Reading, Discovering and Writing Proofs
Version 0.4.0.3

Contents

Preface

These notes are the course notes to accompany the lectures of MATH 135 at the University of Waterloo. The script has been supplemented by worked examples and exercises.

These notes are very much a work in progress. The first time this version of the notes were used is in Fall 2015. Please send any corrections or suggestions to J. P. Pretti at jpretti@uwaterloo.ca

Part I

Introduction to Proof Methods

Chapter 1

In the beginning

1.1 What Makes a Mathematician a Mathematician?

Welcome to MATH 135!

Let us begin with a question. What makes a mathematician a mathematician?

Many people would answer that someone who works with numbers is a mathematician. But bookkeepers for small businesses work with numbers and we don't normally consider a bookkeeper as a mathematician. Others might think of geometry and answer that someone who works with shapes is a mathematician. But architects work with shapes and we don't normally consider architects as mathematicians. Still others might answer that people who use formulas are mathematicians. But engineers work with formulas and we don't normally consider engineers as mathematicians. A more insightful answer would be that people who find patterns and provide descriptions and evidence for those patterns are mathematicians. But scientists search for and document patterns and we don't normally consider scientists as mathematicians.

The answer is *proof* - a rigorous, formal argument that establishes the truth of a statement. This has been the defining characteristic of mathematics since ancient Greece.

This course is about reading, writing and discovering proofs. If you have never done this before, do not worry. The course will provide you with techniques that will help, and we will practice those techniques in the context of some very interesting algebra.

1.2 Why do we reason formally?

But why do we reason so formally at all? Many people believe that humans already know enough mathematics so "Why bother with proofs?" There are quite a few reasons.

To prevent silliness. In solving quadratic equations with non-real roots, some of you will have encountered the number i which has the special property that $i^2 = -1$. But then,

$$-1 = i^2 = i \times i = \sqrt{-1}\sqrt{-1} = \sqrt{-1 \times -1} = \sqrt{1} = 1$$

Clearly, something is amiss.

To understand better. How would most of us answer the question "What's a real number?" We would probably say that any number written as a decimal expansion is a real number and any two different expansions represent different numbers. But then what about this?

$$\text{Let } x = 0.\overline{9} = 0.999\ldots.$$

Multiplying by 10 and subtracting gives

$$\begin{array}{rrcl} & 10x & = & 9.\overline{9} \\ - & x & = & 0.\overline{9} \\ \hline & 9x & = & 9 \end{array}$$

which implies $x = 1$, not $x = 0.\overline{9}$. Consequently, we need a better understanding of how to distinguish between two real numbers.

Or suppose we wanted to evaluate the infinite sum

$$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \ldots$$

If we pair up the first two terms we get zero and every successive pair of terms also gives us 0 so the sum is zero.

$$\overbrace{1-1}+\overbrace{1-1}+\overbrace{1-1}+\overbrace{1-1}+\ldots$$

On the other hand, if we pair up the second and third term we get 0 and all successive pairs of terms give 0 so the sum is 1.

$$1\overbrace{-1+1}\overbrace{-1+1}\overbrace{-1+1}\overbrace{-1+1}+\ldots$$

To resolve this issue, we need to understand how to obtain numbers that represent such infinite sums.

Or suppose we wanted to resolve one of the famous Zeno's paradoxes. Zeno was a famous ancient Greek philosopher who posed the following problem. Suppose the Greek hero Achilles was going to race against a tortoise and suppose, in recognition of the slowness of the tortoise, that the tortoise gets a 100m head start. By the time Achilles has run half the distance between he and the tortoise, the tortoise has moved ahead. And now again, by the time Achilles has run half the remaining distance between he and the tortoise, the tortoise has moved ahead. No matter how fast Achilles runs, the tortoise will always be ahead! You might object that your eyes see Achilles pass the tortoise, but what is logically wrong with Zeno's argument?

To make better commercial decisions. Building pipelines is expensive. Certainly lots of pipelines will be built in the next few decades. Pipelines will ship oil, natural gas, water and sewage. Finding the shortest route given physical constraints (mountains, rivers, lakes, cities), environmental constraints (protection of the water table, no access through national or state parks), and supply chain constraints (access to concrete and steel) is very important. How do pipeline builders *prove* that the route they have chosen for the pipeline is the shortest possible route given the constraints?

To discover solutions. Formal reasoning provides a set of tools that allow us to think rationally and carefully about problems in mathematics, computing, engineering, science, economics and any discipline in which we create models.

Poor reasoning can be very expensive. Inaccurate application of financial models led to losses of hundreds of billions of dollars during the financial crisis of 2008.

To experience joy. Mathematics can be beautiful, just as poetry can be beautiful. But to hear the poetry of mathematics, one must first understand the language.

1.3 How The Course Works

He who seeks for methods without having a definite problem in mind seeks for the most part in vain.

David Hilbert

Let us start with a description of how the course works.

Throughout the course, our goal is to develop our mathematical reasoning. We start with the foundations for mathematical proof and then work on four problems - all of which illustrate the need for proof. The first problem resolves a very important practical commercial problem. The second problem results in a new number system and yields a surprising and beautiful formula. The third problem relies on a profound theorem proved by Karl Friedrich Gauss, the greatest mathematician of the modern age. Here are the four problems. The fourth problem concerns an astonishing result about one of the simplest things we do, count.

How do we secure internet commerce? Have you ever bought a song or movie over iTunes? Have you ever done your banking over the web? How do you make sure that your credit card number and personal information are not intercepted by bad guys? Number theory allows us to enable secure web transactions. And that theory is backed by proof.

Why does $e^{i\pi} + 1 = 0$? This is often heralded as the "most beautiful equation" in mathematics. We know that the natural exponent, e, is a very unusual number that arises in calculus as a limit of a specific sequence of numbers.

On a similar note, i is a very unusual number because it has the property that $i^2 = -1$. This is strange because we know that the square of a real number is always non-negative, and clearly the number i violates this rule.

As mathematicians, we appreciate that π is also a very unusual number even if it is common. It is the unique ratio of the circumference of a circle to its diameter. Why should that ratio be unique?

In addition to all of these, one (1) is the basis of the natural numbers, hence the integers, hence the rationals. Zero (0) is a difficult number and was only accepted into the mathematics of western Europe because of the influence of Hindu and Islamic scholars. Why should all of these numbers be connected in so simple and elegant a form?

How do we factor polynomials? You may have factored positive integers into a product of prime numbers before. We will see in this course that polynomials, which are expressions like $ax^4 + bx^3 + cx^2 + dx + e$, behave a lot like the integers. Hence, there is also a need in mathematics to factor polynomials into the polynomial equivalent of prime numbers.

What does it mean to count? You probably learned to count before you went to school. In fact, counting with our fingers is often the first way we get introduced to the numbers we use in mathematics. We soon realize there are more numbers than we can count with our fingers. But how do you count to infinity? And is there only one infinity?

To understand and solve these problems we will need to learn about various mathematical concepts, such as **modular congruences, modular arithmetic, complex numbers, polynomials**, etc. And to work with these topics, we must learn some foundational mathematics such as logical expressions and sets, and, most importantly, we must learn how to recognize and use proof techniques.

There will be a substantial amount of new definitions and propositions introduced throughout the course. Familiarize yourself with these. We will use a system of acronyms (e.g. (*DML*)) to keep track of the proven propositions (e.g. (*De Morgan's Laws*)) and to refer to them from time-to-time. *Disclaimer: These acronyms are somewhat artificial and may not be meaningful outside the setting of this course. A similar comment applies to the labels (e.g., Select Method, Construct Method, etc.) that we use for our various proof methods.*

Chapter 2

A First Look At Proofs

2.1 Objectives

Learning objectives

1. Define *statement*, *proposition*, and *axioms*.
2. Develop a notion of *proofs* as convincing arguments that verify propositions.
3. Introduce the concept of *Divisibility*.
4. Read a proof of *Transitivity of Divisibility*.

2.2 The Language

> *Mathematics* is the language of mathematicians, and a *proof* is a method of communicating a mathematical truth to another person who speaks the "language". (Solow, *How to Read and Do Proofs*)

Mathematics is an extraordinarily precise language. When a mathematical argument, such as a proof, is fully and correctly presented, there is no ambiguity and no doubt about its correctness.

However, understanding a proof requires understanding the language. This course will help you with the basic grammar of the language of mathematics and is applicable to all proofs. Just as in learning any new language, you will need lots of practice to become fluent.

Hopefully, in the previous lecture, we convinced you of *why* we need to prove things. Now *what* is it that mathematicians prove? Mathematicians prove statements.

Definition 2.2.1
Statement

A **statement** is a sentence that has a definite state of being either true or false.

Example 1

Here are some examples of statements.

1. $2 + 2 = 4$. (A true statement.)
2. $\pi + 2 < 5$. (A false statement.)
3. There is no largest real number. (A true statement.)
4. There exists an angle θ such that $\sin(\theta) > 1$. (A false statement.)

First of all, a statement must have a corresponding truth value. That is, when reading a statement, we should realize that what is being said has to be either true or false (but cannot be both), even if we do not know the truth value of the statement.

Example 2

On the other hand, the following are examples of sentences that are not mathematical statements.

1. Is $7 = 5$?
2. Find the smallest positive integer.
3. Let $x > 0$.

Let us discuss why the above sentences are not statements. Questions, such as "is $7 = 5$?", are never statements. We simply cannot assign a "true" or a "false" state to questions. Similarly, instructions to "find the smallest positive integer" or to "assume that $x > 0$" cannot be given truth values, and are therefore not statements.

2.3 Propositions, Proofs and Axioms

A mathematical statement has a definite true or false value. Given a statement, however, it is not always obvious whether the statement is true or not. Throughout this course we will encounter statements that we would be interested in figuring out whether they are true or false. Such statements are known as *propositions*.

REMARK

A **proposition** is a mathematical claim posed in the form of a statement that either needs to be proven true or demonstrated false by a valid argument. You will encounter several variations on the word proposition. A **theorem** is a particularly significant proposition. A **lemma** is a subsidiary proposition, or more informally, a "helper" proposition, that is used in the proof of a theorem. A **corollary** is a proposition that follows almost immediately from a theorem.

Consider the following proposition.

Proposition 1 For every real number x, $x^2 + 1 \geq 2x$.

This is clearly a statement, but is it true? Well, if we consider the number 5 in place of x, we note that $(5)^2 + 1 = 26$, whereas $2 \times 5 = 10$, and since $26 > 10$, the number 5 does satisfy the claim made in the proposition. However, just as one swallow does not make a summer, knowing that the sentence is true for when $x = 5$ does not guarantee us that it will be true for other instances of x. We need to establish this using a proof.

A **proof** is simply a series of convincing arguments that leaves absolutely no doubt that a given proposition is true. Proofs work by connecting our assumed knowledge from previously proven statements, definitions, axioms, etc. in a mathematically accurate way to deduce a result that establishes the proposed truth.

Let us read our first proof.

Proof of Proposition 1: Suppose x is a real number. Therefore, $x - 1$ must also be a real number, and hence

$$(x - 1)^2 \geq 0.$$

Expanding the terms on the left side, we get $x^2 - 2x + 1 \geq 0$. Adding $2x$ to both sides yields $x^2 + 1 \geq 2x$. □

Note that in the given proof, we did not specify any particular number, rather we worked with the algebraic symbol x. The significance of using x is that it establishes the rule in general. The arguments that are used in the proof are just applications of our common knowledge about real numbers and inequalities. Since we followed a valid line of reasoning, the last expression must hold true for the x we started with, thus proving the statement.

REMARK

Here is a common mistake made by students when they try to prove Proposition 1 given above.

Proposition 1 For every integer x, $x^2 + 1 \geq 2x$.

Attempted Proof: Suppose x is an integer. Then from $x^2 + 1 \geq 2x$, subtract $2x$ from both sides to get $x^2 - 2x + 1 \geq 0$. We recognize that this is just saying $(x - 1)^2 \geq 0$, which is obviously true, so the proposition must be true. □

The problem with this proof is that we are looking at consequences of $x^2 + 1 \geq 2x$. However, this means they have already *assumed* that $x^2 + 1 \geq 2x$ holds, which is exactly what we need to *verify* to be true. This is an example of circular logic, and thus this attempt does not provide us a proof of the proposition at all.

Finally, there are particular statements, known as axioms, that are more foundational. An **axiom** is a statement that is *assumed* to be true. No proof is given, nor needed. Axioms are essentially our fundamental beliefs on how mathematics should work. Obviously, choosing axioms has to be done *very* carefully.

There are some very famous axioms in mathematics, such as *Peano's Axioms on Natural Numbers*, *Euclid's Axioms on Plane Geometry*, the *Zermelo-Fraenkel Axioms of Set Theory*, the *Principle of Mathematical Induction*, etc. However, these formal axioms are often stated for a professional audience, and their importance is sometimes difficult to grasp at a beginner's level.

In this course, we will not use a formal set of axioms. Instead, we will assume that our audience consists other students in the course. Assume other MATH135 students are reading your proofs. They should be able to follow your argument without having to question any facts (axioms) that you use.

Example 3 **(Examples of Axioms That May be Used Without Proof)**

For any two integers x and y, the following are true:

1. $x + y$ and $x - y$ are integers.
2. xy is also an integer, but $\frac{x}{y}$ may or may not be an integer.
3. $x + y = y + x$ and $xy = yx$.
4. $x^2 \geq 0$ and $y^2 \geq 0$.

Self Check 1 Let us now try to solve a few problems on our own.

1. Prove that for every integer x, $x^2 \geq x$.
2. Consider the statement

   Suppose x and y are integers, then $x + y$ must always be even.

   Provide some evidence that the above statement is clearly false.

   Next, identify the mistake in the "attempted proof" of the given statement.

   Attempted Proof: As integers, x and y must be even or odd. When x and y are even, we may write $x = 2k$ and $y = 2m$ for some integers k and m. Then $x + y = 2(k + m)$, which is even.

   Similarly, when x and y are odd, we may instead write $x = 2k + 1$ and $y = 2m + 1$, where k and m are integers. Once again, $x + y = 2(k + m + 1)$, which is even. This shows that $x + y$ is always even. $\square$

Chapter 3

Truth Tables and Logical Operators

3.1 Objectives

Learning Objectives.

1. Define *AND*, *OR*, *NOT* using truth tables.
2. Evaluate logical expressions using truth tables.
3. Use truth tables to establish the equivalence of logical expressions.
4. Prove *De Morgan's Laws*.

3.2 Compound Statements

Throughout this course we work with statements and their proofs. To understand methods for proving statements, we must first understand how complicated statements may often be dissected into a combination of simpler parts. We may then develop ways to string together proofs of such parts to prove the complicated statement in its entirety.

Our objective in this chapter is to develop some rules for combining several statements to produce a new statement. The truth value of the new statement depends on the truth value of the initial statements that are being combined.

Definition 3.2.1 **Compound, Component**

A **compound statement** is a statement composed of several individual statements called **component statements**.

For example, the statement "(π is a real number) and ($3 \neq 4$). " contains two components:

1. π is a real number.
2. $3 \neq 4$.

For the time being, we shall focus on compound statements that are composed of two components. We often label statements with letters such as A, B, C, etc. Suppose A and B are two arbitrary, unrelated statements. Then A would have its own truth value, as would B. We may indicate, for example, that A is *true* (T) but B is *false* (F) by assigning the state (T, F) to the pair of statements (A, B). Thus, the pair (A, B) can achieve any of the following states: $(T, T), (T, F), (F, T)$ and (F, F).

To form a compound statement S, whose components are A and B, we need to declare the truth value of S based on the possible states of its components. The simplest way to do so is to use a *truth table*. A truth table summarizes the information about the states of each component and the corresponding truth value of the compound statements. We have a few examples of how truth tables are used to define compound statements in section 3.3 below.

3.3 Truth Tables as Definitions

In this section, we will use truth tables to introduce three logical operators: "AND", "OR" and "NOT". Note that these do not always coincide with our use of the words *and*, *or*, *not* in the English language.

3.3.1 Negating Statements

Given some statement A, perhaps the simplest compound statement that we may come up with is the *negation of* A. The negation of A, simply known as NOT A, is the statement whose truth value is the exact opposite of that of A. For example, $(3 = 4)$ and $(3 \neq 4)$ are negations of each other.

Definition 3.3.1
NOT

We define **NOT** A, written $\neg A$, using the following truth table.

A	$\neg A$
T	F
F	T

In prose, if the statement A is true, then the statement "NOT A" is false. If the statement A is false, then the statement "NOT A" is true.

Given a statement A, we often try to *negate* A by writing $\neg A$ in a manner that does not involve the $\neg$ symbol. For example, $\neg(3 = 4)$ is written as $(3 \neq 4)$, $\neg(\pi < 4)$ is written as $(\pi \geq 4)$, etc. We will see in later chapters that such practice becomes useful when we are trying to prove complicated statements that have many individual components.

3.3.2 Conjunctions and Disjunctions

Suppose A and B are arbitrary statements. Let us now use truth tables to define two compound statements: $A \wedge B$ (conjunction) and $A \vee B$ (disjunction).

Definition 3.3.2
AND

The definition of A **AND** B, written $A \wedge B$, is

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

The truth table summarizes the fact that $A \wedge B$ is true only when both the components A and B are true.

Truth tables can be used to *define* the truth value of a statement or to *evaluate* the truth value of a statement. For example, if we now specify that

$$\begin{aligned} P &: \pi \text{ is a real number}, \\ \text{and } Q &: (3 \neq 4), \end{aligned}$$

then, according to the truth table above, the compound statement

$$P \wedge Q : (\pi \text{ is a real number}) \wedge (3 \neq 4),$$

must be true as both of its components are true. On the other hand, the statement

$$(\pi \text{ is a real number}) \wedge (3 = 4)$$

is false as the component $(3 = 4)$ is false.

Proof Method
$A \wedge B$

We may also devise methods for proving compound statements by using truth tables. To prove that a statement of the form $A \wedge B$ is true, we must establish, separately, that both A is true and B is true.

On the other hand, showing either A is false or B is false is enough to conclude that $A \wedge B$ must be false.

Definition 3.3.3
OR

The definition of A **OR** B, written $A \vee B$, is

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

This truth table establishes that $A \vee B$ is false only when A and B are both false.

This is an opportune moment to highlight the difference between mathematical language and the English language. In English, we often use the word "or" to dictate exclusivity. For example, a single coin toss will result in a "head" *or* a "tail". Here, we are implying that a coin cannot land with both of its faces ("head" *and* "tail") showing. Similarly, when we defined *statements*, we said that a statement must be either true *or* false. Once again, we implicitly meant that a statement cannot be both true and false at the same time.

Unfortunately, we also often use the word English word "or" in an inclusive setting. For example, if you are ordering coffee at your local coffee shop, you may be asked whether you would like "milk *or* sugar" in your beverage. In this setting, you are free to choose just milk, just sugar, or a combination of both milk *and* sugar in your coffee. As a result, there is some ambiguity about how the word "or" is used in English, and we may have to rely on the context to fully understand how it is being used.

Fortunately, however, mathematicians detest ambiguity in the language of mathematics. For instance, we must always keep in mind that the logical $A \vee B$ results in a true statement when A is true, B is true or both are true. In mathematics, *OR* is inclusive.

Example 1

Each of the following statements are true since at least one of the components is true.

1. (π is a real number) $\vee$ $(3 \neq 4)$.
2. (π is a real number) $\vee$ $(3 = 4)$.
3. (π is an integer) $\vee$ $(3 \neq 4)$.

On the other hand, the statement

$$(\pi \text{ is an integer}) \vee (3 = 4)$$

is false as both components are false.

Proof Method

$A \vee B$

To prove that a statement of the form $A \vee B$ is true, it is enough to establish any one of the statements A or B to be true. On the other hand, to show $A \vee B$ is false, we must show that both A is false and B is false.

3.4 More Complicated Statements

We may now combine more than one logical operator to form more complicated compound statements. We can construct truth tables for compound statements by evaluating parts of the compound statement separately and then combine their corresponding truth value to evaluate the truth value of the overall statement. Consider the following truth table which shows the truth values of $\neg(A \vee B)$ for all possible combinations of truth values of the component statements A and B. (Brackets serve the same purpose in logical expressions as they do in arithmetic: they specify the order of operation.)

Example 2

Construct a truth table for $\neg(A \vee B)$.

A	B	$A \vee B$	$\neg(A \vee B)$
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

In the first row of the table A and B are true, so using the definition of OR, the statement $A \vee B$ is true. Since the negation of a true statement is false, $\neg(A \vee B)$ is false, which appears in the last column of the first row. Take a minute to convince yourself that each of the remaining rows is correct.

Example 3

Construct a truth table for $(\neg A) \wedge (\neg B)$.

A	B	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Exercise 1

Suppose A, B and C are statements.

1. Construct a truth table for $(A \wedge \neg B) \vee C$.
2. Suppose A and B are true, and C is false. What is the truth value of $A \wedge (B \vee C)$?

3.5 Equivalent Logical Expressions

Notice that the effect of taking *double negation*, that is $\neg(\neg A)$, is exactly what we expect: the truth value of $\neg(\neg A)$ is the same as that of A. Thus, *logically*, there is no difference between considering the original statement A or the compound statement $\neg(\neg A)$. We say that A and $\neg(\neg A)$ are *logically equivalent*, and express this idea by writing

$$\neg(\neg A) \equiv A.$$

Definition 3.5.1

Logically equivalent

Two compound statements, say S_1 and S_2, are **logically equivalent** if they have the same truth values for all possible states of their component statements. We write $S_1 \equiv S_2$ to mean S_1 is logically equivalent to S_2.

Essentially, $S_1 \equiv S_2$ tells us that their truth values are *perfectly correlated* - one cannot be true while the other is false, and vice versa. Thus, logically, there is no reason to distinguish between S_1 and S_2.

Proof Method

Logically Equivalent Statements

Equivalent statements are enormously useful in proofs. Suppose you wish to prove S_1 but are having difficulty. If there is a simpler statement S_2 and $S_1 \equiv S_2$, then you can prove S_2 instead. In proving S_2, you will have proved S_1 as well.

Let us look back at examples 2 and 3 from the previous section.

Example 4

Construct a single truth table for $\neg(A \vee B)$ and $(\neg A) \wedge (\neg B)$. Are these statements logically equivalent?

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Since the columns representing $\neg(A \vee B)$ and $(\neg A) \wedge (\neg B)$ are identical for the corresponding truth values of the components, we can conclude that

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

Exercise 2

Use truth tables to show that for statements A, and B, the **Commutativity Laws** hold. That is

1. $A \vee B \equiv B \vee A$
2. $A \wedge B \equiv B \wedge A$

Using a truth table is not the only way to determine whether two statements are logically equivalent; we may also use established equivalences to obtain new ones. In general, if we can establish that $S_1 \equiv S_2$ and $S_2 \equiv S_3$, then we may immediately conclude that $S_1 \equiv S_3$.

Example 5

Suppose A and B are arbitrary statements. Use the fact that we have established

1. $\neg(\neg A) \equiv A$ (double negation)
2. $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$ (negation of OR)

to prove that

$$(\neg A) \vee (\neg B) \equiv \neg(A \wedge B)$$

without using a truth table.

Solution. To establish the logical equivalence between two statements, we must start with one statement and convince the reader that it is logically equivalent to the other. Let us start with the statement to the left of the $\equiv$ sign.

$$\begin{aligned}(\neg A) \vee (\neg B) &\equiv \neg\left[\neg\left((\neg A) \vee (\neg B)\right)\right] \quad \text{(double negation)}\\ &\equiv \neg\left[(\neg(\neg A)) \wedge (\neg(\neg B))\right] \quad \text{(negation of OR)}\\ &\equiv \neg\left[A \wedge B\right] \quad \text{(double negation).}\end{aligned}$$

Note that the final statement is $\neg(A \wedge B)$, exactly what appears on the right of the $\equiv$ sign. Since we managed to arrive at $\neg(A \wedge B)$ from $(\neg A) \vee (\neg B)$ with the help of established logical equivalences, we may conclude that $(\neg A) \vee (\neg B) \equiv \neg(A \wedge B)$.

Exercise 3 Construct a single truth table for $\neg(A \wedge B)$ and $(\neg A) \vee (\neg B)$ and verify that these statements are indeed equivalent.

The preceding examples demonstrate **De Morgan's Laws**.

Proposition 1 **(De Morgan's Laws (DML))**

For any two statements A and B

1. $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$
2. $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$

Self Check 1 Make sure you are able to solve the following problems.

1. Use truth tables to show that for statements A, B and C, the **Associativity Laws** hold. That is
   (a) $A \vee (B \vee C) \equiv (A \vee B) \vee C$
   (b) $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
2. Use truth tables to show that for statements A, B and C, the **Distributivity Laws** hold. That is
   (a) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
   (b) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

3.6 More Examples and Practice

Example 6 Here are a few more examples.

1. Use a truth table to determine whether or not $A \vee (B \wedge C)$ is equivalent to $(A \vee B) \wedge (A \vee C)$.

A	B	C	$B \wedge C$	$A \vee (B \wedge C)$	$A \vee B$	$A \vee C$	$(A \vee B) \wedge (A \vee C)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Since the columns associated with the statements $A \vee (B \wedge C)$ and $(A \vee B) \wedge (A \vee C)$ are identical, the two statements are equivalent. That is, $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.

2. Suppose A is the statement

$$\text{A} : (5 = 2) \vee (3 < 6 < 7).$$

Provide a statement that is logically equivalent to NOT A, but does not contain the word "not" or the negation ($\neg$) symbol (negative symbols such as $\neq, \notin$, etc. are allowed).

Solution. Here, we are asked to *negate* statement A.

There are two obvious components to statement A, namely $(5 = 2)$ and $(3 < 6 < 7)$, that are connected by the logical operator OR ($\vee$). According to *De Morgan's Laws* (*DML*), we would have

$$\text{NOT } A \equiv \neg(5 = 2) \wedge \neg(3 < 6 < 7).$$

However, we are not allowed to use the $\neg$ symbol, so we shall use $(5 \neq 2)$ instead of $\neg(5 = 2)$. At this point, we must realize that $(3 < 6 < 7)$ is actually an abbreviated form of compound statement $(3 < 6) \wedge (6 < 7)$. Thus, using (*DML*) again, we have

$$\neg(3 < 6 < 7) \equiv \neg(3 < 6) \vee \neg(6 < 7).$$

Finally, we may replace $\neg(3 < 6)$ by $(3 \geq 6)$ and $\neg(6 < 7)$ by $(6 \geq 7)$. Collecting all this analysis in one place, we finally get that

$$\text{NOT } A \equiv (5 \neq 2) \wedge [(3 \geq 6) \vee (6 \geq 7)].$$

Chapter 4

Implications and the Direct Proof

4.1 Objectives

The technique objectives are:

1. Understand the definition of $A \implies B$.
2. Use the truth value of $A \implies B$ to draw inferences about A and B.
3. Learn the Direct Proof technique.

4.2 Implications: Hypothesis $\implies$ Conclusion

We have just started our journey towards understanding mathematical statements and developing their proofs. So far, we have discovered that a complicated statement may often be broken down into simpler components, and the connection between these components may then be leveraged to produce a proof of the complicated statement. We would now like to start developing the theory of *how* to prove statements.

The most common type of statement we will prove is an **implication**. An implication is a compound statement that has two components, let's call these components A and B for the time being.

Definition 4.2.1

Implication, Hypothesis, Conclusion

An **implication** is commonly read as A implies B and is written symbolically as $A \implies B$. The definition of $A \implies B$ is given by the following truth table

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

The component A located to the left of the $\implies$ arrow is known as the **hypothesis**, while the component B on the right is known as the **conclusion**.

When translating the mathematical statement $A \Longrightarrow B$ into an English sentence, we often use conditional sentences such as

$$\text{If } A \text{ is true, then } B \text{ must be true}$$

or more commonly written as

$$\text{If } A, \text{then } B.$$

Conditional statements such as implications have been around since the ages of classical Greek philosophy, and it may be worth mentioning that the terms *hypothesis* and *conclusion* are inherited from their usage in logic and philosophy. In English language, the structure of implications is quite easy to understand. The *hypothesis* (also known as *supposition, premise, protasis*, etc.) appears sandwiched between the "if" and the "then". The *conclusion* (also often called *proposition, inference, apodosis*, etc.) shows up after the "then" and states the consequence of the hypothesis condition being met.

Example 1 For example, consider the following statement:

If I read this chapter thoroughly, then I will be able to prove implications.

Here, the hypothesis is "I read this chapter thoroughly" and the conclusion is "I will be able to prove implications."

Example 2 Let x be a positive real number. Identify the hypothesis and the conclusion of the following implication:

If $x > 1$ then $x^2 > x$.

Hypothesis: $x > 1$

Conclusion: $x^2 > x$.

REMARK

1. We usually only use true implications in our day-to-day usage of conditional sentences. False implications (e.g., if the earth is a planet, then all people are mushrooms) are rare. We must always keep in mind that the condition imposed on an implication being false is that the hypothesis must be true while the conclusion is false.

2. Another point of confusion often arises from the last two rows in the definition of $A \Longrightarrow B$:

A	B	$A \Longrightarrow B$
F	T	T
F	F	T

Inexperienced mathematicians often look at these rows and ask questions such as

(a) How can "false" imply "true"?
(b) How is it possible that "false" implies both "true" and "false" at the same time?

These questions arise from our difficulty in appreciating the fact that the truth table is simply *defining* $A \implies B$. The purpose of the truth table is to establish the truth value of $A \implies B$ depending on the state of the pair (A, B). The states (F, T) and (F, F) are just possible truth values for the pair (A, B), and we assign $A \implies B$ to be true for these states.

Example 3 The implications

If $(1 + 1 = 4)$ then $(\pi = 3)$

and

If $(1 + 1 = 4)$ then $(\pi \neq 3)$

are both true.

4.3 Rules of Inference

We may try to use to truth value of $A \implies B$ to obtain information about the truth values of the components A and B respectively. This is a nice exercise in logic, and helps us understand how to use previously proven propositions towards proving new ones.

It will be useful for us to remember the truth table for $A \implies B$ in this section.

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

For example, from the second row of the truth table, whenever $A \implies B$ is false, we immediately determine that A must be true and B must be false.

On the other hand, suppose $A \implies B$ is true. Perhaps we also know that A is true, what can we deduce from this piece of information? From the definition of $A \implies B$, we see that the only row where both $A \implies B$ is true and A is true is the first row. Thus, we may deduce that B must also be true.

Example 4 Consider the following examples that illustrate these rules of inference.

1. In each of the given cases, assume that it has been established that the given implication is true. For the given statements **P** and **Q**, when **P** is true, then discuss whether we can determine if **Q** must be true or not.

   (a) **Implication** : If I do every problem in the text book, then I will learn discrete mathematics.
   P : I learnt discrete mathematics.
   Q : I must have done every problem in the text book.

   Solution: We are told that the implication is true, and that **P** is true. However, **P** only tells us that the conclusion of the implication is satisfied, thus it is still possible for the hypothesis, **Q**, to be either true or false.

   For example, I could have learnt discrete mathematics by other means such as attending relevant lectures, reading different books, etc, rather than solving every problem in the text book.

   (b) **Implication** : If the Earth were flat, then Columbus would not set sail.
   P : Columbus set sail.
   Q : The earth is not flat.

   Solution: Given that **P** is true, this means that the conclusion of the implication is false, but the implication itself is true. From the definition of an implication, the only way this is possible is when the hypothesis of the implication is also false. This means $\neg\mathbf{Q}$ must be false, so this time we may actually deduce that **Q** is true.

2. Let a and b be real numbers. Is it possible for the following implications to be false?

   (a) If $a < b$ and $b < a$ then $a = b$.

   Solution: The hypothesis: "$a < b$ and $b < a$" can never be true for two real numbers a and b. Thus, the hypothesis is always false and so the implication can never fail.

   (b) If $a + b = 2$ then $a - b = 0$.

   Solution: We have no restrictions on a and b other than that they are real numbers. So if we consider the case when $a = 4$ and $b = -2$, then $a + b = 4 + (-2) = 2$ is true, so the hypothesis is satisfied. However, in this case $a - b = 4 - (-2) = 4 + 2 = 6 \neq 0$, and thus the conclusion fails. Hence, for this specific case, the implication is false.

   (c) If $a = 0$ then $a \cdot b = 0$.

   Solution: We know that almost all real numbers are non-zero, and as long as the hypothesis is not satisfied, the implication would be true.

   The only time the hypothesis is true happens to be when a is zero. In that case, in the conclusion, would have $a \cdot b = (0) \times (b) = 0$. This means that when the hypothesis is true, the conclusion is also true, and thus the implication is true.

   Since there is no case where the hypothesis is true but the conclusion is false, this implication can never be false.

4.4 Proving Implications: The Direct Proof

There are a few different methods for proving that an implication is true. In this section, we will focus on the most obvious method: the direct proof.

Proof Method
Direct Proof

To *prove* the implication "A implies B" is true, you assume that A is true and you use this assumption to show that B is true. Statement A is what you start with. Statement B is where you must end up.

Suppose a, b and c are real numbers. You may have seen the following proposition in high school.

Proposition 1 If $a \neq 0$ and $b^2 = 4ac$ and, then $x = -\frac{b}{2a}$ is a solution to $ax^2 + bx + c = 0$.

We shall prove this proposition through a direct proof, but before that, let us start by identifying the hypothesis and the conclusion of the implication above.

Hypothesis: $a \neq 0$ and $b^2 = 4ac$

Conclusion: $x = -\frac{b}{2a}$ is a solution to $ax^2 + bx + c = 0$

Our approach will be to assume "$a \neq 0$ and $b^2 = 4ac$" is true, and try to use this assumption to verify that "$x = -\frac{b}{2a}$ is a solution to $ax^2 + bx + c = 0$" is also a true statement. To check whether a particular value of x solves some equation in the variable x, we need to substitute the proposed value of x in the equation and check that the left side and the right side of the equation evaluates to the same number.

Proof of Proposition 1: Assume that $(a \neq 0) \wedge (b^2 = 4ac)$ is true. This means that the components $a \neq 0$ and $b^2 = 4ac$ are both true.

Since $a \neq 0$, therefore we are allowed to divide by a, and thus the fraction $-\frac{b}{2a}$ is a real number. Substitute $x = -\frac{b}{2a}$ into the left side of $ax^2 + bx + c = 0$ and simplify to get

$$\begin{aligned} ax^2 + bx + c &= a\left(-\frac{b}{2a}\right)^2 + b\left(-\frac{b}{2a}\right) + c \\ &= a\left(\frac{b^2}{4a^2}\right) - \frac{b^2}{2a} + c \\ &= \frac{b^2}{4a} - \frac{b^2}{2a} + c \\ &= \frac{b^2 - 2b^2 + 4ac}{4a} \\ &= \frac{-b^2 + 4ac}{4a}. \end{aligned}$$

Using the assumption that $b^2 = 4ac$, we get that $-b^2 + 4ac$ must equal zero. Hence the left side of the equation evaluates to zero. The right side is already zero, so the two sides match.

Therefore, $x = -\frac{b}{2a}$ is a solution to $ax^2 + bx + c = 0$. $\square$

REMARK

A direct proof of the statement $A \implies B$ should always start with the sentence

> Assume A is true

and the final line of the proof should be

> Therefore B must be true.

All our assumptions should be stated explicitly. At no point during the proof should we give the impression that conclusion, i.e., statement B, has been assumed to be true. It is best to avoid writing statement B until the last line of the proof.

We will see lots of direct proofs in this course, presented in different contexts.

Example 5 Suppose n is an integer. Consider the implication

> If n^2 is even, then n is even.

What is wrong with the following "attempted proof" of the given implication?

Attempted Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Assume n^2 is even.
2. Then $n^2 = 2k$ of some integer k.
3. Let $n = 2l$ for some integer l.
4. Hence, n must be even. □

Solution: In the "attempted proof", we cannot yet justify how we obtain step 3 from any of the previous steps. In fact, in step 3, we are actually assuming that n can be written as $2l$, but this is true only when n is even. Therefore, we have inherently assumed that the conclusion is true instead of deducing it from the hypothesis.

4.5 Negating an Implication

An equivalent way to express an implication is demonstrated in the following example.

Example 6 Construct the truth table for $(\neg A) \vee B$ and demonstrate that this statement is logically equivalent to $A \implies B$.

Solution: Using the following truth table

A	B	$A \implies B$	$\neg A$	$(\neg A) \vee \neg B$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

we get that $(\neg A) \vee B \equiv A \implies B$.

Perhaps the most important aspect of the equivalence $(\neg A) \vee B \equiv A \implies B$ is that it allows us to **negate an implication** through its components. More specifically, using the rule for double negations and *De Morgan's Laws* (*DML*), we get

$$\neg\left[(\neg A) \vee B\right] \equiv A \wedge (\neg B).$$

Thus, $\neg(A \implies B)$ is logically equivalent to $A \wedge (\neg B)$. Notice that the negation of an implication is actually an AND statement.

Example 7 Let x, y and z be integers. Negate the implication

If $x < z < y$ then $x^2 < z^2 < y^2$.

Solution: $(x < z < y)$ and $(x^2 \geq z^2$ or $z^2 \geq y^2)$.

Example 8 John wants to show that for any real number x, the following implication

If $x^2 < 0$ then $x^2 + 1 > 2$

is false. He knows that to disprove $A \implies B$, he must prove that $\neg(A \implies B)$ is true. Furthermore, he recalls that the negation of $A \implies B$ can be written in terms of A and $\neg B$, but he has forgotten the exact relation. Nevertheless, he attempts the following disproof.

Attempted Disproof: Assume $x^2 < 0$. Then adding 1 to both sides of the inequality gives $x^2 + 1 < 1$. Thus $x^2 + 1 > 2$ cannot be true. The hypothesis being true gives us that the conclusion is false, hence the given implication must be false. $\square$

1. Discuss why the implication "If $x^2 < 0$ then $x^2 + 1 > 2$" is true for all real numbers x.

   Solution: Since x is a real number, the hypothesis $x^2 < 0$ is never true, so the implication is always going to be true.

2. Identify the logical flaw in John's attempted disproof.

   Solution: John's attempt has proven "if $x^2 < 0$ then $x^2 + 1 \leq 2$", which is not the correct negation of the given implication, and thus does not allow us to conclude whether the original statement is true or false.

   The correct negation in this case would be "$x^2 < 0$ and $x^2 + 1 \leq 2$", which is false because "$x^2 < 0$" is always false.

4.6 Practice

1. Determine whether $A \implies \neg B$ logically equivalent to $\neg(A \implies B)$.

2. Assume that it has been established that the following implication is true:

   If I don't see my advisor today, then I will see her tomorrow.

   For each of the statements below, determine if it is true or false, or explain why truth value of the statement cannot be determined.

   (a) I don't meet my advisor both today and tomorrow.

   (b) I meet my advisor both today and tomorrow.

   (c) I meet my advisor either today or tomorrow (but not on both days).

3. Four friends: Alex, Ben, Gina and Dana are having a discussion about going to the movies. Ben says that he will go to the movies if Alex goes as well. Gina says that if Ben goes to the movies, then she will join. Dana says that she will go to the movies if Gina does. That afternoon, exactly two of the four friends watch a movie at the theatre. Deduce which two people went to the movies.

4. Let n be an integer. Prove that if $1 - n^2 > 0$, then $3n - 2$ is an even integer.

5. Let n be an integer. Prove that if n is odd, then n^3 is also odd.

6. Let a and b be two integers. Prove each of the following statements about a and b.

   (a) If $ab = 4$, then $(a - b)^3 - 9(a - b) = 0$.

   (b) If a and b are positive, then $a^2(b + 1) + b^2(a + 1) \geq 4ab$.

Chapter 5

Analysis of a Proof

5.1 Objectives

The learning objectives are:

1. Understand what it means to assume $a \mid b$.
2. Learn how to prove $a \mid b$.
3. Read a direct proof: *Transitivity of Divisibility*.
4. Learn how to structure the analysis of a proof.
5. Carry out the analysis of a proof.

We have have just learned how to prove an implication using a direct proof. In this chapter, we shall analyze the proof of the proposition known as Transitivity of Divisibility, and will recognize it as a direct proof. First, let us introduce the concept of divisibility.

5.2 Divisibility of Integers

For the time being, we will focus exclusively on integers. Division turns out to be a fairly complicated operation on integers. If we try to divide 6 by 2, we get the integer 3 as a result; but if we divide say 6 by 4, then the result $\frac{6}{4} = 1.5$ is no longer an integer. Since we want to deal solely with integers, we are interested in learning more about the cases where the result of a division is an integer.

Definition 5.2.1
Divisibility

An integer m **divides** an integer n, and we write $m \mid n$, when there exists an integer k so that $n = km$.

If $m \mid n$, then we say that m is a **divisor** or a **factor** of n, and that n is a **multiple** of m or that n is **divisible by** m.

Example 1 Consider the following examples.

- $3 \mid 6$ since we can find an integer, 2 in this case, so that $6 = 2 \times 3$.
- $5 \nmid 6$ since no integer k exists so that $6 = k \times 5$.
- For all integers a, $a \mid 0$ since $0 = 0 \times a$. This is true for $a = 0$ as well.
- For all non-zero integers a, $0 \nmid a$ since there is no integer k so that $k \times 0 = a$.
- 1 divides all integers. This is because any integer b can be written as $b = b \times 1$.

Some comments about definitions are in order. If mathematics is thought of as a language, then definitions are the vocabulary and our prior mathematical knowledge indicates our experience and versatility with the language.

Mathematics and the English language both share the use of definitions as extremely practical abbreviations. Instead of saying "a domesticated carnivorous mammal known scientifically as *Canis familiaris*" we would say "dog." Instead of writing down "there exists an integer k so that $n = km$", we write "$m \mid n$."

However, mathematics differs greatly from English in precision and emotional content. Mathematical definitions do not allow ambiguity or sentiment.

5.2.1 Understanding the definition of Divisibility

Suppose m and n are two integers. Let us also make the assumption that m is non-zero. We would like to understand what it means:

1. **to assume** $m \mid n$. By definition, we inherently know that there must be some integer k such that $n = k \cdot m$. The value of k is unknown unless we know the values of m and n, so k simply represents the integer $\frac{n}{m}$ (note: $m \neq 0$). This k may be used in later expressions such as $k + 1$, k^2, etc., in order to obtain some desired conclusion.
2. **to prove** $m \mid n$. We must obtain an explicit example of an integer that can be multiplied with m to get n. Often, start with n and try to express it in terms of m. If we can successfully show that n is equal to an integer multiple of m, then $m \mid n$ is true. This desired multiple may be obtained from expressions involving variables that have already been defined earlier in the context of the proof.

5.2.2 Transitivity of Divisibility

We will now look at a proposition involving divisibility.

Proposition 1 **(Transitivity of Divisibility (TD))**

Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

When one first encounters a proposition, it often helps to work through some examples to understand the proof.

Example 2 Suppose $a = 3$, $b = 6$ and $c = 42$. Since $3 \mid 6$ ($a \mid b$) and $6 \mid 42$ ($b \mid c$), Transitivity of Divisibility allows us to conclude that $3 \mid 42$ ($a \mid c$).

Now you might immediately know that $3 \mid 42$. The strength of this proposition is that it works for any integers a, b, c that satisfy the condition "$a \mid b$ and $b \mid c$", not just for the particular integers of our example.

Now take a minute to read the following proof of Transitivity of Divisibility.

Proof: Assume $a \mid b$ and $b \mid c$. Since $a \mid b$, there exists an integer r so that $ra = b$. Since $b \mid c$, there exists an integer s so that $sb = c$. Substituting ra for b in the previous equation, we get $(sr)a = c$. Since sr is an integer, $a \mid c$. $\square$

The proposition Transitivity of Divisibility involves an implication that has some instances of *divisibility of integers* (i.e., $m \mid n$) both in the hypothesis and in the conclusion. The proof highlights the difference between assuming $m \mid n$ versus showing $m \mid n$.

Self Check 1 From the proof above:

1. identify the core proof technique,
2. list all the assumptions being made, and
3. justify each step. Be sure to add any steps that are missing.

5.3 Analyzing the Proof of *TD*

Let us analyze the proof of the Transitivity of Divisibility in detail because it will give us some sense of how to analyze proofs in general.

We will do a line by line analysis, so to make our work easier, we will write each sentence on a separate line. What we do now will seem like overkill but it serves two purposes. It gives us practice at justifying every line of a proof, and a structure that we can use for other proofs.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Assume $a \mid b$ and $b \mid c$.
2. Since $a \mid b$, there exists an integer r so that $ra = b$.
3. Since $b \mid c$, there exists an integer s so that $sb = c$.
4. Substituting ra for b in the previous equation, we get $(sr)a = c$.

5. Since sr is an integer, $a \mid c$.

□

Analysis of Proof We begin by explicitly identifying our assumptions and our desired conclusion.

Assumptions: a, b and c are integers. $a \mid b$ and $b \mid c$.

Desired Conclusion: $a \mid c$.

Core Proof Technique: Work forwards from the hypothesis (Direct Proof).

Preliminary Material: The definition of *divides*. An integer m **divides** an integer n, and we write $m \mid n$, if there exists an integer k so that $n = km$.

Let us try to justify each sentence of the existing proof.

Sentence 1 *Assume $a \mid b$ and $b \mid c$.*

Here, the author clearly indicates that the hypothesis is assumed true. This establishes the core proof technique.

Sentence 2 *Since $a \mid b$, there exists an integer r so that $ra = b$.*

In this sentence, the author of the proof uses the hypothesis $a \mid b$ and the definition of divides. Note that the author is using the symbol 'r' for the integer that multiplies with a to produce b. The value of r is unknown, but its existence is known by our assumption.

Sentence 3 *Since $b \mid c$, there exists an integer s so that $sb = c$.*

In this sentence, the author uses the hypothesis $b \mid c$ and the definition of divides. Here, the author uses a different symbol, 's', to designate the integer whose product with b will give c.

Note that we cannot use the symbol 'r' again to say $rb = c$. Once we have used r in sentence 1, its role is fixed so that $ra = b$, and thus rb has a fixed value. Since c can take any integer value, therefore rb is not an appropriate expression for c.

Sentence 4 *Substituting ra for b in the previous equation, we get $(sr)a = c$.*

Here, the author works forward using arithmetic. The actual work is:

$$c = sb \text{ and } b = ra \text{ implies } c = s(ra) \text{ which implies } c = (sr)a.$$

Sentence 5 *Since sr is an integer, $a \mid c$.*

Lastly, the author uses the definition of divides. In this case, the m, k and n of the definition apply to the a, sr and c of the proof. It is important to note that sr is an integer, otherwise the definition of *divides* does not apply.

At the end of each proof, you should be able to identify where each part of the hypothesis was used. It is obvious where $a \mid b$ and $b \mid c$ were used. The hypothesis "a, b and c are integers" was needed to allow the author to use the definition of divides.

This completes the analysis of our first proof.

Chapter 6

Discovering Proofs

6.1 Objectives

The learning objectives are:

1. Discover a proof using the Direct Proof technique.
2. Prove the *Divisibility of Integer Combinations*.
3. Prove the *Bounds By Divisibility*.
4. Read and analyze a proof.

6.2 Divisibility of Integer Combinations

In the previous chapter we used the proof techniques that we have learned so far to analyze a proof of the *Transitivity of Divisibility*.

When we define a new mathematical concept, such as divisibility, we are usually eager to find out what kind of properties it satisfies. For example, we know that 5 divides both 10 and 15. Then, according to the *Transitivity of Divisibility* (*TD*), 5 would divide all multiples of 10, and similarly, 5 would also divide all multiples of 15. What if we add a multiple of 10 to a multiple of 15, would 5 divide the result? For instance, does 5 divide

$$(10 \times 3) + (15 \times 4) = 90?$$

The answer is a resounding 'yes'! In fact, it is not very difficult to believe that 5 would divide all possible *integer combinations* of 10 and 15 (i.e., any expression of the form $10x + 15y$, where x and y are integers). May be this can be generalized to a new result:

Proposition 1 **(Divisibility of Integer Combinations (DIC))**

Let a, b and c be integers. If $a \mid b$ and $a \mid c$, then for any integers x and y, $a \mid (bx + cy)$.

However, we still need to prove this result. In this chapter, we will *discover* a proof of the above proposition.

6.3 Discovering a Proof of DIC

Discovering a proof of a statement is generally hard. There is no recipe for this, but there are some tips that may be useful, and as we go on through the course, you will learn specific techniques.

Let us begin with a numeric example.

Example 1 Suppose $a = 3$, $b = 6$ and $c = 27$. Then, the proposition claims that for any integers x and y, $3 \mid (6x + 27y)$. That is, 3 divides any integer combination of 6 and 27. You might say, "That's obvious. Just take a common factor of 3 from $6x + 27y$." That is

$$6x + 27y = 3(2x + 9y)$$

That observation is very suggestive of the proof of the Divisibility of Integer Combinations.

The very first thing to do when proving a statement is to explicitly identify the assumptions and the desired conclusion. Let's do that for the *Divisibility of Integer Combinations* (*DIC*).

Assumptions: $a, b, c \in \mathbb{Z}$, $a \mid b$ and $a \mid c$.

Desired Conclusion: For any choice of $x, y \in \mathbb{Z}$, $a \mid (bx + cy)$

Since we are *proving* an implication, not *using* it, we assume that the hypothesis is true, and then demonstrate that the conclusion is true. You may recognize this straightforward approach to be a **Direct Proof**. However, in actually discovering a proof we do not need to work only forwards from hypothesis. We can work backwards from the conclusion and meet somewhere in the middle. When writing the proof we must ensure that we begin with the hypothesis and end with the conclusion.

Whether working forwards or backwards, it is best to proceed by asking questions. When working backwards, we may ask

> What mathematical fact would allow us to deduce the conclusion?

For example, in the proposition under consideration we could ask

> What mathematical fact would allow us to deduce that $a \mid (bx + cy)$?

The answer tells us what to look for or gives us another statement we can work backwards from. In this case the answer would be

> If there exists an integer k so that $bx + cy = ak$, then $a \mid (bx + cy)$.

Note that the answer makes use of the definition of *divides*. Let's record this statement as part of a proof in progress.

Proof in Progress

1. *To be completed.*

2. Since there exists an integer k so that $bx + cy = ka$, then $a \mid (bx + cy)$.

Now we could ask the question

> How can we find such a k?

The answer is not obvious so let's turn to working forwards from the hypothesis. In this case our standard two questions are

> Have we seen something like this before?
> What mathematical fact can we deduce from what we already know?

We have seen $a \mid b$ in an hypothesis before. Twice actually, once in the proof of the Transitivity of Divisibility and once in the prior example. Just as was done in the proof of the Transitivity of Divisibility, we can use $a \mid b$ and the definition of divisibility to assert that

> There exists an integer r such that $b = ra$.

and we'll add this to the proof in progress.

Proof in Progress

1. Since $a \mid b$, there exists an integer r such that $b = ra$.
2. *To be completed.*
3. Since there exists an integer k so that $bx + cy = ka$, then $a \mid (bx + cy)$.

We also know that $a \mid c$ so we can use the definition of divisibility again to assert that

> There exists an integer s such that $c = sa$.

and we will add this to the proof in progress as well.

Proof in Progress

1. Since $a \mid b$, there exists an integer r such that $b = ra$.
2. Since $a \mid c$, there exists an integer s such that $c = sa$.
3. *To be completed.*
4. Since there exists an integer k so that $bx + cy = ka$, then $a \mid (bx + cy)$.

Hmmm, what now? Let's look again at the last sentence. There is a $bx + cy$ in the last sentence and an algebraic expression for b and c in the first two sentences. Substituting gives

$$bx + cy = (ra)x + (sa)y$$

and factoring out the a gives

$$bx + cy = (ra)x + (sa)y = a(rx + sy)$$

Does this look familiar? We factored in our numeric example and we are factoring here. If we let $k = rx + sy$ then, because multiplying integers gives integers and adding integers gives integers, k is an integer. Hence, there exists an integer k so that $bx + cy = ak$. That is, $a \mid (bx + cy)$.

We are done. Almost. We have discovered a proof but this is rough work. We must now write a formal proof. Just like any other writing, the amount of detail needed in expressing your thoughts depends upon the audience. A proof of a statement targeted at an audience of professional specialists in algebra will not look the same as a proof targeted at a high school audience. When you approach a proof, you should first make a judgement about the audience. Write for your peers. That is, write your proof so that you could hand it to a classmate and expect that they would understand the proof.

Proof: Assume that $a \mid b$ and $a \mid c$. Since $a \mid b$, there exists an integer r such that $b = ra$. Since $a \mid c$, there exists an integer s such that $c = sa$. Let x and y be any integers. Now $bx + cy = (ra)x + (sa)y = a(rx + sy)$. Since $rx + sy$ is an integer, it follows from the definition of divisibility that $a \mid (bx + cy)$. $\square$

Note that this proof does not reflect the discovery process, and it is a Direct Proof. It begins with the hypothesis and ends with the conclusion.

Before we leave this proposition, let's consider the significance of the requirement that "x and y are integers". Suppose, as in our numeric example, $a = 3$, $b = 6$ and $c = 27$. If we choose $x = 3/2$ and $y = 1/4$, then $ax + by = 45/4$ which is not even an integer! This simple example emphasizes the importance of the domain of the variables x and y in the conclusion.

Exercise 1 Let a, b, c and d be integers. Prove the following statements.

1. If $a \mid c$ and $b \mid d$, then $ab \mid cd$.
2. If $d \mid (b - a)$ and $d \mid (c - b)$ then $d \mid (c - a)$.

6.4 Proof of Bounds by Divisibility

Here is another proposition and proof.

Proposition 2 **(Bounds By Divisibility (BBD))**

Let a and b be integers. If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

Proof: Since $a \mid b$, there exists an integer q so that $b = qa$. Since $b \neq 0$, $q \neq 0$. But if $q \neq 0$, $|q| \geq 1$. Hence, $|b| = |qa| = |q||a| \geq |a|$. □

Let's analyze this proof. First, we will rewrite the proof line by line.

Proof: (For reference purposes, each sentence of the proof is written on a separate line.)

1. Since $a \mid b$, there exists an integer q so that $b = qa$.
2. Since $b \neq 0$, $q \neq 0$.
3. But if $q \neq 0$, $|q| \geq 1$.
4. Hence, $|b| = |qa| = |q||a| \geq |a|$.

□

REMARK

When reading a proof of a proposition, you should attempt to do the following.

1. *Identify all the assumptions that have been made.* Sometimes the assumptions may not be explicitly stated in the proof, but you should try to locate them anyway. Quite often there are mistakes in incorrect proofs because of unjustified assumptions, so it is a good practice to keep track of all the assumptions and highlight where each assumption is being used.
2. *Record any preliminary material used in the proof*, usually definitions or propositions that have already been proved. As a rule of thumb for Math 135, in our proofs, we are allowed to use any definition that has been stated and any result that has been proven in the duration of the course, unless instructed otherwise.
3. *Justify each step* with reference to the definitions, previously proved propositions or techniques used. *Add missing steps* where necessary and justify these steps as well. If a particular step cannot be justified, then the proof is most definitely incorrect.
4. *Identify the core proof technique.* Although we have not seen this yet, throughout this course we will learn several proof techniques and then apply them in different mathematical scenarios. You should try to identify the technique that is being employed in the proof.

Now the analysis.

Analysis of Proof As usual, we begin by explicitly identifying the assumptions and the desired conclusion.

Hypothesis: a and b are integers. $a \mid b$ and $b \neq 0$.

Conclusion: $|a| \leq |b|$.

Core Proof Technique: Direct Proof.

Preliminary Material: The definition of *divides*.

Now we justify every sentence in the proof.

Sentence 1 *Since $a \mid b$, there exists an integer q so that $b = qa$.*

In this sentence, the author of the proof uses the hypothesis $a \mid b$ and the definition of divides.

Sentence 2 *Since $b \neq 0$, $q \neq 0$.*

If q were zero, then $b = qa$ would imply that b is zero. So by the *Rules of Inference* (*ROI*), since b is not zero, q cannot be zero.

Sentence 3 *But if $q \neq 0$, $|q| \geq 1$.*

Since q is an integer from Sentence 1, and q is not zero from Sentence 2, $q \geq 1$ or $q \leq -1$. In either case, $|q| \geq 1$.

Sentence 4 *Hence, $|b| = |qa| = |q||a| \geq |a|$.*

Sentence 1 tells us that $b = qa$. Taking the absolute value of both sides gives $|b| = |qa|$ and using the properties of absolute values we get $|qa| = |q||a|$. From Sentence 3, $|q| \geq 1$ so $|q||a| \geq |a|$.

6.5 Examples

1. Let a, b be integers. Prove that if $a \mid b$ and $b \mid a$, then $a = \pm b$.

   Solution: Assume that $a \mid b$ and $b \mid a$. When $a = 0$ then b must also be zero since $a \mid b$ and the only integer that is divisible by 0 is 0. In that case, $a = b$ and thus $a = \pm b$ is automatically satisfied.

   Suppose $a \neq 0$. In that case, b cannot be zero either as $b \mid a$. Thus both a and b are non-zero. As $a \mid b$ and $b \neq 0$, then using *Bounds By Divisibility* (*BBD*) we have $|a| \leq |b|$. Similarly, since $b \mid a$ and $a \neq 0$, then (*BBD*) tell us that $|b| \leq |a|$.

   The only way $|a| \leq |b|$ and $|b| \leq |a|$ is satisfied is when $|a| = |b|$. Now $|a| = |b|$ implies $a = \pm b$.

   Therefore, in every possible scenario, the conclusion is satisfied, so the given implication is true.

2. Consider the following proposition about integers a and b.

   If $a^3 \mid b^3$, then $a \mid b$.

   We now give four erroneous proofs of this proposition. Identify the major error in each proof, and explain why it is an error.

   (a) Consider $a = 2, b = 4$. Then $a^3 = 8$ and $b^3 = 64$. We see that $a^3 \mid b^3$ since $8 \mid 64$. Since $2 \mid 4$, we have $a \mid b$.

   Solution: This proof uses specific examples for a and b, and therefore establishes the property only for these values of a and b, but not in general.

   (b) Since $a \mid b$, there exists $k \in \mathbb{Z}$ such that $b = ka$. By cubing both sides, we get $b^3 = k^3a^3$. Since $k^3 \in \mathbb{Z}$, $a^3 \mid b^3$.

   Solution: The conclusion is assumed to be true at the start. (In fact, this proves the converse of the proposition rather than the proposition itself.)

(c) Since $a^3 \mid b^3$, there exists $k \in \mathbb{Z}$ such that $b^3 = ka^3$. Then $b = (ka^2/b^2)a$, hence $a \mid b$.

Solution: This proof does not verify that ka^2/b^2 is an integer.

(d) Suppose $a \nmid b$. Then any multiple of a cannot divide b, so in particular, $a^3 \nmid b$. But $b \mid b^3$, so combining with $a^3 \nmid b$, we get $a^3 \nmid b^3$.

Solution: This proof applies a general rule of the form "if $x|y$ and $y \nmid z$, then $x \nmid z$", which is not a correct statement (e.g., let $x = 2, y = 4, z = 6$, then the rule does not hold).

6.6 Practice

1. Let a, b, c be integers. Prove that if $a \mid b$ then $ac \mid bc$.

2. Prove the following statement. Let $a, b, c \in \mathbb{Z}$. If $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

3. Let $a, b, c \in \mathbb{Z}$. Is the following statement true?

   $a \mid b$ if and only if $ac \mid bc$.

4. Let n be an integer. Prove that if $2 \mid (n^2 - 1)$, then $4 \mid (n^2 - 1)$.

5. Let n be an integer. if $n \mid 1$, then $n = \pm 1$.

6. Let n be an integer. Prove that if $n = 3q + 1$ or $n = 3q + 2$ for some integer q, then $3 \mid (n^2 - 1)$.

7. Let n be an integer. Prove that if $2 \mid n$ and $3 \mid n$, then $6 \mid n$.

Part II

Foundations: Sets and Quantifiers

Chapter 7

Introduction to Sets

7.1 Objectives

The technique objectives are:

1. Learn to define a set using *set-builder notation*.
2. Gain experience working with sets and set operations: *union*, *intersection* and *set-difference*.
3. Understand *Cartesian Products* of sets.

7.2 Describing a Set

We are now going to improve our understanding of some fundamental concepts. In the next two chapters, we will discover sets. Sets are foundational in mathematics and literally appear everywhere.

Definition 7.2.1
Set, Element

A **set** is a collection of objects. The objects that make up a set are called its **elements** (or **members**).

Sets can contain any type of object. Since this is a math course, we frequently use sets of numbers. But sets could contain letters, the letters of the alphabet for example, or books, such as those in a library collection. The simplest way to describe a set is to explicitly list all of its elements inside curly braces, $\{\}$, and separate individual elements with a comma.

Example 1

The following are examples of sets:

1. $\{2, 4, 6, 8\}$ lists all the positive even numbers less that 10.
2. $\{1, 2, \{1, 2, 3\}\}$ is a set that contains three elements: 1, 2 and the set $\{1, 2, 3\}$. Note that the set $\{1, 2, 3\}$ is considered a single element of $\{1, 2, \{1, 2, 3\}\}$, even though $\{1, 2, 3\}$ contains three elements itself.

3. $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ lists the symbols of the four suites in a deck of playing cards.

4. The set of natural numbers, denoted $\mathbb{N}$, lists all the positive integers starting from 1. That is,
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$
Computer scientists begin counting at 0 so the notation $\mathbb{N}$ used in a computer science context usually means the set of integers $0, 1, 2, 3, \ldots$. Be sure to note that in Math 135, we start counting our natural numbers from 1.

It is customary to use uppercase letters (S, T, U, etc.) to represent sets and lowercase letters (x, y, z, etc.) to represent elements. If x is an element of the set S, we write $x \in S$. If x is not an element of the set S, we write $x \notin S$.

Example 2

The following examples show how the notation is used:

1. Suppose $S = \{2, 4, 6, 8\}$. Then $6 \in S$, but $7 \notin S$.

2. Let $T = \{1, 2, \{1, 2, 3\}\}$. In this case, $1 \in T$, $2 \in T$ and $\{1, 2, 3\} \in T$, but $3 \notin T$.

Definition 7.2.2
Empty Set

The set $\{\ \}$ contains no elements and is known as the **empty set**. We usually use $\emptyset$ as a symbol for the empty set, that is,
$$\emptyset = \{\ \}.$$

REMARK

It is quite common for students to mistake the set $\{\emptyset\}$ as the empty set $\emptyset$. However, $\{\emptyset\}$ is actually non-empty, it contains $\emptyset$ as an element! Thus
$$\{\emptyset\} \neq \emptyset.$$

The number of elements in a finite set is called the **cardinality** of the set. For a set S, we use $|S|$ to denote its cardinality. For instance, $|\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}| = 4$, $|\{1, 2, \{1, 2, 3\}\}| = 3$ and $|\{\emptyset,\ \{\emptyset\}\}| = 2$.

The cardinality of the empty set is defined to be zero, i.e., $|\emptyset| = 0$.

Although small sets can be explicitly listed, many sets are too large to comfortably list all their elements. You may have noticed this when we introduced $\mathbb{N}$. Fortunately, a lot of sets can be defined with the help of some common rules that each of their elements must satisfy. In these cases, we employ *set-builder notation* which makes use of a *defining property* of the set.

7.2.1 Set-builder Notation

When we work with sets, we assume the existence of a very large set, known as the **universe of discourse**, usually denoted $\mathcal{U}$, that contains all the objects that we would need in the context of our work. The universe of discourse is very rarely explicitly stated, we simply assume that it exists. For example, in our work on divisibility, we will be primarily be concerned with integers, so it may be safe to assume that the set of integers $\mathbb{Z}$ is the universe of discourse, even when we don't explicitly say so.

Quite often we will come across sets whose elements satisfy some **membership criteria**. The membership criteria of a set S is simply established by a property $P(x)$ that can be evaluated for all the elements of the universe of discourse, and $P(x)$ is true if and only if x is an element of S. Thus $P(x)$ is the **defining property** of the set we are trying to describe.

Definition 7.2.3
Set-builder Notation

Suppose S is a set that has a defining property $P(x)$ for its elements, then the **set-builder notation**

$$\{x \mid P(x)\}$$

is used to describe S. The part of the description following the bar ($|$) is the defining property of the set.

Sometimes we use a colon (:) instead of a bar and write $\{x : P(x)\}$ to describe S as well.

The statement

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

is read as "The elements of S are exactly all the values of x such that $P(x)$ is true".

REMARK

The membership criteria $P(x)$ mentioned here is an example of an *open sentence*.

An **open sentence** is a sentence that contains one or more variables, where

- each variable has values that come from a designated set called the **domain** of the variable, and
- the sentence is either true or false whenever values from the respective domains of the variables are substituted for the variables.

Of course, by substituting a particular element of the domain in place of the variable in the open sentence, we get a statement.

For example, "$x > 0$" is an open sentence. If the domain of x is the set of real numbers, then for a real number, such as π, chosen and substituted for x, the sentence "$\pi > 0$" is a statement.

In the set-builder notation $S = \{x \mid P(x)\}$, the domain of x is assumed to be the universe of discourse.

Example 3 **(Set-Builder Notation)**

There are two distinct ways in which we use the set-builder notation.

1. When the universe of discourse, $\mathcal{U}$, is explicitly known, then we write

$$S = \{x \in \mathcal{U} \mid P(x)\}.$$

- The set of all even integers can be described as

$$\{n \in \mathbb{Z} : 2 \mid n\}.$$

- The set of all real solutions to $x^2 + 4x - 2 = 0$ can be described as

$$\{x \in \mathbb{R} \mid x^2 + 4x - 2 = 0\}.$$

- The set of all positive divisors of 30 can be written as

$$\{n \in \mathbb{N} : n \mid 30\}.$$

- In calculus, we often use intervals of real numbers. The **closed interval** $[a, b]$ is defined as the set

$$\{x \in \mathbb{R} \mid a \leq x \leq b\}.$$

Thus $[1, 2] = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$.

2. When the elements of the set S can be expressed in terms of other variables, then the set builder notation often looks like

$$\{f(x) \mid P(x)\},$$

where $f(x)$ is a typical element of S that has been expressed in terms of the variable x, and the defining property $P(x)$ is true if and only if $f(x)$ is an element of S.

- For example, another way of describing the set of even integers is

$$\{2k \mid k \in \mathbb{Z}\}.$$

In this example, $f(k) = 2k$ and $P(k): \quad k \in \mathbb{Z}$. Here we go over all the integer values of k, the elements of the set of even number will precisely be the values of $2k$.

- The set of rational numbers, denoted $\mathbb{Q}$, is described by

$$\left\{\frac{p}{q} \ : \ p, q \in \mathbb{Z},\ q \neq 0\right\}.$$

Once again, the elements of $\mathbb{Q}$ are fractions of the form $\frac{p}{q}$, where p and q are integers, and $q \neq 0$. Observe that when there are multiple defining properties listed for the variables, we implicitly consider these properties to be connected by an AND.

- The set described by $\{x^2 \mid x \in \mathbb{Z},\ 0 \leq x \leq 4\}$ can be explicitly listed as

$$\{0, 1, 4, 9, 16\}.$$

Example 4

Let $S = \{x \in \mathbb{R} \mid x^2 = 2\}$ and $T = \{x \in \mathbb{Q} \mid x^2 = 2\}$.

1. Describe the set S by listing its elements. What is the cardinality of S?
   Solution: $S = \{\sqrt{2}, -\sqrt{2}\}$. $|S| = 2$.
2. Describe the set T by listing its elements. What is the cardinality of T?
   Solution: $T = \emptyset$. $|T| = 0$.

Self Check 1

It usually takes some time to get used to the set-builder notation. Check to see whether you can answer the following question.

> Let T be the set of integers divisible by 5. Describe T by using the set-builder notation in at least two ways.

7.3 Set Operations - Unions, Intersections and Set-Differences

In this section we shall review some of the basic set operations that you need to be familiar with.

Definition 7.3.1
Union

The **union** of two sets S and T, written $S \cup T$, is the set of all elements belonging to either set S or set T. Symbolically we write

$$S \cup T = \{x \mid x \in S \text{ OR } x \in T\} = \{x \mid (x \in S) \vee (x \in T)\}$$

Note that when we say "set S or set T" we mean the mathematical use of *OR*. That is, the element can belong to S, T or both S and T.

Definition 7.3.2
Intersection

The **intersection** of two sets S and T, written $S \cap T$, is the set of all elements belonging to both set S and set T. Symbolically we write

$$S \cap T = \{x \mid x \in S \text{ AND } x \in T\} = \{x \mid (x \in S) \wedge (x \in T)\}$$

Definition 7.3.3
Set-Difference

The **set-difference** of two sets S and T, written $S - T$ (or $S \setminus T$), is the set of all elements belonging to S but not T. Symbolically we write

$$S - T = \{x \mid x \in S \text{ AND } x \notin T\} = \{x \mid (x \in S) \wedge (x \notin T)\}$$

Definition 7.3.4
Set Complement

Relative to a universal set $\mathcal{U}$, the **complement** of a subset S of $\mathcal{U}$, written $\overline{S}$, is the set of all elements in $\mathcal{U}$ but not in S. Symbolically, we write

$$\overline{S} = \{x \mid x \in \mathcal{U} \text{ AND } x \notin S\} = \{x \mid (x \in \mathcal{U}) \wedge (x \notin S)\}$$

If $\mathcal{U}$ is the universal set and $S \subseteq U$ then $\overline{S} = \mathcal{U} - S$.

Example 5

Let the universal set for this question be $\mathcal{U}$, the set of natural numbers less than or equal to twelve. Let T be the set of integers divisible by three and F be the set of integers divisible by five.

1. Describe T by explicitly listing the set and by using set-builder notation in at least two ways.
2. Find an element which belongs to neither T nor F.
3. Explicitly list the set $\overline{T}$.
4. Determine the sets $T \cup F$, $T \cap F$ and $\overline{T} \cup F$.

Solution:

1. Explicitly listing the set gives $T = \{3, 6, 9, 12\}$. Two set-builder descriptions of the set are $T = \{n \in \mathbb{N} : 3 \mid n, n \leq 12\}$ and $T = \{3k \mid k \in \mathbb{N}, 3k \leq 12\}$.
2. 1. There are several choices possible.
3. $\{1, 2, 4, 5, 7, 8, 10, 11\}$.
4. The sets are

$$T \cup F = \{3, 5, 6, 9, 10, 12\}, \quad T \cap F = \emptyset, \quad \overline{T} \cup F = \{1, 2, 4, 5, 7, 8, 10, 11\}.$$

Exercise 1

Consider the following proposition.

If A and B are sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.

Complete the following table and verify that the proposition holds for each of the following pairs of sets.

1. $A = \{n \in \mathbb{Z} : n \mid 30\}$ and $B = \{n \in \mathbb{Z} : n \mid 42\}$
2. $A = \{x \in \mathbb{R} \mid \sin x = 0, -2\pi \leq x \leq 2\pi\}$ and
   $B = \{x \in \mathbb{R} \mid \cos x = 0, -2\pi \leq x \leq 2\pi\}$

	$\lvert A\rvert$	$\lvert B\rvert$	$\lvert A \cap B\rvert$	$\lvert A \cup B\rvert$	$\lvert A\rvert + \lvert B\rvert - \lvert A \cap B\rvert$
(a)					
(b)					

7.4 Cartesian Products of Sets

Suppose S and T are two sets. We have already seen several ways to combine S and T to form a new set. Here is another way of doing so:

Definition 7.4.1
Cartesian Product, Ordered Pair

The **Cartesian product** of S and T is defined to be the set

$$S \times T = \{(x, y) \mid x \in S,\ y \in T\}.$$

Each element of $S \times T$ is an **ordered pair** of the form (x, y), where the first element of the pair belongs to S and the second element belongs to T. For two ordered pairs (x, y) and (a, b) to be equal, we must have $x = a$ and $y = b$. So, if $x \neq y$, then the pair (x, y) is different from the pair (y, x).

Example 6

Let $S = \{4, 5\}$ and $T = \{n \in \mathbb{N} \ :\ n \mid 6\}$. By explicitly listing all the elements of each set, we have

$$T = \{1, 2, 3, 6\},$$

and so

$$S \times T = \{(4, 1), (4, 2), (4, 3), (4, 6), (5, 1), (5, 2), (5, 3), (5, 6)\}$$

whereas

$$T \times S = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5), (6, 4), (6, 5)\}.$$

As this example shows, typically

$$S \times T \neq T \times S.$$

REMARK

We note the following

1. If $S = \emptyset$ or $T = \emptyset$, then $S \times T = \emptyset$.
2. Suppose S and T are finite sets such that $|S| = n$ and $|T| = m$, where n and m are natural numbers. Then $|S \times T| = n \cdot m$.

7.4.1 Cartesian Products of the form $S \times S$

Given a set S, we can consider collecting all the possible ordered pairs of the elements in S. The resulting set is the Cartesian product $S \times S$.

In an ordered pair, the order in which the elements are listed does matter, so the pair $(4, 5)$ is distinct from the pair $(5, 4)$. So, for example, when $S = \{4, 5\}$, there are four distinct ordered pairs in $S \times S$ as demonstrated below:

$$S \times S = \{(4, 4), (4, 5), (5, 4), (5, 5)\}.$$

Example 7 Let $T = \{n \in \mathbb{N} \ : \ n \mid 6\}$. The Cartesian product $T \times T$ is described using the set-builder notation as

$$T \times T = \{(n, m) \in \mathbb{N} \times \mathbb{N} : \ n \mid 6, m \mid 6\}.$$

Since there are four elements in T, therefore there are *sixteen* elements in $T \times T$, exhaustively listed below:

$$T \times T = \begin{Bmatrix} (1,1), & (1,2), & (1,3), & (1,6), \\ (2,1), & (2,2), & (2,3), & (2,6), \\ (3,1), & (3,2), & (3,3), & (3,6), \\ (6,1), & (6,2), & (6,3), & (6,6), \end{Bmatrix}.$$

REMARK

In the previous example, a common error is to try to describe $T \times T$ as

$$\{(n, n) \in \mathbb{N} \times \mathbb{N} \ : \ n \mid 6\}.$$

However, in the set $\{(n, n) \in \mathbb{N} \times \mathbb{N} : \ n \mid 6\}$, each pair (n, n) has the same number in the first and the second coordinates. Thus $\{(n, n) \in \mathbb{N} \times \mathbb{N} : \ n \mid 6\}$ only has these four elements: $(1, 1), (2, 2), (3, 3)$ and $(4, 4)$ and so it does not consider all possible pairs that can be formed using the elements of T.

In general, for a set $A = \{x \mid P(x)\}$, the Cartesian product $A \times A$ is described by

$$A \times A = \{(x, y) \mid P(x), \ P(y)\},$$

and is usually different from the **diagonal set** $\{(x, x) \mid P(x)\}$.

An example of a Cartesian product that you may be familiar with is the set

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

The elements of this set are represented by the points on a two dimensional Cartesian plane, and the diagonal set contains all the points on the line $y = x$ (see figure 7.4.1).

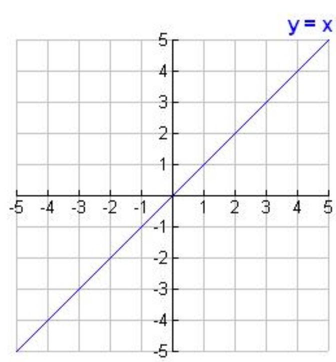


Figure 7.4.1: The Cartesian Plane is a visualization of $\mathbb{R} \times \mathbb{R}$

Chapter 8

Subsets, Set Equality, Converse and If and Only If

8.1 Objectives

The technique objectives are:

1. To understand the concept of *subsets, supersets* and *powersets*.
2. To learn how to decide whether two sets are *disjoint*, or one is *contained as a subset* of the other, or they are *equal*.
3. Define *converse* of an implication.
4. Establish connection between set equality and if and only if statements.

8.2 Comparing Sets

In the previous chapter, we developed some basic understanding of sets and set operations. In this chapter, we will discuss how to compare between any two sets. Our main criteria for comparison between two sets would be the amount of overlap between the two sets, that is, the proportion of elements the sets have in common. This idea of comparison between two sets can then be inductively extended into comparison between numerous sets.

Suppose S and T are two sets that we want to compare. Let us start with a few definitions.

Definition 8.2.1
Disjoint Sets

S and T are said to be **disjoint sets** when $S \cap T = \emptyset$.

In other words, we say S and T are disjoint when they have nothing in common. For example, the sets $\{1, 2, 3\}$ and $\{5, 6, 7\}$ are disjoint. Similarly $\{1, 2, 3\}$ is disjoint from the set $\{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$. Finally, note that the empty set $\emptyset$ is disjoint from every other set.

If we consider two sets S and T from the same universe $\mathcal{U}$, then they may or may not be disjoint. When two sets are not disjoint, they share some common elements (i.e., $S \cap T \neq \emptyset$). In an extreme scenario, it is possible that all the elements of one set, say S, are also shared by T.

Definition 8.2.2
Subset

A set S is called a **subset** of a set T, and is written $S \subseteq T$, when every element of S belongs to T. In other words,

$$S \subseteq T \text{ means } \text{"For all } x \in S, x \in T\text{"}$$

We sometimes say that S is **contained** in T.

Notice that we may rewrite the definition of $S \subseteq T$ in terms of an implication. Suppose we consider an object x from the universe of discourse $\mathcal{U}$, then $S \subseteq T$ **means if** x **is an element of** S **then** x **must be an element of** T. If there is even a single element of S that does not belong to T, then S cannot be a subset of T. When S is not a subset of T, we write $S \not\subseteq T$.

Given two particular sets S and T, mathematicians must become skilled at verifying whether $S \subseteq T$ or not.

Proof Method
$S \subseteq T$

To prove $S \subseteq T$, prove the implication: if $x \in S$ then $x \in T$. Usually, this is done through a *direct proof*.

Example 1

Let S be the set of all roots of $f(x) = (x^2 - 1)\sin x$. We could write S more symbolically as

$$S = \{x \in \mathbb{R} \mid f(x) = 0\}.$$

Let T be the set of integer multiples of π. We could also write T more symbolically as

$$T = \{n\pi \mid n \in \mathbb{Z}\}.$$

1. Show that $T \subseteq S$.

   Solution: We start by assuming that x is an element of T. Therefore, by the defining propoerty of T, $x = n\pi$, for some integer n. Since $\sin(n\pi) = 0$ for all integers n, we know that

   $$f(x) = f(n\pi) = \left((n\pi)^2 - 1\right)\sin(n\pi) = 0.$$

   Now, the defining property of S is that a real number x belongs to S if and only if $f(x) = 0$. Since $f(n\pi) = 0$, $n\pi \in S$. Thus, we have proven that if $x \in T$, then $x \in S$. This is equivalent to showing $T \subseteq S$.

2. Is $S \subseteq T$? Justify your answer.

   Solution: No. Consider $x = 1$. The value $x = 1$ is a solution to $(x^2 - 1)\sin x = 0$ and so belongs to S, but it is not an integer multiple of π, so it does not belong to T. That is, $S \not\subseteq T$.

8.2.1 Concepts related to Subsets

There are a few more concepts related to subsets that we need to define.

Definition 8.2.3
Proper Subset

A set S is called a **proper subset** of a set T, and written $S \subsetneq T$, if every element of S belongs to T and there exists at least one element in T which does not belong to S.

Example 2

For example,

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

REMARK

You may have seen the notation $S \subset T$ being used to denote "S is a proper subset of T". However, this is not universal. Some authors use $S \subset T$ to mean $S \subseteq T$ as well. To avoid any potential confusion, we will not be using the notation $S \subset T$, and will explicitly use $S \subseteq T$ or $S \subsetneq T$ as needed.

Definition 8.2.4
Superset

A set S is called a **superset** of a set T, and written $S \supseteq T$, if every element of T belongs to S. $S \supseteq T$ is equivalent to $T \subseteq S$.

Example 3

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

Definition 8.2.5
Proper Superset

As before, a set S is called a **proper superset** of a set T, and written $S \supsetneq T$, if every element of T belongs to S and there exists an element in S which does not belong to T.

Example 4

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

8.2.2 Examples

Example 5

Here are a few examples.

1. The empty set $\emptyset$ is a subset of any given set S.

   The entire set S is also a subset of itself (i.e., $S \subseteq S$), but it is not a *proper subset*.

2. Let S, T, V and W be sets. Prove that if $S \subseteq V$ and $T \subseteq W$, then $S \times T \subseteq V \times W$.

   Proof: Assume that $S \subseteq V$ and $T \subseteq W$.

   Let $(x, y) \in S \times T$. Then, by definition, $x \in S$ and $y \in T$. Since $S \subseteq V$, therefore $x \in S$ implies $x \in V$. Similarly, $y \in T$ means that $y \in W$. Thus $(x, y) \in V \times W$. Therefore $S \times T \subseteq V \times W$. $\square$

Self Check 1

Let S, T and V be three sets. Check that you can prove each of the following statements:

1. If $S \subseteq \emptyset$, then $S = \emptyset$.
2. If $S \subseteq T$ and $T \subseteq V$ then $S \subseteq V$.

8.3 Showing Two Sets Are Equal

Definition 8.3.1
Set Equality

Saying that two sets S and T are **equal**, and writing $S = T$, means that S and T have exactly the same elements.

According to the definition of set equality, two sets S and T are equal when every element of S is in T *and* every element of T is in S. That is, $S \subseteq T$ and $T \subseteq S$. Consequently, $S = T$ means that for every element x from the universe of discourse,

$$[(x \in S) \implies (x \in T)] \text{ AND } [(x \in T) \implies (x \in S)] .$$

Example 6

Suppose we define three sets A, B and C as

$$A = \{n \in \mathbb{Z} \ : \ 10 \mid n\}, \quad B = \{x \in \mathbb{Z} \ : \ x \text{ is even}\}, \quad C = \{5x \ : \ x \in \mathbb{Z}\}.$$

Show that $A = (B \cap C)$.

Solution: We shall prove that $A = (B \cap C)$ using mutual inclusion. So we must show

1. $A \subseteq (B \cap C)$ and
2. $(B \cap C) \subseteq A$.

Recall that showing $A \subseteq (B \cap C)$ is equivalent to proving the implication: if $x \in A$ then $x \in B \cap C$. We shall prove this implication with a *direct proof*.

Proof of $A \subseteq (B \cap C)$: Assume that $x \in A$. Then, according to the defining property of A, $10 \mid x$. Since $2 \mid 10$ and $10 \mid x$, by the *Transitivity of Divisibility* (*TD*), $2 \mid x$. Hence x is even, so $x \in B$. Similarly, $5 \mid 10$ and $10 \mid x$, therefore $5 \mid x$. Consequently, we may write $x = 5k$ for some integer k, and so $x \in C$. As $x \in B$ and $x \in C$, then $x \in (B \cap C)$. As a result, $A \subseteq (B \cap C)$. $\square$

Next, we need to show that $(B \cap C) \subseteq A$. Once again, this means we will be proving the implication: if $x \in (B \cap C)$ then $x \in A$ through a direct proof.

Proof of $(B \cap C) \subseteq A$: Assume $x \in B \cap C$. Thus $x \in B$ and $x \in C$. Since $x \in B$, x must be even. Since $x \in C$, $x = 5k$ for some integer k. Now 5 is an odd number, but $5k$ must be even as x is even. This means that k must be even. So we may write $k = 2m$ for some integer m, and get $x = 5k = 5(2m) = 10m$. Therefore $10 \mid x$, so $x \in A$. As a result, $(B \cap C) \subseteq A$. $\square$

Since both $A \subseteq (B \cap C)$ and $(B \cap C) \subseteq A$ have been proven, we may conclude that $A = (B \cap C)$.

The implications "if $x \in S$ then $x \in T$" and "if $x \in T$ then $x \in S$" are said to be *converses* of each other. Let us have a brief discussion on the converse of an implication.

8.3.1 Converse of an Implication

Definition 8.3.2
Converse

The statement $B \implies A$ is called the **converse** of $A \implies B$.

To obtain the converse of an implication, we simply switch the places of the hypothesis and the conclusion.

REMARK

It is a common mistake for beginning mathematicians to assume that $A \implies B$ and $B \implies A$ are the same. They are not!

We can use truth tables to show that $A \implies B \not\equiv B \implies A$. Essentially, this means that the truth values of $A \implies B$ and $B \implies A$ are unrelated; when $A \implies B$ is true, it is not possible to deduce whether $B \implies A$ is true or false without knowing the truth values of the components A and B.

Example 7

Look at example 1 and example 6. We may say the following.

1. For all real numbers x, "if $x = n\pi$, for some integer n, then $(x^2 - 1)\sin(x) = 0$" is always true, but its converse "if $(x^2 - 1)\sin(x) = 0$ then $x = n\pi$ for some integer n" is not always true.
2. For any integer k, the implication "if k is even and $5 \mid k$ then $10 \mid k$" is true, and the converse "if $10 \mid k$ then k is even and $5 \mid k$" is true as well.

8.3.2 If and Only If Statements

We shall now define another statement that is closely related to implications and their converses.

Definition 8.3.3
If and Only If

The definition of A **if and only if** B, written $A \iff B$ or A *iff* B, is

A	B	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

The statement $A \iff B$ poses an interesting connection between A and B. According to the truth table above, whenever $A \iff B$ is true, A and B have the same truth value. Thus $A \iff B$ is true exactly when A is logically equivalent to B. On the other hand $A \iff B$ is false indicates that A is not logically equivalent to B.

Using a truth table, we may show that $A \iff B$ is logically equivalent to

$$(A \implies B) \wedge (B \implies A).$$

Proof Method
$\iff$ as "$\implies$" and "$\impliedby$"

To prove a statement of the form $A \iff B$, we could prove

1. $A \implies B$ and
2. $B \implies A$.

This gives us a new method to prove two sets are equal.

8.3.3 Set Equality and If and Only If Statements

Proof Method
$S = T$

Given sets S and T, there are two logically equivalent ways to prove that $S = T$:

Mutual Inclusion: show that each of the set relations $S \subseteq T$ and $T \subseteq S$ is true.

Chain of If and Only Ifs: show, through a chain of true if and only if statements, that $(x \in S) \iff (x \in T)$ is a true statement for every x from the universe of discourse.

Let's take a look at two proofs of the same statement about sets. The first uses a chain of if and only if statements, the second uses mutual inclusion.

Proposition 1

Let A, B and C be arbitrary sets.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Proof: This proof uses a chain of if and only if statements to show that both $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ have exactly the same elements. Let $x \in A \cup (B \cap C)$. Then

$$\begin{aligned}
& x \in A \cup (B \cap C) \\
& \iff (x \in A) \vee (x \in (B \cap C)) && \text{definition of union} \\
& \iff (x \in A) \vee ((x \in B) \wedge (x \in C)) && \text{definition of intersection} \\
& \iff ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)) && \text{Distributive Law of logic} \\
& \iff (x \in A \cup B) \wedge (x \in A \cup C) && \text{definition of union} \\
& \iff x \in ((A \cup B) \cap (A \cup C)) && \text{definition of intersection}
\end{aligned}$$

$\square$

Proof: This proof uses mutual inclusion. That is, we will show

1. $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
2. $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$

Equivalently, we must show

1. If $x \in A \cup (B \cap C)$, then $x \in (A \cup B) \cap (A \cup C)$.
2. If $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup (B \cap C)$.

Let $x \in A \cup (B \cap C)$. By the definition of union, $x \in A$ or $x \in (B \cap C)$. If $x \in A$, then by the definition of union, $x \in A \cup B$ and $x \in A \cup C$, that is $x \in (A \cup B) \cap (A \cup C)$. If $x \in B \cap C$, then by the definition of intersection, $x \in B$ and $x \in C$. But then by the definition of union, $x \in A \cup B$ and $x \in A \cup C$. Hence, by the definition of intersection, $x \in (A \cup B) \cap (A \cup C)$. In both cases, $x \in (A \cup B) \cap (A \cup C)$ as required.

Let $x \in (A \cup B) \cap (A \cup C)$. By the definition of intersection, $x \in A \cup B$ and $x \in A \cup C$. If $x \in A$, then by the definition of union, $x \in A \cup (B \cap C)$. If $x \notin A$, then by the definition of union and the fact that $x \in A \cup B$, $x \in B$. Similarly, $x \in C$. But then, by the definition of intersection, $x \in B \cap C$. By the definition of union, $x \in A \cup (B \cap C)$. In both cases, $x \in A \cup (B \cap C)$. $\square$

REMARK

Which technique is better for proving the equality of two sets: a chain of if and only if statements or mutual inclusion? Though some of the choice is personal style, the choice is primarily determined by the "reversibility" of each step in the proof. A chain of if and only if statements only works if each step in the chain is reversible. That's pretty unusual. Most of the time when you are proving two sets are equal, you will need to use mutual inclusion.

8.4 More Examples

1. Give a specific example to show that the statement "$U \cap (S \cup T) = (U \cap S) \cup T$" is false.

   Solution: Let $U = \emptyset$, $S = \{1\}$ and $T = \{2\}$. Then $U \cap (S \cup T) = \emptyset$ and $(U \cap S) \cup T = \{2\}$. In this case $U \cap (S \cup T) \neq (U \cap S) \cup T$

2. Prove the following statement. Let S, T, U be sets. Then

   $$U \cap (S \cup T) = (U \cap S) \cup (U \cap T)$$

   Solution: We shall prove the given set equality using a chain of if and only if statements.

Proof:

$$
\begin{aligned}
x \in\, & U \cap (S \cup T) \\
&\iff (x \in U) \wedge (x \in S \cup T) && \text{(definition of intersection)} \\
&\iff (x \in U) \wedge ((x \in S) \vee (x \in T)) && \text{(defn of union)} \\
&\iff ((x \in U) \wedge (x \in S)) \vee ((x \in U) \wedge (x \in T)) \\
& && \text{(Distributive Law of logic)} \\
&\iff (x \in (U \cap S)) \vee (x \in (U \cap T)) && \text{(definition of union)} \\
&\iff x \in (U \cap S) \cup (U \cap T) && \text{(defn of intersection)}
\end{aligned}
$$

Hence, $U \cap (S \cup T) = (U \cap S) \cup (U \cap T)$.

□

8.5 Discovering: Sets of Solutions

One common use of sets is to describe values which are solutions to an equation, but care in expression is required here. The following two sentences mean different things.

1. Let $a, b, c \in \mathbb{R}$, $a \neq 0$ and $b^2 - 4ac \geq 0$. The solutions to the quadratic equation $ax^2 + bx + c = 0$ are $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.
2. Let $a, b, c \in \mathbb{R}$, $a \neq 0$ and $b^2 - 4ac \geq 0$. Then $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ are solutions to the quadratic equation $ax^2 + bx + c = 0$.

The first sentence asserts that a complete description of all solutions is given. The second sentence only asserts that $x = (-b \pm \sqrt{b^2 - 4ac})/2a$ are solutions, not that they are the *complete* solution. In the language of sets, if S is the complete solution to $ax^2 + bx + c = 0$, and $T = \{(-b \pm \sqrt{b^2 - 4ac})/2a\}$, Sentence 1 asserts that $S = T$ (which implies $S \subseteq T$ and $T \subseteq S$) but Sentence 2 only asserts that $T \subseteq S$.

This point can be confusing. Statements about solutions are often implicitly divided into two sets: the set S of all solutions and a set T of proposed solutions. One must be careful to determine whether the statement is equivalent to $S = T$ or $T \subseteq S$. Phrases like *the solution* or *complete solution* or *all solutions* indicate $S = T$. Phrases like *a solution* or *are solutions* indicate $T \subseteq S$.

Similar confusion arises when showing that sets have more than one representation. For example, a circle centered at the origin O is often defined geometrically as the set of points equidistant from O. Others define a circle algebraically in the Cartesian plane as the set of points satisfying $x^2 + y^2 = r^2$. To show that the two definitions describe the same object, one must show that the two sets of points are equal.

Self Check 2 Let $a, b, c \in \mathbb{R}$, $a \neq 0$ and $b^2 - 4ac \geq 0$. Check that you can prove the statement:

Proposition 2 The solutions to the quadratic equation $ax^2 + bx + c = 0$ are $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Consider the approach outlined in this section. Define two sets S and T to be

$$S = \{x \in \mathbb{R} \mid ax^2 + bx + c = 0\} \quad \text{and} \quad T = \left\{x \in \mathbb{R} \mid x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\right\}.$$

Demonstrate $S = T$.

8.6 Practice

1. Suppose S and T are two sets. Prove that
   (a) If $S \cap T = S$, then $S \subseteq T$.
   (b) If $S \cup T = T$, then $S \subseteq T$.
2. Give examples of three sets A, B and C such that
   (a) $A \in B$, $B \in C$ and $A \notin C$.
   (b) $A \in B$, $A \subsetneq C$ and $B \notin C$.
3. List all the elements of $\mathcal{P}(\mathcal{P}(\{1, 2\}))$. What is the cardinality of this set?
4. Give an example of three sets A, B, and C such that $B \neq C$ and $B - A = C - A$.
5. Let $A = \{1, \{1, \{1\}\}\}$. List all the elements of $A \times A$.
6. Let S and T be any two sets in a universe $\mathcal{U}$. Prove the following.
   (a) $S - T = S \cap \overline{T}$.
   (b) $(S \cup T) - (S \cap T) = (S - T) \cup (T - S)$.
7. Let A, B and C be three sets. Prove that
   (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
   (b) $A \times (B - C) = (A \times B) - (A \times C)$.
8. Let n be an integer. Prove that $2 \mid (n^4 - 3)$ if and only if $4 \mid (n^2 + 3)$.
9. Let $A = \{n \in \mathbb{Z} \ : \ 2 \mid n\}$ and $B = \{n \in \mathbb{Z} \ : \ 4 \mid n\}$. Prove that $n \in (A - B)$ if and only if $n = 2k$ for some odd integer k.

Chapter 9

Quantifiers

9.1 Objectives

The technique objectives are:

1. Learn the basic structure of statements with quantifiers.
2. Understand the usage of the Universal and the Existential quantifier.
3. Learn how to prove quantified statements.

9.2 Quantifiers

This chapter is devoted towards the final piece of the puzzle required to construct well-formed mathematical statements involving variables. Let us recall some of the statements that we have seen so far:

1. For every integer x, $x^2 + 1 \geq 2x$.
2. For any real number x, if $x^2 < 0$ then $x^2 + 1 > 2$.
3. There exists some integer n such that $n^2 - 1 = 0$.
4. There is an integer k such that $6 = 3k$.

The above sentences are examples of *quantified statements*. Each of the statements above contain a variable, and each variable has been introduced through a phrase such as "for every", "for any", "there exists", "there is", etc. Such phrases are called *quantifiers*, and they give us some information about how to assess whether the statements are true or false.

The role of a **quantifier** is to develop a sense of "how many" elements of a given domain satisfy a given property. In English, words such as "all", "some", "many", "none", "few", etc., are used in quantification. In this course, we will only be interested in two types of quantifiers: **universal** and **existential**. A universal quantifier (e.g., "for all") generalizes a property for all elements of a given domain, while an existential quantifier (e.g., "there exists) demands that the property be satisfied by at least one element from the domain.

REMARK

All statements which use quantified variables share a basic structure:

> Quantified variable in given domain, followed by some open sentence containing the variable.

There are four key parts to a quantified statement.

1. a **quantifier** which will be either an existential or universal quantifier,
2. a **variable** which can be any mathematical object,
3. a set which is the **domain** of the variable, often implicit, and
4. an **open sentence** which involves the variable.

   Recall that an **open sentence** is a sentence that contains one or more variables, where the truth of the sentence is determined by the values from the respective domains of the variables.

It is crucial that you be able to identify the four parts in the structure of quantified statements.

Example 1 Here are some examples of statements with quantified variables. We have identified the four key parts of each statement.

1. For every integer k, $10^4 - 1 = 101k$

Quantifier:	For every
Variable:	k
Domain:	$\mathbb{Z}$
Open sentence:	$10^4 - 1 = 101k$

2. There exists a real number x such that $x^2 - 2 = 0$.

Quantifier:	There exists
Variable:	x
Domain:	$\mathbb{R}$
Open sentence:	$x^2 - 2 = 0$

   After studying quantifiers more carefully in the next sections, you will see that the first statement is false and the second statement is true.

   However, if we change the domain of x in the second statement to integers, we get the statement

   > There exists an integer x such that $x^2 - 2 = 0$.

   This is false because neither of the two real roots, $\sqrt{2}$ or $-\sqrt{2}$, are integers. So changing the domain can change the truth value of the statement. What would be a suitable domain for k in the first statement that will give us a true statement?

9.3 The Universal Quantifier

The **universal quantifier**, denoted by the symbol $\forall$, is used to indicate that all elements of a set satisfy a common property. Thus the statement

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

indicates that all members of the set S satisfy the given property P. We read the above statement as "For all x in S, $P(x)$ is true" or simply as "For all x in S, $P(x)$".

Example 2 Suppose T is a subset of the letters of the English alphabet, given by $T = \{i, o, u\}$. Consider $P(x)$ to be the open sentence "x is a vowel". Then $\forall\, x \in T,\ P(x)$ is a true statement as each of the statements $P(i)$, $P(o)$ and $P(u)$ is true. Notice that this means that $P(i) \wedge P(o) \wedge P(u)$ is a true statement as well.

REMARK

In general, given a finite set $S = \{x_1, x_2, x_3, \ldots, x_n\}$, the statement "$\forall\ x \in S, P(x)$" is logically equivalent to "$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \cdots \wedge P(x_n)$"

When the domain is empty, i.e., $S = \emptyset$, then regardless of what the open sentence $P(x)$ says, the statement "$\forall\ x \in \emptyset,\ P(x)$" is said to be *vacuously* true.

Example 3 Consider the open sentence $P(x):\ x^2 \geq 0$. The statement $\forall\ x \in \mathbb{R},\ P(x)$, or equivalently, $\forall\ x \in \mathbb{R},\ x^2 \geq 0$, is a true statement.

In addition to the standard sentence: "For all x in $\mathbb{R}$, $x^2 \geq 0$", we also often use the following sentences in English to convey the same meaning as '$\forall\ x \in \mathbb{R},\ x^2 \geq 0$".

1. For every $x \in \mathbb{R}$, $x^2 \geq 0$.
2. Any $x \in \mathbb{R}$ satisfies $x^2 \geq 0$.
3. Let x be a real number, then $x^2 \geq 0$.
4. The square of every real number is non-negative.

Here is another example of how we may use the universal quantifier. You may be familiar with the following definition of a prime number.

Definition 9.3.1
Primes

An integer $p > 1$ is called a **prime** if and only if its positive divisors are 1 and p itself. Otherwise, p is called **composite**.

According to this definition, an integer $p > 1$ is a prime if and only if

For all $k \in \mathbb{N}$, if $k \mid p$ then $(k = 1) \vee (k = p)$.

Note how the universal quantifier is being used to convey the condition about the "only positive divisors of p are 1 and p" by looking at "all the positive integers k that divide p" and inferring that k must be 1 or p.

9.3.1 The Select Method

Let us now discuss how to prove that a statement of the form $\forall\ x \in S,\ P(x)$ is true. We want to justify that each element of S satisfies the property $P(x)$. One way to do so would be to go through each and every element of S, and check that the open sentence P is evaluated to be true for each member of S.

However, it is easy to see that this process could get tiresome when S has a lot of elements, perhaps infinitely many, and we have to carefully check that the open sentence is true for each element of S. Instead, we use the **select method**.

Proof Method
Select Method

To prove $\forall\ x \in S,\ P(x)$:

Select a representative mathematical object $x \in S$. This cannot be a specific object. It has to be a placeholder, that is, a variable, so that our argument would work for any specific member of S.

Then show that the open sentence P must be true for our representative x. You may use the rules of algebra, combined with any other previously proven result, to obtain this.

How do we select a representative object x from S? We simply declare "Let x be an arbitrary element of S", or state "Let $x \in S$". Next, we start using the symbol x as if it has all the characteristics of a typical member of S. The philosophy here is that we could replace x by any particular element from S, and all our steps would be correct. Then, when we symbolically show that $P(x)$ must be satisfied, we are guaranteed that the open sentence would be true for any element of S.

Example 4

Prove each of the following statements.

1. For each $x \in \mathbb{R}$, $x < x + 1$.

   Solution: Let x be a real number. Therefore $(x+1)-(x) = 1 > 0$. Since $(x+1)-(x) > 0$,
   $$x < x + 1$$
   is true. Thus, by the *select method*, $\forall\ x \in \mathbb{R},\ x < x + 1$ is a true statement.

2. For every natural number n, $n \leq n^2$.

   Solution: Let $P(x)$: $x \leq x^2$. We know that the set of natural numbers is given by
   $$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}.$$
   Let $n \in \mathbb{N}$. Since n is a natural number, $n \geq 1$.

   Multiply both sides of the inequality by n (note: n is positive) to get
   $$\begin{aligned} n \cdot n &\geq n \cdot 1 \\ \implies n^2 &\geq n. \end{aligned}$$
   Thus, $P(n)$ is true.

   Therefore, by the *select method*, $\forall\ n \in \mathbb{N}, P(n)$ is a true statement.

9.4 The Existential Quantifier

The **existential quantifier**, denoted by the symbol $\exists$, is used to express the idea that at least one element of a given set satisfies a given property. We read the statement

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

as "There exists at least one value of x in S for which $P(x)$ is true" or simply as "There exists x in S such that $P(x)$".

Here are some other ways in which the statement $\exists\, x \in S,\ P(x)$ is expressed in written English:

1. There is an $x \in S$ such that $P(x)$ is true.
2. $P(x)$ is true for some $x \in S$.
3. At least one $x \in S$ satisfies $P(x)$.
4. S has an element x such that $P(x)$ is satisfied.

For example, the symbolic statement

$$\exists\, x \in [0,2],\ x^2 - 1 = 0$$

could be read as "The value of $x^2 - 1$ is 0 for some x between 0 and 2 (inclusive)." However, the standard way to read the above statement is to say "There exists an x in the interval $[0,2]$ such that $x^2 - 1 = 0$."

Example 5 Let us look at a few uses of the existential quantifier.

1. The statement "$\exists\, n \in \mathbb{Z},\ 0 \mid n$" is true because $n = 0$ is an integer and $0 \mid 0$. However, the statement "$\exists\, n \in \mathbb{N}, 0 \mid n$" is false because 0 cannot divide any non-zero integer.
2. Suppose n and m are integers. The statement $n \mid m$ is defined to mean

$$\exists\, k \in \mathbb{Z},\ m = kn.$$

REMARK

In general, given a finite set $S = \{x_1, x_2, x_3, \ldots, x_n\}$ with n-elements, we have

$$[\exists\, x \in S, P(x)] \equiv [P(x_1) \vee P(x_2) \vee P(x_3) \vee \cdots \vee P(x_n)]\,.$$

The statement $\exists\, x \in S,\ P(x)$ is true if and only if we can find at least one element from the set S that satisfies the property P, which happens if and only if $P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$ is a true statement.

Note that $\exists\, x \in S,\ P(x)$ would be a false statement when there are no elements of x that satisfy the property P. This implies that when the domain is empty, the statement "$\exists\, x \in \emptyset,\ P(x)$" is *vacuously* false.

9.4.1 The Construct Method

We use the **construct method** to prove a statement of the form

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

Proof Method

Construct Method

To prove $\exists\, x \in S,\ P(x)$.

Provide an explicit value of x from the domain S, and show that $P(x)$ is true for this value. In other words, find an element in S that satisfies the property P.

The following examples demonstrate how the construct method works.

Example 6

Prove each of the following statements.

1. $\exists\, x \in \{1, 2, 3, 4\}$, such that x is even.

   Proof: Consider $x = 2$. Since 2 is an element of the given domain, and 2 is even, therefore the above statement is true. $\square$

   Note that 4 is also an even number from the domain, so we could have chosen $x = 4$ as well. However, all we need to do is find one element from the domain that satisfies the given property. So once we find one value that works, such as $x = 2$, we don't need to concern ourselves with whether other elements of the domain satisfy the property or not.

2. There is a real number $\theta \in [0, 2\pi]$ such that $\sin\theta = \cos\theta$.

   Proof: Consider $\theta = \dfrac{\pi}{4}$. Clearly, $\theta \in [0, 2\pi]$. Since

   $$\sin\theta = \sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} \text{ and } \cos\theta = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}$$

   $\sin\theta = \cos\theta$ as required. $\square$

3. $x^2 - 2 = 3x$ for some $x \in [-1, 1]$.

   Proof: Consider $x = \frac{3-\sqrt{17}}{2}$.
   Note that $\frac{3-\sqrt{17}}{2} \approx -0.562$, so $\frac{3-\sqrt{17}}{2} \in [-1, 1]$.
   Substitute $x = \frac{3-\sqrt{17}}{2}$ into $x^2 - 2$ to get

   $$x^2 - 2 = \left(\frac{3-\sqrt{17}}{2}\right)^2 - 2 = \frac{(3)^2 + 2(3)(-\sqrt{17}) + (-\sqrt{17})^2 - 8}{4} = \frac{18 - 6\sqrt{17}}{4}.$$

   Similarly, substitute $x = \frac{-3+\sqrt{17}}{2}$ into $3x$ to get

   $$3x = 3\left(\frac{3-\sqrt{17}}{2}\right) = \frac{9 - 3\sqrt{17}}{2} = \frac{18 - 6\sqrt{17}}{4}$$

   as well. Therefore, the value $x = \frac{3-\sqrt{17}}{2}$ satisfies the equation $x^2 - 2 = 3x$.

   $\square$

Let us provide some more insights into *how* to use the construct method. In particular, if we look back at the previous example, how did we manage to obtain the values from the corresponding domain that seem to magically satisfy the required property? There are two ways to find such values as discussed below.

1. *By Trial and Error*: We could attempt to substitute each element of the domain for x in the open sentence until we find one that works. This approach works well when the domain is small, and it is easy to verify whether the property is true or false for each domain element.

   For instance, when $S = \{1, 2, 3, 4\}$ and $P(x) : x$ is even, we can simply exhaustively examine each of the numbers $1, 2, 3$ and 4 until we find an even number. So, we try $x = 1$ and find that $P(1)$ is false. We then move onto $x = 2$, find $P(2)$ is true, and may immediately conclude that $\exists\, x \in S,\ P(x)$ is a true statement.

   When we write down the final proof, we do not need to demonstrate all the values that we tried, but just use the one that we found to work.

2. *By using preliminary knowledge about what we wish to prove.* Clearly, the method of trial and error is not such a great idea when we are dealing with infinite domains such as $[0, 2\pi]$ or $[-1, 1]$. In these cases, we try to use any prior knowledge that we may have about the open sentence to try to come up with a value that works.

   For example, here's a table of special angles for trigonometric ratios that you may remember from high school:

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\sin\theta$	$\frac{\sqrt{0}}{2} = 0$	$\frac{\sqrt{1}}{2} = \frac{1}{2}$	$\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{4}}{2} = 1$
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0

   From this table, we notice that $\sin\theta$ and $\cos\theta$ take the same value when $\theta = \frac{\pi}{4}$. Armed with this knowledge, we may now write a formal proof of the statement "there is a real number $\theta \in [0, 2\pi]$ such that $\sin\theta = \cos\theta$". In our proof, we do not need to mention how we came across the value of $\theta = \frac{\pi}{4}$, but just demonstrate that it works.

   Similarly, while proving "$x^2 - 2 = 3x$ for some $x \in [-1, 1]$", we may use our knowledge of quadratic equations. The equation $x^2 - 2 = 3x$ may be written as $x^2 - 3x - 2 = 0$, and using the quadratic formula to solve for the values of x gives us

$$x = \frac{-(-3) \pm \sqrt{(-3)^2 - (4)(1)(-2)}}{2} = \frac{3 \pm \sqrt{17}}{2}.$$

   Now, $\frac{3+\sqrt{17}}{2} \approx 3.562$, which is not within our intended interval $[-1, 1]$. On the other hand, $\frac{3-\sqrt{17}}{2} \approx -0.562$ is in our domain. Once again, we may write down a formal proof as shown in the previous example.

REMARK

When we apply our preliminary knowledge in a constructive proof, we usually do it on a rough piece of paper. The final written proof does not usually contain any reference of how we obtained the value that works. We simply propose this value for x, make sure the proposed value is in the domain, and then demonstrate that the property holds for this value.

9.5 Negating Quantifiers

Here is a quick summary of what we have learned so far.

Quantified Statement	When True?	When False
$\forall\ x \in S,\ P(x)$	$P(x)$ is true for every $x \in S$	$P(x)$ is false for at least one element in S
$\exists\ x \in S,\ P(x)$	$P(x)$ is true for at least one element in S	$P(x)$ is false for every element in S

It is quite obvious from the discussion above that the following rules of negation should apply for quantified statements.

The negation of "For all $x \in S$, $P(x)$ is true" is

> There exists some $x \in S$ for which $P(x)$ is false.

That is, using the symbols for the quantifiers, we are saying

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

Similarly, the negation of "There exists some $x \in S$ such that $P(x)$ is true" is

> For all $x \in S$, $P(x)$ must be false.

In other words,

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

These rules of negation help us understand the methods for *disproving* quantified statements.

1. To show $\forall\ x \in S,\ P(x)$ is *false*, we need to prove $\exists\ x \in S,\ (\neg P(x))$. Thus, we need to find a value of x from the domain for which P is false. This process is called *finding a counter-example.*

   For example, the statement: $\forall\ x \in \mathbb{N},\ n! < 2^n$ is false, because when $n = 4$, we have $4! = 24$, but $2^4 = 16$, so $4! > 2^4$. Thus $n = 4$ acts as a counter-example to the statement $\forall\ x \in \mathbb{N},\ n! < 2^n$.

2. To show $\exists\ x \in S,\ P(x)$ is *false*, we need to show that $\forall\ x \in S, (\neg P(x))$ is true. This involves the *select method.* We must show that $P(x)$ fails for any arbitrary x from the domain.

   For example, we may show that $\exists\ n \in \mathbb{N}, n^2 < n$ is false by proving $\forall\ n \in \mathbb{N}, n^2 \geq n$, which we have already done in an earlier example (see example 4).

Self Check 1

Check that you can negate the following statement without using the word "not" or the "$\neg$" symbol:

> For all $x \in \mathbb{R}$, if $x^4 + 2x^2 - 2x < 0$ then $0 < x < 1$.

Either prove or disprove the statement above.

9.6 Assuming a Quantified Statement is True

Let us now discuss the consequence of assuming a statement such as "$\forall\ x \in S,\ P(x)$" or "$\exists\ x \in S,\ P(x)$" is true.

9.6.1 The Substitution Method

Let $n \in \mathbb{N}$. Consider the following statement about n:

> If $\forall\ x \in \mathbb{N},\ n \mid x$ then $n = 1$.

To directly prove this implication, we assume that the hypothesis "$\forall\ x \in \mathbb{N},\ n \mid x$" is true. This is a very strong assumption. By our assumption, we may substitute any positive integer in place of x, and the property $n \mid x$ must be satisfied for that value of x.

For example, if we use $x = 12$, then we get $n \mid 12$. So n must be one of the numbers $1, 2, 3, 4, 6$ or 12. On the other hand, if we use $x = 5$, then $n \mid 5$ tells us that n is either 1 or 5, and so on. The trick here is to choose an appropriate value of x from $\mathbb{N}$ such that the information $n \mid x$ helps us get to the desired conclusion that $n = 1$. Let's now write a proof of the given implication.

Proof: Assume that $\forall\ x \in \mathbb{N},\ n \mid x$. Since $1 \in \mathbb{N}$, consider $x = 1$. By our assumption, $n \mid 1$. We know that the only positive divisor of 1 is 1 itself. Therefore $n = 1$. $\square$

Proof Method

Substitution Method

Suppose we assume $\forall\ x \in S,\ P(x)$ is true, and we want to use this assumption in a proof.

Substitute an appropriate value of x from S into the open sentence P, and use the fact that $P(x)$ must be true to arrive at the desired conclusion.

Self Check 2

Let r be a real number. Prove the following statement

> If $\forall\ x \in [0, \infty),\ r^2 \leq x$ then $r = 0$.

9.6.2 The Object Method

Let p be a real number and k be an integer. Consider the following statement about p and k:

> If there exists a non-zero integer q such that $\frac{p}{q} = k$, then p must be an integer.

To prove this statement, we assume that "$\exists$ non-zero integer q, such that $\frac{p}{q} = k$" is true. Here p and k are integers, but we do not know their numerical values. We will now use the symbol "q" as an (hypothetical) *object* that

1. is a non-zero integer, and

2. satisfies the equation $\frac{p}{q} = k$.

Our goal is to use these properties of q to convince the reader that p must be an integer. The proof is below.

Proof: We are given that p and k are integers. Let us assume that q is a non-zero integer for which $\frac{p}{q} = k$.

We may now multiply both sides of $\frac{p}{q} = k$ by q to get $p = qk$. Since q and k are both integers, therefore qk is also an integer. Hence p must be an integer. $\square$

Proof Method
Object Method

Assume $\exists\, x \in S,\ P(x)$ is true.

Use a symbol, such as "x", to denote an element of S for which $P(x)$ is true. Since we do not know exactly which element of S satisfies P, we cannot assign a specific value to x. Instead, we work with x as a variable.

We may then apply the rules of algebra and other established results about the elements of S to this "x" in order to prove the desired conclusion.

Example 7

Let n be an integer. Prove the following statement about n:

If n is of the form $4\ell + 1$ for some positive integer ℓ, then $8 \mid (n^2 - 1)$.

Discussion: Once again, we are proving an implication, so we start by identifying the hypothesis and the conclusion.

Hypothesis: n is of the form $4\ell + 1$ for some integer ℓ.

Conclusion: $8 \mid (n^2 - 1)$.

Note that we may rewrite the hypothesis in its symbolic form:

$$\exists\, \ell \in \mathbb{Z},\ \text{such that } n = 4\ell + 1.$$

Our goal is to prove $8 \mid (n^2 - 1)$, which is equivalent to *proving* that "$\exists\, k \in \mathbb{Z},\ 8k = (n^2 - 1)$".

Proof: Assume, by the *object method*, that we can write $n = 4\ell + 1$ for some integer ℓ.

Let $k = 2\ell^2 + \ell$. Since ℓ is an integer, therefore k must also be an integer. In that case,

$$n^2 - 1 = (4\ell + 1)^2 - 1 = 16\ell^2 + 8\ell + 1 - 1 = 16\ell^2 + 8\ell = 8(2\ell^2 + \ell) = 8k.$$

Thus, according to the *construct method*, we have shown that $\exists\, k \in \mathbb{Z},\ 8k = (n^2 - 1)$ is true. Therefore, $8 \mid (n^2 - 1)$. $\square$

Note that when using the object method, we should not use a variable that already exists in the problem as that can lead to potential confusion and error. The next example shows such a mistake in an attempted "proof".

Example 8

Let $m \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Consider the following statement:

If $m \mid (b-a)$ and $m \mid (c-b)$ then $(c-a)$ is even.

Here is an incorrect proof of this statement:

Incorrect Proof: Assume that the hypothesis is true. Since $m \mid (b-a)$, we may say $\exists\ x \in \mathbb{Z},\ b-a = mx$. Similarly, from $m \mid (c-b)$, we get $\exists\ x \in \mathbb{Z},\ c-b = mx$. We may add $b-a = mx$ and $c-b = mx$ to get $c-a = 2mx$. As $2mx$ is an even number, therefore $(c-a)$ must also be even. $\square$.

Self Check 3

Discuss what is wrong with the previous attempt at proving the above statement. Either prove the given statement, or provide a value for each of the variables m, a, b and c such that the statement is false.

Example 9

Let $m \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Prove the following statement:

If $m \mid (b-a)$ and $m \mid (c-b)$ then $m \mid (c-a)$.

Proof: Assume that $m \mid (b-a)$ and $m \mid (c-a)$.

From $m \mid (b-a)$, we may use the *object method* to say that there exists an integer x for which $(b-a) = mx$. Similarly, from $m \mid (c-b)$, we may say that there is an integer y (note: we are using a variable different from x) such that $(c-b) = my$.

Add $b-a = mx$ with $c-b = my$ to get $c-a = m(x+y)$. As x and y are both integers, $x+y$ must also be an integer. Thus $m \mid (c-a)$. $\square$

9.7 Practice

1. For each of the statements given below:

   (i) Identify the four parts of the quantified statement.

   (ii) Express the negation of the statement without using the word "not" or the "$\neg$" symbol (but symbols such as $\neq$, $\nmid$, etc., are fine).

   (iii) Prove the given statement.

   Statements:

   (a) *There exists an integer k so that $x^2 + kx + 2 = 0$ has an integer solution.*

   (b) *For every prime number p, $p+7$ is composite.*

   (c) *For every integer k, if k^2 is even then k is even.*

   (d) *There exists a real number x such that if $x^2 \geq 0$ then $x = 0$.*

2. For each of the statements given below:

   (i) Identify the four parts of the quantified statement.

   (ii) Express the negation of the statement without using the word "not" or the "$\neg$" symbol (but symbols such as $\neq$, $\nmid$, etc., are fine).

   (iii) Disprove the given statement.

   Statements:

   (a) *For every integer n, $n^2 - n + 41$ is a prime.*

   (b) *There exists an integer k such that $8 \nmid (4k^2 + 12k + 8)$.*

3. Prove or disprove the following statements.

   (a) $\forall\, n \in \mathbb{N},\ n + 1 \geq 2$.

   (b) $\forall\, n \in \mathbb{Z},\ \frac{(5n-6)}{3}$ is an integer.

   (c) $\exists\, n \in \mathbb{Z},\ \frac{(5n-6)}{3}$ is an integer.

   (d) There is a real number solution of the equation $x^4 + x^2 + 1 = 0$.

   (e) The equation $x^3 + x^2 - 1 = 0$ has a real number solution between $x = 0$ and $x = 1$ (inclusive).

Chapter 10

Nested Quantifiers

10.1 Objectives

The technique objectives are:

1. Recognize *nested quantifiers*.
2. Learn how to parse statements with nested quantifiers.
3. Discover proof techniques that apply to a sentence containing nested quantifiers.

10.2 Nested Quantifiers

Most of the statements that we will see in mathematics contain more than one variable. Each variable must come with its own domain and quantifier. When a statement has more than one quantified variable, it is important to note the order in which they appear.

For example, consider the following statement containing three variables: x, y and z.

$$\forall\, x \in \mathbb{R},\ \exists\, y \in \mathbb{Z},\ \exists\, z \in \mathbb{R},\ x + y + z = 0$$

We read mathematical statements from left to right. If a statement contains more than one quantified variable, then we first read the leftmost quantified variable, and regard the rest of the statement as a property of this variable. Thus, the other quantified variables become *nested* within the property of the leftmost variable. We then proceed through the rest of the statement in a similar manner. Therefore, we may parse the above statement in layers. For instance, we can consider this statement to be of the form

$$\forall\, x \in \mathbb{R},\ P(x),$$

$$\text{where}\quad P(x) :\ \exists\, y \in \mathbb{Z},\ Q(x, y),$$

$$\text{where}\quad Q(x, y) :\ \exists\, z \in \mathbb{R},\ R(x, y, z),$$

$$\text{where}\quad R(x, y, z) :\ x + y + z = 0.$$

Here, the quantifier for y is nested within the property $P(x)$, the quantifier for z is nested within the property $Q(x, y)$, and so on. A useful way to think about nested quantifiers is in terms of nested loops that we use in programming.

It takes a bit of practice to become good at parsing and using nested quantifiers in statements. To start, we will focus on statements that have only two variables. There are four possible combinations of nested quantifiers to consider. The following examples illustrate how to prove statements with nested quantifiers.

Example 1

For all $x \in \mathbb{N}$, for all $y \in \mathbb{N}$, $\frac{x+y}{2} \geq \sqrt{xy}$.

Proof. Let $x \in \mathbb{N}$ and $y \in \mathbb{N}$. We know that the following algebraic equation is true for all natural numbers x and y:

$$(x-y)^2 = (x+y)^2 - 4xy.$$

Since $\mathbb{N} \subseteq \mathbb{R}$, $(x-y)^2 \geq 0$. Thus, we have $(x+y)^2 - 4xy \geq 0$, which simplifies to

$$\frac{(x+y)^2}{4} \geq xy.$$

Taking the positive square-root on both sides, we get $\frac{x+y}{2} \geq \sqrt{xy}$.

Proof Method

$\forall\ x \in S,\ \forall\ y \in T$

To prove $\forall\ x \in S,\ \forall\ y \in T,\ Q(x,y)$:

1. either exhaustively verify Q is true for each pair (x,y) from $S \times T$,
2. or use the *select method* on both the variables x and y, show $Q(x,y)$ is true.

Example 2

There exists a positive even integer m such that for every positive integer n,

$$\left|\frac{1}{m} - \frac{1}{n}\right| \leq \frac{1}{2}.$$

Proof. The first quantifier is existential, so we must use the *construct method.* Let $m = 2$. Let n be any arbitrary positive integer. We consider three cases.

Case 1. When $n = 1$, we have $\left|\frac{1}{m} - \frac{1}{n}\right| = \left|\frac{1}{2} - \frac{1}{1}\right| = \left|-\frac{1}{2}\right| = \frac{1}{2}$.

Case 2. When $n = 2$, then $\left|\frac{1}{m} - \frac{1}{n}\right| = \left|\frac{1}{2} - \frac{1}{2}\right| = 0 < \frac{1}{2}$.

Case 3. When $n \geq 3$, then $0 < \frac{1}{n} \leq \frac{1}{3} < \frac{1}{2}$. Thus

$$\left|\frac{1}{m} - \frac{1}{n}\right| = \left|\frac{1}{2} - \frac{1}{n}\right| = \frac{1}{2} - \frac{1}{n} < \frac{1}{2}.$$

We note that in each case, the required inequality is satisfied. Thus "$\left|\frac{1}{2} - \frac{1}{n}\right| \leq \frac{1}{2}$" is true for every $n \in \mathbb{N}$. Consequently, the given statement is true as well.

Proof Method

$\exists\ x \in S,\ \forall\ y \in T$

To prove $\exists\ x \in S,\ \forall\ y \in T,\ Q(x.y)$:

Propose a definite value of x from S. The value of x gets fixed and cannot depend on y, in particular, x should not be an expression in y. Use the *select method* on $y \in T$ to demonstrate $Q(x,y)$ is true for the proposed value of x.

Example 3

For every integer $n \geq 2$, there exists an integer m such that $n < m < 2n$.

Proof. Let n be an integer greater than 2. We need to provide a value of m that satisfies the property "$n < m < 2n$". As the value of m may depend on n, we will try to express m in terms of n.

Let $m = n + 1$. Since n is an integer, $n + 1$ must also be an integer, therefore m is indeed an integer.

Clearly $m = n + 1 > n$. On the other hand, $2n = n + n$. We are given that $n \geq 2$, therefore $n + n \geq n + 2 > n + 1$. In other words, $2n > m$. Thus, our proposed value of m satisfies the property

$$n < m < 2n.$$

Proof Method
$\forall\, x \in S,\ \exists\, y \in T$

To prove $\forall\, x \in S,\ \exists\, y \in T,\ Q(x.y)$:

Use the *select method* to choose x as a representative of S. Construct y in terms of x, and show that the resulting value of the expression is in T. Finally, demonstrate that $Q(x, y)$ is true.

Example 4

There exists a positive even integer s such that there exists a positive odd integer t such that $2^s + 3^t$ is prime.

Proof. Let $s = 2$ and $t = 1$. Then

$$2^2 + 3^1 = 4 + 3 = 7,$$

which is a prime. Therefore the given statement is true.

Proof Method
$\exists\, x \in S,\ \exists\, y \in T$

To prove $\exists\, x \in S,\ \exists\, y \in T,\ Q(x.y)$:

Find a value of x from S and a value of y from T. Show that $Q(x, y)$ is satisfied.

10.2.1 Negating Nested Quantifiers

A statement involving nested quantified variables is negated layer-by-layer.

Here are the general rules:

1. $\neg\,(\forall\, x \in S, \forall\, y \in T,\ Q(x, y)) \equiv \exists\, x \in S,\ \exists\, y \in T,\ \neg Q(x, y)$
2. $\neg\,(\forall\, x \in S, \exists\, y \in T,\ Q(x, y)) \equiv \exists\, x \in S,\ \forall\, y \in T,\ \neg Q(x, y)$
3. $\neg\,(\exists\, x \in S, \forall\, y \in T,\ Q(x, y)) \equiv \forall\, x \in S,\ \exists\, y \in T,\ \neg Q(x, y)$
4. $\neg\,(\exists\, x \in S, \exists\, y \in T,\ Q(x, y)) \equiv \forall\, x \in S,\ \forall\, y \in T,\ \neg Q(x, y)$

For instance, the negation of the statement "$\exists\, n \in \mathbb{N},\ \forall\, m \in \mathbb{Z},\ n \mid m$" is given by

$$\forall\, n \in \mathbb{N},\ \exists\, m \in \mathbb{Z},\ n \nmid m.$$

REMARK

To disprove a statement involving quantifiers, we usually just prove that the negation of the statement is true.

10.3 More Examples with Nested Quantifiers

Prove or disprove each of the following statements.

1. There exists a non-negative integer k such that for every integer n, $k < n$.

   Solution: The given statement is false. Let k be any non-negative integer. Consider $n = k - 1$. Then $k > n$. So we cannot find a non-negative integer k that would satisfy $k < n$ for all values of n. □

2. For every two integers a and c, there exists an integer b such that $a + b = c$.

   Solution: The given statement is true.

   Proof: Let $a, c \in \mathbb{Z}$. Suppose $b = c - a$. Since a and c are integers, therefore $c - a$ must also be an integer, thus $b \in \mathbb{Z}$. Consequently,

   $$a + b = a + (c - a) = c.$$

   □

3. For every $S \in \mathcal{P}(\mathbb{N})$, there exists $t \in S$ such that $t \geq 1$.

   Solution: The given statement is false. Let $S = \emptyset$. Since $\emptyset$ is a subset of $\mathbb{N}$, therefore it is an element of the power set $\mathcal{P}(\mathbb{N})$.

   However, for the empty set, the statement "$\exists\ t \in \emptyset,\ t \geq 1$" is vacuously false. Hence the empty set acts as a counter example to the above statement. □

4. For every non-empty $S \in \mathcal{P}(\mathbb{N})$, there exists $t \in S$ such that $t \geq 1$.

   Solution: The given statement is true.

   Proof: Suppose S is a non-empty subset of $\mathbb{N}$. Since S is non-empty, it must have at least one element, which we shall call t. As $S \subseteq \mathbb{N}$, we get $t \in \mathbb{N}$.

   Now, we know that 1 is the smallest positive integer. Thus, $t \in \mathbb{N}$ implies $t \geq 1$. □

Self Check 1

Prove or disprove the following statements.

1. Suppose $S = \{1, 3, 5\}$ and $T = \{6, 14\}$. For every $x \in S$ there exists some $y \in T$ such that $x + y$ is a prime.

2. There exists a non-negative integer k such that for every non-negative integer n, $k < n$.

3. There exists a non-negative integer k such that for every positive integer n, $k < n$.

4. For every non-negative integer n, there exists a non-negative integer k such that $k < n$.

REMARK (Order of Nested Quantifiers)

It is important to keep track of the order in which the quantified variables appear in a statement. It is also important to note the corresponding domain for each variable. Suppose S and T are two sets, and $Q(x, y)$ is an open sentence. In general, the following rules hold.

1. "$\forall\, x \in S,\ \exists\, y \in T,\ Q(x, y)$" is not logically equivalent to "$\exists\, y \in T,\ \forall\, x \in S,\ Q(x, y)$".

   Similarly, "$\exists\, x \in S,\ \forall\, y \in T,\ Q(x, y)$" is not logically equivalent to "$\forall\, y \in T,\ \exists\, x \in S,\ Q(x, y)$".
2. "$\forall\, x \in S,\ \exists\, y \in T,\ Q(x, y)$" is not logically equivalent to "$\forall\, x \in T,\ \exists\, y \in S,\ Q(x, y)$". whereas $\forall\, x \in \mathbb{N},\ \exists\, y \in \mathbb{Z},\ x = y$ is true.

Exercise 1

Consider the following mathematical statements:

$$\begin{array}{ll} \mathbf{A} & : \forall\, x \in \mathbb{R}\ \exists\, y \in \mathbb{R}\ \left(y^2 - 2xy + x^2 - 2x + 2y \leq 0\right), \\ \mathbf{B} & : \exists\, y \in \mathbb{R}\ \forall\, x \in \mathbb{R}\ \left(y^2 - 2xy + x^2 - 2x + 2y \leq 0\right). \end{array}$$

Prove that statement **A** is true and disprove statement **B**.

10.4 Functions and Surjections

One of the most fundamental notions of modern mathematics is that of a function. You may be familiar with the concept of functions from studying high school mathematics. We may formally define functions with the help of nested quantifiers.

Definition 10.4.1

Function, Domain, Codomain, Value

Let S and T be two sets. A **function** f from S to T, denoted by $f : S \to T$, is a rule that assigns to each element $s \in S$ a unique element $f(s) \in T$. The set S is called the **domain** of the function and the set T is called the **codomain**. The element $f(s)$ is called the **value** of the function f at s.

In terms of nested quantifiers, $f : S \to T$ is a function if and only if

> For every $s \in S$, there exists a unique $t \in T$ such that $f(s) = t$.

Sometimes a picture helps. In this case, Figure 10.4.1 illustrates when a rule is *not* a function.

If there exists an element in the domain which maps to more than one element in the codomain, then the given rule is not a function.

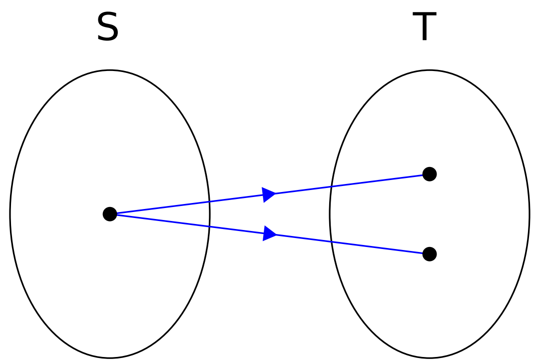


Figure 10.4.1: *NOT* a Function

Example 5

Prove that $f : \mathbb{Q} \to \mathbb{Z}$ defined by

$$f\left(\frac{a}{b}\right) = a + b$$

is not a function.

Solution: Note that $\frac{1}{3} = \frac{2}{6}$ in $\mathbb{Q}$. However, $f\left(\frac{1}{3}\right) = 1 + 3 = 4$, whereas $f\left(\frac{2}{6}\right) = 2 + 6 = 8$. As $4 \neq 8$, f cannot be a function.

Suppose $f : S \to T$ is a function with domain S and codomain T. The set of values that can be obtained by the function f is a subset of T, known as the **image of** f. For example, the familiar function $\sin x$ is often defined with domain $\mathbb{R}$, codomain $\mathbb{R}$ and image $[-1, 1]$. In special cases, the image of f and the codomain of f may be the same set.

Definition 10.4.2
Onto, Surjective

Let S and T be two sets. A function $f : S \to T$ is **onto** (or **surjective**) if and only if for every $y \in T$ there exists an $x \in S$ so that $f(x) = y$.

More prosaically, every element of T is a value of some element of S.

In Calculus, S and T are often equal to $\mathbb{R}$ or are subsets of $\mathbb{R}$.

The important observation for us is that the definition contains two quantifiers. The order of quantifiers matters. We should be able to determine the structure of any proof that a function is onto.

10.4.1 Graphically

As with the illustration of a rule that is not function, sometimes a picture helps to illustrate when a function is not surjective. See Figure 10.4.2.

If there exists an element in the codomain which is not the value of any element in the domain, then the given function is not surjective.

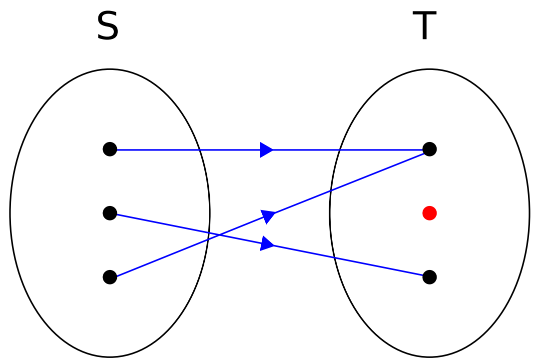


Figure 10.4.2: *NOT* Surjective

10.4.2 Reading a proof about Surjection

Let's work through an example. Notice how closely the proof follows our proof in progress.

Proposition 1 Let $m \neq 0$ and b be fixed real numbers. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = mx + b$ is onto.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let $y \in \mathbb{R}$.
2. Consider $x = (y - b)/m$.
3. Since $y \in \mathbb{R}$, $x \in \mathbb{R}$.
4. But then $f(x) = f((y - b)/m) = m((y - b)/m) + b = y$ as needed.

□

Let's perform an analysis of this proof.

Analysis of Proof The definition of *onto* uses a nested quantifier.

Hypothesis: $m \neq 0$ and b are fixed real numbers. $f(x) = mx + b$.

Conclusion: $f(x)$ is onto.

Core Proof Technique: Nested quantifiers.

Preliminary Material: Let us remind ourselves of the definition of the defining property of *onto* as it applies in this situation.

For every $y \in \mathbb{R}$ there exists $x \in \mathbb{R}$ so that $f(x) = y$.

Sentence 1 *Let $y \in \mathbb{R}$.*

The first quantifier in the definition of onto is a universal quantifier so the author uses the Select Method. That is, the author chooses an element (y) in the domain ($\mathbb{R}$). The author must now show that the open sentence is satisfied (there exists an $x \in \mathbb{R}$ so that $f(x) = y$).

Sentence 2 *Consider $x = (y - b)/m$.*

The second quantifier in the definition is a nested existential quantifier so the author uses the Construct Method. The constructed object in this example is not surprising – we can simply solve for x in $y = mx + b$. In general, though, it can be difficult to construct a suitable object. Note also that the choice of x depends on y so it is not surprising that x is a function of y.

Sentence 3 *Since $y \in \mathbb{R}$, $x \in \mathbb{R}$.*

Because this step is usually straightforward, it is often omitted. It is included here to emphasize that the constructed object lies in the appropriate domain.

Sentence 4 *But then $f(x) = f((y - b)/m) = m((y - b)/m) + b = y$ as needed.*

Here the author confirms that the open sentence is satisfied.

10.4.3 Discovering a proof about Surjection

Having read a proof, let's discover one.

Proposition 2 The function $f : [1, 2] \to [4, 7]$ defined by $f(x) = x^2 + 3$ is onto.

We can begin with the basic proof structure that we discussed earlier.

Proof in Progress

1. Let $y \in [4, 7]$.
2. Consider $x = \ldots$. *We must construct x.*
3. Show that $x \in [1, 2]$. *To be completed.*
4. Now we show that $f(x) = y$. *To be completed.*

What is our candidate value for x? Since x must satisfy

$$y = x^2 + 3$$

we can solve for x to get

$$x = \pm\sqrt{y - 3}$$

Since we want $x \in [1, 2]$, we will choose the positive square root. Let's update the proof in progress.

Proof in Progress

1. Let $y \in [4, 7]$.

2. Consider $x = \sqrt{y-3}$.
3. Show that $x \in [1,2]$. *To be completed.*
4. Now we show that $f(x) = y$. *To be completed.*

It is not immediately obvious that $x \in [1,2]$. Some arithmetic manipulation with inequalities helps us here. Since $y \in [4,7]$, we know that

$$4 \leq y \leq 7$$

Subtracting three gives

$$1 \leq y - 3 \leq 4$$

Now taking the positive square root gives

$$1 \leq \sqrt{y-3} \leq 2$$

and since $x = \sqrt{y-3}$ we have

$$1 \leq x \leq 2$$

which is exactly what we need. We can update our proof in progress.

Proof in Progress

1. Let $y \in [4,7]$.
2. Consider $x = \sqrt{y-3}$.
3. Now
$$4 \leq y \leq 7 \Rightarrow 1 \leq y-3 \leq 4 \Rightarrow 1 \leq \sqrt{y-3} \leq 2 \Rightarrow 1 \leq x \leq 2$$
4. Now we show that $f(x) = y$. *To be completed.*

Substitution will give us the last step. Here is a complete proof. Note that techniques are not named and the steps in the arithmetic are not explicitly justified. These are left to the reader.

Proof: Let $y \in [4,7]$. Consider $x = \sqrt{y-3}$. Now

$$4 \leq y \leq 7 \Rightarrow 1 \leq y-3 \leq 4 \Rightarrow 1 \leq \sqrt{y-3} \leq 2 \Rightarrow 1 \leq x \leq 2$$

Since

$$f(x) = x^2 + 3 = (\sqrt{y-3})^2 + 3 = y$$

f is onto. □

The choice of the domain and codomain for the function is important. Consider the statement

Statement 3 The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 3$ is onto.

This is very similar to the proposition we just proved, and you might think that the same proof would work. But it doesn't. Consider the choice $y = 0 \in \mathbb{R}$. What value of x maps to 0? Since $f(x) = x^2 + 3 \geq 3$ for all real numbers x, there is no choice of x so that $f(x) = 0$, and Statement 3 is false.

10.5 Practice

1. The statement

   There exist integers a and b such that both $ab < 0$ and $a + b > 0$.

   can be expressed in symbolic form as

   $$\exists\, a \in \mathbb{Z}, \exists\, b \in \mathbb{Z},\ (ab < 0) \wedge (a + b > 0)\,.$$

   Express the following statements in their symbolic forms.

   (a) For all real numbers x and y, $x \neq y$ implies that $x^2 + y^2 > 0$.

   (b) For every even integer a and odd integer b, there exists a rational number c such that either $a < c < b$ or $b < c < a$.
   Note: We use $\mathbb{Q}$ to denote the set of rational numbers.

   (c) For every positive integer a, there exists an integer b with $|b| < a$ such that b divides a.

2. For each of the following statements, write down the negation of the statement (without using any negative words such as "not" or the $\neg$ symbol, but negative math symbols like $\neq, \nmid$ are allowed).

   (a) There exists $x \in \mathbb{N}$ such that for all $y \in \mathbb{N}$, $y | x$.

   (b) For all $x, y \in \mathbb{R}$, if $x < y$, then there exists $z \in \mathbb{R}$ such that $x < z < y$.

   (c) There exist $X, Y \in \mathcal{P}(\mathbb{Z})$ such that for all $Z \in \mathcal{P}(\mathbb{Z})$, $X \subseteq Z \subseteq Y$.

   (d) For all real numbers x and y, $x \neq y$ implies that $x^2 + y^2 > 0$.

3. Prove or disprove each of the following statements involving nested quantifiers.

   (a) For all $n \in \mathbb{Z}$, there exists an integer $m \neq 2$ such that $k \mid (n^3 - n)$.

   (b) For every positive integer a, there exists an integer b with $|b| < a$ such that b divides a.

   (c) There exists an integer n such that $m(n - 3) < 1$ for every integer m.

   (d) There exists a positive integer n such that $-nm < 0$ for every integer m.

4. Consider the following statement.

   A: There exists a real number L such that for every positive real number ε, there exists a positive real number δ such that for all real numbers x, if $|x| < \delta$, then $|3x - L| < \varepsilon$.

   (a) Express the statement **A** in symbols.
   Note: We may use the symbol $\mathbb{R}^{>0}$ to denote the set of (strictly) positive real numbers.

   (b) Prove that statement **A** is true.

5. Are the following functions onto? Justify your answer with a proof.

   (a) $f : \mathbb{Z} \to \mathbb{Z}$, defined by $f(n) = 2n + 1$.

   (b) $f : \mathbb{Z} \to \mathbb{Z}$, defined by $f(n) = n - 3$.

   (c) $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 + 4x + 9$.

   (d) $f : (\mathbb{R} - \{2\}) \to (\mathbb{R} - \{5\})$, defined by $f(x) = \frac{5x+1}{x-2}$.

Part III

More Proof Techniques

Chapter 11

Negations and Contradictions

11.1 Objectives

The technique objectives are:

1. To learn when to use negations in proofs.
2. To learn how to read and discover proofs by contradiction.
3. Read a proof of *Prime Factorization*.
4. Discover a proof of *Infinitely Many Primes*.

Let us begin with a riddle. Suppose a group of three mathematicians and four engineers are seated at a round table. Assuming there are no empty chairs, is it possible to make sure that no two engineers sit next to each other?

We may answer the riddle in the following way. Suppose each engineer sits between two mathematicians. Then there must be a mathematician to the right of each engineer, so we get that there must be at least four mathematicians at the table. However, the riddle stipulates that there are three mathematicians in the group, so saying that there are four or more mathematicians at the table does not make any sense.

We reached a conclusion that must be false. The only way this can happen is if our initial assumptions was also false, that is, it is not possible for each engineer to sit between two mathematicians. In other words, we have proven that there must be at least two engineers who sit next to each other. We have just seen an example of a *proof by contradiction*.

11.2 Proof by Contradiction

Definition 11.2.1
Contradiction

Let A be a statement. Note that either A or $\neg A$ must be false, so the compound statement $A \wedge (\neg A)$ is always *false*. The statement "$A \wedge (\neg A)$ is true" is called a **contradiction**.

In other words, any time we come across an argument that claims both A and $\neg A$ to be true, we say that there must be a contradiction in the argument.

Proof Method

Proof by Contradiction

Suppose we are trying to prove statement C.

Start with the assumption that C is false (or that $\neg C$ is true).

Use a series of true implications to deduce that a statement A is true as a direct consequence of C being false, where $\neg A$ is also true because of an earlier assumption or because of some proposition that we have already proven.

As a result, we get a situation where $A \wedge (\neg A)$ is true, also known as a contradiction. Since $A \wedge (\neg A)$ must be false, we trace back our steps to conclude that our initial assumption is not correct.

Thus, we have proven that C is true.

Suppose that we wish to prove that the statement "A implies B" is true. To use a contradiction, we must assume that $\neg(A \implies B)$ is true. Hence, our assumption becomes "A is true and B is false". We must now proceed to find a contradiction. Let us demonstrate this with an example.

Example 1

Let a, b and c be integers. Prove that if $a \mid (b+c)$ and $a \nmid b$, then $a \nmid c$.

Solution: Assume, for the sake of contradiction, that $a \mid (b+c)$ and $a \nmid b$ and $a \mid c$.

Since $a \mid (b+c)$ and $a \mid c$, then by the *Divisibility of Integer Combinations* (*DIC*), we get that

$$a \mid [(1)(b+c) + (-1)(c)],$$

or in other words, $a \mid b$.

Note that a part of our initial assumptions was that $a \nmid b$, and now we have concluded that $a \mid b$. Clearly, we have a contradiction.

As a result, the implication if $a \mid (b+c)$ and $a \nmid b$, then $a \nmid c$ must be true.

11.2.1 When To Use Contradiction

We have mostly used the Direct Method to discover proofs, often in conjunction with one of the methods associated with quantifiers. There are times when this is difficult. A **proof by contradiction** provides a new method. Unfortunately, it is not always clear what contradiction to find, or how to find it. What is more clear is *when* to use contradiction.

The general rule of thumb is to use contradiction when the statement *NOT B* gives you more useful information that B, the statement you wish to prove. There are typically two instances when this is useful. The first instance is when the statement B is one of only two alternatives. For example, if the conclusion B is the statement $f(x) = 0$ then the only two possibilities are $f(x) = 0$ and $f(x) \neq 0$. *NOT B* is the statement $f(x) \neq 0$ which could be useful to you. The second instance is when B contains a negation. As we saw earlier, *NOT B* eliminates the negation.

11.2.2 A more substantial Proof by Contradiction

Suppose we want to prove the following proposition.

Proposition 1 **(Prime Factorization (PF))**

Let $n \in \mathbb{N}$. If n is an integer greater than 1, then n can be expressed as a product of primes.

Example 2 The integers $2, 3, 5$ and 7 are primes and each is a product unto itself, that is, it is a product consisting of one factor. The integers $4 = 2 \times 2$, $6 = 2 \times 3$ and $8 = 2 \times 2 \times 2$ have been factored as products of primes.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let N be the smallest integer, greater than 1, that cannot be written as a product of primes.
2. N is not itself a prime, so we can write $N = rs$ where $1 < r \leq s < N$.
3. Since r and s are less than N, they can be written as a product of primes.
4. But then it follows that $N = rs$ can be written as a product of primes, a contradiction.

□

Analysis of Proof An interpretation of sentences 1 through 4 follows.

Sentence 1 *Let N be the smallest integer, greater than 1, that cannot be written as a product of primes.*

The first sentence of a proof by contradiction usually gives the specific form of *NOT B* that the author is going to work with. In this case, the author identifies that this is a proof by contradiction by assuming the existence of an object which contradicts the conclusion, an integer N which *cannot* be written as a product of primes. Moreover, of all such candidates for N the author chooses the smallest one. Though it may not be obvious when first encountering the proof why the author would stipulate such a condition, it always has to do with something needed later in the argument.

Once you know that this is a proof by contradiction, look ahead to find the contradiction. In this case, the contradiction appears in Sentence 4.

Sentence 2 *N is not itself a prime, so we can write $N = rs$ where $1 < r \leq s < N$.*

If N were prime, then N by itself is a product of primes (with just one factor). But the author has assumed that N is not a product of primes, hence N is composite and can be written as the product of two non-trivial factors r and s.

Sentence 3 *Since r and s are less than N, they can be written as a product of primes.*

This sentence makes it clear why N needs to be the *smallest* integer that cannot be written as a product of primes. In order to generate the contradiction, r and s must be written as products of primes. If it were the case that N was not the smallest such integer, it might be the case that neither r nor s could be written as a product of primes.

Sentence 4 *But then it follows that $N = rs$ can be written as a product of primes, a contradiction.*

Since both r and s can be written as a product of primes, the product $rs = N$ can certainly be written as a product of primes. But this contradicts the assumption in Sentence 1 that N cannot be written as a product of primes.

Since our reasoning is correct, it must be the case that our assumption that there is an integer which cannot be written as a product of primes is incorrect. That is, every integer can be written as a product of primes.

11.2.3 Discovering and Writing a Proof by Contradiction

Discovering a proof by contradiction can be difficult and often requires several attempts at finding the path to a contradiction. Let's see how we might discover a proof to a famous theorem recorded by Euclid.

Proposition 2 **(Infinitely Many Primes (INF P))**

The number of primes is infinite.

We should always be clear about our hypothesis and conclusion. There is no explicit hypothesis in this case and the conclusion is the statement

Conclusion: The number of primes is infinite.

This statement contains a negation, *infinite* is an abbreviation of *not* finite, and so is a candidate for a proof by contradiction. Our first statement in a proof by contradiction is a negation of the conclusion so we have

Proof in Progress

1. Assume that the number of primes is finite. (This is NOT B.)
2. *To be completed.*

Now comes the tough part. What do we do from here? How do we generate a contradiction? Well, if the number of primes is finite, could we somehow use that assumption to find a "new" prime not in our finite list of primes? Our candidate should not have any of the finite primes as a factor. At this point, it sounds like we need to list our primes.

Proof in Progress

1. Assume that the number of primes is finite. (This is NOT B.)
2. Label the finite number of primes $p_1, p_2, p_3, \ldots, p_n$.
3. *To be completed.*

Now we have a way to express a candidate for a "new" prime.

Proof in Progress

1. Assume that the number of primes is finite. (This is *NOT* B.)
2. Label the finite number of primes $p_1, p_2, p_3, \ldots, p_n$.
3. Consider the integer $N = p_1 p_2 p_3 \cdots p_n + 1$.
4. *To be completed.*

Clearly N is larger than any of the p_i so, by the first sentence, N cannot be in the list of primes. Thus

Proof in Progress

1. Assume that the number of primes is finite. (This is *NOT* B.)
2. Label the finite number of primes $p_1, p_2, p_3, \ldots, p_n$.
3. Consider the integer $N = p_1 p_2 p_3 \cdots p_n + 1$.
4. Since $N > p_i$ for all i, N is not a prime.
5. *To be completed.*

And this is where we can find our contradiction. N has no non-trivial factors since dividing N by any of the p_i leaves a remainder of 1. But that means N cannot be written as a product of primes, which contradicts the previous proposition. The contradiction in this proof arises from a result which is inconsistent with something else we have proved.

Proof in Progress

1. Assume that the number of primes is finite. (This is *NOT* B.)
2. Label the finite number of primes $p_1, p_2, p_3, \ldots, p_n$.
3. Consider the integer $N = p_1 p_2 p_3 \cdots p_n + 1$.
4. Since $N > p_i$ for all i, N is not a prime.
5. Since $N = p_i q + 1$ for each of the primes p_i, no p_i is a factor of N. Hence N cannot be written as a product of primes, which contradicts our previous proposition.

Putting all of the statements together gives the following proof.

Proof: Assume that there are only a finite number of primes, say $p_1, p_2, p_3, \ldots, p_n$. Consider the integer $N = p_1 p_2 p_3 \cdots p_n + 1$. Since $N > p_i$ for all i, N is not a prime. But $N = p_i q + 1$ for each of the primes p_i, so no p_i is a factor of N. Hence N cannot be written as a product of primes, which contradicts our previous proposition. $\square$

11.3 Practice

1. Prove the following statements using a proof by contradiction.

   (a) There is no smallest positive real number.

   (b) For all odd integers n, n cannot be expressed as the sum of three even integers.

   (c) If a is an even integer and b is an odd integer, then $4 \nmid (a^2 + 2b^2)$.

   (d) For every integer m such that $2 \mid m$ and $4 \nmid m$, there are no integers x and y that satisfy $x^2 + 3y^2 = m$.

   (e) The sum of a rational number and an irrational number is irrational.

   (f) The real number $\sqrt{2}$ is irrational.

   (g) Let x be a non-zero real number. If $x + \frac{1}{x} < 2$, then $x < 0$.

Chapter 12

Proving Implications: Contrapositives and Other Proof Techniques

12.1 Objectives

We will study implications in more detail. The objectives of this chapter are

1. Learn how to prove statement using the *contrapositive*.
2. Develop proof methods for more complicated implications.

12.2 Proof by Contrapositive

We now have some basic idea about implications and the direct proof method for proving implications. The recipe for a direct proof is simple: assume that the hypothesis is true and use it to prove the conclusion. Unfortunately, there are several implications that are very difficult to prove using a direct proof.

Example 1

Let x be a real number. Consider the implication

> If $x^5 - 3x^4 + 2x^3 - x^2 + 4x - 1 \geq 0$, then $x \geq 0$.

Let us try to prove this implication using a direct proof. If we assume that the hypothesis $x^5 - 3x^4 + 2x^3 - x^2 + 4x - 1 \geq 0$ is true, then we have a monstrous polynomial inequality to deal with. It will be very difficult to try to get information about x from this hypothesis alone. We must find a better method to solve this problem.

Definition 12.2.1
Contrapositive

The statement $\neg B \implies \neg A$ is called the **contrapositive** of $A \implies B$.

We can use truth tables to show that $(A \implies B) \equiv (\neg B \implies \neg A)$.

A	B	$A \implies B$	$\neg B$	$\neg A$	$\neg B \implies \neg A$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The logical equivalence of an implication and its contrapositive is extremely useful. If proving $A \implies B$ seems difficult, we could try to prove $\neg B \implies \neg A$ instead. It may be easier!

Proof Method

Proving the Contrapositive

We want to prove $A \implies B$.

Replace the given implication $A \implies B$ with its contrapositive $\neg B \implies \neg A$. Next, prove the implication $\neg B \implies \neg A$, usually through a direct proof.

That is, assume $\neg B$ is true and thus try to deduce that $\neg A$ must be true as well.

Since the two statements are logically equivalent, proving $\neg B \implies \neg A$ is true establishes that $A \implies B$ is true as well.

Example 2

From the previous example, replace the given implication - if $x^5 - 3x^4 + 2x^3 - x^2 + 4x - 1 \geq 0$, then $x \geq 0$ - by its contrapositive

If $x < 0$ then $x^5 - 3x^4 + 2x^3 - x^2 + 4x - 1 < 0$.

We will now prove this contrapositive using a direct proof. Let us assume that $x < 0$. Then $x^5 < 0$, $2x^3 < 0$ and $4x < 0$. n addition, $-3x^4 < 0$, $-x^2 < 0$ and $-1 < 0$. As all the terms are negative, we add them to get

$$x^5 - 3x^4 + 2x^3 - x^2 + 4x - 1 < 0.$$

Since the contrapositive is true, the original implication must be true as well.

When To Use The Contrapositive

Suppose you need to prove the statement $A \implies B$. Use the contrapositive when the statement *NOT A* or the statement *NOT B* gives you useful information. This is most likely to occur when A or B contains a negation. Especially when both A and B contain negations, it is highly likely that using the contrapositive will be productive.

Another possible motivation for using contrapositive may come from the statements A or B themselves. If A or B contains a condition that is one of only two possibilities, then the negation, which indicates the second possibility, may be useful. For example, an integer can be either odd or even (not both). So if we have a statement about an even integer, the contrapositive will give us a statement about an odd integer.

In addition to that, we often use the method of contrapositve when the hypothesis of an implication looks more complicated than the conclusion.

Finally, these are just rules of thumb. There are no rules that tell you exactly when the contrapositive should be used. However, with practice, you should develop a feel for when it is a good technique to attempt.

REMARK

There is a subtle connection between a proof by contrapositive and a proof by contradiction for an implication $A \implies B$. In a proof by contradiction, we may start by assuming $A \wedge (\neg B)$ is true and end up deduce that A must be false, that is, $\neg A$ is true, to get a contradiction. However, this is the same as proving the contrapositive $\neg B \implies \neg A$.

So a proof by contrapositive may be viewed as a very special instance of a proof by contradiction.

Reading a Proof That Uses the Contrapositive

Consider the following proposition.

Proposition 1 Suppose a is an integer. If $32 \nmid ((a^2+3)(a^2+7))$ then a is even.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. We will prove the contrapositive.
2. If a is odd we can write a as $2k+1$ for some integer k.
3. Substitution gives

$$\begin{aligned}(a^2+3)(a^2+7) &= ((2k+1)^2+3)((2k+1)^2+7)\\ &= (4k^2+4k+1+3)(4k^2+4k+1+7)\\ &= (4k^2+4k+4)(4k^2+4k+8)\\ &= 4(k^2+k+1)\times 4(k^2+k+2)\\ &= 16(k^2+k+1)(k^2+k+2)\end{aligned}$$

4. Since one of k^2+k+1 or k^2+k+2 must be even, and the last line above shows that a factor of 16 already exists disjoint from $(k^2+k+1)(k^2+k+2)$, $(a^2+3)(a^2+7)$ must contain a factor of 32. That is, $32 \mid ((a^2+3)(a^2+7))$.

□

Analysis of Proof As usual, we begin by identifying the hypothesis and the conclusion.

Hypothesis: A: $32 \nmid ((a^2+3)(a^2+7))$.

Conclusion: B: a is even.

Since the hypothesis of the proposition contains a negation, and the conclusion is one of two possible choices, it makes sense to consider the contrapositive.

For the contrapositive

Hypothesis: $NOT\ B$: a is odd.

Conclusion: $NOT\ A$: $32 \mid ((a^2+3)(a^2+7))$

Sentence 1 *We will prove the contrapositive.*

Not all authors will be so obliging as to state the proof technique up front. The provided proof would also be correct if this sentence was omitted. Correct, but less easy to understand.

Sentence 2 *If a is odd we can write a as $2k+1$ for some integer k.*

This is the statement $NOT\ B$. Knowing from Sentence 1 that the author is using the contrapositive we would expect to see statements moving forward from the hypothesis of the contrapositive (a is odd) or backwards from the conclusion of the contrapositive ($32 \mid ((a^2+3)(a^2+7))$).

Sentence 3 *Substitution gives $(a^2+3)(a^2+7) = \ldots = 16(k^2+k+1)(k^2+k+2)$.*

This is just arithmetic.

Sentence 4 *Since one of k^2+k+1 or k^2+k+2 must be even, and the last line above shows that a factor of 16 already exists disjoint from $(k^2+k+1)(k^2+k+2)$, $(a^2+3)(a^2+7)$ must contain a factor of 32. That is, $32 \mid ((a^2+3)(a^2+7))$.*

These sentences establish the conclusion of the contrapositive. Since the contrapositive is true, the original statement is true.

12.3 More Complicated Implications

We have seen that the hypothesis and conclusion of an implication can be compound statements. Let us look as some examples that outline the process for proving such implications. The logical equivalences mentioned here can be proved using truth tables.

Example 3 **$((A \vee B) \implies C$ is logically equivalent to $(A \implies C) \wedge (B \implies C))$**

Let a, b and c be integers. Prove the implication

> If $a \mid b$ or $a \mid c$ then $a \mid (bc)$.

We prove the above implication by proving that both

1. if $a \mid b$ then $a \mid (bc)$, and
2. if $a \mid c$ then $a \mid (bc)$

are true. That is, we can approach this problem by considering cases.

Proof: Assume $a \mid b$ or $a \mid c$. We have

Case I: Assume $a \mid b$. Since $b \mid (bc)$, by *Transitivity of Divisibility* (*TD*), $a \mid (bc)$.

Case II: Assume $a \mid c$. Since $c \mid (bc)$, by *Transitivity of Divisibility* (*TD*), $a \mid (bc)$.

Since $a \mid (bc)$ in both cases, the given implication is true. $\square$

REMARK

Both cases in the previous example use the exact same logic, and in fact case II is a word-for-word rewrite of case I if we simply switch the variables b and c.

In proofs like these, it is redundant to go through both cases. Usually, we use the phrase **Without Loss Of Generality** and only show one case. It is implied that the other case will be proved in exactly the same way apart from some obvious interchange of variables.

12.3.1 Method of Elimination

Let A, B and C be statements. To prove implications of the form $A \implies (B \vee C)$, we usually resort to the method of elimination. We begin with an important exercise.

Exercise 1

Prove that

$$A \implies (B \vee C) \text{ is logically equivalent to } (A \wedge \neg B) \implies C$$

Proof Method
Elimination

To prove If A then B or C.

Prove the logically equivalent statement If A and $\neg B$, then C.

Example 4

Consider the following statement for some $x \in \mathbb{R}$.

If $x^2 - 7x + 12 \geq 0$, then $x \leq 3$ or $x \geq 4$.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Suppose that $x^2 - 7x + 12 \geq 0$ and $x > 3$.
2. Factoring gives $(x - 3)(x - 4) \geq 0$.
3. Since $x > 3$, $x - 3 > 0$.
4. Dividing the inequality in Sentence 2 by $x - 3$ gives $x - 4 \geq 0$, or
5. $x \geq 4$ as desired.

$\square$

Self Check 1 Analyze the proof above. Make sure to justify each sentence.

Proposition 2 Let U be a universal set containing sets S and T. Then

$$\overline{S \cap T} \subseteq \overline{S} \cup \overline{T}$$

This may be mystifying. The word *or* does not appear. But let's rephrase the statement as

$$\text{If } x \in \overline{S \cap T}, \text{ then } x \in \overline{S} \cup \overline{T}$$

or

$$\text{If } x \in \overline{S \cap T}, \text{ then } x \in \overline{S} \text{ or } x \in \overline{T}$$

Now the use of the word *or* is apparent. As usual, we begin by identifying the hypothesis, conclusion, core proof technique and preliminary material.

Hypothesis: $x \in \overline{S \cap T}$

Conclusion: $x \in \overline{S}$ or $x \in \overline{T}$

Core Proof Technique: Since *or* occurs in the conclusion, we will use the Elimination Method.

Preliminary Material: Properties of sets.

Since we will use the Elimination Method, we will negate the first part of the conclusion and establish the second part of the conclusion.

Proof in Progress

1. Suppose $x \in \overline{S \cap T}$ and $x \notin \overline{S}$.
2. *To be completed.*
3. Hence, $x \in \overline{T}$.

We can make some progress just by using set definitions. If $x \in \overline{S \cap T}$, then $x \notin S \cap T$. One might be tempted to say that this implies $x \notin S$ and $x \notin T$ but that would be wrong. (Can you find a counter-example?)

Now let's make use of the statement $x \notin \overline{S}$. Since $x \notin \overline{S}$, $x \in S$. Let's record what we have done.

Proof in Progress

1. Suppose $x \in \overline{S \cap T}$ and $x \notin \overline{S}$.
2. Since $x \in \overline{S \cap T}$, $x \notin S \cap T$.
3. Since $x \notin \overline{S}$, $x \in S$.

4. *To be completed.*
5. Hence, $x \in \overline{T}$.

In order for $x \in \overline{T}$ we must have $x \notin T$. What would happen if $x \in T$? Since $x \in S$ from Sentence 3 that would imply that $x \in S \cap T$, contradicting Sentence 2. So x cannot be in T, which is exactly what we need.

Here is a complete proof. Notice that the author assumes that the reader can make the transition from

$$\overline{S \cap T} \subseteq \overline{S} \cup \overline{T}$$

to

$$\text{If } x \in \overline{S \cap T}, \text{ then } x \in \overline{S} \text{ or } x \in \overline{T}$$

without remark.

Proof: Suppose $x \in \overline{S \cap T}$ and $x \notin \overline{S}$. Since $x \in \overline{S \cap T}$, $x \notin S \cap T$. Since $x \notin \overline{S}$, $x \in S$. Now $x \notin T$ for otherwise if $x \in T$, then $x \in S \cap T$, a contradiction. Since $x \notin T$, $x \in \overline{T}$ as required. □

12.4 Summary Example

Example 5 Let x be a real number. Consider the following statement about x:

Statement 3 If $x^2 - 3x + 2 \leq 0$ then x is between 1 and 2 (inclusive).

1. Rewrite the given statement in symbolic form.
   Solution: $\left(x^2 - 3x + 2 \leq 0\right) \implies (1 \leq x \leq 2)$.
2. State the hypothesis of Statement 3.
   Solution: $x^2 - 3x + 2 \leq 0$.
3. State the conclusion of Statement 3.
   Solution: $1 \leq x \leq 2$.
4. State the negation of Statement 3 without using the word "not" or the $\neg$ symbol.
   Solution: $\left(x^2 - 3x + 2 \leq 0\right) \wedge [(x < 1) \vee (x > 2)]$.
5. State the contrapositive of Statement 3.
   Solution: $[(x < 1) \vee (x > 2)] \implies \left(x^2 - 3x + 2 > 0\right)$
6. Prove or disprove Statement 3.
   Solution: Statement 3 is true.

Proof: We shall prove the given statement through its contrapositive:

$$[(x < 1) \vee (x > 2)] \implies \left(x^2 - 3x + 2 > 0\right).$$

Assume that $(x < 1)$ or $(x > 2)$. For a real number x, since $x < 1$ and $x > 2$ cannot be true simultaneously, this gives us two cases to work with.

Case I: Assume $x < 1$. Note that $x^2 - 3x + 2$ can be factored as $(x-1)(x-2)$. Since $x < 1$, therefore both $(x-1) < 0$ and $(x-2) < 0$. Thus, their product $(x-1)(x-2)$ must be positve. Hence $x^2 - 3x + 2 > 0$.

Case II: Assume $x > 2$. Then $(x-1) > 0$ and $(x-2) > 0$. Once again, the product $(x-1)(x-2)$ must be positive, so $x^2 - 3x + 2 > 0$.

□

12.5 Practice

1. Let x and y be integers. Prove that if $xy = 0$ then $x = 0$ or $y = 0$.
2. Let x be a real number. Prove that if $x^3 - 5x^2 + 3x \neq 15$ then $x \neq 5$.
3. Let a, b, c be integers. Prove that if $a \nmid b$ and $a \mid (b + c)$, then $a \nmid c$.
4. Let x and y be integers. Prove that If $3 \nmid xy$ then $3 \nmid x$ and $3 \nmid y$.
5. Let a and b be non-zero integers. Prove that if $a \mid b$ and $b \mid a$, then $a = \pm b$.
6. Consider the following statement.

   Statement: For all $x \in \mathbb{R}$, if $x^6 + 3x^4 - 3x < 0$, then $0 < x < 1$.

   (a) Rewrite the given statement in symbolic form.
   (b) State the hypothesis of the given statement.
   (c) State the conclusion of the given statement.
   (d) State the converse of the given statement.
   (e) State the contrapositive of the given statement.
   (f) State the negation of the given statement without using the word "not" or the $\neg$ symbol (but symbols such as $\neq$, $\nmid$, etc. are fine).
   (g) Prove that the given statement is true.

Chapter 13

Uniqueness, Injections and The Division Algorithm

13.1 Objectives

The technique objective is:

1. Learn how to prove a statement about uniqueness.
2. Prove the uniqueness of the quotient and the remainder from the Division Algorithm.

13.2 Introduction

To prove a statement of the form

> If ..., then there is a *unique* object x in the set S such that $P(x)$ is true.

there are basically two approaches.

1. **Demonstrate** that there is at least one object in the set S that satisfies P. **Assume** that there are two objects X and Y in the set S such that $P(X)$ and $P(Y)$ are true. **Show** that $X = Y$.
2. **Demonstrate** that there is at least one object in the set S that satisfies P. **Assume** that there are two *distinct* objects X and Y in the set S such that $P(X)$ and $P(Y)$ are true. **Derive** a contradiction.

You can use whichever is easier in the circumstance.

13.3 Showing $X = Y$

The method is as follows.

1. **Demonstrate** that there is at least one object in the set S that satisfies P.
2. **Assume** that there are two objects X and Y in the set S such that $P(X)$ and $P(Y)$ are true.
3. **Show** that $X = Y$.

For example, let us prove the following statement.

Proposition 1 If a and b are integers with $a \neq 0$ and $a \mid b$, then there is a unique integer k so that $b = ka$.

As usual, we begin by explicitly identifying the hypothesis and conclusion.

Hypothesis: a and b are integers with $a \neq 0$ and $a \mid b$.

Conclusion: There is a unique integer k so that $b = ka$.

The appearance of "unique" in the conclusion tells us to use one of the two approaches described in the previous section. In this case, we will assume the existence of two integers k_1 and k_2 and show that $k_1 = k_2$. But first, we need to show that at least one integer k exists, and this follows immediately from the definition of divisibility.

Proof in Progress

1. Since $a \mid b$, at least one integer k exists so that $b = ka$.
2. Let k_1 and k_2 be integers such that $b = k_1a$ and $b = k_2a$. (Note how closely this follows the standard pattern. k_1 corresponds to X. k_2 corresponds to Y. Both come from the set of integers and if $P(x)$ is the statement "$b = xa$", then $P(X)$ and $P(Y)$ are assumed to be true.)
3. *To be completed.*
4. Hence, $k_1 = k_2$.

The obvious thing to do is equate the two equations to get

$$k_1a = k_2a$$

Since a is not zero we can divide both sides by a to get

$$k_1 = k_2$$

A proof might look like the following.

Proof: Since $a \mid b$, by the definition of divisibility there exists an integer k so that $b = ka$. Now let k_1 and k_2 be integers such that $b = k_1a$ and $b = k_2a$. But then $k_1a = k_2a$ and dividing by a gives $k_1 = k_2$. □

13.4 Finding a Contradiction

The method is as follows.

1. **Demonstrate** that there is at least one object in the set S that satisfies P.
2. **Assume** that there are two *distinct* objects X and Y in the set S such that $P(X)$ and $P(Y)$ are true.
3. **Derive** a contradiction.

For example, let us prove the following statement.

Proposition 2 Suppose a solution to the simultaneous linear equations $y = m_1x + b_1$ and $y = m_2x + b_2$ exists. If $m_1 \neq m_2$, then there is a unique solution to the simultaneous linear equations $y = m_1x + b_1$ and $y = m_2x + b_2$.

As usual, we begin by explicitly identifying the hypothesis and conclusion.

Hypothesis: A solution to the simultaneous linear equations $y = m_1x+b_1$ and $y = m_2x+b_2$ exists. $m_1 \neq m_2$.

Conclusion: There is a unique solution to the simultaneous linear equations $y = m_1x + b_1$ and $y = m_2x + b_2$.

The appearance of "unique" in the conclusion tells us to use one of the two approaches described in the previous section. In this case, we will assume the existence of two distinct points of intersection and derive a conclusion.

Proof in Progress

1. Suppose that $y = m_1x + b_1$ and $y = m_2x + b_2$ intersect in the distinct points (x_1, y_1) and (x_2, y_2). (The existence of at least one solution is guaranteed by the hypothesis. Note again how closely this follows the standard pattern. (x_1, y_1) corresponds to X. (x_2, y_2) corresponds to Y. Both come from the set of ordered pairs and both satisfy the statement "are a solution to the simultaneous linear equations $y = m_1x + b_1$ and $y = m_2x + b_2$.")
2. *To be completed,* hence a contradiction.

But now if we substitute (x_1, y_1) and (x_2, y_2) into $y = m_1x + b_1$ we get

$$y_1 = m_1x_1 + b_1 \tag{13.1}$$
$$y_2 = m_1x_2 + b_1 \tag{13.2}$$

which implies that

$$y_1 - y_2 = m_1(x_1 - x_2)$$

Similarly, substituting (x_1, y_1) and (x_2, y_2) into $y = m_2x + b_2$ gives

$$y_1 - y_2 = m_2(x_1 - x_2)$$

Equating the two expressions for $y_1 - y_2$ gives

$$(m_1 - m_2)(x_1 - x_2) = 0$$

Since $m_1 \neq m_2$, $m_1 - m_2 \neq 0$ and we can divide by $(m_1 - m_2)$. This gives $x_1 - x_2 = 0$. That is, $x_1 = x_2$. But then,

$$y_1 - y_2 = m_1(x_1 - x_2) \text{ and } x_1 - x_2 = 0$$

imply

$$y_1 - y_2 = 0$$

That is, $y_1 = y_2$. But then the points (x_1, y_1) and (x_2, y_2) are not distinct, a contradiction.

Exercise 1 Write a proof for the preceding proposition.

13.5 One-to-one (Injective)

You may already be familiar with the concept of *one-to-one* functions, also known as *injections*. Let us now write a formal definition of one-to-one functions. The next definition uses nested quantifiers that are the same.

Definition 13.5.1 **One-to-one, Injective**

Let S and T be two sets. A function $f : S \to T$ is **one-to-one** (or **injective**) if and only if for every $x_1 \in S$ and every $x_2 \in S$, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

We should be able to recognize that the definition above contains the concept of uniqueness, although it is not spelled out explicitly. In particular, according to the above definition, a function f is one-to-one if and only for a given element y from the image of f, there is a unique $x \in S$ such that $y = f(x)$.

Let's work through an example. Notice how closely the proof follows the structure of a one-to-one proof.

Proposition 3 Let $m \neq 0$ and b be fixed real numbers. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = mx + b$ is one-to-one.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let $x_1, x_2 \in S$.
2. Suppose that $f(x_1) = f(x_2)$.
3. Now we show that $x_1 = x_2$.
4. Since $f(x_1) = f(x_2)$, $mx_1 + b = mx_2 + b$.
5. Subtracting b from both sides and dividing by m gives $x_1 = x_2$ as required.

□

Let's perform an analysis of this proof.

Analysis of Proof The definition of *one-to-one* uses a nested quantifier.

Hypothesis: $m \neq 0$ and b are fixed real numbers. $f(x) = mx + b$.

Conclusion: $f(x)$ is one-to-one.

Core Proof Technique: Nested quantifiers.

Preliminary Material: Let us remind ourselves of the definition of the defining property of *one-to-one* as it applies in this situation.

For every $x_1 \in \mathbb{R}$ and every $x_2 \in \mathbb{R}$, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

Sentence 1 *Let $x_1, x_2 \in \mathbb{R}$.*

The author combines the first two sentences of the structure of a one-to-one proof into a single sentence. This works because both of the first two quantifiers in the definition are universal quantifiers and so the author uses the Select Method twice. That is, the author chooses elements (x_1 and x_2) in the domain ($\mathbb{R}$). The author must now show that the open sentence is satisfied ($f(x_1) = f(x_2)$ implies that $x_1 = x_2$).

Sentences 2 and 3 *Suppose that $f(x_1) = f(x_2)$. Now we show that $x_1 = x_2$.*

The open sentence that must be verified is an implication, and $f(x_1) = f(x_2)$ is the hypothesis. To prove an implication, we assume the hypothesis and demonstrate that the conclusion, $x_1 = x_2$, is true.

Sentence 3 *Since $f(x_1) = f(x_2)$, $mx_1 + b = mx_2 + b$.*

This is just substitution.

Sentence 4 *Subtracting b from both sides and dividing by m gives $x_1 = x_2$ as required.*

Here the author confirms that the open sentence is satisfied. Observe that the hypothesis $m \neq 0$ is used here.

13.5.1 Discovering a proof about injections

Having read a proof, let's discover one.

Proposition 4 The function $f : [1, 2] \to [4, 7]$ defined by $f(x) = x^2 + 3$ is one-to-one.

We can begin with the basic proof structure that we discussed earlier.

Proof in Progress

1. Let $x_1, x_2 \in [1, 2]$.
2. Suppose that $f(x_1) = f(x_2)$.
3. Now we show that $x_1 = x_2$. *To be completed.*

The obvious starting point is to write down $f(x_1) = f(x_2)$ and see if algebraic manipulation can take us to $x_1 = x_2$. And that is indeed the case.

$$f(x_1) = f(x_2) \Rightarrow x_1^2 + 3 = x_2^2 + 3 \Rightarrow x_1^2 = x_2^2$$

We need to be careful here since $x_1^2 = x_2^2$ does not generally imply $x_1 = x_2$. For example, $x_1 = 5$ and $x_2 = -5$ satisfy $x_1^2 = x_2^2$ but not $x_1 = x_2$. However, in this case because the domain is $[1, 2]$ we are justified in taking the positive square root and concluding that $x_1 = x_2$. Here is a complete proof.

Proof: Let $x_1, x_2 \in [1, 2]$. Suppose that $f(x_1) = f(x_2)$. But then $x_1^2 + 3 = x_2^2 + 3$ and so $x_1^2 = x_2^2$. Since $x_1, x_2 \in [1, 2]$ we can take the positive square root of both sides to get $x_1 = x_2$. $\square$

Just as with onto functions, the choice of the domain and codomain for the function is important. Consider the statement

Statement 5 The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 3$ is one-to-one.

This is very similar to the proposition we just proved, but this statement is false. It is easier to see why by working with the contrapositive of $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Recall that the contrapositive is logically equivalent to the original statement. For one-to-one functions, we can make the following statement which is equivalent to the definition.

Statement 6 Let S and T be two sets. A function $f : S \to T$ is **one-to-one** (or **injective**) if and only if for every $x_1 \in S$ and every $x_2 \in S$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

For the function $f(x) = x^2 + 3$, consider $x_1 = 1$ and $x_2 = -1$. It is indeed the case that $x_1 \neq x_2$, but $f(x_1) = 4 = f(x_2)$ which contradicts the definition of one-to-one. So, $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 3$ is *not* one-to-one.

13.5.2 Graphically

As with the illustration of a function that is not surjective, sometimes a picture helps to illustrate when a function is not injective. See Figure 13.5.1.

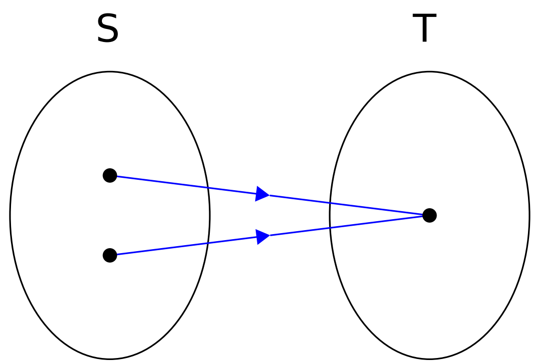


Figure 13.5.1: *NOT* Injective

If there exists an element in the codomain which is the value of more than one element in the domain, then the given function is not injective.

13.6 The Division Algorithm

In this section, we will see the partial proof of an important proposition about divisibility of integers.

Proposition 7 **(Division Algorithm)**

If a and b are integers and $b > 0$, then there exist unique integers q and r such that

$$a = qb + r \text{ where } 0 \leq r < b$$

If the statement of *Division Algorithm*, the integer a is called the **dividend** and b is called the **divisor**. The corresponding q is called the **quotient** and r is called the **remainder**.

Suppose that in a proof of the Division Algorithm it has already been established that integers q and r exist and only uniqueness remains. A proposed proof of uniqueness follows.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Suppose that $a = q_1 b + r_1$ with $0 \leq r_1 < b$. Also, suppose that $a = q_2 b + r_2$ with $0 \leq r_2 < b$ and $r_1 \neq r_2$.
2. Without loss of generality, we can assume $r_1 < r_2$.

3. Then $0 < r_2 - r_1 < b$ and
4. $(q_1 - q_2)b = r_2 - r_1$.
5. Hence $b \mid (r_2 - r_1)$.
6. By Bounds By Divisibility, $b \leq r_2 - r_1$ which contradicts the fact that $r_2 - r_1 < b$.
7. Therefore, the assumption that $r_1 \neq r_2$ is false and in fact $r_1 = r_2$.
8. But then $(q_1 - q_2)b = r_2 - r_1$ implies $q_1 = q_2$.

□

Let's make sure that we understand every line of the proof.

Sentence 1 *Suppose that* $a = q_1 b + r_1$ *with* $0 \leq r_1 < b$. *Also, suppose that* $a = q_2 b + r_2$ *with* $0 \leq r_2 < b$ *and* $r_1 \neq r_2$.

Since a statement about uniqueness appears in the conclusion, we would expect one of the two uniqueness methods to be used. In fact, both are used. The assertion of uniqueness applies to both q and r. Since the author writes $r_1 \neq r_2$, that is, there are distinct values of r_1 and r_2, we should look for a contradiction regarding r. But the author does not assume distinct values of q and so we would expect that the author will show $q_1 = q_2$.

Sentence 2 *Without loss of generality, we can assume* $r_1 < r_2$.

"Without loss of generality" is an expression that means the upcoming argument would hold identically if we made any other choice, so we will simply assume one of the possibilities.

Sentence 3 *Then* $0 < r_2 - r_1 < b$ *and*

This is a particularly important line. It comes, in part, from $r_1 < r_2$ by subtracting r_1 from both sides (this gives $0 < r_2 - r_1$) and by remembering that the largest possible value of r_2 is $b - 1$ and the smallest possible value of r_1 is 0, so the largest possible difference is $b - 1$, thus $r_2 - r_1 < b$

Sentence 4 $(q_1 - q_2)b = r_2 - r_1$.

This follows from equating $a = q_1 b + r_1$ and $a = q_2 b + r_2$.

Sentence 5 *Hence* $b \mid (r_2 - r_1)$.

This follows from the definition of divisibility.

Sentence 6 *By BBD,* $b \leq r_2 - r_1$ *which contradicts the fact that* $r_2 - r_1 < b$.

Note the importance of the strict inequality in the relation

$$b \leq r_2 - r_1 < b$$

Sentence 7 *Therefore, the assumption that* $r_1 \neq r_2$ *is false and in fact* $r_1 = r_2$.

The contradiction we were looking for. The Division Algorithm states that both q and r are unique. So far, only the uniqueness of r has been established.

Sentence 7 *But then* $(q_1 - q_2)b = r_2 - r_1$ *implies* $q_1 = q_2$.

And this is where the uniqueness of q is established. Originally, the author assumed the existence of q_1 and q_2 and now has shown that they are, in fact, the same.

Chapter 14

Simple Induction

14.1 Objectives

The technique objectives are:

1. Learn how to use sum and product notation, and recognize recurrence relations.
2. Learn how to use *Simple Induction*.

14.2 Notation

A number of examples we will discuss use sum, product and recursive notation that you may not be familiar with.

14.2.1 Summation Notation

The sum of the first ten perfect squares could be written as

$$1^2 + 2^2 + 3^2 + \cdots + 10^2$$

In mathematics, a more compact is used: $\sum_{i=1}^{10} i^2$.

Definition 14.2.1
Summation Notation

The notation

$$\sum_{i=m}^{n} x_i$$

is called **summation notation** and it represents the sum

$$x_m + x_{m+1} + x_{m+2} + \cdots + x_n$$

The summation symbol, $\sum$, is the upper case Greek letter *sigma*. The letter i is the **index of summation**; the letter m is the **lower bound of summation**, and the letter n is the **upper bound of summation**. The expression $i = m$ under the summation symbol means that the index i begins with an initial value of m and increments by 1 and stops when $i = n$. The index of summation is a *dummy* variable and any letter could be used in its place.

Example 1

$$\sum_{i=3}^{7} i^2 = 3^2 + 4^2 + 5^2 + 6^2 + 7^2$$

$$\sum_{k=0}^{3} \sin(k\pi) = \sin(0) + \sin(\pi) + \sin(2\pi) + \sin(3\pi)$$

$$\sum_{i=1}^{n} \frac{1}{i^2} = 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2}$$

There are a number of rules that help us manipulate sums.

Proposition 1 **(Properties of Summation)**

1. Multiplying by a constant

$$\sum_{i=m}^{n} cx_i = c\sum_{i=m}^{n} x_i \text{ where } c \text{ is a constant}$$

2. Adding two sums and subtracting two sums

$$\sum_{i=m}^{n} x_i + \sum_{i=m}^{n} y_i = \sum_{i=m}^{n}(x_i + y_i)$$

$$\sum_{i=m}^{n} x_i - \sum_{i=m}^{n} y_i = \sum_{i=m}^{n}(x_i - y_i)$$

3. Changing the bounds of the index of summation

$$\sum_{i=m}^{n} x_i = \sum_{i=m+k}^{n+k} x_{i-k}$$

The first two properties require indices with the same upper and lower bounds. The last property allows us to change the bounds of the index of summation, which is often useful when combining summation expressions.

Self Check 1 Restate the following using a summation notation

> The sum of the first n positive odd numbers is n^2.

14.2.2 Product Notation

Just as summation notation using $\sum$ is an algebraic shorthand for a sum, product notation using $\prod$ is an algebraic shorthand for a product.

Definition 14.2.2
Product Notation

The notation

$$\prod_{i=m}^{n} x_i$$

is called **product notation** and it represents the product

$$x_m \cdot x_{m+1} \cdot x_{m+2} \cdot \cdots \cdot x_n$$

The product symbol, $\prod$, is the upper case Greek letter *pi*. The index i and the upper and lower bounds m and n behave just as they do for sums.

Example 2

$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right) = \left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)\cdots\left(1-\frac{1}{n^2}\right)$$

14.2.3 Recurrence Relations

You are accustomed to seeing mathematical expressions in one of two ways: **iterative** and **closed form**. For example, the sum of the first n integers can be expressed iteratively as

$$1+2+3+\cdots+n$$

or in closed form as

$$\frac{n(n+1)}{2}$$

There is a third way.

Definition 14.2.3
Recurrence Relation

A **recurrence relation** is an equation that defines a sequence of numbers and which is generated by one or more initial terms, and expressions involving prior terms.

Example 3

(Sum of First n Integers)

We can define the sum of the first n terms recursively as

$$\begin{aligned}&f(1) = 1 \text{ and}\\&f(n) = f(n-1)+n \text{ for } n>1\end{aligned}$$

You are probably familiar with the Fibonacci sequence which is a recurrence relation.

Example 4

(Fibonacci Sequence)

The initial two terms are defined as $f_1 = 1$ and $f_2 = 1$. All subsequent terms are defined by the recurrence relation $f_n = f_{n-1} + f_{n-2}$. The first eight terms of the Fibonacci sequence are $1, 1, 2, 3, 5, 8, 13, 21$.

14.3 Principle of Mathematical Induction

Definition 14.3.1
Axiom

An **axiom** of a mathematical system is a statement that is assumed to be true. No proof is given. From axioms we derive propositions and theorems.

Sometimes axioms are described as *self-evident*, though many are not. Axioms are defining properties of mathematical systems. The *Principle of Mathematical Induction* is one such axiom.

Axiom 1

Principle of Mathematical Induction (POMI)

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$.

If

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

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

Induction is a common and powerful technique and should be a consideration whenever you encounter a statement of the form

For every integer $n \geq 1$, $P(n)$ is true.

where $P(n)$ is a statement that depends on n.

The structure of a proof by induction models the Principle of Mathematical Induction. The three parts of the structure are as follows.

Base Case *Verify that* $P(1)$ *is true.* Usually, we prove that a relation (for example, an equality such as $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$, or an inequality such as $3^n > n^2$, or divisibility such as $4 \mid (5^n - 1)$, etc.) holds true for $n = 1$. The typical approach in such a case is to substitute $n = 1$ on the left side and also on the right side of the relation separately, and show that you can obtain the same number or expression from both sides. This is usually easy, but it is best to write this step out completely.

Inductive Hypothesis *Assume that* $P(k)$ *is true for some integer* $k \geq 1$. It is best to write out the statement $P(k)$.

Note that we are using the *select method* on k, so it is important to mention that $P(k)$ is assumed true *for some* $k \in \mathbb{N}$. If the assumption stated $P(k)$ is true *for all* $k \in \mathbb{N}$, then the whole proof would fall apart.

Inductive Conclusion Using the assumption that $P(k)$ is true, *show that* $P(k+1)$ *is true.* Again, it is best to write out the statement $P(k+1)$ before trying to prove it.

14.3.1 Why Does Induction Work?

The basic idea is simple. We show that $P(1)$ is true. We then use $P(1)$ to show that $P(2)$ is true. And then we use $P(2)$ to show that $P(3)$ is true and continue indefinitely. That is

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \ldots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow \ldots$$

14.3.2 Two Examples of Simple Induction

Our first example is very typical and uses an equation containing the integer n.

Proposition 2 For every integer $n \in \mathbb{N}$,

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

Proof: We begin by formally writing out our inductive statement

$$P(n): \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Base Case We verify that $P(1)$ is true where $P(1)$ is the statement

$$P(1): \sum_{i=1}^{1} i^2 = \frac{1(1+1)(2\times 1+1)}{6}.$$

As in most base cases involving equations, we can evaluate the expressions on the left hand side and right hand side of the equals sign. The left hand side expression evaluates to

$$\sum_{i=1}^{1} i^2 = 1^2 = 1$$

and the right hand side expression evaluates to

$$\frac{1(1+1)(2\times 1+1)}{6} = 1.$$

Since both sides equal each other, $P(1)$ is true.

Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 1$.

$$P(k): \sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

$$P(k+1): \sum_{i=1}^{k+1} i^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

This is the difficult part. When working with equations, you can often start with the more complicated expression and decompose it into an instance of $P(k)$ with some leftovers. That's what we will do here.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \left(\sum_{i=1}^{k} i^2\right) + \left((k+1)^2\right) && \text{(partition into } P(k) \text{ and other)} \\
&= \left(\frac{k(k+1)(2k+1)}{6}\right) + \left((k+1)^2\right) && \text{(use the inductive hypothesis)} \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} && \text{(algebraic manipulation)} \\
&= \frac{(k+1)\left(2k^2+7k+6\right)}{6} && \text{(factor out } k+1\text{, expand the rest)} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} && \text{(factor)} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}
\end{aligned}$$

The result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction.

□

Our next example does not have any equations.

Proposition 3 Let $S_n = \{1, 2, 3, \ldots, n\}$. Then S_n has 2^n subsets.

Let's be very clear about what our statement $P(n)$ is.

$P(n)$: S_n has 2^n subsets.

Now we can begin the proof.

Proof: Base Case We verify that $P(1)$ is true where $P(1)$ is the statement

$P(1)$: S_1 has 2 subsets.

Note that $S_1 = \{1\}$. We can enumerate all of the sets of S_1 easily. They are $\{\ \}$ and $\{1\}$, exactly two as required.

Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 1$.

$P(k)$: S_k has 2^k subsets.

Inductive Conclusion Now show that the statement $P(k+1)$ is true.

$P(k+1)$: S_{k+1} has 2^{k+1} subsets.

The subsets of S_{k+1} can be partitioned into two sets. The set A in which no subset contains the element $k+1$, and the complement of A, $\overline{A}$, in which every subset contains the element $k+1$. Now A is just the subsets of S_k and so, by the inductive hypothesis, has 2^k subsets of S_k. $\overline{A}$ is composed of the subsets of S_k to which the element $k+1$ is added. So, again by our inductive hypothesis, there are 2^k subsets of $\overline{A}$. Since A and $\overline{A}$ are disjoint and together contain all of the subsets of S_{k+1}, there must be $2^k + 2^k = 2^{k+1}$ subsets of S_{k+1}.

The result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction.

□

14.3.3 A Different Starting Point

Some true statements cannot start with "for all integers n, $n \geq 1$". For example, "$2^n > n^2$" is false for $n = 2$, 3, and 4 but true for $n \geq 5$. But the basic idea holds. If we can show that a statement is true for some base case $n = b$, and then show that

$$P(b) \Rightarrow P(b+1) \Rightarrow P(b+2) \Rightarrow \ldots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow \ldots$$

this is also induction. Perhaps this is not surprising because we can always recast a statement "For every integer $n \geq b$, $P(n)$" as an equivalent statement "For every integer $m \geq 1$, $P(m)$". For example,

For every integer $n \geq 5$, $2^n > n^2$.

is equivalent to

For every integer $m \geq 1$, $2^{m+4} > (m+4)^2$.

In this case, we have just replaced n by $m + 4$.

The basic structure of induction is the same. To prove the statement

For every integer $n \geq b$, $P(n)$ is true.

the only changes we need to make are that our base case is $P(b)$ rather than $P(1)$, and that in our inductive hypothesis we assume $P(k)$ is true for $k \geq b$ rather than $k \geq 1$.

Here is an example.

Proposition 4 For every integer $n \geq 3$, $n^2 > 2n + 1$.

As usual, let's be very clear about what our statement $P(n)$ is.

$P(n)$: $n^2 > 2n + 1$.

Now we can begin the proof.

Proof: Base Case We verify that $P(3)$ is true where $P(3)$ is the statement

$P(3)$: $3^2 > 2(3) + 1$

This is just arithmetic.

$$3^2 = 9 > 7 = 2(3) + 1$$

Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 3$.

$P(k)$: $k^2 > 2k + 1$

Inductive Conclusion Now show that the statement $P(k + 1)$ is true.

$P(k + 1)$: $(k + 1)^2 > 2(k + 1) + 1$

$$(k + 1)^2 = k^2 + 2k + 1 > (2k + 1) + (2k + 1) = 4k + 2 > 2k + 3 = 2(k + 1) + 1$$

The first inequality follows from the inductive hypothesis and the second inequality uses the fact that $k > 0$.

The result is true for $n = k + 1$, and so holds for all n by the Principle of Mathematical Induction. □

Here is another, similar example.

Proposition 5 For every integer $n \geq 5$, $2^n > n^2$.

The statement $P(n)$ is:

$P(n)$: $2^n > n^2$.

Proof: Base Case We verify that $P(5)$ is true where $P(5)$ is the statement

$P(5)$: $2^5 > 5^2$

This is just arithmetic.

$$2^5 = 32 > 25 = 5^2$$

Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 5$.

$P(k)$: $2^k > k^2$

Inductive Conclusion Now show that the statement $P(k + 1)$ is true.

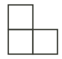
$P(k + 1)$: $2^{k+1} > (k + 1)^2$

We will use the fact that for $k \geq 5$, $k^2 > 2k + 1$ which follows from the previous proposition.

$$2^{k+1} = 2 \times 2^k > 2 \times k^2 = k^2 + k^2 > k^2 + 2k + 1 = (k + 1)^2$$

The result is true for $n = k + 1$, and so holds for all n by the Principle of Mathematical Induction. □

14.4 An Interesting Example

A **triomino** is a tile of the form 

Proposition 6 A $2^n \times 2^n$ grid of squares with one square removed can be covered by triominoes.

As usual, we begin by explicitly stating $P(n)$.

$P(n)$: A $2^n \times 2^n$ grid of squares with one square removed can be covered by triominoes.

We will use Simple Induction.

Proof: Base Case We verify that $P(1)$ is true.

$P(1)$: A 2×2 grid of squares with one square removed can be covered by triominoes.

A 2×2 grid with one square removed looks like  or  or  or  .

Each of these can be covered by one triomino.

Inductive Hypothesis We assume that the statement $P(k)$ is true $k \geq 1$.

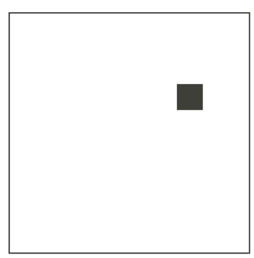
$P(k)$: A $2^k \times 2^k$ grid of squares with one square removed can be covered by triominoes.

Note that our inductive hypothesis covers every possible position for the empty square within the grid.

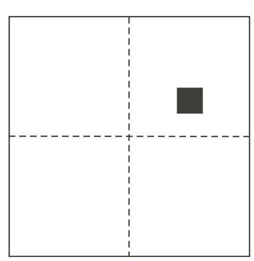
Inductive Conclusion We now show that the statement $P(k+1)$ is true.

$P(k+1)$: A $2^{k+1} \times 2^{k+1}$ grid of squares with one square removed can be covered by triominoes.

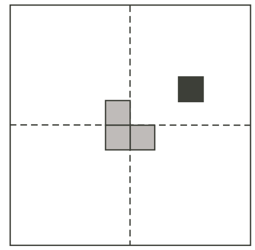
Consider a $2^{k+1} \times 2^{k+1}$ grid with any square removed.



Split the $2^{k+1} \times 2^{k+1}$ grid in half vertically and horizontally.



The missing square occurs in one of the four $2^k \times 2^k$ subgrids formed. We'll start by placing one tile around the centre of the grid, not covering any of the $2^k \times 2^k$ subgrids where the square is missing:



We can now view the grid as being made up of four $2^k \times 2^k$ subgrids, each with one square missing. The Inductive Hypothesis tells us that each of these can be covered by triominoes. Together with one more triomino in the centre, the whole $2^{k+1} \times 2^{k+1}$ grid can be covered. The result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction.

$\square$

14.5 More Examples

1. For all $n \in \mathbb{Z}$, $n \geq 0$

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Proof: We begin by formally writing out our inductive statement

$$P(n) : \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

Base Case We verify that $P(0)$ is true where $P(0)$ is the statement

$$P(0) : \sum_{i=0}^{0} 2^i = 2^{0+1} - 1$$

The left hand side expression evaluates to

$$\sum_{i=0}^{0} 2^i = 2^0 = 1$$

and the right hand side expression evaluates to

$$2^{0+1} - 1 = 2 - 1 = 1$$

Since both sides equal each other, $P(0)$ is true.

Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 0$.

$$P(k) : \sum_{i=0}^{k} 2^i = 2^{k+1} - 1$$

Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

$$P(k+1): \sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$$

$$\begin{aligned}
\sum_{i=0}^{k+1} 2^i &= \left(\sum_{i=0}^{k} 2^i\right) + \left(2^{k+1}\right) && \text{(partition into } P(k) \text{ and other)}\\
&= 2^{k+1} - 1 + 2^{k+1} && \text{(use the inductive hypothesis)}\\
&= 2 \cdot 2^{k+1} - 1 && \text{(algebraic manipulation)}\\
&= 2^{k+2} - 1 && \text{(properties of exponents)}
\end{aligned}$$

The result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction.

□

2. For all $n \in \mathbb{N}$, $4 \mid (5^n - 1)$.

Proof: We begin by formally writing out our inductive statement $P(n): \ 4 \mid (5^n - 1)$

Base Case We verify that $P(1)$ is true where $P(1)$ is the statement $P(1): \ 4 \mid (5^1 - 1)$. This is clearly true.

Inductive Hypothesis We assume that the statement $P(k): 4 \mid (5^k - 1)$ is true for some integer $k \geq 1$.

Inductive Conclusion Now we show that the statement $P(k+1)$ is true. That is, we must show $4 \mid (5^{k+1} - 1)$.

By our Inductive Hypothesis, $4 \mid (5^k - 1)$ and so there exists an integer m so that $4m = 5^k - 1$. Now

$$\begin{aligned}
5^{k+1} - 1 &= 5^{k+1} - 5^k + 5^k - 1 && \text{(add zero)}\\
&= 5^k(5-1) + 5^k - 1 && \text{(factor out } 5^k\text{)}\\
&= 4 \cdot 5^k + 5^k - 1 && \text{(simplify)}\\
&= 4 \cdot 5^k + 4m && \text{(substitute } 4m \text{ for } 5^k - 1\text{)}\\
&= 4(5^k + m) && \text{(factor out 4)}
\end{aligned}$$

Since $5^k + m$ is an integer, $4 \mid (5^{k+1} - 1)$. The result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction.

□

3. Consider the product

$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)$$

(a) What is the value of this product for $n = 2, 3, 4$.

Solution:

$$\prod_{i=2}^{2}\left(1-\frac{1}{i^2}\right)=\frac{3}{4},\quad \prod_{i=2}^{3}\left(1-\frac{1}{i^2}\right)=\frac{2}{3}=\frac{4}{6},\quad \prod_{i=2}^{4}\left(1-\frac{1}{i^2}\right)=\frac{5}{8}$$

(b) Conjecture a value for the product as a function of n.

$$\prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n}$$

(c) Use induction to prove your conjecture.

Proof: We begin by formally writing out our inductive statement

$$P(n):\ \prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)=\frac{n+1}{2n}$$

Base Case Note that the smallest possible value of n in this case is 2. We verify that $P(2)$ is true where $P(2)$ is the statement

$$P(2):\ \prod_{i=2}^{2}\left(1-\frac{1}{i^2}\right)=\frac{2+1}{2\cdot 2}$$

The left hand side evaluates to $\prod_{i=2}^{2}\left(1-\frac{1}{i^2}\right)=1-\frac{1}{4}=\frac{3}{4}$ which is exactly the right hand side. Hence, $P(2)$ holds.

Inductive Hypothesis We assume that the statement

$$P(k):\ \prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)=\frac{k+1}{2k}$$

is true for some integer $k \geq 2$.

Inductive Conclusion Now we show that the statement $P(k+1)$ is true. That is, we show

$$P(k+1):\ \prod_{i=2}^{k+1}\left(1-\frac{1}{i^2}\right)=\frac{k+2}{2(k+1)}$$

Now

$$\begin{aligned}
\prod_{i=2}^{k+1}\left(1-\frac{1}{i^2}\right) &= \prod_{i=2}^{k}\left(1-\frac{1}{i^2}\right)\cdot\left(1-\frac{1}{(k+1)^2}\right) && \text{(partition into } P(k) \text{ and other)}\\
&= \frac{k+1}{2k}\cdot\left(1-\frac{1}{(k+1)^2}\right) && \text{(Inductive Hypothesis)}\\
&= \frac{k+1}{2k}\cdot\frac{k(k+2)}{(k+1)^2} && \text{(arithmetic)}\\
&= \frac{k+2}{2(k+1)} && \text{(simplify)}
\end{aligned}$$

The result is true for $n = k + 1$, and so holds for all n by the Principle of Mathematical Induction.

□

4. Prove that

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}$$

for every positive integer $n > 1$.

Proof: We begin by formally writing out our inductive statement

$$P(n): \; 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}$$

Base Case We verify that $P(2)$ is true where $P(2)$ is the statement

$$P(2): \; 1 + \frac{1}{4} < 2 - \frac{1}{2}$$

The left hand side evaluates to $\frac{5}{4}$ and the right hand side evaluates to $\frac{3}{2} = \frac{6}{4}$ so $P(2)$ holds.

Inductive Hypothesis We assume that the statement

$$P(k): \; 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{k^2} < 2 - \frac{1}{k}$$

is true for some integer $k \geq 2$.

Inductive Conclusion Now we show that the statement $P(k+1)$ is true. That is, we show

$$P(k+1): \; 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}$$

Now

$$\begin{aligned}
& 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{(k+1)^2} \\
= \; & \left[1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{k^2}\right] + \frac{1}{(k+1)^2} \\
< \; & \left[2 - \frac{1}{k}\right] + \frac{1}{(k+1)^2} \qquad \text{(by the induction hypothesis)} \\
= \; & 2 - \frac{(k+1)^2 - k}{k(k+1)^2} \\
= \; & 2 - \frac{k^2 + k + 1}{k(k+1)^2} \\
= \; & 2 - \frac{k^2 + k}{k(k+1)^2} - \frac{1}{k(k+1)^2} \\
< \; & 2 - \frac{k^2 + k}{k(k+1)^2} \qquad \text{(since the last term is negative)} \\
= \; & 2 - \frac{k(k+1)}{k(k+1)^2} \\
= \; & 2 - \frac{1}{k+1}
\end{aligned}$$

The result is true for $n = k + 1$, and so holds for all n by the Principle of Mathematical Induction.

□

14.6 Practice

1. Each of the following "proofs" by induction incorrectly "prove" a statement that is actually false. State what is wrong with each proof.

   (a) A sequence $\{x_n\}$ is defined by $x_1 = 3$, $x_2 = 20$ and $x_i = 5x_{i-1}$ for $i \geq 3$. Then, for all $n \in \mathbb{N}$, $x_n = 3 \times 5^{n-1}$.

   Proof: Let $P(n)$ be the statement: $x_n = 3 \times 5^{n-1}$.
   When $n = 1$ we have $3 \times 5^0 = 3 = x_1$ so $P(1)$ is true. Assume that $P(k)$ is true for some integer $k \geq 1$. That is, $x_k = 3 \times 5^{k-1}$ for some integer $k \geq 1$. We must show that $P(k+1)$ is true, that is, $x_{k+1} = 3 \times 5^k$. Now

   $$x_{k+1} = 5x_k = 5(3 \times 5^{k-1}) = 3 \times 5^k$$

   as required. Since the result is true for $n = k+1$, and so holds for all n by the Principle of Mathematical Induction. □

   (b) All horses are the same colour.

   Proof: Let $P(n)$ be the proposition that all the horses in a set of n horses are the same colour. Clearly, $P(1)$ is true. Now assume that $P(k)$ is true, so that all the horses in any set of k horses are the same colour. Consider any set of $k+1$ horses; number these as horses $1, 2, 3, \ldots, k, k+1$. Now the first k of these horses all must have the same colour, and the last k of these must also have the same colour. Since the set of the first k horses and the set of the last k horses overlap, all $k+1$ must be the same colour. This shows that $P(k+1)$ is true and finishes the proof by induction. □

2. Prove the following statements by induction.

   (a) For all $n \in \mathbb{N}$, $\sum_{i=1}^{n}(2i-1) = n^2$.
   (b) For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
   (c) For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.
   (d) For all $r \in \mathbb{R}$, $r \neq 1$ and $n \in \mathbb{N}$, $\sum_{i=0}^{n} r^i = \frac{1-r^{n+1}}{1-r}$.
   (e) For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} \frac{i}{(i+1)!} = 1 - \frac{1}{(n+1)!}$.
   (f) For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$.

3. Prove the following statements by induction.

   (a) For all $n \in \mathbb{N}$, $3^n > n^2$.
   (b) For all $n \in \mathbb{N}$ where $n \geq 4$, $n! > 2^n$.
   (c) For all $n \in \mathbb{N}$ where $n \geq 4$, $n! > n^2$.

Chapter 15

Strong Induction

15.1 Objectives

The technique objectives are:

1. Learn when to use *Strong Induction*.
2. Learn how to use *Strong Induction*.

15.2 Strong Induction

Sometimes Simple Induction doesn't work where it looks like it should. We then need to change our approach a bit. The following example is similar to examples that we've done earlier. Let's try to make Simple Induction work and see where things go wrong.

Proposition 1 Let the sequence $\{x_n\}$ be defined by $x_1 = 0$, $x_2 = 30$ and $x_m = x_{m-1} + 6x_{m-2}$ for $m \geq 3$. Then

$$x_n = 2 \cdot 3^n + 3 \cdot (-2)^n \text{ for } n \geq 1.$$

The proposition is saying that the recursive definition of x_n implies the closed form of x_n. This seems like a classic case for induction since the conclusion clearly depends on the integer n. Let's begin with our statement $P(n)$.

$P(n)$: $x_n = 2 \cdot 3^n + 3 \cdot (-2)^n$.

Now we can begin the proof.

Proof: Use induction on n,

Base Case We verify that $P(1)$ is true where $P(1)$ is the statement

$P(1)$: $x_1 = 2 \cdot 3^1 + 3 \cdot (-2)^1$.

From the definition of the sequence $x_1 = 0$. The right side of the statement $P(1)$ evaluates to 0 so $P(1)$ is true.

Inductive Hypothesis We assume that the statement $P(k)$ is true for some $k \geq 1$.

$P(k)$: $x_k = 2 \cdot 3^k + 3 \cdot (-2)^k$.

Inductive Conclusion Now show that the statement $P(k+1)$ is true.

$P(k+1)$: $x_{k+1} = 2 \cdot 3^{k+1} + 3 \cdot (-2)^{k+1}$.

$$\begin{aligned} x_{k+1} &= x_k + 6x_{k-1} && \text{(by the definition of the sequence)} \\ &= 2 \cdot 3^k + 3 \cdot (-2)^k + 6x_{k-1} && \text{(by the Inductive Hypothesis)} \end{aligned}$$

(Proof is not completed)

Now two problems are exposed. The more obvious problem is what do we do with x_{k-1}? The more subtle problem is whether we can even validly write the first line. When $k+1 = 2$ we get

$$x_2 = x_1 + 6x_0$$

and x_0 is not even defined.

The basic principle that earlier instances imply later instances is sound. We need to strengthen our notion of induction in two ways. First, we need to allow for more than one base case so that we avoid the problem of undefined terms. Second, we need to allow access to any of the statements $P(1)$, $P(2)$, $P(3)$, ... , $P(k)$ when showing that $P(k+1)$ is true. This may seem like too strong an assumption but is, in fact, quite acceptable. This practice is based on the *Principle of Strong Induction*.

Axiom 2

Principle of Strong Induction (POSI)

Let $P(n)$ be a statement that depends on $n \in \mathbb{N}$.

If

1. $P(1), P(2), \ldots, P(b)$ are true for some positive integer b, and
2. $P(1), P(2), \ldots, P(k)$ are all true implies $P(k+1)$ is true for all $k \in \mathbb{N}$,

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

Just as before, there are three parts in a proof by strong induction.

Base Cases *Verify that* $P(1), P(2), \ldots, P(b)$ *are all true.* This is usually easy.

Inductive Hypothesis *Assume that* $P(1), P(2), \ldots, P(k)$ *are true for some* $k \geq b$. This is sometimes written as *Assume that* $P(i)$ *is true for* $i = 1, 2, 3, \ldots, k$*, for some* $k \geq b$ or *Assume that* $P(i)$ *is true for all* $1 \leq i \leq k$*, for some* $k \geq b$.

Inductive Conclusion Using the assumption that $P(1), P(2), \ldots, P(k)$ are true, *show that* $P(k+1)$ *is true.*

As a rule of thumb, use Strong Induction when the general case depends on more than one previous case. Though we could use Strong Induction all the time, Simple Induction is often easier.

Let's return to our previous proposition.

Proposition 2 Let the sequence $\{x_n\}$ be defined by $x_1 = 0$, $x_2 = 30$ and $x_m = x_{m-1} + 6x_{m-2}$ for $m \geq 3$. Then
$$x_n = 2 \cdot 3^n + 3 \cdot (-2)^n \text{ for } n \geq 1.$$

We will use Strong Induction. Recall our statement $P(n)$.

$P(n)$: $x_n = 2 \cdot 3^n + 3 \cdot (-2)^n$.

Now we can begin the proof.

Proof: Base Case We verify that $P(1)$ and $P(2)$ are true.

$P(1)$: $x_1 = 2 \cdot 3^1 + 3 \cdot (-2)^1$.

From the definition of the sequence $x_1 = 0$. The right side of the statement $P(1)$ evaluates to 0 so $P(1)$ is true.

$P(2)$: $x_2 = 2 \cdot 3^2 + 3 \cdot (-2)^2$.

From the definition of the sequence $x_2 = 30$. The right side of the statement $P(2)$ evaluates to 30 so $P(2)$ is true.

Inductive Hypothesis We assume that the statement $P(i)$ is true for all $1 \leq i \leq k$, for some $k \geq 2$.

$P(i)$: $x_i = 2 \cdot 3^i + 3 \cdot (-2)^i$.

Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

$P(k+1)$: $x_{k+1} = 2 \cdot 3^{k+1} + 3 \cdot (-2)^{k+1}$.

$$\begin{aligned}
x_{k+1} &= x_k + 6x_{k-1} && \text{(by the definition of the sequence)} \\
&= 2 \cdot 3^k + 3 \cdot (-2)^k + 6(2 \cdot 3^{k-1} + 3 \cdot (-2)^{k-1}) && \text{(by the Inductive Hypothesis)} \\
&= 3^{k-1}[2 \cdot 3 + 6 \cdot 2] + (-2)^{k-1}[3 \cdot (-2) + 6 \cdot 3] && \text{(expand and factor)} \\
&= 18 \cdot 3^{k-1} + 12 \cdot (-2)^{k-1} \\
&= 2 \cdot 3^2 \cdot 3^{k-1} + 3 \cdot (-2)^2 \cdot (-2)^{k-1} \\
&= 2 \cdot 3^{k+1} + 3 \cdot (-2)^{k+1}
\end{aligned}$$

The result is true for $n = k + 1$, and so holds for all n by the Principle of Strong Induction.

$\square$

Proposition 3 Every integer $n \geq 9$ can be written in the form $3x + 4y$ for positive integers x and y.

Before we attempt a proof let's check small values.

x	y	$3x + 4y$
3	0	9
2	1	10
1	2	11
4	0	12
3	1	13
2	2	14

There seems to be a pattern. After every group of three integers n, we can generate the next group of three integers by adding one to the preceding values of x. Since this is a case where previous values allow us to generate later values, induction may work.

Our first task is to come up with a suitable statement $P(n)$.

$P(n)$: There exist positive integers x and y so that $3x + 4y = n$.

Now we can begin the proof.

Proof: Base Case We verify that $P(9)$, $P(10)$ and $P(11)$ are true. We repeat the table above for the required values of $9, 10$ and 11. Note that x and y are positive integers.

x	y	$3x + 4y$
3	0	9
2	1	10
1	2	11

Inductive Hypothesis We assume that the statement $P(i)$ is true for all $1 \leq i \leq k$, for some $k \geq 11$.

$P(i)$: There exist positive integers x and y so that $3x + 4y = i$.

Inductive Conclusion Now we show that the statement $P(k + 1)$ is true.

$P(k + 1)$: There exist positive integers x and y so that $3x + 4y = k + 1$.

Consider the integer $(k + 1) - 3 = k - 2$. Since $k - 2 < k$ we can use the Inductive Hypothesis to assert the existence of positive integers x_0 and y_0 such that $3x_0 + 4y_0 = k - 2$. Now consider the positive integers $x_1 = x_0 + 1$ and $y_1 = y_0$.

$$3x_1 + 4y_1 = 3(x_0 + 1) + 4y_0 = 3x_0 + 4y_0 + 3 = (k - 2) + 3 = k + 1$$

The result is true for $n = k + 1$, and so holds for all n by the Principle of Strong Induction.

$\square$

15.3 More Examples

1. A sequence $\{x_n\}$ is defined by $x_1 = 11$, $x_2 = 23$ and $x_n = x_{n-1} + 12x_{n-2}$ for all $n \geq 3$. For all $n \in \mathbb{N}$, $x_n = 2 \cdot 4^n - (-3)^n$.

   Proof: We will use Strong Induction. Our statement $P(n)$ is

   $$P(n) : x_n = 2 \cdot 4^n - (-3)^n$$

   Base Case We verify that $P(1)$ and $P(2)$ are true.

   $$P(1) : x_1 = 2 \cdot 4^1 - (-3)^1$$

   From the definition of the sequence $x_1 = 11$. The right side of the statement $P(1)$ evaluates to 11 so $P(1)$ is true.

   $$P(2) : x_2 = 2 \cdot 4^2 - (-3)^2$$

   From the definition of the sequence $x_2 = 23$. The right side of the statement $P(2)$ evaluates to 23 so $P(2)$ is true.

   Inductive Hypothesis We assume that the statement $P(i)$ is true for all $1 \leq i \leq k$, for some $k \geq 2$.

   $$P(i) : x_i = 2 \cdot 4^i - (-3)^i$$

   Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

   $$P(k+1) : x_{k+1} = 2 \cdot 4^{k+1} - (-3)^{k+1}$$

   $$\begin{aligned}
   x_{k+1} &= x_k + 12x_{k-1} \text{ (by the definition of the sequence)} \\
   &= 2 \cdot 4^k - (-3)^k + 12(2 \cdot 4^{k-1} - (-3)^{k-1}) \text{ (by the Inductive Hypothesis)} \\
   &= 4^{k-1}[2 \cdot 4 + 12 \cdot 2] + (-3)^{k-1}[-(-3) + 12 \cdot -1] \text{ (expand and factor)} \\
   &= 32 \cdot 4^{k-1} + (-9) \cdot (-3)^{k-1} \\
   &= 2 \cdot 4^2 \cdot 4^{k-1} - 3^2 \cdot (-3)^{k-1} \\
   &= 2 \cdot 4^{k+1} - (-3)^{k+1}
   \end{aligned}$$

   The result is true for $n = k+1$, and so holds for all n by the Principle of Strong Induction.

   □

2. If $n \geq 2$ is an integer, then n can be written as a product of primes.

   Proof: Let $P(n)$ be the statement: n can be written as a product of primes.

   $P(2)$ is true since 2 is itself a prime. (A product with one factor is fine.) For our inductive hypothesis, assume that $P(i)$ is true for $2 \leq i \leq k$. That is, any integer $i \geq 2$ can be written as a product of primes. Now we show that $P(k+1)$ is true, that is, $k+1$ can be written as a product of primes. If $k+1$ is a prime, we are done. We have a product consisting of the single prime factor $k+1$. If $k+1$ is composite, then we can write $k+1 = rs$ where r and s are integers and $2 \leq r, s \leq k$. But then, by our Inductive Hypothesis, both r and s can be written as a product of primes, so $rs = k+1$ is a product of primes. The result is true for $n = k+1$, and so holds for all n by the Principle of Strong Induction. □

REMARK

When using Strong induction, we prove the base cases $P(1), P(2), \ldots, P(b)$ are true for some positive integer b. Depending on the nature of the problem, sometimes we may have $b = 1$, and proving $P(1)$ is sufficient for the base case. The proof carried out in the induction conclusion will tell us whether we need more than one base case.

As a rule of thumb, when the induction conclusion is completed, check whether you can use $P(1)$ to logically deduce that $P(2)$ must be true using solely the procedure from the induction conclusion step. Then check whether $P(1)$ and $P(2)$ implies $P(3)$, whether $P(1) \wedge P(2) \wedge P(3)$ implies $P(4)$, and so on. If this can be consistently done, then we need only one base case.

3. Every positive integer n can be written as a sum of non-negative distinct powers of 2.

   Proof: We use strong induction on n.

   Base Case When $n = 1$, $1 = 2^0$.

   Induction Hypothesis Assume that for some $k \in \mathbb{N}$, each integer between 1 and k can be written as a sum of distinct, non-negative powers of 2.

   Induction Conclusion We will break into two cases: $k + 1$ is odd or $k + 1$ is even.

   Suppose $k + 1$ is odd. By induction hypothesis, k is the sum of distinct powers of 2. In particular, k is even, so this sum cannot include 2^0, since it is the only power of 2 that is odd. By adding 2^0 to this sum, we obtain $k + 1$ as a sum of distinct powers of 2.

   Suppose $k+1$ is even. Then $(k+1)/2$ is a positive integer less than $k+1$. So by induction hypothesis, $(k+1)/2$ is the sum of distinct powers of 2. By multiplying each term in the sum by 2, each power increased by 1, but the overall powers are still distinct. So this gives us $k + 1$ as a sum of distinct powers of 2.

   By induction, the result holds for all $n \in \mathbb{N}$.

   □

15.4 Practice

1. Each of the following "proofs" by induction incorrectly "prove" a statement that is actually false. State what is wrong with each proof.

   (a) For all $n \in \mathbb{N}$, $1^{n-1} = 2^{n-1}$.

   Proof: Let $P(n)$ be the statement: $1^{n-1} = 2^{n-1}$.
   When $n = 1$ we have $1^0 = 1 = 2^0$ so $P(1)$ is true. Assume that $P(i)$ is true for all $1 \le i \le k$. That is, $1^{i-1} = 2^{i-1}$ for all $1 \le i \le k$.
   We must show that $P(k + 1)$ is true, that is, $1^{(k+1)-1} = 2^{(k+1)-1}$ or $1^k = 2^k$. By our inductive hypothesis, $P(2)$ is true so $1^1 = 2^1$. Also by our inductive hypothesis, $P(k)$ is true so $1^{k-1} = 2^{k-1}$. Multiplying these two equations together gives $1^k = 2^k$. Since the result is true for $n = k+1$, and so holds for all n by the Principle of Strong Induction. □

(b) For all $n \in \mathbb{N}$, $n = 1$.

Proof: Let $P(n)$ be the statement: $n = 1$.
When $n = 1$ we have $1 = 1$, so the statement $P(1)$ is true. For our Inductive Hypothesis, we assume that $P(i)$ is true for $1 \leq i \leq k$. That is, $i = 1$ for all i in the range $1 \leq i \leq k$. Now we show that $P(k+1)$ is true. Note that

$$k + 1 = k + k - (k - 1)$$

and since, by the inductive hypothesis, $k = 1$ and $k - 1 = 1$

$$k + 1 = k + k - (k - 1) = 1 + 1 - (1) = 1$$

as required. □

2. Prove the following statements by induction.

   (a) A sequence $\{x_n\}$ is defined recursively by $x_1 = 8$, $x_2 = 32$ and $x_i = 2x_{i-1} + 3x_{i-2}$ for $i \geq 3$. For all $n \in \mathbb{N}$, $x_n = 2 \times (-1)^n + 10 \times 3^{n-1}$.

   (b) A sequence $\{t_n\}$ is defined recursively by $t_n = 2t_{n-1} + n$ for all integers $n > 1$. The first term is $t_1 = 2$. For all $n \in \mathbb{N}$, $t_n = 5 \times 2^{n-1} - 2 - n$.

3. You know that the sum of the interior angles of a triangle is 180°.

   (a) Use this fact about triangles to determine the sum of the interior angles of a convex quadrilateral. (A polygon is **convex** if every line segment joining non-adjacent vertices lies wholly inside the polygon.)

   (b) Use (a) and the fact about triangles to determine the sum of the interior angles of a convex pentagon.

   (c) Conjecture a value for the sum of the interior angles of a convex polygon with n sides.

   (d) Use induction to prove your conjecture.

4. The Fibonacci sequence is defined as the sequence $\{f_n\}$ where $f_1 = 1$, $f_2 = 1$ and $f_i = f_{i-1} + f_{i-2}$ for $i \geq 3$. Use induction to prove the following statements.

   (a) For all $n \in \mathbb{N}$,
   $$f_{n+1} < \left(\frac{7}{4}\right)^n$$

   (b) For $n \geq 2$,
   $$f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$$

   (c) Let $a = \dfrac{1+\sqrt{5}}{2}$ and $b = \dfrac{1-\sqrt{5}}{2}$. For all $n \in \mathbb{N}$,
   $$f_n = \frac{a^n - b^n}{\sqrt{5}}$$

Chapter 16

What's Wrong?

16.1 Objectives

The technique objectives are:

1. To practice reading proofs carefully.
2. To gain experience in identifying common errors.

16.2 Failure Is More Common Than Success

Proving statements is hard. Both for beginners and for professionals, it is usually the case that one needs to make several attempts to prove a given statement. Even when it seems like a proof has been discovered, errors are common.

This chapter identifies some of the most common errors and gives you practice in detecting those errors. Being aware of these common errors will hopefully allow you to identify them and so avoid them in your own work.

16.3 Some Questions To Ask

Let's assume you are reading a proposed proof of the statement S. How do you go about assessing whether or not the proof is correct? Here are some questions to ask yourself.

- Is S in the form of an implication, or does it begin with a quantifier? If S is in the form of an implication, explicitly identify the hypothesis and the conclusion.
- Are there any explicit quantifiers in the statement S? If so, identify the four parts of the quantifier and the proof technique associated with the quantifier.
- How can I justify each sentence in the proof? What definition, previously proved proposition or proof technique justifies the sentence?
- Have any steps been omitted? If so, what should those steps be and what definition, previously proved proposition or proof technique justifies the omitted step?

16.4 Assuming What You Need To Prove

To prove an implication, you assume that the hypothesis is true and deduce, by careful reasoning, that the conclusion is true. It is an extremely common error among beginning mathematicians to assume that the conclusion is true. Typically the flawed proof begins by assuming the conclusion and reasons to some true statement. The problem in this case does not lie with the reasoning, but with the assumption.

Consider the following statement and proposed proof.

Statement 1 Suppose a is an integer. If $32 \nmid ((a^2+3)(a^2+7))$, then a is even.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Suppose a is even.
2. Then a^2 is even, so both a^2+3 and a^2+7 are odd.
3. Since 32 is even, $32 \nmid ((a^2+3)(a^2+7))$.

$\square$

The reasoning from Sentence 1 to Sentence 2 is correct. The reasoning from Sentence 2 to Sentence 3 is correct. And $32 \nmid ((a^2+3)(a^2+7))$ does appear in the statement we are trying to prove. But it appears as the hypothesis, not as the conclusion. The problem lies in Step 1 where the author assumed the conclusion, what needed to be proved.

REMARK

When proving an implication, assume that the hypothesis is true and deduce, by careful reasoning, that the conclusion is true. Do not assume that the conclusion is true.

16.5 Incorrectly Invoking A Proposition

This common error is related to the previous one in that inadequate attention is paid to an hypothesis and conclusion. Typically, this error occurs when a proposition is invoked but the hypotheses for the proposition are not satisfied. Hence, invoking the proposition is wrong.

Consider the following statement and proposed proof.

Statement 2 Let a, b, d be integers. If $d \mid a$ and $d \mid b$, then $d \leq |a-b|$.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let $d \mid a$ and $d \mid b$.

2. By the Divisibility of Integer Combinations, $d \mid (1 \cdot a - 1 \cdot b)$, that is, $d \mid (a - b)$.
3. From Bounds By Divisibility, $d \leq |a - b|$.

□

The statement is false but the proof looks convincing. To see that the statement is false, consider the case where $a = b = d = 3$. Since a, b and d are integers, and $3 \mid 3$ the hypotheses are true. But $d = 3 \not\leq 0 = |a - b|$ so the conclusion is false.

Sentence 1 simply restates the hypothesis so it is correct. The reasoning from Sentence 1 to Sentence 2 is correct. So, the error lies somewhere in Sentence 3. Recall the statement of Bounds By Divisibility. We have changed the variable names to make a comparison with the above statement clearer.

Proposition 3 **(Bounds By Divisibility (BBD))**

Let m and n be integers. If $m \mid n$ and $n \neq 0$ then $|m| \leq |n|$.

In going from Sentence 2 to Sentence 3, the author is assuming that $m = d$ and $n = a - b$. Let us check the hypotheses of Bounds By Divisibility. It is certainly the case that m and n are integers and that $m \mid n$ (since $d \mid (a - b)$). But, when $a = b$, $n = 0$, which contradicts the hypothesis that $n \neq 0$. Since the hypotheses of Bounds By Divisibility are not satisfied, the proposition Bounds By Divisibility cannot be invoked.

REMARK

Before invoking a proposition, make sure that all of the hypotheses of the proposition are satisfied.

16.6 Examples With A Universal Quantifier

When you try to prove a statement of the form "For every x in the set S, $P(x)$ is true", you must cover *every* element in the set S. It is not enough to give a particular example.

Consider the following statement and proposed proof.

Statement 4 For every odd integer a, $32 \mid ((a^2 + 3)(a^2 + 7))$.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Consider the case $a = 3$.
2. Then $a^2 + 3 = 12$ and $a^2 + 7 = 16$.
3. Since $(a^2 + 3)(a^2 + 7) = 12 \times 16 = 192$, and $32 \mid 192$, the statement is true.

□

The "proof" shows that in the particular case $a = 3$ the statement is true. It does not address the infinitely many other odd cases all of which are included under "For every odd integer a".

REMARK

You cannot use an example to show that a universal statement is true. Use the Select Method when you want to prove that a universal statement is true.

16.7 Counter-Examples With An Existential Quantifier

When you try to prove a statement of the form "There exists an x in the set S such that $P(x)$ is true", showing that there are elements in S which do not satisfy the statement P is not useful. There may be many, even infinitely many, elements in S which do not satisfy P. The point is to show that at least one element does satisfy P.

Consider the following statement and proposed proof that the statement is false.

Statement 5 There exists an integer in the set $S = \{10, 11, 12, \ldots, 20\}$ such that $2^n - 1$ is prime.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Consider the case $n = 10$.
2. Then $2^{10} - 1 = 1023$.
3. But since $1023 = 3 \times 341$, $2^{10} - 1$ is not prime and the statement is false.

□

The "proof" shows that in the particular case $n = 10$ the statement is false. However, the statement does *not* claim that all of the elements of S have the property that $2^n - 1$ is prime. The statement only claims that one element in the set S has such a property. And in fact, there is an element with that property, $n = 13$.

REMARK

You cannot use a counter-example to show that an existential statement is false. To show that an existential statement is false, negate the statement to get a universal statement and then use the Select Method to prove that this universal statement is true. To show that an existential statement is true, use the Construct Method.

16.8 Using The Same Variable For Different Objects

We see in the example below that using the same variable for different objects can lead to an incorrect conclusion.

Statement 6

Let a, b and c be integers. If $a \mid b$ and $a \mid c$ then $b - c = 0$

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Assume $a \mid b$ and $a \mid c$.
2. From $a \mid b$, $b = ka$ for some integer k.
3. From $a \mid c$, $c = ka$ for some integer k.
4. Therefore $b - c = ka - ka = 0$.

□

REMARK

When using the object method on multiple existential quantifiers, use a new variable for each quantifier.

16.9 The Converse Is Not The Contrapositive

Recall that the contrapositive of $A \Rightarrow B$ is $\neg B \Rightarrow \neg A$ and the converse of $A \Rightarrow B$ is $B \Rightarrow A$. Truth tables tell us that the contrapositive is logically equivalent to the original statement, but the converse is not. Thus, it makes sense to use the contrapositive to prove $A \Rightarrow B$, but not the converse.

If we go back to the very first proof of this chapter, reproduced below, we see that the author begins with the conclusion and ends with the hypothesis, that is, the author proved the converse, not the original statement.

Statement 7

Suppose a is an integer. If $32 \nmid ((a^2 + 3)(a^2 + 7))$, then a is even.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Suppose a is even.
2. Then a^2 is even, so both $a^2 + 3$ and $a^2 + 7$ are odd.
3. Since 32 is even, $32 \nmid ((a^2 + 3)(a^2 + 7))$.

□

REMARK

To prove $A \Rightarrow B$, you can prove the contrapositive $\neg B \Rightarrow \neg A$ which is logically equivalent to $A \Rightarrow B$. Proving or disproving the converse, $B \Rightarrow A$, is not helpful.

16.10 Base Cases in Induction Proofs

Induction works on the basis that

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \ldots \Rightarrow P(k) \Rightarrow P(k+1) \Rightarrow \ldots$$

If $P(1)$ is false, the chain of reasoning fails. Thus, it is always important to establish the base case in induction.

Consider the following statement and proposed proof.

Statement 8 For all $n \in \mathbb{N}$, $n > n + 1$.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let $P(n)$ be the statement: $n > n + 1$.
2. Assume that $P(k)$ is true for some integer $k \geq 1$. That is, $k > k + 1$ for some integer $k \geq 1$.
3. We must show that $P(k + 1)$ is true, that is, $k + 1 > k + 2$.
4. But this follows immediately by adding one to both sides of $k > k + 1$.
5. Since the result is true for $n = k+1$, it holds for all n by the Principle of Mathematical Induction.

$\square$

This induction fails because we did not verify that $P(1)$ is true. In fact, $P(1)$ is not true in this case. One is not greater than two.

REMARK

When doing induction, always verify the base cases.

16.11 Arithmetic and Unusual Cases

It may be that the structure of a proof is correct, but the proof stumbles while doing complicated arithmetic or not properly treating unusual cases. Consider the following statement and proposed proof.

Statement 9 *If r is a positive real number with $r \neq 1$, then there is an integer n such that $2^{\frac{1}{n}} < r$.*

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Let n be any integer with $n > \dfrac{1}{\log_2(r)}$.
2. It then follows that $\dfrac{1}{n} < \log_2(r)$.
3. Hence $2^{\frac{1}{n}} < 2^{\log_2(r)} = r$.

□

Because the error in this proof is more subtle than others we have looked at, let's do a formal analysis of the proof.

Analysis of Proof As usual, we begin by identifying the hypothesis and the conclusion. An interpretation of Sentences 1 through 3 will follow.

Hypothesis: r is a positive real number. $r \neq 1$.
Conclusion: There is an integer n such that $2^{\frac{1}{n}} < r$.

Sentence 1 *Let n be any integer with $n > 1/\log_2(r)$.*

Since an existential quantifier occurs in the conclusion, the author uses the Construct Method. The four parts of the quantifier are:

Quantifier:	$\exists$
Variable:	n
Domain:	$\mathbb{Z}$
Open sentence:	$2^{\frac{1}{n}} < r$

In the first sentence of the proof, the author constructs an integer n. Later in the proof, the author intends to show that n satisfies the open sentence of the quantifier. Since r is a real number (not equal to 1), $1/\log_2(r)$ evaluates to a real number and we can certainly find an integer greater than any given real number.

Sentence 2 *It then follows that $\frac{1}{n} < \log_2(r)$.*

Here the author takes the reciprocal of $n > 1/\log_2(r)$.

Sentence 3 *Hence $2^{\frac{1}{n}} < 2^{\log_2(r)} = r$.*

Use the left and right sides of $\frac{1}{n} < \log_2(r)$ as exponents of 2 and recall that the function 2^x always increases as x increases.

Even the analysis looks good. What went wrong? Let's look again at Sentence 2. Here we used the statement

Statement 10 If $a, b \in \mathbb{R}$, neither equal to 0, and $a < b$, then $1/b < 1/a$.

A proof seems pretty straightforward – divide both sides of $a < b$ by ab. Except that the statement is false. Consider the case $a = -2$ and $b = 4$. $-2 < 4$ but $\frac{1}{4} \not< \frac{1}{-2}$. Our proposition really should be

Statement 11 If $a, b \in \mathbb{R}$, and $0 < a < b$, then $1/b < 1/a$.

Now we see the problem in the proof. Choose r so that $0 < r < 1$, say $r = 1/2$. That will make $\log_2(r)$ negative and hence $1/\log_2(r)$ negative. Choose $n = 1$. Now Sentence 1 is satisfied but Sentence 2 fails.

16.12 Not Understanding A Definition

This is the most common error in our experience. And that is not surprising. Even great mathematicians have had difficulty with definitions. In the historical development of mathematics, correct definitions often come well after the associated mathematics has been used. Cauchy's $\epsilon - \delta$ definition of a limit came two hundred years after Newton's description of calculus.

Consider the following statement and proposed proof.

Statement 12 Let n be an integer. If $n = k^3 + 1 \geq 3$, where $k \in \mathbb{N}$, then n is not prime.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Assume $n = k^3 + 1$, where $k \in \mathbb{N}$.
2. By factoring, $n = (k + 1)(k^2 - k + 1)$.
3. Since $k + 1$ and $k^2 - k + 1$ are integer factors of n, n cannot be a prime.

□

Here, problem is in step 3, which arises from a lack on understanding of the definition of a prime. Recall

Definition 16.12.1
Primes

An integer $p > 1$ is called a **prime** if and only if its positive divisors are 1 and p itself. Otherwise, p is called **composite**.

To convince the reader that n is not a prime, it is not enough to just factor n as $(k+1)(k^2 - k + 1)$. We need to further show that these factors of n are positive and are different from 1 and n.

REMARK

Know your definitions.

16.13 Practice

For each of these questions, work in pairs. Each person should attempt the questions independently first. Exchange your work and independently make an assessment of your partner's work. Where possible, identify specific errors. Finally, compare notes. Do you agree or disagree about the assessments? Why or why not?

1. Each of the following statements concerns even or odd integers. An integer n is **even** if $2 \mid n$. Otherwise, the integer is **odd**. For each of the following statements:

   (i) State the hypothesis.
   (ii) State the conclusion.
   (iii) Prove the statement.

   (a) If a is an even integer and b is an odd integer, then ab is even.
   (b) If a and b are odd integers, then ab is odd.
   (c) If a^2 is an odd integer, then a is an odd integer.
   (d) Let a be an integer. If $2 \mid (a^2 - 1)$, then $4 \mid (a^2 - 1)$.
   (e) If a and b are even integers, then $a + b$ is an even integer.

2. Consider the following statement:

   Suppose a is an integer. If $32 \nmid ((a^2+3)(a^2+7))$, then a is even.

   (a) Each of the following "proofs" of the statement is incorrect. Describe what is wrong in each case.
      (i) Suppose a is even. Then a^2 is even, so both a^2+3 and a^2+7 are odd. Since 32 is even, $32 \nmid ((a^2+3)(a^2+7))$.
      (i) Let $a = 1$. Then $32|((a^2+3)(a^2+7))$, but a is not even. This is a counterexample to the statement.
      (iii) Suppose $32 \nmid ((a^2+3)(a^2+7))$. Since $2|32$, $2 \nmid ((a^2+3)(a^2+7))$. This means that $(a^2+3)(a^2+7)$ must be odd, so both a^2+3 and a^2+7 must be odd. Therefore, a^2 is even, and hence a is even.
   (b) Prove the statement.

3. Consider the following statement: If $a \mid 30$ then $a \mid 60$.

   (a) Each of the following "proofs" of the statement is incorrect. Describe what is wrong in each case.
      (i) Let a be a divisor of 60. Since a can only contain the prime factors 2, 3, and 5, and since all of these integers are factors of 30 as well, $a \mid 30$.
   (b) Prove the statement.

Part IV

Securing Internet Commerce

Chapter 17

The Greatest Common Divisor

17.1 Objectives

The content objectives are:

1. To discover a proof of the proposition *GCD With Remainders*.
2. Do an example of the *Euclidean Algorithm*.
3. Prove the *GCD Characterization Theorem*.

17.2 Greatest Common Divisor

Definition 17.2.1 **Greatest Common Divisor**

Let a and b be integers, not both zero. An integer $d > 0$ is the **greatest common divisor** of a and b, written $\gcd(a, b)$, if and only if

1. $d \mid a$ and $d \mid b$ (this captures the *common* part of the definition), and
2. if $c \mid a$ and $c \mid b$ then $c \leq d$ (this captures the *greatest* part of the definition).

Example 1

Here are some examples.

- $\gcd(24, 30) = 6$
- $\gcd(17, 25) = 1$
- $\gcd(-12, 0) = 12$
- $\gcd(-12, -12) = 12$

Definition 17.2.2 $\gcd(0, 0)$

For $a \neq 0$, the definition implies that $\gcd(a, 0) = |a|$ and $\gcd(a, a) = |a|$. We define $\gcd(0, 0)$ as 0. This may sound counterintuitive, since all integers are divisors of 0, but it is consistent with $\gcd(a, 0) = |a|$ and $\gcd(a, a) = |a|$.

Let's prove a seemingly unusual proposition about gcds.

Proposition 1 **(GCD With Remainders (GCD WR))**

If a and b are integers not both zero, and q and r are integers such that $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Before we begin the proof, let's take a look at a numeric example.

Example 2 Suppose $a = 72$ and $b = 30$. Now $72 = 2\times 30+12$ so the proposition GCD With Remainders asserts that $\gcd(72, 30) = \gcd(30, 12)$. And this is true. The $\gcd(72, 30)$ and $\gcd(30, 12)$ is 6.

How would we discover a proof for GCD With Remainders? Let's try the usual approach: identify the hypothesis and conclusion, and begin asking questions.

Hypothesis: a, b, q and r are integers such that $a = qb + r$.

Conclusion: $\gcd(a, b) = \gcd(b, r)$

My first question typically starts with the conclusion and works backward. What is a suitable first question? How about "How do we show that two integers are equal?" There are lots of possible answers: show that their difference is zero, their ratio is one, each is less than or equal the other. However, here we are working with gcds rather than generic integers so perhaps a better question would be "How do we show that a number is a gcd?" The broad answer is relatively easy. Use the definition of gcd. After all, right now it is the only thing we have! A specific answer is less easy. Do we want to focus on $\gcd(a, b)$ or $\gcd(b, r)$? Here is an easy way to do both. Let $d = \gcd(a, b)$. Then show that $d = \gcd(b, r)$. That gets us two statements in our proof.

Proof in Progress

1. Let $d = \gcd(a, b)$.
2. *To be completed.*
3. Hence $d = \gcd(b, r)$.

But how do we show that $d = \gcd(b, r)$? Use the definition. Our proof can expand to

Proof in Progress

1. Let $d = \gcd(a, b)$.
2. We will show
   (a) $d \mid b$ and $d \mid r$, and
   (b) if $c \mid b$ and $c \mid r$ then $c \leq d$.
3. *To be completed.*

4. Hence $d = \gcd(b, r)$.

For the first part of the definition, we ask "How do we show that one number divides another number?" Interestingly enough, there are two different answers - one for b and one for r, though that is not obvious. For b there is already a connection between d and b in the first sentence. Since $d = \gcd(a, b)$, we know from the definition of gcd that $d \mid b$.

What about r? Using the definition of divisibility seems problematic. What propositions could we use? Transitivity of Divisibility doesn't seem to apply. How about using the Divisibility of Integer Combinations? Recall

Proposition 2 **(Divisibility of Integer Combinations)**

Let a, b and c be integers. If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

Observe that $r = a - qb$. Since $d \mid a$ and $d \mid b$, d divides any integer combination of a and b by the Divisibility of Integer Combinations. That is, $d \mid (a(1) + b(-q))$ so $d \mid r$. Let's extend our proof in progress.

Proof in Progress

1. Let $d = \gcd(a, b)$.
2. We will show
   (a) $d \mid b$ and $d \mid r$, and
   (b) if $c \mid b$ and $c \mid r$ then $c \leq d$.
3. Since $d = \gcd(a, b)$, we know from the definition of gcd that $d \mid b$.
4. Observe that $r = a - qb$. Since $d \mid a$ and $d \mid b$, $d \mid (a(1) + b(-q))$ by the Divisibility of Integer Combinations, so $d \mid r$.
5. *To be completed.*
6. Hence $d = \gcd(b, r)$.

That leaves us with the *greatest* part of greatest common divisor. This second part of the definition is itself an implication, so we assume that $c \mid b$ and $c \mid r$ and we must show $c \leq d$. How do we show one number is less than or equal to another number? There doesn't seem to be anything obvious but ask "Have I seen this anywhere before?". Yes, we have. In the second part of the definition of gcd. But then you might ask "Isn't that assuming what we have to prove?" Let's be precise about what we are saying. We can use d for one inequality.

Since $d = \gcd(a, b)$, for any c where $c \mid a$ and $c \mid b$, $c \leq d$.

What we need to show is: if $c \mid b$ and $c \mid r$ then $c \leq d$.

These two statements are close, but not the same. Make sure that you see the difference. In one, we are using the fact that $d = \gcd(a, b)$. In the other, we are showing that any common factor of b and r is less than or equal to d.

If we assume that $c \mid b$ and $c \mid r$, then $c \mid (b(q) + r(1))$ by the Divisibility of Integer Combinations (again). Since $a = qb + r$, $c \mid a$. And now, since $d = \gcd(a, b)$ and $c \mid a$ and $c \mid b$, $c \leq d$ as needed. Let's add that to our proof in progress.

Proof in Progress

1. Let $d = \gcd(a, b)$.
2. We will show
   (a) $d \mid b$ and $d \mid r$, and
   (b) if $c \mid b$ and $c \mid r$ then $c \leq d$.
3. Since $d = \gcd(a, b)$, we know from the definition of gcd that $d \mid b$.
4. Observe that $r = a - qb$. Since $d \mid a$ and $d \mid b$, $d \mid (a(1) + b(-q))$ by the Divisibility of Integer Combinations, so $d \mid r$.
5. Let $c \mid b$ and $c \mid r$. Then $c \mid (b(q) + r(1))$ by the Divisibility of Integer Combinations. Since $a = qb + r$, $c \mid a$. And now, since $d = \gcd(a, b)$ and $c \mid a$ and $c \mid b$, $c \leq d$ by the second part of the definition of gcd.
6. Hence $d = \gcd(b, r)$.

Having discovered a proof, we should now write the proof. Whenever you write, you should have an audience in mind. You actually have two audiences to keep in mind: your peers with whom you collaborate, and the markers. You do not need to specify each proof technique, since your peers and markers know all of them. It does help to provide an overall plan if you can. Also, proofs tend to work much more forwards than backwards because that helps to emphasize the notion of starting with hypotheses and ending with the conclusion. Here is one possible proof.

Proof: Let $d = \gcd(a, b)$. We will use the definition of gcd to show that $d = \gcd(b, r)$.

Since $d = \gcd(a, b)$, $d \mid b$. Observe that $r = a - qb$. Since $d \mid a$ and $d \mid b$, $d \mid (a - qb)$ by the Divisibility of Integer Combinations. Hence $d \mid r$, and d is a common divisor of b and r.

Let c be a divisor of b and r. Since $c \mid b$ and $c \mid r$, $c \mid (qb + r)$ by the Divisibility of Integer Combinations. Now $a = qb + r$, so $c \mid a$. Because $d = \gcd(a, b)$ and $c \mid a$ and $c \mid b$, $c \leq d$. $\square$

REMARK

1. If $a = b = 0$ this proposition is also true since the only possible choices for b and r are $b = r = 0$.
2. In general, there are many ways to work forwards and backwards.
3. The proof may records steps in a different order than their appearance in the discovery process.
4. Proofs are short and usually omit the discovery process.
5. Be sure that you can identify where each of the hypotheses was used in the proof.

17.3 Certificate of Correctess

Suppose we wanted to compute $\gcd(1386, 322)$. We could factor both numbers, find their common factors and select the greatest. In general, this is very slow.

Repeated use of GCD With Remainders allows us to efficiently compute gcds. For example, let's compute $\gcd(1386, 322)$.

Example 3

Since	$1386 = 4 \times 322 + 98,$	$\gcd(1386, 322) = \gcd(322, 98).$
Since	$322 = 3 \times 98 + 28,$	$\gcd(322, 98) = \gcd(98, 28).$
Since	$98 = 3 \times 28 + 14,$	$\gcd(98, 28) = \gcd(28, 14).$
Since	$28 = 2 \times 14 + 0,$	$\gcd(28, 14) = \gcd(14, 0).$

Since $\gcd(14, 0) = 14$, the chain of equalities from the column on the right gives us

$$\gcd(1386, 322) = \gcd(322, 98) = \gcd(98, 28) = \gcd(28, 14) = \gcd(14, 0) = 14.$$

This process is known as the *Euclidean Algorithm*.

Exercise 1 Randomly pick two positive integers and compute their gcd using the Euclidean Algorithm. How do you know that you have the correct answer? Keep your work. You'll need it soon.

Because mistakes happen when performing arithmetic by hand, and mistakes happen when programming computers, it would be very useful if there were a way to certify that an answer is correct. Think of a *certificate of correctness* this way. You are a manager. You ask one of your staff to solve a problem. The staff member comes back with the proposed solution and a certificate of correctness that can be used to verify that the proposed solution is, in fact, correct. The certificate has two parts: a theorem which you have already proved and which relates to the problem in general, and data which relates to this specific problem.

For example, here's a proposition that allows us to produce a certificate for $\gcd(a, b)$.

Proposition 3 **(GCD Characterization Theorem (GCD CT))**

If d is a positive common divisor of the integers a and b, and there exist integers x and y so that $ax + by = d$, then $d = \gcd(a, b)$.

Our certificate would consist of this theorem along with integers x and y. If our proposed solution was d and $d \mid a$, $d \mid b$ and $ax + by = d$, then we could conclude without doubt that $d = \gcd(a, b)$.

In Example 3 above, the proposed gcd of 1386 and 322 is 14. Our certificate of correctness consists of the *GCD Characterization Theorem* and the integers $d = 14$, $x = 10$ and $y = -43$. Note that $14 \mid 1386$ and $14 \mid 322$ and $1386 \times 10 + 322 \times (-43) = 14$, so we can conclude that $14 = \gcd(1386, 322)$.

Here is a proof of the GCD Characterization Theorem.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. We will show that d satisfies the definition of $\gcd(a, b)$.
2. From the hypotheses, $d \mid a$ and $d \mid b$.
3. Now let $c \mid a$ and $c \mid b$.
4. By the Divisibility of Integer Combinations, $c \mid (ax + by)$ so $c \mid d$.
5. By the Bounds by Divisibility, $c \leq d$, and so $d = \gcd(a, b)$.

□

Let's do an analysis of the proof.

Analysis of Proof As usual, we will begin by explicitly identifying the hypothesis and the conclusion.

Hypothesis: d is a positive common divisor of the integers a and b. There exist integers x and y so that $ax + by = d$.

Conclusion: $d = \gcd(a, b)$

Core Proof Technique: Work forwards recognizing an existential quantifier in the hypothesis.

Preliminary Material: Definition of *gcd*. An integer $d > 0$ is the $\gcd(a, b)$ if and only if

1. $d \mid a$ and $d \mid b$, and
2. if $c \mid a$ and $c \mid b$ then $c \leq d$.

Sentence 1 *We will show that d satisfies the definition of* $\gcd(a, b)$.

The author states the plan - always a good idea. The author is actually answering the question "How do I show that one number is the gcd of two other numbers?"

Sentence 2 *From the hypotheses, $d \mid a$ and $d \mid b$.*

The author is working forwards from the hypothesis. This handles the first part of the definition of gcd.

Sentence 3 *Now let $c \mid a$ and $c \mid b$.*

The second part of the definition of gcd is an implication with hypothesis $c \mid a$ and $c \mid b$. The author must show $c \leq d$.

Sentence 4 *By the Divisibility of Integer Combinations, $c \mid (ax + by)$ so $c \mid d$.*

This is where the author uses an existential quantifier in the hypothesis. The author assumes the existence of two integers x and y such that $ax + by = d$. The author does not state this explicitly.

Having made this assumption, the author can use Sentence 3 to satisfy the hypotheses of Divisibility of Integer Combinations and so invoke the conclusion, that is, $c \mid (ax + by)$.

Sentence 5 *By the Bounds By Divisibility, $c \le d$, and so $d = \gcd(a, b)$.*

Bounds by Divisibility concludes with a statement involving absolute values. Where did the absolute vales signs go? From Sentence 4 we know that $c \mid d$ and from the hypothesis we know that $d \neq 0$ so Bounds by Divisibility implies that $|c| \le |d|$. From the hypothesis we know more than $d \neq 0$. We know that d is positive, so $|c| \le d$. Regardless of the sign of c, if $|c| \le d$, it must be the case that $c \le d$. Having determined that $c \le d$, both parts of the definition of gcd are satisfied and so the author can conclude that $d = \gcd(a, b)$.

Now the obvious questions is: "How do we find x and y?"

17.4 More Examples

1. Prove that for any integer a, $\gcd(22a + 7, 3a + 1) = 1$.

   Proof: Since $22a + 7 = 7 \cdot (3a + 1) + a$, GCD With Remainders tells us that $\gcd(22a + 7, 3a + 1) = \gcd(3a + 1, a)$. Since $3a + 1 = 3 \cdot a + 1$, GCD With Remainders (again) tells us that $\gcd(3a + 1, a) = \gcd(a, 1)$. Since $\gcd(a, 1) = 1$, $\gcd(22a + 7, 3a + 1) = 1$. □

2. Prove that for any integer a, $\gcd(a^2, a + 1) = 1$.

   Proof: Since $a^2 = (a - 1) \cdot (a + 1) + 1$, GCD With Remainders tells us that $\gcd(a^2, a + 1) = \gcd(a + 1, 1)$. Since $\gcd(a + 1, 1) = 1$, $\gcd(a^2, a + 1) = 1$. □

3. Use the definition of gcd to prove the following statement. (Hint: Use the proof of the *GCD With Remainders* proposition as a model.)

   Let $x, y \in \mathbb{Z}$ and let $d = \gcd(x, y)$. Then $d = \gcd(x, 3x + y)$.

   Proof: We will show that d satisfies the definition of gcd for the pair x and $3x + y$. Specifically, we must show that

   (a) $d \mid x$ and $d \mid (3x + y)$, and
   (b) if $c \mid x$ and $c \mid (3x + y)$ then $c \le d$.

   Since $d = \gcd(x, y)$, $d \mid x$. Also, since $d \mid x$ and $d \mid y$, d divides any integer combination of x and y, hence $d \mid (3x + y)$.

   Now suppose that $c \mid x$ and $c \mid (3x + y)$. Then c divides the integer combination $x(-3) + (3x + y)(1))$, that is, $c \mid y$. But since $c \mid x$ and $c \mid y$ and $d = \gcd(x, y)$, $c \le d$.

   All of the conditions of the definition of the gcd are satisfied so $d = \gcd(x, 3x + y)$. □

4. Prove the following statement. Let $a, b, c \in \mathbb{Z}$. If $c > 0$, then $\gcd(ac, bc) = c \gcd(a, b)$. (Suggestion: Let $d = \gcd(a, b)$. Show $cd = \gcd(ac, bc)$.)

Proof: Let $d = \gcd(a, b)$. We will use the GCD Characterization Theorem.

First, we show that cd is a common divisor of ac and bc. Since $d = \gcd(a, b)$, $d \mid a$. By the definition of divisibility, there exists an integer k so that $dk = a$. Multiplying this equation by c gives $cdk = ca$. Since k is an integer, $cd \mid ac$. Similarly, $cd \mid bc$.

Next, we show that there exist integers x_0 and y_0 so that

$$acx_0 + bcy_0 = cd$$

Since $d = \gcd(a, b)$, there exist integers x_1 and y_1 so that

$$ax_1 + by_1 = d$$

Multiplying this equation by c gives

$$acx_1 + bcy_1 = cd$$

Letting $x_0 = x_1$ and $y_0 = y_1$ gives the required values for the GCD Characterization Theorem.

□

17.5 Practice

1. Consider the following statement: For all $a \in \mathbb{Z}$, $\gcd(9a + 4, 2a + 1) = 1$.

   (a) Which proposition belongs in the following proof of this statement?

   Proof: Let $a \in \mathbb{Z}$. By ____________________,

   $$\gcd(9a + 4, 2a + 1) = \gcd(2a + 1, a) = \gcd(a, 1)$$

   Since $\gcd(a, 1) = 1$, $\gcd(9a + 4, 2a + 1) = 1$. □

   (b) If $\gcd(x, y) = d$, express $\gcd(18x + 3y, 3x)$ in terms of d. Justify your answer.

2. Let a and b be non-zero integers. Prove each of the following statements.

   (a) If $a \mid b$, then $ac \mid bc$.
   (b) If $\gcd(a, b) = 1$, then $\gcd(2a + b, a + 2b)$ is 1 or 3.

3. Prove or disprove the following statements. Let a, b, c be fixed integers.

   (a) If there exists an integer solution to $ax^2 + by^2 = c$, then $\gcd(a, b) \mid c$.
   (b) If $\gcd(a, b) \mid c$, then there exists an integer solution to $ax^2 + by^2 = c$.
   (c) For every integer k, $\gcd(a, b) \le \gcd(ak, b)$.
   (d) Let $n \ge 2$ be an integer. If $\gcd(a, b^n) = 1$, then $\gcd(a, b) = 1$.

4. Two integers a and b are **coprime** if $\gcd(a, b) = 1$. Consider the following proposition and proof: If a and b are consecutive integers, then a and b are co-prime.

   Proof: (For reference purposes, each sentence of the proof is written on a separate line.)

(i) Suppose $b > a$.

(ii) We can write b as $a + 1$.

(iii) Since $1(a + 1) - 1(a) = 1$, we know by the ____________________ that $\gcd(a, b) = \gcd(a, a + 1) = 1$ as required.

(iv) The argument is similar if $a > b$.

$\square$

(a) State the hypothesis of Proposition 1.

(b) State the conclusion of Proposition 1.

(c) What proposition or theorem should appear in line (iii) of the proof? State the proposition or theorem precisely.

(d) Recall that propositions or theorems can only be invoked if their hypotheses are satisfied. Show that all of the hypotheses of the proposition or theorem you quoted in (c) are satisfied.

Chapter 18

Properties Of GCDs

18.1 Objectives

The technique objectives are:

1. To practice working with existential quantifiers.

The content objectives are:

1. Define *coprime*.
2. Discover a proof of *Coprimeness and Divisibility*.
3. Discover a proof of *GCD Of One*
4. Exercise: Discover a proof of *Division by the GCD*.
5. Exercise: Discover a proof of *Primes and Divisibility*.

18.2 Some Useful Propositions

We begin with a proposition on coprimeness and divisibility.

Definition 18.2.1
Coprime

Two integers a and b are **coprime** if $\gcd(a, b) = 1$.

Proposition 1

(Coprimeness and Divisibility (CAD))

If a, b and c are integers and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

This proposition has two implicit existential quantifiers, one in the hypothesis and one in the conclusion. You might object and ask "Where?" They are hidden - in the definition of *divides*. Recall the definition. An integer m divides an integer n if *there exists* an integer k so that $n = km$.

We treat an existential quantifier in the hypothesis differently from an existential quantifier in the conclusion. Recall the following remarks from the chapter on quantifiers.

REMARK

When proving that "A implies B" and A uses an existential quantifier, use the Object Method.

1. Identify the four parts of the quantified statement "there exists an x in the set S such that $P(x)$ is true."
2. *Assume* that a mathematical object x exists within the domain S so that the statement $P(x)$ is true.
3. Make use of this information to generate another statement.

When proving that "A implies B" and B uses an existential quantifier, use the Construct Method.

1. Identify the four parts of the quantified statement. "there exists an x in the set S such that $P(x)$ is true."
2. *Construct* a mathematical object x.
3. Show that $x \in S$.
4. Show that $P(x)$ is true.

With all of this in mind, how do we go about discovering a proof for Coprimeness and Divisibility? As usual, we will begin by explicitly identifying the hypothesis, the conclusion, the core proof technique and any preliminary material we think we might need.

Hypothesis: a, b and c are integers and $c \mid ab$ and $\gcd(a, c) = 1$.

Conclusion: $c \mid b$.

Core Proof Technique: We use the Object Method because of the existential quantifier in the hypothesis, and the Construct Method because of the existential quantifier in the conclusion.

Preliminary Material: Definition of *divides* and gcd.

Let's work backwards from the conclusion by asking the question "How do we show that one integer divides another?" We can answer with "the definition of divisibility." We must construct an integer k so that $b = ck$. We will record this as follows.

Proof in Progress

1. *To be completed.*
2. Since $b = kc$, $c \mid b$.

The problem is that it is not at all clear what k should be. Let's work forwards from the hypothesis.

Somehow we need an equation with a b alone on one side of the equality sign. We can't start there but we can get an equation with a b. Since $\gcd(a, c) = 1$, the EEA guarantees that we can find integers x and y so that $ax + cy = 1$. We could multiply this equation by b. Let's record these forward statements.

Proof in Progress

1. Since $\gcd(a, c) = 1$, the EEA guarantees that we can find integers x and y so that $ax + cy = 1$ (1).
2. Multiplying (1) by b gives $abx + cby = b$ (2).
3. *To be completed.*
4. Since $b = kc$, $c \mid b$.

If we could factor the left hand side of (2), we'd be able to get a c and other stuff that we could treat as our k. But the first term has no c. Or maybe it does. Since $c \mid ab$ there exists an integer h so that $ch = ab$. Substituting ch for ab in (2) gives $chx + cby = b$ (3). We record this as

Proof in Progress

1. Since $\gcd(a, c) = 1$, the EEA guarantees that we can find integers x and y so that $ax + cy = 1$ (1).
2. Multiplying (1) by b gives $abx + cby = b$ (2).
3. Since $c \mid ab$ there exists an integer h so that $ch = ab$. Substituting ch for ab in (2) gives $chx + cby = b$ (3).
4. *To be completed.*
5. Since $b = kc$, $c \mid b$.

Now factor.

Proof in Progress

1. Since $\gcd(a, c) = 1$, the EEA guarantees that we can find integers x and y so that $ax + cy = 1$ (1).
2. Multiplying (1) by b gives $abx + cby = b$ (2).
3. Since $c \mid ab$ there exists an integer h so that $ch = ab$. Substituting ch for ab in (2) gives $chx + cby = b$ (3).
4. This gives $c(hx + by) = b$.
5. But then if we let $k = hx + by$ we have an integer k so that $ck = b$.
6. Since $b = kc$, $c \mid b$.

Here is a proof.

Proof: By the Extended Euclidean Algorithm and the hypothesis $\gcd(a, c) = 1$, there exist integers x and y so that $ax + cy = 1$. Multiplying by b gives $abx + cby = b$. Since $c \mid ab$ there exists an integer h so that $ch = ab$. Substituting ch for ab gives $chx + cby = b$. Lastly, factoring produces $(hx + by)c = b$. Since $hx + by$ is an integer, $c \mid b$. $\square$

As a corollary of Coprimeness and Divisibility we have the following proposition.

Corollary 2 **(Primes and Divisibility (PAD))**

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Exercise 1 Prove Primes and Divisibility. Because of the “or” in the conclusion, you will need to use the Elimination Method.

Let us consider more properties of the greatest common divisor.

Proposition 3 **(GCD Of One (GCD OO))**

Let a and b be integers. Then $\gcd(a, b) = 1$ if and only if there are integers x and y with $ax + by = 1$.

This proposition has similar elements to the one we just proved, so it won't be a surprise if we use similar reasoning.

REMARK

The important difference is that this statement is an “if and only if” statement. To prove “A if and only if B” we must prove two statements:

1. If A, then B.
2. If B, then A.

Symbolically, we write “A if and only if B” as $A \iff B$. We established the equivalence of $A \iff B$ and $(A \Rightarrow B) \wedge (B \Rightarrow A)$ in the chapter *Truth Tables*.

We can restate the proposition as

Proposition 4 **(GCD Of One (GCD OO))**

Let a and b be integers.

1. If $\gcd(a, b) = 1$, then there are integers x and y with $ax + by = 1$.
2. If there are integers x and y with $ax + by = 1$, then $\gcd(a, b) = 1$.

In statement (1), there is an existential quantifier in the conclusion, so we would expect to use the Construction Method. The problem is "Where do we get x and y?" In the previous proof, we used the EEA and it makes sense to use it here as well. By the EEA and the hypothesis $\gcd(a, b) = 1$, there exist integers x and y so that $ax + by = 1$.

In statement (2), an existential quantifier occurs in the hypothesis so we use the Object Method and assume the existence of integers x and y so that $ax + by = 1$. Also, $1 \mid a$ and $1 \mid b$. These are exactly the hypotheses of the GCD Characterization Theorem, so we can conclude that $\gcd(a, b) = 1$.

Here is a proof of the GCD Of One proposition.

Proof: Since $\gcd(a, b) = 1$, the EEA assures the existence of integers x and y so that $ax + by = 1$. Statement 1 is proved.

Now, $1 \mid a$ and $1 \mid b$. Also, by the hypothesis of Statement 2, there exist integers x and y so that $ax + by = 1$. These are exactly the hypotheses of the GCD Characterization Theorem, so we can conclude that $\gcd(a, b) = 1$ and Statement 2 is proved. □

REMARK

This proof illustrates the connection between the GCD Characterization Theorem and the Extended Euclidean Algorithm. Both assume integers a and b. The GCD Characterization Theorem starts with an integer d where $d \mid a$, $d \mid b$ and integers x and y so that $ax + by = d$ and concludes that $d = \gcd(a, b)$. The Extended Euclidean Algorithm computes a d so that $d = \gcd(a, b)$, hence it produces a d so that $d \mid a$ and $d \mid b$, and also computes integers x and y so that $ax + by = d$.

So, if we encounter a gcd in the conclusion, we can try the GCD Characterization Theorem. If we encounter a gcd in the hypothesis, we can try the Extended Euclidean Algorithm.

Here is another property of gcds.

Proposition 5 **(Division by the GCD (DB GCD))**

Let a and b be integers. If $\gcd(a, b) = d \neq 0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

As we often do, let's get a sense of the proposition by using numeric examples.

Example 1 First, observe that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)$ is meaningful. Since $d \mid a$ and $d \mid b$, both $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

Now $\gcd(18, 24) = 6$. By the proposition Division by the GCD,

$$\gcd\left(\frac{18}{6}, \frac{24}{6}\right) = 1$$

which is exactly what we would expect from $\gcd(3, 4)$.

Now take minute to read the proof.

Proof: We will use the GCD Characterization Theorem. Since $\gcd(a,b) = d$, the EEA assures the existence of integers x and y so that $ax + by = d$. Dividing by d gives

$$\frac{a}{d}x + \frac{b}{d}y = 1$$

Since 1 divides both $\frac{a}{d}$ and $\frac{b}{d}$, the GCD Characterization Theorem implies that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. $\square$

18.3 More Examples

1. Prove the following proposition. Let $a, b \in \mathbb{Z}$. For every integer $n \in \mathbb{N}$, if $\gcd(a,b) = 1$, then $\gcd(a, b^n) = 1$.

   Proof: We begin by formally writing out our inductive statement

   $$P(n): \text{ If } \gcd(a,b) = 1, \text{ then } \gcd(a, b^n) = 1.$$

   Base Case The statement

   $$P(1): \text{ If } \gcd(a,b) = 1, \text{ then } \gcd(a, b) = 1.$$

   is trivially true.

   Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 1$.

   $$P(k): \text{ If } \gcd(a,b) = 1, \text{ then } \gcd(a, b^k) = 1.$$

   Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

   $$P(k+1): \text{ If } \gcd(a,b) = 1, \text{ then } \gcd(a, b^{k+1}) = 1.$$

   Since $\gcd(a,b) = 1$, the EEA tells us that there exist integers x and y so that

   $$ax + by = 1$$

   Since $\gcd(a, b^k) = 1$ by the Inductive Hypothesis, the EEA tells us that there exist integers x' and y' so that

   $$ax' + b^k y' = 1$$

   Multiplying the two equations together gives

   $$a^2xx' + ab^kxy' + abx'y + b^{k+1}yy' = 1$$

   which we can rewrite as

   $$a(axx' + b^kxy' + bx'y) + b^{k+1}(yy') = 1$$

   Let $x'' = axx' + b^kxy' + bx'y$ and $y'' = yy'$. Since there exist integers x'' and y'' so that

   $$ax'' + b^{k+1}y'' = 1$$

   we can invoke the GCD Of One to assert that $\gcd(a, b^{k+1}) = 1$.

□

2. Prove the following proposition. Given any rational number r, prove that there exist coprime integers p and q, with $q \neq 0$, so that $r = \frac{p}{q}$.

Proof: Since r is rational, we can write r as $r = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Let $d = \gcd(a, b)$. Since $b \neq 0$, $d \neq 0$. Let $p = \frac{a}{d}$ and $q = \frac{b}{d}$. Since d is a divisor of a and b, both p and q are integers. Moreover, the proposition Division by GCD assures us that $\gcd(p, q) = 1$. Thus, there exist coprime integers p and q, with $q \neq 0$, so that $r = \frac{p}{q}$. □

18.4 Practice

1. Consider the following statement and proof.

Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(a, c) = 1$.

Proof: (For reference purposes, each sentence of the proof is written on a separate line.)

(i) Since $\gcd(a, b) = 1$, by __________ there exist integers x and y such that $ax + by = 1$.

(ii) Since $c \mid (a + b)$, by __________ there exists an integer k such that $a + b = ck$.

(iii) Substituting $a = ck - b$ into the first equation, we get $1 = (ck - b)x + by = b(-x + y) + c(kx)$.

(iv) Since 1 is a common divisor of b and c and $-x+y$ and kx are integers, $\gcd(b, c) = 1$ by __________.

□

(a) What proposition or definition should be cited in line (i) of the proof?

(b) What proposition or definition should be cited in line (ii) of the proof?

(c) What proposition or definition should be cited in line (iv) of the proof?

2. Consider the following proposition and proof.

Let $a, b, c \in \mathbb{Z}$. *If* $\gcd(a, b) = 1$ *and* $c \mid a$, *then* $\gcd(b, c) = 1$.

Proof: Since $\gcd(a, b) = 1$, we know that there exist integers x and y so that $ax + by = 1$ (1). Since $c \mid a$, there exists an integer k so that $a = ck$. Substituting this expression for a into Equation (1) gives $c(kx) + b(y) = 1$. Since kx is an integer, $\gcd(b, c) = 1$. □

Justify each line of the proof by writing down each definition or proposition used. Write down the entire definition or proposition, not just the name. For propositions, show that the assumptions of the proposition are satisfied. If only arithmetic is used, write down "By arithmetic."

3. Consider the proposition and proposed proof below.

   Let a, b and c be integers. If $ax + by = c$ has an even solution, then it has an infinite number of even solutions.

   Proof: (a) Suppose (x_0, y_0) is one particular even solution to $ax + by = c$.

   (b) By LDET 2, a complete solution is $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$ where $d = \gcd(a, b)$.

   (c) Since $\frac{b}{d} \in \mathbb{Z}$ and x_0 is even, for every choice of even n, $x = x_0 + \frac{b}{d}n$ is even.

   (d) Since y_0 is even, choosing $n = 0$ for $y = y_0 - \frac{a}{d}n$ gives y_0 which is even,

   (e) Hence,
   $$\{(x_0 + \frac{b}{d}n, y_0) \mid n \text{ is an even integer}\}$$
   is an infinite set of solutions to $ax + by = c$.

   $\square$

   If the proof is correct, justify each sentence. If the proof is incorrect, identify the first sentence in the proof that contains an error and explain why this is an error.

4. Let $a, b \in \mathbb{Z}$. For each of the following statements, either prove the statement or disprove it using a counterexample.

   (a) If p is a prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.

   (b) If $2a^2 = b^2$ where $a, b \in \mathbb{Z}$, then 2 is a common divisor of a and b.

   (c) For any integer a, $\gcd(11a + 5, 2a + 1) = 1$.

5. Prove the following statement. If $\gcd(a, b) = 1$, then $\gcd(a, bc) = \gcd(a, c)$. (Hint: Let $d = \gcd(a, c)$ and let $e = \gcd(a, bc)$.)

Chapter 19

GCD from Prime Factorization

19.1 Objectives

The content objectives are:

1. Recall the definition of *prime* and *composite*.
2. Discover a proof by induction of the *Prime Factorization Theorem*.
3. Read a proof of *Finding A Prime Factor*.
4. State and use *Divisors from Prime Factorization*.
5. State and use *GCD from Prime Factorization*.

In the previous chapter we defined the *greatest common divisor* of two integers. Many of us are familiar with a method for calculating the GCD (also known as the *highest common factor*, HCF, in some parts of the world) of positive integers with the help of prime factorization. For example, given

$$252 = 2^2 \times 3^2 \times 7 \text{ and } 630 - 2 \times 3^2 \times 5 \times 7,$$

we have learned that $\gcd(252, 630)$ should equal $2 \times 3^2 \times 7 = 126$. In this chapter, we will revisit the topic of prime numbers and theoretically prove that we can calculate the GCD of two positive integers using the method shown above.

19.2 Introduction to Primes

Recall our definition of prime number.

Definition 19.2.1
Prime, Composite

An integer $p > 1$ is called a **prime** if its only divisors are 1 and p, and **composite** otherwise.

Example 1

The integers $2, 3, 5$ and 7 are primes. The integers $4 = 2 \times 2$, $6 = 2 \times 3$ and $8 = 2 \times 2 \times 2$ are composite. Note, that by definition, 1 is not a prime.

We have already proved three propositions about primes, one of which is a consequence of Coprimeness and Divisibility, and the other two were proved in the chapter on contradiction.

Proposition 1 **(Primes and Divisibility (PAD))**

If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proposition 2 **(Prime Factorization (PF))**

If n is an integer greater than 1, then n can be written as a product of prime factors.

Proposition 3 **(Infinitely Many Primes (INF P))**

The number of primes is infinite.

19.3 Fundamental Theorem of Arithmetic

In grade school you used prime numbers to write the prime factorization of any positive integer greater than one. You probably never worried about the possibility that there might be more than one way to do this. However, in some sets "prime" factorization is not unique.

Consider the set $S = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. In S, the number $4 = 4 + 0\sqrt{5}$ can be factored in two different ways, $4 = 2 \times 2$ and $4 = (\sqrt{5}+1)(\sqrt{5}-1)$. Moreover, 2, $\sqrt{5}+1$ and $\sqrt{5}-1$ are all prime numbers in S!

Since multiplication in the integers is commutative, the prime factorizations can be written in any order. For example $12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = 3 \times 2 \times 2$. However, up to the order of the factors, the factorization of integers is unique. This property is so basic it is referred to as the Fundamental Theorem of Arithmetic. It is also referred to as the Unique Factorization Theorem.

Theorem 4 **(Fundamental Theorem of Arithmetic or Unique Factorization Theorem (UFT))**

If $n > 1$ is an integer, then n can be written as a product of prime factors and, apart from the order of factors, this factorization is unique.

Observe that the conclusion contains two parts:

1. n can be written as a product of prime factors (which we proved earlier), and
2. apart from the order of factors, this factorization is unique.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. That n can be written as a product of prime factors follows from the proposition Prime Factorization.

2. Now suppose that n is factored into primes in two ways,

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell \tag{19.1}$$

   where all of the p's and q's are primes.

3. Since $p_1 \mid n$, $p_1 \mid q_1 q_2 \dots q_\ell$.

4. By repeatedly applying the proposition Primes and Divisibility, p_1 must divide one of the q's. If necessary, rearrange the q's so that $p_1 \mid q_1$.

5. Since q_1 is prime, and $p_1 > 1$, it must be the case that $p_1 = q_1$.

6. Dividing Equation 19.1 by $p_1 = q_1$ gives

$$p_2 p_3 \dots p_k = q_2 q_3 \dots q_\ell \tag{19.2}$$

7. By continuing in this way, we see that each p must be paired off with one of the qs until there are no factors on either side.

8. Hence $k = \ell$ and, apart from the order of the factors, the two expressions for n are the same.

□

Let's perform an analysis of the proof. As usual, we begin with the hypothesis and the conclusion.

Hypothesis: n is an integer, $n > 1$

Conclusion: There are two parts.

1. n can be written as a product of prime factors, and
2. apart from the order of factors, this factorization is unique.

Core Proof Technique: Uniqueness

Preliminary Material: Primes and Divisibility

Sentence 1 *That n can be written as a product of prime factors follows from the proposition Prime Factorization.*

The first of the two parts of the conclusion is just the conclusion of a previous proposition.

Sentence 2 *Now suppose that n is factored into primes in two ways,*

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$$

where all of the p's and q's are primes.

This is a classic use of the Uniqueness Method. We assume that there are two representations of the same object, and show that the two representations are, in fact, identical. One representation of n is the product $p_1 p_2 \dots p_k$ and the second representation is the product $q_1 q_2 \dots q_\ell$.

Sentences 3 − 5 *Since $p_1 \mid n$, $p_1 \mid q_1q_2 \dots q_\ell$. By repeatedly applying the proposition Primes and Divisibility, p_1 must divide one of the q's. If necessary, rearrange the q's so that $p_1 \mid q_1$. Since q_1 is prime, and $p_1 > 1$, it must be the case that $p_1 = q_1$.*

The author shows that the two representations of n are equal by showing that they have identical factors. Here, the author demonstrates that $p_1 = q_1$.

Sentences 6 − 7 *Dividing Equation 19.1 by $p_1 = q_1$ gives*

$$p_2p_3 \dots p_k = q_2q_3 \dots q_\ell$$

By continuing in this way, we see that each p must be paired off with one of the qs until there are no factors on either side.

This continues the author's plan of showing that the two representations of n are equal by showing that they have identical factors.

Sentence 8 *Hence $k = \ell$ and, apart from the order of the factors, the two expressions for n are the same.*

This is a typical conclusion to the Uniqueness Method. The two representations of the same object are identical.

19.4 Finding a Prime Factor

The previous proposition does not provide an algorithm for finding the prime factors of a positive integer n. The next proposition shows that we do not have to check *all* of the prime factors less than n, only those less than or equal to the square root of n.

Proposition 5 **(Finding a Prime Factor (FPF))**

An integer $n > 1$ is either prime or contains a prime factor less than or equal to $\sqrt{n}$.

Let's begin by identifying the hypothesis and the conclusion.

Hypothesis: n is an integer and $n > 1$.

Conclusion: n is either prime or contains a prime factor less than or equal to $\sqrt{n}$.

Before we see a proof, let's do an example.

Example 2 Is 73 a prime number?

Solution: Using Finding a Prime Factor, we can check for divisibility by primes less than or equal to $\sqrt{73}$. Now $\sqrt{73} \approx 8.544$ so any possible prime factor must be less than or equal to 8. The only candidates to check are 2, 3, 5 and 7. Since none of these divide 73, 73 must be prime.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Suppose that n is not prime.

2. Let p be the smallest prime factor of n.

3. Since n is composite we can write $n = ab$ where a and b are integers such that $1 < a, b < n$.

4. Since p is the smallest prime factor, $p \leq a$ and $p \leq b$ and so $p^2 = p \cdot p \leq a \cdot b = n$. That is $p \leq \sqrt{n}$.

□

Analysis of Proof Since *or* appears in the conclusion, we will use Proof By Elimination. The equivalent statement that is proved is:

> If n is an integer greater than 1 and n is not prime, then n contains a prime factor less than or equal to $\sqrt{n}$.

The word "a" should alert us to the presence of an existential quantifier. We could reword the statement as

> If n is an integer greater than 1 and n is not prime, then there exists a prime factor of n which is less than or equal to $\sqrt{n}$.

This is the statement that will actually be proved.

Hypothesis: n is an integer greater than 1 and n is not prime.

Conclusion: There exists a prime factor of n which is less than or equal to $\sqrt{n}$.

Core Proof Technique: There is an existential quantifier in the conclusion so the author uses the Construct Method.

Sentence 1 *Suppose that n is not prime.*

This sentence tells us that the author is going to use Proof by Elimination.

Sentence 2 *Let p be the smallest prime factor of n.*

The conclusion has an existential quantifier and so the author uses the Construct Method. The prime p will be the desired prime factor though it is not clear yet why "smallest" is important. The proposition on Prime Factorization guarantees us that a prime factor exists.

Sentence 3 *Since n is composite we can write $n = ab$ where a and b are integers such that $1 < a, b < n$.*

By the hypotheses of the restated proposition, $n > 1$ and n is not prime, so n is composite and can be factored.

Sentence 4 *Since p is the smallest prime factor, $p \leq a$ and $p \leq b$ and so $p^2 = p \cdot p \leq a \cdot b = n$. That is $p \leq \sqrt{n}$.*

This is where "smallest" is used. The conclusion follows from arithmetic and the fact that p is the smallest prime factor.

19.5 Working With Prime Factorizations

The *Unique Factorization Theorem* tells us that for any integer $n \geq 2$, if $p_1, p_2, \ldots, p_k$ are all the distinct primes that divide n, then we may express

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$. For example, the prime divisors of 80262 are $2, 3, 7$ and 13, and, in particular, $80262 = 2^1 \times 3^2 \times 7^3 \times 13^1$.

Note that in the unique prime factorization of 80262, we cannot use primes such as $5, 11$ or 17 as they do not divide 80262. However, if we are willing to give up on the uniqueness of the factorization, then we may write $80262 = 2^1 \times 3^2 \times 5^0 \times 7^3 \times 11^0 \times 13^1 \times 17^0$. The key here is that 5^0, 11^0 and 17^0 are all equal to 1, so their inclusion in the product has not changed the overall answer. Nevertheless, this has now allowed us to use a larger list of primes in the factorization of 80262, at the cost of losing the guarantee that these primes will divide 80262.

In general, given any integer $n \geq 2$, if we have a large enough list of distinct primes $p_1, p_2, \ldots, p_m$ that includes all the prime divisors of n, but may also include primes that don't divide n, then we are allowed to express a (non-unique) prime factorization of n using all the primes in this list by saying

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_m$ are non-negative integers. The next proposition uses this idea to list all of the positive divisors of a positive integer.

Proposition 6 **(Divisors From Prime Factorization (DFPF))**

Let $n > 1$ be an integer and $d \in \mathbb{N}$. If

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

is the unique prime factorization of n into powers of distinct primes $p_1, p_2, \ldots, p_k$, where the integers $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$, then d is a positive divisor of n if and only if a (non-unique) prime factorization of d is given by

$$d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \text{ where } 0 \leq d_i \leq \alpha_i \text{ for } i = 1, 2, \ldots, k$$

Proof: Assume $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and the integers $\alpha_1, \alpha_2, \ldots, \alpha_k \geq 1$.

In the case when $d = 1$, we may express $1 = p_1^0 p_2^0 \cdots p_k^0$. Since 1 is a positive divisor of n, the proposition is true for $d = 1$.

Otherwise, suppose $d \geq 2$. Then, by the *Unique Factorization Theorem*, the number d will have its own distinct prime factors $q_1, q_2, \ldots, q_m$, and thus can be expressed as

$$d = q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m},$$

where the integers $d_1, d_2, \ldots, d_m \geq 1$. We will now prove the conclusion of the given proposition by proving each direction of the if and only if statement.

" $\implies$ ": Using the prime factorizations above, if $d \mid n$ then

$$\left(q_1^{d_1} q_2^{d_2} \cdots q_m^{d_m}\right) \mid \left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right).$$

Using a reasoning similar to the one in the proof of *UFT*, this can only happen when $m \le k$, and (after rearranging, if necessary) $q_1 = p_1$, $q_2 = p_2, \ldots, q_m = p_m$ and that $1 \le d_1 \le \alpha_1, 1 \le d_2 \le \alpha_2, \ldots, 1 \le d_m \le \alpha_m$. Hence we have

$$d = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}.$$

Since $m \le k$, there may be some primes $p_{m+1}, p_{m+2}, \ldots, p_k$ leftover from the list of prime factors for n. In that case, we may now include these primes in a prime factorization by expressing

$$d = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m} \cdots p_k^{d_k},$$

where $d_{m+1} = d_{m+2} = \cdots = d_k = 0$. As $\alpha_1, \alpha_2, \ldots, \alpha_k \ge 1$, we have been able to write $d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ where $0 \le d_i \le \alpha_i$ for $i = 1, 2, \ldots, k$.

" $\Longleftarrow$: Suppose a (non-unique) prime factorization satisfies the condition $d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ where $0 \le d_i \le \alpha_i$ for $i = 1, 2, \ldots, k$. Then let us define a rational number q such that $q = \frac{n}{d}$. Using prime factorizations of n and d, we get

$$q = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}{p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}} = p_1^{(\alpha_1 - d_1)} p_2^{(\alpha_2 - d_2)} \cdots p_k^{(\alpha_k - d_k)}.$$

Since for each $i = 1, 2, \ldots, k$ we are given $\alpha_i \ge d_i$, we $(\alpha_i - d_i) \ge 0$ and hence $p_i^{(\alpha_i - d_i)}$ is an integer. Therefore $p_1^{(\alpha_1 - d_1)} p_2^{(\alpha_2 - d_2)} \cdots p_k^{(\alpha_k - d_k)}$ is a product on integers, so q is an integer. This means $n = qd$, where q is an integer, so $d \mid n$. □

Self Check 1

Let $p_1, p_2, \ldots, p_k$ be distinct times and $q_1, q_2, \ldots, q_\ell$ also be a list of distinct primes. Prove that for non-negative integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ and $d_1, d_2, \ldots, d_\ell$, if

$$\left(q_1^{d_1} q_2^{d_2} \cdots q_\ell^{d_\ell}\right) \mid \left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right),$$

then $\ell \le k$ and (after rearranging, if necessary) $q_1 = p_1$, $q_2 = p_2, \ldots, q_\ell = p_\ell$ and, moreover, $d_1 \le \alpha_1, d_2 \le \alpha_2, \ldots, d_\ell \le \alpha_\ell$.

Example 3

(Using Divisors From Prime Factorization)

What are the positive divisors of 72?

We will use Divisors From Prime Factorization. Since

$$72 = 2^3 3^2$$

the positive divisors of a are integers of the form

$$d = 2^{d_1} 3^{d_2} \text{ where } 0 \le d_1 \le 3 \text{ and } 0 \le d_2 \le 2$$

The possibilities are

$$\begin{array}{cccc} 2^0 3^0 = 1 & 2^1 3^0 = 2 & 2^2 3^0 = 4 & 2^3 3^0 = 8 \\ 2^0 3^1 = 3 & 2^1 3^1 = 6 & 2^2 3^1 = 12 & 2^3 3^1 = 24 \\ 2^0 3^2 = 9 & 2^1 3^2 = 18 & 2^2 3^2 = 36 & 2^3 3^2 = 72 \end{array}$$

Exercise 1 Using Divisors From Prime Factorization, list all of the positive factors of 45.

Exercise 2 Show that the number of positive divisors of an integer n, whose unique prime factorization is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

is given by $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

Now that we have a method to obtain all the positive divisors of any positive integer using its prime factorization, we may expect to use this method to calculate the GCD of two positive integers say a and b. First, note that given $a, b \in \mathbb{N}$, since there are infinitely many primes but only a finite number of prime factors of a and b, we may produce a large enough list of distinct primes, say $p_1, p_2, \ldots, p_k$, that contain all the prime divisors of both a and b. This provides us with (non-unique) prime factorizations of both a and b, respectively, expressed in terms of the primes $p_1, p_2, \ldots, p_k$ as

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ and}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ and $\beta_1, \beta_2, \ldots, \beta_k$ are non-negative integers.

Proposition 7 **(GCD From Prime Factorization (GCD PF))**

If

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

are (non-unique) prime factorizations of a and b, where the primes are distinct and some of the exponents may be zero, then

$$\gcd(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \text{ where } d_i = \min\{\alpha_i, \beta_i\} \text{ for } i = 1, 2, \ldots, k$$

Proof: Assume that $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and the exponents are non-negative integers.

Consider $d \in \mathbb{N}$ given by $d = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ where $d_i = \min\{\alpha_i, \beta_i\}$ for $i = 1, 2, \ldots, k$. Since $\min\{\alpha_i, \beta_i\} \leq \alpha_i$ as well as $\min\{\alpha_i, \beta_i\} \leq \beta_i$ for each $i = 1, 2, \ldots, k$, according to *Divisors From Prime Factorization* (*DFPF*), $d \mid a$ and $d \mid b$.

Consider some positive integer c such that $c \mid a$ and $c \mid b$. According to *DFPF*, a prime factorization of c is

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k},$$

where for each $i = 1, 2, \ldots, k$, $0 \leq \gamma_i \leq \alpha_i$ as $c \mid a$ and $0 \leq \gamma_i \leq \beta_i$ as $c \mid b$. On the other hand, for each $i = 1, 2, \ldots, k$, $d_i = \alpha_i$ if $\alpha_i \leq \beta_i$, otherwise $d_i = \beta_i$, which means $0 \leq \gamma_i \leq d_i$. Then, once again by *DFPF*, $c \mid d$, so *Bounds By Divisibility* (*BBD*) gives us $c \leq d$. Note that a similar analysis would apply to all negative common divisors of a and b.

Consequently, the definition of GCD, $d = \gcd(a, b)$. □

Example 4 **(Using GCD From Prime Factorization)**

What is $\gcd(24750, 434511)$?

Since

$$24750 = 2^1 3^2 5^3 11^1 = 2^1 3^2 5^3 7^0 11^1 19^0$$

and

$$434511 = 3^3 7^1 11^2 19^1 = 2^0 3^3 5^0 7^1 11^2 19^1,$$

$$\begin{aligned}\gcd(24750, 434511) &= 2^{\min\{1,0\}} 3^{\min\{2,3\}} 5^{\min\{3,0\}} 7^{\min\{0,1\}} 11^{\min\{1,2\}} 19^{\min\{0,1\}} \\ &= 2^0 3^2 5^0 7^1 11^2 19^0 \\ &= 7623\end{aligned}$$

Though this method of finding the GCD works well enough on small examples, but for larger numbers, this method is very slow an inefficient. Nevertheless, it is an important theoretical tool that can be used to prove other propositions.

Exercise 3 Use GCD PF to compute $\gcd(3^3 5^1 7^4 13^1, 5^2 7^7 13^1 23^2)$.

19.6 More Examples

1. This question deals with prime factorizations.

   (a) Write out the prime factorizations of 12936 and 16380.

   (b) Using part (a), determine $\gcd(12936, 16380)$.

   Solution:

   (a)

   $$12936 = 2^3 3^1 7^2 11^1$$
   $$16380 = 2^2 5^1 3^2 7^1 13^1$$

   (b) $\gcd(12936, 16380) = 2^2 3^1 7^1 = 84$

19.7 Problems

1. Prove that if $p <= n$, then p does not divide $n! + 1$.

2. Let $n >= 0$. What is the power of 2 in the prime factorization of $(2^n)!$? Prove that you have the correct value.

3. An integer n is *perfect* if the sum of all of its positive divisors (including 1 and itself) is $2n$.

   (a) Is 6 a perfect number? Give reasons for your answer.

(b) Is 7 a perfect number? Give reasons for your answer.

(c) Prove the following statement:
If k is a positive integer and $2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is perfect.

4. Note that k divides $n! + k$ for each $k <= n$. Use this fact to show that, for all positive integers m, there exist consecutive primes which are at least m apart.

5. Let a, b and d be positive integers. Use *GCD From Prime Factorization* (*GCD PF*) to prove that for all $n \in \mathbb{N}$, if $d = \gcd(a, b)$ then $\gcd(a^n, b^n) = d^n$.

   You may use the fact that for all non-negative integers α and β,

$$\min\{n \cdot \alpha, n \cdot \beta\} = n \cdot \min\{\alpha, \beta\}.$$

Chapter 20

The Extended Euclidean Algorithm

20.1 Objectives

The content objectives are:

1. Compute gcds and certificates using the Extended Euclidean Algorithm.

20.2 The Extended Euclidean Algorithm (EEA)

Given two positive integers, a and b, the EEA is an efficient way to compute not only $d = \gcd(a, b)$ but the data x and y for the certificate. We'll begin with an example and then formally state the algorithm.

First though, we need to know what the floor of a number is.

Definition 20.2.1 (floor) The **floor** of x, written $\lfloor x \rfloor$, is the largest integer less than or equal to x.

Example 1

1. $\lfloor 9.713 \rfloor = 9$.
2. $\lfloor 9.025 \rfloor = 9$.
3. $\lfloor 9 \rfloor = 9$.
4. $\lfloor -9.713 \rfloor = -10$. Since the floor of x is the largest integer less than or equal to x, -9 cannot be the floor of -9.713 since $-9 > -9.713$.
5. $\left\lfloor \frac{7}{2} \right\rfloor = 3$.

Let's compute $\gcd(1386, 322)$ using the EEA. We begin by creating four columns labelled x, y, r (for remainder) and q (for quotient). We will construct a sequence of rows that will tell us the gcd and provide a certificate. For the i-th row we will label the column entries x_i, y_i, r_i and q_i. There is something very important to observe about the table. If we are computing $\gcd(a, b)$, in each row of the table

$$ax_i + by_i = r_i$$

Where have you seen an expression like that before?

Assuming $a > b$, the first two rows are always

x	y	r	q
1	0	a	0
0	1	b	0

so in our specific problem the first two rows are

x	y	r	q
1	0	1386	0
0	1	322	0

We construct each of the remaining rows by using the two preceding rows. To generate the third row we must first compute a quotient q_3 using the formula

$$q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$$

Here we get

$$q_3 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{1386}{322} \right\rfloor = 4$$

To construct the next row we use the formula

$$\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i\text{Row}_{i-1}$$

When $i = 3$ we get

$$\text{Row}_3 \leftarrow \text{Row}_1 - q_3\text{Row}_2$$

With $q_3 = 4$ we get

$$\text{Row}_3 \leftarrow \text{Row}_1 - 4 \times \text{Row}_2$$

Writing this in the table gives

	x	y	r	q
Row_1	1	0	1386	0
$-4 \times \text{Row}_2$	0	1	322	0
$= \text{Row}_3$	1	-4	98	4

In a similar fashion we get the fourth row. To generate the fourth row we must first compute a quotient q_4 using the formula

$$q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$$

Here we get

$$q_4 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{322}{98} \right\rfloor = 3$$

To construct the next row we use the formula

$$\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i \text{Row}_{i-1}$$

When $i = 4$ we get

$$\text{Row}_4 \leftarrow \text{Row}_2 - q_4 \text{Row}_3$$

With $q_4 = 3$ we get

$$\text{Row}_4 \leftarrow \text{Row}_2 - 3 \times \text{Row}_3$$

and so

	x	y	r	q
	1	0	1386	0
Row_2	0	1	322	0
$-3 \times \text{Row}_3$	1	-4	98	4
$= \text{Row}_4$	-3	13	28	3

The completely worked out example follows.

x	y	r	q
1	0	1386	0
0	1	322	0
1	-4	98	4
-3	13	28	3
10	-43	14	3
-23	99	0	2

We stop when the remainder is 0. The second last row provides the desired d, x and y. The gcd d is the entry in the r column, x is the entry in the x column and y is the entry in the y column. Hence, $d = 14$ (as before), and we can check the conditions of the GCD Characterization Theorem to certify correctness. Since $14 \mid 1386$ and $14 \mid 322$ and $1386 \times 10 + 322 \times (-43) = 14$, we can conclude that $14 = \gcd(1386, 322)$.

If a or b is negative, apply the EEA to $\gcd(|a|, |b|)$ and then change the signs of x and y after the EEA is complete. If $a < b$, simply swap their places in the algorithm. This works because $\gcd(a, b) = \gcd(b, a)$.

Here is a formal statement of the algorithm.

Algorithm 1 Extended Euclidean Algorithm

Require: $a > b > 0$ are integers.
Ensure: The following conditions hold at the end of the algorithm.
  $r_{n+1} = 0$.
  $r_n = \gcd(a, b)$.
  $r_{i-2} = q_i r_{i-1} + r_i$ where $0 \le r_i < r_{i-1}$.
  In every row, $ax_i + by_i = r_i$.
  $x = x_n$, $y = y_n$ is a solution to $ax + by = \gcd(a, b)$.
  {Initialize}
  Construct a table with four columns so that
  The columns are labelled x, y, r and q.
  The first row in the table is $(1, 0, a, 0)$.
  The second row in the table is $(0, 1, b, 0)$.
  {To produce the remaining rows $(i \ge 3)$}
  repeat
    $q_i \leftarrow \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$
    $\text{Row}_i \leftarrow \text{Row}_{i-2} - q_i \text{Row}_{i-1}$
  until $r_i = 0$

We treat the EEA as a proposition where the preconditions of the algorithm are the hypotheses and the postconditions of the algorithm are the conclusions. Let's record the algorithm in the form of a theorem.

Proposition 1 **(Extended Euclidean Algorithm (EEA))**

If $a > b > 0$ are positive integers, then $d = \gcd(a, b)$ can be computed and there exist integers x and y so that $ax + by = d$.

Note that if a or b is negative, we can apply the EEA with $|a|$ and $|b|$ and convert signs afterwards. A proof of the correctness of the EEA is available in the appendix. **[Incomplete: Add to appendix.]**

Exercise 1 Earlier you computed the gcd of two numbers. Repeat that exercise using the EEA and verify that you can produce a certificate of correctness for your proposed gcd.

20.3 More Examples

1. Let $d = \gcd(231, 660)$.
   (a) Use the Extended Euclidean Algorithm to compute d and provide a certificate that d is correct.
   (b) Using part (a) , find $d_1 = \gcd(231, -660)$ and provide a certificate that d_1 is correct.
   (c) Using part (a) of this question, find $d_2 = \gcd(-231, -660)$ and provide a certificate that d_2 is correct.

Solution:

(a)

x	y	r	q
1	0	660	0
0	1	231	0
1	-2	198	2
-1	3	33	1
7	-20	0	6

By the EEA, $d = 33$. Our certificate consists of the GCD Characterization Theorem together with $d = 33$ (d is positive and divides both 660 and 231), and the integers -1 and 3 (since $660(-1) + 231(3) = 33$).

(b) Since $\gcd(231, -660) = \gcd(231, 660)$, $d_1 = 33$. Our certificate consists of the GCD Characterization Theorem together with $d_1 = 33$ (d_1 is positive and divides both -660 and 231), and the integers 1 and 3 (since $-660(1) + 231(3) = 33$).

(c) Since $\gcd(-231, -660) = \gcd(231, 660)$, $d_2 = 33$. Our certificate consists of the GCD Characterization Theorem together with $d_2 = 33$ (d_2 is positive and divides both -660 and -231), and the integers 1 and -3 (since $-660(1) - 231(-3) = 33$).

Chapter 21

Linear Diophantine Equations: One Solution

21.1 Objectives

The technique objectives are:

1. To practice working with existential quantifiers.

The content objectives are:

1. Define *Diophantine equations*.
2. Prove the *Linear Diophantine Equation Theorem (Part 1)*

21.2 Linear Diophantine Equations

In high school, you looked at linear equations that involved real numbers. We will look at linear equations involving only integers.

Definition 21.2.1 **Diophantine Equations**

Equations with integer co-efficients for which integer solutions are sought, are called **Diophantine equations** after the Greek mathematician, Diophantus of Alexandria, who studied such equations. Diophantine equations are called **linear** if each term in the equation is a constant or a constant times a single variable of degree 1.

The simplest linear Diophantine equation is

$$ax = b$$

To emphasize, a and b are given integers in $\mathbb{Z}$ and we want an $x \in \mathbb{Z}$ that solves $ax = b$. From the definition of divisibility, we know that this equation has an integer solution x if and only if $a \mid b$, and if $a \mid b$, then $x = \frac{b}{a}$.

What about linear Diophantine equations with two variables?

$$ax + by = c$$

21.2.1 Finding One Solution to $ax + by = c$

Theorem 1 **(Linear Diophantine Equation Theorem, Part 1 (LDET 1))**

Let $\gcd(a, b) = d$. The linear Diophantine equation

$$ax + by = c$$

has a solution if and only if $d \mid c$.

Before we study a proof of this theorem, let's see how it works in practice.

Example 1 Which of the following linear Diophantine equations has a solution?

1. $33x + 18y = 10$
2. $33x + 18y = 15$

Solution:

1. Since $\gcd(33, 18) = 3$, and 3 does not divide 10, the first equation has no integer solutions.
2. Since $\gcd(33, 18) = 3$, and 3 does divide 15, the second equation does have an integer solution.

But how do we find a solution? Here are two simple steps that will allow us to find a solution.

1. Use the Extended Euclidean Algorithm to find $d = \gcd(a, b)$ and x_1 and y_1 where
$$ax_1 + by_1 = d. \tag{21.1}$$
2. Multiply Equation 21.1 by $k = \frac{c}{d}$ to get $akx_1 + bky_1 = kd = c$. A solution is $x = kx_1$ and $y = ky_1$.

Applying these two steps to Part 2 of the example, the Extended Euclidean Algorithm gives

x	y	r	q
1	0	33	0
0	1	18	0
1	-1	15	1
-1	2	3	1
6	-11	0	5

hence

$$33 \times -1 + 18 \times 2 = 3$$

Multiplying by $k = \dfrac{c}{d} = \dfrac{15}{3} = 5$ gives

$$33 \times -5 + 18 \times 10 = 15$$

so one particular solution is $x = -5$ and $y = 10$.

But are there more solutions? That's where Part 2 of the Linear Diophantine Equation Theorem comes in and we will cover it later.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. First, suppose that the linear Diophantine equation $ax+by = c$ has an integer solution $x = x_0$, $y = y_0$. That is, $ax_0 + by_0 = c$.
2. Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$.
3. But then, by the Divisibility of Integer Combinations, $d \mid (ax_0 + by_0)$. That is $d \mid c$.
4. Conversely, suppose that $d \mid c$.
5. Then there exists an integer k such that $c = kd$.
6. Now, by the Extended Euclidean Algorithm, there exist integers x_1 and y_1 so that
$$ax_1 + by_1 = d.$$
7. Multiplying this equation by $k = \dfrac{c}{d}$ gives
$$akx_1 + bky_1 = kd = c$$
which, in turn, implies that $x = kx_1$ and $y = ky_1$ is a solution to $ax + by = c$.

□

Let's perform an analysis of this proof.

Analysis of Proof This is an "if and only if" statement so we must prove two statements.

1. If the linear Diophantine equation $ax + by = c$ has a solution, then $d \mid c$.
2. If $d \mid c$, then the linear Diophantine equation $ax + by = c$ has a solution.

Core Proof Technique: Both statements contain an existential quantifier in the hypothesis, so each will start with the Object Method. Though both statements also contain an existential quantifier in the conclusion, only one uses the Construct Method. The other uses a proposition we have already proved.

Sentence 1 *First, suppose that the linear Diophantine equation $ax + by = c$ has an integer solution $x = x_0$, $y = y_0$. That is, $ax_0 + by_0 = c$.*

The author does not explicitly rephrase the "if and only if" as two statements. Rather, Sentence 1 indicates which of the two implicit statements will be proved by stating the hypothesis of Statement 1. Moreover, the first statement uses an existential quantifier in the hypothesis. The hypothesis of the first statement could be restated as there exists an integer solution x_0, y_0 to the linear Diophantine equation $ax + by = c$

The four parts are

Quantifier:	$\exists$
Variable:	x_0, y_0
Domain:	$\mathbb{Z}$
Open sentence:	$ax + by = c$.

Since the existential quantifier occurs in the hypothesis, the author uses the Object Method. The author assumes the existence of the corresponding objects (x_0, y_0) in a suitable domain $(\mathbb{Z})$ and assumes that these objects satisfy the related open sentence $(ax + by = c)$.

Sentence 2 *Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$.*

This follows from the definition of gcd.

Sentence 3 *But then, by the Divisibility of Integer Combinations, $d \mid (ax_0 + by_0)$. That is $d \mid c$.*

Since the hypotheses of DIC (a, b and d are integers, and $d \mid a$ and $d \mid b$) are satisfied, the author can invoke the conclusion of DIC ($d \mid (ax_0 + by_0)$). And from Sentence 1, $ax_0 + by_0 = c$ so $d \mid c$.

Sentence 4 *Conversely, suppose that $d \mid c$.*

The *conversely* indicates that the author is about to prove Statement 2. Recall that an "if and only if" always consists of a statement and its converse. The hypothesis of the converse is $d \mid c$. The definition of divides contains an existential quantifier and so, in Sentence 5, the authors uses the Object Method. The conclusion of Statement 2 contains an existential quantifier (there exists an integer solution to the linear Diophantine equation), so the author uses the Construct Method to build a suitable solution. Here are the parts of the existential quantifier in the conclusion.

Quantifier:	$\exists$
Variable:	x, y
Domain:	$\mathbb{Z}$
Open sentence:	$ax + by = c$.

Sentence 5 *Then there exists an integer k such that $c = kd$.*

This is the Object Method and follows from the definition of divisibility.

Sentence 6 *Now, by the Extended Euclidean Algorithm, there exist integers x_1 and y_1 so that*

$$ax_1 + by_1 = d.$$

The author is making use of a previously proved proposition.

Sentence 7 *Multiplying this equation by $k = \frac{c}{d}$ gives*

$$akx_1 + bky_1 = kd = c$$

which, in turn, implies that $x = kx_1$ and $y = ky_1$ is a solution to $ax + by = c$.

This is where the solution is constructed, $x = kx_1$ and $y = ky_1$, and where the open sentence is verified. The author does not explicitly check that kx_1 and kx_2 are integers, though we must when we analyse the proof.

Chapter 22

Linear Diophantine Equations: All Solutions

22.1 Objectives

The technique objectives are:

1. To practice working with universal quantifiers.
2. To practice working with subsets.

The content objectives are:

1. Discover a proof to the *Linear Diophantine Equation Theorem (Part 2)*.
2. Examples of the Linear Diophantine Equation Theorem.

22.2 Finding All Solutions to $ax + by = c$

LDET 1 tells us when solutions exist and how to construct *a* solution. It does not find all of the solutions. That happens next.

Theorem 1 **(Linear Diophantine Equation Theorem, Part 2, (LDET 2))**

Let $\gcd(a, b) = d$ where both a and b are not zero. If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + by = c$, then the complete integer solution is

$$x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ \forall n \in \mathbb{Z}.$$

Before we discover a proof, let's make sure we understand the statement.

Example 1

Find all solutions to $33x + 18y = 15$.

Solution: Since $\gcd(33, 18) = 3$, and 3 does divide 15, this equation does have integer solutions by the Linear Diophantine Equation Theorem, Part 1. If we can find one solution, we can use the Linear Diophantine Equation Theorem, Part 2 to find all solutions. Since we earlier found the solution $x = -5$ and $y = 10$ the complete solution is

$$\{(x, y) \mid x = -5 + 6n, y = 10 - 11n, n \in \mathbb{Z}\}$$

You we can check that these are solutions by substitution.

Check:

$$33x + 18y = 33(-5 + 6n) + 18(10 - 11n) = -165 + 198n + 180 - 198n = 15$$

This check does not verify that we have found all solutions. It verifies that all of the pairs of integers we have found are solutions.

The expression "complete integer solution" in the statement of LDET 2 hides the use of sets. Let's be explicit about what those sets are and what we need to do with them. There are, in fact, two sets in the conclusion, the set of solutions, and the set of x and y pairs. We define them formally as follows.

Complete solution Let $S = \{(x, y) \mid x, y \in \mathbb{Z},\ ax + by = c\}$

Proposed solution Let $T = \{(x, y) \mid x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ n \in \mathbb{Z}\}$

The conclusion of LDET 2 is $S = T$.

How do we show that two sets are equal? Two sets S and T are equal if and only if $S \subseteq T$ and $T \subseteq S$. That is, at the risk of being repetitive, to establish that $S = T$ we must show two things.

1. $S \subseteq T$ and
2. $T \subseteq S$

Normally one of the two is easy and the other is harder.

Suppose we want to show $S \subseteq T$. How do universal quantifiers figure in? Showing that $S \subseteq T$ is equivalent to the following statement.

$S \subseteq T$ if and only if, for every member $s \in S$, $s \in T$.

If you prefer symbolic notation you could write $\forall s \in S, s \in T$ or $s \in S \Rightarrow s \in T$.

What are the components of the universal quantifier?

Quantifier:	$\forall$
Variable:	s
Domain:	S
Open sentence:	$s \in T$

The Select Method works perfectly in these situations.

As frequently as sets are used, they are usually implicit and our first task is to discern what sets exist and how they are used. Let's return to the proof of LDET 2 where our sets are:

Complete solution Let $S = \{(x, y) \mid x, y \in \mathbb{Z},\ ax + by = c\}$

Proposed solution Let $T = \{(x, y) \mid x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ n \in \mathbb{Z}\}$

Let us discover a proof. We must keep in mind that we have two things to prove

1. $S \subseteq T$ and
2. $T \subseteq S$

In this case, item 2 is easier so we will do it first. How do we show that $T \subseteq S$? We must show that "for all $x \in T, x \in S$". We certainly don't want to individually check every element of T so we choose a representative element of T, one that could be replaced by any element of T and the subsequent argument would hold. This is just the Select Method and it provides our first statement.

> Let $n_0 \in \mathbb{Z}$. Then $(x_0 + \frac{b}{d}n_0, y_0 - \frac{a}{d}n_0) \in T$.

To show that this element is in S we must show that the element satisfies the defining property of S, that is, the element is a solution.

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}n_0\right) + b\left(y_0 - \frac{a}{d}n_0\right) \\ &= ax_0 + by_0 + \frac{ab}{d}n_0 - \frac{ab}{d}n_0 \\ &= ax_0 + by_0 \\ &= c \quad \text{(by hypothesis, } x = x_0 \text{ and } y = y_0 \text{ is an integer solution)} \end{aligned}$$

And now we can conclude

$$(x_0 + \frac{b}{d}n_0, y_0 - \frac{a}{d}n_0) \in S$$

To show that $S \subseteq T$ we will need to recall the proposition Division by the GCD.

Proposition 2 **(Division by the GCD)**

Let a and b be integers. If $\gcd(a, b) = d \neq 0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Let's begin our analysis of $S \subseteq T$. How do we show that $S \subseteq T$? We choose a representative element in S and show that it is in T, that is, that it satisfies the defining property of T. Specifically, we must show that an arbitrary solution (x, y) has the form $(x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n)$.

Let (x, y) be an arbitrary solution. Then $(x, y) \in S$ and we must show $(x, y) \in T$. Let (x_0, y_0) be a particular solution to the linear Diophantine equation $ax + by = c$. The existence of (x_0, y_0) is assured by the hypothesis. Let's do the obvious thing and substitute both solutions into the equation.

$$\begin{array}{rcrcl} ax & + & by & = & c \\ ax_0 & + & by_0 & = & c \end{array}$$

Eliminating c and factoring gives

$$a(x - x_0) = -b(y - y_0)$$

Since $a \neq 0$ and $b \neq 0$ we know that $d = \gcd(a, b) \neq 0$. Since d is a non-zero common factor of a and b, $\frac{a}{d}$ and $\frac{b}{d}$ are both integers. Dividing the previous equation by d gives

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0) \tag{22.1}$$

Using Division by the GCD, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Since $\frac{b}{d}$ divides $\frac{a}{d}(x - x_0)$ we know from Coprimeness and Divisibility that

$$\frac{b}{d} \,\Big|\, (x - x_0)$$

By the definition of divisibility, there exists an $n \in \mathbb{Z}$ so that

$$x - x_0 = n\frac{b}{d} \Rightarrow x = x_0 + \frac{b}{d}n$$

Substituting $n\frac{b}{d}$ for $x - x_0$ in Equation (22.1) yields

$$y = y_0 - \frac{a}{d}n$$

So every solution is of the form

$$(x, y) = (x_0 + \frac{b}{d}n, y_0 - \frac{a}{d}n)$$

and so

$$(x, y) \in T$$

A very condensed proof of Linear Diophantine Equation Theorem, Part 2 might look like the following. Notice the lack of mention of sets.

Theorem 3 **(Linear Diophantine Equation Theorem, Part 2, (LDET 2))**

Let $\gcd(a,b) = d \neq 0$. If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + by = c$, then the complete integer solution is

$$x = x_0 + \frac{b}{d}n,\ y = y_0 - \frac{a}{d}n,\ \forall n \in \mathbb{Z}.$$

Proof: Substitution shows that integers of the form $x = x_0 + n\frac{b}{d}$, $y = y_0 - \frac{a}{d}n$, $n \in \mathbb{Z}$ are solutions.

Now, let (x, y) be an arbitrary solution and let (x_0, y_0) be a particular solution to the linear Diophantine equation $ax + by = c$. Then

$$\begin{array}{ccccc} ax & + & by & = & c \\ ax_0 & + & by_0 & = & c \end{array}$$

Eliminating c and factoring gives $a(x - x_0) = -b(y - y_0)$ (1). Dividing by d and using Division by the GCD and Coprimeness and Divisibility we have $\frac{b}{d} \mid (x - x_0)$. Hence, there exists an $n \in \mathbb{Z}$ so that $x = x_0 + \frac{b}{d}n$ (2). Substituting (2) in (1) gives $y = y_0 - \frac{a}{d}n$ as needed. $\square$

Exercise 1 Find all solutions to

1. $35x + 21y = 28$
2. $35x - 21y = 28$

22.3 More Examples

1. (a) Find all integer solutions to the linear Diophantine equation $36x + 48y = 18$.
   Solution: Since $\gcd(36, 48) = 12$ and $12 \nmid 18$, no solutions exists by LDET 1.

   (b) Find all integer solutions to the linear Diophantine equation $36x + 438y = 18$.
   Solution: First, we apply the EEA to 36 and 438.

y	x	r	q
1	0	438	0
0	1	36	0
1	-12	6	12
-6	73	0	6

By the EEA, $\gcd(36, 438) = 6$ and

$$36 \cdot (-12) + 438 \cdot 1 = 6$$

Multiplying by 3 gives

$$36 \cdot (-36) + 438 \cdot 3 = 18$$

and so $x_0 = -36$ and $y_0 = 3$ is one particular solution to $36x + 438y = 18$.
By LDET 2, the complete solution is

$$\left.\begin{array}{rcl} x & = & -36 + 73n \\ y & = & 3 - 6n \end{array}\right\} n \in \mathbb{Z}$$

(c) Find all positive integer solutions, if any, to the linear Diophantine equation $36x + 438y = 18$.

Solution: Following on from part (b), we are looking for values of n so that $x > 0$ and $y > 0$. That is,

$$-36 + 73n > 0 \text{ and } 3 - 6n > 0$$

Now

$$-36 + 73n > 0 \Rightarrow n > \frac{36}{73}$$

Since n is an integer, this gives $n \geq 1$. Also,

$$3 - 6n > 0 \Rightarrow n < \frac{3}{6}$$

Since n is an integer, this gives $n \leq 0$.
There are no integers that simultaneously satisfy $n \geq 1$ and $n \leq 0$, so no positive integer solutions to $36x + 438y = 18$ exist.

2. What is the complete solution to the linear Diophantine equation $1950x - 770y = 30$?

We begin with the EEA applied to 1950 and 770. We will adjust the signs later.

x	y	r	q
1	0	1950	0
0	1	770	0
1	-2	410	2
-1	3	360	1
2	-5	50	1
-15	38	10	7
77	-195	0	5

Now we see that

$$1950(-15) - 770(-38) = 10$$

Multiplying by 3 gives one particular solution, $x_0 = -45$, $y_0 = -114$ to $1950x - 770y = 30$. The complete solution is

$$x = -45 - 77n$$
$$y = -114 - 195n$$

for $n \in \mathbb{Z}$.

Check: $1950x - 770y = 1950(-45-77n) - 770(-114-195n) = 1950(-45) - 1950(77n) + 770(114) + 770(195n) = 1950(-45) + 770(114) = -87750 + 87780 = 30$.

3. (From a collection attributed to Alcuin of York in 775 who is known to have sent a collection of similar problems to Charlemagne.)

   One hundred bushels of grain are distributed among one hundred people in such a way that every man receives three bushels, every woman receives two bushels and every child receives half a bushel. How many men, women and children are there? (Give all possible solutions if more than one exists.)

   Solution: Let m represent the number of men, w the number of women and c the number of children. The statement of the problem implies that

$$\begin{array}{rcrcrcl} m & + & w & + & c & = & 100 \\ 3m & + & 2w & + & 0.5c & = & 100 \end{array}$$

   Multiplying the second equation by 2 and eliminating the c gives

$$5m + 3w = 100 \tag{22.2}$$

   One obvious solution to Equation 22.2 is $m = 20$ and $w = 0$ and the complete solution to Equation 22.2 is

$$\left.\begin{array}{rcl} m & = & 20 + 3n \\ y & = & 0 - 5n \end{array}\right\} n \in \mathbb{Z}$$

   The complete set of solutions for the problem is enumerated in the table below.

n	m	w	c
0	20	0	80
−1	17	5	78
−2	14	10	76
−3	11	15	74
−4	8	20	72
−5	5	25	70
−6	2	30	68

4. Prove the following statement. If k and ℓ are coprime positive integers, then the linear Diophantine equation $kx - \ell y = c$ has infinitely many solutions in the positive integers.

   Proof: Since k and ℓ are coprime, $\gcd(k, \ell) = 1$. By the EEA there exist integers x_0, y_0 such that

$$kx_0 + \ell y_0 = 1$$

   Equivalently

$$kx_0 - \ell(-y_0) = 1$$

   Multiplying by c gives

$$k(cx_0) - \ell(-cy_0) = c$$

   so $x = cx_0$ and $y = -cy_0$ is one particular solution to $kx - \ell y = c$. By LDET 2, the complete solution to $kx - \ell y = c$ is

$$x = cx_0 - \ell n$$
$$y = -cy_0 - kn$$

   where $n \in \mathbb{Z}$.

Since k and ℓ are positive, if we choose $n < 0$ then $-nk$ and $-n\ell$ are positive. Since we want

$$x = cx_0 - \ell n > 0 \text{ and } y = -cy_0 - kn > 0$$

we must have

$$n < \frac{cx_0}{\ell} \text{ and } n < -\frac{cy_0}{k}$$

Thus

$$\begin{aligned} x &= cx_0 - \ell n \\ y &= -cy_0 - kn \end{aligned}$$

for $n < \min\left\{\frac{cx_0}{\ell}, -\frac{cy_0}{k}\right\}$ gives infinitely many positive integer solutions to $kx - \ell y = c$. □

22.4 Practice

1. Solve the following problems.

   (a) Find the complete solution to $7x + 11y = 3$.

   (b) Find the complete solution to $35x - 42y = 14$.

   (c) Find the complete solution to $28x + 60y = 10$.

   (d) For what value of c does $8x + 5y = c$ have exactly one solution where both x and y are strictly positive?

2. Let $a, b, c \in \mathbb{Z}$. Consider the following statement:

   For every integer x_0, there exists an integer y_0 such that $ax_0 + by_0 = c$.

   (a) Determine conditions on a, b, c such that the statement is true if and only if these conditions hold. State and prove this if and only if statement.

   (b) Using part (a), write down one set of values for a, b, c for which the statement is false.

   (c) Write down the negation of the statement without using any form of the word “not” (the symbol $\neq$ is acceptable).

   (d) Prove that the negated statement of part (c) is true for the set of values you have chosen in part (b).

3. Let $a, b, c, n \in \mathbb{Z}$. Consider the following two linear Diophantine equations:

$$ax + by = c \tag{22.3}$$
$$ax + by = nc \tag{22.4}$$

   Let S and T be the set of all integer solutions to equations (22.3) and (22.4) respectively. The following set S^* might be the same as set T:

$$S^* = \{(nx_0, ny_0) \mid (x_0, y_0) \in S\}.$$

   (a) Prove that $S^* \subseteq T$ for all values of $a, b, c, n \in \mathbb{Z}$.

   (b) Determine whether or not $S^* = T$ for all values of $a, b, c, n \in \mathbb{Z}$. Justify your answer with a proof or a counterexample.

4. Prove each of the following propositions.

   (a) Suppose a and b are fixed integers. Then

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \{n \cdot \gcd(a, b) \mid n \in \mathbb{Z}\}.$$

Chapter 23

Congruence

23.1 Objectives

The content objectives are:

1. Define *a is congruent to b modulo m*.
2. Read a proof of *Congruence is an Equivalence Relation*.
3. Discover the proof of *Properties of Congruence*.
4. Read the proof of *Congruences and Division*.
5. Do examples.

23.2 Congruences

23.2.1 Definition of Congruences

One of the difficulties in working out properties of divisibility is that we don't have an "arithmetic" of divisibility. Wouldn't it be nice if we could solve problems about divisibility in much the same way that we usually do arithmetic: add, subtract, multiply and divide?

Carl Friedrich Gauss (1777 – 1855) was the greatest mathematician of the last two centuries. In a landmark work, *Disquisitiones Arithmeticae*, published when Gauss was 23, he introduced congruences and provided a mechanism to treat divisibility with arithmetic.

Definition 23.2.1
Congruent

Let m be a fixed positive integer. If $a, b \in \mathbb{Z}$ we say that a is **congruent** to b **modulo** m, and write

$$a \equiv b \pmod{m}$$

if $m \mid (a-b)$. If $m \nmid (a-b)$, we write $a \not\equiv b \pmod{m}$.

Example 1

Verify each of the following

1. $20 \equiv 2 \pmod{6}$
2. $2 \equiv 20 \pmod{6}$
3. $20 \equiv 8 \pmod{6}$
4. $-20 \equiv 4 \pmod{6}$
5. $24 \equiv 0 \pmod{6}$
6. $5 \not\equiv 3 \pmod{7}$

REMARK

One already useful trait of this definition is the number of equivalent ways we have to work with it.

$$\begin{aligned} & a \equiv b \pmod{m} \\ \iff & m \mid (a-b) \\ \iff & \exists k \in \mathbb{Z} \ni a-b=km \\ \iff & \exists k \in \mathbb{Z} \ni a=km+b \end{aligned}$$

23.3 Elementary Properties

Another extraordinarily useful trait of this definition is that it behaves a lot like equality. Equality is an *equivalence relation*. That is, it has the following three properties:

1. *reflexivity*, $a = a$.
2. *symmetry*, If $a = b$ then $b = a$.
3. *transitivity*, If $a = b$ and $b = c$, then $a = c$.

Most relationships that you can think of do not have these three properties. The relation *greater than* fails reflexivity. The relation *divides* fails symmetry. The non-mathematical relation *is a parent of* fails transitivity.

Proposition 1 **(Congruence Is An Equivalence Relation (CER))**

Let $a, b, c \in \mathbb{Z}$. Then

1. $a \equiv a \pmod{m}$.
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

These may seem obvious but as the earlier examples showed, many relations do not have these properties. So, a proof is needed. We will give a proof for all of them, and then an analysis for part 3.

Proof: We show each part in turn.

1. Because $a - a = 0$ and $m \mid 0$, the definition of congruence gives $a \equiv a \pmod{m}$.
2. Since $a \equiv b \pmod{m}$, $m \mid (a - b)$ which in turn implies that there exists $k \in \mathbb{Z}$ so that $km = a - b$. But if $km = a - b$, then $(-k)m = b - a$ and so $m \mid (b - a)$. By the definition of congruence, $b \equiv a \pmod{m}$.
3. Since $a \equiv b \pmod{m}$, $m \mid (a - b)$. Since $b \equiv c \pmod{m}$, $m \mid (b - c)$. Now, by the Divisibility of Integer Combinations, $m \mid ((1)(a - b) + (1)(b - c))$ so $m \mid (a - c)$. By the definition of congruence, $a \equiv c \pmod{m}$.

□

Analysis of Proof We will prove part 3 of the proposition Congruence Is An Equivalence Relation.

Hypothesis: $a, b, c \in \mathbb{Z}$, $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.

Conclusion: $a \equiv c \pmod{m}$.

Sentence 1 *Since* $a \equiv b \pmod{m}$, $m \mid (a - b)$.

The author is working forward from the hypothesis using the definition of congruence.

Sentence 2 *Since* $b \equiv c \pmod{m}$, $m \mid (b - c)$.

The author is working forward from the hypothesis using the definition of congruence.

Sentence 3 *Now, by the Divisibility of Integer Combinations,* $m \mid ((1)(a - b) + (1)(b - c))$ *so* $m \mid (a - c)$.

Here it is useful to keep in mind where the author is going. The question "How do I show that one number is congruent to another number?" has the answer, in this case, of showing that $m \mid (a - c)$ so the author needs to find a way of generating $a - c$. And $a - c$ follows nicely from an application of the Divisibility of Integer Combinations.

Sentence 4 *By the definition of congruence,* $a \equiv c \pmod{m}$.

The author is working forward from $m \mid (a - c)$ using the definition of congruence.

Proposition 2 **(Properties of Congruence (PC))**

Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a - b \equiv a' - b' \pmod{m}$
3. $ab \equiv a'b' \pmod{m}$

This proposition allows us to perform substitutions of congruent values. We will discover a proof of the third part and leave the first two parts as exercises.

As usual we begin by identifying the hypothesis and the conclusion.

Hypothesis: $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$

Conclusion: $ab \equiv a'b' \pmod{m}$

Let's consider the question "How do we show that two numbers are congruent to one another?" The obvious abstract answer is "Use the definition of congruent." We may want to keep in mind, however, that there are several equivalent forms.

$$\begin{aligned} & a \equiv b \pmod{m} \\ \iff & m \mid (a - b) \\ \iff & \exists k \in \mathbb{Z} \ni a - b = km \\ \iff & \exists k \in \mathbb{Z} \ni a = km + b \end{aligned}$$

It is not at all clear which is best or whether, in fact, several could work. Since the conclusion of part three involves the arithmetic operation of multiplication, and we don't have multiplication properties for equivalence or divisibility, it makes sense to consider either the third or fourth of the equivalent forms. There isn't much to separate them. I'll choose the last form and see how it works. So, the answer to "How do we show that two numbers are congruent to one another?" in the notation of this proof is "We must find an integer k so that $ab = km + a'b'$. Let's record that.

Proof in Progress

1. *To be completed.*
2. Since there exists k so that $ab = km + a'b'$, $ab \equiv a'b' \pmod{m}$.

The problem is how to find k. There is no obvious way backwards here so let's start working forward. The two hypotheses $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ can be restated in any of their equivalent forms. Since we have already decided that we would work backwards with the fourth form, it makes sense to use the same form working forwards. That gives two statements.

Proof in Progress

1. Since $a \equiv a' \pmod{m}$, there exists an integer j such that $a = mj + a'$ (1).
2. Since $b \equiv b' \pmod{m}$, there exists an integer h such that $b = mh + b'$ (2).
3. *To be completed.*
4. Since there exists k so that $ab = km + a'b'$, $ab \equiv a'b' \pmod{m}$.

But now there seems to be a rather direct way to produce an ab and an $a'b'$ which we want for the conclusion. Just multiply equations (1) and (2) together. Doing that produces

$$ab = m^2jh + mjb' + a'mh + a'b' = (mjh + jb' + a'h)m + a'b'$$

If we let $k = mjh + jb' + a'h$ then k is an integer and satisfies the property we needed in the last line of the proof, that is $ab = km + a'b'$. Let's record this.

Proof in Progress

1. Since $a \equiv a' \pmod{m}$, there exists an integer j such that $a = mj + a'$ (1).
2. Since $b \equiv b' \pmod{m}$, there exists an integer h such that $b = mh + b'$ (2).
3. Multiplying (1) by (2) gives $ab = m^2jh+mjb'+a'mh+a'b' = (mjh+jb'+a'h)m+a'b'$.
4. Since there exists k so that $ab = km + a'b'$, $ab \equiv a'b' \pmod{m}$.

Lastly, we write a proof. Note that the reader of the proof is expected to be familiar with the equivalent forms.

Proof: Since $a \equiv a' \pmod{m}$, there exists an integer j such that $a = mj + a'$ (1). Since $b \equiv b' \pmod{m}$, there exists an integer h such that $b = mh + b'$ (2). Multiplying (1) by (2) gives

$$ab = m^2jh + mjb' + a'mh + a'b' = (mjh + jb' + a'h)m + a'b'.$$

Since $mjh + jb' + a'h$ is an integer, $ab \equiv a'b' \pmod{m}$. □

Exercise 1 Prove the remainder of the Properties of Congruence proposition.

There are four arithmetic operations with integers, but analogues to only three have been given. It turns out that division is problematic. A statement of the form

$$ab \equiv ab' \pmod{m} \Rightarrow b \equiv b' \pmod{m}$$

seems natural enough, simply divide by a. This works with the integer equation $ab = ab'$. But consider the case where $m = 12$, $a = 6$, $b = 3$ and $b' = 5$. It is indeed true that

$$18 \equiv 30 \pmod{12}$$

and so

$$6 \times 3 \equiv 6 \times 5 \pmod{12}$$

But "dividing" by 6 gives the clearly false statement

$$3 \equiv 5 \pmod{12}.$$

Division works only under the specific conditions of the next proposition.

Proposition 3 **(Congruences and Division (CD))**

If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Before we read the proof, let's look at an example.

Example 2 Examples of division in congruence relations.

1. $8 \times 7 \equiv 17 \times 7 \pmod{3} \Rightarrow 8 \equiv 17 \pmod{3}$
2. For $6 \times 3 \equiv 6 \times 5 \pmod{12}$, CD cannot be invoked. Why?

   Because $\gcd(c, m) = \gcd(6, 12) = 6 \neq 1$, the hypotheses of CD are not satisfied and so the conclusion of CD cannot be invoked.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Since $ac \equiv bc \pmod{m}$, $m \mid (ac - bc)$. That is, $m \mid c(a - b)$.
2. By the proposition Coprimeness and Divisibility, $m \mid (a - b)$.
3. Hence, by the definition of congruence $a \equiv b \pmod{m}$.

□

Exercise 2 Analyze the proof of the proposition on Congruences and Division.

23.4 More Examples

1. In each of the following cases, find all values of a, $0 \leq a < m$ where m is the modulus, that satisfy the congruence relation.

   (a) $a \equiv 52 \pmod{12}$
   (b) $-14 \equiv a \pmod{15}$
   (c) $2a \equiv 5 \pmod{7}$
   (d) $2a \equiv 5 \pmod{8}$
   (e) $2a \equiv 4 \pmod{8}$
   (f) $a^2 \equiv 1 \pmod{7}$

   Solution:

   (a) $a = 4$
   (b) $a = 1$
   (c) $a = 6$
   (d) No solution exists
   (e) $a \in \{2, 6\}$
   (f) $a \in \{1, 6\}$

23.5 Practice

1. This question deals with divisibility by nine.

   (a) Let $n = 387140$ and let d be the sum of the digits of n.

      i. Determine the value of d?

      ii. Does $9 \mid d$?

      iii. Does $9 \mid n$?

   (b) Let $n = 6532488$ and let d be the sum of the digits of n.

      i. Determine the value of d?

      ii. Does $9 \mid d$?

      iii. Does $9 \mid n$?

   (c) Prove the following statement. Let n be a positive integer and let d be the sum of the digits of n. Then n is divisible by 9 if and only if d is divisible by 9.

   Hint: Let the decimal representation of n be $a_r a_{r-1} a_{r-2} \ldots a_1 a_0$. Then

$$n = 10^r a_r + 10^{r-1} a_{r-1} + 10^{r-2} a_{r-2} + \ldots + 10a_1 + a_0$$

Chapter 24

Congruence and Remainders

24.1 Objectives

The content objectives are:

1. Read the proof of *Congruent Iff Same Remainder*.
2. Do examples.

24.2 Congruence and Remainders

We now give one more statement that is equivalent to $a \equiv b \pmod{m}$.

Proposition 1 **(Congruent Iff Same Remainder (CISR))**

$a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m.

Because this proposition is an "if and only if" proposition, there are two parts to the proof: a statement and its converse. We can restate the proposition to make the two parts more explicit.

Proposition 2 **(Congruent Iff Same Remainder (CISR))**

1. If $a \equiv b \pmod{m}$, then a and b have the same remainder when divided by m.
2. If a and b have the same remainder when divided by m, then $a \equiv b \pmod{m}$.

In practice, the two statements are not usually written out separately. The author assumes that you do that whenever you read "if and only if". Many "if and only if" proofs begin with some preliminary material that will help both parts of the proof. For example, they often introduce notation that will be used in both parts.

Let's look at a proof of the *Congruent Iff Same Remainder* proposition. Before we do an analysis, make sure that you can identify

1. preliminary material (if any exists)
2. the proof of a statement
3. the proof of the converse of the statement

Proof: The Division Algorithm applied to a and m gives

$$a = q_1 m + r_1, \text{where } 0 \leq r_1 < m$$

The Division Algorithm applied to b and m gives

$$b = q_2 m + r_2, \text{where } 0 \leq r_2 < m$$

Subtracting the second equation from the first gives

$$a - b = (q_1 - q_2)m + (r_1 - r_2), \text{where } -m < r_1 - r_2 < m$$

If $a \equiv b \pmod{m}$, then $m \mid (a - b)$ and there exists an integer h so that $hm = a - b$. Hence

$$a - b = (q_1 - q_2)m + (r_1 - r_2) \Rightarrow hm = (q_1 - q_2)m + (r_1 - r_2) \Rightarrow r_1 - r_2 = m(h - q_1 + q_2)$$

which implies $m \mid (r_1 - r_2)$. But, $-m < r_1 - r_2 < m$ so $r_1 - r_2 = 0$.

Conversely, if a and b have the same remainder when divided by m, then $r_1 = r_2$ and $a - b = (q_1 - q_2)m$ so $a \equiv b \pmod{m}$.

□

The preliminary material is quoted below.

> *The Division Algorithm applied to a and m gives*
>
> $$a = q_1 m + r_1, \textit{where } 0 \leq r_1 < m$$
>
> *The Division Algorithm applied to b and m gives*
>
> $$b = q_2 m + r_2, \textit{where } 0 \leq r_2 < m$$
>
> *Subtracting the second equation from the first gives*
>
> $$a - b = (q_1 - q_2)m + (r_1 - r_2), \textit{where } -m < r_1 - r_2 < m$$

The proof of Statement 1 is

> *If $a \equiv b \pmod{m}$, then $m \mid (a - b)$ and there exists an integer h so that $hm = a - b$. Hence*
>
> $$a - b = (q_1 - q_2)m + (r_1 - r_2) \Rightarrow hm = (q_1 - q_2)m + (r_1 - r_2) \Rightarrow r_1 - r_2 = m(h - q_1 + q_2)$$
>
> *which implies $m \mid (r_1 - r_2)$. But, $-m < r_1 - r_2 < m$ so $r_1 - r_2 = 0$.*

The proof of the converse of Statement 1, Statement 2, is

Conversely, if a and b have the same remainder when divided by m, then $r_1 = r_2$ and $a - b = (q_1 - q_2)m$ so $a \equiv b \pmod{m}$.

We will do an analysis of the proof of Statement 1. An analysis of the proof of Statement 2 is left as an exercise.

Analysis of Proof In many "if and only if" statements one direction is much easier than the other. In this particular case, we are starting with the harder of the two directions.

Hypothesis: $a \equiv b \pmod{m}$.

Conclusion: a and b have the same remainder when divided by m.

Sentence 1 *If $a \equiv b \pmod{m}$, then $m \mid (a - b)$ and there exists an integer h so that $hm = a - b$.*

Here the author is working forwards using two definitions. The definition of congruence allows the author to assert that "If $a \equiv b \pmod{m}$, then $m \mid (a - b)$". The definition of divisibility allows the author to assert that "$m \mid (a - b)$ [implies that] there exists an integer h so that $hm = a - b$."

Sentence 2 *Hence*

$$a-b = (q_1-q_2)m+(r_1-r_2) \Rightarrow hm = (q_1-q_2)m+(r_1-r_2) \Rightarrow r_1-r_2 = m(h-q_1+q_2)$$

which implies $m \mid (r_1 - r_2)$.

This is mostly arithmetic. The author begins with $a-b = (q_1-q_2)m+(r_1-r_2)$ from the preliminary paragraph, substitutes hm for $a - b$, isolates $r_1 - r_2$ and factors out an m from the remaining terms. Since $h - q_1 + q_2$ is an integer, the author deduces that $m \mid (r_1 - r_2)$.

Sentence 3 *But, $-m < r_1 - r_2 < m$ so $r_1 - r_2 = 0$.*

This part is not so obvious. The author is working with two pieces of information. The prefatory material provides $-m < r_1 - r_2 < m$. Let's take a minute to think about why this statement is true. Sentence 2 provides $m \mid (r_1 - r_2)$. Now, what are the possible values of $r_1 - r_2$? Certainly $r_1 - r_2$ can be zero but are there any other possible choices? If there were another choice it would be of the form mx with $x \neq 0$. But that would make $r_1 - r_2 = xm \geq m$ or $r_1 - r_2 = xm \leq -m$ both of which are impossible because $-m < r_1 - r_2 < m$. Hence, $r_1 - r_2 = 0$.

The conclusion does not say $r_1 - r_2 = 0$. It says that a and b have the same remainder when divided by m. Since r_1 and r_2 are those remainders, and $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$, the author leaves it to the reader to deduce the conclusion.

Exercise 1 Perform an analysis of the proof of Statement 2.

REMARK

The proposition Congruent Iff Same Remainder gives us another part to our chain of equivalent statements.

$$\begin{aligned} & a \equiv b \pmod{m} \\ \iff & m \mid (a-b) \\ \iff & \exists k \in \mathbb{Z} \ni a-b = km \\ \iff & \exists k \in \mathbb{Z} \ni a = km+b \\ \iff & a \text{ and } b \text{ have the same remainder when divided by } m \end{aligned}$$

The propositions covered in this lecture are surprisingly powerful. Consider the following example.

Example 1 What is the remainder when 3^{47} is divided by 7?

Solution: You could attempt to compute 3^{47} with your calculator but it might explode. Here is a simpler way. By the Division Algorithm,

$$3^{47} = 7q + r \text{ where } 0 \le r < 7$$

If we reduce this expression modulo 7 we get

$$\begin{aligned} 3^{47} &\equiv 7q + r \pmod{7} \\ &\equiv r \pmod{7} \end{aligned}$$

Thus, the remainder when 3^{47} is divided by 7 is just $3^{47} \pmod{7}$. Now observe that $3^2 \equiv 2 \pmod{7}$ and $3^3 \equiv 27 \equiv 6 \equiv -1 \pmod{7}$. But then

$$\begin{aligned} 3^{47} &\equiv 3^{45}3^2 \pmod{7} && \text{arithmetic} \\ &\equiv (3^3)^{15}3^2 \pmod{7} && \text{arithmetic} \\ &\equiv (-1)^{15}(2) \pmod{7} && \text{Properties of Congruence (3), twice} \\ &\equiv (-1)(2) \pmod{7} && \text{arithmetic} \\ &\equiv -2 \pmod{7} && \text{arithmetic} \\ &\equiv 5 \pmod{7} && \text{since } 0 \le r < 7 \end{aligned}$$

Hence, the remainder when 3^{47} is divided by 7 is 5.

Example 2 Is $3^{47} \equiv 5^{21} \pmod{7}$?

Solution: By Congruences Iff the Same Remainder $3^{47} \equiv 5^{21} \pmod{7}$ if and only if 3^{47} and 5^{21} have the same remainder when divided by 7. The previous example showed that 5 is the remainder when 3^{47} is divided by 7. We only need to compute the remainder when 5^{21} is divided by 7.

By the Division Algorithm,

$$5^{21} = 7q + r \text{ where } 0 \leq r < 7$$

If we reduce this expression modulo 7 we get

$$\begin{aligned} 5^{21} &\equiv 7q + r \pmod 7 \\ &\equiv r \pmod 7 \end{aligned}$$

Since $5 \equiv -2 \pmod 7$ and $-2^3 \equiv -8 \equiv -1 \pmod 7$, we know $5^3 \equiv -1 \pmod 7$ hence

$$5^{21} \equiv (5^3)^7 \equiv (-1)^7 \equiv -1 \equiv 6 \pmod 7$$

Thus,

$$3^{47} \not\equiv 5^{21} \pmod 7$$

24.3 More Examples

1. What is the remainder when $2^{271}3^{314}$ is divided by 7? Provide justification for your work.

   Solution: First, observe that $2^3 \equiv 1 \pmod 7$ and $3^3 \equiv -1 \pmod 7$ and so by the proposition on the Properties of Congruence,

   $$2^{271}3^{314} \equiv (2^3)^{90}2^1(3^3)^{104}3^2 \equiv (1)^{90}2^1(-1)^{104}3^2 \equiv 2 \cdot 9 \equiv 18 \equiv 4 \pmod 7$$

   Thus, by the proposition Congruent Iff Same Remainder, $2^{271}3^{314}$ has remainder 4 when divided by 7.

24.4 Practice

1. This question deals with divisibility by nine.

   (a) Let $n = 387144$ and d be the sum of the digits of n.

      i. Determine the value of d.

      ii. Does $9 \mid d$?

      iii. Does $9 \mid n$?

   (b) Let $n = 6532422$ and d be the sum of the digits of n.

      i. Determine the value of d.

      ii. Does $9 \mid d$?

      iii. Does $9 \mid n$?

   (c) Prove the following statement.

      Let n be a positive integer and let d be the sum of the digits of n. Then n is divisible by 9 if and only if d is divisible by 9.

      Hint: Let the decimal representation of n be $a_r a_{r-1} a_{r-2} \ldots a_1 a_0$. Then

      $$n = 10^r a_r + 10^{r-1} a_{r-1} + 10^{r-2} a_{r-2} + \ldots + 10a_1 + a_0$$

Chapter 25

Linear Congruences

25.1 Objectives

The content objectives are:

1. Define a *linear congruence in the variable x*.
2. State and prove the *Linear Congruence Theorem*.
3. Do examples.

25.2 The Problem

One of the advantages of congruence over divisibility is that we have an "arithmetic" of congruence. This allows us to solve new kinds of "equations".

Definition 25.2.1
Linear Congruence

A relation of the form

$$ax \equiv c \pmod{m}$$

is called a **linear congruence in the variable** x. A **solution** to such a linear congruence is an integer x_0 so that

$$ax_0 \equiv c \pmod{m}$$

The problem for this lecture is to determine when linear congruences have solutions and how to find them.

Recalling our table of statements equivalent to $a \equiv b \pmod{m}$ we see that

REMARK

$$\begin{aligned}
& ax \equiv c \pmod{m} \text{ has a solution} \\
\iff & \text{there exists an integer } x_0 \text{ such that } ax_0 \equiv c \pmod{m} \\
\iff & \text{there exist integers } x_0, y_0 \text{ such that } ax_0 + my_0 = c \\
\iff & \gcd(a, m) \mid c \qquad \text{(by the Linear Diophantine Equation Theorem, Part 1)}
\end{aligned}$$

Moreover, the Linear Diophantine Equation Theorem, Part 2 tells us what the solutions to $ax + by = c$ look like.

Theorem 1 **(Linear Diophantine Equation Theorem, Part 2, (LDET 2))**

Let $\gcd(a, m) = d \neq 0$.
If $x = x_0$ and $y = y_0$ is one particular integer solution to the linear Diophantine equation $ax + my = c$, then the complete integer solution is

$$x = x_0 + \frac{m}{d}n,\ y = y_0 - \frac{a}{d}n,\ \forall n \in \mathbb{Z}.$$

But then, if $x_0 \in \mathbb{Z}$ is one solution to $ax \equiv c \pmod{m}$ the complete solution will be

$$x \equiv x_0 \pmod{\frac{m}{d}} \text{ where } d = \gcd(a, m)$$

Let's think about why that is. If we reduce the solution given in LDET 2 above modulo $\frac{m}{d}$, then the term involving $\frac{m}{d}$ evaluates to 0 leaving $x \equiv x_0 \pmod{\frac{m}{d}}$.
Since the original problem was posed modulo m, we might like to give solutions modulo m. In which case, $x \equiv x_0 \pmod{\frac{m}{d}}$ is equivalent to

$$x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d} \pmod{m}$$

Note that there are $d = \gcd(a, m)$ distinct solutions modulo m and one solution modulo $\frac{m}{d}$.

We record this discussion as the following theorem.

Theorem 2 **(Linear Congruence Theorem, Version 1, (LCT 1))**

Let $\gcd(a, m) = d \neq 0$.

The linear congruence

$$ax \equiv c \pmod{m}$$

has a solution if and only if $d \mid c$.

Moreover, if $x = x_0$ is one particular solution, then the complete solution is

$$x \equiv x_0 \pmod{\frac{m}{d}}$$

or, equivalently,

$$x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d} \pmod{m}$$

25.3 Examples

Example 1 If possible, solve the linear congruence

$$3x \equiv 5 \pmod{6}$$

Solution: Since $\gcd(3, 6) = 3$ and $3 \nmid 5$, there is no solution to $3x \equiv 5 \pmod{6}$ by the Linear Congruence Theorem, Version 1.

Example 2 If possible, solve the linear congruence

$$4x \equiv 6 \pmod{10}$$

Solution: Since $\gcd(4, 10) = 2$ and $2 \mid 6$, we would expect to find two solutions to $4x \equiv 6 \pmod{10}$. Since ten is a small modulus, we can simply test all possibilities modulo 10.

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$4x \pmod{10}$	0	4	8	2	6	0	4	8	2	6

Hence, $x \equiv 4$ or $9 \pmod{10}$.

Example 3 If possible, solve the linear congruence

$$3x \equiv 5 \pmod{76}$$

Solution: Since $\gcd(3, 76) = 1$ and $1 \mid 5$, we would expect to find one solution to $3x \equiv 5 \pmod{76}$. We could try all 76 possibilities but there is a more efficient way. Thinking of our list of equivalencies, solving $3x \equiv 5 \pmod{76}$ is equivalent to solving $3x + 76y = 5$ and that we know how to do that using the Extended Euclidean Algorithm.

x	y	r	q
1	0	76	0
0	1	3	0
1	-25	1	25
-3	76	0	3

From the second last row, $76(1) + 3(-25) = 1$, or to match up with the order of the original equation, $3(-25) + 76(1) = 1$. Multiplying the equation by 5 gives $3(-125) + 76(5) = 5$. Hence

$$x \equiv -125 \equiv 27 \pmod{76}$$

We can check our work by substitution. $3 \cdot 27 \equiv 81 \equiv 5 \pmod{76}$.

25.4 More Examples

1. For each of the following, determine the complete solution, if a solution exists.

   (a) $4x \equiv 7 \pmod{20}$

   (b) $21x \equiv 9 \pmod{117}$

   Solution:

   (a) Since $\gcd(4, 20) = 4$ and $4 \nmid 7$, no solution exists by LCT 1.

(b) Since $\gcd(21, 117) = 3$ and $3 \mid 9$, a solution exists by LCT 1. We can find a particular solution by solving $21x + 117y = 9$.

First, we apply the EEA to 21 and 117.

y	x	r	q
1	0	117	0
0	1	21	0
1	-5	12	5
-1	6	9	1
2	-11	3	1
-7	39	0	3

By the EEA, $\gcd(21, 117) = 3$ and

$$21 \cdot (-11) + 117 \cdot 2 = 3$$

Multiplying by 3 gives

$$21 \cdot (-33) + 117 \cdot 6 = 9$$

and so $x_0 = -33$ and $y_0 = 6$ is one particular solution to $21x + 117y = 9$.

Thus, a solution to $21x \equiv 9 \pmod{117}$ is $x \equiv -33 \equiv 84 \pmod{117}$ and the complete solution is

$$x \equiv 84, 84 + 39, 84 + 39 \cdot 2 \equiv 84, 6, 45 \pmod{117}$$

or, alternatively,

$$x \equiv 6 \pmod{39}$$

25.5 Practice

1. For each linear congruence, determine the complete solution, if a solution exists.

   (a) $3x \equiv 11 \pmod{18}$

   (b) $4x \equiv 5 \pmod{21}$

   (c) $36x \equiv 8 \pmod{116}$

2. This question asks you to carefully examine the properties of linear congruences.

   (a) Find integers $c \neq 0, a, b, m$ such that the solution set of $ax \equiv b \pmod{m}$ is different from the solution set of $cax \equiv cb \pmod{m}$.

   (b) Suppose we want a proposition that says:

   If ________________, then $ax \equiv b \pmod{m}$ and $cax \equiv cb \pmod{m}$ have the same set of solutions.

   Determine a simple condition on c and m for the hypothesis that makes this proposition correct, and prove this proposition.

Chapter 26

Modular Arithmetic

26.1 Objectives

The content objectives are:

1. Define the *congruence class modulo m*.
2. Construct $\mathbb{Z}_m$ and perform modular arithmetic. Highlight the role of additive and multiplicative identities, and additive and multiplicative inverses.

26.2 Modular Arithmetic

In this section we will see the creation of a number system which will likely be new to you.

Definition 26.2.1
Congruence Class

The **congruence class modulo m** of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

Example 1

For example, when $m = 4$

$$\begin{array}{lllllll} [0] & = & \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} & = & \{\ldots, -8, -4, 0, 4, 8, \ldots\} & = & \{4k \mid k \in \mathbb{Z}\} \\ [1] & = & \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} & = & \{\ldots, -7, -3, 1, 5, 9, \ldots\} & = & \{4k+1 \mid k \in \mathbb{Z}\} \\ [2] & = & \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{m}\} & = & \{\ldots, -6, -2, 2, 6, 10, \ldots\} & = & \{4k+2 \mid k \in \mathbb{Z}\} \\ [3] & = & \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{m}\} & = & \{\ldots, -5, -1, 3, 7, 11, \ldots\} & = & \{4k+3 \mid k \in \mathbb{Z}\} \end{array}$$

REMARK

Note that congruence classes have more than one representation. In the example above $[0] = [4] = [8]$ and, in fact $[0]$ has infinitely many representations. If this seems strange to you, remember that fractions are another example of where one number has infinitely many representations. For example $1/2 = 2/4 = 3/6 = \cdots$.

Definition 26.2.2
$\mathbb{Z}_m$

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

and we define two operations on $\mathbb{Z}_m$, addition and multiplication, as follows:

$$[a] + [b] = [a+b]$$
$$[a] \cdot [b] = [a \cdot b]$$

Though the definition of these operations may seem obvious there is a fair amount going on here.

1. Sets are being treated as individual "numbers". Modular addition and multiplication are being performed on congruence classes which are sets.
2. The addition and multiplication symbols on the left of the equals signs are in $\mathbb{Z}_m$ and those on the right are operations in the integers.
3. We are assuming that the operations are *well-defined*. That is, we are assuming that these operations make sense even when there are multiple representatives of a congruence class.

REMARK

Since
$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$
we can extend our list of equivalent statements to

$$\begin{aligned} & [a] = [b] \text{ in } \mathbb{Z}_m \\ \Longleftrightarrow\ & a \equiv b \pmod{m} \\ \Longleftrightarrow\ & m \mid (a-b) \\ \Longleftrightarrow\ & \exists k \in \mathbb{Z} \ni a - b = km \\ \Longleftrightarrow\ & \exists k \in \mathbb{Z} \ni a = km + b \\ \Longleftrightarrow\ & a \text{ and } b \text{ have the same remainder when divided by } m \end{aligned}$$

Just as there were addition and multiplication tables in grade school for the integers, we have addition and multiplication tables in $\mathbb{Z}_m$.

Example 2 Addition and multiplication tables in $\mathbb{Z}_4$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Note that all of the entries have representatives between 0 and 3. Even though there are many representatives for each congruence class, we usually choose a representative between 0 and $m-1$.

Exercise 1 Write out the addition and multiplication tables in $\mathbb{Z}_5$

26.2.1 $[0] \in \mathbb{Z}_m$

By looking at the tables for $\mathbb{Z}_4$ and $\mathbb{Z}_5$ it seems that $[0] \in \mathbb{Z}_m$ behaves just like $0 \in \mathbb{Z}$. In $\mathbb{Z}$

$$\forall a \in \mathbb{Z}, a + 0 = a$$
$$\forall a \in \mathbb{Z}, a \cdot 0 = 0$$

and in $\mathbb{Z}_m$

$$\forall [a] \in \mathbb{Z}_m, [a] + [0] = [a]$$
$$\forall [a] \in \mathbb{Z}_m, [a] \cdot [0] = [0]$$

This actually follows from our definition of addition and multiplication in $\mathbb{Z}_m$.

$$\forall [a] \in \mathbb{Z}_m, [a] + [0] = [a + 0] = [a]$$
$$\forall [a] \in \mathbb{Z}_m, [a] \cdot [0] = [a \cdot 0] = [0]$$

26.2.2 $[1] \in \mathbb{Z}_m$

In a similar fashion, by looking at the multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_5$ it seems that $[1] \in \mathbb{Z}_m$ behaves just like $1 \in \mathbb{Z}$. In $\mathbb{Z}$

$$\forall a \in \mathbb{Z}, a \cdot 1 = a$$

and in $\mathbb{Z}_m$

$$\forall [a] \in \mathbb{Z}_m, [a] \cdot [1] = [a]$$

This follows from our definition of multiplication in $\mathbb{Z}_m$.

$$\forall [a] \in \mathbb{Z}_m, [a] \cdot [1] = [a \cdot 1] = [a]$$

26.2.3 Identities and Inverses in $\mathbb{Z}_m$

Many of us think of subtraction and division as independent from the other arithmetic operations of addition and multiplication. In fact, subtraction is just addition of the inverse. Now, what's an inverse? To answer that question we must first define an *identity*.

Definition 26.2.3
Identity

Given a set and an operation, an identity is, informally, "something that does nothing". More formally, given a set S and an operation designated by $\circ$, an **identity** is an element $e \in S$ so that

$$\forall a \in S, a \circ e = a$$

The element e has no effect. Having something that does nothing is extremely useful – though parents might not say that of teenagers.

Example 3

Here are examples of sets, operations and identities.

- The set of integers with the operation of addition has the identity 0.
- The set of rational numbers excluding 0 with the operation of multiplication has the identity 1.
- The set of real valued functions with the operation of function composition has the identity $f(x) = x$.
- The set of integers modulo m with the operation of modular addition has the identity $[0]$.

Definition 26.2.4
Inverse

The element $b \in S$ is an **inverse** of $a \in S$ if $a \circ b = b \circ a = e$.

Example 4

Here are examples of inverses.

- Under the operation of addition, the integer 3 has inverse -3 since $3 + (-3) = (-3) + 3 = 0$.
- Under the operation of multiplication, the rational number $\frac{3}{4}$ has inverse $\frac{4}{3}$ since $\frac{3}{4} \cdot \frac{4}{3} = \frac{4}{3} \cdot \frac{3}{4} = 1$.
- Under the operation of function composition $\ln x$ has the inverse e^x since $\ln(e^x) = e^{\ln x} = x$
- Under the operation of modular addition, $[3]$ has the inverse $[-3]$ in $\mathbb{Z}_7$ since $[3] + [-3] = [-3] + [3] = [0]$.

When the operation is addition, we usually denote the inverse by $-a$. Otherwise, we typically denote the inverse of a by a^{-1}. This does cause confusion. Many students interpret

a^{-1} as the reciprocal. This works for real or rational multiplication but fails in other contexts like function composition. We will use $-a$ to mean the inverse of a under addition and a^{-1} to mean the inverse under all other operations.

26.2.4 Subtraction in $\mathbb{Z}_m$

Let's return to $\mathbb{Z}_m$. The identity under addition in $\mathbb{Z}_m$ is [0] since

$$\forall [a] \in \mathbb{Z}_m, [a] + [0] = [a]$$

Given any $[a] \in \mathbb{Z}_m$, $[-a]$ exists and

$$[a] + [-a] = [a - a] = [0]$$

That is, every element $[a] \in \mathbb{Z}_m$ has an additive inverse, $[-a]$. This allows us to define subtraction in $\mathbb{Z}_m$.

Definition 26.2.5
Subtraction

We will define **subtraction** as addition of the inverse. Thus

$$[a] - [b] = [a] + [-b] = [a - b]$$

26.2.5 Division in $\mathbb{Z}_m$

Division is related to multiplication in the same way that subtraction is related to addition. So first, we must identify the multiplicative identity in $\mathbb{Z}_m$. Since

$$\forall [a] \in \mathbb{Z}_m, [a][1] = [a]$$

we know that [1] is the identity under multiplication in $\mathbb{Z}_m$.

Inverses are more problematic with multiplication. Looking at the multiplication table for $\mathbb{Z}_5$ we see that $[2]^{-1} = [3]$ since $[2][3] = [6] = [1]$. But what is the inverse of [2] in $\mathbb{Z}_4$? It doesn't exist! Looking at the row containing [2] in the multiplication table for $\mathbb{Z}_4$ we cannot find [1]. Unlike addition in $\mathbb{Z}_m$ where every element has an additive inverse, it is not always the case that a non-zero element in $\mathbb{Z}_m$ has a multiplicative inverse.

We define division analogously to subtraction.

Definition 26.2.6
Division

Division by $a \in \mathbb{Z}_m$ is defined as multiplication by the multiplicative inverse of $a \in \mathbb{Z}_m$, assuming that the multiplicative inverse exists.

26.3 More Examples

1. Construct addition and multiplication tables for $\mathbb{Z}_6$. Which elements of $\mathbb{Z}_6$ have multiplicative inverses?

   Solution:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

×	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

   The elements [1] and [5] are the only elements with an inverse in $\mathbb{Z}_6$.

2. In each of the following cases, find all values of $[x] \in \mathbb{Z}_m$, $0 \leq x < m$, that satisfy the equation.

   (a) $[4][3] + [5] = [x] \in \mathbb{Z}_{10}$
   (b) $[7]^{-1} - [2] = [x] \in \mathbb{Z}_{10}$
   (c) $[2][x] = [4] \in \mathbb{Z}_8$
   (d) $[3][x] = [9] \in \mathbb{Z}_{11}$

   Solution:

   (a) $x = [7]$
   (b) $x = [1]$
   (c) $x \in \{[2], [6]\}$
   (d) $x = [3]$

26.4 Linear Congruences and Modular Classes

Recall that a **linear congruence** is a relation of the form

$$ax \equiv c \pmod{m}.$$

Another way of considering the same problem is to reframe it in $\mathbb{Z}_m$. Since

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

solving

$$ax \equiv c \pmod{m}$$

is equivalent to finding a congruence class $[x_0] \in \mathbb{Z}_m$ that solves

$$[a][x] = [c] \text{ in } \mathbb{Z}_m$$

Thus

Theorem 1 **(Linear Congruence Theorem, Version 2, (LCT 2))**

Let $\gcd(a, m) = d \neq 0$.

The equation

$$[a][x] = [c] \text{ in } \mathbb{Z}_m$$

has a solution if and only if $d \mid c$.

Moreover, if $x = x_0$ is one particular solution, then the complete solution is

$$\left\{[x_0], \left[x_0 + \frac{m}{d}\right], \left[x_0 + 2\frac{m}{d}\right], \cdots, \left[x_0 + (d-1)\frac{m}{d}\right]\right\} \text{ in } \mathbb{Z}_m$$

26.5 Extending Equivalencies

Putting all of this together we have several views of the same problem.

REMARK

$$\begin{aligned}
&[a][x] = [c] \text{ has a solution in } \mathbb{Z}_m \\
\iff & ax \equiv c \pmod{m} \text{ has a solution} \\
\iff & \text{ there exists an integer } x_0 \text{ such that } ax_0 \equiv c \pmod{m} \\
\iff & \text{ there exist integers } x_0, y_0 \text{ such that } ax_0 + my_0 = c \\
\iff & \gcd(a, m) \mid c
\end{aligned}$$

Moreover, if x_0, y_0 is a particular integer solution to $ax + my = c$ then

$$\begin{aligned}
&\text{the complete solution to } ax + my = c \text{ is } x = x_0 + \frac{m}{d}n,\ y = y_0 - \frac{a}{d}n,\ \forall n \in \mathbb{Z} \\
\iff & \text{the complete solution to } ax \equiv c \pmod{m} \text{ is } x \equiv x_0 \pmod{\frac{m}{d}} \\
\iff & \text{the complete solution to } ax \equiv c \pmod{m} \text{ is} \\
& x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \cdots, x_0 + (d-1)\frac{m}{d} \pmod{m} \\
\iff & \text{the complete solution to } [a][x] = [c] \text{ in } \mathbb{Z}_m \text{ is} \\
& \left\{[x_0], \left[x_0 + \frac{m}{d}\right], \left[x_0 + 2\frac{m}{d}\right], \cdots, \left[x_0 + (d-1)\frac{m}{d}\right]\right\} \text{ in } \mathbb{Z}_m
\end{aligned}$$

Example 5

1. For each of the given elements, determine its inverse, if an inverse exists. Express the inverse as $[b]$ where $1 \leq b < m$.

   (a) $[5] \in \mathbb{Z}_{10}$

(b) $[5] \in \mathbb{Z}_{47}$

Solution:

(a) Finding $[5]^{-1} \in \mathbb{Z}_{10}$ is equivalent to solving $[5][b] = [1]$ in $\mathbb{Z}_{10}$. Since $\gcd(5, 10) = 5$ and $5 \nmid 1$, this equation has no solution by LCT 2.

(b) Finding $[5]^{-1} \in \mathbb{Z}_{47}$ is equivalent to solving $[5][b] = [1]$ in $\mathbb{Z}_{47}$. Since $\gcd(5, 47) = 1$ and $1 \mid 1$, this equation has a solution by LCT 2. Now, solving $[5][b] = [1]$ in $\mathbb{Z}_{47}$ is equivalent to solving $5b + 47y = 1$. We can use the EEA to find a solution.

b	y	r	q
1	0	47	0
0	1	5	0
1	-9	2	9
-2	19	1	2
5	-47	0	2

(Note that the x of the EEA has been written as b to be consistent with the linear Diophantine equation.) The EEA gives $5(19) + 47(-2) = 1$ and so $[5]^{-1} = [19]$ in $\mathbb{Z}_{47}$.

2. Find the inverse of $[13]$ in $\mathbb{Z}_{29}$.

Solution: By definition, the inverse of $[13]$ in $\mathbb{Z}_{29}$ is the congruence class $[x]$ so that $[13][x] = [1]$ in $\mathbb{Z}_{29}$. Since $\gcd(13, 29) = 1$, we know by the Linear Congruence Theorem, Version 2 that there is exactly one solution. We could try all 29 possibilities or recall that solving

$$[13][x] = [1] \text{ in } \mathbb{Z}_{29}$$

is equivalent to solving

$$13x + 29y = 1$$

and that we know how to do using the Extended Euclidean Algorithm.

x	y	r	q
1	0	29	0
0	1	13	0
1	-2	3	2
-4	9	1	4
13	-29	0	3

From the second last row, $29(-4) + 13(9) = 1$, or to match up with the order of the original equation, $13(9) + 29(-4) = 1$. Hence

$$[13]^{-1} = [9] \text{ in } \mathbb{Z}_{29}$$

We can check our work by substitution. $[13][9] = [117] = [1]$ in $\mathbb{Z}_{29}$.

Chapter 27

Fermat's Little Theorem

27.1 Objectives

The content objectives are:

1. State *Fermat's Little Theorem*.
2. Read a proof of Fermat's Little Theorem.
3. Read a proof to a corollary of Fermat's Little Theorem.
4. Discover a proof to the *Existence of Inverses in* $\mathbb{Z}_p$.

27.2 Fermat's Little Theorem

Pierre de Fermat proved a useful result called Fermat's Little Theorem. This should not be confused with one of the great conjectures, now theorem, of the last 400 years, Fermat's Last Theorem.

Theorem 1 **(Fermat's Little Theorem (FℓT))**

If p is a prime number that does not divide the integer a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Let's begin by understanding what the theorem is saying by using a numeric example.

Example 1 Suppose $p = 29$ and $a = 18$. Computing 18^{28} and reducing it modulo 29 is difficult without the aid of a computer. However, by Fermat's Little Theorem we know that

$$18^{28} \equiv 1 \pmod{29}$$

Take a minute to read the rather complicated proof.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. If $p \nmid a$, we first show that all of the integers
$$a, 2a, 3a, \ldots, (p-1)a$$
are all distinct modulo p.

2. Suppose that $ra \equiv sa \mod p$ where $1 \leq r < s \leq p-1$.

3. Since $\gcd(a, p) = 1$, Congruences and Division tells us that $r \equiv s \mod p$, but this is not possible when $1 \leq r < s \leq p-1$.

4. Because $a, 2a, 3a, \ldots, (p-1)a$ are all distinct mod p, it must be the case that these integers are equivalent to the integers $1, 2, 3, \ldots, p-1$ in some order.

5. Multiplying these integers together gives
$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod p$$

6. Since $\gcd(p, (p-1)!) = 1$, Congruences and Division (again) tells us that
$$a^{p-1} \equiv 1 \pmod p$$

□

Let's analyze the proof. As usual, we begin by identifying the hypothesis and the conclusion.

Hypothesis: p is a prime number. $p \nmid a$.

Conclusion: $a^{p-1} \equiv 1 \pmod p$

Analysis of Proof This is the most complicated proof in the course so far, so we will be very thorough. In fact, this proof contains a proof within a proof.

Sentence 1 *If $p \nmid a$, we first show that the integers $a, 2a, 3a, \ldots, (p-1)a$ are all distinct modulo p.*

The reason for this sentence is not at all obvious. The sentence is needed, but not until Sentence 4. The word *distinct* should alert us to a need to prove uniqueness.

Sentence 2 *Suppose that $ra \equiv sa \mod p$ where $1 \leq r < s \leq p-1$.*

The author treats Sentence 1 as a mini-proposition and begins a proof of the distinctness of the integers $a, 2a, 3a, \ldots, (p-1)a$. How? The author assumes that two of the integers, ra and sa with $r \neq s$, are the same modulo p and looks for a contradiction. The expression $1 \leq r < s \leq p-1$ is needed to make clear that ra and sa come from the integers under consideration, and that $r \neq s$. Since r and s are not the same, one is less than the other. Without any loss of generality, we can assume $r < s$.

Sentence 3 *Since* $\gcd(a, p) = 1$, *Congruences and Division tells us that* $r \equiv s \mod p$, *but this is not possible when* $1 \le r < s \le p - 1$.

The statement $\gcd(a, p) = 1$ is not one of the hypotheses. Where did it come from? Since p is a prime and $p \nmid a$, it must be the case that $\gcd(a, p) = 1$. It is always useful to identify where the hypotheses of a proposition are used in a proof. The hypotheses of Fermat's Little Theorem are used right here.

To invoke Congruences and Division, we must show that its hypotheses are satisfied. One of those hypotheses is $ra \equiv sa \mod p$. The other is $\gcd(a, p) = 1$. Invoking CD gives $r \equiv s \mod p$. But r and s are distinct, positive integers less than p, so this is not possible. This concludes the proof of distinctness of the integers $a, 2a, 3a, \ldots, (p-1)a$.

Sentence 4 *Because* $a, 2a, 3a, \ldots, (p-1)a$ *are all distinct mod* p, *it must be the case that these integers are equivalent to the integers* $1, 2, 3, \ldots, p-1$ *in some order.*

The set $\{a, 2a, 3a, \ldots, (p-1)a\}$ is a set of $p-1$ integers all distinct mod p. The set $\{1, 2, 3, \ldots, p-1\}$ is a set of $p-1$ integers all distinct mod p. Thus, the two sets must be the same modulo p.

Sentence 5 *Multiplying these integers together gives*

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$
$$(p-1)!a^{p-1} \equiv (p-1)! \pmod p$$

This is another sentence whose purpose is not yet clear.

Sentence 6 *Since* $\gcd(p, (p-1)!) = 1$, *Congruences and Division (again) tells us that* $a^{p-1} \equiv 1 \pmod p$.

The second of the congruences above is almost what we need. If we could divide out the $(p-1)!$ we would be done. But Congruences and Division allows us to do exactly that.

Now we examine two corollaries.

Corollary 2 For any integer a and any prime p

$$a^p \equiv a \pmod p$$

Proof: Let $a \in \mathbb{Z}$ and let p be a prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$. Multiplying both sides of the equivalence by a gives $a^p \equiv a \pmod p$. If $p \mid a$, then $a \equiv 0 \pmod p$ and $a^p \equiv 0 \pmod p$. Thus $a^p \equiv a \pmod p$. □

Let's make sure we understand the proof.

Analysis of Proof There are two important items to note: the use of nested quantifiers and the use of cases.

Sentence 1 *Let $a \in \mathbb{Z}$ and let p be a prime.*

The corollary begins with two universal quantifiers, so we use the Select Method twice, once for integers and once for primes.

Sentence 2 *If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

The author breaks up the proof into two parts depending on whether or not p divides a. The author will need two distinct cases because the approach differs based on the case. In the case where p does not divide a, the author uses Fermat's Little Theorem.

Sentence 3 *Multiplying both sides of the equivalence by a gives $a^p \equiv a \pmod{p}$.*

This is just modular arithmetic.

Sentence 4 *If $p \mid a$, then $a \equiv 0 \pmod{p}$ and $a^p \equiv 0 \pmod{p}$. Thus $a^p \equiv a \pmod{p}$.*

This is the second case where p does divide a. Both a^p and a are congruent to zero mod p so they are congruent to each other by the transitivity of the congruence relation.

Corollary 3 **(Existence of Inverses in $\mathbb{Z}_p$ (INV $\mathbb{Z}_p$))**

Let p be a prime number. If $[a]$ is any non-zero element in $\mathbb{Z}_p$, then there exists an element $[b] \in \mathbb{Z}_p$ so that $[a] \cdot [b] = [1]$

This corollary is equivalent to stating that every non-zero element of $\mathbb{Z}_p$ has an inverse. Let's discover a proof. As usual, we begin by identifying the hypothesis and the conclusion.

Hypothesis: p is a prime number. $[a]$ is any non-zero element in $\mathbb{Z}_p$.

Conclusion: There exists an element $[b] \in \mathbb{Z}_p$ so that $[a] \cdot [b] = [1]$.

Three points are salient. First, the corollary only states that an inverse exists. It doesn't tell us what the inverse is or how to compute the inverse. Second, there are three quantifiers.

1. *Let p be a prime number* is equivalent to *For all primes p*. Since this is an instance of a universal quantifier we would expect to use the Select Method.
2. $[a]$ is *any* non-zero element in $\mathbb{Z}_p$ is another instance of a universal quantifier so we would expect to use the Select Method again.
3. There is an existential quantifier in the conclusion so we would expect to use the Construct Method.

Together these give us the following.

Proof in Progress

1. Let p be a prime number.
2. Let $[a]$ be a non-zero element in $\mathbb{Z}_p$.
3. Construct $[b]$ as follows.
4. *To be completed.*

The third salient point is that this statement is a corollary of Fermat's Little Theorem. Now Fermat's Little Theorem uses congruences, not congruence classes. But we could restate Fermat's Little Theorem with congruence classes as

Theorem 4 **(Fermat's Little Theorem (FℓT))**

If p is a prime number that does not divide the integer a, then

$$[a^{p-1}] = [1] \text{ in } \mathbb{Z}_p$$

Now an analogy to real numbers provides the final step. In the reals $a^{p-1} = a \cdot a^{p-2}$ so why not let $[b] = [a^{p-2}]$? This would give

Proof in Progress

1. Let p be a prime number.
2. Let $[a]$ be a non-zero element in $\mathbb{Z}_p$.
3. Consider $[b] = [a^{p-2}]$.
4. *To be completed.*

Now we can invoke Fermat's Little Theorem but first we need to make sure the hypotheses are satisfied.

Proof in Progress

1. Let p be a prime number.
2. Let $[a]$ be a non-zero element in $\mathbb{Z}_p$.
3. Consider $[b] = [a^{p-2}]$.
4. Since $[a] \neq [0]$ in $\mathbb{Z}_p$, $p \nmid a$ and so by FℓT
$$[a][b] = [a][a^{p-2}] = [a^{p-1}] = [1]$$

A proof might look as follows.

Proof: Let p be a prime number. Let $[a]$ be a non-zero element in $\mathbb{Z}_p$. Consider $[b] = [a^{p-2}]$. Since $[a] \neq [0]$ in $\mathbb{Z}_p$, $p \nmid a$ and so by Fermat's Little Theorem

$$[a][b] = [a][a^{p-2}] = [a^{p-1}] = [1]$$

$\square$

REMARK

In summary, if p is a prime number and $[a]$ is any non-zero element in $\mathbb{Z}_p$, then

$$[a]^{-1} = [a^{p-2}]$$

Exercise 1 What is $[3]^{-1}$ in $\mathbb{Z}_7$?

27.3 More Examples

1. What is the remainder when 3141^{2001} is divided by 17?

   Solution: We are looking for an r that satisfies the Division Algorithm. That is

   $$3141^{2001} = 17q + r \text{ where } 0 \leq r < 17$$

   Reducing the above equation modulo 17 indicates that we must find r satisfying

   $$3141^{2001} \equiv r \pmod{17} \text{ where } 0 \leq r < 17$$

   Observe that

   $$3141 \equiv 13 \pmod{17}$$

   and that by Fermat's Little Theorem

   $$a^{16} \equiv 1 \pmod{17}$$

   when $17 \nmid a$. Putting all of this together gives

   $$3141^{2001} \equiv 13^{2001} \equiv 13^{125 \cdot 16+1} \equiv (13^{16})^{125} \cdot 13^1 \equiv 1^{16} \cdot 13 \equiv 13 \pmod{17}$$

27.4 Practice

1. (a) Prove that: if $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $ab \mid c$.

   (b) Show that the following statement is false. If $a \mid c$ and $b \mid c$, then $ab \mid c$.

   (c) Prove that: For all integers n, $21 \mid (3n^7 + 7n^3 + 11n)$.

Chapter 28

Chinese Remainder Theorem

28.1 Objectives

The content objectives are:

1. Do examples of solving simultaneous linear congruences.
2. Discover a proof of the *Chinese Remainder Theorem*.

28.2 An Old Problem

The following problem was posed, likely in the third century CE, by Sun Zi in his *Mathematical Manual* and republished in 1247 by Qin Jiushao in the *Mathematical Treatise in Nine Sections*.

> There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

The word problem asks us to find an integer n that simultaneously satisfies the following three linear congruences.

$$\begin{aligned} n &\equiv 2 \pmod 3 \\ n &\equiv 3 \pmod 5 \\ n &\equiv 2 \pmod 7 \end{aligned}$$

Before we solve this problem with three simultaneous linear congruences, we will begin with two simultaneous congruences whose moduli are coprime.

28.3 Chinese Remainder Theorem

Example 1 Solve

$$n \equiv 2 \pmod 5$$
$$n \equiv 9 \pmod{11}$$

Solution: The first congruence is equivalent to

$$n = 5x + 2 \text{ where } x \in \mathbb{Z} \tag{28.1}$$

Substituting this into the second congruence we get

$$5x + 2 \equiv 9 \pmod{11} \Rightarrow 5x \equiv 7 \pmod{11}$$

Have we seen anything like this before? Of course, this is just a linear congruence and we solved those in the previous chapter. Since $\gcd(5, 7) = 1$, there is exactly one solution modulo 11,

$$x \equiv 8 \pmod{11}$$

Now $x \equiv 8 \pmod{11}$ is equivalent to

$$x = 11y + 8 \text{ where } y \in \mathbb{Z} \tag{28.2}$$

Substituting Equation 28.2 into Equation 28.1 gives the solution

$$n = 5(11y + 8) + 2 = 55y + 42 \text{ for all } y \in \mathbb{Z}$$

which is equivalent to

$$n \equiv 42 \pmod{55}$$

We can check by substitution. If $n = 55y + 42$, then $n \equiv 2 \pmod 5$ and $n \equiv 9 \pmod{11}$.

We can formalize this process.

Theorem 1 **(Chinese Remainder Theorem (CRT))**

Let $a_1, a_2 \in \mathbb{Z}$. If $\gcd(m_1, m_2) = 1$, then the simultaneous linear congruences

$$n \equiv a_1 \pmod{m_1}$$
$$n \equiv a_2 \pmod{m_2}$$

have a unique solution modulo m_1m_2. Thus, if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv n_0 \pmod{m_1m_2}$$

Let's identify, as usual, the hypothesis and the conclusion.

Hypothesis: $a_1, a_2 \in \mathbb{Z}$. $\gcd(m_1, m_2) = 1$.

Conclusion: The simultaneous linear congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

have a unique solution modulo $m_1 m_2$.

Since there is an existential quantifier in the conclusion, we use the Construct Method and construct a solution. There is nothing obvious from the statement of the theorem that will help us, but we have already solved such a problem once in Example 1. Perhaps we could mimic what we did there.

From the first linear congruence

> The integer n satisfies $n \equiv a_1 \pmod{m_1}$ if and only if
>
> $$n = a_1 + m_1 x \qquad \text{for some } x \in \mathbb{Z}$$

The next thing we did was substitute this expression into the second congruence.

> The number n satisfies the second congruence if and only if
>
> $$\begin{aligned} a_1 + m_1 x &\equiv a_2 \pmod{m_2} \\ m_1 x &\equiv a_2 - a_1 \pmod{m_2} \end{aligned}$$

Have we seen anything like this before? Of course, this is just a linear congruence!

> Since $\gcd(m_1, m_2) = 1$, the Linear Congruence Theorem tells us that this congruence has a solution, say $x = b$ and that the complete solution is
>
> $$x = b + m_2 y \qquad \text{for all } y \in \mathbb{Z}$$
>
> Substituting this expression for x into $n = a_1 + m_1 x$ gives
>
> $$n = a_1 + m_1 x = a_1 + m_1(b + m_2 y) = (a_1 + m_1 b) + m_1 m_2 y$$
>
> where y can take any integer value. But this is just
>
> $$n \equiv a_1 + m_1 b \pmod{m_1 m_2}$$
>
> Since a_1, m_1 and b are all fixed integers, exactly one congruence class modulo $m_1 m_2$ is identified.

Since the solution to the pair of simultaneous linear congruences is unique modulo $m_1 m_2$, if we can find one solution, say n_0 then all solutions must be congruent to n_0 modulo $m_1 m_2$.

Exercise 1 Using the analysis above, write a proof for the Chinese Remainder Theorem.

Example 2 Solve

$$n \equiv 2 \pmod 3$$
$$n \equiv 3 \pmod 5$$

Solution: The first congruence is equivalent to

$$n = 3x + 2 \text{ where } x \in \mathbb{Z} \tag{28.3}$$

Substituting this into the second congruence we get

$$3x + 2 \equiv 3 \pmod 5 \Rightarrow 3x \equiv 1 \pmod 5$$

This linear congruence has the solution

$$x \equiv 2 \pmod 5$$

Now $x \equiv 2 \pmod 5$ is equivalent to

$$x = 5y + 2 \text{ where } y \in \mathbb{Z} \tag{28.4}$$

Substituting Equation (28.4) into Equation (28.3) gives the solution

$$n = 3(5y + 2) + 2 = 15y + 8 \text{ for all } y \in \mathbb{Z}$$

which is equivalent to

$$n \equiv 8 \pmod{15}$$

We can check by substitution. If $n = 15y + 8$, then $n \equiv 2 \pmod 3$ and $n \equiv 3 \pmod 5$.

Exercise 2 Solve

$$n \equiv 2 \pmod 3$$
$$n \equiv 3 \pmod 5$$
$$n \equiv 4 \pmod{11}$$

Solution: The first two of the three linear congruences were solved above so we can replace

$$n \equiv 2 \pmod 3$$
$$n \equiv 3 \pmod 5$$

by

$$n \equiv 8 \pmod{15}$$

This reduces a problem of three linear congruences to a problem in two linear congruences.

$$n \equiv 8 \pmod{15}$$
$$n \equiv 4 \pmod{11}$$

We leave the remainder of the exercise to the reader.

The exercises above make it clear that we can solve more than two simultaneous linear congruences simply by solving pairs of linear congruences successively. We record this as

Theorem 2 **(Generalized Chinese Remainder Theorem (GCRT))**

If $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, \ldots, a_k$, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}$$

You should ask yourself "What happens if the moduli are *not* coprime?" That investigation is left as an exercise.

Exercise 3 Solve the problem posed by Sun Zi that began this lecture.

28.4 More Examples

1. What is the complete solution to the following pair of simultaneous linear congruences?

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 5 \pmod{12} \end{aligned}$$

Solution: Since $\gcd(7, 12) = 1$, we know by the Chinese Remainder Theorem that a solution to this pair of linear congruences exists. Rewriting $x \equiv 3 \pmod 7$ as $x = 7y + 3$ (1) for $y \in \mathbb{Z}$ and substituting into the second linear congruence gives $7y + 3 \equiv 5 \pmod{12}$. This reduces to $7y \equiv 2 \pmod{12}$ and the solution is $y \equiv 2 \pmod{12}$. Rewriting $y \equiv 2 \pmod{12}$ as $y = 12z + 2$ for $z \in \mathbb{Z}$ and substituting in Equation 1 gives $x = 7(12z + 2) + 3 = 17 + 84z$ for $z \in \mathbb{Z}$, or, equivalently,

$$x \equiv 17 \pmod{84}$$

Check $17 \equiv 3 \pmod 7$ and $17 \equiv 5 \pmod{12}$.

2. Solve each of the following systems of equations.

(a) $\begin{aligned} x &\equiv 5 \pmod 9 \\ x &\equiv 3 \pmod 7 \end{aligned}$

Since $\gcd(7, 9) = 1$, we know by the Chinese Remainder Theorem that a solution to this pair of linear congruences exists. Rewriting $x \equiv 5 \pmod 9$ as $x = 9y + 5$

(1) for $y \in \mathbb{Z}$ and substituting into the second linear congruence gives $9y+5 \equiv 3 \pmod 7$. This reduces to $2y \equiv 5 \pmod 7$ and the solution is $y \equiv 6 \pmod 7$. Rewriting $y \equiv 6 \pmod 7$ as $y = 7z+6$ for $z \in \mathbb{Z}$ and substituting in Equation 1 gives $x = 9(7z+6)+5 = 59+63z$ for $z \in \mathbb{Z}$, or, equivalently,

$$x \equiv 63 \pmod{84}$$

Check $59 \equiv 5 \pmod 9$ and $59 \equiv 3 \pmod 7$.

(b) $$\begin{aligned} 3x &\equiv 2 \pmod 8 \\ 4x &\equiv 9 \pmod{11} \end{aligned}$$

This system of congruences is equivalent to $\begin{aligned} x &\equiv 6 \pmod 8 \\ x &\equiv 5 \pmod{11} \end{aligned}$

Since $\gcd(8,11) = 1$, we know by the Chinese Remainder Theorem that a solution to this pair of linear congruences exists. Rewriting $x \equiv 6 \pmod 8$ as $x = 8y+6$ (1) for $y \in \mathbb{Z}$ and substituting into the second linear congruence gives $8y+6 \equiv 5 \pmod{11}$. This reduces to $8y \equiv 10 \pmod{11}$ and the solution is $y \equiv 4 \pmod{11}$. Rewriting $y \equiv 4 \pmod{11}$ as $y = 11z+4$ for $z \in \mathbb{Z}$ and substituting in Equation 1 gives $x = 8(11z+4)+6 = 38+88z$ for $z \in \mathbb{Z}$, or, equivalently,

$$x \equiv 38 \pmod{88}$$

Check $3 \cdot 38 \equiv 114 \equiv 14 \cdot 8 + 2 \equiv 2 \pmod 8$ and $4 \cdot 38 \equiv 152 \equiv 13 \cdot 11 + 9 \equiv 9 \pmod{11}$.

(c) In $\mathbb{Z}_{11}$,

$$[2][x] + [7][y] = [4] \tag{28.5}$$
$$[3][x] + [2][y] = [9] \tag{28.6}$$

There are several ways to solve this. We will use elimination just as you would have used in high school. In $\mathbb{Z}_{11}$, [3] times equation (1) plus [2] times equation (2) gives

$$[17][y] = [-6] \Rightarrow [6][y] = [-6] \Rightarrow [y] = [-1] \Rightarrow [y] = [10]$$

Substituting $[y] = [10]$ into Equation (1) gives

$$[2][x] + [7][10] = [4] \Rightarrow [2][x] = [0] \Rightarrow [x] = [0]$$

Thus, the solution is $[x] = [0], [y] = [10]$.
Check

$$[2][x] + [7][y] = [2][0] + [7][10] = [70] = [4]$$
$$[3][x] + [2][y] = [3][0] + [2][10] = [20] = [9]$$

28.5 Splitting a Modulus

We may now prove the following theorem.

Theorem 3 **(Splitting Modulus (SM))**

Let p and q be coprime positive integers. Then for any two integers x and a,

$$\begin{cases} x \equiv a \pmod{p} \\ x \equiv a \pmod{q} \end{cases} \text{(simultaneously)} \iff x \equiv a \pmod{pq}.$$

Proof: Assuming $x \equiv a \pmod{pq}$, we get $pq \mid (x-a)$. By *Transitivity of Divisibility* (*TD*), we get $p \mid (x-a)$ and $q \mid (x-a)$. Therefore $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$.

On the other hand, starting with the simultaneous congruences $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$, since $\gcd(p,q) = 1$, we may use the *Chinese Remainder Theorem* (*CRT*) to get $x \equiv a \pmod{pq}$. □

28.6 Practice

1. Provide the complete solution for each of the following.

   (a)

$$\begin{aligned} x &\equiv 7 \pmod{11} \\ x &\equiv 5 \pmod{12} \end{aligned}$$

   (b)

$$\begin{aligned} 3x - 2 &\equiv 7 \pmod{11} \\ 5 &\equiv 4x - 1 \pmod{9} \end{aligned}$$

2. The Chinese Remainder Theorem deals with the case where the moduli are coprime. We now investigate what happens if the moduli are not coprime.

   (a) Consider the following two systems of linear congruences:

$$A : \begin{cases} n \equiv 2 \pmod{12} \\ n \equiv 10 \pmod{18} \end{cases} \qquad B : \begin{cases} n \equiv 5 \pmod{12} \\ n \equiv 11 \pmod{18} \end{cases}$$

   Determine which one has solutions and which one has no solutions. For the one with solutions, give the complete solutions to the system. For the one with no solutions, explain why no solutions exist.

   (b) Let a_1, a_2 be integers, and let m_1, m_2 be positive integers. Consider the following system of linear congruences

$$S : \begin{cases} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \end{cases}$$

   Using your observations in (a), complete the following two statements.
   The system S has a solution if and only if ____________________.
   (This blank needs to be filled with a simple condition on a_1, a_2, m_1, m_2.)
   If n_0 is a solution to S, then the complete solution is

$$n \equiv \underline{\hspace{4cm}}.$$

(c) Prove the first statement.

3. (a) Prove: If $\gcd(m_1, m_2) = 1$ then $x \equiv a \pmod{m_1 m_2}$ iff $x \equiv a \pmod{m_1}$ and $x \equiv a \pmod{m_2}$.

   (b) Let p be a prime number greater than 15. Determine the remainder of p^{360} divided by 1001.

4. Let a and n be positive integers. A sequence of n consecutive positive integers $(a, a+1, a+2, ..., a+(n-1))$ is called a **Wolczuk of length** n if every integer in the sequence is divisible by some perfect square greater than 1. For example, $(8, 9)$ is a Wolczuk of length 2 since $2^2 \mid 8$ and $3^2 \mid 9$.

   (a) Verify that $(48, 49, 50)$ is a Wolczuk of length 3.

   (b) Consider the system of linear congruences

$$\begin{aligned} a &\equiv 0 \pmod{4} \\ a &\equiv -1 \pmod{25} \\ a &\equiv -2 \pmod{49} \end{aligned}$$

   Solve this system and hence generate two distinct Wolczuks of length 3.

   (c) Prove that for any positive integer n, there exist infinitely many Wolczuks of length n.

Chapter 29

Practice, Practice, Practice: Congruences

29.1 Objectives

The content objectives are:

1. Computational practice.
2. Preparing for RSA.

29.2 Worked Examples

Let's recall how to solve linear congruences.

Example 1 Solve $13x \equiv 1 \pmod{60}$.

Solution: Since this is a linear congruence, we will use the Linear Congruence Theorem. Because $\gcd(13, 60) = 1$ and $1 \mid 1$ we would expect to find one congruence class mod 60 as a solution to $13x \equiv 1 \pmod{60}$. Now $13x \equiv 1 \pmod{60}$ is equivalent to the linear Diophantine equation $13x+60y = 1$ so we can use the EEA. (Note that we have interchanged the labels for x and y. Why?)

y	x	r	q
1	0	60	0
0	1	13	0
1	-4	8	4
-1	5	5	1
2	-9	3	1
-3	14	2	1
5	-23	1	1
-13	60	0	2

Thus $13(-23)+60(5) = 1$ and so $x \equiv -23 \equiv 37 \pmod{60}$ is a solution to $13x \equiv 1 \pmod{60}$.

Though we have efficient means to solve linear congruences, we have no equivalent means to solve polynomial congruences.

Example 2 Solve $x^2 \equiv 1 \pmod 8$ by substitution.

Your first reaction might be that there are zero, one or two solutions as there would be when working with real numbers.

Solution: We use a table to test all possible values of x.

$x \pmod 8$	0	1	2	3	4	5	6	7
$x^2 \pmod 8$	0	1	4	1	0	1	4	1

Hence, the solution is $x \equiv 1, 3, 5$ or $7 \pmod 8$.

Example 3 Solve $36x^{47} + 5x^9 + x^3 + x^2 + x + 1 \equiv 2 \pmod 5$. Reduce terms and use Fermat's Little Theorem or its corollaries before substitution.

Solution: Since $36 \equiv 1 \pmod 5$ the term $36x^{47}$ reduces to $x^{47} \pmod 5$.
Since $5 \equiv 0 \pmod 5$ the term $5x^9$ reduces to $0 \pmod 5$. Thus,

$$36x^{47} + 5x^9 + x^3 + x^2 + x + 1 \equiv 2 \pmod 5$$

reduces to

$$x^{47} + x^3 + x^2 + x + 1 \equiv 2 \pmod 5$$

Now observe that $x \equiv 0 \pmod 5$ cannot be a solution, otherwise we have $1 \equiv 2 \pmod 5$ by substitution in the preceding equation. Since 5 is a prime and $5 \nmid x$, we can use Fermat's Little Theorem which implies that $x^4 \equiv 1 \pmod 5$ and so

$$x^{47} \equiv x^{44}x^3 \equiv (x^4)^{11}x^3 \equiv 1^{11}x^3 \equiv x^3 \pmod 5$$

and the polynomial congruence further reduces to

$$x^3 + x^3 + x^2 + x + 1 \equiv 2 \pmod 5$$

or, more simply,

$$2x^3 + x^2 + x + 1 \equiv 2 \pmod 5$$

Now we can use a table.

$x \pmod 5$	0	1	2	3	4
$2x^3 + x^2 + x + 1 \pmod 5$	1	0	3	2	4

Hence, the only solution to

$$36x^{47} + 5x^9 + x^3 + x^2 + x + 1 \equiv 2 \pmod 5$$

is

$$x \equiv 3 \pmod 5$$

Example 4 Solve $n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{35}$.

Solution: We could try all 35 possibilities but even then, computing something like 20^{37} is a problem. Perhaps there is another way. Observing that $35 = 5 \times 7$ and both factors are relatively prime, maybe we could split the problem into two linear congruences and then apply the Chinese Remainder Theorem. Unfortunately, the polynomial is not linear. Let's see what happens anyway.

If n_0 is a solution to

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{35}$$

then n_0 is also a solution to

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{5} \tag{29.1}$$

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{7} \tag{29.2}$$

Well, have we seen anything like these before? Indeed, we have. The previous example solved congruences just like these. We'll solve each of the polynomial congruences individually. As in the previous example, we can reduce terms and use Fermat's Little Theorem or its corollaries to simplify the congruence before substitution. Let's start with Equation (29.1).

Since $10 \equiv 0 \pmod{5}$ the term $10n^8$ reduces to $0 \pmod{5}$.
Since $14 \equiv 4 \pmod{5}$ the term $14n^7$ reduces to $4n^7 \pmod{5}$.
Finally, since $5 \equiv 0 \pmod{5}$, the right hand side constant reduces to $0 \pmod{5}$.
Thus,

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{5}$$

reduces to

$$n^{37} + 4n^7 + 1 \equiv 0 \pmod{5}$$

This looks like progress! Now observe that $n_0 \equiv 0 \pmod{5}$ cannot be a solution, otherwise we have $1 \equiv 0 \pmod{5}$ by substitution in the preceding equation. Since 5 is a prime and $5 \nmid n_0$, we use Fermat's Little Theorem to get $n^4 \equiv 1 \pmod{5}$. Hence

$$n^{37} \equiv n^{36}n \equiv (n^4)^9 n \equiv 1^9 n \equiv n \pmod{5}$$

and

$$n^7 \equiv n^4 n^3 \equiv n^3 \pmod{5}$$

and so the polynomial congruence further reduces to

$$n + 4n^3 + 1 \equiv 0 \pmod{5}$$

Now we can use a table.

$n \pmod{5}$	0	1	2	3	4
$n + 4n^3 + 1 \pmod{5}$	1	1	0	2	1

Hence, the only solution to

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod 5$$

is

$$n \equiv 2 \pmod 5$$

This is a linear congruence so that supports the idea of using the Chinese Remainder Theorem. Now let's examine Equation (29.2) repeated below.

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod 7$$

Reducing each term modulo 7 gives

$$n^{37} + 3n^8 + 1 \equiv 5 \pmod 7$$

Since $n_0 \equiv 0 \pmod 7$ cannot be a solution, otherwise $1 \equiv 5 \pmod 7$, and 7 is a prime, we can use Fermat's Little Theorem to assert $n^6 \equiv 1 \pmod 7$. This allows us to say

$$n^{37} \equiv n^{36}n \equiv (n^6)^6 n \equiv 1^6 n \equiv n \pmod 7$$

and

$$n^8 \equiv n^6 n^2 \equiv n^2 \pmod 7$$

Thus, Equation (29.2) reduces to

$$n + 3n^2 + 1 \equiv 5 \pmod 7$$

This is a good time to use a table.

$n \pmod 7$	0	1	2	3	4	5	6
$n + 3n^2 + 1 \pmod 7$	1	5	1	3	4	4	3

Hence, the only solution to

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod 7$$

is

$$n \equiv 1 \pmod 7$$

But now we have two simultaneous linear congruences

$$n \equiv 2 \pmod 5$$
$$n \equiv 1 \pmod 7$$

Since the moduli are coprime, we know by the Chinese Remainder Theorem that a solution exists. The proof of CRT gave us a way to solve two simultaneous linear congruences.

The first congruence is equivalent to

$$n = 5x + 2 \text{ where } x \in \mathbb{Z} \tag{29.3}$$

Substituting this into the second congruence we get

$$5x + 2 \equiv 1 \pmod 7 \Rightarrow 5x \equiv 6 \pmod 7$$

Solving this linear congruence gives

$$x \equiv 4 \pmod 7$$

Now $x \equiv 4 \pmod 7$ is equivalent to

$$x = 7y + 4 \text{ where } y \in \mathbb{Z} \tag{29.4}$$

Substituting Equation (29.4) into Equation (29.3) gives the solution

$$n = 5(7y+4) + 2 = 35y + 22 \text{ for all } y \in \mathbb{Z}$$

which is equivalent to

$$n \equiv 22 \pmod{35}$$

Thus, the solution to

$$n^{37} + 10n^8 + 14n^7 + 1 \equiv 5 \pmod{35}$$

is

$$n \equiv 22 \pmod{35}$$

Example 5 Solve $n^3 \equiv 127 \pmod{165}$.

Solution: We could try all 165 possibilities but perhaps it is better to follow the lead of the previous question. Observing that $165 = 3 \times 5 \times 11$ and all three factors are relatively prime as pairs, maybe we can split the problem into three linear congruences and then apply the Chinese Remainder Theorem.

If n_0 is a solution to

$$n^3 \equiv 127 \pmod{165}$$

then n_0 is a solution to

$$\begin{aligned} n^3 &\equiv 127 \equiv 1 \pmod 3 \\ n^3 &\equiv 127 \equiv 2 \pmod 5 \\ n^3 &\equiv 127 \equiv 6 \pmod{11} \end{aligned}$$

Let's consider each of the three congruences separately. In the case $n^3 \equiv 1 \pmod 3$ we can use a corollary to Fermat's Little Theorem. Since $n^3 \equiv n \pmod 3$ by Fermat's Little Theorem, $n^3 \equiv 1 \pmod 3$ reduces to $n \equiv 1 \pmod 3$ which is just the solution to the first congruence.

For the case $n^3 \equiv 2 \pmod 5$ we will use a table.

$n \pmod 5$	0	1	2	3	4
$n^3 \pmod 5$	0	1	3	2	4

The only solution to $n^3 \equiv 2 \pmod 5$ is $n \equiv 3 \pmod 5$

For the case $n^3 \equiv 6 \pmod{11}$ we will again use a table.

$n \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$n^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

The only solution to $n^3 \equiv 6 \pmod{11}$ is $n \equiv 8 \pmod{11}$

Hence, a solution to $n^3 \equiv 127 \pmod{165}$ can be found by solving the simultaneous linear congruences

$$\begin{aligned} n &\equiv 1 \pmod{3} \\ n &\equiv 3 \pmod{5} \\ n &\equiv 8 \pmod{11} \end{aligned}$$

Though these could be solved by eye (note that $n \equiv 8 \pmod{55}$ is a solution to the last two) we will solve these, for practice, by writing out and substituting equations.

From $n \equiv 1 \pmod{3}$ we have

$$n = 3x + 1 \text{ where } x \in \mathbb{Z} \tag{29.5}$$

Substituting into the second congruence we get

$$3x + 1 \equiv 3 \pmod{5} \Rightarrow 3x \equiv 2 \pmod{5} \Rightarrow x \equiv 4 \pmod{5}$$

Now $x \equiv 4 \pmod{5}$ is equivalent to

$$x = 5y + 4 \text{ where } y \in \mathbb{Z} \tag{29.6}$$

Substituting Equation (29.6) into Equation (29.5) gives the solution to the first two linear congruences.

$$n = 3(5y + 4) + 1 = 15y + 13 \text{ for all } y \in \mathbb{Z}$$

which is equivalent to

$$n \equiv 13 \pmod{15}$$

Now we need to solve

$$\begin{aligned} n &\equiv 13 \pmod{15} \\ n &\equiv 8 \pmod{11} \end{aligned}$$

From $n \equiv 13 \pmod{15}$ we have

$$n = 15x + 13 \text{ where } x \in \mathbb{Z} \tag{29.7}$$

Substituting into the second congruence we get

$$15x+13 \equiv 8 \pmod{11} \Rightarrow 4x+2 \equiv 8 \pmod{11} \Rightarrow 4x \equiv 6 \pmod{11} \Rightarrow x \equiv 7 \pmod{11}$$

Now $x \equiv 7 \pmod{11}$ is equivalent to

$$x = 11y + 7 \text{ where } y \in \mathbb{Z} \tag{29.8}$$

Substituting Equation (29.8) into Equation (29.7) gives the solution.

$$n = 15(11y + 7) + 13 = 165y + 118 \text{ for all } y \in \mathbb{Z}$$

which is equivalent to

$$n \equiv 118 \pmod{165}$$

and this is the solution to the original problem $n^3 \equiv 127 \pmod{165}$.

Checking we have $n^2 \equiv 118^2 \equiv 64 \pmod{165}$ and $n^3 \equiv n^2 \cdot n \equiv 64 \times 118 \equiv 127 \pmod{165}$.

REMARK

Let's summarize what we have learned from these examples.

- By the Linear Congruence Theorem, all linear congruences can be solved.
- There is no efficient means to solving a polynomial congruence. Substitution always works but can be very slow.
- Polynomial congruences may have many solutions.
- One approach that sometimes works when the modulus is composite, is to break the problem into parts, solve each of the parts, and then combine the partial solutions to get a complete solution. Specifically,
  1. Create a new polynomial congruence for each prime factor of the modulus.
  2. Solve each of these new polynomial congruences by reducing coefficients, applying Fermat's Little Theorem to reduce exponents (which is why we need to use *prime* factors), and then using observation, the Linear Congruence Theorem or a table of values.
  3. If the original problem has a solution, this process will give at least one linear congruence for each factor. Use the Chinese Remainder Theorem to combine these solutions into a solution for the original problem.

Example 6 Determine, with justification, all solutions of the congruence equation

$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{77}$$

Solution: We break the problem into parts, solve each of the parts, and then combine the partial solutions to get a complete solution.

Observe that if x_0 is a solution to

$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{77}$$

then x_0 is also a solution to

$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{7} \tag{29.9}$$

$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{11} \tag{29.10}$$

We begin with the polynomial congruence (29.9)

$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{7}$$

and reduce each term modulo 7. This gives

$$x^{91} + 4x^{31} + x \equiv 1 \pmod{7}$$

Since 7 is prime, as long as $7 \nmid x_0$, we can use Fermat's Little Theorem which implies that

$$x^{6} \equiv 1 \pmod{7}$$

So then
$$x^{91} \equiv x^{90}x^1 \equiv (x^{15})^6 x^1 \equiv 1^{15}x^1 \equiv x \pmod 7$$
Similarly, $x^{31} \equiv x \pmod 7$ and so the congruence (29.9) reduces to
$$x + 4x + x \equiv 1 \pmod 7$$
or
$$6x \equiv 1 \pmod 7$$
Solving this linear congruence gives
$$x \equiv 6 \pmod 7$$
We still have to deal with the possibility that $7 \mid x_0$. If 7 did divide x_0, then $x_0 \equiv 0 \pmod 7$ would be a solution to
$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod 7$$
Substituting 0 for x in the above equation gives $0 \equiv 1 \pmod 7$ which is false. So $7 \nmid x_0$. Similarly,
$$x^{91} + 77x^{51} + 11x^{31} + x \equiv 1 \pmod{11}$$
reduces to
$$2x \equiv 1 \pmod{11}$$
Solving this linear congruence gives
$$x \equiv 6 \pmod{11}$$
Note again that $11 \nmid x_0$.

But now we have two simultaneous linear congruences
$$x \equiv 6 \pmod 7$$
$$x \equiv 6 \pmod{11}$$
The integer 6 is an obvious elution to both congruences so by the Chinese Remainder Theorem
$$x \equiv 6 \pmod{77}$$

29.3 Quiz

Example 7 (20 marks) Determine, with justification, all solutions of the congruence equation

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{143}$$

Solution: We break the problem into parts, solve each of the parts, and then combine the partial solutions to get a complete solution.

Observe that if x_0 is a solution to

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{143}$$

then x_0 is also a solution to

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{11}\checkmark \tag{29.11}$$

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{13}\checkmark \tag{29.12}$$

We begin with the polynomial congruence (29.11)

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{11}$$

and reduce each term modulo 11. This gives

$$x^{61} + 4x^{41} + 5 \equiv 0 \pmod{11}\checkmark$$

Since 11 is prime $\checkmark$, as long as $11 \nmid x_0$ $\checkmark$, we can use Fermat's Little Theorem $\checkmark$which implies that

$$x^{10} \equiv 1 \pmod{11}\checkmark$$

So then

$$x^{61} \equiv x^{60}x^1 \equiv (x^{10})^6x^1 \equiv 1^6x^1 \equiv x \pmod{11}\checkmark$$

Similarly, $x^{41} \equiv x \pmod{11}$ and so the congruence reduces to

$$x + 4x + 5 \equiv 0 \pmod{11}\checkmark$$

or

$$5x \equiv -5 \pmod{11}$$

By Congruences and Division

$$x \equiv -1 \equiv 10 \pmod{11}\checkmark$$

We still have to deal with the possibility that $11 \mid x_0$. If 11 did divide x_0, then $x_0 \equiv 0 \pmod{11}$ would be a solution to

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{11}$$

Substituting 0 for x in the above equation gives $5 \equiv 0 \pmod{11}$ which is false $\checkmark$. So $11 \nmid x_0$. Similarly,

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{13}$$

reduces to

$$12x + 5 \equiv 0 \pmod{13}\checkmark$$

or, since $12 \equiv -1 \pmod{13}$

$$-x \equiv -5 \pmod{13}$$

which has the solution

$$x \equiv 5 \pmod{13}\checkmark$$

Note again that $13 \nmid x_0$.

But now we have two simultaneous linear congruences

$$x \equiv 10 \pmod{11}$$
$$x \equiv 5 \pmod{13}$$

The first congruence is equivalent to

$$x = 11y + 10 \text{ where } y \in \mathbb{Z}\checkmark \tag{29.13}$$

Substituting this into the second congruence we get

$$11y + 10 \equiv 5 \pmod{13} \Rightarrow 11y \equiv 8 \pmod{13}\checkmark$$

Solving this linear congruence gives

$$y \equiv 9 \pmod{13}\checkmark$$

Now $y \equiv 9 \pmod{13}$ is equivalent to

$$y = 13z + 9 \text{ where } z \in \mathbb{Z}\checkmark \tag{29.14}$$

Substituting Equation (29.14) into Equation (29.13) gives the solution

$$x = 11(13z + 9) + 10 = 109 + 143z \text{ for all } z \in \mathbb{Z}\checkmark$$

which is equivalent to

$$x \equiv 109 \pmod{143}\checkmark$$

Thus, the solution to ✓

$$x^{61} + 26x^{41} + 11x^{25} + 5 \equiv 0 \pmod{13}$$

is

$$x \equiv 109 \pmod{143}$$

29.4 Preparing for RSA

This exercise will help us understand the implementation of the RSA scheme which we will look at next. In commercial practice the numbers chosen are large but here, choose numbers small enough to work with by hand.

I will give an example. You follow along but use your own numbers.

1. Choose two distinct primes p and q and let $n = pq$. I will choose $p = 7$ and $q = 11$ so $n = 77$.

2. Select an integer e so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$. I will choose $e = 13$ which satisfies $\gcd(13, 60) = 1$ and $1 < 13 < 60$.

3. Solve
$$ed \equiv 1 \pmod{(p-1)(q-1)}$$
for an integer d where $1 < d < (p-1)(q-1)$. In my case, I must solve
$$13d \equiv 1 \pmod{60}$$
The solution is $d = 37$.

Chapter 30

The RSA Scheme

30.1 Objectives

The content objectives are:

1. Illustrate the use of RSA.
2. Prove that the message sent will be the message received.

30.2 Public Key Cryptography

The need for secret communications has been known for millenia. In the modern world, the need for secret communication is much larger than it was even in the recent past. Certainly the traditional requirements of military and diplomatic secrecy continue, but the credit card, debit card and web transactions of modern commerce, as well as privacy concerns for health, citizenship and other electronic records, have raised the need for secure communications and storage dramatically.

In its most elemental form, the objective of any secret communication scheme is to allow two parties, usually referred to as Alice (for person A) and Bob (for person B), to communicate over an insecure channel so that an opponent, often called Oscar, cannot understand what is being communicated. The information Alice wishes to communicate is called the **message** or the **plaintext**. The act of transforming the plaintext into a **ciphertext** is called **enciphering** or **encryption**. The rules for enciphering make use of a **key**, which is an input to the algorithm. The act of transforming the ciphertext to plaintext using the key is called **deciphering** or **decryption**.

Alice and Bob both must share some secret key to be able communicate using cryptography. This raises the problem of how to distribute a large number of keys between users, especially if these keys need to be changed frequently. For example, there are almost 200 countries in the world. If Canada maintains an embassy in each country and allows Canadian embassies to communicate with one another, the embassies must exchange a common key between each pair of embassies. That means there are $\binom{200}{2} = 19,900$ keys to exchange. Worse yet, for security reasons, keys should be changed frequently and so $19,900$ keys might need to be exchanged daily.

The possibility of public key cryptography was first published in 1976 in a paper by Diffie, Hellman and Merkle. The RSA scheme, named after its discoverers Rivest, Shamir and Adleman is an example of a commercially implemented public key scheme.

In a public key cryptographic scheme, keys are divided into two parts: a private decryption key held secretly by each participant, and a public encryption key, derived from the private key, which is shared in an open repository of some sort. For user A to send a private message to user B, A would look up B's public key, encrypt the message and send it to B. Since B is the only person who possesses the secret key required for decryption, only B can read the message.

Such an arrangement solves the key distribution problem. The public keys do not need to be kept secret and only one per participant needs to be available. Thus, in our embassy example previously, only 200 keys need to be published.

RSA is now widely deployed. The following protocols and products, which embed RSA, are used by many of us daily. SSL (Secure Sockets Layer) is the most commonly used protocol for secure communication over the web. It is frequently used to encrypt payment data before sending that data to a server. PGP (Pretty Good Privacy) is used by individuals and businesses to encrypt and authenticate messages. It was originally intended for email messages and attachments but is now also used for encrypting files, folders or entire hard drives. EMV (Europay, MasterCard and VISA) is a global standard for authenticating credit and debit card transactions at point of sale (POS) or automated teller machines (ATM).

In the next section, we will introduce the RSA scheme and then prove that it works. The security of the RSA scheme is a widely studied subject, but we will not address that here.

30.3 Implementing RSA

In RSA, messages are integers. How does one get an integer from plaintext? In much the same way we did with a Vigenère cipher, assign a number to each letter of the alphabet and then concatenate the digits together.

30.3.1 Setting up RSA

1. Choose two large, distinct primes p and q and let $n = pq$.
2. Select an integer e so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.
3. Solve
$$ed \equiv 1 \pmod{(p-1)(q-1)}$$
for an integer d where $1 < d < (p-1)(q-1)$.
4. Publish the public encryption key (e, n).
5. Keep secure the private decryption key (d, n).

30.3.2 Sending a Message

To send a message:

1. Look up the recipient's public key (e, n).
2. Generate the integer message M so that $0 \leq M < n$.
3. Compute the ciphertext C as follows:
$$M^e \equiv C \pmod{n} \text{ where } 0 \leq C < n$$
4. Send C.

30.3.3 Receiving a Message

To decrypt a message:

1. Use your private key (d, n).
2. Compute the messagetext R from the ciphertext C as follows:
$$C^d \equiv R \pmod{n} \text{ where } 0 \leq R < n$$
3. R is the original message.

30.3.4 Example

All of the computation in this part was done in Maple.

Setting up RSA

1. Choose two large, distinct primes p and q and let $n = pq$.
   Let p be
   `9026694843 0929817462 4847943076 6619417461`
   `5791443937,`
   and let q be
   `7138718791 1693596343 0802517103 2405888327`
   `6844736583`
   so n is
   `6443903609 8539423089 8003779070 0502485677`
   `1034536315 4526254586 6290164606 1990955188`
   `1922989980 3977447271.`

2. Select an integer e so that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.
   Now $(p-1)(q-1)$ is
   `6443903609 8539423089 8003779070 0502485677`
   `1034536313 8360840952 3666750800 6340495008`
   `2897684191 1341266752.`

   Choose e as
   `9573596212 0300597326 2950869579 7174556955`
   `8757345310 2344121731.`
   It is indeed the case that $\gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.

3. Solve
   $$ed \equiv 1 \pmod{(p-1)(q-1)}$$
   for an integer d where $1 < d < (p-1)(q-1)$. Solving this LDE gives d as
   `5587652122 6351022927 9795248536 5522717791`
   `7285682675 6100082011 1849030646 3274981250`
   `2583120946 4072548779.`

4. Publish the public encryption key (e, n).

5. Keep secure the private decryption key (d, n).

Sending a Message

To send a message:

1. Look up the recipient's public key (e, n).

2. Generate the integer message M so that $0 \leq M < n$.
   We will let $M = 3141592653$.

3. Compute the ciphertext C as follows:

$$M^e \equiv C \pmod{n} \text{ where } 0 \le C < n$$

Computing gives C
`4006696554 3080815610 2814019838 8509626485`
`8151054441 5245547382 5506759308 1333888622`
`4491394825 3742205367.`

4. Send C.

Receiving a Message

To decrypt a message:

1. Use your private key key (d, n).
2. Compute the messagetext R from the ciphertext C as follows:

$$C^d \equiv R \pmod{n} \text{ where } 0 \le R < n$$

3. R is the original message.
$R = 3141592653$.

30.3.5 RSA calculations without using computers

When the value of n is small and can be easily factored into $n = pq$ for distinct primes p and q, we can carry out the calculations without using computers. For this, we need to recall the theorem about splitting a congruence modulo n into multiple simultaneous congruences using the factors of n.

Theorem 1 **(Splitting Modulus (SM))**

Let p and q be coprime positive integers. Then for any two integers x and a,

$$\begin{cases} x \equiv a \pmod{p} \\ x \equiv a \pmod{q} \end{cases} \text{(simultaneously)} \iff x \equiv a \pmod{pq}.$$

Even though the end results of an RSA calculation is presented modulo n, the *Splitting Modulus* (SM) theorem allows us to carry out the intermediate work in $\pmod{p}$ and in $\pmod{q}$ separately, and combine the results using the *Chinese Remainder Theorem* (CRT) to get the final answer in $\pmod{n}$.

The advantage of using p and q is that these numbers are prime, so we can use *Fermat's litte Theorem* $(F\ell T)$ and its corollaries in $\bmod p$ and $\bmod q$.

Example 1 Let us carry out some RSA calculations.

1. Given $p = 5$, and $q = 11$, and $e = 3$, find the private key (dn) for an RSA scheme.

   Solution: In this case, $n = 5 \times 11 = 55$ and $(p-1)(q-1) = 4 \times 10 = 40$. To find d, we solve
   $$3d \equiv 1 \pmod{40}.$$

   Set up the Linear Diophantine Equation
   $$40x + 3d = 1$$
   and use the *Extended Euclidean Algorithm* table

x	y	r	q	Division Algorithm
1	0	40	0	$40 = 0(3) + 40$
0	1	3	0	$23 = 0(40) + 3$
1	-13	1	13	$40 = 13(3) + 1$

   So so our solution for d is
   $$d \equiv -13 \pmod{40}.$$

   How many solutions do we expect for d? Since $\gcd(3, 40) = 1$, by *Linear Congruence Theorem* (LCT), there is only one solution modulo 40.

   As d must satisfy $1 < d < 40$, the answer is $d = (40 - 13) = 27$.

   Note that we could have solved for d simply from the observation that $3 \times 27 = 81$, which leaves a remainder of 1 when divided by 40.

   The private key is the pair $(d, n) = (27, 55)$ (and not just d).

2. Suppose you receive the cipher-text $C = 47$. Decrypt the message using your private key $(27, 55)$.

   Solution: So we will compute
   $$R = (47)^{27} \pmod{55}.$$

   The *Splitting Modulus* (SM) theorem allows us to instead solve the simultaneous congruences
   $$R \equiv (47)^{27} \pmod{5}$$
   $$\text{and } R \equiv (47)^{27} \pmod{11}.$$

   We know $47 \equiv 2 \pmod{5}$ and $47 \equiv 4 \pmod{11}$, which provides us with slightly simpler congruences
   $$R \equiv 2^{27} \pmod{5}$$
   $$\text{and } R \equiv 3^{27} \pmod{11}.$$

   Since 5 and 11 are both prime numbers, we may now use *Fermat's litte Theorem* $(F\ell T)$, which tells us $2^4 \equiv 1 \pmod{5}$ and $3^{10} \equiv 1 \pmod{11}$.

Using $27 = (6)(4) + 3$, we get $R \equiv (2^4)^6 2^3 \equiv 2^3 \equiv 8 \equiv 3 \pmod 5$. Similarly, from $27 = 2(10) + 7$, we get that $R \equiv (3^{10})^2(3)^7 \equiv (3^7) \equiv 9 \pmod{11}$. Finally, we have to solve

$$\begin{aligned} R &\equiv 3 \pmod 5 \\ \text{and } R &\equiv 9 \pmod{11}. \end{aligned}$$

Solving simultaneous congruences like this should become second nature to you by now. The end result is that $R = 53$.

30.4 Does $M = R$?

Are we confident that the message sent is the message received?

Theorem 2 **(RSA)**

If

1. p and q are distinct primes,
2. $n = pq$
3. e and d are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$,
4. $0 \le M < n$
5. $M^e \equiv C \pmod n$
6. $C^d \equiv R \pmod n$ where $0 \le R < n$

then $R = M$.

The proof is long and can appear intimidating but, in fact, it is structurally straightforward if we break it into pieces. The proof is done in four parts.

1. Write R as a function of M, specifically
$$R \equiv MM^{k(p-1)(q-1)} \pmod n$$
2. Show that $R \equiv M \pmod p$. We will do this in two cases: (i) $p \nmid M$ and (ii) $p \mid M$.
3. Show that $R \equiv M \pmod q$.
4. Use the Chinese Remainder Theorem to deduce that $R = M$.

Proof: First, we will show that

$$R \equiv MM^{k(p-1)(q-1)} \pmod n$$

Since $ed \equiv 1 \pmod{(p-1)(q-1)}$, there exists an integer k so that

$$ed = 1 + k(p-1)(q-1)$$

Now

$$\begin{aligned} R &\equiv C^d \pmod{n} \\ &\equiv (M^e)^d \pmod{n} \\ &\equiv M^{ed} \pmod{n} \\ &\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\ &\equiv MM^{k(p-1)(q-1)} \pmod{n} \end{aligned}$$

Second, we will show that $R \equiv M \pmod{p}$. Suppose that $p \nmid M$. By Fermat's Little Theorem,

$$M^{p-1} \equiv 1 \pmod{p}$$

Hence

$$\begin{aligned} M^{k(p-1)(q-1)} &\equiv (M^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv 1^{k(q-1)} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

Multiplying both sides by M gives

$$MM^{k(p-1)(q-1)} \equiv M \pmod{p}$$

Since

$$R \equiv MM^{k(p-1)(q-1)} \pmod{n} \Rightarrow R \equiv MM^{k(p-1)(q-1)} \pmod{p}$$

we have

$$R \equiv M \pmod{p}$$

Now suppose that $p \mid M$. But then $M \equiv 0 \pmod{p}$ and so $MM^{k(p-1)(q-1)} \equiv 0 \pmod{p}$. That is,

$$MM^{k(p-1)(q-1)} \equiv M \pmod{p}$$

Again, since

$$R \equiv MM^{k(p-1)(q-1)} \pmod{n} \Rightarrow R \equiv MM^{k(p-1)(q-1)} \pmod{p}$$

we have

$$R \equiv M \pmod{p}$$

In either case, we have $R \equiv M \pmod{p}$.

Third, we will show that $R \equiv M \pmod{q}$. But this is very similar to $R \equiv M \pmod{p}$.

Fourth and last, we will show that $R = M$. So far we have generated two linear congruences that have to be satisfied simultaneously.

$$\begin{aligned} R &\equiv M \pmod{p} \\ R &\equiv M \pmod{q} \end{aligned}$$

Since $\gcd(p, q) = 1$ we can invoke the Chinese Remainder Theorem and conclude that

$$R \equiv M \pmod{pq}$$

Since $pq = n$ we have

$$R \equiv M \pmod{n}$$

Now, R and M are both integers congruent to each other modulo n, and both lie between 0 and $n - 1$, so $R = M$. $\square$

Part V

Complex Numbers and Euler's Formula

Chapter 31

Complex Numbers

31.1 Objectives

The content objectives are :

1. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. Define: *complex number*, $\mathbb{C}$, *real part*, *imaginary part*
3. Operations: *complex addition*, *complex multiplication*, *equality of complex numbers*
4. State and prove properties of complex numbers.

31.2 Different Equations Require Different Number Systems

When humans first counted, we tallied. We literally made notches on sticks, stones and bones. Thus the natural numbers, $\mathbb{N}$, were born. But it wouldn't be long before the necessity of fractions became obvious. One animal to be shared by four people (we will assume uniformly) meant that we had to develop the notion of 1/4. Though it would not have been expressed this way, the equation

$$4x = 1$$

does not have a solution in $\mathbb{N}$ and so we would have had to extend our notion of numbers to include fractions, the rationals.

$$\mathbb{Q} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0 \right\}$$

This is an overstatement historically, because recognition of zero and negative numbers which are permitted in $\mathbb{Q}$ were very slow to come. But even these new numbers would not help solve equations of the form

$$x^2 = 2$$

which would arise naturally from isosceles right angled triangles. For this, the notion of number had to be extended to include irrational numbers, which combined with the rationals, give us the real numbers.

Eventually, via Hindu and Islamic scholars, western mathematics began to recognize and accept both zero and negative numbers. Otherwise, equations like

$$3x = 5x$$

or

$$2x + 4 = 0$$

have no solution. Thus, mathematicians recognized that

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

but even $\mathbb{R}$ was inadequate because equations of the form

$$x^2 + 1 = 0$$

had no real solutions.

And so, our number system was extended again.

31.3 Complex Numbers

Definition 31.3.1
Complex Number

A **complex number** z in **standard form** is an expression of the form $x+yi$ where $x, y \in \mathbb{R}$. The set of all complex numbers is denoted by

$$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$$

Example 1

Some examples are $3 + 4i$, $0 + 5i$ (usually written $5i$), $7 - 0i$ (usually written 7) and $0 + 0i$ (usually written 0).

Definition 31.3.2
Real Part, Imaginary Part

For a complex number $z = x + yi$, the real number x is called the **real part** and is written $\Re(z)$ and the real number y is called the **imaginary part** and is written $\Im(z)$.

So $\Re(3+4i) = 3$ and $\Im(3+4i) = 4$. If z is a complex number where $\Im(z) = 0$, we will treat z as a real number and we will not write the term containing i. For example, $z = 3 + 0i$ will be treated as a real number and will be written $z = 3$. Thus

$$\mathbb{R} \subset \mathbb{C}$$

and so

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

One has to wonder how much further the number system needs to be extended!

Definition 31.3.3
Equality

The complex numbers $z = x + yi$ and $w = u + vi$ are **equal** if and only if $x = u$ and $y = v$.

Definition 31.3.4
Addition

Addition is defined as

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

Example 2

$$(1 + 7i) + (2 - 3i) = (1 + 2) + (7 - 3)i = 3 + 4i$$

Definition 31.3.5
Multiplication

Multiplication is defined as

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + cb)i$$

Example 3

Let's begin with what is really the defining property of $\mathbb{C}$.

$$i \cdot i = (0 + 1i) \cdot (0 + 1i) = (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 0 \cdot 1)i = -1$$

This property that $i^2 = -1$ is what gives complex numbers their strangeness and their strength. In the next example, note that the definition of multiplication coincides exactly with the usual binomial multiplication where i^2 is replaced by -1.

$$(1 + 7i) \cdot (2 - 3i) = (1 \cdot 2 - 7 \cdot (-3)) + (1 \cdot (-3) + 7 \cdot 2)i = 23 + 11i$$

The multiplication symbol is usually omitted and we write zw or $(a + bi)(c + di)$.

Exercise 1

Let $u = 3 + i$ and $v = 2 - 7i$. Compute

1. $u + v$
2. $u - v$
3. uv
4. u^2v
5. u^3
6. $\dfrac{v}{u}$ (write the solution in the form $x + yi$ where $x, y \in \mathbb{R}$)

Solution:

1. $u + v = (3 + i) + (2 - 7i) = 5 - 6i$
2. $u - v = (3 + i) - (2 - 7i) = 1 + 8i$
3. $uv = (3 + i)(2 - 7i) = (6 - (-7)) + (-21 + 2)i = 13 - 19i$
4. $u^2v = (3 + i)^2(2 - 7i) = (3 + i)((3 + i)(2 - 7i)) = (3 + i)(13 - 19i) = 58 - 44i$

5. $u^3 = (3+i)^3 = (3+i)^2(3+i) = (8+6i)(3+i) = 18+26i$

6. $$\frac{v}{u} = \frac{2-7i}{3+i} = \frac{2-7i}{3+i} \cdot \frac{3-i}{3-i} = \frac{-1-23i}{10} = \frac{-1}{10} + \frac{-23}{10}i$$

Exercise 2 Compute

1. i^{4k} for any non-negative integer k
2. i^{4k+1} for any non-negative integer k
3. i^{4k+2} for any non-negative integer k
4. i^{4k+3} for any non-negative integer k

Solution:

1. $i^{4k} = 1$ for any non-negative integer k
2. $i^{4k+1} = i$ for any non-negative integer k
3. $i^{4k+2} = -1$ for any non-negative integer k
4. $i^{4k+3} = -i$ for any non-negative integer k

The usual properties of associativity, commutativity, identities, inverses and distributivity that we associate with rational and real numbers also apply to complex numbers.

Proposition 1 Let $u, v, z \in \mathbb{C}$. Then

1. Associativity of addition: $(u+v)+z = u+(v+z)$
2. Commutativity of addition: $u+v = v+u$
3. Additive identity: $0 = 0+0i$ has the property that $z+0 = z$
4. Additive inverses: If $z = x+yi$ then there exists an *additive inverse* of z, written $-z$ with the property that $z+(-z) = 0$. The additive inverse of $z = x+yi$ is $-z = -x-yi$.
5. Associativity of multiplication: $(u \cdot v) \cdot z = u \cdot (v \cdot z)$
6. Commutativity of multiplication: $u \cdot v = v \cdot u$
7. Multiplicative identity: $1 = 1+0i$ has the property that $z \cdot 1 = z$.
8. Multiplicative inverses: If $z = x+yi \neq 0$ then there exists a *multiplicative inverse* of z, written z^{-1}, with the property that $z \cdot z^{-1} = 1$. The multiplicative inverse of $z = x+yi$ is $z^{-1} = \frac{x-yi}{x^2+y^2}$.
9. Distributivity: $z \cdot (u+v) = z \cdot u + z \cdot v$

We will only prove the eighth property.

Proof: We only need to demonstrate that $\dfrac{x-yi}{x^2+y^2}$ is well-defined and that

$$x+yi\cdot\frac{x-yi}{x^2+y^2}=1$$

Since $z\neq 0$, $x^2+y^2\neq 0$ and so $\dfrac{x-yi}{x^2+y^2}$ is well-defined. Now we simply use complex arithmetic.

$$x+yi\cdot\frac{x-yi}{x^2+y^2}=\frac{x^2+xy-xy-y^2i^2}{x^2+y^2}=\frac{x^2+y^2}{x^2+y^2}=1$$

$\square$

31.4 More Examples

1. Let $z=3+4i$, $u=1-2i$ and $w=3i$. Express each of the following in standard form.

   (a) $z+3u-wi$

   (b) z/u

   Solution:

   (a) $z+3u-wi=(3+4i)+(3-6i)+(3)=9-2i$

   (b) $\dfrac{z}{u}=\dfrac{3+4i}{1-2i}=\dfrac{3+4i}{1-2i}\cdot\dfrac{1+2i}{1+2i}=\dfrac{-5+10i}{5}=-1+2i$

2. Express your answers to the following questions in standard form.

   (a) Use the quadratic formula to find solutions to $2x^2+3x+2=0$.
   Solution:

   $$\begin{aligned}x&=\frac{-b\pm\sqrt{b^2-4ac}}{2a}\\&=\frac{-3\pm\sqrt{-7}}{4}\\&=\frac{-3}{4}-\frac{7}{4}i\end{aligned}$$

   (b) Use the quadratic formula to find solutions to $ix^2+3x-2i=0$.
   Solution:

   $$\begin{aligned}x&=\frac{-b\pm\sqrt{b^2-4ac}}{2a}\\&=\frac{-3\pm1}{2i}\\&=\frac{-3\pm1}{2i}\cdot\frac{-2i}{-2i}\\&=2i\text{ or }i\end{aligned}$$

(c) The equation $x^3-x^2+x-1=0$ has one real solution but it also has two non-real complex solutions. What are the three solutions?

Solution: Observe that

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

so solutions to $x^3-x^2+x-1=0$ exist when

$$(x^2+1)=0 \text{ or } (x-1)=0$$

The second factor yields the real root $x=1$ and the first factor yields the two non-real complex roots $\pm i$.

3. Use the Binomial Theorem to expand $(2ix-i)^3$.

Solution:

$$\begin{aligned}(2ix-i)^3 &= \sum_{r=0}^{3}\binom{3}{r}(2ix)^{3-r}(-i)^r \\ &= \binom{3}{0}(2ix)^3+\binom{3}{1}(2ix)^2(-i)^1+\binom{3}{2}(2ix)^1(-i)^2+\binom{3}{3}(-i)^3 \\ &= -8ix^3+12ix^2-6ix+i\end{aligned}$$

Chapter 32

Properties Of Complex Numbers

32.1 Objectives

The content objectives are:

1. Define *conjugate* and *modulus*
2. State and prove several properties of complex numbers.

32.2 Conjugate

Definition 32.2.1
Conjugate

The **complex conjugate** of $z = x + yi$ is the complex number

$$\overline{z} = x - yi$$

The conjugate of $z = 2 + 3i$ is $\overline{z} = 2 - 3i$.

Proposition 1

(Properties of Conjugates (PCJ))

If z and w are complex numbers, then

1. $\overline{z + w} = \overline{z} + \overline{w}$
2. $\overline{zw} = \overline{z}\,\overline{w}$
3. $\overline{\overline{z}} = z$
4. $z + \overline{z} = 2\Re(z)$
5. $z - \overline{z} = 2i\Im(z)$

We will prove the first of these properties and leave the remainder as exercises.

Proof: Let $z = x + yi$ and $w = u + vi$. Then

$$\begin{aligned}
\overline{z+w} &= \overline{(x+yi)+(u+vi)} && \text{(substitution)}\\
&= \overline{(x+u)+(y+v)i} && \text{(defn of addition)}\\
&= (x+u)-(y+v)i && \text{(defn of conjugate)}\\
&= (x-yi)+(u-vi) && \text{(Properties of Addn and Mult)}\\
&= \overline{z}+\overline{w} && \text{(defn of conjugate)}
\end{aligned}$$

□

Exercise 1 Prove each of the remaining parts of the Properties of Conjugates proposition.

Example 1 Prove: Let $z \in \mathbb{C}$. The complex number z is a real number if and only if $z = \overline{z}$.

Solution: Let $z = x + yi$.

$$\begin{aligned}
z \text{ is real} &\iff \Im(z) = 0 && \text{(from the previous lecture)}\\
&\iff y = 0\\
&\iff x + 0i = x - 0i\\
&\iff z = \overline{z}
\end{aligned}$$

Exercise 2 Prove: Let $z \in \mathbb{C}$ and $z \neq 0$. The complex number z is purely imaginary ($\Re(z) = 0$) if and only if $z = -\overline{z}$.

Exercise 3 Let w and z be complex numbers in standard form. Prove that

$$\overline{\left(\frac{1}{w}\right)} = \frac{1}{\overline{w}}$$

and hence

$$\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$$

Example 2

For $z \neq i$ define

$$w = \frac{z+i}{z-i}$$

Prove that w is a real number if and only if z is zero or purely imaginary.

Solution:

$$\begin{aligned}
w \text{ is real} &\iff w = \overline{w} \\
&\iff \frac{z+i}{z-i} = \overline{\left(\frac{z+i}{z-i}\right)} \\
&\iff \frac{z+i}{z-i} = \frac{\overline{z}-i}{\overline{z}+i} \\
&\iff z\overline{z} - 1 + (z+\overline{z})i = z\overline{z} - 1 - (z+\overline{z})i \\
&\iff 2i(z+\overline{z}) = 0 \\
&\iff z + \overline{z} = 0 \\
&\iff 2\Re(z) = 0 \\
&\iff \Re(z) = 0 \\
&\iff z \text{ is zero or purely imaginary}
\end{aligned}$$

32.3 Modulus

Definition 32.3.1
Modulus

The **modulus** of the complex number $z = x + yi$ is the non-negative real number

$$|z| = |x + yi| = \sqrt{x^2 + y^2}$$

Example 3

The modulus of $z = 2 - 5i$ is $|z| = \sqrt{(2^2) + (-5)^2} = \sqrt{29}$.

Given two real numbers, say x_1 and x_2, we can write either $x_1 \leq x_2$ or $x_2 \leq x_1$. However, given two complex numbers, z_1 and z_2, we cannot meaningfully write $z_1 \leq z_2$ or $z_2 \leq z_1$. But since the modulus of a complex number is a real number, we can meaningfully write $|z_1| \leq |z_2|$. The modulus gives us a means to compare the magnitude of two complex numbers, but not compare the numbers themselves.

If $\Im(z) = 0$, then the modulus corresponds to the absolute values of real numbers.

Proposition 2 **(Properties of Modulus (PM))**

If z and w are complex numbers, then

1. $|z| = 0$ if and only if $z = 0$
2. $|\overline{z}| = |z|$
3. $\overline{z}z = |z|^2$
4. $|zw| = |z||w|$
5. $|z + w| \leq |z| + |w|$. This is the **triangle inequality**.

Exercise 4 Prove each of the parts of the Properties of Modulus proposition.

32.4 More Examples

1. Find all $z \in \mathbb{C}$ which satisfy $\overline{z} = z^2$.

   Solution: Let $z = x + yi$ with $x, y \in \mathbb{R}$. Then $\overline{z} = z^2$ gives $x - yi = (x + yi)^2$ or $x - yi = (x^2 - y^2) + 2xyi$. Equating real and imaginary parts we have

   $$\begin{aligned} x &= x^2 - y^2 \\ -y &= 2xy \end{aligned}$$

   From the second equation we get

   $$2xy + y = 0 \Rightarrow y(2x + 1) = 0 \Rightarrow y = 0 \text{ or } x = \frac{-1}{2}$$

   If $y = 0$ then the first equation gives

   $$x = x^2 \Rightarrow x^2 - x = 0 \Rightarrow x(x - 1) = 0 \Rightarrow x = 0 \text{ or } x = 1$$

   If $x = \frac{-1}{2}$ then the first equation gives

   $$\frac{-1}{2} = \frac{1}{4} - y^2 \Rightarrow y^2 = \frac{3}{4} \Rightarrow y = \pm\frac{\sqrt{3}}{2}$$

   Thus, the solutions are

   $$0, 1, \frac{-1}{2} + \frac{\sqrt{3}}{2}i, \frac{-1}{2} - \frac{\sqrt{3}}{2}i$$

2. Let $z \in \mathbb{C}$, $z \neq \pm i$. Prove that $\dfrac{z}{1+z^2}$ is real if and only if z is real or $|z| = 1$.

   Proof: We will use the fact that $w \in \mathbb{C}$ is real iff $w = \overline{w}$.

$$
\begin{aligned}
& \frac{z}{1+z^2} = \overline{\left(\frac{z}{1+z^2}\right)} \\
\iff & \frac{z}{1+z^2} = \frac{\overline{z}}{1+\overline{z}^2} \\
\iff & z + z\overline{z}^2 = \overline{z} + \overline{z}z^2 \\
\iff & (z-\overline{z}) + (z\overline{z}^2 - \overline{z}z^2) = 0 \\
\iff & (z-\overline{z}) + z\overline{z}(\overline{z} - z) = 0 \\
\iff & (z-\overline{z}) - z\overline{z}(z - \overline{z}) = 0 \\
\iff & (z-\overline{z})(1 - z\overline{z}) = 0 \\
\iff & z - \overline{z} = 0 \text{ or } 1 - z\overline{z} = 0 \\
\iff & z = \overline{z} \text{ or } 1 - |z|^2 = 0 \\
\iff & z = \overline{z} \text{ or } |z|^2 = 1 \\
\iff & z \text{ is real or } |z| = 1
\end{aligned}
$$

   as required. □

3. For each step of the following argument that purports to show that $|z| = 1$ for all complex numbers z, provide justification (by citing an appropriate proposition, for example) or state that the logic is incorrect and give a reason why.

   Let z be any complex number.

$$
\begin{aligned}
0 &= |1| - 1 && (32.1)\\
&= |zz^{-1}| - 1 && (32.2)\\
&= |z||z^{-1}| - 1 && (32.3)\\
&= |(z+1) - 1||z^{-1}| - 1 && (32.4)\\
&= (|z+1| + |-1|)|z^{-1}| - 1 && (32.5)\\
&= (|z+1| + 1)|z^{-1}| - 1 && (32.6)\\
&= |z+1||z^{-1}| + |z^{-1}| - 1 && (32.7)\\
&= |z+1||z| + |z| - 1 && (32.8)\\
&= (|z| + |1|)|z| + |z| - 1 && (32.9)\\
&= (|z| + 1)|z| + |z| - 1 && (32.10)\\
&= |z|^2 + 2|z| - 1 && (32.11)\\
&= (|z| - 1)^2 && (32.12)
\end{aligned}
$$

   Therefore $|z| = 1$ for all complex numbers z.

32.5 Practice

1. Let z be a complex number. Prove that $|z|^n = |z^n|$ for any positive integer n.
2. Find all $z \in \mathbb{C}$ which satisfy
   (a) $z^2 + 2z + 1 = 0$
   (b) $z^2 + 2\overline{z} + 1 = 0$
   (c) $z^2 = \dfrac{1+i}{1-i}$.
3. Let $a, b, c \in \mathbb{C}$. Prove: If $|a| = |b| = |c| = 1$, then $\overline{a+b+c} = \dfrac{1}{a} + \dfrac{1}{b} + \dfrac{1}{c}$.

Chapter 33

Graphical Representations of Complex Numbers

33.1 Objectives

The content objectives are:

1. Define *complex plane*, *polar coordinates*, *polar form*.
2. Convert between Cartesian and polar form.
3. Multiplication in polar form.

33.2 The Complex Plane

33.2.1 Cartesian Coordinates (x, y)

Definition 33.2.1
Complex Plane

The notation $z = x + yi$ suggests a non-algebraic representation. Each complex number $z = x + yi$ can be thought of as a point (x, y) in a plane with orthogonal axes. Label one axis the **real axis** and the other axis the **imaginary axis**. The complex number $z = x+yi$ then corresponds to the point (x, y) in the plane. This interpretation of the plane is called the **complex plane** or the **Argand plane**.

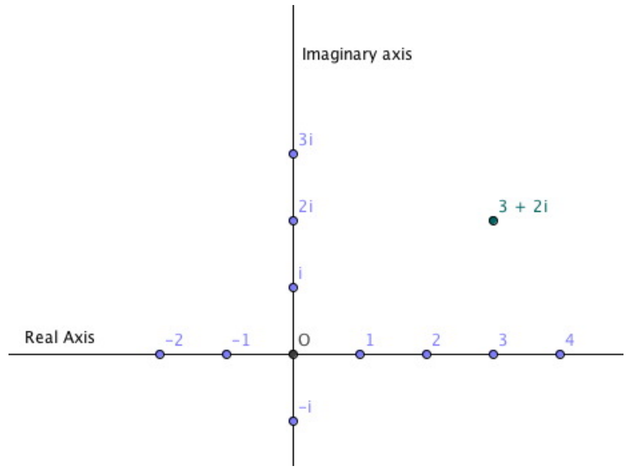


Figure 33.2.1: The Complex Plane

Exercise 1 Plot the following points in the complex plane.

1. $4+i$
2. $-2+3i$
3. $-2-i$

33.2.2 Modulus

Recall that the modulus of the complex number $z = x+yi$ is the non-negative real number

$$|z| = |x+yi| = \sqrt{x^2+y^2}$$

There are a couple of geometric points to note about the modulus of $z = x+yi$. The Pythagorean Theorem is enough to prove that $|z|$ is the distance from the origin to z in the complex plane, and that the distance between z and $w = u+vi$ is just $|z-w| = \sqrt{(x-u)^2+(y-v)^2}$.

Exercise 2 Sketch all of the points in the complex plane with modulus 1.

33.3 Polar Representation

There is another way to represent points in a plane which is very useful when working with complex numbers. Instead of beginning with the origin and two orthogonal axes, we begin with the origin O and a **polar axis** which is a ray leaving from the origin. The point $P(r,\theta)$ is plotted so that the distance OP is r, and the counter clockwise angle of rotation from the polar axis, measured in radians, is θ.

Note that this allows for multiple representations since (r,θ) identifies the same point as $(r,\theta+2\pi k)$ for any integer k.

The obvious problem is how to go from one to the other.

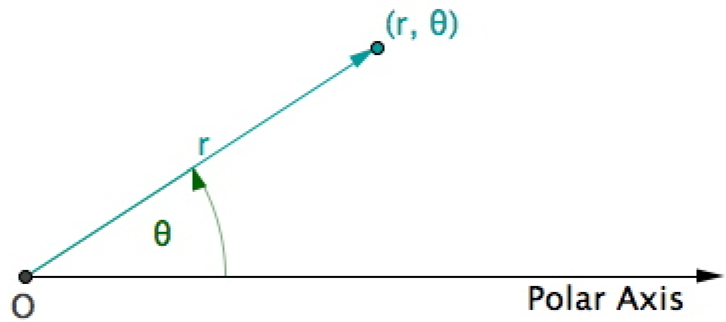


Figure 33.3.1: Polar Representation

33.4 Converting Between Representations

Simple trigonometry allows us to convert between polar and Cartesian coordinates.

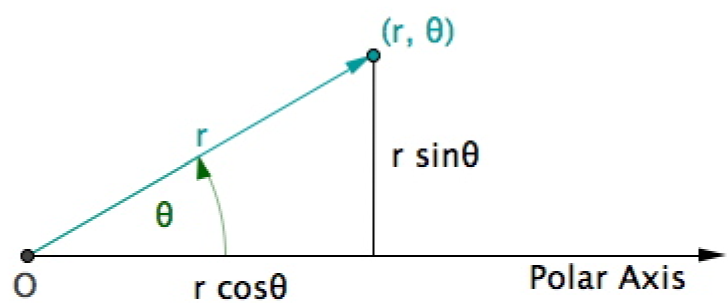


Figure 33.4.1: Connecting Polar and Cartesian Representations

Given the polar coordinates (r, θ), the corresponding Cartesian coordinates (x, y) are

$$\begin{aligned} x &= r\cos\theta \\ y &= r\sin\theta \end{aligned}$$

Given the Cartesian coordinates (x, y), the corresponding polar coordinates are determined by

$$\begin{aligned} r &= \sqrt{x^2 + y^2} \\ \cos\theta &= \frac{x}{r} \\ \sin\theta &= \frac{y}{r} \end{aligned}$$

Example 1 Here are points in standard form, Cartesian coordinates and polar coordinates.

Standard Form	Cartesian Coordinates	Polar Coordinates
$-1+i$	$(-1, 1)$	$(\sqrt{2}, 3\pi/4)$
$-1-\sqrt{3}i$	$(-1, -\sqrt{3})$	$(2, 4\pi/3)$
1	$(1, 0)$	$(1, 0)$

Exercise 3

For each of the following polar coordinates, plot the point and convert to Cartesian coordinates.

1. $(1, 0)$
2. $(2, \pi/2)$
3. $(3, \pi)$
4. $(2, 7\pi/2)$
5. $(4, \pi/4)$
6. $(4, 4\pi/3)$

Exercise 4

For each of the following Cartesian coordinates, plot the point and convert to polar coordinates.

1. $(1, 0)$
2. $(0, 1)$
3. $(-1, 0)$
4. $(0, -1)$
5. $(1, 1)$
6. $(-1, 1)$
7. $(2, -2\sqrt{3})$

From our earlier description of conversions, we can write the complex number

$$z = x + yi$$

as

$$z = r\cos\theta + ri\sin\theta = r(\cos\theta + i\sin\theta)$$

Definition 33.4.1
Polar Form

The **polar form** of a complex number z is

$$z = r(\cos\theta + i\sin\theta)$$

where r is the modulus of z and the angle θ is called an **argument** of z.

Example 2 The following are representations of complex numbers in both standard and polar form.

1. $1 = \cos 0 + i \sin 0$
2. $-1 + i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$
3. $-1 - \sqrt{3}i = 2\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)$

One of the advantages of polar representation is that multiplication becomes very straightforward.

Proposition 1 **(Polar Multiplication of Complex Numbers (PMCN))**

If $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ are two complex numbers in polar form, then

$$z_1 z_2 = r_1 r_2\left(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\right)$$

Example 3

$$\begin{aligned}
&\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) \cdot 2\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right)\\
&= 2\sqrt{2}\left(\cos\left(\frac{3\pi}{4} + \frac{4\pi}{3}\right) + i\sin\left(\frac{3\pi}{4} + \frac{4\pi}{3}\right)\right)\\
&= 2\sqrt{2}\left(\cos\left(\frac{25\pi}{12}\right) + i\sin\left(\frac{25\pi}{12}\right)\right)\\
&= 2\sqrt{2}\left(\cos\left(\frac{\pi}{12}\right) + i\sin\left(\frac{\pi}{12}\right)\right)
\end{aligned}$$

Proof:

$$\begin{aligned}
z_1 z_2 &= r_1(\cos\theta_1 + i\sin\theta_1) \cdot r_2(\cos\theta_2 + i\sin\theta_2)\\
&= r_1 r_2\left((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)\right)\\
&= r_1 r_2\left(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\right)
\end{aligned}$$

□

33.5 More Examples

1. Write $z = \dfrac{9+i}{5-4i}$ in the form $r(\cos\theta + i\sin\theta)$ with $r \geq 0$ and $0 \leq \theta < 2\pi$.

   Solution:

   $$z = \frac{9+i}{5-4i} = \frac{(9+i)(5+4i)}{(5-4i)(5+4i)} = \frac{41+41i}{5^2+4^2} = 1 + i = \sqrt{2}(\cos\pi/4 + i\sin\pi/4).$$

Chapter 34

De Moivre's Theorem

34.1 Objectives

The content objectives are:

1. State and prove *De Moivre's Theorem* and do examples.
2. Derive Euler's Formula.

34.2 De Moivre's Theorem

De Moivre's Theorem dramatically simplifies exponentiation of complex numbers.

Theorem 1 **(De Moivre's Theorem (DMT))**

If $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, then

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

Example 1 Consider the complex number

$$z = 1/\sqrt{2} + i/\sqrt{2}$$

which, in polar form is

$$z = \cos\pi/4 + i\sin\pi/4$$

By De Moivre's Theorem,

$$z^{10} = (\cos\pi/4 + i\sin\pi/4)^{10} = \cos 10\pi/4 + i\sin 10\pi/4 = \cos\pi/2 + i\sin\pi/2 = i.$$

Proof: We will prove DeMoivre's Theorem using three cases.

1. $n = 0$
2. $n > 0$
3. $n < 0$

For the case $n = 0$, DeMoivre's Theorem reduces to $(\cos\theta + i\sin\theta)^0 = \cos 0 + i\sin 0$. By convention $z^0 = 1$ so the left hand side of the equation is 1. Since $\cos 0 = 1$ and $\sin 0 = 0$, the right hand side also evaluates to 1.

For the case $n > 0$ we will use induction.

$P(n)$: $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$.

Base Case We verify that $P(1)$ is true where $P(1)$ is the statement

$P(1)$: $(\cos\theta + i\sin\theta)^1 = \cos 1\theta + i\sin 1\theta$.

This is trivially true.

Inductive Hypothesis We assume that the statement $P(k)$ is true for some $k \geq 1$.

$P(k)$: $(\cos\theta + i\sin\theta)^k = \cos k\theta + i\sin k\theta$.

Inductive Conclusion Now show that the statement $P(k+1)$ is true.

$P(k+1)$: $(\cos\theta + i\sin\theta)^{k+1} = \cos(k+1)\theta + i\sin(k+1)\theta$

$$\begin{aligned}
(\cos\theta + i\sin\theta)^{k+1} &= (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta) && \text{(by separating out one factor)}\\
&= (\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta) && \text{(by the Inductive Hypothesis)}\\
&= \cos(k+1)\theta + i\sin(k+1)\theta && \text{(Polar Multiplication)}
\end{aligned}$$

Since $P(k+1)$ is true, $P(n)$ is true for all natural numbers n by the Principle of Mathematical Induction.

Lastly, for the case $n < 0$ we will use complex arithmetic. Since $n < 0$, $n = -m$ for some $m \in \mathbb{N}$.

$$\begin{aligned}
(\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{-m}\\
&= \frac{1}{(\cos\theta + i\sin\theta)^m}\\
&= \frac{1}{(\cos m\theta + i\sin m\theta)}\\
&= \cos m\theta - i\sin m\theta\\
&= \cos(-m\theta) + i(\sin(-m\theta))\\
&= \cos n\theta + i\sin n\theta
\end{aligned}$$

$\square$

Corollary 2

If $z = r(\cos\theta + i\sin\theta)$ and n is an integer,

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

34.3 Complex Exponentials

If you were asked to find a real-valued function y with the property that

$$\frac{dy}{dx} = ky \text{ and } y = 1 \text{ when } x = 0$$

for some constant k, you would choose

$$y = e^{kx}$$

And if you were asked to find the derivative of $f(\theta) = \cos\theta + i\sin\theta$ where i was treated as any other constant you would almost certainly write

$$\frac{df(\theta)}{d\theta} = -\sin\theta + i\cos\theta$$

but then

$$\frac{df(\theta)}{d\theta} = -\sin\theta + i\cos\theta = i(\cos\theta + i\sin\theta) = if(\theta)$$

and so

$$\frac{df(\theta)}{d\theta} = if(\theta) \text{ and } f(\theta) = 1 \text{ when } \theta = 0$$

Definition 34.3.1
Complex Exponential

By analogy, we define the **complex exponential function** by

$$e^{i\theta} = \cos\theta + i\sin\theta$$

As an exercise, prove the following.

Proposition 3

(Properties of Complex Exponentials (PCE))

$$e^{i\theta} \cdot e^{i\phi} = e^{i(\theta+\phi)}$$
$$\left(e^{i\theta}\right)^n = e^{in\theta} \qquad \forall n \in \mathbb{Z}$$

The polar form of a complex number z can now be written as

$$z = re^{i\theta}$$

where $r = |z|$ and θ is an argument of z.

Out of this arises one of the most stunning formulas in mathematics. Setting $r = 1$ and $\theta = \pi$ we get

$$e^{i\pi} = \cos\pi + i\sin\pi = -1 + 0i = -1$$

That is

$$e^{i\pi} + 1 = 0$$

Who would have believed that $e, i, \pi, 1$ and 0 would have such a wonderful connection!

34.4 More Examples

1. This question asks you to compute $(\sqrt{3}+i)^4$ in two ways. Write your answer in standard form.

   (a) Use the Binomial Theorem.

   (b) Use De Moivre's Theorem.

   Solution:

   (a) Using the Binomial Theorem we have

$$\begin{aligned}(\sqrt{3}+y)^4 &= \sum_{r=0}^{4}\binom{4}{r}(\sqrt{3})^{4-r}i^r \\ &= \binom{4}{0}(\sqrt{3})^{4-0}i^0 + \binom{4}{1}(\sqrt{3})^{4-1}i^1 + \binom{4}{2}(\sqrt{3})^{4-2}i^2 + \\ &\qquad \binom{4}{3}(\sqrt{3})^{4-3}i^3 + \binom{4}{4}(\sqrt{3})^{4-4}i^4 \\ &= 9 + 4\cdot 3\sqrt{3}i - 6\cdot 3 - 4i\sqrt{3} + 1 \\ &= -8 + 8\sqrt{3}i\end{aligned}$$

   (b) Using De Moivre's Theorem we have First, write $\sqrt{3}+i$ in polar form. The modulus is $r = \sqrt{\sqrt{3}^2 + 1^2} = 2$. An argument is $\frac{\pi}{6}$. Thus, $\sqrt{3}+i = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6})$. By De Moivre's Theorem

$$\begin{aligned}\left(2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)\right)^4 &= 2^4\left(\cos\frac{4\pi}{6} + i\sin\frac{4\pi}{6}\right) \\ &= 16\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right) \\ &= 16\left(\frac{-1}{2} + \frac{\sqrt{3}i}{2}\right) \\ &= -8 + 8\sqrt{3}i\end{aligned}$$

   (c) Write $z = \left(\dfrac{e^{i5\pi/12}}{\sqrt{3}}\right)^{-6}$ in the form $x + iy$ with $x, y \in \mathbb{R}$.

   Solution:

$$z = \left(\frac{e^{i5\pi/12}}{\sqrt{3}}\right)^{-6} = (\sqrt{3})^6(e^{i5\pi/12})^{-6} = 3^3e^{-i5\pi/2} = 27(e^{-i\pi/2}) = -27i.$$

34.5 Practice

1. Compute each of the following twice: once using the Binomial Theorem and once using De Moivre's Theorem. Write your answer in standard form.

   (a) $(\sqrt{3} - 3i)^4$

   (b) $(2 - 2\sqrt{3}i)^4$

Chapter 35

Roots of Complex Numbers

35.1 Objectives

The content objectives are:

1. State and prove the *Complex n-th Roots Theorem* and do examples.

35.2 Complex n-th Roots

Definition 35.2.1
Complex Roots

If a is a complex number, then the complex numbers that solve

$$z^n = a$$

are called the **complex n-th roots**. De Moivre's Theorem gives us a straightforward way to find complex n-th roots of a.

Theorem 1 **(Complex n-th Roots Theorem (CNRT))**

If $r(\cos\theta + i\sin\theta)$ is the polar form of a complex number a, then the solutions to $z^n = a$ are

$$\sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right) \qquad \text{for } k = 0, 1, 2, \ldots, n-1$$

The modulus $\sqrt[n]{r}$ is the unique non-negative n-th root of r. This theorem asserts that any complex number, including the reals, has exactly n different complex n-th roots.

Example 1 Find all the complex fourth roots of -16.

Solution: We will use the Complex n-th Roots Theorem. First, we write -16 in polar form as

$$-16 = 16(\cos\pi + i\sin\pi)$$

Using the Complex n-th Roots Theorem the solutions are

$$\begin{aligned}
&\sqrt[4]{16}\left(\cos\left(\frac{\pi+2k\pi}{4}\right)+i\sin\left(\frac{\pi+2k\pi}{4}\right)\right) && \text{for } k=0,1,2,3\\
&= 2\left(\cos\left(\frac{\pi}{4}+\frac{k\pi}{2}\right)+i\sin\left(\frac{\pi}{4}+\frac{k\pi}{2}\right)\right) && \text{for } k=0,1,2,3
\end{aligned}$$

The four distinct roots are given below

When $k=0$, $z_0 = 2\left(\cos\left(\frac{\pi}{4}\right)+i\sin\left(\frac{\pi}{4}\right)\right) = 2\left(\frac{1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right) = \sqrt{2}+i\sqrt{2}$

When $k=1$, $z_1 = 2\left(\cos\left(\frac{3\pi}{4}\right)+i\sin\left(\frac{3\pi}{4}\right)\right) = 2\left(\frac{-1}{\sqrt{2}}+\frac{i}{\sqrt{2}}\right) = -\sqrt{2}+i\sqrt{2}$

When $k=2$, $z_2 = 2\left(\cos\left(\frac{5\pi}{4}\right)+i\sin\left(\frac{5\pi}{4}\right)\right) = 2\left(\frac{-1}{\sqrt{2}}+\frac{-i}{\sqrt{2}}\right) = -\sqrt{2}-i\sqrt{2}$

When $k=3$, $z_3 = 2\left(\cos\left(\frac{7\pi}{4}\right)+i\sin\left(\frac{7\pi}{4}\right)\right) = 2\left(\frac{1}{\sqrt{2}}+\frac{-i}{\sqrt{2}}\right) = \sqrt{2}-i\sqrt{2}$

Graphing these solutions is illuminating.

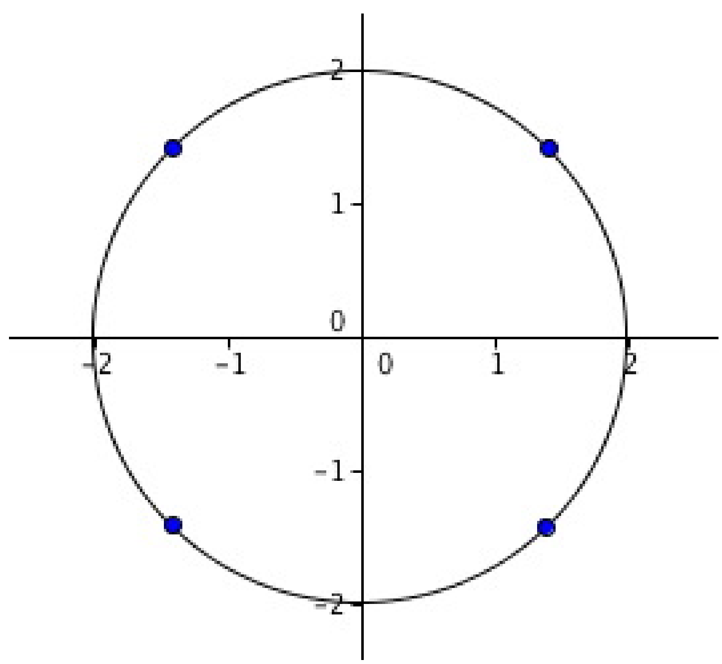


Figure 35.2.1: The Fourth Roots of -16

Note that the solutions are uniformly distributed around a circle whose radius is $\sqrt[4]{16}$.

Proof: As usual, when showing that a complete solution exists we work with two sets: the set S of solutions and the set T of specific representations of the solution. We then show that $S = T$ by mutual inclusion. Our two sets are

$$S = \{z \in \mathbb{C} \mid z^n = a\}$$

and

$$T = \left\{ \sqrt[n]{r} \left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i \sin\left(\frac{\theta + 2k\pi}{n}\right)\right) \middle| k = 0, 1, 2, \ldots, n-1 \right\}$$

where $a = r(\cos\theta + i\sin\theta)$.

We begin by showing that $T \subseteq S$. Let $t = \sqrt[n]{r}\left(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right)$ be an element of T. Now

$$\begin{aligned} t^n &= \left(\sqrt[n]{r}\right)^n \left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right)^n \\ &= r(\cos(\theta + 2k\pi) + i\sin(\theta + 2k\pi)) \qquad \text{De Moivre's Theorem} \\ &= r(\cos\theta + i\sin\theta) \qquad \text{trigonometry} \\ &= a \end{aligned}$$

Hence, t is a solution of $z^n = a$, that is, $t \in S$.

Now we show that $S \subseteq T$. Let $w = s(\cos\phi + i\sin\phi)$ be an n-th root of a.
Since $a = r(\cos\theta + i\sin\theta)$ we have

$$\begin{aligned} & w^n = a \\ \iff & (s(\cos\phi + i\sin\phi))^n = r(\cos\theta + i\sin\theta) \\ \iff & s^n(\cos n\phi + i\sin n\phi) = r(\cos\theta + i\sin\theta) \qquad \text{De Moivre's Theorem} \end{aligned}$$

Now two complex numbers in polar form are equal if and only if their moduli are equal and their arguments differ by an integer multiple of 2π. So

$$s^n = r \Rightarrow s = \sqrt[n]{r}$$

and

$$n\phi - \theta = 2\pi k \Rightarrow \phi = \frac{\theta + 2\pi k}{n}$$

where $k \in \mathbb{Z}$. Hence, the n-th roots of a are of the form

$$\sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\sin\left(\frac{\theta + 2k\pi}{n}\right)\right) \qquad \text{for } k \in \mathbb{Z}$$

But this is $k \in \mathbb{Z}$, not $k = 0, 1, 2, \ldots, n-1$. Since w is an n-th root of a, there exists an integer k_0 so that

$$w = \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k_0\pi}{n}\right) + i\sin\left(\frac{\theta + 2k_0\pi}{n}\right)\right)$$

If we can show that

$$w = \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k_1\pi}{n}\right) + i\sin\left(\frac{\theta + 2k_1\pi}{n}\right)\right)$$

if and only if $k_0 \equiv k_1 \pmod{n}$ whenever $r \neq 0$, then $w \in T$. Now

$$\begin{aligned} & k_0 \equiv k_1 \pmod{n} & \\ \iff\ & k_0 - k_1 = n\ell & \text{for some } \ell \in \mathbb{Z} \\ \iff\ & 2\pi k_0 - 2\pi k_1 = 2\pi n\ell & \text{for some } \ell \in \mathbb{Z} \\ \iff\ & \frac{2\pi k_0}{n} - \frac{2\pi k_1}{n} = 2\pi\ell & \text{for some } \ell \in \mathbb{Z} \\ \iff\ & \frac{\theta + 2\pi k_0}{n} - \frac{\theta + 2\pi k_1}{n} = 2\pi\ell & \text{for some } \ell \in \mathbb{Z} \end{aligned}$$

□

Exercise 1 An **n-th root of unity** is a complex number that solves $z^n = 1$. Find all of the sixth roots of unity. Express them in standard form and graph them in the complex plane.

Exercise 2 Find the square roots of $-2i$. Express them in standard form and graph them in the complex plane.

35.3 More Examples

1. (a) Find the cube roots of -1. Express your answers in standard form and plot these solutions in the complex plane.

   Solution: We will use the Complex n-th Roots Theorem. First, we write -1 in polar form as
   $$-1 = 1(\cos\pi + i\sin\pi)$$
   Using the Complex n-th Roots Theorem the solutions are
   $$\sqrt[3]{1}\left(\cos\left(\frac{\pi + 2k\pi}{3}\right) + i\sin\left(\frac{\pi + 2k\pi}{3}\right)\right) \qquad \text{for } k = 0, 1, 2$$
   The three distinct roots are given below
   $$\begin{aligned} &\text{When } k = 0,\ z_0 = 1\left(\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2} \\ &\text{When } k = 1,\ z_1 = 1\left(\cos\left(\frac{3\pi}{3}\right) + i\sin\left(\frac{3\pi}{3}\right)\right) = -1 \\ &\text{When } k = 2,\ z_2 = 1\left(\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right)\right) = \frac{1}{2} - i\frac{\sqrt{3}}{2} \end{aligned}$$
   The diagram is omitted.

   (b) Find all of the cube roots of 2. Express your answers in standard form and plot these solutions in the complex plane.

   Solution: We will use the Complex n-th Roots Theorem to solve $z^3 = 2$. First, we write 2 in polar form as
   $$2 = 2(\cos 0 + i\sin 0)$$

Using the Complex n-th Roots Theorem the solutions are

$$\sqrt[3]{2}\left(\cos\left(\frac{2k\pi}{3}\right)+i\sin\left(\frac{2k\pi}{3}\right)\right) \qquad \text{for } k=0,1,2$$

The three distinct roots are given below

When $k=0$, $z_0=\sqrt[3]{2}\,(\cos(0)+i\sin(0))=\sqrt[3]{2}$

When $k=1$, $z_1=\sqrt[3]{2}\left(\cos\left(\frac{2\pi}{3}\right)+i\sin\left(\frac{2\pi}{3}\right)\right)=\sqrt[3]{2}\left(\frac{-1}{2}+\frac{i\sqrt{3}}{2}\right)=-\frac{1}{\sqrt[3]{4}}+\frac{\sqrt{3}}{\sqrt[3]{4}}i$

When $k=2$, $z_1=\sqrt[3]{2}\left(\cos\left(\frac{4\pi}{3}\right)+i\sin\left(\frac{4\pi}{3}\right)\right)=\sqrt[3]{2}\left(\frac{-1}{2}-\frac{i\sqrt{3}}{2}\right)=-\frac{1}{\sqrt[3]{4}}-\frac{\sqrt{3}}{\sqrt[3]{4}}i$

The diagram is omitted.

(c) Solve $z^6-z^3-2=0$. (Hint: factor the left side of the equation into a product of two cubic polynomials first. Think of it as a quadratic in z^3.)

Solution: Since $z^6-z^3-2=(z^3-2)(z^3+1)$ it is enough to solve $z^3-2=0$ and $z^3+1=0$. The roots of $z^3-2=0$ are given in part (b). The roots of $z^3+1=0$ are given in part (a).

35.4 Practice

1. Find all of the cube roots of unity. Write them in standard form and plot the solutions in the complex plane.

2. A complex number z is called a *primitive* n-th root of unity if $z^n=1$ and $z^k\neq 1$ for all $1\leq k\leq n-1$.

   (a) For each $n=1,2,3,6$, list all the primitive n-th roots of unity. (You may express your answers in standard, polar form or exponential form.)

   (b) Let z be a primitive n-th root of unity. Prove the following statements.

      i. For any $k\in\mathbb{Z}$, $z^k=1$ if and only if $n\mid k$.

      ii. For any $m\in\mathbb{Z}$, if $\gcd(m,n)=1$, then z^m is a primitive n-th root of unity.

Chapter 36

Practice, Practice, Practice: Complex Numbers

36.1 Objectives

This class provides an opportunity to practice working with quantifiers and sets.

36.2 Worked Examples

Example 1 Calculate $(-1+\sqrt{3}i)^{17}$.

Solution: The size of the exponent makes the use of the Binomial Theorem impractical so we use De Moivre's Theorem. The polar form of $-1+\sqrt{3}i$ is

$$z = 2(\cos 2\pi/3 + i\sin 2\pi/3)$$

By De Moivre's Theorem,

$$\begin{aligned}
(-1+\sqrt{3}i)^{17} &= 2^{17}(\cos 2\pi/3 + i\sin 2\pi/3)^{17} \\
&= 2^{17}(\cos 34\pi/3 + i\sin 34\pi/3) \\
&= 2^{17}(\cos 4\pi/3 + i\sin 4\pi/3) \\
&= 2^{17}(-\frac{1}{2} - \frac{\sqrt{3}}{2}i) \\
&= 2^{16}(-1-\sqrt{3}i)
\end{aligned}$$

Example 2 Find all the cube roots of i.

Solution: We will use the Complex n-th Roots Theorem. First, we write i in polar form as

$$i = \cos \pi/2 + i \sin \pi/2$$

Using the Complex n-th Roots Theorem the solutions are

$$\begin{aligned} &\cos\left(\frac{\frac{\pi}{2} + 2k\pi}{3}\right) + i \sin\left(\frac{\frac{\pi}{2} + 2k\pi}{3}\right) && \text{for } k = 0, 1, 2 \\ = &\cos\left(\frac{\pi + 4k\pi}{6}\right) + i \sin\left(\frac{\pi + 4k\pi}{6}\right) && \text{for } k = 0, 1, 2 \end{aligned}$$

The three distinct roots are given below.

$$\begin{aligned} &\text{When } k = 0,\, z_0 = \cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{i}{2} \\ &\text{When } k = 1,\, z_1 = \cos\left(\frac{5\pi}{6}\right) + i \sin\left(\frac{5\pi}{6}\right) = \frac{-\sqrt{3}}{2} + \frac{i}{2} \\ &\text{When } k = 2,\, z_2 = \cos\left(\frac{3\pi}{2}\right) + i \sin\left(\frac{3\pi}{2}\right) = -i \end{aligned}$$

Example 3 Find all $z \in \mathbb{C}$ which satisfy $z^2 + 2\overline{z} + 1 = 0$.

Solution: Let $z = x + yi$ where $x, y \in \mathbb{R}$. Then

$$z^2 + 2\overline{z} + 1 = 0 \Rightarrow (x^2 - y^2 + 2xyi) + 2(x - yi) + 1 = 0$$

or

$$(x^2 - y^2 + 2x + 1) + (2xy - 2y)i = 0$$

Equating real and imaginary parts we have

$$\begin{aligned} x^2 - y^2 + 2x + 1 &= 0 \\ 2xy - 2y &= 0 \end{aligned}$$

From the second equation we get

$$2xy - 2y = 0 \Rightarrow 2y(x - 1) = 0 \Rightarrow y = 0 \text{ or } x = 1$$

If $y = 0$ then the first equation gives

$$x^2 + 2x + 1 = 0 \Rightarrow x = -1$$

If $x = 1$ then the first equation gives

$$1 - y^2 + 2 + 1 = 0 \Rightarrow y^2 = 4 \Rightarrow y = \pm 2$$

Thus, the solutions are

$$-1, 1 + 2i, 1 - 2i$$

Example 4 Use De Moivre's Theorem and the Binomial Theorem to show that

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$
$$\sin 3\theta = 3\sin\theta - 4\sin^3\theta$$

Solution: By De Moivre's Theorem

$$(\cos\theta + i\sin\theta)^3 = \cos 3\theta + \sin 3\theta$$

By the Binomial Theorem

$$(\cos\theta + i\sin\theta)^3 = \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta$$

Equating the two right and sides gives

$$\cos 3\theta + \sin 3\theta = \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta$$

Equating real and imaginary parts gives

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$$
$$\sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta$$

Now using the identity $\sin^2\theta + \cos^2\theta = 1$ we have

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta = \cos^3\theta - 3\cos\theta(1-\cos^2\theta) = 4\cos^3\theta - 3\cos\theta$$
$$\sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta = 3(1-\sin^2\theta)\sin\theta - \sin^3\theta = 3\sin\theta - 4\sin^3\theta$$

as required.

Example 5 Using the fact that $\theta = \frac{2}{5}\pi$ satisfies $\cos 2\theta = \cos 3\theta$, calculate $\cos\frac{2}{5}\pi$.

Solution: From the previous example and substituting $1-\cos^2\theta$ for $\sin^2 theta$ we have

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Now, by the hint, we get

$$\cos 2\theta = 4\cos^3\theta - 3\cos\theta \Rightarrow 2\cos^2\theta - 1 = 4\cos^3\theta - 3\cos\theta$$

by the double angle formula for the cosine. Rearranging this and letting $X = \cos\theta$, we get

$$4X^3 - 2X^2 - 3X + 1 = 0$$

Note that $X = 1$ is a solution (extraneous) to this polynomial: that would mean that $\theta = 0$, contrary to assumption. So, divide the polynomial by $X - 1$ to get

$$(X-1)(4X^2 + 2X - 1) = 0$$

The real value of $\cos\theta$ is one of the roots of this polynomial, and it is not 1. Now apply the quadratic formula taking the positive root since $\theta = \frac{2}{5}\pi < \frac{1}{2}\pi$ to get

$$X = \frac{-2 \pm \sqrt{20}}{8} \text{ and } X > 0 \Rightarrow X = \frac{-1+\sqrt{5}}{4}$$

Therefore, $\cos\frac{2}{5}\theta = \frac{-1+\sqrt{5}}{4}$.

Example 6

For $z \in \mathbb{C}$, $z \neq i$ define $w = \dfrac{z+i}{z-i}$. Prove that $|w| < 1$ if and only if $\Im(z) < 0$.

Solution: Let $z = x + yi$ with $x, y \in \mathbb{R}$.

$$\begin{aligned}
|w| < 1 &\iff \left|\frac{z+i}{z-i}\right| < 1 \\
&\iff \frac{|z+i|}{|z-i|} < 1 \\
&\iff |z+i| < |z-i| \\
&\iff |x + (y+1)i| < |x + (y-1)i| \\
&\iff \sqrt{x^2 + (y+1)^2} < \sqrt{x^2 + (y-1)^2} \\
&\iff x^2 + (y+1)^2 < x^2 + (y-1)^2 \\
&\iff 2y < -2y \\
&\iff 4y < 0 \\
&\iff y < 0 \\
&\iff \Im(z) < 0
\end{aligned}$$

36.3 Quiz

Example 7

(10 marks) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with real coefficients. A number $c \in \mathbb{C}$ is called a **root** of the real polynomial $f(x)$ if $f(c) = 0$. Prove the following proposition.

Theorem 1 **(Conjugate Roots Theorem (CJRT))**

If $c \in \mathbb{C}$ is a root of $f(x)$, then $\overline{c} \in \mathbb{C}$ is a root of $f(x)$.

Proof: Since c is a root of $f(x)$

$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0 = 0 \checkmark\checkmark$$

Taking the complex conjugate of both sides gives ✓

$$\checkmark\,\overline{a_n c^n + a_{n-1}c^{n-1} + \cdots + a_1 c + a_0} = \overline{0}$$

and using the properties of conjugates

$$\checkmark\,\overline{a_n}\,\overline{c}^n + \overline{a_{n-1}}\,\overline{c}^{n-1} + \cdots + \overline{a_1}\,\overline{c} + \overline{a_0} = \overline{0}\checkmark$$

Since $\overline{a} = a$ whenever a is real, ✓we now have

$$\checkmark\,a_n\,\overline{c}^n + a_{n-1}\,\overline{c}^{n-1} + \cdots + a_1\,\overline{c} + a_0 = 0\checkmark$$

that is,

$$f(\overline{c}) = 0$$

✓and so $\overline{c}$ is a root of $f(x)$. □

Part VI

Factoring Polynomials

Chapter 37

An Introduction to Polynomials

37.1 Objectives

The content objectives are:

1. Define *polynomial*, *coefficient*, $\mathbb{F}[x]$, *degree*, *zero polynomial*, *linear polynomial*, *quadratic polynomial*, *cubic polynomial*, *equal*, *sum*, *difference*, *product*, *quotient*, *remainder*, *polynomial division* and *factor*.
2. Define operations on polynomials.
3. State the *Division Algorithm for Polynomials*.

37.2 Polynomials

Our number systems were developed in response to the need to find solutions to real polynomials. We are now able to solve all equations of the form

$$a_2x^2 + a_1x + a_0 = 0$$

or

$$x^n - a_0 = 0$$

whether the coefficients are real or complex. In fact, a great deal more is known.

Let $\mathbb{F}$ be a field. Roughly speaking, a field is a set of numbers that allows addition, subtraction, multiplication and division. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$ and the integers modulo a prime p, $\mathbb{Z}_p$, are all fields. The integers are not a field because we cannot divide 2 by 4 and get an integer. Since division is just multiplication by an inverse, $\mathbb{Z}_6$ is not a field since $[3]$ has no inverse.

Most of us have seen polynomials in high school, and know how to add and multiply two polynomials, or divide one polynomial by another. Here, we will review and practice some of these skills. Let's start with a formal definition:

Definition 37.2.1
Polynomial

A **polynomial in** x over the field $\mathbb{F}$ is an algebraic expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $n \geq 0$ is an integer, and

- x is the **indeterminate**,
- the numbers $a_0, a_1, \ldots, a_n$ are called the **coefficients** of the polynomial,
- each individual expression of the form $a_i x^i$ is called a **term** of the polynomial.

The coefficients a_i belong to $\mathbb{F}$.

We use the notation $\mathbb{F}[x]$ to denote the set of all polynomials over a set $\mathbb{F}$, where typically, $\mathbb{F}$ is either $\mathbb{C}, \mathbb{R}$ or $\mathbb{Q}$.

REMARK

In most cases we will have polynomials whose coefficients are all complex number, that is, we have a **complex polynomial**, also known as a **polynomial over** $\mathbb{C}$.

In some cases, we will be interested in polynomials whose coefficients are all real numbers, that is, we have a **real polynomial**. Furthermore, we may also be interested in polynomials where all the coefficients are rational numbers, or where all the coefficients are integers, although $\mathbb{Z}$ is not a field.

Example 1

Here are some polynomials.

1. $2x^3 + (\sqrt{2} - i)x^2 - \frac{7\pi}{2}ix + (5 - 2i) \in \mathbb{C}[x]$. Here $a_3 = 2, a_2 = \sqrt{2} - i, a_1 = -\frac{7\pi}{2}i$ and $a_0 = 5 - 2i$. Notice that these are all complex numbers.
2. $x^2 + \sqrt{7}x - 1 \in \mathbb{R}[x]$. Note that since $\mathbb{R} \subsetneq \mathbb{C}$, all real polynomials are also polynomials over $\mathbb{C}$.
3. $\frac{1}{2}x^5 - \frac{5}{13}x^4 + x^3 - x^2 + 5x + \frac{3}{2} \in \mathbb{Q}[x]$. This is also a polynomial in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$.
4. $5x^4 + 0x^3 - 1x^2 + 0x - 2 \in \mathbb{Z}[x]$ (also in $\mathbb{Q}[x], \mathbb{R}[x]$ and $\mathbb{C}[x]$). We would usually express the term $1x^2$ simply as x^2, and omit the terms $0x^3$ and $0x$ from the polynomial expression, and simplify the polynomial as $5x^4 - x^2 - 2$.

Finally, note that $2x^3 + x^2 - \frac{7\pi}{2}ix + \sqrt{5} \notin \mathbb{R}[x]$ as at least one of the coefficients is not a real number. In fact, as we have

$$\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C},$$

we also get a similar relationship for the polynomials:

$$\mathbb{Z}[x] \subsetneq \mathbb{Q}[x] \subsetneq \mathbb{R}[x] \subsetneq \mathbb{C}[x].$$

37.2.1 Comparing Polynomials

Are the two polynomials $x^3 - x + \frac{1}{2}$ and $\ln(1)x^4 + \tan\left(\frac{\pi}{4}\right)x^3 - \sin(\pi)x^2 - e^0 x + \frac{\sqrt{4}}{4}$ the same? How would we compare two polynomials?

Definition 37.2.2
Degree of Polynomial

Let $n \geq 0$ be an integer. If $a_n \neq 0$ in the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

then the polynomial is said to have **degree** n. In other words, the degree of a polynomial is the largest exponent of x that has a non-zero coefficient.

The **zero** polynomial has all of its coefficients zero and its degree is not defined. Polynomials of degree 1 are called **linear** polynomials, of degree 2, **quadratic** polynomials, and of degree 3 **cubic** polynomials.

Example 2

Using some of the polynomials from the previous example,

1. $2x^3 + (\sqrt{2} - i)x^2 - \frac{7\pi}{2}ix + (5 - 2i)$ is a cubic polynomial.
2. $x^2 + \sqrt{7}x - 1$ is a quadratic polynomial.
3. $\frac{1}{2}x^5 - \frac{5}{13}x^4 + x^3 - x^2 + 5x + \frac{3}{2}$ is a polynomial of degree 5.

Note that the polynomial $0x^3 + 0x^2 + 1x + 0$ is actually linear as the largest exponent of x with a non-zero coefficient is 1.

In the following discussion, suppose all the coefficients of our polynomials are members of a set $\mathbb{F}$ (this could be $\mathbb{C}, \mathbb{R}, \mathbb{Q}$, etc.). We very frequently use $f(x)$ to denote an element of $\mathbb{F}[x]$ and write

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

Definition 37.2.3
Equal

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ both be polynomials in $\mathbb{F}[x]$.

The polynomials $f(x)$ and $g(x)$ are **equal** if and only if $a_i = b_i$ for all i.

Thus, $x^3 - x + \frac{1}{2}$ and $\ln(1)x^4 + \tan\left(\frac{\pi}{4}\right)x^3 - \sin(\pi)x^2 - e^0 x + \frac{\sqrt{4}}{4}$ are indeed the same polynomial.

37.3 Operations on Polynomials

Polynomials can be added, subtracted and multiplied as algebraic expressions exactly as you have done in high school.

Example 3

Polynomials are added "term-by-term", that is, we add the coefficients of the same powers of x.

1. In $\mathbb{R}[x]$, if $f(x) = x^2 + 7x - 1$ and $g(x) = 3x^4 - x^3 + 4x^2 - x + 5$ then $f(x) + g(x) = 3x^4 - x^3 + 5x^2 + 6x + 4$.
2. In $\mathbb{C}[x]$, if $f(x) = x^3 - 7ix + (5 - 2i)$ and $g(x) = (4 + 3i)x + (7 + 7i)$ then $f(x) + g(x) = x^3 + (4 - 4i)x + (12 + 5i)$.

Definition 37.3.1
Sum

The **sum** of the polynomials $f(x)$ and $g(x)$ is defined as

$$f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i$$

where $\deg(f(x)) = n$, $\deg(g(x)) = m$, and any "missing" terms have coefficient zero.

Definition 37.3.2
Difference

The **difference** of the polynomials $f(x)$ and $g(x)$ is defined as

$$f(x) - g(x) = \sum_{i=0}^{\max(n,m)} (a_i - b_i)x^i$$

where $\deg(f(x)) = n$, $\deg(g(x)) = m$, and any "missing" terms have coefficient zero.

Example 4

In $\mathbb{Z}_7[x]$, if $f(x) = [3]x^5 + [2]x^3 + [6]$ and $g(x) = [2]x^4 - [5]x^3 + [2]x^2 + [4]$ then $f(x) - g(x) = [3]x^5 - [2]x^4 - [2]x^2 + [2]$.

Exercise 1

Find the difference of each of the pairs of polynomials given in Example 3.

Example 5

(Polynomial Multiplication)

Polynomials are multiplied in a "distributive" manner, we just collect all of the terms having x^i that we would get through distributive multiplication.

In $\mathbb{R}[x]$, let $f(x) = x^2 + 7x - 1$ and $g(x) = 3x + 2$. We will compute the product $f(x) \cdot g(x)$ using long multiplication and see how it captures the definition of multiplication just given.

$$\begin{array}{rrrrrrrr}
 & & & x^2 & + & 7x & - & 1 \\
\times & & & & & 3x & + & 2 \\
\hline
 & & & 2x^2 & + & 14x & - & 2 \\
 & 3x^3 & + & 21x^2 & - & 3x & & \\
\hline
 & 3x^3 & + & 23x^2 & + & 11x & - & 2
\end{array}$$

The x^2 column simply displays the combinations of terms from $f(x)$ and $g(x)$ whose product gives x^2, that is $x^2 \times 2$, $7x \times 3x$ and 0×-1, which is exactly what the definition would give.

The definition of the product of two polynomials looks more complicated than it is.

Definition 37.3.3
Product

The **product** of the polynomials $f(x)$ and $g(x)$ is defined as

$$f(x) \cdot g(x) = \sum_{i=0}^{m+n} c_i x^i$$

where

$$c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 = \sum_{j=0}^{i} a_j b_{i-j}$$

Exercise 2

Find $f(x)g(x)$ for the two polynomials given.

1. Let $f(x)$ and $g(x)$ be the real polynomials $f(x) = 2x^4 + 6x^3 - x + 4$ and $g(x) = x^2 + 3$.
2. Let $f(z)$ and $g(z)$ be the complex polynomials $f(z) = iz^2 + (3-i)z + 2i$ and $g(z) = -iz + (2-2i)$.

Now we run into the same issue we had with the integers, division. Though it makes sense to say that $x-3$ divides $x^2 - 9$ since $x^2 - 9 = (x-3)(x+3)$, what do we do when there is a remainder? Just as we had a division algorithm for integers, we have a division algorithm for polynomials.

Proposition 1

(Division Algorithm for Polynomials (DAP))

If $f(x)$ and $g(x)$ are polynomials in $\mathbb{F}[x]$ and $g(x)$ is not the zero polynomial, then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x) \qquad \text{where } \deg r(x) < \deg g(x) \text{ or } r(x) = 0$$

Definition 37.3.4
Quotient, Remainder

The polynomial $q(x)$ is called the **quotient polynomial**. The polynomial $r(x)$ is called the **remainder polynomial**. If $r(x) = 0$, we say that $g(x)$ **divides** $f(x)$ or $g(x)$ is a **factor** of $f(x)$ and we write $g(x) \mid f(x)$.

How do we find the quotient and remainder polynomials? Long division.

Example 6 **(Long Division of Polynomials over $\mathbb{R}$)**

What are the quotient and remainder polynomials when $f(x) = 3x^4 + x^3 - 4x^2 - x + 5$ is divided by $g(x) = x^2 + 1$ in $\mathbb{R}[x]$?

Before we begin, we would expect from the Division Algorithm for Polynomials a remainder polynomial of degree at most one.

$$
\begin{array}{rrr|rrrrrrrrr}
 & & & & & & & 3x^2 & + & x & - & 7 \\
\cline{4-12}
x^2 & + & 1 & 3x^4 & + & x^3 & - & 4x^2 & - & x & + & 5 \\
 & & & 3x^4 & & & + & 3x^2 & & & & \\
\cline{4-12}
 & & & & & x^3 & - & 7x^2 & - & x & & \\
 & & & & & x^3 & & & + & x & & \\
\cline{6-12}
 & & & & & & - & 7x^2 & - & 2x & + & 5 \\
 & & & & & & - & 7x^2 & & & - & 7 \\
\cline{7-12}
 & & & & & & & & - & 2x & + & 12
\end{array}
$$

Thus, the quotient polynomial is $q(x) = 3x^2 + x - 7$ and the remainder polynomial is $r(x) = -2x + 12$ and $f(x) = q(x)g(x) + r(x)$.

Example 7 **(Long Division of Polynomials over $\mathbb{C}$)**

What are the quotient and remainder polynomials when
$f(z) = iz^3 + (2 + 4i)z^2 + (3 - i)z + (40 - 4i)$ is divided by $g(z) = iz + (2 - 2i)$ in $\mathbb{C}[x]$?

From the Division Algorithm for Polynomials, we would expect a constant remainder.

$$
\begin{array}{rrr|rrrrrrr}
 & & & & & z^2 & + & 6z & + & (11+9i) \\
\cline{4-10}
iz & + & (2-2i) & iz^3 & + & (2+4i)z^2 & + & (3-i)z & + & (40-4i) \\
 & & & iz^3 & + & (2-2i)z^2 & & & & \\
\cline{4-10}
 & & & & & 6iz^2 & + & (3-i)z & & \\
 & & & & & 6iz^2 & + & (12-12i)z & & \\
\cline{6-10}
 & & & & & & & (-9+11i)z & + & (40-4i) \\
 & & & & & & & (-9+11i)z & + & (40-4i) \\
\cline{8-10}
 & & & & & & & & & 0
\end{array}
$$

Thus, the quotient polynomial is $q(z) = z^2 + 6z + (11 + 9i)$ and the remainder is 0. Therefore, $g(z)$ divides $f(z)$.

Exercise 3 For each $f(x)$ and $g(x)$, find the quotient and remainder polynomials.

1. Let $f(x)$ and $g(x)$ be the real polynomials $f(x) = 2x^4 + 6x^3 - x + 4$ and $g(x) = x^2 + 3$.
2. Let $f(z)$ and $g(z)$ be the complex polynomials
   $f(z) = iz^3 + z^2 - (1 + i)z + 10$ and $g(z) = z + 2i$.

Chapter 38

Factoring Polynomials

38.1 Objectives

The content objectives are:

1. Define *polynomial equation*, *solution* and *root*.
2. State the Fundamental Theorem of Algebra.
3. State and prove the Rational Roots Theorem.
4. State and prove the Remainder Theorem and its corollaries.
5. State and prove the Conjugate Roots Theorem.
6. State and prove two propositions about factoring real polynomials.

38.2 Polynomial Equations

Definition 38.2.1
Polynomial Equation

A **polynomial equation** is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

which will often be written as $f(x) = 0$. An element $c \in \mathbb{F}$ is called a **root** or **zero** of the polynomial $f(x)$ if $f(c) = 0$. That is, c is a **solution** of the polynomial equation $f(x) = 0$.

The history of mathematics is replete with exciting and sometimes bizarre stories of mathematicians as they looked, in vain, for an algorithm that would find a root of an arbitrary polynomial. We can now prove that no such algorithm exists. It is known though, that a root exists for every complex polynomial. This was proved in 1799 by the brilliant mathematician Karl Friedrich Gauss.

Theorem 1

(Fundamental Theorem of Algebra (FTA))

For all complex polynomials $f(z)$ with $\deg(f(z)) \geq 1$, there exists a $z_0 \in \mathbb{C}$ so that $f(z_0) = 0$.

Ironically, we can prove a root exists, we just can't construct one in general. The proof of this fact and the Fundamental Theorem of Algebra are both demanding and are left for later courses.

We can use the Division Algorithm for Polynomials to help find roots though. Recall

Proposition 2 **(Division Algorithm for Polynomials (DAP))**

If $f(x)$ and $g(x)$ are polynomials in $\mathbb{F}[x]$ and $g(x)$ is not the zero polynomial, then there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

$$f(x) = q(x)g(x) + r(x) \qquad \text{where } \deg r(x) < \deg g(x) \text{ or } r(x) = 0$$

We can use the Division Algorithm for Polynomials to prove a very useful theorem.

Proposition 3 **(Remainder Theorem (RT))**

The remainder when the polynomial $f(x)$ is divided by $(x - c)$ is $f(c)$.

Example 1 Find the remainder when $f(z) = 3z^{12} - 8iz^5 + (4 + i)z^2 + z + 2 - 3i$ is divided by $z + i$.

Solution: One could do the painful thing and carry out long division. Another possibility is to use the Remainder Theorem and compute $f(-i)$.

$$\begin{aligned} f(-i) &= 3(-i)^{12} - 8i(-i)^5 + (4 + i)(-i)^2 + (-i) + 2 - 3i \\ &= 3 - 8i(-i) + (4 + i)(-1) - i + 2 - 3i \\ &= 3 - 8 - 4 - i - i + 2 - 3i \\ &= -7 - 5i \end{aligned}$$

The remainder is $-7 - 5i$.

Proof: By the Division Algorithm for Polynomials, there exist unique polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x)(x - c) + r(x) \qquad \text{where } \deg r(x) < 1 \text{ or } r(x) = 0$$

Therefore, the remainder $r(x)$ is a constant (which could be zero) which we will write as r_0. Hence

$$f(x) = q(x)(x - c) + r_0$$

Substituting $x = c$ into this equation gives $f(c) = r_0$. $\square$

Corollary 4 **(Factor Theorem 1 (FT 1))**

The linear polynomial $(x - c)$ is a factor of the polynomial $f(x)$ if and only if $f(c) = 0$.

Equivalently,

Corollary 5 **(Factor Theorem 2 (FT 2))**

The linear polynomial $(x-c)$ is a factor of the polynomial $f(x)$ if and only if c is a root of the polynomial $f(x)$.

Induction, together with the Fundamental Theorem of Algebra and the Factor Theorems, allow us to prove the following very useful corollary.

Proposition 6 **(Complex Polynomials of Degree n Have n Roots (CPN))**

If $f(z)$ is a complex polynomial of degree $n \geq 1$, then $f(z)$ has n roots and can be written as the product of n linear factors. The n roots and factors may not be distinct.

Exercise 1 Prove the proposition Complex Polynomials of Degree n Have n Roots.

How do we go about actually factoring polynomials? In general, this is hard to do. There are no formulas for roots if the polynomial has degree five or more. But if the polynomial has integer coefficients, we have a good starting point.

Theorem 7 **(Rational Roots Theorem (RRT))**

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ be a polynomial with integer coefficients. If $\frac{p}{q}$ is a rational root with $\gcd(p,q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

In order to find a rational root of $f(x)$, we only need to examine a *finite* set of rational numbers, those whose numerator divides the constant term and those whose denominator divides the leading coefficient. Note that the theorem only suggests those rational numbers that *might* be roots. It does not guarantee that any of these numbers are roots.

Example 2 If possible, find a rational root of $f(x) = 2x^4 + x^3 + 6x + 3$.

Solution: We will use the Rational Roots Theorem. The divisors of 2 are ± 1 and ± 2. The divisors of 3 are ± 1 and ± 3. Hence, the candidates for rational roots are

$$\pm 1, \pm \frac{1}{2}, \pm 3, \pm \frac{3}{2}$$

Now test each of these candidates.

x	1	-1	$\frac{1}{2}$	$\frac{-1}{2}$	3	-3	$\frac{3}{2}$	$\frac{-3}{2}$
$f(x)$	12	-2	$\frac{25}{4}$	0	210	120	$\frac{51}{2}$	$\frac{3}{4}$

Thus, the only rational root is $\frac{-1}{2}$.

Proof: If $\dfrac{p}{q}$ is a root of $f(x)$ then

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_2\left(\frac{p}{q}\right)^2 + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

Multiplying by q^n gives

$$a_np^n + a_{n-1}p^{n-1}q + \cdots + a_2p^2q^{n-2} + a_1pq^{n-1} + a_0q^n = 0$$

and

$$a_np^n = -q\left(a_{n-1}p^{n-1} + \cdots + a_2p^2q^{n-3} + a_1pq^{n-2} + a_0q^{n-1}\right)$$

Since all of the symbols in this equation are integers, both the right hand side and left hand side are integers. Since q divides the the right hand side, q divides the left hand side, that is

$$q \mid a_np^n$$

Since $\gcd(p, q) = 1$ we can repeatedly use the proposition on Coprimeness and Divisibility to show that $q \mid a_n$. In a similar way, we can show that $p \mid a_0$. $\square$

Exercise 2 Is $x+1$ a factor of $x^{10}+1$, of x^9+1? When does $x+1$ divide (or not divide) $x^{2n}+1$ for n a positive integer? When does $x+1$ divide (or not divide) $x^{2n+1}+1$ for n a positive integer?

Exercise 3 Prove that if p is a prime, then $\sqrt[n]{p}$ is irrational for any integer $n > 1$.

The next, very useful theorem is like a "two for one special". If you find one complex root of a real polynomial, you get another one for free.

Theorem 8 **(Conjugate Roots Theorem (CJRT))**

Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with real coefficients. If $c \in \mathbb{C}$ is a root of $f(x)$, then $\bar{c} \in \mathbb{C}$ is a root of $f(x)$.

Example 3 Let $f(x) = x^4 - x^3 - 5x^2 - x - 6$. Given that i is a root of $f(x)$, factor $f(x)$.

Solution: Since $f(x)$ is a polynomial with real coefficients, we can use the Conjugate Roots Theorem. Thus, i and $-i$ are both roots and, by the Factor Theorem 2, $(x-i)$ and $(x+i)$ are factors of $f(x)$. The product of these two factors is x^2+1. Dividing $f(x)$ by x^2+1 yields x^2-x-6 which factors as $(x-3)(x+2)$. Thus

$$f(x) = (x-i)(x+i)(x-3)(x+2)$$

Proof: Since c is a root of $f(x)$

$$a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 = 0$$

Taking the complex conjugate of both sides gives

$$\overline{a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0} = \overline{0}$$

and using the properties of conjugates

$$\overline{a_n}\, \overline{c}^n + \overline{a_{n-1}}\, \overline{c}^{n-1} + \cdots + \overline{a_1}\, \overline{c} + \overline{a_0} = \overline{0}$$

Since $\overline{a} = a$ whenever a is real, we now have

$$a_n\, \overline{c}^n + a_{n-1}\, \overline{c}^{n-1} + \cdots + a_1\, \overline{c} + a_0 = 0$$

that is,

$$f(\overline{c}) = 0$$

and so $\overline{c}$ is a root of $f(x)$. □

Exercise 4 If $x + (2 + i)$ is a factor of $f(x) = x^4 + 4x^3 + 2x^2 - 12x - 15$, factor $f(x)$ into products of real polynomials and complex polynomials of lowest degree.

The Conjugate Roots Theorem has a very useful corollary.

Corollary 9 **(Real Quadratic Factors (RQF))**

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with real coefficients. If $c \in \mathbb{C}$, $\Im(c) \neq 0$, is a root of $f(x)$, then there exists a real quadratic factor of $f(x)$ with c as a root.

Proof: Let $c \in \mathbb{C}$, $\Im(c) \neq 0$, be a root of $f(x)$. By the Conjugate Roots Theorem, $\overline{c}$ is also a root of $f(x)$. Consider

$$q(x) = (x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c} = x^2 - 2\Re(c)x + |c|^2$$

where the last equality follows from Properties of Conjugates and Properties of Modulus. Since $-2\Re(c) \in \mathbb{R}$ and $|c|^2 \in \mathbb{R}$, $q(x)$ is a real quadratic polynomial with c as a root. □

This corollary is useful in characterizing the factorization of all real polynomials.

Theorem 10 **(Real Factors of Real Polynomials (RFRP))**

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with real coefficients. Then $f(x)$ can be written as a product of real linear and real quadratic factors.

Proof: Complex polynomials of degree n have n roots. Those roots which are real correspond to real linear factors. Those roots which are not real come in conjugate pairs (Conjugate Roots Theorem) and give rise to real quadratic polynomials (Real Quadratic Factors). Since real and not real roots exhaust all possible choices of roots, real linear and real quadratic factors exhaust all possible types of factors of least degree. □

Chapter 39

Practice, Practice, Practice: Polynomials

39.1 Objectives

This class provides an opportunity to practice factoring polynomials.

39.2 Worked Examples

Example 1 For each of the following, you are given several roots of a polynomial $f(x)$. Find a polynomial of lowest degree in $\mathbb{F}[x]$ that has the given roots.

1. $\mathbb{R}[x]$: $3+\sqrt{2}i$, 5

   Solution: Since we are looking for a polynomial in $\mathbb{R}[x]$, we can use the Conjugate Roots Theorem for complex roots. Hence, $3+\sqrt{2}i \notin \mathbb{R}$ will be paired with its conjugate $3-\sqrt{2}i$. The product of the corresponding factors will produce a real quadratic. Hence,

$$\begin{aligned} f(x) &= (x-(3+\sqrt{2}i))(x-(3-\sqrt{2}i))(x-5) \\ &= (x^2-6x+11)(x-5) \\ &= x^3-11x^2+41x-55 \end{aligned}$$

2. $\mathbb{C}[x]$: $3+\sqrt{2}i$, 5

   Solution: Since both $3+\sqrt{2}i$ and 5 are complex numbers, the corresponding linear factors are in $\mathbb{C}[x]$ so

$$f(x) = (x-(3+\sqrt{2}i))(x-5) = x^2+(-8+\sqrt{2}i)x+(15+5\sqrt{2}i)$$

3. $\mathbb{R}[x]$: $1-\sqrt{5}$, $2i$, 0

   Solution: Since we are looking for a polynomial in $\mathbb{R}[x]$, we can use the Conjugate Roots Theorem for complex roots. The only root not in $\mathbb{R}$ is $2i$ so we need to pair this root with its conjugate $-2i$. The product of the corresponding factors will produce a real quadratic. Hence,

$$\begin{aligned} f(x) &= (x-(1-\sqrt{5}))(x-2i)(x+2i)(x-0) \\ &= (x-(1-\sqrt{5}))(x^2+4)x \\ &= (x-(1-\sqrt{5}))(x^3+4x) \\ &= x^4+(-1+\sqrt{5})x^3+4x^2+4(-1+\sqrt{5})x \end{aligned}$$

4. $\mathbb{Z}_7[x]$: $[2]$, $[1]$

   Solution: Both $[2]$, $[1]$ correspond to linear factors so

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

Example 2 For each of the following polynomials $f(x) \in \mathbb{F}[x]$, factor $f(x)$ into factors with degree as small as possible over $\mathbb{F}[x]$. Cite appropriate propositions to justify each step of your reasoning.

1. $f(x) = x^2 - x - 6 \in \mathbb{Q}[x]$

   Solution: The quadratic formula gives the roots 3 and -2. These are values in $\mathbb{Q}$ so there are linear factors $x-3$ and $x+2$ by Factor Theorem 2. Hence,

$$f(x) = (x-3)(x+2)$$

2. $f(x) = x^2 - x + 6 \in \mathbb{Q}[x]$

   Solution: The quadratic formula gives only complex roots in this instance. Since complex numbers do not belong to $\mathbb{Q}$ there are no linear factors in $\mathbb{Q}[x]$, hence $f(x) = x^2 - x + 6$ cannot be factored any further in $\mathbb{Q}[x]$.

3. $f(x) = x^2 - 3ix - 2 \in \mathbb{C}[x]$

   Solution: Applying the quadratic formula gives two roots, i and $2i$, hence

$$f(x) = x^2 - 3ix - 2 = (x-i)(x-2i)$$

4. $f(x) = 2x^3 - 3x^2 + 2x + 2 \in \mathbb{R}[x]$

   Solution: Since all of the coefficients are integers, we can use the Rational Roots Theorem. The divisors of a_0 are $\{\pm 1, \pm 2\}$ and the divisors of a_n are $\{\pm 1, \pm 2\}$ so the only candidates for rational roots are

$$\pm 1, \pm 2, \pm\frac{1}{2}$$

   Now test each of these candidates.

x	1	-1	2	-2	$\frac{1}{2}$	$\frac{-1}{2}$
$f(x)$	3	-5	10	-30	$5/2$	0

Long division produces

$$f(x) = (2x+1)(x^2 - 2x + 2)$$

The quadratic formula gives two complex roots for $x^2 - 2x + 2$ so the quadratic does not factor any further.

5. $f(x) = z^4 + 27z \in \mathbb{C}[x]$

Solution: Since $f(z)$ is a complex polynomial of degree four, it will have four linear factors. Now $f(z) = z(z^3 + 27)$. Factoring $z^3 + 27$ can be done with the aid of the Complex n-th Roots Theorem applied to $z^3 = -27$. First, we write -27 in polar form as

$$-27 = 27(\cos\pi + i\sin\pi)$$

Using the Complex n-th Roots Theorem the solutions are

$$\begin{aligned} &\sqrt[3]{27}\left(\cos\left(\frac{\pi+2k\pi}{3}\right) + i\sin\left(\frac{\pi+2k\pi}{3}\right)\right) && \text{for } k = 0,1,2 \\ &= 3\left(\cos\left(\frac{\pi}{3} + \frac{2k\pi}{3}\right) + i\sin\left(\frac{\pi}{3} + \frac{2k\pi}{3}\right)\right) && \text{for } k = 0,1,2 \end{aligned}$$

The three distinct roots are given below

$$\begin{aligned} &\text{When } k=0,\ z_0 = 3\left(\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right) = 3\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{3}{2} + \frac{3\sqrt{3}}{2}i \\ &\text{When } k=1,\ z_1 = 3\left(\cos\pi + i\sin\pi\right) = -3 \\ &\text{When } k=2,\ z_2 = 3\left(\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right)\right) = 3\left(\frac{1}{2} + \frac{-\sqrt{3}}{2}i\right) = \frac{3}{2} - \frac{3\sqrt{3}}{2}i \end{aligned}$$

Thus,

$$f(x) = x(x+3)\left(x - \left(\frac{3}{2} + \frac{3\sqrt{3}}{2}i\right)\right)\left(x - \left(\frac{3}{2} - \frac{3\sqrt{3}}{2}i\right)\right)$$

Example 3

Factor $f(x) = 3x^4 - 5x^3 + x^2 - 5x - 2$ over $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

Solution: Since all of the coefficients are integers, we can use the Rational Roots Theorem. The divisors of a_0 are $\{\pm1, \pm2\}$ and the divisors of a_n are $\{\pm1, \pm3\}$ so the only candidates for rational roots are

$$\pm1, \pm2, \pm\frac{1}{3}, \pm\frac{2}{3}$$

Now test each of these candidates.

x	1	-1	2	-2	$\frac{1}{3}$	$\frac{-1}{3}$	$\frac{2}{3}$	$\frac{-2}{3}$
$f(x)$	-8	-12	0	100	$\frac{-100}{27}$	0	$\frac{-156}{27}$	$\frac{104}{27}$

Since 2 and $\frac{-1}{3}$ are roots, $x - 2$ and $x + \frac{1}{3}$ (or $3x + 1$) are factors. We can perform long division with $f(x)$ and the divisor $(x-2)(3x+1) = 3x^2 - 5x - 2$ to get

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

Since x^2+1 cannot be factored in $\mathbb{R}[x]$, the factorizations are

$$f(x) = (x-2)(3x+1)(x^2+1) \in \mathbb{R}[x]$$

and

$$f(x) = (x-2)(3x+1)(x-i)(x+i) \in \mathbb{C}[x]$$

39.3 Quiz

Example 4 (20 marks) Let $f(z) = z^6 + 4z^4 + z^2 + 4$. If $f(2i) = 0$, factor $f(z)$ into factors with degree as small as possible over $\mathbb{C}[x]$.

Solution: Over $\mathbb{C}$, a polynomial of degree six will have six linear factors.✓Since all of the coefficients of $f(z)$ are real, the Conjugate Roots Theorem applies.✓Since $2i$ is a root, $-2i$ is also a root. ✓Thus

$$(z-2i)(z+2i) = z^2+4$$

is a factor of $f(z)$.✓Long division produces

$$f(z) = z^6+4z^4+z^2+4 = (z^2+4)(z^4+1)\checkmark\checkmark$$

We now factor z^4+1 using the Complex n-th Roots Theorem ✓applied to $z^4 = -1$. First, we write -1 in polar form as

$$-1 = 1(\cos\pi + i\sin\pi)\checkmark$$

$$\begin{aligned}
&\sqrt[4]{1}\left(\cos\left(\frac{\pi+2k\pi}{4}\right) + i\sin\left(\frac{\pi+2k\pi}{4}\right)\right) && \text{for } k = 0,1,2,3\checkmark\checkmark \\
&= \cos\left(\frac{\pi}{4}+\frac{k\pi}{2}\right) + i\sin\left(\frac{\pi}{4}+\frac{k\pi}{2}\right) && \text{for } k = 0,1,2,3
\end{aligned}$$

The four distinct roots are given below

$$\begin{aligned}
&\text{When } k=0,\ z_0 = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\checkmark\checkmark \\
&\text{When } k=1,\ z_0 = \cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right) = \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\checkmark\checkmark \\
&\text{When } k=2,\ z_0 = \cos\left(\frac{5\pi}{4}\right) + i\sin\left(\frac{5\pi}{4}\right) = \frac{-1}{\sqrt{2}} + \frac{-i}{\sqrt{2}}\checkmark\checkmark \\
&\text{When } k=3,\ z_0 = \cos\left(\frac{7\pi}{4}\right) + i\sin\left(\frac{7\pi}{4}\right) = \frac{1}{\sqrt{2}} + \frac{-i}{\sqrt{2}}\checkmark\checkmark
\end{aligned}$$

Thus,

$$f(z) = (z-2i)(z+2i)(z-z_0)(z-z_1)(z-z_2)(z-z_3)\checkmark\checkmark$$

where the z_i are defined above.

39.4 Practice

1. For each of the following polynomials $f(x) \in \mathbb{F}[x]$,

   (i) Find all of the roots in the given field $\mathbb{F}$.

   (ii) Factor $f(x)$ into factors with degree as small as possible over $\mathbb{F}[x]$.

   (a) $x^4 - 4 \in \mathbb{Q}[x]$
   (b) $x^4 - 4 \in \mathbb{R}[x]$
   (c) $x^4 - 4 \in \mathbb{C}[x]$
   (d) $x^4 - [4] \in \mathbb{Z}_5[x]$
   (e) $x^4 - a^4 \in \mathbb{F}[x]$ where $a \in \mathbb{F}$, $a \neq 0$

2. For each of the following polynomials $f(x) \in \mathbb{F}[x]$, factor $f(x)$ into factors with degree as small as possible over $\mathbb{F}[x]$. Cite appropriate propositions to justify each step of your reasoning.

   (a) $x^2 - 2x + 2 \in \mathbb{C}[x]$
   (b) $x^2 + (-3i + 2)x - 6i \in \mathbb{C}[x]$
   (c) $2x^3 - 3x^2 + 2x + 2 \in \mathbb{R}[x]$
   (d) $3x^4 + 13x^3 + 16x^2 + 7x + 1 \in \mathbb{R}[x]$ (from Gilbert)
   (e) $z^4 + 27z \in \mathbb{C}[x]$

3. Let $z \in \mathbb{C}$. Prove that $(x - z)(x - \overline{z}) \in \mathbb{R}[x]$. Hence, prove that all real polynomials can be factored into a product of real linear and real quadratic polynomials.

4. (*Conjugate Roots Theorem Extended* (CJRE)) Let $\mathbb{F}$ be a field, $k \in \mathbb{F}$ but $\sqrt{k} \notin \mathbb{F}$. Define $\mathbb{F}(k)$ as follows.
$$\mathbb{F}(k) = \{a + b\sqrt{k} \mid a, b \in \mathbb{F}\}$$

   (a) Prove that there are solutions to $x^2 = k$ in $\mathbb{F}(k)$.
   (b) Let $c \in \mathbb{F}(k)$. Thinking of the complex numbers, make an analogous definition of the *conjugate* of c, $\overline{c}$, in $\mathbb{F}(k)$.
   (c) Prove that $\overline{x + y} = \overline{x} + \overline{y}$ in $\mathbb{F}(k)$.
   (d) Prove that $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$ in $\mathbb{F}(k)$.
   (e) Let $f(x) \in \mathbb{F}(x)$. Prove that if $c \in \mathbb{F}(k)$ is a root of $f(x)$, then $\overline{c}$ is also a root.
   (f) Find a polynomial in $\mathbb{Q}[x]$ with the root $2 - \sqrt{7}$.

5. Is $\sqrt{3} + \sqrt{5}$ rational or irrational? Provide compelling evidence for your answer.

Part VII

Applying the Fundamentals: Functions, Bijections and Counting

Chapter 40

Compositions and Bijections

40.1 Objectives

The content objectives are:

1. Define *injection*.
2. Read and discover proofs that specified functions are injections.
3. Define *bijection*.

40.2 Functions, Surjections and Injections

Earlier, we learned about nested quantifiers and used them to define the concept of functions, surjections and injections. Here is a quick summary of the definitions.

Definition 40.2.1
Function, Surjective, Injective, Bijective

Let S and T be two sets.

A **function** f from S to T, denoted by $f : S \to T$, is a rule that assigns to each element $s \in S$ a unique element $f(s) \in T$. The set S is called the **domain** of the function and the set T is called the **codomain**. The element $f(s)$ is called the **value** of the function f at s.

A function $f : S \to T$ is **surjective** (or **onto**) if and only if for every $y \in T$ there exists an $x \in S$ so that $f(x) = y$.

A function $f : S \to T$ is **injective** (or **one-to-one**) if and only if for every $x_1 \in S$ and every $x_2 \in S$, $f(x_1) = f(x_2)$ implies that $x_1 = x_2$.

Symbolically, we can write out these definitions a follows.

REMARK

A rule $f : S \to T$ is a function if and only if

$$\forall s \in S \ \exists! t \in T, \ f(s) = t$$

where the exclamation mark after the existential quantifier means unique.

A function $f : S \to T$ is surjective if and only if

$$\forall t \in T \ \exists s \in S, \ f(s) = t$$

A function $f : S \to T$ is injective if and only if

$$\forall x_1 \in S \ \forall x_2 \in S, \ f(x_1) = f(x_2) \implies x_1 = x_2$$

Equivalently, a function $f : S \to T$ is injective if and only if

$$\forall x_1 \in S \ \forall x_2 \in S, \ x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

In prose, we can say the following.

REMARK

Suppose f is a rule that defines a mapping from set S to set T.

- f is a function if it assigns to each element $s \in S$ exactly one element $f(s) \in T$.
- f is surjective if, for each element $t \in T$, there is at *least* one element $s \in S$ so that $f(s) = t$.
- f is injective if, for each element $t \in T$, there is at *most* one element $s \in S$ so that $f(s) = t$.

40.3 Composition of Functions

We may combine two functions to create a third function using the concept of composition of functions defined below:

Definition 40.3.1
Composition of Functions

Suppose S, T and V are three sets, and $f : T \to V$ and $g : S \to T$ are two functions. Then we may define the **composite function** $f \circ g : S \to V$, given by

$$f \circ g(x) = f\left(g(x)\right) \text{ for all } x \in S.$$

Note that for the composition $f \circ g$ to be defined, the codomain of g must be equal of the domain of f. As a consequence, the composition $g \circ f$ may not be defined unless the codomain of f is equal to the domain of g. Therefore $f \circ g$ and $g \circ f$ are quite different.

40.3.1 Composing onto functions

Mathematics makes great use of the composition of functions. The next proposition, whose proof may be intimidating the first time you see it, states that the composition of onto functions is also onto.

Proposition 1 Let $f : T \to V$ and $g : S \to T$ be onto functions. Then $f \circ g$ is an onto function.

Analysis of Proof The definition of *onto* uses nested quantifiers.

Hypothesis: $f : T \to V$ and $g : S \to T$ are both onto functions.

Conclusion: $f \circ g$ is onto.

Core Proof Technique: Nested quantifiers.

Preliminary Material: Let us recast the definition of *onto* for $f \circ g$. To do this we need to be aware of the fact that $f : T \to V$ and $g : S \to T$ and $f \circ g : S \to V$. So the statement we need to prove is:

For every $y \in V$ there exists $x \in S$ so that $f(g(x)) = y$.

There are three instances of *onto* in the proposition. Two occur in the hypothesis and are associated with the functions f and g. The third occurs in the conclusion and is associated with the function $f \circ g$. That is the one that interests us right now. The definition of *onto* begins with a universal qualifier. So we will use the Select Method applied to $f \circ g$. Using our proof template we have the following.

Proof in Progress

1. Let $y \in V$.
2. Consider the object x. *We must construct the object x.*
3. First, we show that $x \in S$. *To be completed.*
4. Now we show that $f(g(x)) = y$. *To be completed.*

Constructing x seems difficult. We do not know what the sets S, T and V are and we have no idea what the functions f and g look like. But we have not made use of our hypotheses at all so let's see if they can give us any ideas.

Since $f : T \to V$ is onto, we know that for any $u \in V$, there exists a $t \in T$ so that $f(t) = u$.

Since $g : S \to T$ is onto, we know that for any $t \in T$, there exists an $s \in S$ so that $g(s) = t$.

How does y fit in? Observe that $y \in V$. But $f : T \to U$ and is onto, so there exists a $t' \in T$ so that $f(t') = y$. Since $t' \in T$ and $g : S \to T$ is onto, there exists an $s' \in S$ so that $g(s') = t'$.

But what have we constructed? If we let $x = s'$ then we have an element that maps from S to T and then from T to V for which $f(g(s')) = y$. Let's record these thoughts.

Proof in Progress

1. Let $y \in V$.
2. Since $f : T \to V$ is onto, there exists a $t' \in T$ so that $f(t') = y$.
3. Since $t' \in T$ and $g : S \to T$ is onto, there exists an $s' \in S$ so that $g(s') = t'$.
4. Hence, there exists $s' \in S$ so that $f(g(s')) = f(t') = y$.
5. Hence, there exists $x \in S$ so that $f(g(x)) = y$.

Notice that our last two lines are essentially duplicates. When doing rough work, this is common. However, when writing up a proof, such duplications should be removed, consistent notation should be enforced and omitted steps should be included. In this case, the proof is almost done for us.

Proof: Let y in V. Since $f : T \to V$ is onto, there exists a $t' \in T$ so that $f(t') = y$. Since $t' \in T$ and $g : S \to T$ is onto, there exists an $s' \in S$ so that $g(s') = t'$. Hence, there exists $s' \in S$ so that $f(g(s')) = f(t') = y$. $\square$

40.3.2 Composing one-to-one functions

The next proposition asserts that the composition of one-to-one functions is also one-to-one.

Proposition 2 Let $f : T \to U$ and $g : S \to T$ be one-to-one functions. Then $f \circ g$ is a one-to-one function.

Analysis of Proof The definition of *one-to-one* uses nested quantifiers.

Hypothesis: $f : T \to U$ and $g : S \to T$ are both one-to-one functions.

Conclusion: $f \circ g$ is one-to-one.

Core Proof Technique: Nested quantifiers.

Preliminary Material: Let us recast the definition of *one-to-one* for $f \circ g$.

> For every $x_1 \in S$ and every $x_2 \in S$, $(f \circ g)(x_1) = (f \circ g)(x_2)$ implies that $x_1 = x_2$.

There are three instances of *one-to-one* in the proposition. Two occur in the hypothesis and are associated with the functions f and g. The third occurs in the conclusion and is associated with the function $f \circ g$. Let's use the structure of a one-to-one proof as our starting point.

Proof in Progress

1. Let $x_1, x_2 \in S$.
2. Suppose that $(f \circ g)(x_1) = (f \circ g)(x_2)$.
3. Now we show that $x_1 = x_2$.
4. *To be completed.*
5. Hence, $x_1 = x_2$ as required.

Since f and g are not specified, this may seem impossible. But let's "follow our nose" and see what happens. Since $(f \circ g)(x_1) = (f \circ g)(x_2)$, we know that $f(g(x_1)) = f(g(x_2))$. But since f is one-to-one, we know that $g(x_1) = g(x_2)$. If this seems confusing, since f is one-to-one, $f(y_1) = f(y_2)$ implies $y_1 = y_2$. In this case, $y_1 = g(x_1)$ and $y_2 = g(x_2)$. Now back to $g(x_1) = g(x_2)$. Since g is one-to-one, we know that $x_1 = x_2$, which is exactly what we needed to show.

A proof might look like the following.

Proof: Let $x_1, x_2 \in S$. Suppose that $(f \circ g)(x_1) = (f \circ g)(x_2)$. Since $(f \circ g)(x_1) = (f \circ g)(x_2)$, we know that $f(g(x_1)) = f(g(x_2))$. Since f is one-to-one, we know that $g(x_1) = g(x_2)$. And since g is one-to-one, $x_1 = x_2$ as required. □

40.4 Bijections

An extraordinarily useful class of functions is described next.

Definition 40.4.1
Bijective

A function $f : S \to T$ is **bijective** if and only if f is both surjective and injective.

Example 1

Here are a few examples that we have already discussed in previous chapters.

1. We have already shown that for $m \neq 0$ and b a fixed real numbers, the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = mx + b$ is both surjective and injective. Hence, f is bijective.
2. We have shown that the function $f : [1, 2] \to [4, 7]$ defined by $f(x) = x^2 + 3$ is both one-to-one and onto, and is thus a bijection. However, the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2 + 3$ is neither one-to-one nor onto.

40.4.1 Inverses

There are many instances in mathematics when *undoing* an operation is very useful. Subtraction undoes addition. Division undoes multiplication. Taking a square root undoes the operation of squaring. Here is a way to generalize all such *undoings*.

Definition 40.4.2
Inverse

If $f : S \to T$ and $g : T \to S$ are functions that satisfy

- for every $s \in S$, $g(f(s)) = s$, and
- for every $t \in T$, $f(g(t)) = t$

then g is called the **inverse** of f and we write $g = f^{-1}$.

A common mistake is to assume that the inverse is the reciprocal. The inverse of the function $f(x) = x^2$ is $f^{-1} = \sqrt{x}$, not $f^{-1} = 1/x^2$.

Example 2

The inverse of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = mx + b$ is the function $g(x) = (x - b)/m$. Let's verify that the two defining properties of an inverse hold.

For every $s \in \mathbb{R}$,

$$g(f(s)) = \frac{(ms + b) - b}{m} = s$$

as required, and for every $t \in \mathbb{R}$,

$$f(g(t)) = m\frac{t - b}{m} + b = t$$

as required.

It is not surprising that the function f in our example is bijective. The following theorem, which we will not prove, establishes the fact that inverses only exist for bijective functions.

Theorem 3

(Inverse Theorem)

A function has an inverse if and only if the function is bijective.

Bijections are commonly used in calculus to identify invertible functions. Bijections are used in linear algebra and group theory to show that two algebraic structures, which may look very different, are essentially the same. We will use bijections to count.

40.5 More Examples

1. (a) Let f map from the set of country names to the letters of the alphabet be defined by taking as the image of the name of the country the first letter of the name. For example, $f(\text{Canada}) = C$. Prove that f is a bijection or show by counterexample that it is not. You will find the list of countries at `http://en.wikipedia.org/wiki/List_of_sovereign_states` helpful.

   (b) Let $f : \mathbb{Z}_m \setminus \{[0]\} \to \mathbb{Z}_m \setminus \{[0]\}$ be defined by $f([x]) = [x]^{-1}$. For each of the following, prove that f is a bijection or show by counterexample that it is not.

      i. $m = 5$
      ii. $m = 6$

Solution:

(a) Since $f(\text{Albania}) = A$ and $f(\text{Algeria}) = A$, f is not injective and hence not a bijection.

(b) Let $f : \mathbb{Z}_m \setminus \{[0]\} \to \mathbb{Z}_m \setminus \{[0]\}$ be defined by $f([x]) = [x]^{-1}$.

i. $m = 5$
The function f is explicitly listed below.

$[x]$	$[1]$	$[2]$	$[3]$	$[4]$
$[x]^{-1}$	$[1]$	$[3]$	$[2]$	$[4]$

By inspection, f is bijective.

ii. $m = 6$
This rule fails in several regards. Most basically, it is not defined for $[x] = [2]$, so f is not a function. It is also not surjective since no element maps to $[2]$.

40.6 Practice

1. For each of the following mappings f, first determine whether or not f is a function. If f is a function, determine whether or not f is surjective, injective or bijective. In all cases, provide reasons for your answer.

   (a) Let S be the set of words in the English language. Let T be the English alphabet, that is, $T = \{a, b, c, \ldots, z\}$. The mapping $f : S \to T$ maps a word to the word's first letter. For example, $f(\text{mathematics}) = m$.

   (b) Let $f : \mathbb{N} \to \mathbb{N}$ be defined by
   $$f(n) = \sum_{d|n} d$$
   That is, n maps to the sum of the divisors of n.

   (c) Let $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ be defined by $f(x) = [3]x$.

2. Prove the following statement: If f and g are bijections, then $f \circ g$ is a bijection.

3. Suppose X, Y and Z are three sets. Let $f : X \to Y$ and $g : Y \to Z$ be two functions. Prove or disprove the following.

   (a) If g is onto, then $g \circ f : X \to Z$ is onto.

   (b) If $g \circ f$ is onto, then g is onto.

4. Let $\mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}$. If $k, \ell \in \mathbb{Z}$ are fixed, when is $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(x, y) = kx + \ell y$, a bijection?

Chapter 41

Counting

41.1 Objectives

The content objectives are:

1. Define what it means for two sets to have the same cardinality.
2. State and prove the *Cardinality of Disjoint Sets*.
3. State and prove the *Cardinality of Intersecting Sets*.

41.2 African Shepherds

Many, many years ago, Dr. Furino lived high up in the mountains of southern Africa. Herd boys would be sent with their flocks of sheep and goats to the high pastures to allow the animals to graze. The herd boys were uneducated, and very few knew how to "count". So, how did they know if they had the right number of animals at any given time? An animal might get lost at night, be out of sight among the ridges during the day, or be taken by jackals.

Before the herd boys were sent out from their family compounds they would be given a very small bag that contained pebbles, one pebble for each animal. So, to "count" the animals, they would simply match up a pebble against each animal they could see. If there were more pebbles than animals, an animal was missing. If there were more animals than pebbles, another animal had joined their flock, presumably from a nearby herd. If there was exactly one pebble for each animal, the herd boy had the correct number of animals.

The herd boys "counted" by forming a bijection between the set of pebbles in their bag and the set of animals in their flock. When we count by saying $1, 2, 3, \ldots$ we are creating a bijection between a subset of the integers and the set of objects we are counting. Now, how do we formalize this idea?

41.3 What Does It Mean To Count?

Recall that we used the notation $|S|$ to mean the cardinality, or number of elements, in the set S. Now it is time to be clear about what that really means.

Definition 41.3.1 **Cardinality**

If there exists a bijection between the sets S and T, we say that the sets have the same **cardinality** and we write $|S| = |T|$.

Let $\mathbb{N}_n$ denote the set of all natural numbers less than or equal to n.

- $\mathbb{N}_0 = \emptyset$
- $\mathbb{N}_1 = \{1\}$
- $\mathbb{N}_2 = \{1, 2\}$
- $\mathbb{N}_3 = \{1, 2, 3\}$
- $\mathbb{N}_n = \{1, 2, 3, \ldots, n\}$

Definition 41.3.2 **Number of Elements, Finite, Infinite**

If there exists a bijection between a set S and $\mathbb{N}_n$, we say that the **number of elements** in S is n, and we write $|S| = n$. Moreover, we also say that S is a **finite set**. If no bijection exists between a set S and $\mathbb{N}_n$ for any n, we say that S is an **infinite set**.

This formal definition corresponds exactly to what herd boys do with pebbles, what children do when "counting" on fingers, and what we do when "counting" with the words "one, two, three". This definition extends the bijection notion to infinite sets as well, but that extension brings some weirdness which we will see next lecture.

41.4 Showing That A Bijection Exists

To show that $|S| = |T|$ using a bijection is equivalent to proving a proposition of the following form.

Proposition 1

Let $S = \ldots$ Let $T = \ldots$ Then there exists a bijection $f : S \to T$. Hence, $|S| = |T|$.

The presence of an existential quantifier in the conclusion suggests we use the Construct Method. Let's begin by identifying the parts of the quantified sentence.

Quantifier:	$\exists$
Variable:	f
Domain:	all functions from S to T
Open sentence:	$f : S \to T$ is a bijection.

To show that the open sentence is true, we must show that f is a bijection, that is, we must show that f is surjective and injective. So any proof that $|S| = |T|$ which uses bijections will have the following structure.

Proof in Progress

1. Consider the rule $f : S \to T$ defined by $f(s) =$ *to be completed.*
2. We show that f is a function. *This shows f is in the domain of the quantified statement we just examined.*
3. We show that f is surjective. *To be completed.*
4. We show that f is injective. *To be completed.*
5. Hence, $f : S \to T$ is a bijection and $|S| = |T|$.

In practice, the first two steps are usually combined and authors typically write "Consider the function f mapping from S to T defined by ...". The task of verifying that the rule is really a function is left to the reader. A more formal proof would require that the details be presented, but this is where understanding your audience is important. In many instances, verifying that a rule is a function is straightforward and including such a verification would actually distract from the proof. With the preceding remark in mind, and already knowing how to handle Steps 3 and 4, we can produce a more typical proof structure.

Proof in Progress

1. Consider the function $f : S \to T$ defined by $f(s) =$ *to be completed.*
2. We show that f is surjective. Let $t \in T$. Consider $s =$ *to be completed.* We show that $s \in S$ *to be completed.* Now we show that $f(s) = t$ *to be completed.*
3. We show that f is injective. Let $s_1, s_2 \in S$ and suppose that $f(s_1) = f(s_2)$. Now we show that $s_1 = s_2$ *to be completed.*
4. Hence, $f : S \to T$ is a bijection and $|S| = |T|$.

The structure contains two parts which are, in themselves, proofs: a proof that f is surjective, and a proof that f is injective.

We should emphasize that bijections are not the only way to show that two sets have the same cardinality. We can use bijections to establish propositions which are simpler to work with, and then use the propositions.

REMARK

Even though it is often obvious that a rule is a function, we want to emphasize that many common rules are not functions. For example, the (x, y) pairs that satisfy $x^2 + y^2 = 1$ do not constitute a function using the rule $f(x) = y$ since $(0, 1)$ and $(0, -1)$ are among the pairs. That is, $x = 0$ does not map to a unique value of y. The parabola $x = y^2$ is not a function. Though $y = \sin x$ is a function, its reflection in the line $y = x$, $x = \sin y$, is not a function which is why the domain must be restricted when you are looking for an inverse sine relation.

Many real life rules are not functions. Think of a university timetable which implicitly embeds a rule that maps rooms to students. Since one room contains many students, the rule that maps rooms to students is not a function.

41.5 Finite Sets

We begin by proving two fundamental theorems about counting and sets for which you probably already have an intuitive understanding but may never have proved.

Definition 41.5.1 Disjoint

Sets S and T are **disjoint** if $S \cap T = \emptyset$.

Proposition 2 **(Cardinality of Disjoint Sets (CDS))**

If S and T are disjoint finite sets, then

$$|S \cup T| = |S| + |T|$$

A simple example can be taken from any room in any building. If S is a set of m chairs in the room, and T is a set of n tables in the room, then the number of tables and chairs is $m + n$.

Before we read a proof of the Cardinality of Disjoint Sets, it is important to keep two things in mind. First, we are proving a statement about set cardinality, not a statement about set equality. Second, to establish basic properties of set cardinality we must work with bijections.

The intuitive idea underlying the proof is very simple. Count the first m elements in S, and then continue counting the next n elements in T. As you will see, a formal proof is more complicated. Note how closely the proof follows the structure described in the previous section.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Since S is a finite set, there exists a bijection $f : S \to \mathbb{N}_m$ for some non-negative integer m, and $|S| = m$.

2. Since T is a finite set, there exists a bijection $g : T \to \mathbb{N}_n$ for some non-negative integer n, and $|T| = n$.

3. Construct a function $h : S \cup T \to \mathbb{N}_{m+n}$ as follows.

$$h(x) = \begin{cases} f(x) & \text{if } x \in S \\ g(x) + m & \text{if } x \in T \end{cases}$$

4. To show that h is surjective, let $y \in \mathbb{N}_{m+n}$. If $y \leq m$, then because f is surjective, there exists an element $x \in S$ so that $f(x) = y$, hence $h(x) = y$. If $m+1 \leq y \leq m+n$, then because g is surjective, there exists an element $x \in T$ so that $g(x) = y - m$ and so $h(x) = (y - m) + m = y$.

5. To show that h is injective, let $x_1, x_2 \in S \cup T$ and suppose that $h(x_1) = h(x_2)$. If $h(x) \leq m$ then $h(x) = f(x)$ so if $h(x_1) \leq m$ we have

$$h(x_1) = h(x_2) \Rightarrow f(x_1) = f(x_2)$$

But since f is a bijection $f(x_1) = f(x_2)$ implies $x_1 = x_2$ as needed.

If $h(x) > m$ then $h(x) = g(x)$ so if $h(x_1) > m$ we have

$$h(x_1) = h(x_2) \Rightarrow g(x_1) + m = g(x_2) + m \Rightarrow g(x_1) = g(x_2)$$

But since g is a bijection $g(x_1) = g(x_2)$ implies $x_1 = x_2$ as needed.

Since h is a function which is both injective and surjective, h is bijective.

6. Thus
$$|S \cup T| = |\mathbb{N}_{m+n}| = m + n = |\mathbb{N}_m| + |\mathbb{N}_n| = |S| + |T|$$

□

Let's spend some time analyzing the proof.

Analysis of Proof As usual, we begin with the hypothesis and the conclusion.

Hypothesis: S and T are disjoint finite sets

Conclusion: $|S \cup T| = |S| + |T|$

Sentence 1 *Since S is a finite set, there exists a bijection $f : S \to \mathbb{N}_m$ for some non-negative integer m, and $|S| = m$.*

This makes use of the hypothesis and the definition of $\mathbb{N}_m$. The second sentence is similar.

Sentence 2 *Since T is a finite set, there exists a bijection $g : T \to \mathbb{N}_n$ for some non-negative integer n, and $|T| = n$.*

Sentence 3 Before looking at Sentence 3, we are going to skip ahead to the last sentence. Fortunately, when reading a proof we are free to do that. This last sentence drives what we need to do. Sentence 3 constructs a function $h : S \cup T \to \mathbb{N}_{m+n}$. How are we going to use h?

$$\begin{aligned} |S \cup T| &= |\mathbb{N}_{m+n}| && \text{because of the bijection } h \\ &= m + n && \text{from the cardinality of the finite set } \mathbb{N}_{m+n} \\ &= |\mathbb{N}_m| + |\mathbb{N}_n| && \text{from the cardinality of the finite sets } \mathbb{N}_m \text{ and } \mathbb{N}_n \\ &= |S| + |T| && \text{because of the bijections } f \text{ and } g \end{aligned}$$

The first equality sign relies on the bijection h. All of the remaining equality signs can be justified from the definition of $\mathbb{N}_\ell$ or Sentences 1 and 2. The difficult part is constructing h and then establishing that h is a bijection. Sentence 3 constructs a function $h : S \cup T \to \mathbb{N}_{m+n}$ as follows.

$$h(x) = \begin{cases} f(x) & \text{if } x \in S \\ g(x) + m & \text{if } x \in T \end{cases}$$

Notice that h is defined in terms of f and g. Note also that elements in the set S will be mapped to the integers $1, 2, \ldots, m$ and the elements in the set T will be mapped to the integers $m + 1, m + 2, \ldots, m + n$.

Having defined a function h, the author must still establish

- h is surjective
- h is injective

This occurs in the next two paragraphs, each of which is a proof in its own right.

Paragraph 4 *To show that h is surjective, ...*

In this paragraph the author establishes that h is surjective by using the definition of surjective. The checking of each sentence is left to the reader.

Paragraph 5 *To show that h is injective, ...*

In this paragraph the author establishes that h is injective by using the definition of injective. The checking of each sentence is left to the reader.

Who would have thought that counting was so complicated!

Proposition 3 **(Cardinality of Intersecting Sets (CIS))**

If S and T are any finite sets, then

$$|S \cup T| = |S| + |T| - |S \cap T|$$

After having just endured an arduous proof, you might be disinclined to go looking for a complicated mapping and then proving that it is a bijection. That's sensible. What we can do in this case is to use the Cardinality of Disjoint Sets by writing $S \cup T$ and T as the union of disjoint sets.

Proof in Progress

1. $S \cup T = S \cup (T - S)$ where S and $T - S$ are disjoint sets. (Draw a Venn diagram to make this clear.)
2. $T = (S \cap T) \cup (T - S)$ where $S \cap T$ and $T - S$ are disjoint sets. (Draw a Venn diagram to make this clear.)
3. *To be completed.*

But now that we have the unions of finite disjoint sets we can invoke the Cardinality of Disjoint Sets.

Proof in Progress

1. $S \cup T = S \cup (T - S)$ where S and $T - S$ are disjoint sets.
2. Hence, by the Cardinality of Disjoint Sets, $|S \cup T| = |S| + |T - S|$.
3. $T = (S \cap T) \cup (T - S)$ where $S \cap T$ and $T - S$ are disjoint sets.
4. Hence, by the Cardinality of Disjoint Sets, $|T| = |S \cap T| + |T - S|$
5. *To be completed.*

Subtracting the two cardinality equations and rearranging will give us what we need. Take a minute to read a complete proof.

Proof: Since S and $T - S$ are disjoint sets, and

$$S \cup T = S \cup (T - S)$$

the Cardinality of Disjoint Sets implies

$$|S \cup T| = |S| + |T - S|$$

Since $S \cap T$ and $T - S$ are disjoint sets, and

$$T = (S \cap T) \cup (T - S)$$

the Cardinality of Disjoint Sets implies

$$|T| = |S \cap T| + |T - S|$$

Subtracting the two cardinality equations gives

$$|S \cup T| - |T| = |S| - |S \cap T|$$

hence

$$|S| + |T| - |S \cap T|$$

as required. □

Proposition 4 **(Cardinality of Subsets of Finite Sets (CSFS))**

If S and T are finite sets, and $S \subsetneq T$, then $|S| < |T|$.

The proof uses the same partitioning idea that was used in the proof of the Cardinality of Intersecting Sets.

Proof: The sets S and $T - S$ are disjoint sets where

$$S \cup (T - S) = T$$

By the Cardinality of Disjoint Sets and the fact above

$$|S| + |T - S| = |S \cup (T - S)| = |T|$$

Since $S \subsetneq T$, $T - S$ is a non-empty finite subset so $|T - S| > 0$. Hence

$$|S| + |T - S| = |T| \Rightarrow |S| < |T|$$

□

41.6 Practice

1. The rule $h : S \cup T \to \mathbb{N}_{m+n}$ defined below appears in the proof of the Cardinality of Disjoint Sets.

$$h(x) = \begin{cases} f(x) & \text{if } x \in S \\ g(x) + m & \text{if } x \in T \end{cases}$$

   Prove that the rule is a function.

Chapter 42

Cardinality of Infinite Sets

42.1 Objectives

The content objectives are:

1. State and prove the *Cardinality of Subsets of Finite Sets.*
2. Discover a proof that $|\mathbb{N}| = |2\mathbb{N}|$.
3. State and prove that $|\mathbb{Q}_{>0}| = |\mathbb{N}|$.
4. State and prove that $|\mathbb{N}| \neq |(0,1)|$.

42.2 Infinite Sets Are Weird

With respect to counting, finite sets behave pretty much as we expect. For example, if S is a proper subset of T, then $|S| < |T|$.

This is not the case for infinite sets. Consider the following proposition.

Proposition 1 ($|\mathbb{N}| = |2\mathbb{N}|$)

Let $2\mathbb{N}$ be the set of positive even natural numbers. Then $|\mathbb{N}| = |2\mathbb{N}|$.

Let's be clear about what this proposition is saying. Even though the set of positive even numbers is a proper subset of the set of natural numbers, and even though there are infinitely many odd numbers excluded from the set of even numbers, the cardinality of the sets of even numbers and all natural numbers is the same!

How would we prove this? Two sets have the same cardinality if and only if there exists a bijection between the two sets. So we can use the same proof structure that was used in the previous chapter to build a bijection between two sets.

Proof in Progress

1. Consider the function $f : \mathbb{N} \to 2\mathbb{N}$ defined by $f(s) =$ *to be completed.*

2. We show that f is surjective. Let $t \in 2\mathbb{N}$. Consider $s =$ *to be completed*. We show that $s \in \mathbb{N}$ *to be completed*. Now we show that $f(s) = t$ *to be completed*.

3. We show that f is injective. Let $s_1, s_2 \in \mathbb{N}$ and suppose that $f(s_1) = f(s_2)$. Now we show that $s_1 = s_2$ *to be completed*.

4. Hence, $f : \mathbb{N} \to 2\mathbb{N}$ is a bijection and $|\mathbb{N}| = |2\mathbb{N}|$.

How do we construct a bijection? There is an obvious mapping from $\mathbb{N}$ to $2\mathbb{N}$:

$$f(s) = 2s$$

$$\begin{array}{cccccc} \mathbb{N} & 1 & 2 & 3 & 4 & \dots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \\ 2\mathbb{N} & 2 & 4 & 6 & 8 & \dots \end{array}$$

Let's update the proof in progress.

Proof in Progress

1. Consider the function $f : \mathbb{N} \to 2\mathbb{N}$ defined by $f(s) = 2s$.

2. We show that f is surjective. Let $t \in 2\mathbb{N}$. Consider $s = \dots$ (*to be completed*).

   We show that $s \in \mathbb{N}$ (*to be completed*).

   Now we show that $f(s) = t$ (*to be completed*).

3. We show that f is injective. Let $s_1, s_2 \in \mathbb{N}$ and suppose that $f(s_1) = f(s_2)$. Now we show that $s_1 = s_2$ (*to be completed*).

4. Hence, $f : \mathbb{N} \to 2\mathbb{N}$ is a bijection and $|\mathbb{N}| = |2\mathbb{N}|$.

Exercise 1 Complete the proof that $|\mathbb{N}| = |2\mathbb{N}|$.

42.3 Infinite Sets are Even Weirder Than You Thought

There are infinitely many rational numbers between the natural numbers 1 and 2 so it is a real shock to most people that the cardinality of the positive rational numbers and the natural numbers is the same. For technical reasons, we won't prove that but we will prove something very close. Consider the sets

$$\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$$

and

$$\mathbb{Q}_{>0} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{N}, \gcd(a, b) = 1 \right\}.$$

The obvious mapping $f : \mathbb{Q}_{>0} \to \mathbb{N} \times \mathbb{N}$ defined by

$$f\left(\frac{a}{b}\right) = (a, b)$$

is injective but not surjective since, for example, $(2, 2) \in \mathbb{N} \times \mathbb{N}$ but $\frac{2}{2} \notin \mathbb{Q}_{>0}$. Since $\mathbb{N} \times \mathbb{N}$ is at least as large as $\mathbb{Q}_{>0}$, it is even more surprising that $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ have the same cardinality.

Proposition 2 **($|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$)**

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

To prove this we will make use of the following proposition, whose proof will be left as an exercise.

Proposition 3 **(Even-Odd Factorization of Natural Numbers (EOFNN))**

Any natural number n can be written uniquely as $n = 2^i q$ where i is a non-negative integer and q is an odd natural number.

Proof: The proof is left as an exercise.

Example 1 Here are some examples of the Even-Odd Factorization of Natural Numbers.

$$60 = 2^2 \times 15$$
$$64 = 2^6 \times 1$$
$$65 = 2^0 \times 65$$

Here is a proof that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Notice how closely it follows the proof structure that we have been using.

Proof: (For reference, each sentence of the proof is written on a separate line.)

1. Consider the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(a, b) = 2^{a-1}(2b - 1)$. Observe that mathematicians usually write $f(a, b)$ instead of $f((a, b))$.
2. We show that f is surjective. Let $t \in \mathbb{N}$. By the Even-Odd Factorization of Natural Numbers, $t = 2^i q$ where i is a non-negative integer and q is an odd natural number. Since q is odd, there exists a natural number b such that $q = 2b - 1$. If t is odd then $t = 2^0(2b - 1)$ and $f(1, b) = t$. If t is even then there exists a natural number a so that $t = 2^{a-1}(2b - 1)$ and $f(a, b) = t$.
3. We show that f is injective. Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ and suppose that $f(a, b) = f(c, d)$. But then
$$\begin{aligned} f(a, b) = f(c, d) &\Rightarrow 2^{a-1}(2b - 1) = 2^{c-1}(2d - 1) \\ &\Rightarrow (2^{a-1} = 2^{c-1}) \text{ and } (2b - 1 = 2d - 1) \\ &\Rightarrow (a = c) \text{ and } (b = d) \\ &\Rightarrow (a, b) = (c, d) \end{aligned}$$
as required.
4. Hence, $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a bijection and $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

$\square$

You might well ask, do all infinite sets have the same size? The surprising answer is no.

42.4 Not All Infinite Sets Have The Same Cardinality

Recall that $(0,1)$ denotes the open interval of real numbers between 0 and 1. That is

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

Proposition 4 ($|\mathbb{N}| \neq |(0,1)|$)

The set of natural numbers and the open interval $(0,1)$ of real numbers do not have the same cardinality. That is, $|\mathbb{N}| \neq |(0,1)|$

Proof: By way of contradiction, assume that $|\mathbb{N}| = |(0,1)|$. But then some bijection $f : \mathbb{N} \to |(0,1)|$ must exist. Write each element of $|(0,1)|$ as an infinite decimal and list all of the real numbers in $(0,1)$ as follows.

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}a_{14}\ldots \\
f(2) &= 0.a_{21}a_{22}a_{23}a_{24}\ldots \\
f(3) &= 0.a_{31}a_{32}a_{33}a_{34}\ldots \\
&\vdots \\
f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}\ldots \\
&\vdots
\end{aligned}$$

Construct the real number $c = 0.c_1c_2c_3c_4\ldots$ as follows. For c_i, choose any digit from $1, 2, 3, \ldots, 8$ with the property that $c_i \neq a_{ii}$. The number c does not end in an infinite sequence of 0's or 9's so has only one decimal representation (a subtlety that requires its own explanation in another course). The real number c appears nowhere in the list since it differs from $f(i)$ in position i for every i.

But then f is not surjective, hence not bijective which contradicts our assumption. $\square$

This chapter raises a whole set of questions about infinite sets.

- How many "infinities" are there?
- Can we say that the cardinality of one infinite set is less than or greater than another infinite set?
- Can there be infinite sets whose cardinality lies between that of other infinite sets of distinct cardinalities?
- How does one construct "new" infinite sets?

These are very interesting questions with even more interesting answers. Unfortunately, the questions and answers will have to be left to another course.

Chapter 43

Practice, Practice, Practice: Bijections and Cardinality

43.1 Objectives

This class provides an opportunity to practice working with bijections and cardinality.

43.2 Worked Examples

Example 1 For each of the following functions, determine if the function is a surjection, injection, or bijection.

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

   Solution: This function is not surjective. Consider the real number -1. Since $f(x) > 0$ for all $x \in \mathbb{R}$, there is no real number x_0 so that $f(x_0) = -1$. To show that this function is injective, let $x_1, x_2 \in \mathbb{R}$ and suppose that $e^{x_1} = e^{x_2}$. Taking the natural log of both sides gives $\ln(e^{x_1}) = \ln(e^{x_2})$ which implies that $x_1 = x_2$. Since f is not surjective, it is not bijective.

2. $f : \mathbb{R} \to (0, +\infty)$ defined by $f(x) = e^x$.

   Solution: To show that this function is surjective, let $y \in (0, +\infty)$. Consider $x_0 = \ln y$. Now $x_0 \in \mathbb{R}$ and $f(x_0) = e^{x_0} = e^{\ln y} = y$. To show that this function is injective, let $x_1, x_2 \in \mathbb{R}$ and suppose that $e^{x_1} = e^{x_2}$. Taking the natural log of both sides gives $\ln(e^{x_1}) = \ln(e^{x_2})$ which implies that $x_1 = x_2$. Since f is both surjective and injective, f is bijective.

3. Let p be a prime and let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be defined by $f(x) = [3]x$.

   Solution: Since p is a prime, $[3]$ has an inverse by the corollary Existence of Inverses in $\mathbb{Z}_p$. To show that this function is surjective, let $y \in \mathbb{Z}_p$. Consider $x_0 = [3]^{-1}y$. Now $x_0 \in \mathbb{Z}_p$ and $f(x_0) = [3]([3]^{-1}y) = ([3][3]^{-1})y = y$. To show that this function is injective, let $x_1, x_2 \in \mathbb{Z}_p$ and suppose that $[3]x_1 = [3]x_2$. Multiplying both sides by $[3]^{-1}$ gives $[3]^{-1}([3]x_1) = [3]^{-1}([3]x_2)$ which implies that $x_1 = x_2$. Since f is both surjective and injective, f is bijective.

4. $f : \mathbb{Z} \to \mathbb{Z}_7$ defined by $f(x) = [x]$.

   Solution: Recall that $\mathbb{Z}_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$. Since $f(i) = [i]$ for $i = 0, 1, 2, 3, 4, 5, 6$, f is surjective. This function is not injective since 0 and 7 both map to $[0]$. Since f is not injective, it is not bijective.

5. $f : \mathbb{N} \to \mathbb{N}$ where $d(n)$ is the number of natural number divisors of n.

   Solution: To show that this function is surjective, let $y \in \mathbb{N}$. Since the natural number 2^{y-1} has the y divisors $2^0, 2^1, 2^2, \ldots, 2^{y-1}$, $f(2^{y-1}) = y$ so f is surjective. This function is not injective since $d(2) = d(3) = 2$. Since f is not injective, it is not bijective.

Example 2 Let S denote the set of all finite subsets of the natural numbers. Let $D(n)$ denote the set of all natural number divisors of n. Thus, $D(12) = \{1, 2, 3, 4, 6, 12\}$. Is the function $f : \mathbb{N} \to S$ defined by $D(n)$ a surjection?

Solution: D is not a surjection. Consider any set without the element 1, $T = \{2, 3\}$ for example. Suppose there exists an integer n so that $D(n) = T$. Since $1 \mid n$, 1 must be in T, but it is not. Hence, no natural number can map to T.

Example 3 Prove the following proposition.

Proposition 1 Let S, T, U be sets. If $|S| = |T|$ and $|T| = |U|$, then $|S| = |U|$.

Proof: Since $|S| = |T|$, there exists a bijection $f : S \to T$. Since $|T| = |U|$, there exists a bijection $g : T \to U$. By Proposition 5 in Section 31.2.4, $g \circ f : S \to U$ is a bijection from S to U so $|S| = |U|$. □

Example 4 Suppose S is a non-empty finite set with k elements and $a \notin S$. Find a bijection f from $S \cup \{a\}$ to $\mathbb{N}_{k+1}$. You do not need to prove that f is a bijection, simply state it. Use this bijection to prove that $|S \cup \{a\}| = |S| + 1$.

Proof: Since S is a non-empty finite subset, there exists a bijection g between S and $\mathbb{N}_k$ for some integer k. Define f as follows.

$$f(x) = \begin{cases} g(x) & \text{if } x \in S \\ k+1 & \text{if } x = a \end{cases}$$

Now

$$|S \cup \{a\}| = |\mathbb{N}_{k+1}| = k + 1 = |S| + 1$$

as needed. □

Example 5 The **power set** of a set S, denoted $\mathcal{P}(S)$ is the set of all subsets of S, including the empty set and the set itself. So, if $S = \{a, b\}$, $\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. For the remainder of this question, you may suppose that S is a finite set.

1. What are the power sets of $\emptyset$, $\{a\}$, $\{a, b\}$, and $\{a, b, c\}$?
2. If $|S| = n$, conjecture $|\mathcal{P}(S)|$.
3. Prove your conjecture. (Hint: you do not need to use a bijection.)
4. Prove that $|S| < |\mathcal{P}(S)|$.

Solution:

1. What are the power sets of $\emptyset$, $\{a\}$, $\{a, b\}$, and $\{a, b, c\}$?

   Solution: $\mathcal{P}(\{\emptyset\}) = \{\emptyset\}$,
   $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$,
   $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,
   $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

2. If $|S| = n$, $|\mathcal{P}(S)| = 2^n$.

3. **Proof:** We proceed by induction. We begin by formally writing out our inductive statement

   $P(|S|)$: If S is a finite set with cardinality $|S|$, then $|\mathcal{P}(S)| = 2^{|S|}$.

   Base Case We verify that $P(0)$ is true where $P(0)$ is the statement

   $P(0)$: If S is a finite set with cardinality 0, then $|\mathcal{P}(S)| = 2^0$.

   Since S has cardinality 0, S must be the empty set. Since $\mathcal{P}(S) = \{\emptyset\}$, it is certainly the case that $|\mathcal{P}(S)| = |\{\emptyset\}| = 1$ as needed.

   Inductive Hypothesis We assume that the statement $P(k)$ is true for some integer $k \geq 0$.

   $P(k)$: If S is a finite set with cardinality k, then $|\mathcal{P}(S)| = 2^k$.

   Inductive Conclusion Now we show that the statement $P(k+1)$ is true.

   $P(k+1)$: If S is a finite set with cardinality $k+1$, then $|\mathcal{P}(S)| = 2^{k+1}$.

   Since $k + 1 > 0$, there is at least one element, say x, in S. The set $S - \{x\}$ has cardinality k and so by the Inductive Hypothesis, $|\mathcal{P}(S - \{x\})| = 2^k$. Now, create a new set T by adding x to all of the elements of $\mathcal{P}(S - \{x\})$. Thus $|T| = 2^k$. Since

   $$\mathcal{P}(S) = \mathcal{P}(S - \{x\}) \cup T$$

   and $\mathcal{P}(S - \{x\})$ and T are disjoint finite subsets, we can use the Cardinality of Disjoint Sets to assert that

   $$|\mathcal{P}(S)| = |\mathcal{P}(S - \{x\})| + |T| = 2^k + 2^k = 2^{k+1}$$

   as needed.

   □

4. **Solution:** $|S| = n < 2^n = |\mathcal{P}(S)|$. (You can prove that $n < 2^n$ by induction.)

Example 6 Let S be a non-empty finite set disjoint from $\mathbb{N}$. Find a bijection $f : \mathbb{N} \cup S \to \mathbb{N}$.

Solution: Since S is a non-empty finite set, $|S| = n$ for some natural number n and there exists a bijection $g : S \to \mathbb{N}_n$. Define f as follows.

$$f(x) = \begin{cases} g(x) & \text{if } x \in S \\ n+m & \text{if } m \in \mathbb{N} \end{cases}$$

Example 7 Let (a, b) denote the real interval $a < x < b$. Prove that $|(0,1)| = |(1,\infty)|$.

Proof: Consider the function $f : (0,1) \to (1,\infty)$ defined by $f(x) = 1/x$. We shall show that f is a bijection and so conclude that $|(0,1)| = |(1,\infty)|$.

To show that f is surjective, let $y \in (1,\infty)$. Consider $x = 1/y$. Since $y > 0$, $x > 0$. Since $y > 1$, $1/y < 1$ (take the reciprocals of both sides of $y > 1$). But then $x < 1$, so $x \in (0,1)$. Now

$$f(x) = \frac{1}{1/y} = y$$

as needed.

To show that f is injective, let $x_1, x_2 \in (0,1)$ and let $f(x_1) = f(x_2)$. But then

$$f(x_1) = f(x_2) \Rightarrow \frac{1}{x_1} = \frac{1}{x_2} \Rightarrow x_2 = x_1$$

as needed.

Since f is surjective and injective, f is bijective and so $|(0,1)| = |(1,\infty)|$. $\square$

43.3 Quiz

Example 8 (10 marks) Let (a, b) denote the real interval $a < x < b$. Prove that $|(0, 1)| = |(0, \infty)|$.

Proof: Let $f : (0, 1) \to (0, \infty)$ be the function defined by

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

We claim that f is a bijection. Note that

$$\begin{aligned} 0 < x < 1 &\Rightarrow 0 > -x > -1 \\ &\Rightarrow 1 > 1 - x > 0 \\ &\Rightarrow \frac{1}{1-x} > 1 \\ &\Rightarrow \frac{1}{1-x} - 1 > 0 \end{aligned}$$

So, f maps correctly into $(0, \infty)$. ✓✓

Now we show that f is injective. ✓Suppose that $f(x) = f(y)$, for some $x, y \in (0, 1)$. Rearranging the expressions for this, we get $x = y$ immediately. ✓

Now we show that f is surjective. ✓Let $v \in (0, \infty)$. We must find an x so that

$$\frac{1}{1-x} - 1 = v \checkmark$$

Arithmetic shows us that

$$x = 1 - \frac{1}{v+1} \checkmark$$

Thus, $f(x) = f(1 - \frac{1}{v+1}) = v$. We only have to check that the $1 - \frac{1}{v+1}$ is actually in the domain. Note that

$$1 + v > 1 \Rightarrow 1 > \frac{1}{1+v} > 0 \Rightarrow 0 < 1 - \frac{1}{1+v} < 1$$

Thus, surjectivity is proved. ✓

Hence, we have that f is a bijection, so the two sets have the same cardinality. □

Index