ and $11 \mid 4y + 7z$, then 11 divides their sum:

  $$(4x + 7y) + (4y + 7z) = 4x + 7z + 11y$$

  Since $11 \mid 11y$, we can demonstrate that $11 \mid 4x + 7z$.

Equivalence classes. This is the same relation as congruence modulo 11. There is one equivalence class for each of the 11 possible remainders.

(d)

- (R): $x/x = 1 = 2^0$.
- (S): If $x/y = 2^k$ then $y/x = 2^{-k}$ and $-k \in \mathbb{Z}$.
- (T): If $x/y = 2^k$ and $y/z = 2^\ell$ then $x/z = (x/y)(y/z) = 2^{k+\ell}$.

Equivalence classes. Each class is all numbers that differ by a power of 2:

$$[x]_{\doteq} = \{2^k x : k \in \mathbb{Z}\}.$$

To pick a simple representative for each class, write $x = \dfrac{a}{b}$ in lowest terms. Then divide out every factor of 2 from both a and b until they are both odd. The fraction you get (with its sign) is a canonical representative.

For example, $\dfrac{12}{5}$ and $\dfrac{3}{20}$ are in the same class, since both reduce to the representative $\dfrac{3}{5}$ after removing factors of 2.

(e)

- **Well-defined remark:** For integers n we have $\cos n \neq 0$ (cosine vanishes only at $(2k+1)\pi/2$, which is never an integer), so $\cos n \cos n > 0$ holds for every integer n.

- (R): $\cos^2(x) > 0$ for all $x \in \mathbb{Z}$, so $x \approx x$.
- (S): $\cos(x)\cos(y) > 0 \iff \cos(y)\cos(x) > 0$.
- (T): If $\cos x$ and $\cos y$ have the same sign, and $\cos y$ and $\cos z$ have the same sign, then $\cos x$ and $\cos z$ have the same sign, hence $\cos x \cos z > 0$.

Equivalence classes. The relation partitions $\mathbb{Z}$ into two classes:

$$\{n \in \mathbb{Z} : \cos n > 0\} \quad \text{and} \quad \{n \in \mathbb{Z} : \cos n < 0\}.$$

(There is no integer with $\cos n = 0$, so no third class occurs.)

Exercise 19.1.8

Prove the following properties of $\mathbb{Z}$ using the equivalence class construction:

(a) Show that the element $[(a, a)]_\sim$ serves as the additive identity in $\mathbb{Z}$.

Proof. Let $(x, y) \in \mathbb{N}^2$ and let $a \in \mathbb{N}$ be arbitrary. We want to show that

$$[(x, y)]_\sim + [(a, a)]_\sim = [(x, y)]_\sim.$$

By definition,

$$[(x, y)]_\sim + [(a, a)]_\sim = [(x + a, y + a)]_\sim.$$

It remains to show that $[(x + a,\, y + a)]_\sim = [(x, y)]_\sim$. To see this, observe that

$$x + (y + a) = y + (x + a),$$

so $(x, y) \sim (x + a,\, y + a)$. Hence $[(x, y)]_\sim = [(x + a,\, y + a)]_\sim$, as desired. □

(b) Prove that for each $[(a, b)]_\sim \in \mathbb{Z}$, the element $[(b, a)]_\sim$ is its additive inverse.

Proof. Let $(a, b) \in \mathbb{N}^2$. We want to show that

$$[(a, b)]_\sim + [(b, a)]_\sim = [(0, 0)]_\sim.$$

By definition,

$$[(a, b)]_\sim + [(b, a)]_\sim = [(a + b, b + a)]_\sim.$$

Furthermore,

$$(a + b) + 0 = 0 + (b + a),$$

so $(a + b, b + a) \sim (0, 0)$, and hence $[(a + b, b + a)]_\sim = [(0, 0)]_\sim$, as desired. □

(c) Show that $[(1, 0)]_\sim$ is the multiplicative identity in $\mathbb{Z}$.

Proof. Let $(a, b) \in \mathbb{N}^2$. We want to show that

$$[(a, b)]_\sim \cdot [(1, 0)]_\sim = [(a, b)]_\sim.$$

By definition,

$$[(a, b)]_\sim \cdot [(1, 0)]_\sim = [(a + 0, 0 + b)]_\sim = [(a, b)]_\sim,$$

as desired. Therefore $[(1, 0)]_\sim$ is the multiplicative identity. □

(d) Verify that addition and multiplication in $\mathbb{Z}$ are commutative.

Proof. Let $(a, b), (c, d) \in \mathbb{N}^2$.

- **Addition**: From the commutativity of addition in $\mathbb{N}$ we have

$$\begin{aligned}[(a, b)]_\sim + [(c, d)]_\sim &= [(a + c, b + d)]_\sim \\ &= [(c + a, d + b)]_\sim \\ &= [(c, d)]_\sim + [(a, b)]_\sim.\end{aligned}$$

- **Multiplication**: From the commutativity of addition and multiplication in $\mathbb{N}$ we have

$$\begin{aligned}[(a, b)]_\sim \cdot [(c, d)]_\sim &= [(ad + bc, ac + bd)]_\sim \\ &= [(cb + da, ca + db)]_\sim \\ &= [(c, d)]_\sim \cdot [(a, b)]_\sim.\end{aligned}$$

Therefore, addition and multiplication are commutative in $\mathbb{Z}$. □

(e) Prove that multiplication distributes over addition.

Proof. Let $(a, b), (c, d), (e, f) \in \mathbb{N}^2$. We want to show that

$$[(a, b)]_\sim \cdot ([(c, d)]_\sim + [(e, f)]_\sim) = ([(a, b)]_\sim \cdot [(c, d)]_\sim) + ([(a, b)]_\sim \cdot [(e, f)]_\sim).$$

By definition of addition and multiplication in $\mathbb{Z}$,

$$\begin{aligned}[(a, b)]_\sim \cdot ([(c, d)]_\sim + [(e, f)]_\sim) &= [(a, b)]_\sim \cdot [(c + e,\ d + f)]_\sim \\ &= [(a(d + f) + b(c + e),\ a(c + e) + b(d + f))]_\sim.\end{aligned}$$

Expanding both components and regrouping terms using commutativity and associativity in $\mathbb{N}$ gives

$$[(ad + af + bc + be,\ ac + ae + bd + bf)]_\sim.$$

On the other hand,

$$\begin{aligned}([(a,b)]_\sim \cdot [(c,d)]_\sim) + ([(a,b)]_\sim \cdot [(e,f)]_\sim) &= [(ad+bc,\, ac+bd)]_\sim + [(af+be,\, ae+bf)]_\sim \\ &= [(ad+af+bc+be,\, ac+ae+bd+bf)]_\sim.\end{aligned}$$

The two results are equal, so multiplication distributes over addition. □

(f) Prove that $\mathbb{Z}$ has no zero divisors. That is, if $[(a,b)]_\sim \cdot [(c,d)]_\sim = [(0,0)]_\sim$ then $[(a,b)]_\sim = [(0,0)]_\sim$ or $[(c,d)]_\sim = [(0,0)]_\sim$.

Proof. Let $(a,b),(c,d) \in \mathbb{N}^2$ such that

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(0,0)]_\sim.$$

By definition,

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ad+bc,\, ac+bd)]_\sim.$$

Hence $(ad+bc,\, ac+bd) \sim (0,0)$, which means

$$ad+bc+0 = ac+bd+0,$$

or equivalently,

$$ad+bc = ac+bd.$$

Rearranging terms yields

$$(a-b)(c-d) = 0.$$

Since $\mathbb{N}$ has no zero divisors, either $a=b$ or $c=d$.

- If $a=b$, then $[(a,b)]_\sim = [(0,0)]_\sim$;
- if $c=d$, then $[(c,d)]_\sim = [(0,0)]_\sim$.

Thus $\mathbb{Z}$ has no zero divisors. □

Exercise 19.1.12

Prove that addition and multiplication are well-defined operations on the set of rationals.

(a) Addition:

Proof. Let $(a,b),(a',b'),(c,d),(c',d') \in \mathbb{Z} \times \mathbb{Z}^*$ such that $(a,b) \simeq (a',b')$ and $(c,d) \simeq (c',d')$. Then, by definition of $\simeq$, we have $ab' = a'b$ and $cd' = c'd$. This implies

$$(ab')(dd') + (cd')(bb') = (a'b)(dd') + (c'd)(bb')$$

Factoring this equation on the left and right we have

$$(ad+bc)b'd' = (a'd'+b'c')bd$$

Hence $(ad+bc, bd) \simeq (a'd'+b'c', b'd')$ and we conclude that our definition of addition is well-defined. □

(b) Multiplication:

Proof. Let $(a,b),(a',b'),(c,d),(c',d') \in \mathbb{Z} \times \mathbb{Z}^*$ such that $(a,b) \simeq (a',b')$ and $(c,d) \simeq (c',d')$. Then $ab' = a'b$ and $cd' = c'd$. This implies

$$(ab')(cd') = (a'b)(c'd)$$

By the commutativity of multiplication on $\mathbb{Z}$ we have

$$acb'd' = a'c'bd$$

which implies $(ac,bd) \simeq (a'c',b'd')$, as desired. Therefore multiplication is well-defined. □

19. October 10

Exercise 20.1.3

Define a relation $\preceq$ on $\mathbb{N}$ by

$$m \preceq n \quad \text{iff} \quad m \mid n.$$

(a) Prove that $\preceq$ is a partial order on $\mathbb{N}$.

Proof. We proceed to prove integer divisibility is reflexive, antisymmetric, and transitive.

- (R): Let $n \in \mathbb{N}$. Since $n = 1 \cdot n$, we have $n \mid n$, and hence $n \preceq n$, as desired.
- (AS): Let $m,n \in \mathbb{N}$ such that $m \mid n$ and $n \mid m$. Then there exists $k,\ell \in \mathbb{N}$ such that $n = mk$ and $m = n\ell$. Substituting the latter into the former and rearranging we have

  $$n = nk\ell \quad \Rightarrow \quad n(1 - k\ell) = 0$$

  Then either $n = 0$ or $k\ell = 1$. If $n = 0$ then $m = 0$ and we have $n = m$. Else, $k\ell = 1$ implies that $k = \ell = 1$ because $k,\ell \geq 0$. Therefore, $m = n$, as desired.

  In either case we concluded that $m = n$, so $\preceq$ is antisymmetric.
- (Tr): Proven in Theorem 2.1.6.

Therefore, $(\mathbb{N}, |)$ is a poset. □

(b) Prove that $\preceq$ is not a total order on $\mathbb{N}$.

Counterexample. Consider $m = 2$ and $n = 3$. Then $m \neq n$ but $m \nmid n$ and $n \nmid m$. Therefore, $\preceq$ is not total.

(c) An element $n \in \mathbb{N}$ is called a *minimal element* if there is no $m \in \mathbb{N}$ such that $m \preceq n$, other than n itself. Find all minimal elements of $\mathbb{N}$ under this ordering.

Solution. 1 is the only minimal element under this ordering. For any $n \in \mathbb{N}$, $1 \mid n$, so $1 \preceq n$ for all $n \in \mathbb{N}$. Furthermore, for any $m \in \mathbb{N}$, if $m \mid 1$ then $m = 1$.

(d) An element $n \in \mathbb{N}$ is called a *maximal element* if there is no $m \in \mathbb{N}$ such that $n \preceq m$, other than n itself. Find all maximal elements of $\mathbb{N}$ under this ordering.

Solution. 0 is the only maximal element under this ordering. For any $n \in \mathbb{N}$, $n \mid 0$. Furthermore, if $0 \mid n$ then $n = 0$.

Exercise 20.1.4

Define a relation $\preceq$ on $\mathbb{Q}^+$ (the set of positive rational numbers) by

$$a \preceq b \quad \text{iff} \quad \exists m \in \mathbb{Z}^+, a = bm$$

Determine whether or not $\preceq$ is a partial order on $\mathbb{Q}^+$. If so, determine whether it is also a total order. If not, identify a property that it fails to satisfy.

Claim. $(\mathbb{Q}^+, \preceq)$ is a poset but not a toset.

Proof. To show that $\preceq$ is a partial order, we need to demonstrate that it is reflexive, antisymmetric, and transitive.

- (R): Let $a \in \mathbb{Q}^+$. Since $a = 1 \cdot a$, we have $a \preceq a$.

- (AS): Let $a, b \in \mathbb{Q}^+$ such that $a \preceq b$ and $b \preceq a$. This means there exist $m, n \in \mathbb{Z}^+$ such that $a = bm$ and $b = an$. Thus,

  $$a = bm \quad \text{and} \quad b = an \implies a \geq b \quad \text{and} \quad b \geq a.$$

  Consequently, we have $a = b$, satisfying the antisymmetry property.

- (Tr): Let $a, b, c \in \mathbb{Q}^+$ such that $a \preceq b$ and $b \preceq c$. Then there exist $m, n \in \mathbb{Z}^+$ such that $a = bm$ and $b = cn$. Thus,

  $$a = bm = (cn)m = c(nm).$$

  Since $nm \in \mathbb{Z}^+$, it follows that $a \preceq c$, demonstrating the transitive property.

Therefore, $\preceq$ is a partial order on $\mathbb{Q}^+$.

Next, to establish that $\preceq$ is not total, consider the elements $a = \frac{1}{2}$ and $b = \frac{1}{3} \in \mathbb{Q}^+$. We find that:

- $a \not\preceq b$ because $\frac{3}{2} \notin \mathbb{Z}$, and
- $b \not\preceq a$ because $\frac{2}{3} \notin \mathbb{Z}$.

Since neither $a \preceq b$ nor $b \preceq a$ holds, we conclude that $\preceq$ is not a total order. □

Exercise 20.1.5

A relation R on a set U is called *asymmetric* if and only if for all $x, y \in U$, if $(x, y) \in R$ then $(y, x) \notin R$. Prove that a relation R on a set U is asymmetric if and only if R is both anti-symmetric and irreflexive.

Proof. Let R be a binary relation on a set U.

($\Rightarrow$): Assume R is asymmetric. We need to show that R is both anti-symmetric and irreflexive.

- (Irreflexivity): Let $x \in U$. Assume for the sake of contradiction that $(x, x) \in R$. Then, since R is asymmetric, we have that $(x, x) \notin R$, an obvious contradiction. So it must be the case that $(x, x) \notin R$. Since $x \in U$ was arbitrary, we have that R is irreflexive.
- (Antisymmetry): Let $x, y \in U$ such that $x \neq y$. We wish to show that $(x, y) \notin R$ or $(y, x) \notin R$. If $(x, y) \notin R$ then we're done. If $(x, y) \in R$ then, since R is asymmetric, we have that $(y, x) \notin R$ as desired. Thus R is antisymmetric.

($\Leftarrow$): Assume R is irreflexive and antisymmetric. We need to show that R is asymmetric.

Let $x, y \in U$ and assume for the sake of contradiction that $(x, y) \in R$ and $(y, x) \in R$. Since R is antisymmetric, we have $x = y$. Hence, $(x, x) \in R$, contradicting the fact that R is irreflexive. Thus for any $x, y \in U$, if $(x, y) \in R$ then $(y, x) \notin R$ and we conclude that R is asymmetric. □

20. October 20

Exercise 21.2.8

Let X and Y be non-empty sets with $|X| = m$ and $|Y| = n$. Prove that the number of functions $f : X \to Y$ is n^m.

Proof. Let $\mathcal{F}$ be the set of all functions $f : X \to Y$. Fix a bijection $\varphi : [m] \to X$

(this exists because $|X| = m$). We exhibit a bijection between Y^m (the set of all ordered m-tuples from Y) and $\mathcal{F}$.

Define

$$\Phi : Y^m \to \mathcal{F}, \qquad \Phi((y_1, \ldots, y_m)) = f$$

where $f : X \to Y$ is defined by

$$f(\varphi(i)) := y_i \qquad (1 \leq i \leq m).$$

That is, the i-th coordinate of the tuple because of the value of f at the i-th element of X under the fixed enumeration φ. To see that f is a bijection:

- *Injectivity.* Let $(y_1, \ldots, y_m), (y'_1, \ldots, y'_m) \in Y^m$ such that $\Phi(y_1, \ldots, y_m) = \Phi(y'_1, \ldots, y'_m)$. Then the two resulting functions agree on every element of X. (In particular, they agree at $\varphi(i)$ for each i.) So $y_i = y'_i$ for all i, and hence $(y_1, \ldots, y_m) = (y'_1, \ldots, y'_m)$.
- *Surjectivity.* Let $f \in \mathcal{F}$. Define the tuple $(y_1, \ldots, y_m) \in Y^m$ by

  $$y_i = f(\varphi(i)) \quad \text{for } 1 \leq i \leq m$$

  Then $\Phi(y_1, \ldots, y_m) = f$, by definition.

Thus $|\mathcal{F}| = |Y^m|$. It follows from Theorem 21.2.5 and induction that $|Y^m| = |Y|^m = n^m$. Hence, $|\mathcal{F}| = n^m$. □

Exercise 21.2.9

Define a relation $\cong$ on $\mathcal{P}(\mathbb{Z})$ by

$$A \cong B \quad \text{if and only if} \quad A \triangle B \text{ is finite}$$

(a) Prove that $\cong$ is an equivalence relation on $\mathcal{P}(\mathbb{Z})$.

Proof. We proceed to show $\cong$ is reflexive, symmetric, and transitive.

- (R): Let $X \in \mathcal{P}(\mathbb{Z})$. Since $X \triangle X = \varnothing$ and $|\varnothing| = 0$, we have that $X \cong X$, as desired.
- (S): Let $X, Y \in \mathcal{P}(\mathbb{Z})$ such that $X \cong Y$. This implies that $X \triangle Y$ is finite. Since $A \triangle B = B \triangle A$ (by the commutativity of unions and intersections), we have that $B \cong A$, as desired.
- (T): Let $X, Y, Z \in \mathcal{P}(\mathbb{Z})$ such that $X \cong Y$ and $Y \cong Z$. Then $A \triangle B$ and $B \triangle C$ are finite. Note that by Theorem 21.2.7 this implies that $(A \triangle B) \cup (B \triangle C)$ is finite. To see that $A \triangle C$ is finite, it suffices to prove that

  $$A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$$

Let $x \in A \triangle C$. Then $x \in A \cup C$ but $x \notin A \cap C$. Without loss of generality, assume $x \in A$ and $x \notin C$.

- If $x \notin B$ then $x \in A \triangle B$ and hence $x \in (A \triangle B) \cup (B \triangle C)$.
- If $x \in B$ then $x \in B \triangle C$ and hence $x \in (A \triangle B) \cup (B \triangle C)$.

Therefore, $A \triangle C \subseteq (A \triangle B \cup (B \triangle C)$ and we conclude that $A \cong C$, as desired.

Therefore, $\cong$ is an equivalence relation on $\mathcal{P}(\mathbb{Z})$. □

(b) Describe the elements in $[\varnothing]_{\cong}$. List 3 distinct elements from this set.

Solution. The equivalence class $[\varnothing]_{\cong}$ consists of all finite sets. Examples include $\varnothing, \{1\}, \{2\}, \{1, 2\}, \ldots$.

(c) Describe the elements in $[\mathbb{N}]_{\cong}$. List 3 distinct elements from this set.

Solution. The equivalence class $[\mathbb{N}]_{\cong}$ all sets X such that $X \setminus \mathbb{N}$ and $\mathbb{N} \setminus X$ are both finite. Examples include $\mathbb{N}$, $\mathbb{N} \setminus \{1\}$, $\mathbb{N} \cup \{-1\}$, etc.

21. October 24

Exercise 22.1.9

This problem explores the existence of bijections between the open interval $(0, 1)$ and the closed interval $[0, 1]$.

Consider the inclusion map $f : (0, 1) \to [0, 1]$ defined by $f(x) = x$ and the function $g : [0, 1] \to (0, 1)$ defined by $g(x) = \frac{2x+1}{4}$.

(a) Briefly justify that f and g are injections, verifying the hypothesis of the CBS Theorem.

Proofs.

- For $x_1, x_2 \in (0, 1)$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$ immediately.
- For $x_1, x_2 \in [0, 1]$, if $g(x_1) = g(x_2)$ then $\frac{2x_1+1}{4} = \frac{2x_2+1}{4}$ implying that $x_1 = x_2$. □

(b) The CBS Theorem implies that a bijection $h : (0, 1) \to [0, 1]$ exists. Give an explicit formula for the bijection h constructed by the proof of the theorem using these specific functions f and g.

Solution. We find

$$\begin{aligned} S &= (A \smallsetminus \mathrm{Im}(g)) \cup \mathrm{Im}_{g\circ f}(A \smallsetminus \mathrm{Im}(g)) \cup \mathrm{Im}_{g\circ f\circ g\circ f}(A \smallsetminus \mathrm{Im}(g)) \cup \cdots \\ &= \left(\left(0, \tfrac{1}{4}\right) \cup \left(\tfrac{3}{4}, 1\right) \right) \cup \left(\left(\tfrac{1}{4}, \tfrac{3}{8}\right) \cup \left(\tfrac{5}{8}, \tfrac{3}{4}\right) \right) \cup \left(\left(\tfrac{3}{8}, \tfrac{7}{16}\right) \cup \left(\tfrac{9}{16}, \tfrac{5}{8}\right) \right) \cup \cdots \\ &= (0,1) \smallsetminus \left\{ x \in (0,1) \mid \exists n \in \mathbb{N}, \left(x = \tfrac{1}{2} - \tfrac{1}{2^{n+2}} \vee x = \tfrac{1}{2} + \tfrac{1}{2^{n+2}} \right) \right\} \end{aligned}$$

Since f is the inclusion map, and $g^{-1}(x) = \frac{4x-1}{2}$, the resulting bijection h is

$$h(x) = \begin{cases} \frac{1}{2} - \frac{1}{2^{n+1}} & \text{if } \exists n \in \mathbb{N}, x = \frac{1}{2} - \frac{1}{2^{n+2}} \\ \frac{1}{2} + \frac{1}{2^{n+1}} & \text{if } \exists n \in \mathbb{N}, x = \frac{1}{2} + \frac{1}{2^{n+1}} \\ x & \text{otherwise} \end{cases}$$

The bijection h makes room for the endpoints 0 and 1 by shifting two countable sequences:

Domain $(0,1)$:	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{7}{16}$	$\frac{15}{32}$	$\cdots$
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
Codomain $[0,1]$:	0	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{7}{16}$	$\cdots$

and similarly for the upper sequence:

Domain $(0,1)$:	$\frac{3}{4}$	$\frac{5}{8}$	$\frac{9}{16}$	$\frac{17}{32}$	$\cdots$
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
Codomain $[0,1]$:	1	$\frac{3}{4}$	$\frac{5}{8}$	$\frac{9}{16}$	$\cdots$

All other elements are fixed.

(c) Find another bijection $j : (0,1) \to [0,1]$ (or vice versa) without using the CBS Theorem.

Possible Solution. We use a similar idea and take a countable subset of $(0,1)$ and shift the terms up or down (depending on the direction you are going) to account for the two additional elements. Define $j : (0,1) \to [0,1]$ by

$$j(x) = \begin{cases} 0 & \text{if } n = \frac{1}{2} \\ \frac{1}{n-2} & \text{if } \exists n \in \mathbb{N}, \left(n \geq 3 \wedge x = \frac{1}{n} \right) \\ x & \text{otherwise} \end{cases}$$

In this function, all elements get mapped to themselves except those of the form $\frac{1}{n}$. These elements shift as follows:

$$\begin{array}{lccccccccc} \text{Domain:} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7} & \cdots & \text{All other } x \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow \\ \text{Codomain:} & 0 & 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots & x \end{array}$$

Exercise 22.1.10

Let $S = \{n \in \mathbb{Z} \mid n \not\equiv 0 \pmod 7\}$. Use the CBS Theorem to show that there exists a bijection between S and $\mathbb{N}$.

Possible Solution.

- Define $f : \mathbb{N} \to S$ by $f(n) = 7n + 1$. It is a straightforward verification that f is injective.
- Define $g : S \to \mathbb{N}$ by
$$f(n) = \begin{cases} n & \text{if } n \geq 0 \\ -7n & \text{if } n < 0 \end{cases}$$
Since $n \not\equiv 0 \pmod 7$, we assure injectivity by sending negative values to multiples of 7. It is left to the reader to work out the details of the injectivity proof.

By the CBS Theorem, there must exist a bijection $h : \mathbb{N} \to S$. □

22. October 27

Exercise 23.1.8

Show that the following sets are countably infinite.

(a) $A = \{f : \{0, 1\} \to \mathbb{N} \mid f \text{ is a function}\}$

Proof Sketch. Construct a bijection $\varphi : A \to \mathbb{N}^2$ by $\varphi(f) = (f(0), f(1))$. Since $\mathbb{N}^2$ is countably infinite, so must be A.

(b) $B =$ the set of circles in $\mathbb{R}^2$ whose centers have integer coordinates and whose radii have rational lengths.

Proof Sketch. Each circle in the plane can be uniquely identified by its center $(h, k) \in \mathbb{R}^2$ and its radius $r \in [0, \infty)$. Since B is the set of circles whose centers have *integer* coordinates and whose radii have *rational* length we have that $|B| = |B'|$ where
$$B' = \{(h, k, r) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Q} \mid r \geq 0\} \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Q}$$

Since $\mathbb{Z}$ and $\mathbb{Q}$ are both countable, we have that $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Q}$ is countable (finite Cartesian product of countable sets) and hence B' is countable. Finally, we note that B' is clearly infinite since we can inject $f : \mathbb{Z} \to B'$ by $f(n) = (n, 0, 1)$. Since $|B'| = |B|$ we conclude that B is countably infinite

(c) $C = \{f : \mathbb{N} \to \mathbb{N} \mid \forall x \in \mathbb{N}, f(x+1) = f(x) + 1\}$

Proof Sketch. Define a function $\varphi : C \to \mathbb{N}$ by $\varphi(f) = f(0)$. To see that φ is a bijection:

- (1-to-1): Let $f, g \in A$ such that $\varphi(f) = \varphi(g)$. Proceed by induction to show that $f(n) = g(n)$ for all $n \in \mathbb{N}$ to conclude that $f = g$.
- (Onto): Let $y \in \mathbb{N}$ be arbitrary. Define $f : \mathbb{N} \to \mathbb{N}$ recursively by $f(0) = y$ and $f(n+1) = f(n) + 1$ for all $n \in \mathbb{N}$. Then $f \in A$ by definition and $\varphi(f) = f(0) = y$, as desired.

Since φ is a bijection we have $|A| = |\mathbb{N}|$ and thus A is countably infinite.

(d) D = the set of all "words", where a "word" is a finite string of letters from the English alphabet.

Proof Sketch. The set of all words can be expressed as $D = \bigcup_{i \in \mathbb{N}} W_i$ where each W_i is the set of words of length i. Since $|W_i| = 26^i$ for each $i \in \mathbb{N}$, each W_i is finite. Since D is a countable union of countable sets, it must also be countable. The set of all words is clearly not finite, since we can inject $\mathbb{N}$ into D by mapping n to the "word" consisting of only n-many `A`'s. Therefore, D must be countably infinite.

Exercise 23.2.1

Suppose that $x \in [0, 1)$ has two distinct decimal expansions:

$$x = 0.a_1a_2a_3\cdots,$$
$$x = 0.b_1b_2b_3\cdots,$$

where $a_i, b_i \in \{0, 1, \ldots, 9\}$ for all i. Let M be the smallest positive integer such that $a_M \neq b_M$ and assume that $a_M > b_M$. Prove that:

- $a_i = b_i$ for all $1 \leq i < M$,
- $a_M = b_M + 1$,
- $a_i = 0$ and $b_i = 9$ for all $i > M$.

Proof. By the definition of a decimal expansion, we have

$$x = \sum_{i=1}^{\infty} \frac{a_i}{10^i} = \sum_{i=1}^{\infty} \frac{b_i}{10^i}.$$

Let M be the smallest positive integer such that $a_M \neq b_M$. By the minimality of M, it follows immediately that

$$a_i = b_i \quad \text{for all } 1 \leq i < M.$$

Subtracting the finite sum of these identical terms from both sides yields

$$\sum_{i=M}^{\infty} \frac{a_i}{10^i} = \sum_{i=M}^{\infty} \frac{b_i}{10^i}.$$

We now prove the remaining two properties.

- Assume, for the sake of contradiction, that $a_M \neq b_M + 1$. Since $a_M > b_M$ by hypothesis, this implies $a_M \geq b_M + 2$.

  Rearranging the equation above, we isolate the M-th terms:

  $$\frac{a_M - b_M}{10^M} = \sum_{i=M+1}^{\infty} \frac{b_i - a_i}{10^i}.$$

  Since $a_i, b_i \in \{0, 1, \ldots, 9\}$, the maximum value of $b_i - a_i$ is 9. Therefore,

  $$\sum_{i=M+1}^{\infty} \frac{b_i - a_i}{10^i} \leq \sum_{i=M+1}^{\infty} \frac{9}{10^i} = 9 \cdot \frac{1/10^{M+1}}{1 - 1/10} = \frac{1}{10^M}.$$

  Combining these inequalities gives

  $$\frac{a_M - b_M}{10^M} \leq \frac{1}{10^M},$$

  which implies $a_M - b_M \leq 1$. This contradicts our assumption that $a_M \geq b_M + 2$. Hence, $a_M = b_M + 1$.

- Substituting $a_M = b_M + 1$ into the previous equation gives

  $$\frac{1}{10^M} = \sum_{i=M+1}^{\infty} \frac{b_i - a_i}{10^i}.$$

  We also have the established bound:

  $$\sum_{i=M+1}^{\infty} \frac{b_i - a_i}{10^i} \leq \sum_{i=M+1}^{\infty} \frac{9}{10^i} = \frac{1}{10^M}.$$

Since the left-hand side equals $\frac{1}{10^M}$, both inequalities must be equalities. In particular,

$$\sum_{i=M+1}^{\infty} \frac{b_i - a_i}{10^i} = \sum_{i=M+1}^{\infty} \frac{9}{10^i}.$$

For this to hold, we must have $b_i - a_i = 9$ for all $i > M$, because if $b_j - a_j < 9$ for any $j > M$, then the series would be strictly less than $\frac{1}{10^M}$. Since $a_i, b_i \in \{0, \ldots, 9\}$, the condition $b_i - a_i = 9$ is equivalent to $b_i = 9$ and $a_i = 0$ for all $i > M$.

23. October 29

Exercise 24.1.7

Show that the following sets are uncountable.

(a) $A = \{f : \mathbb{N} \to \{0, 1\} \mid f \text{ is a function}\}$

Proof Sketch. This set is essentially the same as $\{0, 1\}^{\mathbb{N}}$. We can define a bijection $f : \{0, 1\}^{\mathbb{N}} \to A$ by, for each binary sequence $g \in \{0, 1\}^{\mathbb{N}}$, defining a function $f_g \in A$ by $f_g(n) = g_n$.

(b) $B = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a function}\}$

Proof Sketch. $A \subseteq B$. Since A is uncountable, so is B.

(c) $C = \{f : \mathbb{N} \to \mathbb{N} \mid f \text{ is a bijection}\}$

Proof Sketch. We could inject $\{0, 1\}^{\mathbb{N}}$ into S_∞ by, for each binary sequence $g \in \{0, 1\}^{\mathbb{N}}$, defining a bijection $f_g : \mathbb{N} \to \mathbb{N}$ by

$$\begin{cases} \text{if } g_n = 0 & \text{then } f_g(2n) = 2n \text{ and } f_g(2n+1) = 2n+1 \\ \text{if } g_n = 1 & \text{then } f_g(2n) = 2n+1 \text{ and } f_g(2n+1) = 2n \end{cases}$$

Then define $\varphi : \{0, 1\}^{\mathbb{N}} \to S_\infty$ by $\varphi(g) = f_g$.

(d) $D =$ the set of infinite sequences of integers.

Proof Sketch. This is a superset of $\{0, 1\}^{\mathbb{N}}$ which we already know is uncountable.

(e) $E = \mathbb{R} \setminus \mathbb{Q}[\sqrt{2}]$ where

$$\mathbb{Q}[\sqrt{2}] = \{x \in \mathbb{R} \mid \exists a, b \in \mathbb{Q}, x = a + b\sqrt{2}\}$$

Proof Sketch. Since $\mathbb{Q}$ is countably infinite, so is $\mathbb{Q}^2$. The function $f : \mathbb{Q}^2 \to \mathbb{Q}[\sqrt{2}]$ defined by $f(a, b) = a + b\sqrt{2}$ is a bijection. Therefore, $\mathbb{Q}[\sqrt{2}]$ is countable.

Since $\mathbb{R}$ is uncountable and $\mathbb{Q}[\sqrt{2}]$ is countable, it must be the case that $\mathbb{R} \setminus \mathbb{Q}[\sqrt{2}]$ is uncountable. Otherwise, $\mathbb{R} = \left(\mathbb{R} \setminus \mathbb{Q}[\sqrt{2}]\right) \cup \mathbb{Q}[\sqrt{2}]$ is the finite union of countable sets, making it also countable, and contradicting the uncountability of $\mathbb{R}$.

Exercise 25.1.5

Determine which of the following integers are primes.

(a) 201

Solution. $\boxed{\text{No}}$. Divisible by 3

(b) 203

Solution. $\boxed{\text{No}}$. Divisible by 7

(c) 207

Solution. $\boxed{\text{No}}$. Divisible by 3

(d) 211

Solution. $\boxed{\text{Yes}}$.

(e) 213

Solution. $\boxed{\text{No}}$. Divisible by 3

(f) 221

Solution. $\boxed{\text{No}}$. Divisible by 13

24. October 31

Exercise 26.1.3

Find the greatest common divisor of each of the following pairs of integers.

(a) 5,15

Solution. $\gcd(5, 15) = 5$

(b) 0, 111

Solution. $\gcd(0, 111) = 111$

(c) $-27, -45$

Solution. $\gcd(-27, -45) = 9$

(d) -90, 100

Solution. $\gcd -90, 100 = 10$

(e) 100, 121

Solution. $\gcd(100, 121) = 1$

(f) 1001, 289

Solution. $\gcd(1001, 289) = 1$

Exercise 26.1.6

Without a calculator, use the Euclidean Algorithm to compute the GCD of the following pairs of integers.

(a) 171 and 33

Solution. $\boxed{\gcd(171, 33) = 3}$

$$\begin{aligned} 171 &= 33(5) + 633 & &= 6(5) + 3 \\ 6 &= 3(2) + 0 \end{aligned}$$

(b) 1872 and 300

Solution. $\boxed{\gcd(1872, 300) = 12}$

$$\begin{aligned} 1872 &= 300(6) + 72 \\ 300 &= 72(4) + 12 \\ 72 &= 12(6) + 0 \end{aligned}$$

(c) 325299 and 325

Solution. $\boxed{\gcd(325299, 325) = 13}$

$$\begin{aligned} 325299 &= 325(1000) + 299 \\ 325 &= 299(1) + 26 \\ 299 &= 26(11) + 13 \\ 26 &= 13(2) + 0 \end{aligned}$$

(d) $n^7 - 1$ and $n^5 - 1$ where $n > 1$

Solution. We use polynomial long division below:

$$\begin{aligned} n^7 - 1 &= (n^5 - 1)(n^2) + (n^2 - 1) \\ n^5 - 1 &= (n^2 - 1)(n^3 + n) + (n - 1) \\ n^2 - 1 &= (n - 1)(n + 1) + 0 \end{aligned}$$

Therefore,

$$\gcd(n^7-1, n^5-1) = \gcd(n^5-1, n^2-1) = \gcd(n^2-1, n-1) = \gcd(n-1, 0) = \boxed{n - 1}$$

Exercise 26.1.7

Prove that for any $n \in \mathbb{N}$, $5n + 3$ and $3n + 2$ are coprime.

Proof. Let $n \in \mathbb{N}$ be arbitrary and fixed. We perform the Euclidean algorithm on $5n+3$ and $3n + 2$.

$$\begin{aligned} 5n + 3 &= 1(3n + 2) + (2n + 1) \\ 3n + 2 &= 1(2n + 1) + (n + 1) \\ 2n + 1 &= 1(n + 1) + n \\ n + 1 &= 1(n) + 1 \\ n &= n(1) + 0 \end{aligned}$$

Therefore $\gcd(5n + 3, 3n + 2) = 1$. □

Exercise 26.1.11

(a) Use the Euclidean Algorithm to find $\gcd(1819, 3587)$.

Solution.

$$\begin{aligned} 3587 &= 1819(1) + 1768 \\ 1819 &= 1768(1) + 51 \\ 1768 &= 51(34) + 34 \\ 51 &= 34(1) + 17 \\ 34 &= 17(2) + 0 \end{aligned}$$

Thus $\boxed{\gcd(3587, 1819) = 17}$.

(b) Find a pair $(x, y) \in \mathbb{Z}^2$ such that $1819x + 3587y = \gcd(1819, 3587)$.

Solution. Back-substituting we get

$$\boxed{17 = 1819(71) + 3587(-36)}$$

This is just for you to check your answer. Full details should always be provided on assigned problems.

Exercise 26.1.12

Let $a, b \in \mathbb{Z}$, not both 0, and $m \in \mathbb{Z}^+$. Prove that $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Proof. Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(ma, mb)$. Further, let $(x_1, y_1), (x_2, y_2) \in \mathbb{Z}^2$ such that

$$\begin{aligned} ax_1 + by_1 &= d_1 \\ (ma)x_2 + (mb)y_2 &= d_2 \end{aligned}$$

Such pairs exist by Bézout's Lemma. Multiplying the first equation by m we have

$$(ma)x_1 + (mb)y_1 = md_1$$

Since md_1 can be written as a linear combination of ma and mb, we have $d_2 \mid md_1$, by the corollary to Bézout's Lemma.

From the second equation, we have that $m \mid d_2$ so $d_2 = mk$ for some $k \in \mathbb{Z}$. Dividing through by m we get

$$ax_2 + by_2 = k$$

Again, by the corollary to Bézout's Lemma we have that $d_1 \mid k$. Therefore $k = d_1\ell$ for some $\ell \in \mathbb{Z}$ and thus $d_2 = md_1\ell$. Hence $md_1 \mid d_2$.

Since $md_1 \mid d_2$ and $d_2 \mid md_1$, we have that $|md_1| = |d_2|$. But m, d_1, and d_2 are all positive, so we can conclude that $md_1 = d_2$, as desired. □

Exercise 26.1.13

Prove that if a and b are relatively prime integers then $\gcd(a + b, a - b) = 1$ or 2, with $\gcd(a + b, a - b) = 2$ if and only if a and b have the same parity.

Proof. Let $a, b \in \mathbb{Z}$ such that $gcd(a, b) = 1$. We first show that the only possibilities for the $\gcd(a + b, a - b)$ are 1 and 2.

Let $d \in \mathbb{Z}^+$ such that $d \mid a + b$ and $d \mid a - b$. Then we have $d \mid ((a + b) + (a - b)) = 2a$ and $d \mid ((a + b) - (a - b)) = 2b$. Since d is a common divisor of $2a$ and $2b$, we have

$d \mid \gcd(2a, 2b)$. Since $\gcd(ma, mb) = m \cdot \gcd(a, b)$ for all $m \in \mathbb{Z}^+$, along with our assumption that $\gcd(a, b) = 1$, we have that

$$\gcd(2a, 2b) = 2 \cdot \gcd(a, b) = 2.$$

This implies that $d \mid 2$. Therefore the only possible values for d are 1 and 2.

It remains to show that $\gcd(a + b, a - b) = 2$ iff $a \equiv b \pmod 2$.

- ($\Rightarrow$): By contraposition. Suppose $a \not\equiv b \pmod 2$. Then $2 \nmid a - b$ by definition of congruence modulo 2. Then 2 cannot be a common divisor of $a - b$ and $a + b$. Therefore $\gcd(a + b, a - b) \neq 2$, as desired.
- ($\Leftarrow$): Suppose $a \equiv b \pmod 2$. Then $2 \mid a - b$ by definition of congruence modulo 2. Additionally, $b \equiv -b \pmod 2$ because $2 \mid (b + b)$, so $a \equiv -b \pmod 2$ as well, implying that $2 \mid a + b$. Since $2 \mid a + b$, $2 \mid a - b$ and $\gcd(a + b, a - b)$ is at most 2, we can conclude that $\gcd(a + b, a - b) = 2$, as desired. □

25. November 3

Exercise 27.1.4

Find all integer solutions to the following linear Diophantine equations, or state why none exist.

(a) $123x + 45y = 17$

(b) $123x + 45y = 18$

Solutions. We first perform the Euclidean algorithm to compute $\gcd(123, 45)$:

$$\begin{aligned} 123 &= 45(2) + 33 \\ 45 &= 33(1) + 12 \\ 33 &= 12(2) + 9 \\ 12 &= 9(1) + 3 \\ 9 &= 3(3) + 0 \end{aligned}$$

Therefore, $\gcd(123, 45) = 3$.

1. There is $\boxed{\text{No Solution}}$ to $123x + 45y = 17$ because $3 \nmid 17$.

2. There are $\boxed{\text{Infinitely Many Solutions}}$ to $123x + 45y = 18$ because $3 \mid 18$. Back-substituting through the Euclidean algorithm yields:

$$123(-4) + 45(11) = 3$$

Multiplying through by 6 we have:

$$123(-24) + 45(66) = 18$$

Therefore $(x_0, y_0) = (-24, 66)$ is one solution to $123x + 45y = 18$. Hence the set of all solutions is:

$$\boxed{\{(-24 + 15k, 66 - 41k) \mid k \in \mathbb{Z}\}}$$

Exercise 27.1.7

Prove the statements in Corollary 27.1.6

Proofs.

1. Let $a, b \in \mathbb{Z}$, not both 0.

   ($\Rightarrow$): Suppose $\text{lcm}[a, b] = |b|$. This implies that $a \mid |b|$ and hence $a \mid b$.

   ($\Leftarrow$): Suppose $a \mid b$. Then $|b|$ is a common multiple of a and b. Hence, by the previous theorem, $\text{lcm}[a, b] \mid |b|$. By definition, $b \mid \text{lcm}[a, b]$, so $|b| | \text{lcm}[a, b]$. By the antisymmetry of divisibility on the natural numbers, we have $\text{lcm}[a, b] = |b|$. □

2. Let $m \in \mathbb{Z}^+$. Further, let $L = \text{lcm}[a, b]$ and $M = \text{lcm}[ma, mb]$. We want to show $M = mL$.

   - Since $a \mid L$ and $b \mid L$ by definition, it follows that $ma \mid mL$ and $mb \mid mL$. Thus, by the previous theorem, $M \mid mL$.
   - Conversely, since $ma \mid M$ and $mb \mid M$, there exists $k, \ell \in \mathbb{Z}$ such that

     $$M = mak = mb\ell.$$

     This implies that $\frac{M}{m} \in \mathbb{Z}$, since $\frac{M}{m} = ak = b\ell$. Thus, $a \mid \frac{M}{m}$ and $b \mid \frac{M}{m}$, implying that $L \mid \frac{M}{m}$, by the previous theorem. Hence, $mL \mid M$.

   Since $M \mid mL$ and $mL \mid M$, and both are positive, we conclude that $M = mL$. □

26. November 5

Exercise 28.1.7

(a) Prove that a positive integer n is a perfect square if and only if the exponent of each prime factor of n is even.

Proof. Let $n \in \mathbb{Z}^+$ with prime factorization

$$n = \prod_{i=1}^{k} p_i^{n_i} = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

In the case that $n = 1$, we can express this as $n = 2^0$.

($\Rightarrow$): Suppose n is a perfect square. Then $n = m^2$ for some $m \in \mathbb{Z}^+$. Furthermore, since $m \mid n$, we know that m can be expressed as

$$m = \prod_{i=1}^{k} p_i^{m_i} \quad \text{where } 0 \leq m_i \leq n_i \text{ for each } 1 \leq i \leq k.$$

Then

$$\prod_{i=1}^{k} p_i^{n_i} = n = m^2 = \prod_{i=1}^{k} p_i^{2m_i}.$$

By uniqueness of prime factorizations, we must have $n_i = 2m_i$ for each $1 \leq i \leq k$. Hence each n_i is even, as desired.

($\Leftarrow$): Suppose each exponent n_i is even. Then, for each $1 \leq i \leq k$, $n_i = 2m_i$ for some $m_i \in \mathbb{Z}^+$. Let

$$m = \prod_{i=1}^{k} p_i^{m_i}$$

Then $m^2 = n$, so n is a perfect square. □

(b) Prove that if a and b are coprime positive integers and their product is a perfect square, then a and b are themselves perfect squares.

Proof Sketch. Let $a, b \in \mathbb{Z}^+$ such that $ab = m^2$ for some $m \in \mathbb{Z}^+$. For any prime p appearing in the factorization of m^2, p cannot appear in both a and b, due to coprimality. Since the exponents of the factorization of ab are all even, by part (a), the exponents of p in the factorizations of either a or b must also be even. Thus, by part (a), both a and b are perfect squares.

(c) Prove that if a and b are positive integers and ab is a perfect square, then $a = dm^2$ and $b = dn^2$ where $d = \gcd(a, b)$, for some coprime integers m and n.

Proof. Let $d = \gcd(a, b)$ and write $a = da_1$ and $b = db_1$ for $a_1, b_1 \in \mathbb{Z}^+$. We know, from a previous theorem, that $\gcd(a_1, b_1) = 1$. Since $ab = (da_1)(db_1) = d^2 a_1 b_1$ is a perfect square, and d^2 is a perfect square, it follows that $a_1 b_1$ must also be a perfect square. Since $\gcd(a_1, b_1) = 1$, we can apply part (b) to conclude that a_1 and b_1 are themselves perfect squares. So, $a_1 = m^2$ and $b_1 = n^2$ for some coprime integers m, n. Substituting back, we get $a = da_1 = dm^2$ and $b = db_1 = dn^2$. □

(d) Reprove the irrationality of $\sqrt{2}$ in the following way:

- Assume for the sake of contradiction that $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ are coprime. Use part (a) to arrive at a contradiction.

Proof. Assume $\sqrt{2} = \frac{a}{b}$ with $a, b \in \mathbb{Z}^+$ coprime. Then $a^2 = 2b^2$. By part (a), the exponent of 2 in the prime factorization of both a^2 and b^2 must be even. However, $a^2 = 2b^2$ and the uniqueness of prime factorizations, implies that the exponent of 2 in a^2 is one more than the exponent of 2 in b^2, making the exponent of 2 in a^2 odd. This is a contradiction, so $\sqrt{2}$ must be irrational. □

Exercise 28.1.8

Use the fundamental theorem of arithmetic to prove that $17^{1/3}$ is irrational.

Proof Sketch. Assume, for the sake of contradiction, that there exists coprime $a, b \in \mathbb{Z}^+$ such that $\sqrt[3]{17} = \frac{a}{b}$.

$$\begin{aligned} \sqrt[3]{17} = \frac{a}{b} &\implies 17 = \frac{a^3}{b^3} \\ &\implies a^3 = 17b^3 \end{aligned}$$

Since 17 is prime, using a similar argument from the previous exercise, we have that the number of factors of 17 in a^3 and b^3 is a multiple of 3. However, $a^3 = 17b^3$ would imply that the number of factors of 17 in a^3 is one more than a multiple of 3, a contradiction. Therefore, $\sqrt[3]{17}$ is irrational.

Exercise 28.2.5

For each part below, determine whether the given set of integers S forms a complete set of residues modulo m.

(a) $S = \{4, 21, 104\}$, $m = 3$

Solution. $\boxed{\text{Yes}}$. We have 3 elements, one representing each congruence class.

$$\begin{aligned} 4 &\equiv 1 \pmod 3 \\ 21 &\equiv 0 \pmod 3 \\ 104 &\equiv 2 \pmod 3 \end{aligned}$$

(b) $S = \{-33, -5, -2, 2, 5, 12, 41\}$, $m = 8$

Solution. $\boxed{\text{No}}$. $|S| \neq 8$, so S can't possibly be a complete set of residues modulo 8.

(c) $S = \{-25, -15, -5, 0, 10, 20\}$, $m = 6$

Solution. Yes. We have 6 elements, one representing each congruence class.

$$\begin{aligned} -25 &\equiv 5 \pmod 6 \\ -15 &\equiv 3 \pmod 6 \\ -5 &\equiv 1 \pmod 6 \\ 0 &\equiv 0 \pmod 6 \\ 10 &\equiv 4 \pmod 6 \\ 20 &\equiv 2 \pmod 6 \end{aligned}$$

(d) $S = \{-68, -14, -6, 4, 40, 63, 83\}$, $m = 7$

Solution. No. There are multiple elements of S representing the same congruence class modulo 7.

$$-14 \equiv 63 \equiv 0 \pmod 7$$

27. November 7

Exercise 29.1.4

Prove that $4^n \equiv 1 + 3n \pmod 9$ for all $n \in \mathbb{N}$.

Proof. We proceed by induction on $n \in \mathbb{N}$.

- (Base Case): If $n = 0$ then we have $1 = 1 + 3(0)$ and hence $4^0 \equiv 1 + 3(0) \pmod 9$.
- (Inductive Step): Let $k \in \mathbb{N}$ and assume $4^k \equiv 1 + 3k \pmod 9$. We consider $n = k + 1$.

$$\begin{aligned} 4^{k+1} &\equiv 4 \cdot 4^k \pmod 9 \\ &\equiv 4(1 + 3k) \pmod 9 \quad \text{(By IH)} \\ &\equiv 4 + 12k \pmod 9 \\ &\equiv 1 + 3 + 3k \pmod 9 \\ &\equiv 1 + 3(k + 1) \pmod 9 \end{aligned}$$

By PMI, we conclude $4^n \equiv 1 + 3n \pmod 9$ for all $n \in \mathbb{N}$. □

Exercise 29.1.7

Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $\gcd(a, m) = 1$.

(a) Prove that for all $k, \ell \in \mathbb{Z}$, $k \equiv \ell \pmod{m}$ if and only if $ak \equiv a\ell \pmod{m}$.

Proof. Let $k, \ell \in \mathbb{Z}$.

($\Rightarrow$): Suppose $k \equiv \ell \pmod{m}$. Then, by the modular arithmetic lemma, $ak \equiv a\ell \pmod{m}$, and we're done.

($\Leftarrow$): Suppose $ak \equiv a\ell \pmod{m}$. Since $\gcd(a, m) = 1$ by assumption, the cancellation law yields

$$k \equiv \ell \pmod{\frac{m}{1}}.$$

Equivalently, $k \equiv \ell \pmod{m}$. □

(b) Prove that the following set forms a complete set of residues modulo m.

$$\{n \in \mathbb{Z} \mid \exists k \in [m], n = ak + b\}$$

Proof. Let

$$S = \{n \in \mathbb{Z} \mid \exists k \in [m],\ n = ak + b\}.$$

Suppose $k, \ell \in [m]$ and that $ak + b \equiv a\ell + b \pmod{m}$. Subtracting b from both sides of the congruence yields $ak \equiv a\ell \pmod{m}$. Since $\gcd(a, m) = 1$, part (a) implies $k \equiv \ell \pmod{m}$.

Thus, S consists of m distinct integers, each incongruent modulo m. Therefore, S forms a complete set of residues modulo m. □

Exercise 29.1.15

Use mental math or guess-and-check to find the multiplicative inverse of a modulo m for each of the following pairs (a, m).

(a) $a = 4$, $m = 9$

Solution. $4^{-1} \equiv 7 \pmod{9}$

(b) $a = 5$, $m = 22$

Solution. $5^{-1} \equiv 9 \pmod{22}$

(c) $a = 9$, $m = 41$

Solution. $9^{-1} \equiv 32 \pmod{41}$

Exercise 29.1.17

Use the Euclidean algorithm to find a multiplicative inverse of a modulo m for each of the following pairs (a, m).

(a) $a = 37$, $m = 101$

Solution. $37^{-1} \equiv 71 \pmod{101}$

(b) $a = 123$, $m = 256$

Solution. $123^{-1} \equiv 179 \pmod{256}$

Exercise 29.1.18

(a) Use the Euclidean algorithm to determine $\gcd(999, 102)$.

Solution.

$$\begin{aligned} 999 &= 9 \cdot 102 + 81 \\ 102 &= 1 \cdot 81 + 21 \\ 81 &= 3 \cdot 21 + 18 \\ 21 &= 1 \cdot 18 + 3 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

Therefore $\boxed{\gcd(999, 102) = 3}$.

(b) Find all $x, y \in \mathbb{Z}$ such that $999x + 102y = \gcd(999, 102)$.

Solution. Starting with the penultimate equation from part (a) and back-substituting we have the following chain of equalities.

$$\begin{aligned} 3 &= 21 - 18 \\ &= 21 - (81 - 3 \cdot 21) \\ &= 4 \cdot 21 - 81 \\ &= 4 \cdot (102 - 81) - 81 \\ &= 4 \cdot 102 - 5 \cdot 81 \\ &= 4 \cdot 102 - 5 \cdot (999 - 9 \cdot 102) \\ &= -5 \cdot 999 + 49 \cdot 102 \end{aligned}$$

Therefore one solution is given by $(x_0, y_0) = (-5, 49)$ and hence the set of all solutions is $\boxed{\{(-5 - 34k, 49 + 333k) \mid k \in \mathbb{Z}\}}$

(c) Find all integer solutions, if any, to the congruence $102x + 20 \equiv 461 \pmod{999}$.

Solution. From the previous part we have that $999(-5) + 102(49) = 3$. Dividing by 3 yields

$$333(-5) + 34(49) = 1$$

Observe that this implies that $34^{-1} \equiv 49 \pmod{333}$. This will be necessary for the rest of the solution. To find all $x \in \mathbb{Z}$ satisfying the congruence equation, we follow the chain of logical equivalences below.

$$\begin{aligned} 102x + 20 \equiv 461 \pmod{999} &\Leftrightarrow 102x \equiv 441 \pmod{999} \\ &\Leftrightarrow 34x \equiv 147 \pmod{333} \\ &\Leftrightarrow x \equiv 49 \cdot 147 \pmod{333} \\ &\Leftrightarrow x \equiv 210 \pmod{333} \end{aligned}$$

Therefore the solution set is $\boxed{\{x \in \mathbb{Z} \mid x \equiv 210 \pmod{333}\}}$. We may equivalently write this as $\boxed{\{x \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, x = 333k + 210\}}$ or $\boxed{[210]_{333}}$. (All are acceptable.)

28. November 10

Exercise 30.1.6

Use Fermat's little theorem to find the least nonnegative residue of a modulo m for each of the following:

(a) $a = 5^{100}$, $m = 7$

Solution. By Fermat's Little Theorem, $5^6 \equiv 1 \pmod{7}$. Since $100 = 6(16) + 4$, we have

$$5^{100} = \left(5^6\right)^{16} \cdot 5^4 \equiv 1^{16} \cdot 5^4 \equiv \left(5^2\right)^2 \equiv 4^2 \equiv 2 \pmod{7}$$

(b) $a = 6^{2000}$, $m = 11$

Solution. By FLT, $6^{10} \equiv 1 \pmod{11}$. Since $2000 = 10(200)$, we have

$$6^{2000} = \left(6^{10}\right)^{200} \equiv 1^{200} \equiv 1 \pmod{11}$$

(c) $a = 3^{999999999}$, $m = 7$

Solution. By FLT, $3^6 \equiv 1 \pmod{7}$. Since $999999999 = 6(166666666) + 3$, we have

$$3^{999999999} \equiv 3^3 \equiv 6 \pmod{7}$$

(d) $a = 2^{1000009}$, $m = 17$

Solution. By FLT, $2^{16} \equiv 1 \pmod{17}$. Since $1000009 = 16(62500) + 9$, we have

$$2^{1000009} \equiv 2^9 \equiv 2 \cdot 2^4 \cdot 2^4 \equiv 2 \cdot (-1) \cdot (-1) \equiv 2 \pmod{17}$$

Exercise 30.1.7

(a) Determine the order of 4 modulo 19.

Solution. By the corollary to Fermat's little theorem, $\text{ord}_{19}(4) \mid 18$, so the possible orders are 2, 3, 6, 9, 18.

- $4^2 \equiv 16 \equiv -3 \pmod{19}$
- $4^3 \equiv 4(-3) \equiv -12 \equiv 7 \pmod{19}$
- $4^6 \equiv \left(4^3\right)^2 \equiv 49 \equiv 11 \pmod{19}$
- $4^9 \equiv 4^3 \cdot 4^6 \equiv 7 \cdot 11 \equiv 77 \equiv 1 \pmod{19}$

Therefore, $\text{ord}_{19}(4) = 9$.

(b) Use your answer from part (a) to find 4^{-1} modulo 19. Give your answer as the least nonnegative residue.

Solution. Since $4^9 \equiv 1 \pmod{19}$, we have

$$4^{-1} \equiv 4^8 \equiv \left(4^2\right)^4 \equiv (-3)^4 \equiv 9^2 \equiv 81 \equiv 5 \pmod{19}$$

(c) Solve the congruence equation:

$$4x \equiv 11 \pmod{19}$$

Give your final answer in the form $x \equiv b \pmod{19}$, where b is the least nonnegative residue.

Solution. Since $4^{-1} \equiv 5 \pmod{19}$,

$$\begin{aligned} 4x \equiv 11 \pmod{19} &\implies 5 \cdot 4x \equiv 5 \cdot 11 \pmod{19} \\ &\implies x \equiv 55 \equiv 17 \pmod{19} \end{aligned}$$

Exercise 30.1.8

Prove that if $n \in \mathbb{Z}$ is odd and $3 \nmid n$ then $n^2 \equiv 1 \pmod{24}$.

Proof. Let $n \in \mathbb{Z}$ be odd such that $3 \nmid n$.

First, since n is odd, we have that $n \equiv \pm 1$ or $\pm 3 \pmod 8$. Then

$$n^2 \equiv (\pm 1)^2 \equiv 1 \pmod 8 \quad \text{or} \quad n^2 \equiv (\pm 3)^2 \equiv 1 \pmod 8.$$

In either case, we have $n^2 \equiv 1 \pmod 8$. Hence $n^2 - 1 = 8m$ for some $m \in \mathbb{Z}$.

Furthermore, since $3 \nmid n$ and 3 is prime, we have that $\gcd(3, n) = 1$, so $n^2 \equiv 1 \pmod 3$ by Fermat's little theorem. Hence,

$$3 \mid n^2 - 1 = 8m$$

Sice $\gcd(3, 8) = 1$, we can apply Euclid's lemma to conclude that $3 \mid m$. Thus, $m = 3k$ for some $k \in \mathbb{Z}$ and we have

$$n^2 - 1 = 8(3k) = 24k \implies 24 \mid n^2 - 1$$

Therefore, $n^2 \equiv 1 \pmod{24}$, as required. □

Exercise 30.1.9

Prove that $30 \mid n^9 - n$ for all $n \in \mathbb{Z}$.

Proof. Let $n \in \mathbb{Z}$. Note that $30 = 2 \cdot 3 \cdot 5$. We will show that $n^9 \equiv n$ modulo 2, 3, and 5, in order to show that $n^9 \equiv n \pmod{30}$.

- Modulo 2: Working modulo 2, $n \equiv 0$ or $1 \pmod 2$. In either case, we have $n^k \equiv n \pmod 2$ for all $k \in \mathbb{Z}^+$. In particular, $n^9 \equiv n \pmod 2$.
- Modulo 3: By Fermat's little theorem we have that $n^3 \equiv n \pmod 3$. Then $n^9 \equiv n^3 \equiv n \pmod 3$, as desired.
- Modulo 5: Note that if $n \equiv 0 \pmod 5$ then we trivially have $n^9 \equiv n \pmod 5$. Otherwise, n and 5 are coprime and Fermat's little theorem implies that $n^4 \equiv 1 \pmod 5$. Then
$$n^9 \equiv n^4 \cdot n^4 \cdot n \equiv n \pmod 5$$

$n^9 \equiv n \pmod 2$ implies that $n^9 - n = 2k$ for some $k \in \mathbb{Z}$. Then $n^9 \equiv n \pmod 3$ implies $3 \mid 2k$ and hence $3 \mid k$ by Euclid's lemma. Therefore $k = 3m$ for some $m \in \mathbb{Z}$ and we have $n^9 - n = 6m$. Finally, $n^9 \equiv n \pmod 5$ implies $5 \mid 6m$ and hence $5 \mid m$ by Euclid's lemma. Then $m = 5n$ for some $n \in \mathbb{Z}$ and we have $n^9 - n = 30n$. Therefore, $n^9 \equiv n \pmod{30}$, as desired. □

Exercise 30.1.14

Find the value of the $\phi(n)$ for each of the following values of n.

(a) 100

Solution.

$$\phi(100) = \phi(2^2)\phi(5^2) = 2 \cdot 20 = \boxed{40}$$

(b) 256

Solution.

$$\phi(256) = \phi(2^8) = \boxed{128}$$

(c) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

Solution.

$$\phi(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) = \phi(2)\phi(3)\phi(5)\phi(7)\phi(11)\phi(13) = 1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = \boxed{5760}$$

(d) 20!

Solution. The primes which divide 20! are $2, 3, 5, 7, 11, 13, 17, 19$, so

$$\begin{aligned}\phi(20!) &= 20!\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right)\left(1-\tfrac{1}{5}\right)\left(1-\tfrac{1}{7}\right)\left(1-\tfrac{1}{11}\right)\left(1-\tfrac{1}{13}\right)\left(1-\tfrac{1}{17}\right)\left(1-\tfrac{1}{19}\right) \\ &= \boxed{416084687585280000}\end{aligned}$$

Exercise 30.1.15

Find all $n \in \mathbb{Z}^+$ such that $\phi(n) = 12$. Be sure to prove that you found all solutions.

Solution. Suppose $\phi(n) = 12$ and p is a prime that divides n. Then $p-1 \mid 12$, implying

$$p - 1 = 1,\ 2,\ 3,\ 4,\ 6,\ \text{or } 12 \implies p = 2,\ 3,\ 5,\ 7,\ \text{or } 13$$

If $p^2 \mid n$ then $p \mid 12$, so this can only happen when $p = 2$ or 3. Note that $3^3 \nmid n$ because $\phi(3^3) = 18 > 12$. Similarly, note that $2^4 \nmid n$ because $\phi(2^4) = 8 \nmid 12$.

- If $2^3 \mid n$ then $n = 8k$ for k odd. Then $12 = \phi(n) = 4\phi(k)$ implies $\phi(k) = 3$, which is impossible.
- If $3^2 \mid n$ then $n = 9k$ for some k coprime to 3. Then $12 = \phi(n) = 6\phi(k)$ implies $\phi(k) = 2$ and hence $k = 4$ (since $k \neq 3$). Therefore, $n = 36$.
- If $5 \mid n$ then $n = 5k$ for some k coprime to 5. Then $12 = \phi(n) = 4\phi(k)$ implies $\phi(k) = 3$, which is impossible.

So, either $n = 36$ or n is of the form

$$n = 2^a 3^b 7^c 13^d \text{ for } a \in \{0, 1, 2\},\ b, c, d \in \{0, 1\}$$

- If $a = 2$ then $n = 4k$ for some odd k. Then $12 = \phi(n) = 2\phi(k)$ implies $\phi(k) = 6$. From the options available, this can only occur when $k = 7$. Hence $n = 28$.
- If $a = 0$ or 1 then $12 = \phi(n) = \phi(k)$. This can occur if either $k = 13$ or $k = 3 \cdot 7$. Since $a = 0$ or 1, we have $n = 13, 26, 21,$ or 42.

Possible values of n: $\boxed{13,\ 21,\ 26,\ 28,\ 36,\ \text{and } 42}$.

Exercise 30.1.16

Show that there is no positive integer n such that $\phi(n) = 14$.

Proof. Assume for the sake of contradiction that there exists $n \in \mathbb{Z}^+$ such that $\phi(n) = 14$. If prime $p \mid n$ then $p - 1 \mid 14$, implying $p - 1 = 1, 2, 7,$ or 14. This can only occur if $p = 2$ or 3. Note that $3^2 \nmid n$ because $3 \nmid 14$. Hence, $n = 2^a 3^b$ for $b \in \{0, 1\}$. However, this implies

$$\phi(n) = \begin{cases} 2^{a-1} & \text{if } b = 0 \\ 2^a & \text{if } b = 1 \end{cases}$$

In either case, $\phi(n) \neq 14$, contradicting our assumption. □

29. November 12

Exercise 31.1.4

(a) Calculate $\phi(14)$ and list all elements in $[14]$ which are coprime to 14.

Solution.

- $\phi(14) = \phi(2)\phi(7) = \boxed{6}$
- Reduced residue system modulo 14:

$$\{1, 3, 5, 9, 11, 13\}$$

(b) Determine the multiplicative inverse of each integer from part (a).

Solution.

- $1^{-1} \equiv 1 \pmod{14}$
- $3^{-1} \equiv 5 \pmod{14}$
- $5^{-1} \equiv 3 \pmod{14}$
- $9^{-1} \equiv 11 \pmod{14}$
- $11^{-1} \equiv 9 \pmod{14}$
- $13^{-1} \equiv 13 \pmod{14}$

(c) Find the least nonnegative residue of 9^{999999} modulo 14.

Solution. By Euler's theorem, we have $9^6 \equiv 1 \pmod{14}$. Since $999999 = 6(166666) + 3$, Euler's theorem implies

$$9^{999999} \equiv 9^3 \equiv (-5)^2 \cdot 9 \equiv 11 \cdot 9 \equiv (-3)(-5) \equiv 1 \pmod{14}$$

Exercise 31.1.5

(a) Calculate $\phi(35)$ and list all elements in $[35]$ which are coprime to 35.

Solution.

- $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = \boxed{24}$
- $\boxed{\{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \pm 11, \pm 12, \pm 13, \pm 16, \pm 17\}}$

(b) Determine $\mathrm{ord}_{35}(3)$, the order of 3 modulo 35.

Solution. The possible orders are the divisors of 24.

- $3^2 \equiv 9 \pmod{35}$
- $3^3 \equiv 27 \equiv -8 \pmod{35}$
- $3^4 \equiv -24 \equiv 11 \pmod{35}$
- $3^6 \equiv 9 \cdot 11 \equiv 29 \equiv -6 \pmod{35}$
- $3^{12} \equiv (-6)^2 \equiv 1 \pmod{35}$

Therefore, $\boxed{\mathrm{ord}_{35}(3) = 12}$.

(c) Find the least nonnegative residue of 3^{-1} modulo 35.

Solution. From above, we know that $3^{-1} \equiv 3^{11} \pmod{35}$.

$$3^{11} = 3 \cdot 3^4 \cdot 3^6 \equiv 3 \cdot 11 \cdot (-6) \equiv (-2) \cdot (-6) \equiv 12 \pmod{35}$$

Therefore, $\boxed{3^{-1} \equiv 12 \pmod{35}}$.

Alternatively, we may simply observe that $3 \cdot 12 = 36 \equiv 1 \pmod{35}$.

(d) Find the least nonnegative residue of 3^{100000} modulo 35.

Solution. Since $\mathrm{ord}_{35}(3) = 12$ and $100000 = 12(8333) + 4$, we have

$$3^{100000} \equiv 3^4 \equiv \boxed{11} \pmod{35}$$

Exercise 31.1.6

(a) Calculate $\phi(50)$

Solution. $\phi(50) = \phi(2)\phi(5^2) = 1 \cdot 20 = \boxed{20}$.

(b) Determine $\text{ord}_{50}(7)$.

Solution. The possible orders of 7 are the divisors of 20.

- $7^2 \equiv 49 \equiv -1 \pmod{50}$
- $7^4 \equiv \left(7^2\right)^2 \equiv (-1)^2 \equiv 1 \pmod{50}$

Therefore, $\boxed{\text{ord}_{50}(7) = 4}$.

(c) Find the least nonnegative residue of 7^{-1} modulo 50.

Solution. Since $7 \cdot 7 \equiv -1 \pmod{50}$, we have $7 \cdot (-7) \equiv 1 \pmod{50}$. Therefore, $\boxed{7^{-1} \equiv 43 \pmod{50}}$.

(d) Find all integer solutions to the congruence $7x + 27 \equiv 4 \pmod{50}$.

Solution.

$$\begin{aligned} 7x + 27 \equiv 4 \pmod{50} &\iff 7x \equiv -23 \pmod{50} \\ &\iff x \equiv (-7)(-23) \equiv 11 \pmod{50} \end{aligned}$$

Solution set: $\boxed{\{x \in \mathbb{Z} \mid x \equiv 11 \pmod{50}\}}$.

Exercise 31.1.7

Let $m \in \mathbb{Z}$ with $m > 2$, and let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. Prove that $\sum_{i=1}^{\phi(m)} r_i \equiv 0 \pmod{m}$.

Proof. Since $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ is a reduced residue system modulo m, we have $\gcd(r_i, m) = 1$ for all i. Note that for each i, $\gcd(-r_i, m) = \gcd(r_i, m) = 1$. Then $-r_i = r_j$ for some $j \in \{1, 2, \ldots, \phi(m)\}$.

Now, suppose for contradiction that $r_i \equiv -r_i \pmod{m}$. Then $2r_i \equiv 0 \pmod{m}$, so $m \mid 2r_i$. Since $\gcd(r_i, m) = 1$, Euclid's lemma implies $m \mid 2$. But this contradicts our assumption that $m > 2$. Therefore, $r_i \not\equiv -r_i \pmod{m}$.

Thus, the elements of the reduced residue system can be partitioned into $\phi(m)/2$ disjoint pairs of the form $\{r_i, -r_i\}$, where each pair sums to 0 modulo m. (Note that $\phi(m)$ is even for $m > 2$, which ensures the pairing is possible.)

Hence, $\sum_{i=1}^{\phi(m)} r_i \equiv 0 \pmod{m}$. □

Exercise 31.1.8

Use Euler's theorem to prove that $51 \mid \left(10^{32n+9} - 7\right)$ for all $n \in \mathbb{N}$.

Proof. Note that $\phi(51) = \phi(3)\phi(17) = 32$, so $10^{32} \equiv 1 \pmod{51}$. Thus

$$10^{32n+9} \equiv 10^9 \equiv (-2)^4 \cdot 10 \equiv 160 \equiv 7 \pmod{51}$$

Therefore, $51 \mid 10^{32n+9} - 7$. □

Exercise 31.1.9

Find all solutions, if any, to the following congruence equations.

(a) $3x \equiv 5 \pmod{7}$

Solution. $\boxed{x \equiv 4 \pmod{7}}$

(b) $100x - 2 \equiv 24 \pmod{12}$

Solution. $\boxed{\text{No Solutions}}$.

(c) $15x \equiv 7 \pmod{32}$

Solution. $\boxed{x \equiv 9 \pmod{32}}$

(d) $22x \equiv 3 \pmod{40}$

Solution. $\boxed{\text{No Solutions}}$.

(e) $39x \equiv 52 \pmod{130}$

Solution. $\boxed{x \equiv 8 \pmod{10}}$

(f) $80x \equiv 51 \pmod{171}$

Solution. $\boxed{x \equiv 84 \pmod{171}}$

Exercise 31.1.10

Find the least nonnegative residue of each of the following

(a) 100 modulo 13

Solution.

$$100 = 13(7) + 9 \implies 100 \equiv \boxed{9} \pmod{13}$$

(b) 99 modulo 28

Solution.

$$99 = 28(3) + 15 \implies 99 \equiv \boxed{15} \pmod{28}$$

(c) 103^{2025} modulo 48

Solution.

$$103^{2025} \equiv 7^{2025} \equiv \left(7^2\right)^{1012} \cdot 7 \equiv 1^{1012} \cdot 7 \equiv \boxed{7} \pmod{48}$$

(d) 3^{341} modulo 124

Solution. Since $\phi(124) = \phi(2^2)\phi(31) = 60$, Euler's theorem implies

$$3^{341} = \left(3^{60}\right)^5 \cdot 3^{41} \equiv 3^{41} \pmod{124}$$

Next, note $3^{41} = 3^{32} \cdot 3^8 \cdot 3$. By successively squaring, we have

- $3^2 \equiv 9 \pmod{124}$
- $3^4 \equiv 81 \equiv -43 \pmod{124}$
- $3^8 \equiv (-43)^2 \equiv 1849 \equiv 113 \equiv -11 \pmod{124}$
- $3^{16} \equiv (-11)^2 \equiv 121 \equiv -3 \pmod{124}$
- $3^{32} \equiv (-3)^2 \equiv 9 \pmod{124}$

Therefore,

$$3^{41} \equiv 3 \cdot (-11) \cdot 9 \equiv -99 \cdot 3 \equiv 25 \cdot 3 \equiv \boxed{75} \pmod{124}$$

(e) $\displaystyle\sum_{k=1}^{100} k!$ modulo 7

Solution.

$$\begin{aligned}\sum_{k=1}^{100} k! &\equiv 1!+2!+3!+4!+5!+6! \pmod 7\\ &\equiv 1+2+(-1)+3+1+(-1) \pmod 7\\ &\equiv \boxed{5} \pmod 7\end{aligned}$$

(f) $\sum_{k=1}^{100} k!$ modulo 12

Solution.

$$\sum_{k=1}^{100} k! \equiv 1!+2!+3! \equiv \boxed{9} \pmod{12}$$

Exercise 31.1.15

For each part below, find all solutions to the given system of congruences.

(a)
$$\begin{aligned}x &\equiv 5 \pmod 7\\ x &\equiv 3 \pmod 8\\ x &\equiv 1 \pmod 9\end{aligned}$$

Solution. First note that 7, 8, and 9 are pairwise relatively prime, so the Chinese remainder theorem states that there is a unique solution modulo $7 \cdot 8 \cdot 9 = 504$. We proceed to find the solution below.

$$\begin{aligned}x \equiv 1 \pmod 9 &\implies \exists k \in \mathbb{Z}, x = 9k+1\\ x \equiv 3 \pmod 8 &\implies 9k+1 \equiv 3 \pmod 8\\ &\implies k \equiv 2 \pmod 8\\ &\implies \exists \ell \in \mathbb{Z}, k = 8\ell+2\\ &\implies x = 9(8\ell+2)+1 = 72\ell+19\end{aligned}$$

$$\begin{aligned}x \equiv 5 \pmod 7 &\implies 72\ell+19 \equiv 5 \pmod 7\\ &\implies 2\ell \equiv 0 \pmod 7\\ &\implies \ell \equiv 0 \pmod 7\\ &\implies \exists m \in \mathbb{Z}, \ell = 7m\\ &\implies x = 72(7m)+19 = 504m+19\end{aligned}$$

Thus, $x = 19$ is one solution to the system of congruences, and $\boxed{[19]_{504}}$ is the set of all solutions to the congruence.

(b)
$$\begin{aligned} 2x &\equiv 1 \pmod{23} \\ 9x &\equiv 12 \pmod{31} \end{aligned}$$

Solution. First observe that $2^{-1} \equiv 12 \pmod{23}$ and $9^{-1} \equiv 7 \pmod{31}$. Our system of congruences can then be rewritten as follows.

$$\begin{aligned} x &\equiv 12 \cdot 11 \equiv 17 \pmod{23} \\ x &\equiv 7 \cdot 12 \equiv 22 \pmod{31} \end{aligned}$$

Since $\gcd(23, 31) = 1$ the Chinese remainder theorem implies that there is a unique solution modulo $23 * 31 = 713$. Let $x \in \mathbb{Z}$ be such a solution. Since $x \equiv 22 \pmod{31}$ we know that $x = 31k + 22$ for some $k \in \mathbb{Z}$. We then plug this into the other congruence and solve for k using the fact that $8^{-1} \equiv 3 \pmod{23}$.

$$\begin{aligned} x \equiv 17 \pmod{23} &\Rightarrow 31k + 22 \equiv 17 \pmod{23} \\ &\Rightarrow 8k - 1 \equiv 17 \pmod{23} \\ &\Rightarrow 8k \equiv 18 \pmod{23} \\ &\Rightarrow k \equiv 3 \cdot 18 \equiv 8 \pmod{23} \end{aligned}$$

We then have that $k = 23\ell + 8$ for some $\ell \in \mathbb{Z}$. Plugging this into our equation for x we have

$$x = 31(23\ell + 8) + 22 = 713\ell + 270$$

Since $x \equiv 270 \pmod{713}$, the Chinese remainder theorem implies that the solution set is precisely the congruence class $\boxed{[270]_{713}}$.

(c)
$$\begin{aligned} 3x + 1 &\equiv 2 \pmod{11} \\ x &\equiv 3 \pmod{17} \\ 5x &\equiv 12 \pmod{18} \end{aligned}$$

Solution. First note that 11, 17, and 18 are pairwise relatively prime, so the Chinese remainder theorem states that there is a unique solution modulo $11 \cdot 17 \cdot 18 = 3366$. We proceed to find the solution below.

$$
\begin{aligned}
5x \equiv 12 \pmod{18} &\Rightarrow 11 \cdot 5x \equiv 11 \cdot 12 \pmod{18} \\
&\Rightarrow x \equiv 6 \pmod{18} \\
&\Rightarrow x = 18k + 6 \text{ for some } k \in \mathbb{Z} \\
x \equiv 3 \pmod{17} &\Rightarrow 18k + 6 \equiv 3 \pmod{17} \\
&\Rightarrow k \equiv -3 \equiv 14 \pmod{17} \\
&\Rightarrow k = 17\ell + 14 \text{ for some } \ell \in \mathbb{Z} \\
&\Rightarrow x = 18(17\ell + 14) + 6 = 306\ell + 258 \\
3x + 1 \equiv 2 \pmod{11} &\Rightarrow 3x \equiv 1 \pmod{11} \\
&\Rightarrow x \equiv 4 \pmod{11} \\
&\Rightarrow 306\ell + 258 \equiv 4 \pmod{11} \\
&\Rightarrow 9\ell + 5 \equiv 4 \pmod{11} \\
&\Rightarrow 9\ell \equiv -1 \pmod{11} \\
&\Rightarrow \ell \equiv -5 \equiv 6 \pmod{11} \\
&\Rightarrow \ell = 11m + 6 \text{ for some } m \in \mathbb{Z} \\
&\Rightarrow x = 306(11m + 6) + 258 = 3366m + 2094
\end{aligned}
$$

Thus $x = 2094$ is a solution to the system of linear congruences and the congruence class $\boxed{[2094]_{3366}}$ is the set of all solutions to the system of linear congruences.

Exercise 31.1.16

Three roommates Adam, Bill, and Carol eat pizza on a regular basis. Adam eats pizza once every 3 days, Bill eats pizza once every 5 days, and Carol eats pizza once every 7 days. In 2025, Adam ate pizza on January 1, Bill ate pizza on January 2, and Carol ate pizza on January 3. What was the first date in 2025 that they all ate pizza on the same day?

Solution. Let x be the number of days since January 1, 2025 until the roommates eat pizza together. Then we have the following system of linear congruences

$$
\begin{aligned}
x &\equiv 0 \pmod{3} \\
x - 1 &\equiv 0 \pmod{5} \\
x - 2 &\equiv 0 \pmod{7}
\end{aligned}
$$

Since 3, 5, and 7 are pairwise relatively prime, the Chinese remainder theorem implies

that there exists a unique solution modulo 105.

$$\begin{aligned}
x-2 \equiv 0 \pmod 7 &\Rightarrow x = 7k+2 \text{ for some } k \in \mathbb{Z} \\
x-1 \equiv 0 \pmod 5 &\Rightarrow 7k+1 \equiv 0 \pmod 5 \\
&\Rightarrow 2k \equiv 4 \pmod 5 \\
&\Rightarrow k \equiv 2 \pmod 5 \\
&\Rightarrow k = 5\ell + 2 \text{ for some } \ell \in \mathbb{Z} \\
&\Rightarrow x = 7(5\ell+2)+2 \\
&\Rightarrow x = 35\ell + 16 \\
x \equiv 0 \pmod 3 &\Rightarrow 35\ell + 16 \equiv 0 \pmod 3 \\
&\Rightarrow 2\ell \equiv 2 \pmod 3 \\
&\Rightarrow \ell \equiv 1 \pmod 3 \\
&\Rightarrow \ell = 3m+1 \text{ for some } m \in \mathbb{Z} \\
&\Rightarrow x = 35(3m+1)+16 \\
&\Rightarrow x = 105m + 51
\end{aligned}$$

Therefore, 51 days from January 1, 2025 the three roommates will eat pizza together. This date is $\boxed{\text{February 21, 2025}}$.

Exercise 31.1.19

Use modular arithmetic to find all solutions to the following linear Diophantiune equations.

(a) $15x + 24y = 57$

Solution. For $y \in \mathbb{Z}$,

$$\begin{aligned}
\exists x \in \mathbb{Z}, 15x + 24y = 57 &\iff 24y \equiv 57 \pmod{15} \\
&\iff 9y \equiv 12 \pmod{15} \\
&\iff 3y \equiv 4 \pmod 5 \quad \text{by Cancellation Law} \\
&\iff y \equiv 3 \pmod 5 \\
&\iff \exists k \in \mathbb{Z}, y = 3 + 5k
\end{aligned}$$

Let $k \in \mathbb{Z}$ and $y = 3 + 5k$. Then

$$15x + 24(3+5k) = 57 \iff 15x = -15 - 120k \iff x = -1 - 8k$$

Therefore, the solution set is $\boxed{\{(-1-8k, 3+5k) \mid k \in \mathbb{Z}\}}$.

(b) $63x + 17y = 5$

Solution. For $x \in \mathbb{Z}$,

$$\begin{aligned} \exists y \in \mathbb{Z}, 63x + 17y = 5 &\iff 63x \equiv 5 \pmod{17} \\ &\iff -5x \equiv 5 \pmod{17} \\ &\iff x \equiv -1 \pmod{17} \quad \text{by Cancellation Law} \\ &\iff \exists k \in \mathbb{Z}, x = -1 + 17k \end{aligned}$$

Let $k \in \mathbb{Z}$ and $x = -1 + 17k$. Then

$$63(-1 + 17k) + 17y = 5 \iff 17y = 68 - 63 \cdot 17k \iff y = 4 - 63k$$

Therefore, the solution set is $\boxed{\{(-1 + 17k, 4 - 63k) \mid k \in \mathbb{Z}\}}$.

30. November 14

Exercise 32.2.3

Let A be a finite subset and $A_1 \subseteq A$. Use the Rule of Sum to prove that $|A \setminus A_1| = |A| - |A_1|$.

Proof. Note that $A = A_1 \cup (A \setminus A_1)$ and $A_1 \cap (A \setminus A_1) = \varnothing$, so $\{A_1, A \setminus A_1\}$ is a partition of A. Then the Rule of Sum implies

$$|A| = |A_1| + |A \setminus A_1|.$$

Rearranging this equation yields the desired result:

$$|A \setminus A_1| = |A| - |A_1|$$

□

Exercise 32.2.11

A student is choosing a two-course meal from a menu that has 4 appetizers, 6 main courses, and 3 desserts. How many meals are possible if the student can choose to have:

(a) An appetizer and a main course?

Solution. $\boxed{24}$ (Rule of Product)

(b) A main course and a dessert?

Solution. $\boxed{18}$ (Rule of Product)

(c) An appetizer and a dessert?

Solution. $\boxed{12}$ (Rule of Product)

(d) Any two distinct courses? (Meaning: an appetizer and a main, OR a main and a dessert, OR an appetizer and a dessert).

Solution. $24 + 18 + 12 = \boxed{54}$ (Rule of Sum)

Exercise 32.2.12

A car model comes in 4 colors, with 3 interior options, and 2 transmission types. Additionally, there is an optional sunroof that can be added only if the car is either red or blue. How many distinct car configurations are possible?

Solution. We partition the possible car configurations based on whether the color is red/blue or something else.

- Case 1: The color is red or blue. Then there are 2 choices for the color, 3 choices for the interior, 2 choices of transmission, and 2 choices for the sunroom (yes/no). Therefore, by the Rule of Product, there are

$$2 \cdot 3 \cdot 2 \cdot 2 = 24$$

possible configurations that are either red or blue.

- Case 2: The color is not red or blue. Then there are 2 choices for the color, 3 choices for the interior, 2 choices for transmission, and 1 choice for sunroom (not allowed). Therefore, by the Rule of Product, there are

$$2 \cdot 3 \cdot 2 \cdot 1 = 12$$

possible configurations that are neither red nor blue.

Then, by the Rule of Sum, there are $24 + 12 = \boxed{36}$ possible car configurations.

Exercise 32.2.13

How many even 4-digit numbers are there with distinct digits?

Solution. Note that any even integer must have its last digit in $\{0, 2, 4, 6, 8\}$. Since a 4-digit number cannot begin with 0, our counting argument will differ depending on whether the last digit is 0 or not. We partition the set of even 4-digit numbers with all distinct digits into two disjoint cases:

- Case 1: The last digit is 0. Each such number can be constructed uniquely through the following multi-step process:
  - Choose the units digit: 1 way (it must be 0).
  - Choose the thousands digit: 9 choices (any of $1, 2, 3, 4, 5, 6, 7, 8, 9$).
  - Choose the hundreds digit distinct from the previous ones: 8 choices.
  - Choose the tens digit distinct from the previous ones: 7 choices.

  By the Rule of Product, there are $1 \cdot 9 \cdot 8 \cdot 7 = 504$ such numbers.
- Case 2: The last digit is not 0. Each such number can be constructed uniquely as follows:
  - Choose the units digit: 4 choices $(2, 4, 6, 8)$.
  - Choose the thousands digit: 8 choices (any digit except 0 and the chosen units digit).
  - Choose the hundreds digit distinct from the previous ones: 8 choices.
  - Choose the tens digit distinct from the previous ones: 7 choices.

  By the Rule of Product, there are $4 \cdot 8 \cdot 8 \cdot 7 = 1792$ such numbers.

By the Rule of Sum, the total number of even 4-digit numbers with all distinct digits is $504 + 1792 = \boxed{2296}$.

Exercise 32.2.14

In how many ways can 5 people sit around a circular table? (Two arrangements are considered the same if one can be rotated to obtain the other).

Solution. If the seats were arranged in a straight line, there would be

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

ways to seat the 5 people, by the Rule of Product.

However, when the seats are arranged in a circle, any rotation of a given seating results in the same circular arrangement. Because each circular arrangement can be rotated into 5 equivalent linear arrangements (one for each possible choice of who sits in the first seat), every distinct circular seating has been counted 5 times above.

Therefore, by the Rule of Division, the number of distinct circular arrangements is $\frac{5!}{5} = \boxed{24}$.

Exercise 32.2.15

How many binary strings of length 8 start with `1` or end with `00`?

Solution. Let us count the complement - the number of binary strings of length 8 that *do not* start with `1` and *do not* end with `00`. Each such string can be constructed uniquely as follows:

- The first bit must be `0`. This can be chosen in 1 way.
- The next five bits (positions 2 through 6) can each be either `0` or `1`, giving 2^5 possible combinations.
- The final two bits must form one of the patterns `01`, `10`, or `11`. Hence, there are 3 possible choices for the last two bits.

By the Rule of Product, the number of binary strings that neither start with `1` nor end with `00` is $1 \cdot 2^5 \cdot 3 = 96$.

Since there are $2^8 = 256$ binary strings of length 8 in total, it follows from the Rule of Difference that the number of binary strings that start with `1` or end with `00` is $2^8 - 96 = \boxed{160}$.

Exercise 32.2.20

A drawer contains 10 black socks and 10 white socks. What is the minimum number of socks you must take out (without looking) to guarantee a pair of the same color?

Solution. It is possible to select one sock of each color, so the answer must be more than 2. Since there are only 2 colors (2 pigeonholes), if you take 3 socks (3 pigeons) at least 2 must be the same color by the pigeonhole principle. Therefore, $\boxed{3}$ is the minimum number of socks you must take to *guarantee* that you've selected a matching pair.

Exercise 32.2.21

Prove that among any 6 integers, there are two whose difference is divisible by 5.

Proof. There are 5 distinct congruence classes modulo 5. With 6 integers, the pigeonhole principle guarantees that at least 2 of them, say a and b, must lie in the same congruence class. Therefore, $a \equiv b \pmod 5$ and hence $5 \mid a - b$. □

Exercise 32.2.22

How many distinct numbers must be chosen from the set [30] to ensure that at least one pair sums to 31?

Solution. $\boxed{16}$. Partition the set into 15 pairs that sum to 31:

$$\{1, 30\}, \{2, 29\}, \ldots, \{15, 16\}$$

If you choose 16 different numbers from [30], the pigeonhole principle guarantees that you must have chosen both numbers from at least one pair. Moreover, if we select one element from each of the 15 pairs above, we will have selected 15 different numbers with no pair that sums to 31, so 16 is the optimal number.

Exercise 32.2.23

Given 5 points placed on a line segment of length 1, prove that two of them are within distance $\frac{1}{4}$ of each other.

Proof. Divide the line segment into 4 intervals, each of length $\frac{1}{4}$. Given 5 points on this line segment, the pigeonhole principle guarantees that 2 lie within in the same interval. Hence, the distance between them is at most $\frac{1}{4}$. □

Exercise 32.2.24

Suppose there are 5 teaching track professors in the math department. Each year, 2 are chosen to teach Concepts of Mathematics. How many years can the department go without repeating the same selection of 2 professors? Prove this is optimal by exhibiting such a sequence of that length, as well as invoking the Pigeonhole Principle to show that any longer sequence necessarily uses a pairing more than once.

Proof. There are $\frac{5 \cdot 4}{2} = 10$ possible pairings of math professors, so the maximum number of years they can go without repeat is $\boxed{10}$. A sequence of 10 is possible, as illustrated below:

$$\{x_1, x_2\}, \{x_1, x_3\}, \{x_1, x_4\}, \{x_1, x_5\}, \{x_2, x_3\}, \{x_2, x_4\}, \{x_2, x_5\}, \{x_3, x_4\}, \{x_3, x_5\}, \{x_4, x_5\}$$

but any sequence of 11 must include a repeat, due to the pigeonhole principle. □

Exercise 32.2.25

Let $n \in \mathbb{Z}^+$ and $A \in \mathcal{P}(\mathbb{Z})$ with $|A| = n$. Prove that there exists a nonempty $X \in \mathcal{P}(A)$ such that

$$\sum_{x \in X} x \equiv 0 \pmod{n}$$

Proof. Enumerate A by $A = \{a_1, a_2, \ldots, a_n\}$. Define the sequence of integers b_i for $i \in \{0\} \cup [n]$ recursively as

$$\begin{aligned} b_0 &= 0 \\ b_k &= b_{k-1} + a_k \quad (\text{for } k \in [n]) \end{aligned}$$

There are $(n+1)$-many b_i's. Of the $(n+1)$-many b_i's, at least 2 must lie in the same congruence class modulo n by the pigeonhole principle. Let $i, j \in \{0\} \cup [n]$ such that $i > j$ and $b_i \equiv b_j \pmod{n}$ (such an i and j exist by the previous line). Then $n \mid b_i - b_j$ by definition of congruence modulo n. Hence

$$n \mid a_{j+1} + a_{j+2} + \cdots + a_i$$

And thus for $X = \{a_k \mid j < k \leq i\}$ we have $n \mid \sum_{x \in X} x$, as desired. □

Exercise 32.2.26

Show that among any 13 real numbers, there are two numbers whose difference is within $\frac{1}{12}$ of an integer.

Proof. Partition the interval $[0, 1)$ into 12 equal subintervals:

$$\left[0, \frac{1}{12}\right), \left[\frac{1}{12}, \frac{1}{6}\right), \ldots, \left[\frac{11}{12}, 1\right).$$

Let $x_1, x_2, \ldots, x_{13} \in \mathbb{R}$, and for each i define the fractional part

$$\text{Frac}(x_i) := x_i - \lfloor x_i \rfloor \in [0, 1).$$

Since there are 13 numbers but only 12 subintervals, the pigeonhole principle guarantees that there exist $i \neq j$ such that $\text{Frac}(x_i)$ and $\text{Frac}(x_j)$ lie in the same subinterval. Without loss of generality, assume $\text{Frac}(x_i) \geq \text{Frac}(x_j)$. Then

$$0 \leq \text{Frac}(x_i) - \text{Frac}(x_j) < \frac{1}{12}.$$

Observe that

$$x_i - x_j = (\lfloor x_i \rfloor - \lfloor x_j \rfloor) + (\text{Frac}(x_i) - \text{Frac}(x_j)).$$

It follows that

$$0 \leq (x_i - x_j) - (\lfloor x_i \rfloor - \lfloor x_j \rfloor) < \frac{1}{12},$$

which is equivalent to

$$\lfloor x_i \rfloor - \lfloor x_j \rfloor \leq x_i - x_j < \lfloor x_i \rfloor - \lfloor x_j \rfloor + \frac{1}{12}.$$

Since $\lfloor x_i \rfloor - \lfloor x_j \rfloor \in \mathbb{Z}$, this shows that the difference $x_i - x_j$ is within $\frac{1}{12}$ of an integer. □

Exercise 32.2.27

Let $S = [2n]$ for some $n \in \mathbb{Z}^+$, and let $T \in \mathcal{P}(S)$ such that $|T| = n + 1$. Prove that there must exist $x, y \in T$ such that x and y are coprime.

Proof. Let $S = [2n] = \{1, 2, \ldots, 2n\}$ and let $T \subseteq S$ with $|T| = n + 1$. Partition S into n subsets of size 2 as follows:

$$\{1, 2\},\ \{3, 4\},\ \ldots,\ \{2n - 1, 2n\}.$$

Since T has $n + 1$ elements but there are only n subsets in the partition, the pigeonhole principle guarantees that there exists at least one subset in the partition containing at least two distinct elements of T. Let x and y be two such elements in the same subset. Then there exists $k \in [n]$ such that $\{x, y\} \subseteq \{2k - 1, 2k\}$. Since $x \neq y$, without loss of generality, we may assume $x = 2k - 1$ and $y = 2k$. Since consecutive integers are always coprime, we conclude that x and y are coprime. □

31. November 17

Exercise 33.2.13

(a) In how many ways can you arrange 7 distinct books on a bookshelf?

Solution. $\boxed{7!}$

(b) A pizza place offers 12 distinct toppings. How many pizzas are possible with 3 distinct toppings?

Solution. $\boxed{\binom{12}{3}}$

(c) A class has 20 students. How many ways are there to choose a committee of 4 students?

Solution. $\boxed{\binom{20}{4}}$

(d) 8 runners compete in a race. In how many different orders can the first, second, and third place finishers be decided?

Solution. $\boxed{8 \cdot 7 \cdot 6 = 336}$

(e) How many different 5-digit binary sequences are there?

Solution. $\boxed{2^5 = 32}$

(f) How many anagrams of the word `ORANGE` are there?
As mathematicians, we consider an anagram to be any rearrangement of the letters, even if it doesn't make an actual word.

Solution. $\boxed{6!}$ because all of the letters are distinct.

Exercise 33.2.12

(a) How many ways can 4 boys and 3 girls stand in a line if the girls must stand together?

Solution. First, treat the girls as a single block. Then we have 4 boys + 1 block, which can be arranged in 5! ways. Within the block, the girls can be arranged in 3! ways. Therefore, by the Rule of Product, the boys and girls can be arranged in $\boxed{5! \cdot 3!}$ ways.

(b) From a club of 8 men and 7 women, how many ways are there to form a committee of 5 people if the committee must have at least 2 women?

Solution. There are $\binom{15}{5}$ total ways to form a committee of 5 from the 15 people. There are $\binom{8}{5}$ ways to do this if there are 0 women (choose 5 men out of 8), and there are $\binom{7}{1}\binom{8}{4}$ ways to do this if there is exactly 1 woman on the committee (choose 1 woman out of 7, choose 4 men out of 8). Therefore, by the Rule of Difference, there are $\boxed{\binom{15}{5} - \binom{8}{5} - 7\binom{8}{4}}$ ways to form a committee with at least 2 women.

(c) How many triangles can be formed by connecting vertices of a regular octagon?

Solution. A triangle is formed by choosing any 3 of the 8 vertices. This can be done in $\boxed{\binom{8}{3}}$ ways.

(d) A password must be 6 characters long. The first 3 characters must be distinct letters from the English alphabet (not case sensitive), and the last 3 characters

must be distinct digits from 0-9. How many such passwords are possible?

Solution. We have a 6-step procedure for constructing such a password. First, select the 3 distinct letters at the beginning of the password, and then select the 3 distinct digits at the end of the password. By the rule of product, this can be done in $\boxed{26 \cdot 25 \cdot 24 \cdot 10 \cdot 9 \cdot 8}$ different ways.

(e) How many (distinct) anagrams of the word `BANANA` are there?

Solution. Rule of Product Procedure:

- Choose 3 of the 6 positions to be an `A`: $\binom{6}{3}$ options.
- From remaining 3 positions, choose 2 to be a `N`: $\binom{3}{2}$ options
- Place the `B` in the remaining position: 1 option.

By the Rule of Product, there are $\boxed{\binom{6}{3}\binom{3}{2}}$ anagrams of `BANANA`.

(f) A company has 10 engineers and 7 salespeople. How many ways can a team of 5 be selected to go to a conference if the team must have at least one engineer and at least one salesperson?

Solution. There are 17 total people. The total number of teams of 5 that can be formed without restriction is $\binom{17}{5}$. There are $\binom{7}{5}$ teams with no engineers and $\binom{10}{5}$ teams with no salespeople. Therefore, there are

$$\boxed{\binom{17}{5} - \binom{7}{5} - \binom{10}{5}} \text{ valid teams.}$$

Exercise 33.2.13

(a) Given $(a, b) \in \mathbb{N}^2$, how many distinct lattice paths are there to (a, b)?

Solution. Each path from $(0, 0)$ to (a, b) consists of exactly a right moves and b up moves, in some order. The number of such paths is the number of ways to choose a positions for the right moves from a total of $a + b$ moves. Thus there are $\boxed{\binom{a+b}{a}}$ lattice paths to (a, b).

(b) Let $n \in \mathbb{N}$. How many lattice paths from $(0, 0)$ to $(2n, 2n)$ pass through the point (n, n)?

Solution. Any such path can be split into two independent segments:

- From $(0, 0)$ to (n, n): $\binom{2n}{n}$ paths

- From (n, n) to $(2n, 2n)$: $\binom{2n}{n}$ paths

By the Rule of Product, the total number is $\boxed{\binom{2n}{n}^2}$.

Exercise 33.2.14

From a group of 7 mathematicians and 4 physicists, how many ways are there to form a committee of 5 that has more mathematicians than physicists and has a designated chairperson who must be a mathematician?

Solution. Any such committee with more mathematicians than physicists must consist of at least 3 mathematicians. We partition based on the number of mathematicians in the committee.

- 5 Mathematicians, 0 Physicists:
  - Choose 5 mathematicians from 7: $\binom{7}{5}$ options.
  - Choose a chairperson from these 5 mathematicians: 5 options.

  By the Rule of product, there are $5\binom{7}{5}$ such committees.
- 4 Mathematicians, 1 Physicist:
  - Choose 4 mathematicians from 7: $\binom{7}{4}$ options.
  - Choose 1 physicist from 4: $\binom{4}{1} = 4$ options.
  - Choose a chairperson from the 4 mathematicians: 4 options.

  By the Rule of product, there are $16\binom{7}{4}$ such committees.
- 3 Mathematicians, 2 Physicists:
  - Choose 3 mathematicians from 7: $\binom{7}{3}$ options.
  - Choose 2 physicists from 4: $\binom{4}{2}$ options.
  - Choose a chairperson from the 3 mathematicians: 3 options.

  By the Rule of product, there are $3\binom{7}{3}\binom{4}{2}$ such committees.

Finally, we apply the Rule of Sum to determine the desired number of committees.

$$\boxed{5\binom{7}{5} + 16\binom{7}{4} + 3\binom{7}{3}\binom{4}{2}}$$

Exercise 33.2.15

In how many ways can 5 married couples be seated around a circular table if each couple must sit together?

Solution. We first treat each couple as a block, and then determine the arrangement within the couple.

- Treat each couple as a block and determine an arrangement of the 5 blocks around the circular table. Since any rotation of an arrangement around a circular table is considered the same, there are $\frac{5!}{5} = 4! = 24$ options.
- Within each block, determine the order of the 2 people. For each couple, there are 2 arrangements, giving $2^5 = 32$ options for couple arrangements within the blocks.

By the rule of product, there are $24 \cdot 32 = \boxed{768}$ such arrangements.

32. November 21

Exercise 34.1.3

A *Three-of-a-Kind* is a 5-card hand that contains 3 cards of one rank, with the remaining 2 cards each of different ranks, distinct from the three-of-a-kind and from each other (that is, not a Full House and not a Four-of-a-Kind). How many distinct Three-of-a-Kind hands are possible?

Solution. We uniquely construct an arbitrary 3-of-a-kind hand via the following multi-step procedure.

- Choose the 3 ranks to appear in the hand. There are $\binom{13}{3}$ choices.
- Choose one of the 3 ranks to form the 3-of-a-kind. There are $\binom{3}{1}$ choices.
- Choose 3 suits for the 3-of-a-kind. There are $\binom{4}{3}$ choices.
- Choose suit for the lowest unmatched card. There are $\binom{4}{1}$ choices.
- Choose suit for other unmatched card. There are $\binom{4}{1}$ choices.

The Rule of Product implies that there are $\boxed{\binom{13}{3}\binom{3}{1}\binom{4}{3}\binom{4}{1}\binom{4}{1} = 54912}$ possible 3-of-a-kind hands.

Exercise 34.1.6

Let $n \in \mathbb{Z}^+$ and S be the set of all binary strings of length n. Each of the following expressions is the size of some subset of S. For each one, identify such a subset and explain why it works.

(a) 2^{n-2}

Solution. Subset of strings that start with `00`. Since the first 2 digits are fixed, all such strings are generated by choosing either `0` or `1` for the remaining $n-2$ positions.

(b) $2^n - \binom{n}{n} - \binom{n}{n-1} - \binom{n}{n-2} - \binom{n}{n-3}$

Solution. Subset of strings with at least four `0`'s. From the 2^n binary strings, we subtract the number of strings with less than four `0`'s. The number of binary strings with exactly k-many `0`'s is completely determined by choosing the $n-k$ spots for the `1`'s. Thus, there are $\binom{n}{n-k}$ strings with exactly k-many `0`'s.

(c) $\binom{n}{2} - \binom{n-1}{1}$

Solution. Subset of strings with exactly two `0`'s which are also nonconsecutive. There are $\binom{n}{2}$ strings with exactly two `0`'s (choosing the two spots for the `0`'s). If the `0`'s were consecutive, we could treat `00` as a single block. There are $\binom{n-1}{1}$ strings consisting of exactly $n-2$ `1`'s and single block `00`.

(d) $\displaystyle\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k}$

Solution. Subset of strings with at least as many `0`'s as `1`'s. If there are k `1`'s then there are $n-k$ `0`'s.

$$k \leq n-k \implies 2k \leq n \implies k \leq \left\lfloor \frac{n}{2} \right\rfloor \quad \text{(because } k \in \mathbb{Z}\text{)}$$

The total number of such strings is $\binom{n}{k}$ for $0 \leq k \leq \lfloor \frac{n}{2} \rfloor$.

Exercise 34.1.7

Consider finding the number of 4-tuples from the set $\{1, 2, 3\}$ that include one of each number. In both parts (a) and (b) a student proposes a "Proof" for the number of such 4-tuples. Explain why their reasoning is incorrect by exhibiting an object in the set that has been counted twice.

(a) Pick one of the 4 spots in the tuple for the 1, then pick a spot for the 2, then pick

a spot for the 3. Then pick one of the three numbers to appear in the 4th empty spot.

$$\binom{4}{1}\binom{3}{1}\binom{2}{1}\binom{3}{1} = 72$$

Solution. The 4-tuple $(1, 1, 2, 3)$ is counted twice.

- Pick positions 1, 3, 4 for digits 1, 2, 3, respectively. Pick digit 1 for position 2.
- Pick positions 2, 3, 4 for digits 1, 2, 3, respectively. Pick digit 1 for position 1.

(b) Pick 3 of the 4 spots to be filled by the numbers 1,2,3. Permute those elements in those chosen spots. Pick a number for the 4th empty spot.

$$\binom{4}{3} \cdot 3! \cdot 3 = 72$$

Solution. The 4-tuple $(1, 1, 2, 3)$ is counted twice.

- Pick spots 1, 3, 4 and permutation $(1, 2, 3)$. Pick digit 1 for position 2.
- Pick spots 2, 3, 4 and permutation $(1, 2, 3)$. Pick digit 1 for position 1.

(c) Provide a correct counting argument for the number of possible 4-tuples.

Solution. Multi-step procedure:

- Choose which digit repeats: $\binom{3}{1}$ options.
- Choose two of the four positions for this repeated digit: $\binom{4}{2}$ options.
- Permute the remaining two digits in the remaining two positions: 2! options.

Therefore, the number of such 4-tuples is

$$\binom{3}{1}\binom{4}{2} \cdot 2! = \boxed{36}$$

33. November 24

Exercise 35.1.5

Use the Binomial Theorem to show the following identities.

(a) $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$

Solution. Recognizing that $0 = (1-1)^n$ we have

$$0 = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(-1)^k = \sum_{k=0}^{n}(-1)^k\binom{n}{k}$$

(b) $3^n = \sum_{k=0}^{n}\binom{n}{k}2^k = \sum_{k=0}^{n}\binom{n}{k}2^{n-k}$

Solution. Recognizing $3^n = (1+2)^n = (2+1)^n$ we have

$$\begin{aligned} 3^n = (1+2)^n &= \sum_{k=0}^{n}\binom{n}{k}1^{n-k}2^k = \sum_{k=0}^{n}\binom{n}{k}2^k \\ &= (2+1)^n = \sum_{k=0}^{n}\binom{n}{k}2^{n-k}1^k = \sum_{k=0}^{n}\binom{n}{k}2^{n-k} \end{aligned}$$

(c) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}2^{n-k} = 1$

Solution. Recognizing $1 = (2-1)^n$ we have

$$1 = \sum_{k=0}^{n}\binom{n}{k}(-1)^k2^{n-k}$$

(d) $(1+x)^{2n} = \sum_{k=0}^{2n}\left(\sum_{j=0}^{k}\binom{n}{j}\binom{n}{k-j}\right)x^k$

Solution. We have $(1+x)^{2n} = (1+x)^n(1+x)^n$. From the Binomial Theorem:

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{j}x^k$$

Multiplying this expression by itself gives

$$(1+x)^{2n} = \left(\sum_{j=0}^{n}\binom{n}{j}x^j\right)\left(\sum_{k=0}^{n}\binom{n}{j}x^k\right)$$

Collect the coefficients of x^i in the product. The term x^i arises precisely when the first series contributes x^j and the second contributes x^{i-j}. Summing over all

possible such j, we find

$$\text{Coeff. of } x^i = \sum_{j=0}^{i} \binom{n}{j}\binom{n}{i-j}$$

Since this holds for every i with $0 \leq i \leq 2n$, we obtain

$$(1+x)^{2n} = \sum_{i=0}^{2n} \left(\sum_{j=0}^{i} \binom{n}{j}\binom{n}{i-j} \right) x^k$$

as claimed. □

Exercise 35.1.7

Let $n \in \mathbb{Z}^+$. Prove that

$$n \cdot 2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k}.$$

Proof Sketch. Let S be the set non-empty committees with a chair person that can be formed from a group of n-many people. Equivalently,

$$S = \{(T, t) \in \mathcal{P}([n]) \times [n] \mid t \in T\}$$

- (LHS): First select a leader, then select the rest of the committee.
- (RHS): Partition based on the size of the committee, $1 \leq k \leq n$.

34. December 1

Exercise 36.1.2

Prove the following identities via a "counting in two ways" argument. Use the exact form given. Do not simplify algebraically.

(a) Let $a, b, k \in \mathbb{Z}^+$ with $a + b \geq k$.

$$\binom{a+b}{k} = \sum_{i=0}^{k} \binom{a}{i}\binom{b}{k-i}$$

Proof Sketch. Suppose there are a-many republicans and b-many democrats, and they need to form a committee of size k. Let be the set of all k-person committees that that can be formed.

- (LHS): $|S| = \binom{a+b}{k}$ by definition, because we are selecting k people from $a+b$ total people.
- (RHS): Partition based on the number of republicans in the committee, $0 \leq i \leq k$.

(b) Let $n \in \mathbb{Z}^+$.

$$3^n - 2^n = \sum_{k=1}^{n} 2^{k-1} \cdot 3^{n-k}$$

Proof Sketch. Let S be the set of ternary n-tuples ($\{0,1,2\}^n$) with at least one 2.

- (LHS): Count the complement.
- (RHS): Partition based on the position of the first 2, $1 \leq i \leq n$.

(c) Let $m, n \in \mathbb{Z}^+$ with $n \geq m$.

$$\binom{n}{m} \cdot 2^{n-m} \cdot m = \sum_{k=m}^{n} k \binom{n}{k} \binom{k-1}{m-1}$$

Proof Sketch. From n people, we want to form 2 committees - one of size m with a chairperson, and the other a (possibly empty) committee, disjoint from the first. Let S be the set of all possible committees/chairperson combinations.

- (LHS): Choose the m-person committee, choose a leader from these m committee members, and then, from the remaining $n-m$ people, choose a (possibly empty) subset.
- (RHS): Partition based on the total number of people in either committee, $m \leq k \leq n$. For each piece of the partition, choose a group of k people, choose a chair person, and then from the $k-1$ remaining people, pick the remaining $m-1$ members of the m-sized committee. The other committee is then completely determined.

(d) Let $n \in \mathbb{N}$ with $n \geq 4$.

$$\binom{\binom{n}{2}}{2} = 3 \cdot \binom{n}{4} + 3 \cdot \binom{n}{3}$$

Proof Sketch. Let S be the set of all ways to choose 2 distinct pairs of people from a total of n-many people.

- (LHS): There are $\binom{n}{2}$ pairs of people and you want to select 2 different pairs.

- (RHS): Partition based on whether or not the 2 pairs of people are disjoint or not.

35. December 3

Exercise 37.1.2

Consider the Diophantine equation $a+b+c+d=25$.

(a) How many nonnegative integer solutions are there?

Solution. We need to distribute twenty-five '1's across four variables. By the stars-and-bars theorem, the number of nonnegative integer solutions is

$$\binom{25+4-1}{4-1} = \binom{28}{3} = \boxed{3276}.$$

(b) How many positive integer solutions are there?

Solution. First assign one '1' to each variable to ensure positivity. The remaining twenty-one '1's can be distributed arbitrarily. By the stars-and-bars theorem, the number of positive integer solutions is

$$\binom{21+4-1}{4-1} = \binom{24}{3} = \boxed{2024}.$$

Equivalently, define new variables $x_1 = a-1$, $x_2 = b-1$, $x_3 = c-1$, and $x_4 = d-1$, which are all nonnegative integers. Substituting into the original equation gives

$$(x_1+1)+(x_2+1)+(x_3+1)+(x_4+1) = 25,$$

which simplifies to $x_1+x_2+x_3+x_4 = 21$. The number of nonnegative integer solutions to this equation is, as before,

$$\binom{21+4-1}{4-1} = \binom{24}{3}.$$

(c) How many nonnegative integer solutions are there with $a \geq 3$ and $b \geq 2$?

Solution. First assign three '1's to a and two '1's to b to satisfy the lower bounds. The remaining twenty '1's can be distributed arbitrarily among the four variables. By the stars-and-bars theorem, the number of such solutions is

$$\binom{20+4-1}{4-1} = \binom{23}{3} = \boxed{1771}.$$

Solution. To transform the problem into one involving nonnegative integers, define:

$$\begin{aligned} x_1 &= a - 3 \quad (\text{so } x_1 \geq 0), \\ x_2 &= b - 2 \quad (\text{so } x_2 \geq 0), \\ x_3 &= c \qquad (\text{so } x_3 \geq 0), \\ x_4 &= d + 4 \quad (\text{so } x_4 \geq 0). \end{aligned}$$

Substituting into the original equation $a + b + c + d = 25$ yields:

$$(x_1 + 3) + (x_2 + 2) + x_3 + (x_4 - 4) = 25.$$

Simplifying gives $x_1 + x_2 + x_3 + x_4 = 24$. The number of nonnegative integer solutions to this equation is

$$\binom{24 + 4 - 1}{4 - 1} = \binom{27}{3} = \boxed{2925}.$$

(d) How many nonnegative integer solutions are there with $a \leq 9$ and $b \leq 8$?

Solution. Let S be the set of all nonnegative integer solutions. From part (a), $|S| = \binom{28}{3}$.

Define:

- A: the set of solutions with $a \geq 10$,
- B: the set of solutions with $b \geq 9$.

We wish to find the number of solutions in $\overline{A} \cap \overline{B}$, i.e., those satisfying $a \leq 9$ and $b \leq 8$. Since $\overline{A \cup B} = \overline{A} \cap \overline{B}$ by DeMorgan's Law, the principle of inclusion-exclusion (version 1) implies

$$|\overline{A} \cap \overline{B}| = |\overline{A \cup B}| = |S| - |A| - |B| + |A \cap B|.$$

We compute the sizes of A, B, and $A \cap B$ using the stars-and-bars theorem:

- $|A|$: Assign 10 to a. The remaining sum is 15, distributed among 4 variables: $\binom{15+4-1}{3} = \binom{18}{3}$.
- $|B|$: Assign 9 to b. The remaining sum is 16, distributed among 4 variables: $\binom{16+4-1}{3} = \binom{19}{3}$.
- $|A \cap B|$: Assign 10 to a and 9 to b. The remaining sum is 6, distributed among 4 variables: $\binom{6+4-1}{3} = \binom{9}{3}$.

Therefore, the number of solutions satisfying $a \leq 9$ and $b \leq 8$ is

$$\binom{28}{3} - \binom{18}{3} - \binom{19}{3} + \binom{9}{3} = \boxed{1575}.$$

Exercise 37.1.3

A baker has 48 cupcakes to distribute among 4 distinct serving tables.

(a) In how many ways can the baker distribute the cupcakes if all 48 cupcakes are distinct?

Solution. This is a problem of counting arrangements with repetition. There are 4 choices for the table of each cupcake. By the multiplication principle, the total number of distributions is

$$\boxed{4^{48} = 79,228,162,514,264,337,593,543,950,336}.$$

(b) In how many ways can this be done if all 48 cupcakes are identical?

Solution. This is a problem of counting selections with repetition. We need to distribute 48 identical cupcakes across 4 distinct tables. By the stars-and-bars theorem, the number of nonnegative integer solutions to $x_1 + x_2 + x_3 + x_4 = 48$ is

$$\binom{48+4-1}{4-1} = \boxed{\binom{51}{3} = 20,825}.$$

(c) Suppose there are 6 flavors of cupcakes, with 8 identical cupcakes of each flavor. How many distributions are possible?

Solution. The distribution of each flavor is independent. For a single flavor, we need to distribute 8 identical cupcakes across 4 distinct tables. By the stars-and-bars theorem, this can be done in $\binom{8+4-1}{4-1} = \binom{11}{3}$ ways. Since the choices for the 6 flavors are independent, by the rule of product, the total number of distributions is

$$\boxed{\binom{11}{3}^6 = 20,179,187,015,625}.$$

(d) How many distributions are possible if the cupcakes are identical and no table is left empty?

Solution. First, place one cupcake on each table to ensure none are empty. The remaining 44 identical cupcakes can be distributed arbitrarily among the 4 tables. By the stars-and-bars theorem, the number of such distributions is

$$\binom{44+4-1}{4-1} = \boxed{\binom{47}{3} = 16,215}.$$

(e) Suppose the baker faces the following constraints: Tables 1 and 2 may not receive more than 10 cupcakes each, and Tables 3 and 4 must not be empty. If all cupcakes are identical, how many valid distributions are possible?

Solution. Let S be the set of all distributions where Tables 3 and 4 are non-empty. We first find $|S|$ by placing one cupcake on each of Tables 3 and 4. The remaining $48 - 2 = 46$ identical cupcakes can be distributed arbitrarily among all 4 tables. Thus,

$$|S| = \binom{46+4-1}{4-1} = \binom{49}{3}.$$

Now, define subsets of S that violate the constraints on Tables 1 and 2:

- A: distributions where Table 1 receives ≥ 11 cupcakes.
- B: distributions where Table 2 receives ≥ 11 cupcakes.

We wish to find the number of distributions in S that are in neither A nor B, i.e., $|\overline{A} \cap \overline{B}|$. By the principle of inclusion-exclusion (version 1),

$$|\overline{A} \cap \overline{B}| = |S| - |A| - |B| + |A \cap B|.$$

We compute the sizes of A, B, and $A \cap B$ using the stars-and-bars theorem, after pre-assigning cupcakes to violate the conditions:

- $|A|$: Assign 11 cupcakes to Table 1. With Tables 3 and 4 already having one cupcake each, the remaining $48 - 2 - 11 = 35$ cupcakes are distributed arbitrarily among all 4 tables: $\binom{35+4-1}{3} = \binom{38}{3}$.
- $|B|$: By symmetry, $|B| = \binom{38}{3}$.
- $|A \cap B|$: Assign 11 cupcakes to Table 1 and 11 to Table 2. With the initial cupcakes on Tables 3 and 4, the remaining $48 - 2 - 11 - 11 = 24$ cupcakes are distributed arbitrarily: $\binom{24+4-1}{3} = \binom{27}{3}$.

Therefore, the number of valid distributions is

$$\binom{49}{3} - 2\binom{38}{3} + \binom{27}{3} = \boxed{4{,}477}.$$

Exercise 37.1.4

Your bank requires you to create a 4-digit ATM PIN code (digits `0`–`9`). How many PIN codes are possible if the digits form a *non-decreasing* sequence? (That is, $d_1 \leq d_2 \leq d_3 \leq d_4$.)

Solution. Once the 4 digits of the PIN code are determined, there is only one way to arrange them in a non-decreasing order. Therefore, counting the number of non-decreasing PINs is equivalent to counting the number of ways to choose 4 digits from

the 10 possible digits (0–9), where we are allowed to choose the same digit more than once and the order of selection does not matter (because the non-decreasing condition will enforce a unique order). This is a standard selections with repetition problem. By the stars-and-bars theorem, there are

$$\binom{4+10-1}{10-1} = \boxed{\binom{13}{9} = 715}$$

possible PIN codes.

Exercise 37.2.6

In a group of 100 students, 45 study mathematics, 38 study physics, 42 study chemistry, 15 study both mathematics and physics, 18 study both mathematics and chemistry, 16 study both physics and chemistry, and 7 study all three. How many students study none of these subjects?

Solution. Let S be the set of students, so $|S|= 100$. Further, define $M, P, C \subseteq S$ by

- M = set of students studying math.
- P = set of students studying physics.
- C = set of students studying chemistry.

We wish to find $|\overline{M} \cap \overline{P} \cap \overline{C}|$. We are told

- $|M|= 45$
- $|P|= 38$
- $|C|= 42$
- $|M \cap P|= 15$
- $|M \cap C|= 18$
- $|P \cap C|= 16$
- $|M \cap P \cap C|= 7$

Then, by the principle of inclusion-exclusion:

$$\begin{aligned}|\overline{M} \cap \overline{P} \cap \overline{C}| &= |S|-|M|-|P|-|C|+|M \cap P|+|M \cap C|+|P \cap C|-|M \cap P \cap C| \\ &= 100 - 45 - 38 - 42 + 15 + 18 + 16 - 7 \\ &= 17\end{aligned}$$

So $\boxed{17}$ students study neither math, physics, nor chemistry.

Exercise 37.2.7

Use the Principle of Inclusion–Exclusion to find the number of integers between 1 and 2500 that are not divisible by 4, 5, or 6.

Solution. Let S be the set of integers from 1 to 2500. Define $A_4, A_5, A_6 \subseteq S$ by letting A_4 be the subset of S consisting of the integers divisible by 4, A_5 be the subset consisting of the integers divisible by 5, and A_6 be the subset consisting of the integers divisible by 6. Then

$$\begin{aligned}
|A_4| &= \left\lfloor \frac{2500}{4} \right\rfloor = 625 \\
|A_5| &= \left\lfloor \frac{2500}{5} \right\rfloor = 500 \\
|A_6| &= \left\lfloor \frac{2500}{6} \right\rfloor = 416 \\
|A_4 \cap A_5| &= \left\lfloor \frac{2500}{20} \right\rfloor = 125 \\
|A_4 \cap A_6| &= \left\lfloor \frac{2500}{12} \right\rfloor = 208 \\
|A_5 \cap A_6| &= \left\lfloor \frac{2500}{30} \right\rfloor = 83 \\
|A_4 \cap A_5 \cap A_6| &= \left\lfloor \frac{2500}{60} \right\rfloor = 41
\end{aligned}$$

The subset of integers not divisible by 4,5, or 6 is $\overline{A_4} \cap \overline{A_5} \cap \overline{A_6}$. By the principle of inclusion/exclusion we have

$$|\overline{A_4} \cap \overline{A_5} \cap \overline{A_6}| = 2500 - 625 - 500 - 416 + 125 + 208 + 83 - 41 = 1334$$

Therefore there are $\boxed{1334}$ integers between 1 and 2500 which are not divisible by 4, 5, or 6.

Exercise 37.2.8

How many orderings of the eight letters $\{a, b, c, d, e, f, g, h\}$ contain none of the consecutive patterns ab, cd, ef, or gh?

Solution. Let S be the set of all possible orderings of $\{a, b, c, d, e, f, g, h\}$. Then $|S| = 8!$ since each element is a permutation of the 8 letters. Define $A_1, A_2, A_3, A_4 \subseteq S$ by

$$\begin{aligned}
A_1 &= \text{ the arrangements in which the pattern } ab \text{ appears} \\
A_2 &= \text{ the arrangements in which the pattern } cd \text{ appears} \\
A_3 &= \text{ the arrangements in which the pattern } ef \text{ appears} \\
A_4 &= \text{ the arrangements in which the pattern } gh \text{ appears}
\end{aligned}$$

For each $i \in [4]$, $|A_i| = 7!$, treating the block of 2 letters as a single letter. Similar, for $i \neq j \in [4]$, we have $|A_i \cap A_j| = 6!$, treating each block of 2 letters as a single letter. For $i \neq j \neq k \in [4]$, $|A_i \cap A_j \cap A_k| = 5!$. Finally, $|A_1 \cap A_2 \cap A_3 \cap A_4| = 4!$ since each element is a permutation of the 4 blocks of letters ab, cd, ef, gh. Then, by the Principle of Inclusion/Exclusion we have

$$|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \overline{A_4}| = \boxed{8! - \binom{4}{1}7! + \binom{4}{2}6! - \binom{4}{3}5! + 4!}$$

Exercise 37.2.9

How many permutations of [7] contain at least one of the consecutive increasing patterns 123, 345, or 567?

Solution. Let S be the set of permutations of [7], so $|S| = 7!$. Define $A, B, C \subseteq S$ by

- $A =$ permutations that contain the consecutive pattern 123,
- $B =$ permutations that contain the consecutive pattern 345,
- $C =$ permutations that contain the consecutive pattern 567.

We wish to find $|A \cup B \cup C|$.

- To compute $|A|$, treat 123 as a single block. The block 123 together with the remaining elements $\{4, 5, 6, 7\}$ gives 5 objects to permute. Thus $|A| = 5!$.
- By the same reasoning, $|B| = |C| = 5!$.
- For $A \cap B$, both 123 and 345 must appear as consecutive increasing patterns. This forces the pattern 12345 to appear as a single block. Together with the remaining elements $6, 7$, this gives 3 objects to permute, so $|A \cap B| = 3!$.
- For $A \cap C$, the blocks 123 and 567 are disjoint, and the remaining element is 4. Thus we permute the three objects $123, 4, 567$, giving $|A \cap C| = 3!$.
- For $B \cap C$, the patterns 345 and 567 force the block 34567. Together with the remaining elements $1, 2$, we again get 3 objects, so $|B \cap C| = 3!$.
- For $A \cap B \cap C$, all three patterns occur. This forces the block 1234567, so only one permutation works (the identity permutation). Thus $|A \cap B \cap C| = 1$.

By the principle of inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 3 \cdot 5! - 3 \cdot 3! + 1 \\ &= 343 \end{aligned}$$

Therefore, there are $\boxed{343}$ such permutations.

Exercise 37.2.10

Determine the number of nonnegative integer solutions to

$$x_1 + x_2 + x_3 + x_4 = 20$$

satisfying $x_1 \leq 7$, $x_2 \leq 5$, $x_3 \leq 6$, and $x_4 \leq 4$.

Solution. Let S be the set of all nonnegative integer solutions to $x_1+x_2+x_3+x_4 = 20$. By stars and bars, $|S| = \binom{20+4-1}{4-1} = \binom{23}{3}$.

Define subsets $A, B, C, D \subseteq S$ by

- A = solutions with $x_1 \geq 8$,
- B = solutions with $x_2 \geq 6$,
- C = solutions with $x_3 \geq 7$,
- D = solutions with $x_4 \geq 5$.

We wish to compute $|\overline{A} \cap \overline{B} \cap \overline{C} \cap \overline{D}|$.

- For $|A|$: set $x_1 = 8$ and distribute the remaining 12 units. Thus $|A| = \binom{12+4-1}{4-1} = \binom{15}{3}$.
- For $|B|$: set $x_2 = 6$ and distribute 14 units. Thus $|B| = \binom{17}{3}$.
- For $|C|$: set $x_3 = 7$ and distribute 13 units. Thus $|C| = \binom{16}{3}$.
- For $|D|$: set $x_4 = 5$ and distribute 15 units. Thus $|D| = \binom{18}{3}$.
- For $|A \cap B|$: assign 8 to x_1 and 6 to x_2, leaving 6 units. Thus $|A \cap B| = \binom{9}{3}$.
- For $|A \cap C|$: assign 8 to x_1 and 7 to x_3, leaving 5 units. Thus $|A \cap C| = \binom{8}{3}$.
- For $|A \cap D|$: assign 8 to x_1 and 5 to x_4, leaving 7 units. Thus $|A \cap D| = \binom{10}{3}$.
- For $|B \cap C|$: assign 6 to x_2 and 7 to x_3, leaving 7 units. Thus $|B \cap C| = \binom{10}{3}$.
- For $|B \cap D|$: assign 6 to x_2 and 5 to x_4, leaving 9 units. Thus $|B \cap D| = \binom{12}{3}$.
- For $|C \cap D|$: assign 7 to x_3 and 5 to x_4, leaving 8 units. Thus $|C \cap D| = \binom{11}{3}$.
- $|A \cap B \cap C| = 0$ since $8 + 6 + 7 > 20$.
- For $|A \cap B \cap D|$: assign 8, 6, and 5, leaving 1 unit. Thus $|A \cap B \cap D| = \binom{4}{3}$.
- $|A \cap C \cap D| = 1$ since $8 + 7 + 5 = 20$.
- For $|B \cap C \cap D|$: assign 6, 7, and 5, leaving 2 units. Thus $|B \cap C \cap D| = \binom{5}{3}$.
- $|A \cap B \cap C \cap D| = 0$ since $8 + 6 + 7 + 5 > 20$.

Applying the principle of inclusion–exclusion:

$$\begin{aligned}|\overline{A}\cap\overline{B}\cap\overline{C}\cap\overline{D}| &= |S|-(|A|+|B|+|C|+|D|)+(|A\cap B|+|A\cap C|+|A\cap D|+|B\cap C|+|B\cap D|+|C\cap D|)\\ &\quad-(|A\cap B\cap C|+|A\cap B\cap D|+|A\cap C\cap D|+|B\cap C\cap D|)+|A\cap B\cap C\cap D|\\ &=\binom{23}{3}-\binom{15}{3}-\binom{16}{3}-\binom{17}{3}-\binom{18}{3}+\binom{9}{3}+\binom{8}{3}+2\binom{10}{3}\\ &\quad+\binom{11}{3}+\binom{12}{3}-\binom{4}{3}-1-\binom{5}{3}\\ &=10.\end{aligned}$$

Therefore, there are $\boxed{10}$ such solutions.

Exercise 37.2.11

Eight people sit in a row. How many seatings avoid all three of the following adjacency restrictions?

- Alice cannot sit next to Bob
- Claire cannot sit next to Diana
- Evan cannot sit next to Fiona

Solution. Let S be the set of all seatings of the 8 people in a row, so $|S|=8!$. Define subsets $A, C, E \subseteq S$ by

- A = permutations in which Alice sits next to Bob,
- C = permutations in which Claire sits next to Diana,
- E = permutations in which Evan sits next to Fiona.

We wish to compute $|\overline{A}\cap\overline{C}\cap\overline{E}|$.

- For $|A|$: treat the pair `AB` as a single block. There are 7! ways to arrange the block with the remaining six individuals, and the pair can appear as `AB` or `BA`. Hence $|A|=2\cdot 7!$.
- Similarly, $|C|=|E|=2\cdot 7!$.
- For $|A\cap C|$: treat both `AB` and `CD` as blocks. There are 6! permutations of the two blocks together with the remaining four individuals, and each block may appear in either internal order. Thus $|A\cap C|=2^2\cdot 6!$.
- The same reasoning gives $|A\cap E|=|C\cap E|=2^2\cdot 6!$.

- For $|A \cap C \cap E|$: treat `AB`, `CD`, and `EF` as blocks. There are 5! permutations of these three blocks with the remaining two individuals, and each block has 2 internal orders. Hence $|A \cap C \cap E| = 2^3 \cdot 5!$.

Applying the principle of inclusion–exclusion,

$$|\overline{A} \cap \overline{C} \cap \overline{E}| = 8! - 3(2 \cdot 7!) + 3(2^2 \cdot 6!) - 2^3 \cdot 5! = \boxed{17760}.$$

Exercise 37.2.12

How many lattice paths from $(0, 0)$ to $(10, 10)$ using only steps $(1, 0)$ and $(0, 1)$ avoid all three points $(3, 3)$, $(5, 6)$, and $(7, 5)$?

Solution. Let S be the set of all lattice paths from $(0, 0)$ to $(10, 10)$ using steps $(1, 0)$ and $(0, 1)$. Then $|S| = \binom{20}{10}$. Define subsets $A, B, C \subseteq S$ by

- $A =$ paths that pass through $(3, 3)$,
- $B =$ paths that pass through $(5, 6)$,
- $C =$ paths that pass through $(7, 5)$.

We seek $|\overline{A} \cap \overline{B} \cap \overline{C}|$.

- To count $|A|$: a path must go from $(0, 0)$ to $(3, 3)$ and then from $(3, 3)$ to $(10, 10)$. Hence, $|A| = \binom{6}{3}\binom{14}{7}$.
- For $|B|$: a path must go through $(5, 6)$, so $|B| = \binom{11}{5}\binom{9}{4}$.
- For $|C|$: a path must go through $(7, 5)$, so $|C| = \binom{12}{5}\binom{8}{3}$.
- For $|A \cap B|$: the path must go

  $$(0, 0) \to (3, 3) \to (5, 6) \to (10, 10),$$

  giving $|A \cap B| = \binom{6}{3}\binom{5}{2}\binom{9}{4}$.
- For $|A \cap C|$: the path must go

  $$(0, 0) \to (3, 3) \to (7, 5) \to (10, 10),$$

  giving $|A \cap C| = \binom{6}{3}\binom{6}{2}\binom{8}{3}$.
- There is no lattice path from $(5, 6)$ to $(7, 5)$ (it requires a negative step), so $|B \cap C| = 0$.
- Likewise, no path can visit all three points in any valid order, so $|A \cap B \cap C| = 0$.

Applying the principle of inclusion–exclusion,

$$\binom{20}{10} - \binom{6}{3}\binom{14}{7} - \binom{11}{5}\binom{9}{4} - \binom{12}{5}\binom{8}{3} + \binom{6}{3}\binom{5}{2}\binom{9}{4} + \binom{6}{3}\binom{6}{2}\binom{8}{3} = 55552.$$

Thus there are $\boxed{55,552}$ such lattice paths.