Number Theory

MAT-255 Davidson College

Claire Merriman

Spring 2024

Contents

Part I

Course Notes

These notes served as course notes for the Spring 2024 Number Theory course at Davidson College. This course can also serve as an introduction to proofs course.

The official textbook for the course was *Elementary Number Theory* by James K. Strayer. Some topics that are not covered in these notes were assigned as reading before class. In order to reference these results in the notes, they are provided in Appendix A. The reading assignments are visible by using the `instructornote` option in the TEX file.

The introduction to proofs used An Introduction to Proof via Inquiry-Based Learning by Dana C. Ernst, an open source textbook. My best effort has been made to link directly to this resource, although some standard staments and exercies are included in the notes.

Solutions to some problems from Strayer and Ernst are omitted. Solutions to some standard number theory problems from these sources are included.

These notes are also based on my notes teaching the Elementary Number Theory at The Ohio State University. Those courses use *An Introduction to the Theory of Numbers* by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery and *Elementary Number Theory* by Gareth A. Jones and J. Mary Jones. These notes were also influenced by *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by James Pommersheim, Tim Marks, Erica Flapan.

Support for converting these notes to Ximera was provided by a Ximera Flash Grant.

1 Introduction

What is number theory?

Elementary number theory is the study of integers, especially the positive integers. A lot of the course focuses on prime numbers, which are the multiplicative building blocks of the integers. Another big topic in number theory is integer solutions to equations such as the Pythagorean triples $x^2+y^2=z^2$ or the generalization $x^n+y^n=z^n$. Proving that there are no integer solutions when $n>2$ was an open problem for close to 400 years.

The first part of this course reproves facts about divisibility and prime numbers that you are probably familiar with. There are two purposes to this: 1) formalizing definitions and 2) starting with the situation you understand before moving to the new material.

1.1 Mathematical definitions and notation

Learning Objectives. By the end of class, students will be able to:

- Formally define even and odd
- Complete basic algebraic proofs .

Definition. We will use the following number systems and abbreviations:

- The *integers,* written $\mathbb{Z}$, is the set $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- The *natural numbers,* written $\mathbb{N}$. Most elementary number theory texts either define $\mathbb{N}$ to be the positive integers or avoid using $\mathbb{N}$. Some mathematicians include 0 in $\mathbb{N}$.
- The *real numbers,* written $\mathbb{R}$.
- The *integers modulo n,* written $\mathbb{Z}_n$. We will define this set in Strayer Chapter 2, although Strayer does not use this notation.

We will also use the following notation:

- The symbol $\in$ means "element of" or "in." For example, $x \in \mathbb{Z}$ means "x is an element of the integers" or "x in the integers."

This first section will cover basic even, odd, and divisibility results. These first few definitions and results will use algebraic proofs, before we cover formal proof methods.

Definition (Even and odd, multiplication definition)**.** An integer n is *even* if $n = 2k$ for some $k \in \mathbb{Z}$. That is, n is a *multiple* of 2.

An integer n is odd if $n = 2k + 1$ for some $k \in \mathbb{Z}$.

Now, the preceding definition is standard in an introduction to proofs course, but it is not the only definition of even/odd. We also have the following definition that is closer to the definition you are probably used to:

Definition (Even and odd, division definition)**.** Let $n \in \mathbb{Z}$. Then n is said to be *even* if 2 divides n and n is said to be *odd* if 2 does not divide n.

Note that we need to define *divides* in order to use the second definition. We will formally prove that these definitions are *equivalent,* but for now, let's use the first definition.

Theorem 1. If n is an even integer, then n^2 is even.

In-class Problem 1 Prove this theorem.

Proof If n is an even integer, then by definition, there is some $k \in \mathbb{Z}$ such that $n = 2k$. Then

$$n^2 = (2k)^2 = 2(2k^2).$$

Since $2(k^2)$ is an integer, we have written n^2 in the desired form. Thus, n^2 is even. ■

Proposition 1. The sum of two consecutive integers in odd.

For this problem, we need to figure out how to write two consecutive integers.

Proof Let $n, n+1$ be two consecutive integers. Then their sum is $n+n+1 = 2n+1$, which is odd by definition. ■

2 Divisibility, primes, and greatest common divisors

The goal of this chapter is to review basic facts about divisibility, get comfortable with the new notation, and solve some basic linear equations.

We will also use this material as an opportunity to get used to the course.

2.1 Divisibility

Learning Objectives. By the end of class, students will be able to:

- Define "divisible" and "factor"
- Prove basic facts about divisibility .

Reading assignment:

Read: Read Ernst Chapter 1 and Section 2.1. Also read Strayer Introduction and Section 1.1 through the proof of Proposition 1.2 (that is, pages 1-5).

Turn in: From Ernst: Problem 2.6 and 2.8

Definition (a divides b)**.** Let $a, b \in \mathbb{Z}$. The a *divides* b, denoted $a \mid b$, if there exists an integer c such that $b = ac$. If $a \mid b$, then a is said to be a *divisor* or *factor of* b. The notation $a \nmid b$ means a does not divide b.

Note that 0 is not a divisor of any integer other than itself, since $b = 0c$ implies $a = 0$. Also all integers are divisors of 0, as weird as that sounds at first. This is because for any $a \in \mathbb{Z}$, $0 = a0$.

Proposition 2. Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Since this is the first result in the chapter, the only tool we have is the definition of "$a \mid b$".

Proof Since $a \mid b$ and $b \mid c$, there exist $d, e \in \mathbb{Z}$ such that $b = ae$ and $c = bf$. Combining these, we see

$$c = bf = (ae)f = a(ef),$$

so $a \mid c$. ■

This means that division is *transitive*.

Proposition 3. Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.

Proof Let $a, b, c, m, n \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. Then by definition of divisibility, there exists $j, k \in \mathbb{Z}$ such that $cj = a$ and $ck = b$. Thus,

$$ma + nb = m(cj) + n(ck) = c(mj + nk).$$

Therefore, $c \mid ma + nb$ by definition. ■

Definition. The expression $ma + nb$ in **??** is called *an (integral) linear combination of* a *and* b.

?? says that an integer dividing each of two integers also divides any integral linear combination of those integers. This fact will be extremely valuable in establishing theoretical results. But first, let's get some more practice with proof writing

Break into three groups. Using the proofs of **??** and **??** as examples, prove the following facts. Each group will prove one part.

In-class Problem 2 Prove or disprove the following statements.

(a) If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $a + c \mid b + d$.

(b) If a, b, c, and d are integers such that if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

(c) If a, b, and c are integers such that if $a \nmid b$ and $b \nmid c$, then $a \nmid c$.

Solution: Problem on Homework.

2.2 Symbolic logic

This section is included for students who have not seen symbolic logic and truth tables or need a review.

Learning Objectives. By the end of class, students will be able to:

- Prove basic mathematical statements using definitions and direct proof
- Use truth tables to understand compound propositions
- Prove statements by contradiction
- Use the greatest integer function .

Reading assignment:

Read: Read Ernst Chapter 1 and Section 2.1. Also read Strayer Introduction and Section 1.1 through the proof of Proposition 1.2 (that is, pages 1-5).

Turn in: From Ernst: Problem 2.6 and 2.8

If you have not seen proof by induction or need a review, see Ernst Chapter 1 and Section 2.1 and Section 2.2 through Example 2.21. Problem 2.17 is also provided below:

In-class Problem 3 Determine whether each of the following is a proposition. Explain your reasoning.

- All cars are red.
- Every person whose name begins with J has the name Joe.
- $x^2 = 4$.
- There exists a real number x such that $x^2 = 4$.
- For all real numbers x, $x^2 = 4$.
- $\sqrt{2}$ is an irrational number.
- p is prime.
- Is it raining?
- It will rain tomorrow.
- Led Zeppelin is the best band of all time.

In-class Problem 4 Construct a truth table for $A \Rightarrow B, \neg(A \Rightarrow B)$ and $A \wedge \neg B$

Solution:

A	B	$A \Rightarrow B$	$\neg(A \Rightarrow B)$	$A \wedge \neg B$
True	True	True	False	False
True	False	False	True	True
False	True	True	False	False
False	True	True	False	False

This is the basis for *proof by contradiction.* We assume both A and $\neg B$, and proceed until we get a contradiction. That is, A and $\neg B$ cannot both be true.

Definition (Proof by contradiction)**.** Let A and B be propositions. To prove A implies B by contradiction, first assume the B is false. Then work through logical steps until you conclude $\neg A \wedge A$.

All definitions are ‘biconditionals but we normally only write the “if.”

We say that two definitions are *equivalent* if definition A is true if and only if definition B is true.

2.3 The Division Algorithm

Learning Objectives. By the end of class, students will be able to:

- Prove existence and uniqueness for the Division Algorithm
- Prove existence and uniqueness for the general Division Algorithm .

Reading assignment:

Read: Ernst Section 2.2 and Section 2.4

Turn in: Ernst, Problem 2.59 and 2.64

This section introduces the division algorithm, which will come up repeatedly throughout the semester, as well as the definition of divisors from last class.

First, let's define a *lemma.* A lemma is a minor result whose sole purpose is to help in proving a theorem, although some famous named lemmas have become important results in their own right.

Definition (greatest integer (floor) function)**.** Let $x \in \mathbb{R}$. The *greatest integer function of* x*,* denoted $[x]$ or $\lfloor x \rfloor$, is the greatest integer less than or equal to x.

Lemma 1. Let $x \in \mathbb{R}$. Then $x - 1 < [x] \leq x$.

Proof By the definition of the floor function, $[x] \leq x$.

To prove that $x - 1 < [x]$, we proceed by contradiction. Assume that $x - 1 \geq [x]$ (the negation of $x - 1 < [x]$). Then, $x \geq [x] + 1$. This contradicts the assumption that $[x]$ is the greatest integer *less than or equal to* x. Thus, $x - 1 < [x]$. ■

Theorem 2 (Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < b.$$

Before proving this theorem, let's think about division with remainders, ie long division. The quotient q should be the largest integer such that $bq \leq a$. If we divide both sides by b, we have $q \leq \frac{a}{b}$. We have a function to find the greatest integer less than or equal to $\frac{a}{b}$, namely $q = \left\lfloor \frac{a}{b} \right\rfloor$. If we rearrange the equation $a = bq + r$, we gave $r = a - bq$. This is our scratch work for existence.

Proof Let $a, b \in \mathbb{Z}$ with $b > 0$. Define $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - b \left\lfloor \frac{a}{b} \right\rfloor$. Then $a = bq + r$ by rearranging the equation. Now we need to show $0 \leq r < b$.

Since $x - 1 < \lfloor x \rfloor \leq x$ by Lemma **??**, we have

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}.$$

Multiplying all terms by $-b$, we get

$$-a + b > -b \left\lfloor \frac{a}{b} \right\rfloor \geq -a.$$

Adding a to every term gives

$$b > a - b \left\lfloor \frac{a}{b} \right\rfloor \geq 0.$$

By the definition of r, we have shown $0 \leq r < b$.

Finally, we need to show that q and r are unique. Assume there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

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

We need to show $q_1 = q_2$ and $r_1 = r_2$. We can subtract the two equations from each other.

$$\begin{aligned} a &= bq_1 + r_1, \\ \underline{-(a &= bq_2 + r_2)}, \\ 0 &= bq_1 + r_1 - bq_2 - r_2 = b(q_1 - q_2) + (r_1 - r_2). \end{aligned}$$

Rearranging, we get $b(q_1 - q_2) = r_2 - r_1$. Thus, $b \mid r_2 - r_1$. From rearranging the inequalities:

$$\begin{aligned} 0 &\leq r_2 < b \\ \underline{-b &< -r_1 \leq 0} \\ -b &< r_2 - r_1 < b. \end{aligned}$$

Thus, the only way $b \mid r_2 - r_1$ is that $r_2 - r_1 = 0$ and thus $r_1 = r_2$. Now, $0 = b(q_1 - q_2) + (r_1 - r_2)$ becomes $0 = b(q_1 - q_2)$. Since we assumed $b > 0$, we have that $q_1 - q_2 = 0$. ■

In-class Problem 5 Use the **??** on $a = 47, b = 6$ and $a = 281, b = 13$.

Solution: For $a = 47, b = 6$, we have that $a = (7)6 + 5, q = 7, r = 5$. For $a = 281, b = 13$, we have that $a = (21)13 + 8, q = 21, r = 8$.

Corollary 1. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

One proof method is using an existing proof as a guide.

In-class Problem 6 Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

(a) Use the **??** to prove this statement as a corollary. That is, use the *conclusion* of the **??** as part of the proof. Use the following outline:

(i) Let a and b be nonzero integers. Since $|b| > 0$, the **??** says that there exist unique $p, s \in \mathbb{Z}$ such that $a = p|b| + s$ and $0 \leq s < |b|$.

(ii) There are two cases:

i. When $b > 0$, the conditions are already met and $r = s$ and $q = answerb$.

ii. Otherwise, $b < 0$, $r = s$ and $q = answer - b$. .

(iii) Since both cases used that the p, s are unique, then q, r are also unique

(b) Use the *proof* of the **??** as a template to prove this statement. That is, repeat the steps, adjusting as necessary, but do not use the conclusion.

(i) In the proof of the **??**, we let $q = \left\lfloor \frac{a}{b} \right\rfloor$. Here we have two cases:

i. When $b > 0$, $q = \left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - bq$.

ii. When $b < 0$, $q = -\left\lfloor \frac{a}{b} \right\rfloor$ and $r = a - bq$.

(ii) Follow the steps of the *proof* of the **??** to finish the proof.

2.4 Greatest Common Divisors

Learning Objectives. By the end of class, students will be able to:

- Define the greatest common divisor of two integers
- Prove basic facts about the greatest common divisor .

Definition (greatest common divisor)**.** If $a \mid b$ and $a \mid c$ then a is a *common divisor* of b and c.

If at least one of b and c is not 0, the greatest (positive) number among their common divisors is called the *greatest common divisor of a and b* and is denoted $gcd(a, b)$ or just (a, b).

If $gcd(a, b) = 1$, we say that a and b are *relatively prime*.

If we want the greatest common divisor of several integers at once we denote that by $\gcd(b_1, b_2, b_3, \ldots, b_n)$.

For example, $\gcd(4, 8)$ is 4 but $\gcd(4, 6, 8)$ is 2.

The GCD always exists when at least one of the integers is nonzero. How to show this: 1 is always a divisor, and no divisor can be larger than the maximum of $|a|, |b|$. So there is a finite number of divisors, thus there is a maximum.

Proposition 4 (Bézout's Identity)**.** Let $a, b \in \mathbb{Z}$ with a and b not both zero. Then

$$\{(a, b) = \min\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}.$$

This proof brings together definitions (of greatest common divisor), previous results (**??**, factors of linear combinations), the well-ordering principle, and some methods for minimum and maximum/greatest.

Proof Since $a, b \in \mathbb{Z}$ are not both zero, at least one of $1a + 0b, -1a + 0b, 0a + 1b, 0a + (-1)b$ is in $\{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$. Therefore, the set is nonempty and has a minimal element by the **??**. Call this element d, and $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

First we will show that $d \mid a$. By the **??**, there exist unique $q, r \in \mathbb{Z}$ such that $a = qd + r$ with $0 \leq r < d$. Then,

$$r = a - qd = a - q(xa + yb) = (1 - qx)a - qyb,$$

so r is an integral linear combination of a and b. Since d is the least positive such integer, $r = 0$ and $d \mid a$. Similarly, $d \mid b$.

It remains to show that d is the *greatest* common divisor of a and$b$. Let $c$be any common divisor of a and b. Then $c \mid ax + by = d$, so $c \mid d$. ■

Since we assume a and b are not both zero, we could also simplify the first sentence using *without loss of generality*. Since there is no difference between a and b, we can assume $a \neq 0$.

2.5 Induction

This section is included as a review of proof by induction.

Learning Objectives. By the end of class, students will be able to:

- Construct a proof by induction .

If you have not seen proof by induction or need a review, see Ernst Section 4.1 and Section 4.2

In-class Problem 7 Theorems in Ernst Section 4.1

Theorem 3 (Ernst Theorem 4.5). For all $n \in \mathbb{N}$, 3 divides $4^n - 1$.

Solution: We proceed by induction. When $n = 1$, $3 \mid 4^n - 1 = 3$. Thus, the statement is true for $n = 1$.

Now assume $k \geq 1$ and the desired statement is true for $n = k$. Then the induction hypothesis is

$$3 \mid 4^k - 1.$$

By the definition of **??**, there exists $m \in \mathbb{Z}$ such that $3m = 4^k - 1$. In other words, $3m + 1 = 4^k$. Multiplying both sides by 4 gives $12m + 4 = 4^{k+1}$. Rewriting this equation gives $3(4m + 1) = 4^{k+1} - 1$. Thus, $3 \mid 4^{k+1} - 1$, and the desired statement is true for $n = k + 1$. By the (first) principle of mathematical induction, the statement is true for all positive integers, and the proof is complete.

In-class Problem 8 (Strayer Exercise 1) . Use the first principle of mathematical induction to prove each statement.

(a) If n is a positive integer, then

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

(b) If n is an integer with $n \geq 5$, then

$$2^n > n^2.$$

2.6 The Euclidean Algorithm

Learning Objectives. By the end of class, students will be able to:

- Prove the Euclidean Algorithm halts and generates the greatest common divisor of two positive integers
- Use the Euclidean Algorithm to findd the greate common divisor of two integers
- Use the (extended) **??** to write (a, b) as a linear combination of a and b.

Typically by *Euclidean Algorithm*, we mean both the algorithm and the theorem that the algorithm always generates the greatest common divisor of two (positive) integers.

Theorem 4 (Euclidean algorithm)**.** Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the **??**, there exist $q_1, r_1 \in \mathbb{Z}$ such that

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

If $r_1 > 0$, there exist $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 > 0$, there exist $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Continuing this process, $r_n = 0$ for some n. If $n > 1$, then $\gcd(a, b) = r_{n-1}$. If $n = 1$, then $\gcd(a, b) = b$.

Proof Note that $r_1 > r_2 > r_3 > \cdots \geq 0$ by construction. If the sequence did not stop, then we would have an infinite, decreasing sequence of positive integers, which is not possible. Thus, $r_n = 0$ for some n.

When $n = 1$, $a = bq + 0$ and $\gcd(a, b) = b$.

?? states that for $a = bq_1 + r_1$, $\gcd(a, b) = \gcd(b, r_1)$. This is because any common divisor of a and b is also a divisor of $r_1 = a - bq_1$.

If $n > 1$, then by repeated application of the **??**, we have

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$$

Then $r_{n-2} = r_{n-1}q_n + 0$. Thus $\gcd(r_{n-2}, r_{n-1}) = r_{n-1}$. ■

When using the **??**, it can be tricky to keep track of what is happening. Doing a lot of examples can help.

Work in pairs to answer the following. Each pair will be assigned parts the following question.

In-class Problem 9 Find the greatest common divisors of the pairs of integers below and write the greatest common divisor as a linear combination of the integers.

(a) $(21, 28)$

Solution: By inspection: $28 - 21 = 7$.

Using the **??**: $a = 28, b = 21$

$$28 = 21(1) + 7 \qquad q_1 = 1, r_1 = 7 \qquad 7 = 21(1) + 28(-1)$$
$$21 = 7(3) + 0 \qquad q_2 = 3, r_2 = 0$$

so $28 + (-1)21 = 7 = (28, 21)$

(b) $(32, 56)$

Solution: Using the **??**: $a = 56, b = 32$

$$\begin{array}{lll} 56 = 32(1) + 24 & q_1 = 1, r_1 = 24 & 24 = 56(1) + 32(-1) \\ 32 = 24(1) + 8 & q_2 = 1, r_2 = 8 & 8 = 32(1) + 24(-1) = 32(1) + (56(1) + 32(-1))(-1) = 32(2) + 56(-1) \\ 32 = 8(4) + 0 & q_3 = 4, r_3 = 0. & \end{array}$$

so $56(-1) + 32(2) = 8 = (56, 32)$

(c) $(0, 113)$

Solution: Since $0 = 113(0)$, $(0, 113) = 113 = 0(0) = 113(1)$.

(a) $(78, 708)$

Solution: Using the **??**: $a = 708, b = 78$

$$\begin{array}{lll} 708 = 78(9) + 6 & q_1 = 9, r_1 = 6 & 6 = 708(1) + 78(-9) \\ 78 = 6(13) + 0 & q_2 = 13, r_2 = 0. & \end{array}$$

so $708(1) + 78(-6) = 6 = (78, 708)$

2.7 Primes

Learning Objectives. By the end of class, students will be able to:

- Prove every integer greater than 1 has a prime divisor.
- Prove that there are infinitely many prime numbers.

Reading assignment:

Read Strayer, Section 1.2

Turn in

- The proof method for Euclid's infinitude of primes is an important method. Summarize this method in your own words.

  Solution: Summaries will vary

- Identify any other new proof methods in this section

  Solution: Proof by construction may be new to some students. Students also identified:

  – Introducing a variable to aid in proof

  – Without loss of generality

- Exercise 22. Prove that 2 is the only even prime number.

Definition (prime and composite)**.** An integer $p > 1$ is *prime* if the only positive divisors of p are 1 and itself. An integer n which is not prime is *composite*.

Why is 1 not prime?

Lemma 2. Every integer greater than 1 has a prime divisor.

Proof Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the **??**, we may assume n is the least such integer. By definition, $n \mid n$, so n is not prime. Thus, n is composite and there exists $a, b \in \mathbb{Z}$ such that $n = ab$ and $1 < a < n$, $1 < b < n$. Since $a < n$, then it has a prime divisor p. But since $p \mid a$ and $p \mid n$, $p \mid n$. This contradicts our assumption, so no such integer exists. ■

We will not go over this proof in class.

Theorem 5 (Euclid's Infinitude of Primes)**.** There are infinitely many prime numbers.

Proof Assume by way of contradiction, that there are only finitely many prime numbers, so $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Now N has a prime divisor, say, p, by **??**. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p \mid N - p_1 p_2 \ldots p_n$, which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

One famous open problem is the Twin Primes Conjecture. A *conjecture* is a proposition you (or in this case, the mathematical community) believe to be true, but have not proven.

Conjecture 1 (Twin Prime Conjecture)**.** There are infinitely many prime number p for which $p + 2$ is also prime number.

Another important fact is there are arbitrarily large sequences of composite numbers. Put another way, there are arbitrarily large gaps in the primes. Another important proof method, which is a *constructive proof*:

Theorem 6. For any positive integer n, there are at least n consecutive positive integers.

Proof Given the positive integer n, consider the n consecutive positive integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

Let i be a positive integer such that $2 \leq i \leq n+1$. Since $i \mid (n+1)!$ and $i \mid i$, we have

$$i \mid (n+1)!+i, \quad 2 \leq i \leq n+1$$

by linear combination. So each of the n consecutive positive integers is composite. ■

In-class Problem 10 Let n be a positive integer with $n \neq 1$. Prove that if n^2+1 is prime, then n^2+1 can be written in the form $4k+1$ with $k \in \mathbb{Z}$.

Solution: Assume that n is a positive integer, $n \neq 1$, and n^2+1 is prime. If n is odd, then n^2 is odd, which would imply $n^2+1=2$, the only even prime. However, $n \neq 1$ by assumption. Thus, n is even.

By definition of even, there exists $j \in \mathbb{Z}$ such that $n=2k$ and $n^2=4j^2$. Thus, $n^2+1=4k+1$ when $k=j^2$.

In-class Problem 11 Prove or disprove the following conjecture, which is similar to **??**:

Conjecture 2. There are infinitely many prime number p for which $p+2$ and $p+4$ are also prime numbers.

2.8 The Fundamental Theorem of Arithmetic

Learning Objectives. By the end of class, students will be able to:

- Prove the Fundamental Theorem of Arithmetic
- Prove $\sqrt{2}$ is irrational .

Reading assignment:

Read Strayer, Section 1.5 through Proposition 1.17

Turn in

- Answer these questions about the proof of the Fundamental Theorem of Arithmetic (taken from Helping Undergraduates Learn to Read Mathematics):
  - Can you write a brief outline (maybe 1/10 as long as the theorem) giving the logic of the argument – proof by contradiction, induction on n, etc.? (This is KEY.)
  - What mathematical raw materials are used in the proof? (Do we need a lemma? Do we need a new definition? A powerful theorem? and do you recall how to prove it? Is the full generality of that theorem needed, or just a weak version?)
  - What does the proof tell you about why the theorem holds?
  - Where is each of the hypotheses used in the proof?
  - Can you think of other questions to ask yourself?
- Strayer states that the proof of **??** is "obvious from the Fundamental Theorem of Arithmetic and the definitions of (a, b) and $[a, b]$." Is this true? If so, why? If not, fill in the gaps.

Solution: Answers to both questions will vary between students.

Theorem 7 (Fundamental Theorem of Arithmetic)**.** Every integer greater than one can be written in the form $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. This factorization into primes is unique up to the ordering of the terms.

Proof We will show that every integer n greater than 1 has a prime factorization. First, note that all primes are already in the desired form. We will use induction to show that every composite integer can be factored into the product of primes. When $n = 4$, we can write $n = 2^2$, so 4 has the desired form.

Assume that for all integers k with $1 < k < n$, k can be written in the form $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. If n is prime, we are done, otherwise there exists $a, b \in \mathbb{Z}$ with $1 < a, b < n$ such that $n = ab$. By the induction hypothesis, there exist primes $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ and positive integers $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots b_s$ such that $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $b = q_1^{b_1} q_2^{a_2} \cdots q_s^{b_a}$. Then

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{a_2} \cdots q_s^{b_a}.$$

■

We will use an idea similar to the proof of the Fundamental Theorem of Arithmetic to proof the following:

In-class Problem 12

Proposition 5. $\sqrt{2}$ is irrational

As class, put the steps of the proof in order, then fill in the missing information.

Put the following steps in order:

10 Therefore, $\sqrt{2}$ is not rational. 2 Assume that $\sqrt{2}$ is rational, ie, there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$.
6 Therefore there exists $k \in \mathbb{Z}$ such that $p = 2k$ by definition of $2 \mid p$
4 Then (include to remove fractions and the radical) $2q^2 = p^2$.
5 Then $2 \mid p^2$ by definition of divisibility and $2 \mid p$ by **??**
9 This contradicts our assumption that $(p, q) = 1$ 7 Then (more algebraic manipulations) $2q^2 = 4k^2$ and $q^2 = 2k^2$.
1 We proceed by contradiction.
8 Then $2 \mid q^2$ and $2 \mid q$ by **??** and definition of $2 \mid q$
3 Without loss of generality, we may assume $(p, q) = 1$, since

Finally, work two groups. Each group will be assigned one of the following question.

In-class Problem 13 Let p be prime.

(a) If $(a, b) = p$, what are the possible values of (a^2, b)? Of (a^3, b)? Of (a^2, b^3)?

(b) If $(a, b) = p$ and $(b, p^3) = p^2$, find (ab, p^4) and $(a + b, p^4)$.

2.9 Arithmetic Progressions

Learning Objectives. By the end of class, students will be able to:

- State and prove facts about prime factorizations using the Fundamental Theorem of Arithmetic
- Prove there are infinitely many primes of the form $4n + 3$. .

Reading assignment:

Reading Strayer, Appendix B

Turn in Let R be the equivalence relation on $\mathbb{R}$ defined by

$$[a] = \{b \in \mathbb{R} : \sin(a) = \sin(b) \text{ and } \cos(a) = \cos(b)\}.$$

Prove that R is an equivalence relation on $\mathbb{R}$. Describe the equivalence classes on $\mathbb{R}$

Solution: Since $\sin(a) = \sin(a)$ and $\cos(a) = \cos(a)$, the relation R is reflexive.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, the $\sin(b) = \sin(a)$ and $\cos(b) = \cos(a)$, so the relation is symmetric.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, $\sin(b) = \sin(c)$ and $\cos(b) = \cos(c)$, then $\sin(a) = \sin(c)$ and $\cos(a) = \cos(c)$ is transitive.

Note that $\sin(a) = \sin(b)$ if $b = a + 2\pi k$ or $b = -a + \pi + 2\pi k$ for some $k \in \mathbb{Z}$, and $\cos(a) = \cos(b)$ if $b = a + 2\pi k$ or $b = -a + 2\pi k$ for some $k \in \mathbb{Z}$. These conditions are both true with $b = a + 2\pi k$. Thus, for $a \in [0, 2\pi)$,

$$[a] = \{\ldots, a - 4\pi, a - 2\pi, a, a + 2\pi, a + 4\pi, \ldots\}.$$

Prime factorizations

Note on $m^4 - n^4 = (m^2 - n^2)(m^2 + n^2)$: In order to sho w this is not prime, must prove that the factors cannot be 1 and the number itself. Hint: show that if one of the factors is 1 the other is 1 or 0 (or -1).

Corollary 2. Let $a, b \in \mathbb{Z}$ with $a, b > 0$. Then $[a, b] = ab$ if and only if $(a, b) = 1$.

A note on "if and only if" proofs:

- You can do two directions:
  - If $[a, b] = ab$, then $(a, b) = 1$.
  - If $(a, b) = 1$, then $[a, b] = ab$.
- Sometimes you can string together a series of "if and only if statements." Definitions are always "if and only if," even though rarely stated that way. For example, an integer n is even if and only if there exist an integer m such that $n = 2m$:
  - An integer n is even if and only if $2 \mid n$ (definition of even)
  - if and only if there exist an integer m such that $n = 2m$ (definition of $2 \mid n$).

Theorem 8 (Dirichlet's Theorem)**.** Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression

$$a, a + b, a + 2b, \ldots, a + nb, \ldots$$

contains infinitely many primes.

Surprisingly, this proof involves complex analysis. The statement that there are infinitely many prime numbers is the case $a = b = 1$.

Warning 1. You may not use this result to prove special cases, ie, specific values of a and b.

Lemma 3 (Lemma 1.23)**.** If $a, b \in \mathbb{Z}$ such that $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n, then ab can also be written in that form.

Proof Let $a = 4m + 1$ and $b = 4n + 1$ for some integers m and n. Then

$$\begin{aligned} ab &= (4m + 1)(4n + 1) \\ &= 16mn + 4m + 4n + 1 \\ &= 4(4mn + m + n) + 1. \end{aligned}$$

■

We will not go over the proof in class.

Proposition 6. There are infinitely may prime numbers expressible in the form $4n + 3$ where n is a nonnegative integer.

Proof (Similar to the proof that there are infinitely many prime numbers). Assume, by way of contradiction, that there are only finitely many prime numbers of the form $4n+3$, say $p_0 = 3, p_1, p_2, \ldots, p_r$, where the p_i are distinct. Let $N = 4p_1p_2 \cdots p_r + 3$. If every prime factor of N has the form $4n + 1$, then so does N, by repeated applications of **??**. Thus, one of the prime factors of N, say p, have the for $4n + 3$. We consider two cases:

Case 1, $p = 3$**:** If $p = 3$, then $p \mid N - 3$ by linear combination. Then $p \mid 4p_1p_2 \cdots p_r$. Then by **??**, either $3 \mid 4$ or $3 \mid p_1p_2 \cdots p_r$. This implies that $p \mid p_i$ for some $i = 1, 2, \ldots, r$. However, $p_1, p_2, \ldots, p_r$ are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq 3$.

Case 2, $p = p_i$ **for some** $i = 1, 2, \ldots, r$**:** If $p = p_i$, then $p \mid N - 4p_1p_2 \cdots p_r$ by linear combination. Then $p \mid 3$. However, $p_1, p_2, \ldots, p_r$ are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq p_i$ for $i = 1, 2, \ldots, r$.

Therefore, N has a prime divisor of the form $4n + 3$ which is not on the list $p_0, p_1, \ldots, p_r$, which contradicts the assumption that $p_0, p_1, \ldots, p_r$ are all primes of this form. Thus, there are infinitely many primes of the form $4n+3$. ■

3 Linear Diophantine Equations

3.1 Linear Diophantine Equations

Definition 1. A *Diophantine equation* is any equation in one or more variables to be solved in the integers.

Definition 2. Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$ with $a_1, a_2, \ldots, a_n$ not zero. A Diophantine equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

is a *linear Diophantine equation in the n variable* $x_1, \ldots, x_n$.

The question of whether there are solutions to Diophantine equations becomes harder when there is more than one variable.

Theorem 9. Let $ax + by = c$ be a linear Diophantine equation in the variables x and y. Let $d = (a, b)$. If $d \nmid c$, then the equation has no solutions; if $d \mid c$, then the equation has infinitely many solutions. Furthermore, if x_0, y_0 is a particular solution of the equation, then all solution are given by $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$ where $n \in \mathbb{Z}$.

Proof Since $d \mid a, d \mid b$, we have that $d \mid c$. So, if $d \nmid c$, then the given linear Diophantine equation has no solutions.

Assume that $d \mid c$. Then, there exists $r, s \in \mathbb{Z}$ such that

$$d = (a, b) = ar + bs.$$

Furthermore, $d \mid c$ implies $c = de$ for some $e \in \mathbb{Z}$. Then

$$c = de = (ar + bs)e = a(re) + b(se).$$

Thus, $x = re$ and $y = se$ are integer solutions.

Let x_0, y_0 be a particular solution to $ax + by = c$ Then, if $n \in \mathbb{Z}, x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$,

$$ax + by = a(x_0 + \frac{b}{d}n) + b(y_0 - \frac{a}{d}n) = ax_0 + \frac{abn}{d} + by_0 - \frac{abn}{d} = c.$$

We now need to show that every solution has this form. Let x and y be any solution to $ax + by = c$. Then

$$(ax + by) - (ax_0 + by_0) = c - c = 0.$$

Rearranging, we get

$$a(x - x_0) = b(y_0 - y).$$

Dividing both sides by d gives

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Now $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$ and $(\frac{a}{d}, \frac{b}{d}) = 1$, so $\frac{b}{d} \mid x - x_0$. Thus, $x - x_0 = \frac{b}{d}n$ for some $n \in \mathbb{Z}$. The proof for y is similar. ■

Example 1. Is $24x + 60y = 15$ is solvable?

Multiple Choice:

(a) Yes

(b) No ✓

Example 2. Find all solutions to $803x + 154y = 11$.

Using the Euclidean Algorithm, we find:

$$\begin{aligned} 803 &= 154 * 5 + 33 \\ 154 &= 33 * 4 + 22 \\ 33 &= 22 * 1 + 11 \end{aligned}$$

Thus

$$\begin{aligned} (803, 154) &= 33 - 22 \\ &= 33 - (154 - 33 * 4) = 33 * 5 - 154 \\ &= (803 - 154 * 5) * 5 - 154 = 803 * 5 - 154 * 26 \end{aligned}$$

Thus, all solutions to the Diophantine equation have the form $x = 5 + \frac{154}{11}n$ and $y = -26 - \frac{803}{11}n$.

Example 3. There is a famous riddle about Diophantus: "God gave him his boyhood one-sixth of his life, One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life."

That is: Diophantus's childhood was $1/6^{th}$ of his life, adolescence was $1/12^{th}$ of his life, after another $1/7^{th}$ of his life he married, his son was born 5 years after he married, his son then died at half the age that Diophantus died, and 4 years later Diophantus died.

The Diophantine equation that let's us solve this riddle is:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4.$$

Then, Diophantus's childhood was 14 years, his adolescence was 7 years, he married when he was 33, his son was born when he was 38 and died 42 years later, then Diophantus died when he was 84.

3.2 Greatest common divisors and Diophantine equations

Learning Objectives. By the end of class, students will be able to:

- Proof various facts about the greatest common divisor of three or more integers
- Find the solutions to a specific Diophantine equation in three variables
- Prove that when a Diophantine equation in three variables has a solutions, it has infinitely many.
- State when integer solution exist for $a_1x_1 + \cdots + a_kx_k = c$. .

Reading assignment:

Read: Strayer, Section 6.1

Turn in: Exercise 2a.

Greatest Common Divisors of three or more integers

Lemma 4. Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. Then $(a, b, c) = ((a, b), c)$.

Proof Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. Define $d = (a, b, c)$ and $e = ((a, b), c)$. We will show that $d \mid e$ and $e \mid d$. Since the greatest common divisor is positive, we can conclude that $d = e$[1].

Since $d = (a, b, c)$, we know $d \mid a, d \mid b$, and $d \mid c$. By **??**, which we are about to prove, $d \mid (a, b)$. Thus, d is a common divisor of (a, b) and c, so $d \mid e$.

Since $e = ((a, b), c)$, $e \mid (a, b)$ and $e \mid c$. Since $e \mid (a, b)$, we know $e \mid a$ and $e \mid b$ by **??**. Thus, e is a common divides of a, b and c ■

Lemma 5. Let $a, b \in \mathbb{Z}$, not both zero. Then any common divisor of a and b divides the greatest common divisor.

Proof Let $a, b \in \mathbb{Z}$, not both zero. By **??**, $(a, b) = am + bn$ for some $n, m \in \mathbb{Z}$. Thus, $d \mid (a, b)$ by linear combination. ■

Lemma 6. Let $a, b \in \mathbb{Z}$, not both zero. Then any divisor of (a, b) is a common divisor of a and b.

Proof Let c be a divisor of (a, b). Since $(a, b) \mid a$ and $(a, b) \mid b$, then $c \mid a$ and $c \mid b$ by transitivity. ■

Proposition 7. Let $a_1, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Then

$$(a_1, \ldots, a_n) = ((a_1, a_2, a_3, \ldots, a_{n-1}), a_n).$$

Proof Let $k = 2$. The since $((a_1, a_2)) = (a_1, a_2)$ by the definition of **??** of one integer, $(a_1, a_2) = ((a_1, a_2))$. The $k = 3$ case is the first lemma in this section (**??**).

Assume that for all $2 \leq k < n$,

$$(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k).$$

Let $d = (a_1, a_2, a_3, \ldots, a_k)$, $e = ((a_1, a_2, a_3, \ldots, a_k), a_{k+1}) = (d, a_{k+1})$, and $f = (a_1, a_2, a_3, \ldots, a_k, a_{k+1})$. We will show that $e \mid f$ and $f \mid e$. Since both e and f are positive, this will prove that $e = f$.

Note that $e \mid (a_1, a_2, a_3, \ldots, a_k)$ and $e \mid a_{k+1}$ by definition. Since $(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k)$ by the induction hypothesis, $e \mid (a_1, a_2, a_3, \ldots, a_{k-1})$ and $e \mid a_k$ by **??**. Again, by the induction hypothesis, $(a_1, a_2, a_3, \ldots, a_{k-1}) = ((a_1, a_2, a_3, \ldots, a_{k-2}), a_{k-1})$, so $e \mid a_{k-1}$ and $e \mid (a_1, a_2, a_3, \ldots, a_{k-2})$ by **??**. Repeat this process until we get

[1] This is not true in general and a common mistake. In general $d = \pm e$

$(a_1, a_2, a_3) = ((a_1, a_2), a_3)$, so $e \mid a_3$ and $e \mid (a_1, a_2)$ by **??**. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of **??**. By the generalized version of the **??** (**??**), $e \mid f$.

To show that $f \mid e$, we note that $f \mid a_1, a_2, \ldots, a_k, a_{k+1}$ by definition. Then $f \mid d$ by **??**. Since $e = (d, a_k)$, we have that $f \mid e$ by **??**. ■

Linear Diophanitine equations in three variables

Proposition 8. Let $a, b, c, d \in \mathbb{Z}$ and let $ax + by + cz = d$ be a linear Diophantine equation. If $(a, b, c) \nmid d$, then the equation has no solutions. If $(a, b, c) \mid d$, then there are infinitely many solutions.

In-class Problem 14 Find integral solutions to the Diophantine equation

$$8x_1 - 4x_2 + 6x_3 = 6.$$

(a) Since $(8, -4, 6) = 2$, solutions exist

(b) The linear Diophantine equation $8x_1 - 4x_2 = 4y$ has infinitely many solutions for all $y \in \mathbb{Z}$ by **??**. Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by **??**, since $(4, 6) = 2 \mid 6$. Find them.

Solution: By inspection, $y = 0, x_3 = 1$ is a particular solution. Then by **??**, the solutions have the form

$$\begin{aligned} y &= 0 + \frac{6n}{2}, \quad x_3 = 1 - \frac{4n}{2}, \quad \text{or} \\ y &= 0 + 3n, \quad x_3 = 1 - 2n, \qquad n \in \mathbb{Z}. \end{aligned}$$

(c) For a particular value of y, the Diophantine equation $8x_1 - 4x_2 = 0$ has solutions, find them.

Solution: By inspection, $x_1 = 1, x_2 = 2$ is a particular solution. Then by **??**, the solutions have the form

$$\begin{aligned} x_1 &= 1 + \frac{-4m}{4}, \quad x_2 = 2 - \frac{8m}{4}, \quad \text{or} \\ x_1 &= 1 - m, \quad x_2 = 2 - 2m, \qquad m \in \mathbb{Z}. \end{aligned}$$

(d) Then $x_1 = 1 - m, x_2 = 2 - 2m, x_3 = 1$ for $m \in \mathbb{Z}$.

***Proof of* ??** Let $a, b, c, d \in \mathbb{Z}$ and let $ax + by + cz = d$ be a linear Diophantine equation. If $(a, b, c) \mid d$, let $e = (a, b)$. Then

$$ax + by = ew \tag{1}$$

has a solution for all $w \in \mathbb{Z}$ by **??**. Similarly, the linear Diophantine equation

$$ew + cz = d \tag{2}$$

has infinitely many solutions by **??**, since $(e, c) = (a, b, c)$ by the **??** and $(a, b, c) \mid d$ by assumption. These solutions have the form

$$w = w_0 + \frac{cn}{(a, b, c)}, \quad z = z_0 - \frac{en}{(a, b, c)}, \qquad n \in \mathbb{Z},$$

where w_0, z_0 is a particular solution. Let x_0, y_0 be a particular solution to

$$ax + by = ew_0.$$

Then the general solution is

$$x = x_0 + \frac{bm}{e}, \quad y = y_0 - \frac{am}{e}, \qquad m \in \mathbb{Z}.$$

To verify that these formulas for x, y, and z give solutions to $ax + by + cz = d$, we substitute into equation **??** then **??**

$$\begin{aligned} e\left(w_0 + \frac{cn}{(a,b,c)}\right) + c\left(z_0 - \frac{en}{(a,b,c)}\right) &= d \\ ew_0 + cz_0 &= d \\ a\left(x_0 + \frac{bm}{e}\right) + b\left(y_0 - \frac{am}{e}\right) + cz_0 &= d \\ ax_0 + by_0 + cz_0 &= d. \end{aligned}$$

When $(a,b,c) \nmid d$, $\dfrac{a}{(a,b,c)}, \dfrac{b}{(a,b,c)}, \dfrac{c}{(a,b,c)} \in \mathbb{Z}$ by definition, but $\dfrac{d}{(a,b,c)}$ is not an integer. Therefore, there are no integers such that

$$\frac{a}{(a,b,c)}x + \frac{b}{(a,b,c)}y + \frac{c}{(a,b,c)}z = \frac{d}{(a,b,c)}.$$

■

4 Modular arithmetic

Modular arithmetic and congruences modulo m generalize the concept of even and odd. We typically think of even and odd as "divisible by 2" and "not divisible by 2", but often a more useful interpretation is even means "there is a remainder of 0 divided by 2" and "there is a remainder of 1 when divided by 2". This interpretation gives us more flexibility when replacing 2 by 3 or larger numbers. Instead of "divisible" or "not divisible" we have several gradations.

There's two major reasons. One is that, calculations are much simplier using modular arithmetic. We'll see later that taking MASSIVE powers of MASSIVE numbers is a fairly doable feat in modular arithmetic. The second reason is that by reducing a question from all integers to modular arithmetic, we often have an easier time seeing what solutions are not allowed.

4.1 Introduction to modular arithmetic

Learning Objectives. By the end of class, students will be able to:

- Prove that congruence modulo m is an equivalence relation on $\mathbb{Z}$.
- Define a complete residue system.
- Practice using modular arithmetic. .

Definition (divisibility definition of $a \equiv b \pmod{m}$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is *congruent to b modulo m* and write $a \equiv b \pmod{m}$ if $m \mid b - a$, and m is said to be the *modulus of the congruence*. The notation $a \not\equiv b \pmod{m}$ means a is not congruent to b modulo m, or a is *incongruent to b modulo m.*

Definition (remainder definition of $a \equiv b \pmod{m}$)**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is congruent to b modulo m if a and b have the same remainder when divided by m.

Be careful with this idea and negative values. Make sure you understand why $-2 \equiv 1 \pmod{3}$ or $-10 \equiv 4 \pmod{7}$.

Proposition 9 (Definitions of congruence modulo m are equivalent)**.** These two definitions are equivalent. That is, for $a, b, m \in \mathbb{Z}$ with $m > 0$, $m \mid b - a$ if and only if a and b have the same remainder when divided by m.

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$. By the **??**, there exists $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$aq_1m + r_1, 0 \leq r_1 < m, \text{ and}$$
$$bq_2m + r_2, 0 \leq r_2 < m.$$

If $m \mid b-a$, then by definition, there exists $k \in \mathbb{Z}$ such that $mk = b-a$. Thus, $mk = q_2m+r_2-q_1m-r_1$. Rearranging, we get $m(k - q_2 + q_1) = r_2 - r_1$ and $m \mid r_2 - r_1$. Since $0 \leq r_1 < m, 0 \leq r_2 < m$, we have $-m < r_2 - r_1 < m$. Thus, $r_2 - r_1 = 0$, so a and b have the same remainder when divided by m.

In the other direction, if $r_1 = r_2$, then $a - b = q_1m - q_2m = m(q_1 - q_2)$. Thus, $m \mid a - b$. ■

Example 4. We will eventually find a function that generates all integers solutions to the equation $a^2 + b^2 = c^2$ (this can be done with only divisibility, so feel free to try for yourself after class).

Modular arithmetic allows us to say a few things about solutions.

First, let's look at $\pmod{2}$**.** Note that $0^2 \equiv 0 \pmod{2}$ and $1^2 \equiv 1 \pmod{2}$.

Case 1: $c^2 \equiv 0 \pmod{2}$ In this case, $c \equiv 0 \pmod{2}$ and either $1^2 + 1^2 \equiv 0 \pmod{2}$ or $0^2 + 0^2 \equiv 0 \pmod{2}$. So, we know $a \equiv b \pmod{2}$. *(Note:* $\pmod{4}$ *will eliminate the* $a \equiv b \equiv 1 \pmod{2}$ *case)*

Case 2: $c^2 \equiv 1 \pmod{2}$ In this case, $c \equiv 1 \pmod{2}$ and either $0^2 + 1^2 \equiv 1 \pmod{2}$. So, we know $a \not\equiv b \pmod{2}$.

Let's start with $\pmod{3}$**.** Note that $0^2 \equiv 0 \pmod{3}$, $1^2 \equiv 1 \pmod{3}$, and $2^2 \equiv 1 \pmod{3}$.

Case 1: $c^2 \equiv 0 \pmod{3}$**.** In this case, $c \equiv 0 \pmod{3}$ and $0^2 + 0^2 \equiv 0 \pmod{3}$. So, we know $a \equiv b \equiv c \equiv 0 \pmod{3}$.

Case 2: $c^2 \equiv 1 \pmod{3}$**.** In this case, c could be 1 or 2 modulo 3. We also know $0^2 + 1^2 \equiv 1 \pmod{3}$, so $a \not\equiv b \pmod{3}$.

Case 3: $c^2 \equiv 2 \pmod{3}$ has no solutions.

So at least one of a, b, c is even, and at least one is divisible by 3.

We can use the idea of congruences to simplify divisibility arguments, as well as nonlinear Diophantine equations.

4.2 Practice with modular arithmetic

Learning Objectives. By the end of class, students will be able to:

- Prove that $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.
- Prove basic facts about modular arithmetic. .

Definition (complete residue system)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$. We call the set of all $b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ the *equivalence class of* a. A set of integers such that every integer is congruent modulo m is called a *complete residue system modulo* m.

Proposition 10. Let m be a positive integer. Then equivalence modulo m partition the integers. That is, every integer is in exactly one equivalence class modulo m.

Proof This is an immediate consequence of the fact that equivalence modulo m is an equivalence relation. ■

Notice that this arguments also simplifies the proof the $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proposition 11. The set $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$. By the **??**, there exist unique $q, r \in \mathbb{Z}$ such that $a = qm + r$ with $0 \leq r < m$. In fact, since $0 \leq r < m$, we know $r = 0, 1, \ldots, m-2$, or $m-1$. Therefore, every integer is in the equivalence class of $0, 1, \ldots, m-2$ or $m-1$ modulo m. Since every integer is in exactly one equivalence class modulo m, and the remainder from the division algorithm is unique, it is not possible for a to be equivalent to any other element of $\{0, 1, \ldots, m-1\}$. ■

In-class Problem 15 Practice: addition and multiplication tables modulo $3, 4, 5, 6, 7$. I am adding 9 to include an odd composite.

Solution: **Modulo** 3

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Modulo 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]

*	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Modulo 5

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[0]
[4]	[4]	[0]	[1]	[2]	[3]

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Modulo 6

+	[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]

Modulo 7

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Modulo 8

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Modulo 9

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

∗	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[0]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Definition $(a \equiv b \pmod{m})$**.** Let $a, b, m \in \mathbb{Z}$ with $m > 0$. From Friday, we have the following equivalent definitions of congruence modulo m :

(a) $a \equiv b \pmod{m}$ if and only if[2] $m \mid b - a$ (standard definition, generalizing even/odd based on divisibility)

(b) $a \equiv b \pmod{m}$ if and only if a and b have the same remainder with divided by m. That is, That is, there exists unique $q_1, q_2, r \in \mathbb{Z}$ such that $a = mq_1 + r,\ b = mq_2 + r,\ 0 \leq r < m$. (definition generalizing even/odd based on remainder)

(c) $a \equiv b \pmod{m}$ if and only if a and b differ by a multiple of m. That is, $b = a + mk$ for some $k \in \mathbb{Z}$. (arithmetic progression definition)

Different statements of the definition will be useful in different situations

Proposition 12. Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, then:

(a) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ implies $a \equiv c \pmod{m}$

(b) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$

(c) $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.

(d) $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$ implies $a \equiv b \pmod{d}$

(e) $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{mc}$ for $c > 0$.

Proof Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$.

(a) Assume $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then using the second definition of equivalence, there exists $q_1, q_2, q_3, r \in \mathbb{Z}$ such that

$$\begin{aligned} a &= mq_1 + r, \qquad 0 \leq r < m, \\ b &= mq_2 + r, \qquad 0 \leq r < m, \\ c &= mq_3 + r, \qquad 0 \leq r < m. \end{aligned}$$

Thus, a and c have the same remainder when divided by m, so $a \equiv c \pmod{m}$.

??/?? Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then by the third definition of equivalence, there exists $j, k \in \mathbb{Z}$ such that $b = a + mj$ and $d = c + mk$. Thus,

$$\begin{aligned} b + d &= a + c + m(j + k), \qquad \text{and} \\ bd &= ac + m(ak + cj + mjk). \end{aligned}$$

Thus, $a + c \equiv b + d \pmod{m}$ and $ac = bd \pmod{m}$.

(d) Assume $a \equiv b \pmod{m}$, and $d > 0$ with $d \mid m$. From the first definition of equivalence modulo m, $m \mid b - a$. Since division is transitive, $d \mid b - a$, so $a \equiv b \pmod{d}$.

(e) Assume $a \equiv b \pmod{m}$, and $c > 0$. From the third definition of equivalence modulo m, there exists $k \in \mathbb{Z}$ such that $b = a + mk$. Thus, $bc = ac + mck$, so $ac \equiv bc \pmod{mc}$.

■

Example 5. Note that $2 \equiv 5 \pmod{3}$. Then $4 \equiv 10 \pmod{3}$ by Proposition **????**, since $2 \equiv 2 \pmod{3}$. From part **??**, $4 \equiv 10 \pmod{6}$, but $2 \not\equiv 5 \pmod{6}$.

[2] all definitions are if and only if

4.3 Equivalence Relations

Learning Objectives. By the end of class, students will be able to:

- Prove a given set is an equivalence relation .

Reading assignment:

Read: Strayer, Appendix B

Turn in: Let R be the equivalence relation on $\mathbb{R}$ defined by

$$[a] = \{b \in \mathbb{R} : \sin(a) = \sin(b) \text{ and } \cos(a) = \cos(b)\}.$$

Prove that R is an equivalence relation on $\mathbb{R}$. Describe the equivalence classes on $\mathbb{R}$

Solution: Since $\sin(a) = \sin(a)$ and $\cos(a) = \cos(a)$, the relation R is reflexive.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, the $\sin(b) = \sin(a)$ and $\cos(b) = \cos(a)$, so the relation is symmetric.

If $\sin(a) = \sin(b)$ and $\cos(a) = \cos(b)$, $\sin(b) = \sin(c)$ and $\cos(b) = \cos(c)$, then $\sin(a) = \sin(c)$ and $\cos(a) = \cos(c)$ is transitive.

Note that $\sin(a) = \sin(b)$ if $b = a + 2\pi k$ or $b = -a + \pi + 2\pi k$ for some $k \in \mathbb{Z}$, and $\cos(a) = \cos(b)$ if $b = a + 2\pi k$ or $b = -a + 2\pi k$ for some $k \in \mathbb{Z}$. These conditions are both true with $b = a + 2\pi k$. Thus, for $a \in [0, 2\pi)$,

$$[a] = \{\ldots, a - 4\pi, a - 2\pi, a, a + 2\pi, a + 4\pi, \ldots\}.$$

In-class Problem 16 Prove that

$$[a] = \{b \in \mathbb{Z} : 3 \mid (a - b)\}$$

is an equivalence relation on $\mathbb{Z}$.

Proof Let $a, b \in \mathbb{Z}$. We must show that the relation is reflexive, symmetric, and transitive.

To show the relation is reflexive, we must show $a \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. Since $3 \mid a - a = 0$, $a \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$.

To show the relation is symmetric, we must show that if $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$, then $a \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$. If $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$, then there exists $k \in \mathbb{Z}$ such that $3k = a - x$. Therefore, $-3k = b - a$ and $a \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$.

To show the relation is transitive, we must show that if $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$ and $y \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$, then $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. If $x \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$, then there exists $k \in \mathbb{Z}$ such that $3k = a - x$. Similarly, if $y \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$, then there exists $m \in \mathbb{Z}$ such that $3m = x - y$. Therefore, $3(m + k) = a - k$ and $y \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation. ■

4.4 Linear congruences in one variable

Learning Objectives. By the end of class, students will be able to:

- Prove when a linear congruence in one variable has a solution
- Find all solutions to a linear congruence given a particular solution
- Find the number of incongruent solutions to a linear congruence .

Reading assignment:

Paper 1 due

Remark 1. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Every row/column of addition modulo m contains $\{0, 1, \ldots, m-1\}$.

We can also say that $a + x \equiv b \pmod{m}$ always has a solution, since $x \equiv b - a \pmod{m}$.

Theorem 10. Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and $d = (a, m)$. The linear congruence in one variable $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$. When $d \mid b$, there are exactly d incongruent solutions modulo m corresponding to the congruence classes

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \pmod{m}.$$

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and $d = (a, m)$. From the definition of congruence modulo m, $ax \equiv b \pmod{m}$ if and only if $m \mid (ax - b)$. That is, $ax \equiv b \pmod{m}$ if and only if $my = ax - b$ for some $y \in \mathbb{Z}$ from the definition of divisibility. Sine $ax - my = b$ is a linear Diophantine equation, **??** says solutions exist if and only if $(a, -m) = d \mid b$.

In the case that solutions exist, let x_0, y_0 be a particular solution to the linear Diophantine equation. Then x_0 is also a solution to the linear congruence in one variable, since $ax_0 - my_0 = b$, implies $ax_0 \equiv b \pmod{m}$. From **??**, all solutions have the from $x = x_0 + \frac{mn}{d}$ for all $n \in \mathbb{Z}$. We need to show that these solutions are in exactly d distinct congruence classes modulo m.

Consider the solutions $x_0 + \frac{mi}{d}$ and $x_0 + \frac{mj}{d}$ for some integers i and j. Then $x_0 + \frac{mj}{d} \equiv x_0 + \frac{mk}{d} \pmod{m}$ if and only if $m \mid \left(\frac{mi}{d} - \frac{mj}{d}\right)$. That is, if and only if there exists $k \in \mathbb{Z}$ such that $mk = \frac{mi}{d} - \frac{mj}{d}$. Rearranging this equation, we get that $x_0 + \frac{mj}{d} \equiv x_0 + \frac{mk}{d} \pmod{m}$ if and only if $dk = i - j$. Thus, $i \equiv j \pmod{\ }$ by definition of equivalence modulo d. Thus, the incongruent solutions to $ax \equiv b \pmod{m}$ are the congruence classes

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \pmod{m}.$$

■

Example 6. Let's consider several linear congruences modulo 12.

- The linear congruence $2x \equiv 1 \pmod{12}$ has no solutions, since $2 \nmid 1$.
- The linear congruence $8x \equiv b \pmod{12}$ has a solution if and only if $4 \mid b$. Considering the least nonnegative residues, the options for b are:
  - $8x \equiv 0 \pmod{12}$. The incongruent solutions are $0, 3, 6, 9 \pmod{12}$.
  - $8x \equiv 4 \pmod{12}$. The incongruent solutions are $2, 5, 8, 11 \pmod{12}$. Notice we cannot divide across the equivalence, since $2x \equiv 1 \pmod{12}$ has no solutions.

  - $8x \equiv 8 \pmod{12}$. The incongruent solutions are $1, 4, 7, 10 \pmod{12}$.
- The linear congruence $5x \equiv 1 \pmod{12}$ has solution $x \equiv 5 \pmod{12}$. Since $(5, 12) = 1$, the solution is unique.
- The linear congruence $5x \equiv 7 \pmod{12}$ has solution $x \equiv -1 \equiv 11 \pmod{12}$. Since $(5, 12) = 1$, the solution is unique. Note that instead of $12 + 5(-1) = 7$, we could have done

$$5(5x) \equiv 5(7) \equiv 11 \pmod{12}.$$

Corollary 3. [Corollary of **??**] Let $a, m \in \mathbb{Z}$ with $m > 0$. The linear congruence in one variable $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$. If $(a, m) = 1$, then the solution is unique modulo m.

Definition (multiplicative inverse of a modulo m)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. We call the unique incongruent solution to $ax \equiv 1 \pmod{m}$ the *multiplicative inverse of a modulo m*.

Example 7. Examples of multiplicative inverses:

- $5(3) \equiv 1 \pmod{7}$ so 3 is the multiplicative inverse of 5 modulo 7 and 5 is the multiplicative inverse of 3 modulo 7.
- $9(5) \equiv 1 \pmod{11}$ so 5 is the multiplicative inverse of 9 modulo 11 and 9 is the multiplicative inverse of 5 modulo 11.
- $8(-4) \equiv 8(7) \equiv 1 \pmod{11}$ so $7 \equiv -4 \pmod{11}$ is the multiplicative inverse of 8 modulo 11 and 8 is the multiplicative inverse of $7 \equiv -4 \pmod{11}$ modulo 11.
- $8(5) \equiv 1 \pmod{13}$ so 5 is the multiplicative inverse of 8 modulo 13 and 8 is the multiplicative inverse of 5 modulo 13.

Example using multiplicative inverses:

$$\begin{aligned} 6! &\equiv 6 * 5 * 4 * 3 * 2 * 1 \pmod{7} \\ &\equiv 6 * 5(3) * 4(2) * 1 \pmod{7} \\ &\equiv 6 \pmod{7} \end{aligned}$$

Think-Pair-Share 0.1. Find $10! \pmod{11}$ and $12! \pmod{13}$. Is there a pattern?

Solution:

$$\begin{aligned} 10! &\equiv 10 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 \pmod{11} \\ &\equiv 10 * 9(5) * 8(7) * 6(2) * 4(3) * 1 \pmod{11} \\ &\equiv 1 \pmod{11} \end{aligned}$$

$$\begin{aligned} 12! &\equiv 12 * 11 * 10 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 \pmod{13} \\ &\equiv 12 * 11(6) * 10(4) * 9(3) * 8(5) * 7(2) * 1 \pmod{13} \\ &\equiv 1 \pmod{13} \end{aligned}$$

For a prime p, $(p-1)! \equiv 1 \pmod{p}$.

Remark 2. We do need the condition that p is prime. For example, $3! \equiv 2 \pmod{4}$, and $8! \equiv 0 \pmod{9}$.

4.5 Chinese Remainder Theorem

Learning Objectives. By the end of class, students will be able to:

- Solve system of linear equations in one variable.
- Prove the Chinese Remainder Theorem. .

Example 8. Consider the system of linear equations

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \\ x &\equiv 1 \pmod 8. \end{aligned}$$

A slow way to find an integer x that satisfies all three congruences is to write out the congruence classes:

$$\begin{aligned} &2, 2+5, 2+5(2), \boxed{2+5(3)}, \dots \\ &3, 3+7, \boxed{3+7(2)}, 3+7(3), \dots \\ &1, 1+8, 1+8(2), \boxed{1+8(3)}, \dots \end{aligned}$$

and see what integers are on all three lists. In addition to being tedius, we this doesn't help find *all* such integers.

To find all such integers, define $M = 5(7)(8) = 280$, and $M_1 = \dfrac{M}{5} = 7(8), M_2 = \dfrac{M}{7} = 5(8), M_3 = \dfrac{M}{8} = 5(7)$. Then each M_i is relatively prime to M by construction. Thus, by **??** the congruences

$$\begin{aligned} M_1 x_1 &\equiv 1 \pmod 5, & 7(8)x_1 \equiv x_1 &\equiv 1 \pmod 5 \\ M_2 x_2 &\equiv 1 \pmod 7, & 5(8)x_2 \equiv 5x_2 &\equiv 1 \pmod 7 \\ M_3 x_3 &\equiv 1 \pmod 8, & 5(7)x_3 \equiv 3x_3 &\equiv 1 \pmod 8 \end{aligned}$$

have solutions. Thus, $x_1 \equiv 1 \pmod 5, x_2 \equiv 3 \pmod 7$, and $x_3 \equiv 3 \pmod 8$.

Note that

$$\begin{aligned} M_1 x_1(2) = 56(1)(2) &\equiv 2 \pmod 5, & M_2 \equiv M_3 &\equiv 0 \pmod 5 \\ M_2 x_2(3) = 40(3)(3) &\equiv 3 \pmod 7, & M_1 \equiv M_3 &\equiv 0 \pmod 7 \\ M_3 x_3(1) = 35(3)(1) &\equiv 1 \pmod 8, & M_1 \equiv M_2 &\equiv 0 \pmod 8 \end{aligned}$$

Thus,

$$x = M_1 x_1(2) + M_2 x_2(3) + M_3 x_3(1) = 56(1)(2) + 40(3)(3) + 35(3)(1)$$

is a solution to all three congruences.

Theorem 11 (Chinese Remainder Theorem)**.** Let $m_1, m_2, \dots m_k$ be pairwise relatively prime positive integers (that is, any pair $\gcd(m_i, m_j) = 1$ when $i \neq j$). Let $b_1, b_2, \dots, b_k$ be integers. Then the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_k} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \dots m_k$. This solution has the form

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k,$$

where $M_i = \dfrac{M}{m_i}$ and $M_i x_i \equiv 1 \pmod{m_i}$.

Proof Let $m_1, m_2, \dots m_k$ be pairwise relatively prime positive integers. We start by constructing a solution modulo $M = m_1 m_2 \dots m_k$. By construction, $M_i = \dfrac{M}{m_i}$ is an integer. Since each the m_i are pairwise relatively prime, $(M_i, m_i) = 1$. Thus, by **??**, for each i there is an integer x_i where $M_i x_i \equiv 1 \pmod{m_i}$. Thus $M_i x_i b_i \equiv b_i \pmod{m_i}$. We also have that $(M_i, m_j) = m_j$ when $i \neq j$, so $M_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Let

$$x = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdot + M_k x_k b_k.$$

Then $x \equiv M_i x_i b_i \equiv b_i \pmod{m_i}$ for each $i = 1, 2, \dots, k$ and $x \equiv M_i x_i b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Thus, we have found a solution to the system of equivalences.

To show the solution is unique modulo M, consider two solutions x_1, x_2. Then $x_1 \equiv x_2 \pmod{m_i}$ for each $i = 1, 2, \dots, k$. Thus $m_i \mid x_2 - x_1$. Since $(m_i, m_j) = 1$ when $i \neq j$, $M = [m_1, m_2, \dots, m_k]$ and $M \mid x_2 - x_1$. Thus, $x_1 \equiv x_2 \pmod{M}$. ■

4.6 Wilson's Theorem

Learning Objectives. By the end of class, students will be able to:

- Characterize when a is its own inverse modulo a prime.
- Prove Wilson's Theorem and its converse .

Reading assignment:

Read: Strayer, Section 2.4

Turn: Does this match with your conjecture from Exercise 5? If not, what is the difference?

Lemma 7. Let p be a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo m if and only if $a \equiv \pm 1 \pmod{p}$.

Proof Let p be a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo m if and only if $a^2 \equiv 1 \pmod{p}$ if and only if $p \mid a^2 - 1 = (a-1)(a+1)$. Since p is prime, $p \mid a-1$ or $a+1$ by **??**. Thus, $a \equiv \pm 1 \pmod{p}$. ■

Corollary 4. Let p be a prime. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Remark 3. It is important to note why we require p is prime. **??** is only true for primes:

- $8 \mid ab$ is true when $8 \mid a$, $8 \mid b$, $4 \mid a$ and $2 \mid b$, or $2 \mid a$ and $4 \mid b$.

Let $a = 2k+1$ for some integer k. Then

$$a^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Since either k or $k+1$ is even, $a^2 = 8m + 1$ for some $m \in \mathbb{Z}$. Thus, $a^2 \equiv 1 \pmod{8}$ for all odd integers $a \in \mathbb{Z}$.

- When $a \equiv 1 \pmod{8}$, then $8 \mid (a-1)$.
- When $a \equiv 3 \pmod{8}$, then $8k = a - 3$ for some $k \in \mathbb{Z}$. Thus $2 \mid (a-1)$ and $4 \mid (a+1)$.
- When $a \equiv 5 \pmod{8}$, then $8k = a - 5$ for some $k \in \mathbb{Z}$. Thus $4 \mid (a-1)$ and $2 \mid (a+1)$.
- When $a \equiv 7 \pmod{8}$, then $8 \mid (a+1)$.

Theorem 12 (Wilson's Theorem)**.** Let p be a prime number. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof When $p = 2$, $(2-1)! = 1 \equiv -1 \pmod{2}$. Now consider p an odd prime. By **??**, each $a = 1, 2, \ldots, p-1$ has a unique multiplicative inverse modulo p. **??** says the only elements that are their own multiplicative inverse are 1 and $p-1$. Thus $(p-2)!$ is the product of 1 and $\dfrac{p-3}{2}$ pairs of a, a' where $aa' \equiv 1 \pmod{p}$. Therefore,

$$\begin{aligned}(p-2)! &\equiv 1 \pmod{p}\\ (p-1)! &\equiv p - 1 \equiv -1 \pmod{p}.\end{aligned}$$

■

Wilson's Theorem is normally stated as above, but the converse is also true. It can also be a (very ineffective) prime test.

Proposition 13 (Converse of Wilson's Theorem)**.** Let n be a positive integer. If $(n-1)! \equiv 1 \pmod{n}$, then n is prime.

Proof Let a and b be positive integers where $ab = n$. It suffices to show that if $1 \leq a < n$, then $a = 1$. If $a = n$, then $b = 1$. If $1 \leq a < n$, then $a \mid (n-1)!$ by the definition of factorial. Then $(n-1)! \equiv -1 \pmod{n}$ implies $a \mid (n-1)! + 1$ by transitivity of division. Thus, $a \mid (n-1)! + 1 - (n-1)! = 1$ by linear combination and $a = 1$. Therefore, the only positive factors of n are 1 and n, so n is prime. ■

In-class Problem 17 (Part of Strayer, Chapter 2 Exercise 47) Let p be an odd prime. Use (a) $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ to show

(b) If $p \equiv 1 \pmod{4}$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod{p}$

(c) If $p \equiv 3 \pmod{4}$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$