
MAT-255 Number Theory–Spring 2024

Claire Merriman

Spring 2024

Contents

Wednesday, January 17: Introduction and Divisibility

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

- Understand the course structure
- Formally define even and odd
- Formally define “divides”
- Complete basic algebraic proofs.

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.

Go over syllabus highlights: Deadlines, make-up policy, in-class work, reading assignments.

Mathematical definitions, mathematical notation

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 results in both Strayer and Ernst.

Definition (Ernst, Definition 2.1). An integer n is *even* if $n = 2k$ for some $k \in \mathbb{Z}$. 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 (Strayer, Definition 4). 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 Strayer’s definition. We will formally prove that these definitions are *equivalent*, but for now, let’s use Ernst definition.

Theorem (Ernst, Theorem 2.2). *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 ??, 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. ■

Theorem (Ernst, Theorem 2.3). *The sum of two consecutive integers is 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 ??. ■

Divisibility

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.

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 odd as that sounds at first. This is because for any $a \in \mathbb{Z}$, $0 = a0$.

Reminding students about the reading for Friday.

Friday, January 19: Division algorithm, divisibility

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

- Prove facts about divisibility
- 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 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. For $n, m \in \mathbb{Z}$, how are the following mathematical expressions similar and how are they different? In particular, is each one a sentence or simply a noun?

(a) $n \mid m$

(b) $\frac{m}{n}$

(c) m/n

Solution: The first means “ n divides m ,” which is a relationship between n and m . This is a sentence. The other two are nouns, that is, the rational number $\frac{m}{n}$.

- Problem 2.8 Let $a, b, n, m \in \mathbb{Z}$. Determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

(a) If $a \mid n$, then $a \mid mn$

Solution: Let $a \mid n$. Then by ??, there exists $k \in \mathbb{Z}$ such that $ak = n$. Multiplying both sides of the equation by m gives

$$a(km) = mn,$$

so $a \mid mn$ by definition of ??.

(b) If 6 divides n , then 2 divides n and 3 divides n .

Solution: Let $6 \mid n$. Then by definition of ??, there exists $k \in \mathbb{Z}$ such that $6k = n$. By factoring out 6, we see that $2(3k) = 3(2k) = n$, so $2 \mid n$ and $3 \mid n$.

(c) If ab divides n , then a divides n and b divides n .

Solution: Let $ab \mid n$. Then by definition of ??, there exists $k \in \mathbb{Z}$ such that $abk = n$. Thus, we see that $a(bk) = b(ak) = n$, so $a \mid n$ and $b \mid n$.

- Problem 2.12. Determine whether the converse of each of Corollary 2.9, Theorem 2.10, and Theorem 2.11 is true. That is, for $a, n, m \in \mathbb{Z}$, determine whether each of the following statements is true or false. If a statement is true, prove it. If a statement is false, provide a counterexample.

(a) If a divides n^2 , then a divides n . (Converse of Corollary 2.9)

Solution: False; $4 \mid 4$ but $4 \nmid 2$.

(b) If a divides $-n$, then a divides n . (Converse of Theorem 2.10)

Solution: True. If $a \mid -n$, then by definition of ??, there exists $k \in \mathbb{Z}$ such that $ak = -n$. Multiplying both sides by -1 gives

$$-ak = a(-k) = n.$$

Therefore, $a \mid n$.

(c) If a divides $m + n$, then a divides m and a divides n . (Converse of Theorem 2.11)

Solution: False; $3 \mid 2 + 1$ but $3 \nmid 2$ and $3 \nmid 1$.

Reminders and Homework Guide Review

Updated In Class Work logistics: if I am able to give individual feedback during class or have pairs/groups present the answers during class, then I will not collect the work.

Logic, proof by contradiction, and biconditionals

We will begin by working through Ernst Section 2.2 through Example 2.21. Discuss Problem 2.17 as a class, and note that Problem 2.19 is on Homework 1.

In-class Problem 2 Construct a truth table for $A \Rightarrow B$, $\neg(A \Rightarrow B)$ and $A \wedge \neg B$

Solution:

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

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 $\neg A \wedge A$.

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 (Strayer, Lemma 1.3). Let $x \in \mathbb{R}$. Then $x - 1 < [x] \leq x$.

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

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, $x - 1 < [x]$. ■

Monday, January 22: Division algorithm and quantifiers

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

- Understand universal and existential quantifiers
- Negate statements using quantifiers
- Negate conditional statements using quantifiers
- Prove existence and uniqueness for the Division Algorithm.

Read Ernst Section 2.2 and Section 2.4

Turn in • Ernst, Problem 2.59. Both of the following sentences are propositions. Decide whether each is true or false. What would it take to justify your answers?

- (a) For all $x \in \mathbb{R}$, $x^2 - 4 = 0$.

Solution: False—find a counterexample.

- (b) There exists $x \in \mathbb{R}$ such that $x^2 - 4 = 0$.

Solution: True—find a solution x .

- Ernst Problem 2.64. Suppose the universe of discourse is the set of real numbers and consider the predicate $F(x, y) := “x = y^2”$. Interpret the meaning of each of the following statements.

- (a) There exists x such that there exists y such that $F(x, y)$.

Solution: There exists x such that for some y , $x = y^2$.

- (b) There exists y such that there exists x such that $F(x, y)$.

Solution: There exists $y \in \mathbb{R}$ such that for some $x \in \mathbb{R}$, $x = y^2$.

- (c) For all y , for all x , $F(x, y)$.

Solution: For all real numbers x and y , $x = y^2$.

Go over reading assignment at the start of class.

Division Algorithm (45 minutes)

Section 1.1 introduces the division algorithm, which will come up repeatedly throughout the semester, as well as the definition of divisors from last class.

Theorem (Division Algorithm). (*Theorem 1.4*) 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 have $r = a - bq$. 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 Strayer, Lemma 1.3, 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.

$$\begin{array}{r} a = bq_1 + r_1, \\ -(a = bq_2 + r_2), \\ \hline 0 = bq_1 + r_1 - bq_2 - r_2 = b(q_1 - q_2) + (r_1 - r_2). \end{array}$$

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

$$\begin{array}{r} 0 \leq r_2 < b \\ -b < -r_1 \leq 0 \\ \hline -b < r_2 - r_1 < b. \end{array}$$

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 3 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 4 Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that

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

(Outline updated from class)

(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

$$a = p|b| + s \quad \text{and} \quad 0 \leq s < |b|.$$

(ii) There are two cases:

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

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

(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 $q = \lfloor \frac{a}{b} \rfloor$. Here we have two cases:

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

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

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

Solution: Problem on Homework 2. You only need to provide one proof on Homework 2.

Wednesday, January 24: Primes

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

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

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.

Solution: Assume that there exists another even prime number, call it p . Then there exists $2 \mid p$ by the definition of even, but that implies that $p = 2$ by the definition of prime. Thus, 2 is the only even prime number.

Primes (50 minutes)

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 (Lemma 1.5). *Every integer greater than 1 has a prime divisor.*

We will not go over this proof in class.

Proof Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the [Well Ordering Principle](#), 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 $p \mid n$, $p \mid b$. This contradicts our assumption, so no such integer exists. ■

Theorem (Euclid's Infinitude of Primes). (*Theorem 1.6*) *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, \dots, 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 , $i = 1, 2, \dots, n$. Then $p \mid N - p_1 p_2 \cdots p_n$, which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

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*:

Proposition (Proposition 1.8). *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

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

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 ([Proposition 1.2](#)). So each of the n consecutive positive integers is composite. ■

In-class Problem 5 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 6 Prove or disprove the following conjecture, which is similar to Conjecture 1:

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

Solution: On Homework 2.

Friday, January 26: Quiz 1, Induction, Greatest Common Divisors

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

- Understand induction
- Prove basic facts about the greatest common divisor .

Read Strayer Appendix A.1: The First Principle of Mathematical Induction or Ernst [Section 4.1](#) and [Section 4.2](#)

Turn in Strayer Exercise Set A, Exercise 1a. If n is a positive integer, then

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof We proceed by induction. The base case is $n = 1$. Since $1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$, we are done.

Now assume that if $k \geq 1$ and for $n = k$,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Adding $(k+1)^2$ to both sides gives,

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\ &= \frac{(k+1)[2k^2 + k + 6k + 6]}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}. \end{aligned}$$

So the desired statement is true for $n = k + 1$. By the first principle of mathematical induction, the desired statement is true for all positive integers, and the proof is complete. ■

Quiz (10 minutes)

Greatest common divisor (20 min)

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 $\gcd(b_1, b_2, b_3, \dots, b_n)$.

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 (Proposition 1.11). *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 \gcd), 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 **Well Ordering Principle**. 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 $a \neq 0$.

More induction (15 minutes)

In-class Problem 7 *Theorems in Ernst Section 4.1*

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

Solution: We proceed by induction. When $n = 1$, $3 \mid 4^1 - 1 = 3$. 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 a divides b , 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.

Theorem (Ernst Theorem 4.7). *Let p_1, p_2, \dots, p_n be n distinct points arranged on a circle. Then the number of line segments joining all pairs of points is $\frac{n^2 - n}{2}$.*

Solution: We proceed by induction. When $n = 1$, there is only one point, so there are no lines connecting pairs of points. Additionally, $\frac{1^2 - 1}{2} = 0$.¹

Now assume $k \geq 1$ and the desired statement is true for $n = k$. Then the induction hypothesis is for k distinct points arranged in a circle, the number of line segments joining all pairs of points is $\frac{k^2 - k}{2}$. Adding a $(k + 1)^{\text{st}}$ point on the circle will add an additional k line segments joining pairs of points, one for each existing point. Note that

$$\frac{k^2 - k}{2} + k = \frac{k^2 + k}{2} = \frac{k^2 + k + k + 1 - (k + 1)}{2} = \frac{(k + 1)^2 - (k + 1)}{2}$$

In-class Problem 8 . Use the first principle of mathematical induction to prove each statement.

(b) If n is a positive integer, then

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

Solution: We proceed by induction. When $n = 1$, $1^3 = \frac{1^2(1 + 1)^2}{4}$. 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

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

Adding $(k + 1)^3$ to both sides gives

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + k^3 + (k + 1)^3 &= \frac{k^2(k + 1)^2 + 4(k + 1)^3}{4} \\ &= \frac{(k + 1)^2(k^2 + 4(k + 1))}{4} \\ &= \frac{(k + 1)^2(k + 2)^2}{4} \end{aligned}$$

Thus, 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.

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

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

Solution: We proceed by induction with base case $n = 5$. When $n = 5$, $32 = 2^5 > 5^2 = 25$. Thus, the statement is true for $n = 5$.

Now assume $k \geq 5$ and

$$2^k > k^2$$

¹Alternately, you could use $n = 2$ for the base case. Then there is one line connecting the only pair of points and $\frac{2^2 - 2}{2} = 1$

is true for $n = k$. Multiplying both sides of the inequality by 2 gives $2^{k+1} > 2k^2$. Notice that $2k^2 > k^2 + 2k + 1$ when $(k - 1)^2 > 0$, which is true for all $k \geq 5$. Thus

$$2^{k+1} > 2k^2 > (k + 1)^2.$$

Thus, 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.

Monday, January 29: More algebraic proofs and the Euclidean Algorithm

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

- Understand turning scratch work into proof for algebraic proofs
- Approach the floor function problems from Homework 1
- Prove the Euclidean Algorithm halts and generates the greatest common divisor of two positive integers.

Read None

Turn in The Learn TeX assignment using a copy of the Homework Template.

Example of proof like the floor function (30 minutes)

I did not go over the entire example in class. This also took the place of in class problems.

Let's explicitly think about the floor function as a function. That is, $f(x) : \mathbb{R} \rightarrow \mathbb{Z}$ (a function from the real numbers to the integers). Here is a restatement of the homework problem:

Homework Problem. For each of the following equations, find a domain for $f(x) = \lfloor x \rfloor$ make the statement true. Prove your statement.

- (a) $f(x) + f(x) = f(2x)$
- (b) $f(x + 3) = 3 + f(x)$
- (c) $f(x + 3) = 3 + x$

Here is a similar problem with proofs where $g : \mathbb{R} \rightarrow \mathbb{R}$. Note that the scratch work is one way to think about solving the problem but would not be included in the homework writeup.

Example 1. For each of the following equations, find the full domain for $g(x) = 3 \sin(\pi x)$ that makes the statement true. Prove that the equation is always true on this domain.

- (a) $g(x) + g(x) = g(2x)$

Scratch Work. We want to find a restriction such that $3 \sin(\pi x) + 3 \sin(\pi x) = 3 \sin(2\pi x)$. Using the double angle formula, we get

$$3 \sin(2\pi x) = 6 \sin(\pi x) \cos(2\pi x).$$

This means we are actually looking for

$$\begin{aligned} 6 \sin(\pi x) \cos(2\pi x) &= 6 \sin(\pi x) \\ \cos(2\pi x) &= 1. \end{aligned}$$

Solution: If $x \in \mathbb{Z}$, then $g(x) + g(x) = g(2x)$.

Proof Let $x \in \mathbb{Z}$. Then $g(x) + g(x) = 3 \sin(\pi x) + 3 \sin(\pi x) = 0$ and $g(2x) = 3 \sin(2\pi x) = 0$. Thus, $g(x) + g(x) = g(2x)$. ■

- (b) $g(x + 3) = 3 + g(x)$

Scratch Work. We want to find a restriction such that $3 \sin(\pi(x+3)) = 3 + 3 \sin(\pi x)$. Using the angle addition formula, we get

$$3 \sin(\pi x + 3\pi) = 3 \sin(\pi x) \cos(3\pi) + 3 \cos(\pi x) \sin(3\pi) = -3 \sin(\pi x).$$

This means we are actually looking for

$$\begin{aligned} -3 \sin(\pi x) &= 3 \sin(\pi x) + 3 \\ -1 &= 2 \sin(\pi x) \end{aligned}$$

Solution: If $x = 2k + \frac{7}{6}$ or $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$, then $g(x+3) = g(x) + 3$.

Proof Note that $g(x+3) = 3 \sin(\pi x + 3\pi) = -3 \sin(\pi x)$ by the angle addition formula. We will consider two cases:

Case 1: Let $x = 2k + \frac{7}{6}$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} g(x+3) &= -3 \sin(\pi x) \\ &= -3 \sin(2k\pi + \frac{7\pi}{6}) \\ &= \frac{3}{2}, \end{aligned}$$

$$\text{and } g(x) + 3 = 3 \sin(2k\pi + \frac{7\pi}{6}) + 3 = \frac{3}{2}.$$

Case 2: Let $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} g(x+3) &= -3 \sin(\pi x) \\ &= -3 \sin(2k\pi - \frac{\pi}{6}) \\ &= \frac{3}{2}, \end{aligned}$$

$$\text{and } g(x) + 3 = 3 \sin(2k\pi - \frac{\pi}{6}) + 3 = \frac{3}{2}.$$

Thus, $g(x+3) = g(x) + 3$ when $x = 2k + \frac{7}{6}$ or $x = 2k - \frac{1}{6}$ for some $k \in \mathbb{Z}$. ■

(c) Let $h(x) = x^2 - 1$. For each of the following equations, find the full domain for $h(x)$ that makes the statement true. Prove your statement.

(i) $h(x+3) = h(x) + 3$

(ii) $h(x+3) = x + 3$

Scratch Work. First, $h(x+3) = (x+3)^2 - 1 = x^2 + 6x + 8$.

For (a)

$$\begin{aligned} x^2 + 6x + 8 &= x^2 - 1 + 3 \\ 6x &= -6 \end{aligned}$$

For (b)

$$\begin{aligned} x^2 + 6x + 8 &= x + 3 \\ x^2 + 5x + 5 &= 0 \\ x &= \frac{-5 \pm \sqrt{5}}{2} \end{aligned}$$

Solution: (i) For $h(x) = x^2 - 1$, $h(x+3) = h(x) + 3$ if and only if $x = -1$.

Proof Let $h(x) = x^2 - 1$ and $x = -1$. Then $h(x+3) = 3 = 0 + 3 = h(x) + 3$.

To prove that this is the only such x , let $h(x+3) = h(x) + 3$. Then $x^2 + 6x + 8 = x^2 + 2$, which simplifies to $x = -1$. ■

(ii) For $h(x) = x^2 - 1$, $h(x+3) = x + 3$ if and only if $x = \frac{-5 \pm \sqrt{5}}{2}$.

Proof Let $h(x) = x^2 - 1$. First we consider the case $x = \frac{-5 + \sqrt{5}}{2}$. Then $h(x+3) = \frac{1 + \sqrt{5}}{2} = \frac{-5 + \sqrt{5}}{2} + 3 = x + 3$.

Next, we consider the case $x = \frac{-5 - \sqrt{5}}{2}$. Then $h(x+3) = \frac{1 - \sqrt{5}}{2} = \frac{-5 - \sqrt{5}}{2} + 3 = x + 3$.

To prove that these are the only such x , let $h(x+3) = x + 3$. Then $x^2 + 6x + 8 = x + 3$, which has the solutions $x = \frac{-5 \pm \sqrt{5}}{2}$. ■

The Euclidean Algorithm (20 minutes)

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 (Euclidean algorithm). Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the *Division Algorithm*, 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

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

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

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

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 $r_1 > r_2 > r_3 > \dots \geq 0$ 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 $\gcd(a, b) = b$.

Lemma 1.12 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 **Lemma 1.12**, we have

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

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.

Wednesday, January 31: Practice with the Euclidean Algorithm and the Fundamental Theorem of Arithmetic

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

- Use the (extended) ?? to write (a, b) as a linear combination of a and b
- Prove the Fundamental Theorem of Arithmetic
- Prove $\sqrt{2}$ is irrational.

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 Proposition 1.17 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.

Announcements

We have gotten a bit ahead of the reading. I adjusted the reading assignments—make sure to read Section 6.1 for Friday! This section does not use any facts beyond divisibility.

Practice with the ?? (15 minutes)

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.

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

32(d) $(0, 113)$

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

54(b) $(78, 708)$

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

$$708 = 78(9) + 6$$

$$q_1 = 9, r_1 = 6$$

$$6 = 708(1) + 78(-9)$$

$$78 = 6(13) + 0$$

$$q_2 = 13, r_2 = 0.$$

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

Fundamental Theorem of Arithmetic (35 minutes)

Observations from reading assignment

- Lemma 1.14 and $??$ (if $p \mid a_1 a_2 \dots a_n$ then $p \mid a_i$ for some i)
 - Lemma 1.14 is used as the base case in the proof of $??$
 - Prove factorization is unique by contradiction

Theorem (Fundamental Theorem of Arithmetic). *Every integer greater than one can be written in the form $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ 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.*

Alternate proof for existence 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 $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ 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 $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ and positive integers $a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s$ such that $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ and $b = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$. Then

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}.$$

■

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

In-class Problem 10

Proposition. $\sqrt{2}$ is irrational

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

Friday, February 2: Quiz 2, Greatest Common Divisors and Diophantine Equations

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

- Prove the formula for integer solutions to $ax + by = c$.
- State when integer solution exist for $a_1x_1 + \cdots + a_kx_k = c$.

Read Strayer, Section 6.1

Turn in Exercise 2a. Find all integer solutions to $18x + 28y = 10$

Quiz (10 minutes)

More greatest common divisor (40 min)

Lemma 1. 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 $d = e^2$.

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

Lemma 2. 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 Proposition 1.11, $(a, b) = am + bn$ for some $n, m \in \mathbb{Z}$. Thus, $d \mid (a, b)$ by linear combination. ■

Lemma 3. 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 1. Let $a_1, \dots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Then

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

Proof Let $k = 2$. The since $((a_1, a_2)) = (a_1, a_2)$ by the definition of greatest common divisor 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 $2 \leq k < n$,

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

Let $d = (a_1, a_2, a_3, \dots, a_k)$, $e = ((a_1, a_2, a_3, \dots, a_k), a_{k+1}) = (d, a_{k+1})$, and $f = (a_1, a_2, a_3, \dots, a_k, a_{k+1})$. 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 $e \mid (a_1, a_2, a_3, \dots, a_k)$ and $e \mid a_{k+1}$ by definition. Since $(a_1, \dots, a_k) = ((a_1, a_2, a_3, \dots, a_{k-1}), a_k)$ by the induction hypothesis, $e \mid (a_1, a_2, a_3, \dots, a_{k-1})$ and $e \mid a_k$ by Lemma ??. Again, by the induction hypothesis, $(a_1, a_2, a_3, \dots, a_{k-1}) = ((a_1, a_2, a_3, \dots, a_{k-2}), a_{k-1})$, so $e \mid a_{k-1}$ and $e \mid (a_1, a_2, a_3, \dots, a_{k-2})$ by Lemma ??. Repeat this process until we get $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$, so $e \mid a_3$ and $e \mid (a_1, a_2)$ by Lemma ??. Thus $e \mid a_1, a_2, \dots, a_{k+1}$ by repeated applications of Lemma ??. By the generalized version of the Lemma ?? on Homework 3, $e \mid f$.

To show that $f \mid e$, we note that $f \mid a_1, a_2, \dots, a_k, a_{k+1}$ by definition. Then $f \mid d$ by the generalized version of the Lemma ?? on Homework 3. Since $e = (d, a_{k+1})$, we have that $f \mid e$ by Lemma ??. ■

²This is not true in general and a common mistake on the homework. In general $d = \pm e$

Monday February 5: More facts about greatest common divisor and primes

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

- 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. .

Reading Strayer Section 1.5.

Turn in (a) The proof of Theorem 1.19 ends with “the cases $a = 1$ and $b > 1$, $a > 1$ and $b = 1$, and $a = b = 1$ are easily checked and are left as exercises. Do this.

(b) For Corollary 1.20, the book states “The (extremely easy) proof is left as an exercise for the reader.” Complete this proof.

Solution: (a) When $a = 1$ and $b > 1$, then $(a, b) = 1$ and $[a, b] = b$. Then $(a, b)[a, b] = b = ab$. Similarly for $a > 1, b = 1$. When $a = b = 1$, then $(a, b) = [a, b] = 1$ and $(a, b)[a, b] = 1 = ab$.

(b) From Theorem 1.19, we know that $\gcd(a, b) \operatorname{lcm}[a, b] = ab$. Since $\gcd(a, b)$, $\operatorname{lcm}[a, b]$, and ab are all positive, $\operatorname{lcm}[a, b] = \frac{ab}{\gcd(a, b)}$ if and only if $\gcd(a, b) = 1$.

Greatest common divisor and Diophantine equations (30 minutes)

Finish proof from Friday–end of notes from Week 3.

Proposition 2. 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 11 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 Theorem 6.2. Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by Theorem 6.2, since $(4, 6) = 2 \mid 6$. Find them.

Solution: By inspection, $y = 0, x_3 = 1$ is a particular solution. Then by Theorem 6.2, the solutions have the form

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

(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 Theorem 6.2, the solutions have the form

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

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

Proof of Proposition ?? 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 $e = (a, b, c)$. Then

$$ax + by = ew \quad (1)$$

has a solution for all $w \in \mathbb{Z}$ by Theorem 6.2. Similarly, the linear Diophantine equation

$$ew + cz = d \quad (2)$$

has infinitely many solutions by Theorem 6.2, since $(e, c) = (a, b, c)$ by the Lemma 1 and $(a, b, c) \mid d$ by assumption. These solutions have the form

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

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

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

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

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

■

Wednesday February 7: Arithmetic progressions and introduction to Congruences

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 $4n + 3$.
- Prove a given set is an equivalence relation.

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 $a \in [0, 2\pi)$,

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

Practice with gcd proofs (20 minutes)

Finish proof from Monday.

In-class Problem 12 (a) Do there exist integers x and y such that $x + y = 100$ and $(x, y) = 8$?

Solution: On Homework 3.

(b) Prove that there exist infinitely many pairs of integers x and y such that $x + y = 87$ and $(x, y) = 3$.

Scratch Work. Note that $87 = 3(29)$. To ensure that $(x, y) = 3$, not just $3 \mid x$ and $3 \mid y$, let $x = 3n$ where $29 \nmid n$.

Proof Let $x \in \mathbb{Z}$ with $3 \nmid x$. Let $y = 87 - x$. Then $3 \mid y$ by $3 \mid 87$ and $3 \nmid x$. Then $(x, y) = 3$ since $3 \mid y$ and $3 \nmid x$. Thus, there are infinitely many $x, y \in \mathbb{Z}$ such that $x + y = 87$ and $(x, y) = 3$. ■

In-class Problem 13 Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.

Using the hint in the back of the book and Exercise 37, which states $(ca, cb) = |c|(a, b)$ for all $a, b \in \mathbb{Z}$, not both 0.

Proof Let $(a + b, a - b) = d$ and note that $d \mid (a + b) + (a - b)$ and $d \mid (a + b) - (a - b)$ by linear combination. Thus, $d \mid 2a$ and $d \mid 2b$. Since a and b are relatively prime, $d \mid 2$. Thus, $d = 1$ or $d = 2$. ■

Prime factorizations (20 minutes)

Note on $m^4 - n^4 = (m^2 - n^2)(m^2 + n^2)$: In order to show 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 (Corollary 1.20). 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 (Dirichlet’s Theorem). *Let $a, b \in \mathbb{Z}$ with $a, b > 0$ and $(a, b) = 1$. Then the arithmetic progression*

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

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 (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.*

We will not go over the proof in class.

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

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

■

Proposition (Proposition 1.22). *There are infinitely many 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 $p_0 = 3, p_1, p_2, \dots, p_r$, 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 combinations. Then $p \mid 4p_1p_2 \cdots p_r$. Then by Corollary 1.15, either $3 \mid 4$ or $3 \mid p_1p_2 \cdots p_r$. This implies that $p \mid p_i$ for some $i = 1, 2, \dots, r$. However, p_1, p_2, \dots, 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 $i = 1, 2, \dots, r$: If $p = p_i$, then $p \mid N - 4p_1p_2 \cdots p_r$ by linear combinations. Then $p \mid 3$. However, p_1, p_2, \dots, p_r are distinct primes not equal to 3, so this is not possible. Therefore, $p \neq p_i$ for $i = 1, 2, \dots, r$.

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

Equivalence Relation Practice (10 minutes)

In-class Problem 14 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 $\text{there exists } k \in \mathbb{Z} \text{ such that } 3k = a - x$. 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 $\text{there exists } k \in \mathbb{Z} \text{ such that } 3k = a - x$. Similarly, if $y \in \{b \in \mathbb{Z} : 3 \mid (x - b)\}$, then $\text{there exists } m \in \mathbb{Z} \text{ such that } 3m = x - y$. Therefore, $3(m + k) = a - y$ and $y \in \{b \in \mathbb{Z} : 3 \mid (a - b)\}$. Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation. ■

Friday, February 9: 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.

Reading Strayer, Section 2.1 through Example 1.

Turn in The book concludes the section with a caution about division. It states that $6a \equiv 6b \pmod{3}$ for all integers a and b . Explain why this is true.

Solution: Since $3 \mid 6a - 6b = 3(2a - 2b)$, $6a \equiv 6b \pmod{3}$ for all integers a and b .

Quiz (10 min)

Definitions and examples of $(\text{mod } m)$ (20 minutes)

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 3 (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 Division Algorithm, there exists $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

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

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, $m \mid a - b$. ■

Congruences generalize the concept of evenness and oddness. We typically think of even and odd as “divisible by 2” and “not divisible by 2”, but a more useful interpretation is even means “there is no remainder when 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. As we’ve already seen, calculations get simplified for 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 is not allowed.

Example 2. *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 $(\text{mod } 2)$. *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: $(\text{mod } 4)$ 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 $(\text{mod } 3)$. *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

Monday, February 12: Peer review and introduction to congruences

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

- Prove basic facts about modular arithmetic.
- Understand gaps in argument and writing of proof of Exercise 83. Give classmates useful feedback on their proofs. .

Proposition and examples of $(\text{mod } m)$ (30 minutes)

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 if³ $m \mid b - a$ (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, 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 4 (Restatement of Propositions 2.1, 2.4, and 2.5). *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

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

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

- 2/3. 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,

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

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

- (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 $a \equiv b \pmod{d}$.

³all definitions are if and only if

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

Peer review Chapter 1 Exercise 83 (20 minutes)

Wednesday, February 14: More congruence facts

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

- Prove that $\{0, 1, \dots, m-1\}$ is a complete residue system modulo m .

Basic facts of working modulo m (35 minutes)

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 (Consequence 2.2, rephrased). 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 $\{0, 1, \dots, m-1\}$ is a complete residue system modulo m .

Proposition (Proposition 2.3). The set $\{0, 1, \dots, m-1\}$ is a complete residue system modulo m .

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$. By the Division Algorithm, 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 $r = 0, 1, \dots, m-2$, or $m-1$. Therefore, every integer is in the equivalence class of $0, 1, \dots, m-2$ 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 $\{0, 1, \dots, m-1\}$. ■

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

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]	[2]
[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]

Friday, February 16: 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.

Paper 1 due

Quiz (10 min)

Linear congruences in one variable (40 min)

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

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

Theorem (Strayer Theorem 2.6 and Porism 2.7). *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*

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

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. Since $ax - my = b$ is a linear Diophantine equation, Theorem 6.2 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 Theorem 6.2, all solutions have the form $x = x_0 + \frac{mn}{d}$ 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, $i \equiv j \pmod{d}$ by definition of equivalence modulo d . Thus, the incongruent solutions to $ax \equiv b \pmod{m}$ are the congruence classes

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

■

Example 4. *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*

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

Monday, February 19: 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. .

Reading None

Multiplicative inverses (20 min)

From Friday

Corollary (Corollary 2.8). *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 5. *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 1. We do need the condition that p is prime. For example, $3! \equiv 2 \pmod{4}$, and $8! \equiv 0 \pmod{9}$.

Simultaneous Linear congruences in one variable (30 min)

Example 6. 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 tedious, we this doesn't help find all such integers.

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

$$\begin{aligned}M_1x_1 &\equiv 1 \pmod{5}, & 7(8)x_1 &\equiv x_1 \equiv 1 \pmod{5} \\M_2x_2 &\equiv 1 \pmod{7}, & 5(8)x_2 &\equiv 5x_2 \equiv 1 \pmod{7} \\M_3x_3 &\equiv 1 \pmod{8}, & 5(7)x_3 &\equiv 3x_3 \equiv 1 \pmod{8}\end{aligned}$$

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

Note that

$$\begin{aligned}M_1x_1(2) &= 56(1)(2) \equiv 2 \pmod{5}, & M_2 &\equiv M_3 \equiv 0 \pmod{5} \\M_2x_2(3) &= 40(3)(3) \equiv 3 \pmod{7}, & M_1 &\equiv M_3 \equiv 0 \pmod{7} \\M_3x_3(1) &= 35(3)(1) \equiv 1 \pmod{8}, & M_1 &\equiv M_2 \equiv 0 \pmod{8}\end{aligned}$$

Thus,

$$x = M_1x_1(2) + M_2x_2(3) + M_3x_3(1) = 56(1)(2) + 40(3)(3) + 35(3)(1)$$

is a solution to all three congruences.

Theorem (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

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

has a unique solution modulo $M = m_1m_2 \dots m_k$. This solution has the form

$$x = M_1x_1b_1 + M_2x_2b_2 + \dots + M_kx_kb_k,$$

where $M_i = \frac{M}{m_i}$ and $M_ix_i \equiv 1 \pmod{m_i}$.

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, $M_i = \frac{M}{m_i}$ 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

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

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, $x_1 \equiv x_2 \pmod{M}$. ■

Wednesday, February 21: 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 Strayer, Section 2.4

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

Wilson's Theorem (50 min)

Lemma (Lemma 2.10). *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 Lemma 1.14. Thus, $a \equiv \pm 1 \pmod{p}$. ■

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

Remark 2. *It is important to note why we require p is prime. Lemma 1.14 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 (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 $a = 1, 2, \dots, p - 1$ 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 $\frac{p-3}{2}$ 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 (Proposition 2.12). *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 16 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 $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod{p}$

Solution: (b) Let p be a prime with $p \equiv 1 \pmod{4}$. Then $p = 4k + 1$ for some $k \in \mathbb{Z}$. From part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+1+1)/2} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}.$$

(c) Let p be a prime with $p \equiv 3 \pmod{4}$. Then $p = 4k + 3$ for some $k \in \mathbb{Z}$. From part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \equiv (-1)^{(4k+3+1)/2} \equiv (-1)^{2k+2} \equiv 1 \pmod{p}.$$

Theorem (On Paper 2, Polynomial Factorization option). *Let p be a prime number. The congruence $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Friday, February 23: Euler's Theorem and Fermat's Little Theorem

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

- Define and find a reduced residue system modulo m
- Define the Euler ϕ -function $\phi(n)$
- Prove Euler's Generalization of Fermat's Little Theorem.

Read Strayer, Section 2.5

Turn in Exercise 50. Prove that $9^{10} \equiv 1 \pmod{11}$ by following the steps of the proof of Fermat's Little Theorem.

Solution: Consider the 10 integers given by $9, 2(9), 3(9), \dots, 9(10)$. Note that $11 \mid 9i$ for $i = 1, 2, \dots, 10$ since 11 is prime and $11 \nmid 10$ and $11 \nmid i$. By ??, since $(9, 11) = 1$ if $9i \equiv 9j \pmod{11}$ implies $i \equiv j \pmod{11}$. Therefore, no two of $9, 2(9), 3(9), \dots, 9(10)$ are congruent modulo 11. So the least nonnegative residues modulo 11 of the integers $9, 2(9), 3(9), \dots, 9(10)$, taken in some order, must be $1, 2, \dots, p-1$. Then

$$(9)(2(9))(3(9)) \cdots (9(10)) \equiv (1)(2) \cdots (10) \pmod{11}$$

or, equivalently,

$$9^{10} 10! \equiv 10! \pmod{11}.$$

By ??, the congruence above becomes $-9^{10} \equiv -1 \pmod{11}$, which is equivalent to $9^{10} \equiv 1 \pmod{11}$.

Quiz (10 min)

Euler's Generalization of Fermat's Little Theorem (40 min)

There are several different ways to present the material in Sections 2.4 through 2.6. In class, we will do the other order: Fermat's Little Theorem to prove Wilson's Theorem. I will keep the result numbering from the book, so they will be out of order.

Definition (reduced residue system modulo m). Let m be a positive integer. We say that $\{r_1, r_2, \dots, r_k\}$ is a *reduced residue system modulo m* if

- $(r_i, m) = 1$ for all $i = 1, 2, \dots, k$,
- $r_i \not\equiv r_j \pmod{m}$ when $i \neq j$,
- for all $a \in \mathbb{Z}$ with $(a, m) = 1$, $a \equiv r_i \pmod{m}$ for some $i = 1, 2, \dots, k$.

Example 7. • The sets $\{1, 2, 3, 4, 5, 6\}$ and $\{5, 10, 15, 20, 25, 30, 35\}$ are both reduced residue systems modulo 7.

- If p is prime, then $\{1, 2, \dots, p-1\}$ is a complete residue system modulo p . If $p \neq 5$, $\{5, 10, \dots, 5(p-1)\}$ is a complete residue system modulo p .
- The sets $\{1, 5, 7, 11\}$ and $\{5, 25, 35, 55\}$ are both reduced residue systems modulo 12.

Lemma (Porism 2.18). Let m be a positive integer and let $\{r_1, r_2, \dots, r_k\}$ be a reduced residue system modulo m . If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \dots, ar_k\}$ is a reduced residue system modulo m .

This result is also implicitly used in the proof of ?? since $\{1, 2, \dots, p-1\}$ is a reduced residue system.

Proof Let $\{r_1, r_2, \dots, r_k\}$ be a reduced residue system modulo m and $a \in \mathbb{Z}$ with $(a, m) = 1$. Since $\{r_1, r_2, \dots, r_k\}$ and $\{ar_1, ar_2, \dots, ar_k\}$ have the same number of elements, it suffices to show that $(ar_i, m) = 1$ and $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$. If there exist some prime p such that $p \mid (ar_i, m)$ then $p \mid ar_i$ and $p \mid m$ by Definition (greatest common divisor). By Lemma 1.14, $p \mid a$ or $p \mid r_i$, so either $p \mid (a, m)$ or $p \mid (r_i, m)$. which is a contradiction. Thus, $(ar_i, m) = 1$.

By ??, $ar_i \equiv ar_j \pmod{m}$ if and only if $r_i \equiv r_j \pmod{\frac{m}{(a, m)}}$. Since $(a, m) = 1$, $ar_i \not\equiv ar_j \pmod{m}$ when $i \neq j$. ■

Definition (Euler ϕ -function). Let n be a positive integer. The Euler ϕ -function $\phi(n)$ is

$$\phi(n) = \#\{a \in \mathbb{Z} : a > 0 \text{ and } (a, n) = 1\}.$$

Remark 3. For a positive integer m , $\phi(m)$ is the number of reduced residues modulo m

Example 8. • $\phi(7) = 6$

- If p is prime, $\phi(p) = p - 1$
- $\phi(12) = 4$

Theorem (Euler's Generalization of ??). Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Corollary (Fermat's Little Theorem). Let p be prime and $a \in \mathbb{Z}$. If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof Let p be prime and $a \in \mathbb{Z}$, then $(a, p) = 1$ if and only if $p \nmid a$. Since $\phi(p) = p - 1$, $a^{p-1} \equiv 1 \pmod{p}$. ■

Warning 2. The converse of both of these theorems is false. The easiest example is $1^k \equiv 1 \pmod{m}$ for all positive integers k, m . Also note that $2^{341} \equiv 2 \pmod{341}$. Since $(2, 341) = 1$, there exists an integer a such that $2a \equiv 1 \pmod{341}$. Thus

$$a2^{341} \equiv (2a)2^{340} \equiv 2^{340} \equiv 2a \equiv 1 \pmod{341}.$$

However, $341 = (11)(31)$.

Proof of ?? Let m be a positive integer and let $\{r_1, r_2, \dots, r_{\phi(m)}\}$ be a reduced residue system modulo m . If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \dots, ar_{\phi(m)}\}$ is a reduced residue system modulo m by ??. Thus, for all $i = 1, 2, \dots, \phi(m)$, then $r_i \equiv ar_j \pmod{m}$ for some $j = 1, 2, \dots, \phi(m)$. Thus

$$r_1 r_2 \cdots r_{\phi(m)} \equiv ar_1 ar_2 \cdots ar_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Since $(r_i, m) = 1$, there exists $x_i \in \mathbb{Z}$ such that $r_i x_i \equiv 1 \pmod{m}$. Thus,

$$\begin{aligned} r_1 x_1 r_2 x_2 \cdots r_{\phi(m)} x_{\phi(m)} &\equiv a^{\phi(m)} r_1 x_1 r_2 x_2 \cdots r_{\phi(m)} x_{\phi(m)} \pmod{m} \\ 1 &\equiv a^{\phi(m)} \pmod{m}. \end{aligned}$$

■

Monday, February 26: Modular arithmetic calculations

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

- Use Wilson’s Theorem to find the least nonnegative residue modulo a prime
- Use Fermat’s Little Theorem to find the least nonnegative residue modulo a prime.

Reading None

Multiplicative inverses using Wilson’s Theorem (30 min)

First, some important algebra for multiplicative inverses

Example 9. (a) Let n be an odd positive integer. Then

$$2 \left(\frac{n+1}{2} \right) = n+1 \equiv 1 \pmod{n}.$$

So $\frac{n+1}{2}$ is the multiplicative inverse of 2 modulo n .

Think-Pair-Share 0.2. Why is $\left(\frac{n+1}{2}, n \right) = 1$?

We also have that $n - \frac{n+1}{2} = \frac{n-1}{2}$ and $n-2 \equiv -2 \pmod{n}$, so $\frac{n-1}{2}$ is the multiplicative inverse of $n-2$ modulo n . Another way to see this is

$$-2 \left(\frac{n-1}{2} \right) = -n+1 \equiv 1 \pmod{n}.$$

(b) Let m and n be positive integers such that $n \equiv 1 \pmod{m}$. Then there exists $k \in \mathbb{Z}$ such that $n = mk + 1$ by the definition. Then

$$-m \left(\frac{n-1}{m} \right) = -n+1 \equiv 1 \pmod{n}.$$

(c) Let m and n be positive integers such that $n \equiv -1 \pmod{m}$. Then there exists $k \in \mathbb{Z}$ such that $n = mk - 1$ by definition. Then

$$m \left(\frac{n+1}{m} \right) = n+1 \equiv 1 \pmod{n}.$$

Example 10. (a) Practice with Wilson’s Theorem: Find $\frac{31!}{23!} \pmod{11}$.

$$\begin{aligned} x \equiv \frac{31!}{23!} &\equiv 24(25)(26)(27)(28)(29)(30)(31) \pmod{11} \\ &\equiv 2(3)(4)(5)(6)(7)(8)(9) \pmod{11}. \end{aligned}$$

Then $-x \equiv 10! \equiv -1 \pmod{11}$. Therefore, $x \equiv 1 \pmod{11}$.

(b) Let p be an odd prime p , then $2(p-3)! \equiv -1 \pmod{p}$.

Proof Let p be an odd prime, then $(p-1)! \equiv -1 \pmod{p}$ by Wilson's Theorem. Multiplying both sides of the congruence by -1 gives $(p-2)! \equiv 1 \pmod{p}$. Since $(p-2)! = (p-3)!(p-2)$ by the definition of factorial, $p-2 \equiv -2 \pmod{p}$ is the multiplicative inverse of $(p-3)!$ modulo p . Thus,

$$\begin{aligned} -2(p-3)! &\equiv 1 \pmod{p} \\ 2(p-3)! &\equiv -1 \pmod{p}. \end{aligned}$$

■

Finding least nonnegative residue Fermat's Little Theorem (20 min)

Example 11. (a) Find the least nonnegative residue of 29^{202} modulo 13.

First, note that $29 \equiv 3 \pmod{13}$ and $202 = 12(10) + 82 = 12(10) + 12(6) + 10 = 12(16) + 10$. Thus,

$$29^{202} \equiv 3^{202} \equiv (3^{12})^{16} 3^{10} \equiv 1^{16} 3^{10} \pmod{13}$$

From here, we have two options:

Keep reducing: For this problem, this is the easier method:

$$3^{10} \equiv (3^3)^3 3 \equiv (27)^3 3 \equiv 3 \pmod{13}.$$

Find inverse: Note that $3^{12} \equiv 1 \pmod{13}$, so 3^{10} is the multiplicative inverse of $3^2 \equiv 9 \pmod{13}$. Since $9(3) \equiv 1 \pmod{13}$, $3^{10} \equiv 1 \pmod{13}$.

(b) Find the least nonnegative residue of 71^{71} modulo 17.

First, note that $71 \equiv 3 \pmod{17}$ and $71 = 8(8) + 7$. Thus,

$$71^{71} \equiv 3^{71} \equiv (3^8)^8 3^7 \equiv 1^8 3^7 \pmod{17}$$

Then

$$3^7 \equiv 3^3(3^3)(3) \equiv 10(10)(3) \equiv 10(-4) \equiv -6 \equiv 11 \pmod{17}.$$

Corollary (Corollary 2.14). Let p be a prime. If $a \in \mathbb{Z}$ with $p \nmid a$, then a^{p-2} is the multiplicative inverse of a modulo p .

Think-Pair-Share 0.3. Prove: Let p be a prime. If $a, k \in \mathbb{Z}$ with $p \nmid a$ and $0 \leq k < p$, then a^{p-k} is the multiplicative inverse of a^k modulo p .

Proof Let p be a prime. If $a \in \mathbb{Z}$ with $p \nmid a$, then by Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. If $k \in \mathbb{Z}$ with $0 \leq k < p$, then $a^{p-1} = a^{p-k} a^k$. Thus, $a^{p-k} a^k \equiv 1 \pmod{p}$. ■

Example 12. Find all incongruent solutions to $9x \equiv 21 \pmod{23}$.

Since $(9, 23) = 1$, there is only one incongruent solution modulo 23. By ??, 9^{21} is the multiplicative inverse of 9 modulo 23. Thus, $x \equiv 21(9^{21}) \pmod{23}$.

Alternately, 3^{20} is the multiplicative inverse of 3^2 modulo 23, so $x \equiv 21(3^{20}) \equiv (3^{21})7 \pmod{23}$. Since 3^{21} is the multiplicative inverse of 3 modulo 23, so $3^{21} \equiv 8 \pmod{23}$. Thus, $x \equiv 7(8) \equiv 10 \pmod{23}$.

Example 13. Let p be prime and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then $a^p \equiv b^p \pmod{p}$ if and only if $a \equiv b \pmod{p}$.

Proof Let p be prime and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$.

(\Leftarrow) If $a \equiv b \pmod{p}$, then $a^p \equiv b^p \pmod{p}$ by repeated applications of Proposition 2.4.

(\Rightarrow) If $a^p \equiv b^p \pmod{p}$, then by Fermat's Little Theorem,

$$a \equiv a^{p-1}a \equiv b^{p-1}b \equiv b \pmod{p}.$$

■

Warning 3. This statement is only true for primes. Since

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8}, \quad 2^2 \equiv 6^2 \pmod{8},$$

$$1^8 \equiv 3^8 \equiv 5^8 \equiv 7^8 \pmod{8}, \quad 2^8 \equiv 6^8 \pmod{8}.$$

Wednesday, February 28: Modular arithmetic calculations and the ϕ -function

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

- Use Euler's Theorem to find the least nonnegative residue modulo a composite
- Use Euler's Theorem to find the multiplicative inverse of an integer modulo m
- Prove $\phi(4)\phi(5) = \phi(20)$ using an outline that mirrors the proof that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

Reading None

Multiplicative inverses using Euler's Extension of Fermat's Little Theorem (30 min)

Example 14. (a) Find the least nonnegative residue of 29^{202} modulo 20.

The integers 1, 3, 7, 9, 11, 13, 17, 19 are relatively prime to 20. Thus $\phi(20) = 8$. Also note that $29 \equiv 9 \pmod{20}$ and $202 = 8(25) + 2$, so

$$29^{202} \equiv 9^{202} \equiv (9^8)^{25}9^2 \equiv 1^{25}9^2 \equiv 1 \pmod{20}$$

(b) Find the least nonnegative residue of 71^{71} modulo 16.

The integers 1, 3, 5, 7, 9, 11, 13, 15 are relatively prime to 16. Thus $\phi(16) = 8$. Also note that $71 \equiv 7 \pmod{16}$ and $71 = 8(8) + 7$, so

$$71^{71} \equiv 7^{71} \equiv (7^8)^8 7^7 \equiv 1^8 7^7 \pmod{16}$$

Since $7^8 \equiv 7^7 7 \equiv 1 \pmod{16}$, 7^7 is the multiplicative inverse of 7 modulo 16.

Using the Euclidean algorithm,

$$\begin{aligned} 16 &= 7(2) + 2, & 2 &= 16 + 7(-2) \\ 7 &= 2(3) + 1, & 1 &= 7 - 2(3) = 7 - (16 + 7(-2))(3) = 16(-3) + 7(7) \end{aligned}$$

Thus, $7(7) \equiv 1 \pmod{16}$, and $7^7 \equiv 7 \pmod{16}$.

Corollary (Corollary 2.19). Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then $a^{\phi(m)-1}$ is the multiplicative inverse of a modulo m .

Example 15. Find all incongruent solutions to $9x \equiv 21 \pmod{25}$.

The only positive integers less than 25 that are not relatively prime to 25 are 5, 10, 15, 20. Thus, $\phi(25) = 24 - 4 = 20$.

Since $(9, 25) = 1$, there is only one incongruent solution modulo 25. By ??, 9^{19} is the multiplicative inverse of 9 modulo 25. Thus, $x \equiv 21(9^{19}) \pmod{25}$.

Alternately, 3^{18} is the multiplicative inverse of 3^2 modulo 25, so $x \equiv 21(3^{18}) \equiv (3^{19})7 \pmod{25}$.

The previous example does not ask for the least nonnegative residue, but let's find it anyway.

Example 16. Find the least nonnegative residue of $(9^{19})21$ modulo 25.

First, note that $(9^{19})21 = (3^2)^{19}9(21)$. From here there are two options:

Factor 21:

$$(9^{19})21 \equiv (3^2)^{19}9(7) \equiv (3^{39})(7) \equiv (3^{20})(3^{19})(7) \pmod{25}$$

By Euler's Generalization of Fermat's Little Theorem, $3^{20} \equiv 1 \pmod{25}$ and by ??, 3^{19} is the multiplicative inverse of 3 modulo 25. Since $3(-8) \equiv -24 \equiv 1 \pmod{25}$, $3^{19} \equiv -8 \pmod{25}$. Thus,

$$(9^{19})21 \equiv (-8)(7) \equiv -56 \equiv 19 \pmod{25}.$$

Using $21 \equiv -4 \pmod{25}$:

$$(9^{19})21 \equiv (3^2)^{19}9(-4) \equiv (3^{38})(-4) \equiv (3^{20})(3^{18})(-4) \pmod{25}$$

Since $3^{20} = 3^{18}(3^2) \equiv 1 \pmod{25}$ by Euler's Generalization of Fermat's Little Theorem, 3^{18} is the multiplicative inverse of $3^2 = 9$ modulo 25. Since $9(-11) \equiv -99 \equiv 1 \pmod{25}$, we have $3^{18} \equiv -11 \pmod{25}$. Thus,

$$(9^{19})21 \equiv (-11)(-4) \equiv 44 \equiv 19 \pmod{25}.$$

In-class Problem 17 Let p, q be distinct primes. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Proof Let p, q be distinct primes. Then $\boxed{q^{p-1} \equiv 1} \pmod{p}$ and $\boxed{p^{q-1} \equiv 1} \pmod{q}$ by Fermat's Little Theorem, and $\boxed{p^{q-1} \equiv 1} \equiv 0 \pmod{p}$ and $\boxed{q^{p-1} \equiv 1} \equiv 0 \pmod{q}$ by definition.

Thus, $p^{q-1} + q^{p-1} \equiv \boxed{1} \pmod{p}$ and $p^{q-1} + q^{p-1} \equiv \boxed{1} \pmod{q}$ by modular addition.

(Finish proof using definition of congruence modulo p and q) ■

The Euler ϕ -function (20 min)

We will also find a formula for $\phi(n)$ in general. The following exercise will outline the general proof:

In-class Problem 18 Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) = \boxed{2}$ and $\phi(5) = \boxed{4}$, so $\phi(20) = \boxed{8}$.

- A number a is relatively prime to 20 if and only if a is relatively prime to $\boxed{4}$ and $\boxed{5}$
- We can partition the positive integers less than 20 into

$$\begin{aligned} 0 &\equiv \boxed{4} \equiv \boxed{8} \equiv \boxed{12} \equiv \boxed{16} \pmod{4} \\ 1 &\equiv \boxed{5} \equiv \boxed{9} \equiv \boxed{13} \equiv \boxed{17} \pmod{4} \\ 2 &\equiv \boxed{6} \equiv \boxed{10} \equiv \boxed{14} \equiv \boxed{18} \pmod{4} \\ 3 &\equiv \boxed{7} \equiv \boxed{11} \equiv \boxed{15} \equiv \boxed{19} \pmod{4} \end{aligned}$$

For any b in the range $0, 1, 2, 3$, define s_b to be the number of integers a in the range $0, 1, 2, \dots, 19$ such that $a \equiv b \pmod{4}$ and $\gcd(a, 20) = 1$. Thus, $s_0 = \boxed{0}$, $s_1 = \boxed{4}$, $s_2 = \boxed{0}$, and $s_3 = \boxed{4}$.

We can see that when $(b, 4) = 1$, $s_b = \phi(\boxed{5})$ and when $(b, 4) > 1$, $s_b = \boxed{0}$.

(c) $\phi(20) = s_0 + s_1 + s_2 + s_3$. Why?

Solution: All of the positive integers less than or equal to 20 is in exactly one of the congruence classes above. The s_i count how many integers in each congruence class are relatively prime to 20. If we add them up, we have counted all positive integers less than or equal to 20.

(d) We have seen that $\phi(20) = s_0 + s_1 + s_2 + s_3$, that when $(b, 4) = 1$, $s_b = \phi(5)$, and that when $(b, 4) > 1$, $s_b = 0$. Thus, we can say that $\phi(20) = 0 + \phi(\boxed{5}) + 0 + \phi(\boxed{5})$. To finish the “proof” we show that there are $\phi(\boxed{4})$ integers b where $(b, 4) = 1$.

Solution: There are $\boxed{4}$ congruence classes modulo 4. Of these, $\boxed{2} = \phi(\boxed{4})$ have elements that are relatively prime to 20. Thus, $\phi(20) = \phi(4)\phi(5)$.

Friday, March 1: The ϕ -function and a preview of primitive roots

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

- Prove that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

Reading None

Turn In Paper 2

Quiz (10 min)

The Euler ϕ -function (20 min)

We will use ?? as an outline to prove

Theorem (Theorem 3.2). Let m and n be positive integers where $(m, n) = 1$. Then $\phi(mn) = \phi(m)\phi(n)$.

maybe works?

Proof First, we note that an integer a is relatively prime to mn if and only if it is relatively prime to m and n , since m and n (together) have the same prime divisors as mn .

We can partition the positive integers less than mn into

$$\begin{array}{llll} 0 & \equiv m & \equiv 2m & \equiv \cdots \equiv (n-1)m \pmod{m} \\ 1 & \equiv m+1 & \equiv 2m+1 & \equiv \cdots \equiv (n-1)m+1 \pmod{m} \\ 2 & \equiv m+2 & \equiv 2m+2 & \equiv \cdots \equiv (n-1)m+2 \pmod{m} \\ \vdots & \vdots & \vdots & \vdots \\ m-1 & \equiv 2m-1 & \equiv 3m-1 & \equiv \cdots \equiv nm-1 \pmod{m} \end{array}$$

For any b in the range $0, 1, 2, \dots, m-1$, define s_b to be the number of integers a in the range $0, 1, 2, \dots, mn-1$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. For each equivalence class b , $\gcd(b, m) \mid km + b$ by linear combination. Thus, $s_b = 0$ if $(b, m) > 1$. If $\gcd(b, m) = 1$, the arithmetic progression, $\{b, m+b, 2m+b, \dots, (n-1)m+b\}$ contains n elements. By ??, the arithmetic progression is a complete residue system modulo n , so $\phi(n)$ elements are relatively prime to n and thus mn .

Thus, can see that when $(b, m) = 1$, $s_b = \phi(n)$ and when $(b, m) > 1$, $s_b = 0$.

Since all of the positive integers less than or equal to mn is in exactly one of the congruence classes above and the s_i count how many integers in each congruence class are relatively prime to mn , $\phi(mn) = s_0 + s_1 + \cdots + s_{m-1}$.

Since $\phi(m)$ of the $s_i = \phi(n)$ and the rest are 0, $\phi(mn) = s_0 + s_1 + \cdots + s_{m-1} = \phi(m)\phi(n)$.

■

In-class Problem 19 Complete the proof of ?? by proving that, if m, n , and i are positive integers with $(m, n) = (m, i) = 1$, then the integers $i, m + i, 2m + i, \dots, (n - 1)m + i$ form a complete system of residues modulo n .

btheo-prim-roots1

Monday, March 11: Order of elements modulo m

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

- Define the order of an element modulo m
- Find the order of an element modulo m
- Prove basic facts about the order of an element modulo m .

Reading None

Review of ϕ -function (15 minutes)

Remark 4. From before break, *Theorem 3.2* states if $(m, n) = 1$ for positive integers m and n , then $\phi(mn) = \phi(m)\phi(n)$. Thus, $\phi(63) = \phi(9(7)) = \phi(9)\phi(7) = 6(6)$.

Homework Problem 20 Chapter 2, Exercise 71, using *Euler's Generalization of Fermat's Little Theorem* and the *Chinese Remainder Theorem*

- (a) Let n be an integer not divisible by 3. Prove that $n^7 \equiv n \pmod{63}$.

Proof Let n be an integer that is not divisible by 3. By the *Chinese Remainder Theorem*,

$$x \equiv n^7 \pmod{7}$$

$$x \equiv n^7 \pmod{9}$$

has a unique solution modulo 63. By *Corollary 2.15*, $n^7 \equiv n \pmod{7}$.

Since $(n, 9) = 1$ and $\phi(9) = 6$, *Euler's Generalization of Fermat's Little Theorem* says that $n^6 \equiv 1 \pmod{9}$. Multiplying both sides of the congruence by n gives $n^7 \equiv n \pmod{9}$. Thus, $7 \mid n^7 - n$ and $9 \mid n^7 - n$ by definition. Since $(7, 9) = 1$, $63 \mid n^7 - n$, so $n^7 \equiv n \pmod{63}$. ■

- (b) Let n be an integer divisible by 9. Prove that $n^7 \equiv n \pmod{63}$.

Remark 5. Reviewing the proof of part ??: *Corollary 2.15* only requires the modulus is prime. *Euler's Generalization of Fermat's Little Theorem* does require $(n, m) = 1$, so you cannot use it for this problem, but $n \equiv 0 \pmod{9}$.

Order of a modulo m (35 minutes)

Definition 1 (order of a modulo m). Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then the order of a modulo m , denoted $\text{ord}_m a$, is the smallest positive integer n such that $a^n \equiv 1 \pmod{m}$.

a^1	a^2	a^3	a^4	a^5	a^6	$\text{ord}_7 a$
1	1	1	1	1	1	1
2	4	1	2	4	1	3
3	2	6	4	5	1	6
4	2	1	4	2	1	3
5	4	6	2	3	1	6
6	1	6	1	6	1	2

Table 1: Table of exponents modulo 7

There are many patterns in this table that we will talk about in the future, but the first is that $\text{ord}_m a \mid \phi(m)$.

Proposition (Proposition 5.1). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $\text{ord}_m a \mid n$. In particular, $\text{ord}_m a \mid \phi(m)$.*

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$.

(\Rightarrow) We want to show if $a^n \equiv 1 \pmod{m}$ for some positive integer n , then $\text{ord}_m a \mid n$.

By the [Division Algorithm](#), there exist unique integers q, r such that $n = (\text{ord}_m a)q + r$ and $0 \leq r < \text{ord}_m a$. Thus,

$$1 \equiv a^n \equiv a^{(\text{ord}_m a)q+r} \equiv (a^{(\text{ord}_m a)})^q a^r \equiv a^r \pmod{m}$$

since $a^{(\text{ord}_m a)} \equiv 1 \pmod{m}$ by definition of $\text{ord}_m a$. Since $a^r \equiv 1 \pmod{m}$ and $0 \leq r < \text{ord}_m a$, it must be that $r = 0$, otherwise $\text{ord}_m a$ is not the smallest positive integer where $a^k \equiv 1 \pmod{m}$.

(\Leftarrow) We want to show if $\text{ord}_m a \mid n$ for some positive integer n , then $a^n \equiv 1 \pmod{m}$.

If $\text{ord}_m a \mid n$, then there exists an integer k such that $(\text{ord}_m a)k = n$. Thus,

$$a^n \equiv (a^{\text{ord}_m a})^k \equiv 1 \pmod{m}$$

by definition of $\text{ord}_m a$. ■

Proposition (Proposition 5.2). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then $a^i \equiv a^j \pmod{m}$ for nonnegative integers i, j if and only if $i \equiv j \pmod{\text{ord}_m a}$.*

Example 17. Let $a = 2$ and $m = 7$. Since $\text{ord}_7 2 = 3$, $2^i \equiv 2^j \pmod{7}$ if and only if $i \equiv j \pmod{3}$.

Sketch of Proof Let $a = 2$ and $m = 7$. Without loss of generality, assume that $i \geq j$.

(\Rightarrow) Assume that $2^i \equiv 2^j \pmod{7}$. Then by exponent rules, $2^j 2^{i-j} \equiv 2^j \pmod{7}$. Since $(2^j, 7) = 1$, there exists a multiplicative inverse of 2^j modulo 7 by [Corollary 2.8](#), say $(2^j)'$. Multiplying both sides of the congruence by this inverse, we get,

$$2^{i-j} \equiv (2^j)' 2^j 2^{i-j} \equiv (2^j)' 2^j \equiv 1 \pmod{7}.$$

By $\text{ord}_7 2 = 3$, $\text{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\text{ord}_m a}$ by definition.

(\Leftarrow) Assume that $i \equiv j \pmod{3}$. Then $3 \mid i - j$ by definition. Since $\text{ord}_7 2 = 3$, $\text{ord}_m a \mid i - j$ states that $2^{i-j} \equiv 1 \pmod{7}$. Multiplying both sides of the congruence by 2^j gives $2^i \equiv 2^j \pmod{7}$. ■

Proof of ?? Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Without loss of generality, assume that $i \geq j$ for nonnegative integers i and j .

(\Rightarrow) Assume that $a^i \equiv a^j \pmod{m}$. Then by exponent rules, $a^j a^{i-j} \equiv a^j \pmod{m}$. Since $(a^j, m) = 1$ by assumption, there exists a multiplicative inverse of a^j modulo m by [Corollary 2.8](#), say $(a^j)'$. Multiplying both sides of the congruence by this inverse, we get,

$$a^{i-j} \equiv (a^j)' a^j a^{i-j} \equiv (a^j)' a^j \equiv 1 \pmod{m}.$$

By $\text{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\text{ord}_m a}$ by definition.

(\Leftarrow) Assume that $i \equiv j \pmod{\text{ord}_m a}$. Then $\text{ord}_m a \mid i - j$ by definition, and $\text{ord}_m a \mid i - j$ states that $a^{i-j} \equiv 1 \pmod{m}$. Multiplying both sides of the congruence by a^j gives $a^i \equiv a^j \pmod{m}$. ■

Wednesday, March 13: Primitive roots modulo a prime

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

- Find the order of an element modulo m using primitive roots.

Reading Uploaded notes

Turn in For each result in the scanned notes, identify the result in our textbook. If it is a special case of the theorem in the textbook, (ie, the reading only proves the theorem for primes or $d = q^s$), also note this.

Primitive roots and comparing Strayer to the reading

Definition 2 (primitive root). Let $r, m \in \mathbb{Z}$ with $m > 0$ and $(r, m) = 1$. Then r is said to be a primitive root modulo m if $\text{ord}_m r = \phi(r)$.

We saw in the reading that primitive roots always exist modulo a prime. What about composites?

Example 18. • Since $\phi(4) = 2$, and $\text{ord}_4 3 = 2$, 3 is a primitive root modulo 4. The powers $\{3^1, 3^2\}$ are a reduced residue system modulo 4.

- Since $\phi(6) = \phi(3)\phi(2) = 2$ and $\text{ord}_6 5 = 2$, 5 is a primitive root modulo 6. The powers $\{5^1, 5^2\}$ are a reduced residue system modulo 6.
- There are no primitive roots modulo 8. By Theorem 3.3, $\phi(8) = 4$. Since every odd number squares to 1 modulo 8, $\text{ord}_8 1 = 1$ and $\text{ord}_8 3 = \text{ord}_8 5 = \text{ord}_8 7 = 2$.
- Since $\phi(9) = 3^1(3 - 1) = 6$ by Theorem 3.3, we check:

$$2^1 = 1, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 \equiv 7 \pmod{9}, \quad 2^5 \equiv 5 \pmod{9}, \quad 2^6 \equiv 1 \pmod{9}$$

So 2 is a primitive root modulo 9, but are there more?

$$4^1 = 4, \quad 4^2 = 2^4 \equiv 7 \pmod{9}, \quad 4^3 = 2^6 \equiv 1 \pmod{9}$$

We can also use exponent rules and ?? to simplify some calculations. For example, $5 \equiv 2^5 \pmod{9}$, so $5^i \equiv 2^{5i} \equiv 2^j \pmod{9}$ if and only if $5i \equiv j \pmod{6}$.

$$\begin{aligned} 5^1 &\equiv 5 \pmod{9}, & 5^2 &\equiv 2^{10} \equiv 2^4 \equiv 7 \pmod{9}, & 5^3 &\equiv 2^{15} \equiv 2^3 \equiv 8 \pmod{9}, \\ 5^4 &\equiv 2^{20} \equiv 2^2 \equiv 4 \pmod{9}, & 5^5 &\equiv 2^{25} \equiv 2^1 \equiv 2 \pmod{9}, & 5^6 &\equiv 1 \pmod{9}, \end{aligned}$$

$$7^1 \equiv (-2) \equiv 7 \pmod{9}, \quad 7^2 \equiv (-2)^2 \equiv 4 \pmod{9}, \quad 7^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod{9}$$

$$\begin{aligned} \text{ord}_9(1) &= 1 \\ \text{ord}_9(2) &= \text{ord}_9(5) = 6 \\ \text{ord}_9(4) &= \text{ord}_9(7) = 3 \\ \text{ord}_9(8) &= 2 \end{aligned}$$

Proposition (Proposition 5.3). Let r be a primitive root modulo m . Then

$$\{r, r^2, \dots, r^{\phi(m)}\}$$

is a set of reduced residues modulo m .

This is the general version of [Proposition 10.3.2](#), using exponents $1, 2, \dots, \phi(m)$ instead of $0, 1, \dots, \phi(m) - 1$. Since Strayer's statement of ?? is already stated and proved for composites, and both lists have the same number of elements, the only changes to the proof is replacing $p - 1$ with $\phi(m)$. Note $a^0 \equiv a^{\phi(m)} \equiv 1 \pmod{m}$ when $(a, m) = 1$.

Proposition (Proposition 5.4). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then*

$$\text{ord}_m(a^i) = \frac{\text{ord}_m a}{\gcd(\text{ord}_m a, i)}.$$

In-class Problem 21 *Use only the results through ??/Lemma 10.3.5 to prove the primitive root version:*

Proposition. *Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m . If i is a positive integer, then*

$$\text{ord}_m(r^i) = \frac{\phi(m)}{\gcd(\phi(m), i)}.$$

Proof Let $i, r, m \in \mathbb{Z}$ with $i, m > 0$ and r a primitive root modulo m . Then $\text{ord}_m r = \phi(m)$ by definition. Let $d = (\phi(m), i)$. Then there exists positive integers j, k such that $\phi(m) = dj, i = dk$ and $(j, k) = 1$ by [Proposition 1.10](#). Then using the preceding equations and exponent rules, we find

$$(a^i)^j = (a^{dk})^{\phi(m)/d} = (a^{\phi(m)})^k \equiv 1 \pmod{m}$$

since $a^{\phi(m)} \equiv 1 \pmod{p}$ by definition. ?? says that $\text{ord}_p(a^i) \mid j$.

Since $a^{i \text{ord}_p(a^i)} \equiv (a^i)^{\text{ord}_p(a^i)} \equiv 1 \pmod{p}$ by definition of order, ?? says that $\text{ord}_p a \mid i \text{ord}_p(a^i)$. Since $\text{ord}_p a = \phi(m) = dj$ and $i = dk$, we have $dj \mid dk \text{ord}_p(a^i)$ which simplifies to $j \mid k \text{ord}_p(a^i)$. Since $(j, k) = 1$, we can conclude $j \mid \text{ord}_p(a^i)$.

Since $\text{ord}_p(a^i) \mid j, j \mid \text{ord}_p(a^i)$ and both values are positive, we can conclude that $\text{ord}_p(a^i) = j$. Finally, we have

$$\text{ord}_p(a^i) = j = \frac{\phi(m)}{d} = \frac{\phi(m)}{(\phi(m), i)}.$$

■

Exercises cited in the reading, also on Homework 6:

In-class Problem 22 *Prove the following statement, which is the converse of [Proposition 10.3.2](#):*

Let p be prime, and let $a \in \mathbb{Z}$. If every $b \in \mathbb{Z}$ such that $p \nmid b$ is congruent to a power of a modulo p , then a is a primitive root modulo p .

In-class Problem 23 *Prove the following generalization of [Lemma 10.3.5](#)*

Lemma. *Let $n \in \mathbb{Z}$ and let x_1, x_2, \dots, x_m be reduced residues modulo n . Suppose that for all $i \neq j$, $\text{ord}_n(x_i)$ and $\text{ord}_n(x_j)$ are relatively prime. Then*

$$\text{ord}_n(x_1 x_2 \cdots x_m) = (\text{ord}_n x_1)(\text{ord}_n x_2) \cdots (\text{ord}_n x_m).$$

Friday, March 15: Lagrange's Theorem

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

- Prove Lagrange's Theorem.

Reading Strayer Section 5.2

Turn in: (a) Exercise 10a: Determine the number of incongruent primitive roots modulo 41

Solution: Since 41 is prime, Theorem 10.3.7 says there are $\phi(41) = 40$ primitive roots modulo 41.

(b) Exercise 11a: Find all incongruent integers having order 6 modulo 31.

Solution: From Appendix E, Table 3, 3 is a primitive root modulo 31. By ??, the elements of order 6 modulo 31 are those where

$$6 = \text{ord}_{31}(3^i) = \frac{\phi(31)}{(\phi(31), i)} = \frac{30}{5}.$$

The positive integers less than 31 where $(30, i) = 5$ are $i = 5, 25$. So the elements of order 6 are $3^5, 3^{25}$.

The problem does not ask for the least nonnegative residues. However, we can also find those:

$$3^5 \equiv (-4)(9) \equiv -5 \equiv 26 \pmod{31}$$

$$3^{25} \equiv (-5)^5 \equiv (-6)^2(-5) \equiv -25 \equiv 6 \pmod{31}$$

Quiz (10 minutes)

Lagrange's Theorem

The goal is to finish proving the [Primitive Root Theorem](#) with a look at polynomials.

Theorem (Theorem 5.7 (Lagrange)). *Let p be a prime number and let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

for integers a_0, a_1, \dots, a_n . Let d be the greatest integer such that $a_d \not\equiv 0 \pmod{p}$ then d is the degree of $f(x)$ modulo p . Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most d incongruent solutions. We call these solutions roots of $f(x)$ modulo p .

Proof from class We proceed by induction on the degree d .

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$. Then $f(x) \equiv a_1 x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by [Corollary 2.8](#), there is a unique solution modulo p to $a_1 x + a_0 \equiv 0 \pmod{p}$.

Induction Hypothesis: Assume that for all $k < d$, if $f(x)$ has degree k modulo p , then

$$f(x) \equiv a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

We will proceed by contradiction. That is, assume that there exists $f(x)$ with degree d modulo p and at least $d + 1$ roots modulo p . Call these roots $r_1, r_2, \dots, r_d, r_{d+1}$. Consider the polynomial

$$g(x) = a_d(x - r_1)(x - r_2) \cdots (x - r_d).$$

Then $f(x)$ and $g(x)$ have the same leading term modulo p . The polynomial $h(x) = f(x) - g(x)$ is either the 0 polynomial or it has degree less than d modulo p .

If $h(x)$ is the 0 polynomial, then

$$h(r_1) \equiv h(r_2) \equiv \cdots \equiv h(r_{d+1}) \equiv 0 \pmod{p}$$

and

$$f(r_1) \equiv f(r_2) \equiv \cdots \equiv f(r_{d+1}) \equiv 0 \pmod{p}$$

implies

$$g(r_1) \equiv g(r_2) \equiv \cdots \equiv g(r_{d+1}) \equiv 0 \pmod{p}.$$

That is,

$$a_d(r_{d+1} - r_1)(r_{d+1} - r_2) \cdots (r_{d+1} - r_d) \equiv 0 \pmod{p}.$$

Since p is prime, repeated applications of Homework 4, Problem 9a gives that one of $a_d, r_{d+1} - r_1, r_{d+1} - r_2, \dots, r_{d+1} - r_d$ is 0 modulo p . Now, $a_d \not\equiv 0 \pmod{p}$ by assumption, and the r_i are distinct modulo p , so we have a contradiction. Thus, $h(x)$ is not the 0 polynomial.

Since r_1, r_2, \dots, r_d are roots of both $f(x)$ and $g(x)$, they are also roots of $h(x)$. This contradicts the induction hypothesis, since $h(x)$ has degree less than d by construction.

Thus, $f(x)$ has at most d incongruent solution modulo p . ■

Modified proof from Strayer We proceed by induction on the degree d .

First, for degree $d = 0$, note that $f(x) \equiv a_0 \not\equiv 0 \pmod{p}$ by assumption, so $f(x) \equiv 0 \pmod{p}$ for 0 integers.

Base Case: $d = 1$. Then $f(x) \equiv a_1x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by Corollary 2.8, there is a unique solution modulo p to $a_1x \equiv -a_0 \pmod{p}$.

Induction Hypothesis: Assume that for all $k < d$, if $f(x)$ has degree k modulo p , then

$$f(x) \equiv a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \equiv 0 \pmod{p}$$

has at most k incongruent solutions.

If the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions we are done. Otherwise, assume that there exists at least one solution, say a . Dividing $f(x)$ by $(x - a)$ gives

$$f(x) \equiv (x - a)q(x) \pmod{p}$$

where $q(x)$ is a polynomial of degree $d - 1$ modulo p . Since $q(x)$ has at most $d - 1$ roots modulo p by the induction hypothesis, there are at most $d - 1$ incongruent additional roots of $f(x)$ modulo p . Thus, there are a total of at most d incongruent roots modulo p . ■

Proposition (Proposition 5.8). *Let p be prime and m a positive integer where $m \mid p - 1$. Then*

$$x^m \equiv 1 \pmod{p}$$

has m incongruent solutions modulo p .

Proof Let p be prime and m a positive integer where $m \mid p-1$. Then there exists $k \in \mathbb{Z}$ such that $mk = p-1$. Then

$$x^{p-1} - 1 = (x^m - 1)(x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1)$$

By Fermat's Little Theorem, there are $p-1$ incongruent solutions to $x^{p-1} - 1 \equiv 0 \pmod{p}$, namely $1, 2, \dots, p-1$. We will show that m of these are solutions to $x^m - 1 \equiv 0 \pmod{p}$ and the rest are solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$.

By ??, there are at most $(k-1)m$ solutions to $x^{(k-1)m} + x^{(k-2)m} + \cdots + x^{2m} + x^m + 1 \equiv 0 \pmod{p}$. Thus, there are at least $p-1 - (k-1)m = m$ incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$. Since there are also at least m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ by ??, there are exactly m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ and thus $x^m \equiv 1 \pmod{p}$. ■

Definition 3 (Roots of unity). Let p be prime and m a positive integer. We call the solutions to

$$x^m \equiv 1 \pmod{p}$$

the m^{th} roots of unity modulo p .

Monday, March 18: Proof of Primitive Root Theorem

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

- Find the number of roots of unity modulo m
- Prove primitive roots exist modulo a prime.

Reading None

Roots of unity (35 minutes)

Finish proof of Proposition 5.8

In-class Problem 24 Let p be prime, m a positive integer, and $d = (m, p - 1)$. Prove that $a^m \equiv 1 \pmod{p}$ if and only if $a^d \equiv 1 \pmod{p}$.

Solution: Let p be prime, m a positive integer, and $d = (m, p - 1)$. Let $a \in \mathbb{Z}$. If $p \mid a$, then $a^i \equiv 0 \pmod{p}$ for all positive integers i . Thus, we are only considering $a \in \mathbb{Z}$ such that $p \nmid a$. Otherwise, $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem.

By Proposition 5.1, $a^m \equiv 1 \pmod{p}$ if and only if $\text{ord}_p a \mid m$. Similarly, $a^{p-1} \equiv 1 \pmod{p}$ if and only if $\text{ord}_p a \mid p - 1$. Thus, $\text{ord}_p a$ is a common divisor of m and $p - 1$. Combining and gives $\text{ord}_p a$ is a common divisor of m and $p - 1$ if and only if $\text{ord}_p a \mid d$. One final application of Proposition 5.1 gives $\text{ord}_p a \mid d$ if and only if $a^d \equiv 1 \pmod{p}$.

In-class Problem 25 Let p be prime and m a positive integer. Prove that

$$x^m \equiv 1 \pmod{p}$$

has exactly $(m, p - 1)$ incongruent solutions modulo p .

Proof Let p be prime, m a positive integer, and $d = (m, p - 1)$. By ??, $x^m \equiv 1 \pmod{p}$ if and only if $x^d \equiv 1 \pmod{p}$. By Proposition 5.8 there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, there are exactly d solutions to $x^m \equiv 1 \pmod{p}$. ■

Primitive roots modulo a prime (15 minutes)

We will now prove the existence of primitive roots modulo a prime combining the two methods from the reading: we will show that when $d \mid p - 1$, there are $\phi(d)$ incongruent integers of order d modulo p , like Strayer. However, we will prove this using the method from Lemma 10.3.4 instead of results from Chapter 3.

Theorem (Theorem 5.9). Let p be a prime and let $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p - 1$. Then there are exactly $\phi(d)$ incongruent integers of order d modulo p .

Proof Let p be a prime and let $d \in \mathbb{Z}$ with $d > 0$ and $d \mid p - 1$. First we will prove the theorem for $d = q^s$ modulo p where q is prime and s is a nonnegative integer.

By Proposition 5.8, there are exactly q^s incongruent solutions to

$$x^{q^s} \equiv 1 \pmod{p} \tag{3}$$

and exactly q^{s-1} incongruent solutions to

$$x^{q^{s-1}} \equiv 1 \pmod{p}. \quad (4)$$

Since $(x^{q^{s-1}})^q = x^{q^s}$, all solutions to (??) are solutions to (??). Thus, there are exactly $q^s - q^{s-1} = q^{s-1}(q-1)$ integers a where $a^{q^s} \equiv 1 \pmod{p}$ and $a^{q^{s-1}} \not\equiv 1 \pmod{p}$. Thus, by Proposition 5.1, $\text{ord}_p a \mid q^s$ and $\text{ord}_p a \nmid q^{s-1}$. Since q is prime, $\text{ord}_p a = q^s$. By Theorem 3.3, $\phi(q^s) = q^s - q^{s-1} = q^{s-1}(q-1)$, so we have shown there are $\phi(q^s)$ incongruent integers with order q^s modulo p .

Now we will prove the general case. Let

$$d = q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k}$$

for distinct primes q_1, q_2, \dots, q_k and positive integers s_1, s_2, \dots, s_k . Let a_1, a_2, \dots, a_k be elements of order $q_1^{s_1}, q_2^{s_2}, \dots, q_k^{s_k}$ respectively. Consider $a = a_1 a_2 \cdots a_k$ and a^2, a^3, \dots, a^d . By Homework 6, Problem 6, a has order $q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k} = d$. By Proposition 5.8, there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, a, a^2, \dots, a^d are all incongruent solutions to $x^d \equiv 1 \pmod{p}$ by Proposition 5.1. By Proposition 5.4, $\text{ord}_p a^i = \frac{d}{(d, i)} = d$ if and only if $(d, i) = 1$. Since there are $\phi(d)$ such integers i , there are in fact $\phi(d)$ incongruent integers with order d modulo p . ■

Corollary (Corollary 5.10). *Let p be prime. There are exactly $\phi(p-1)$ primitive roots modulo p .*

Wednesday, March 20: Introduction to quadratic residues

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

- Define a quadratic residue modulo m
- Prove that the quadratic congruence $x^2 \equiv a \pmod{p}$ has zero or one solution modulo a prime when $p \nmid a$
- Use the solution to a quadratic congruence modulo a prime to find the other solution.

Reading: Strayer Section 4.1

Turn in: Exercise 3 Find all incongruent solutions of the quadratic congruence $x^2 \equiv 1 \pmod{8}$. Is it not true that quadratic congruences have either no solutions or exactly two incongruent solutions? Explain.

Solution: As we have seen on many previous questions, $x^2 \equiv 1 \pmod{8}$ for all odd numbers. So there are 4 incongruent solutions modulo 8, which is not a contradiction because 8 is not an odd prime number.

Finish proof of the existence of primitive roots modulo a prime (10 minutes)

Quadratic residues (40 minutes)

Definition 4 (quadratic residue). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The a is said to be a quadratic residue modulo m if the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable in \mathbb{Z} . Otherwise, a is said to be a quadratic nonresidue modulo m .*

Remark 6. *When finding squares modulo m , we only need to check up to $\frac{m}{2}$, since $(-a)^2 = a^2$ and $m - a \equiv -a \pmod{m}$.*

In-class Problem 26 Find all incongruent quadratic residues and nonresidues modulo 2, 3, 4, 5, 6, 7, 8, and 9.

Solution: I also included solutions modulo 10, 11, 12

Modulus	least nonnegative reduced residues	quadratic residues	quadratic residues	non-
2	1	1	N/A	
3	1, 2	1	2	
4	1, 3	1	3	
5	1, 2, 3, 4	1, 4	2, 3	
6	1, 5	1	5	
7	1, 2, 3, 4, 5	1, 2, 4	3, 5, 6	
8	1, 3, 5, 7	1	3, 5, 7	
9	1, 2, 4, 5, 7, 8	1, 4, 7	2, 4, 8	
10	1, 3, 7, 9	1, 9	3, 7	
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10	1, 3, 4, 5, 9	2, 6, 7, 8, 10	
12	1, 5, 7, 11	1	5, 7, 11	

Lemma (Generalized Porism 4.2). *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable, say with $x = x_0$, then $m - x_0$ is also a solution. If $m > 2$, then $x_0 \not\equiv m - x_0 \pmod{m}$, and solutions occur in pairs.*

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{m}$ is solvable, say with $x = x_0$. Then

$$(m - x_0)^2 \equiv (-x_0)^2 \equiv x_0^2 \equiv a \pmod{m}.$$

If $x_0 \equiv m - x_0 \pmod{m}$, then $2x_0 \equiv m \equiv 0 \pmod{m}$ and $m \mid 2x_0$ by definition. Since $(a, m) = 1$, it must be that $(x_0, m) = 1$ since $(x_0, m) \mid (a, m)$. Thus, $m \mid 2$, so $m = 2$. Therefore, when $m > 2$, then $x_0 \not\equiv m - x_0 \pmod{m}$, and solutions occur in pairs. ■

Remark 7. *Since $x_0 \equiv m - x_0 \pmod{m}$ implies $x_0 \equiv \frac{m}{2}$, we can say that if $x^2 \equiv a \pmod{m}$ is solvable and $\frac{m}{2}$ is not a solution, then solutions occur in pairs.*

Proposition (Proposition 4.1). *Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Then the quadratic congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p .*

Proof Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Consider the quadratic congruence $x^2 \equiv a \pmod{p}$. If no solutions exist, we are done.

If solutions to the quadratic congruence exist, then ?? says that there are at least two solutions, since $p > 2$. Theorem 5.7 (Lagrange) says that there are at most two solutions to $x^2 - a \equiv 0 \pmod{p}$ and therefore $x^2 \equiv a \pmod{p}$. Thus, there are exactly two incongruent solutions modulo p . ■

Proposition (Proposition 4.3). *Let p be an odd prime number. Then there are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues modulo p .*

Proof Consider the $p - 1$ quadratic congruences

$$\begin{aligned}x^2 &\equiv 1 \pmod{p} \\x^2 &\equiv 2 \pmod{p} \\&\vdots \\x^2 &\equiv p - 1 \pmod{p}.\end{aligned}$$

Since each congruence has either zero or two incongruent solutions modulo p by ??, and no integer is a solution to more than one of the congruences, exactly half are solvable. Therefore, there are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues modulo p . ■

Friday, March 22: Legendre symbol

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

- Define the Legendre symbol
- Prove basic facts about the Legendre symbol
- Use the definition and basic facts to find the Legendre symbol for specific examples.

Reading: Strayer Section 4.2 through Example 4

Turn in: Exercise 12 Use Euler's Criterion to evaluate the following Legendre symbols

(a) $\left(\frac{11}{23}\right)$

Solution: $\left(\frac{11}{23}\right) \equiv 11^{(23-1)/2} \equiv 11^{11} \pmod{23}$ By Euler's Criterion. Then

$$11^{11} \equiv (11^2)^5(11) \equiv 6^5(11) \equiv (6^2)(6^3)(11) \equiv (13)(9)(11) \equiv (-90)(11) \equiv -1 \pmod{23}$$

(b) $\left(\frac{-6}{11}\right)$

Solution: $\left(\frac{-6}{11}\right) \equiv (-6)^{(11-1)/2} \equiv (-6)^5 \pmod{11}$ By Euler's Criterion. Then

$$(-6)^5 \equiv ((6)^2)^2(-6) \equiv 3^2(-6) \equiv -54 \equiv 1 \pmod{11}$$

Quiz (15 minutes)

Technical difficulties with printer and projector.

Legendre symbol (35 minutes)

Definition 5 (Legendre symbol). Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. The Legendre symbol, denoted $\left(\frac{a}{p}\right)$, is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

Theorem (Euler's Criterion). Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

We will not prove this today, but we will use it to go over the solution to the reading assignment and to prove the following proposition.

Proposition (Proposition 4.5). Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then

$$(a) \quad \left(\frac{a^2}{p}\right) = 1$$

$$(b) \quad \text{If } a \equiv b \pmod{p} \text{ then } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

$$(c) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

Proof Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then a^2 is a quadratic residue modulo p , by definition, so $\left(\frac{a^2}{p}\right) = 1$ by the definition of the Legendre symbol.

If $a \equiv b \pmod{p}$, then either both a and b are quadratic residues modulo p or both a and b are quadratic nonresidues modulo p . Thus $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

For the last part, ?? gives

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv (a^{(p-1)/2})(b^{(p-1)/2}) \equiv \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$$

■

Monday, March 25: Quadratic residue of -1

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

- Prove Euler's Criterion
- Classify when -1 is a quadratic residue modulo an odd prime.

Reading None

Proof of Euler's Criterion

We will prove Euler's Criterion.

Theorem (Euler's Criterion). *Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Proof Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. If there exists $b \in \mathbb{Z}$ such that $b^2 \equiv a \pmod{p}$, then $\left(\frac{a}{p}\right) = 1$ by definition. Note that

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} \equiv b^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem. Thus $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

If a is a quadratic nonresidue modulo p , consider the reduced residue system $\{1, 2, \dots, p-1\}$. For each element c of the list, there exists a unique element d , also on the list, such that $cd \equiv a \pmod{p}$ by Theorem 2.6 since $(a, p) = 1$. Since a is a quadratic nonresidue by assumption, $c \not\equiv d \pmod{p}$. Thus, there are $\frac{p-1}{2}$ pairs c, d where $cd \equiv a \pmod{p}$. Thus,

$$-1 \equiv (p-1)! \equiv a^{(p-1)/2} \pmod{p}$$

by Wilson's Theorem. Since a is a quadratic nonresidue modulo p , $\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$. ■

Remark 8. Some sources define $\left(\frac{a}{p}\right) = 0$ when $p \mid a$. In this case, Let p be an odd prime and $a \in \mathbb{Z}$. If $p \mid a$, then $a^{(p-1)/2} \equiv 0^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

When is -1 a quadratic residue?

Theorem (Theorem 4.6). *Let p be an odd prime number. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}.$$

Proof Let p be an odd prime number. Then from Euler's Criterion, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Since both values are ± 1 , we can say $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

If $p \equiv 1 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k + 1$. Thus, $\frac{p-1}{2} = 2k$ and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k} = 1.$$

If $p \equiv 3 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k + 3$. Thus, $\frac{p-1}{2} = 2k + 1$ and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k+1} = -1.$$

■

Wednesday, March 27: Introduction to quadratic reciprocity

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

- Use quadratic reciprocity to find the Legendre symbol of an integer modulo p .
- Characterize the primes where $3, -3, 5, -5, 7, -7$ are quadratic residues. .

Reading: Scanned notes, Pommersheim-Marks-Flapan Section 11.2 and part of 11.3.

Turn in: Use the results from the reading to find $\left(\frac{-3}{71}\right)$.

Solution: From Theorem 4.5(c), $\left(\frac{-3}{71}\right) = \left(\frac{-1}{71}\right) \left(\frac{3}{71}\right)$. Since $71 \equiv 3 \pmod{4}$, from ??, $\left(\frac{-1}{71}\right) = -1$, and from ?? $\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right)$. Putting this together, we get

$$\begin{aligned} \left(\frac{-3}{71}\right) &= \left(\frac{-1}{71}\right) \left(\frac{3}{71}\right) = (-1) \left(-\left(\frac{71}{3}\right)\right) \\ &= \left(\frac{71}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{aligned}$$

from Theorem 4.5(b) and the fact that 2 is a quadratic nonresidue modulo 3.

Quadratic reciprocity (20 minutes)

Theorem (Quadratic Reciprocity (first statement)). *Let p and q be distinct primes.*

- (a) *If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.*
- (b) *If $p \equiv q \equiv 3 \pmod{4}$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

It will take time to prove the lemmas for quadratic reciprocity, but we can immediately prove some results. The first is that this initial statement is equivalent to the more standard statement. This is our first example where one statement of a result (??) is more useful in calculations and proofs, but the proof involves proving an equivalent statement (??).

Theorem (Law of Quadratic Reciprocity). (*Theorem 4.9*) Let p and q be distinct primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Remark 9. We can quickly prove the second equality,

$$(-1)^{(p-1)/2 \cdot (q-1)/2} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then one of $\frac{p-1}{2}$ and $\frac{q-1}{2}$ is even. Thus $(-1)^{(p-1)/2 \cdot (q-1)/2} = 1$. If $p \equiv q \equiv 3 \pmod{4}$, then $\frac{p-1}{2}$ and $\frac{q-1}{2}$ are both odd. Thus $(-1)^{(p-1)/2 \cdot (q-1)/2} = -1$.

Proposition 5. ?? is equivalent to ??. That is, ?? implies ?? and ?? implies ?? .

Proof We will first show that ?? implies ??.

Let p and q be distinct primes. Then ?? says that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv q \equiv 3 \pmod{4}. \end{cases}$$

Since $\left(\frac{p}{q}\right) = \pm 1$ and $\left(\frac{q}{p}\right) = \pm 1$, we know that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ if and only if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Thus, when $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Similarly, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$ if and only if $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Thus, when $p \equiv q \equiv 3 \pmod{4}$, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

The other direction is on next homework assignment. ■

Notice that we also proved the converse of ??:

Corollary 3. Let p and q be distinct primes.

(a) If $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, then $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$.

(b) If $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, then $p \equiv q \equiv 3 \pmod{4}$.

Quadratic reciprocity practice (30 minutes)

In-class Problem 27 Let p be an odd prime number. Prove the following statements the following provided outlines, which will help solve the next problem, as well.

(b) $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(c) $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{6}$.

Proof (b) Since $3 \equiv \boxed{3} \pmod{4}$,⁴ we need two cases for ??.

(i) If $p \equiv 1 \pmod{4}$, then $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by ??, and $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv \boxed{1 \pmod{3}}$. Then $p \equiv \boxed{1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod{4}$, then $\left(\frac{3}{p}\right) = \left[-\left(\frac{p}{3}\right)\right]$ by ??, and $\left(\frac{p}{3}\right) = -1$ if and only if $p \equiv \boxed{2 \equiv -1 \pmod{3}}$. Then $p \equiv \boxed{-1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

(c) From Theorem 4.25(c), $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. Again, we have two cases.

(i) If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = \boxed{1}$ by ?? and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by ??. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv \boxed{1 \pmod{3}}$. Then $p \equiv \boxed{1} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = \boxed{-1}$ by ?? and $\left(\frac{3}{p}\right) = \left[-\left(\frac{p}{3}\right)\right]$ by ??. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv \boxed{1 \pmod{3}}$. Then $p \equiv \boxed{7} \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

Therefore, $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv \boxed{1, 7} \pmod{12}$, which is equivalent to $p \equiv 1 \pmod{6}$.

■

In-class Problem 28 Find congruences characterizing all prime numbers p for which the following integers are quadratic residues modulo p , as done in the previous exercise.

Outline is provided for the first part. Outline for second part added after class.

- (a) 5
- (b) -5
- (c) 7
- (d) -7

Solution: (a) Since $5 \equiv \boxed{1} \pmod{4}$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by ??. Then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \boxed{\pm 1 \pmod{5}}$.

(b) From Theorem 4.25(c), $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{5}\right)$ by ??. Again, we have two cases.

⁴In this problem, this step is repetitive, but it is needed when $p \neq 3$.

- (i) If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = \boxed{1}$ by ?? and $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)}$ by ?. Thus, $\left(\frac{-5}{p}\right) = \boxed{\left(\frac{p}{5}\right)} = 1$ if and only if $p \equiv \boxed{\pm 1 \pmod{5}}$. When $p \equiv \boxed{1 \pmod{5}}$, we have $p \equiv \boxed{1 \pmod{20}}$ and when $p \equiv \boxed{-1 \pmod{5}}$, we have $p \equiv \boxed{9 \pmod{20}}$. In each case, there is a unique equivalence class modulo $\boxed{20}$ by the Chinese Remainder Theorem.
- (ii) If $p \equiv 3 \pmod{4}$, then $\left(\frac{-1}{p}\right) = \boxed{-1}$ by ?? and $\left(\frac{5}{p}\right) = \boxed{\left(\frac{p}{5}\right)}$ by ?. Thus, $\left(\frac{-5}{p}\right) = \boxed{-\left(\frac{p}{5}\right)} = 1$ if and only if $p \equiv \boxed{\pm 2 \pmod{5}}$. When $p \equiv \boxed{2 \pmod{5}}$, we have $p \equiv \boxed{7 \pmod{20}}$ and when $p \equiv \boxed{3 \pmod{5}}$, we have $p \equiv \boxed{3 \pmod{20}}$. In each case, there is a unique equivalence class modulo $\boxed{20}$ by the Chinese Remainder Theorem.

Therefore, $\left(\frac{-5}{p}\right) = 1$ if and only if $p \equiv \boxed{1, 3, 7, 9 \pmod{20}}$.

Friday March 29: No class for Good Friday

Axiom 1 (Well Ordering Principle). *Every nonempty set of positive integers contains a least element.*

Divisibility facts

Lemma (Proposition 1.2). *Let $a, b, c, d \in \mathbb{Z}$. If $c \mid a$ and $c \mid d$, then $c \mid ma + nb$.*

Proposition (Proposition 1.10). *Let $a, b \in \mathbb{Z}$ with $(a, b) = d$. Then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Lemma (Lemma 1.12). *If $a, b \in \mathbb{Z}$, $a \geq b > 0$, and $a = bq + r$ with $q, r \in \mathbb{Z}$, then $(a, b) = (b, r)$.*

Prime facts

Lemma (Lemma 1.14). *Let $a, b, p \in \mathbb{Z}$ with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Corollary (Corollary 1.15). *Let $a_1, a_2, \dots, a_n, p \in \mathbb{Z}$ with p prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i .*

Proposition (Proposition 1.17). *Let $a, b \in \mathbb{Z}$ with $a, b > 1$. Write $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ where p_1, p_2, \dots, p_n are distinct primes and $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ are nonnegative integers (possibly zero). Then*

$$(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}$$

and

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Theorem (Theorem 1.19). *Let $a, b \in \mathbb{Z}$ with $a, b > 0$. Then $(a, b)[a, b] = ab$.*

Congruences

Proposition (Proposition 2.1). *Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, then:*

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

Proposition (Proposition 2.4). *Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, then:*

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

Proposition (Proposition 2.5). *Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$. Then $ca \equiv cb \pmod{m}$ if and only if $a \equiv b \pmod{\frac{m}{(a, m)}}$.*

Lemma (Chapter 2, Exercise 9). *Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$. If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$.*

Corollary (Corollary 2.15). *Let p be a prime number and let $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.*

The Euler Phi-Function

Theorem (Theorem 3.3). *Let p be prime and let $a \in \mathbb{Z}$ with $a > 0$. Then $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$.*

Diophantine equations

Theorem (Theorem 6.2). *Let $ax + by = c$ be a linear Diophantine equation in two variables x and y and let $d = (a, b)$. If $d \nmid c$, then the equation has no solutions. If $d \mid c$ then there are infinitely many solutions of the form*

$$x = x_0 + \frac{b}{d}n, y = y_0 - \frac{a}{d}n, \text{ for } n \in \mathbb{Z}.$$