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 $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$.
- 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, this definition is standard in an introduction to proofs course, but it is not the only definition of even/odd.

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.

In-class Problem 1

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

Prove this theorem.

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

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

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

Crowd Sourced Proof.

Theorem 2. *The sum of two consecutive integers in odd.*

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

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

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. 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 $a \in \mathbb{Z}$, $0 = a0$.

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) $\dfrac{m}{n}$

(c) ${}^{m}\!/_{n}$

- 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 $a \mid mn$

- 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)

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

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

Divisibility practice

Proposition (Strayer, Proposition 1.1)**.** *Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

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

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

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

so $a \mid c$. ■

This means that division is *transitive*.

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

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

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

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

Definition. The expression $ma + nb$ in Proposition 1.2 is called *an (integral) linear combination of a and b.*

Proposition 1.2 says that an integer dividing each of two integers also divides any integral linear combination of those integers. This fact will be extremely valuable in establishing theoretical results. But first, let's get some more practice with proof writing

Break into three groups. Using the proofs of Propositions 1.1 and 1.2 as examples, prove the following facts. Each group will prove one part.

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

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

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

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

Solution: Problem on Homework 1.

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 3 *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. 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 3 (Strayer, Lemma 1.3)**.** *Let* $x \in \mathbb{R}$. *Then* $x - 1 < [x] \leq x$.

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

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

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 $x \in \mathbb{R}$, $x^2 - 4 = 0$.
  (b) There exists $x \in \mathbb{R}$ such that $x^2 - 4 = 0$.
- 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 $F(x, y)$.
  (b) There exists y such that there exists x such that $F(x, y)$.
  (c) For all y, for all x, $F(x, y)$.

Go over reading assignment at the start of class.

Division Algorithm

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 4 (The 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*

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

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

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

Since $x - 1 < \lfloor x \rfloor \le x$ by Lemma 1.3, we have

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

Multiplying all terms by $-b$, we get

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

Adding a to every term gives

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

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

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

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

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

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

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

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

$$\begin{array}{c} 0 \le r_2 < b \\ -\underline{b < -r_1 \le 0} \\ -b < r_2 - r_1 < b. \end{array}$$

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 4 *Use the division algorithm 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 5. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that*

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

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

In-class Problem 5 *Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that*

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

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

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

  (ii) *There are two cases:*

    i. *When $\boxed{b > 0}$, the conditions are already met and $\boxed{r = s \text{ and } q = p}$.*

    ii. *Otherwise, $\boxed{b < 0}$, $r = \boxed{s}$ and $q = \boxed{-b}$.*

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

(b) *Use the* proof *of the Division Algorithm 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 Division Algorithm, we let* $q = \lfloor \frac{a}{b} \rfloor$. *Here we have two cases:*

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

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

(ii) *Follow the steps of the* proof *of the Division Algorithm 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

- Prove that 2 is the only even prime number.

Primes

Definition. 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 $p \mid n$, $p \mid n$. This contradicts our assumption, so no such integer exists. ■

Theorem 6 (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 $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1 p_2 \cdots p_n + 1$. Now N has a prime divisor, say, p, by Lemma 1.5. So $p = p_i$ for some i, $i = 1, 2, \ldots, n$. Then $p \mid N - p_1 p_2 \ldots p_n$, which implies that $p \mid 1$, a contradiction. Hence, there are infinitely many prime numbers. ■

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

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

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

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

by Proposition 1.2. So each of the n consecutive positive integers is composite. ■

In-class Problem 6 *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 7 *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

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

Quiz (10 minutes)

Greatest common divisor

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

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

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

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

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

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

Proposition 7 (Bézout's Identify, 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 (division algorithm, factors of linear combinationd), 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 division algorithm, 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

In-class Problem 8 *Theorems in Ernst Section 4.1*

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

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

In-class Problem 9 . *Use the first principle of mathematical induction to prove each statement.*

(b) *If n is a positive integer, then*

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

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

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

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

Remark 1. *This section was a response to a misconception on the homework. If keeping, it is best to come up with a better example and move to right after Lemma 3*

Let's explicitly think about the floor function as a function. That is, $f(x) : \mathbb{R} \to \mathbb{Z}$ (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 $g : \mathbb{R} \to \mathbb{R}$. 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

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

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

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

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)

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

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 $x = \dfrac{-5 \pm \sqrt{5}}{2}$.*

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

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

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

The Euclidean algorithm

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 8 (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

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

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

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

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

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

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

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

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

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

When using the Euclidean algorithm, 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) Euclidean algorithm 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.

Practice with the Euclidean algorithm

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

In-class Problem 10 *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) $(32, 56)$

54(b) $(78, 708)$

Fundamental Theorem of Arithmetic

Theorem 9 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than one can be written in the form $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the p_i are distinct prime numbers and the a_i are positive integers. This factorization into primes is unique up to the ordering of the terms.*

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

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

■

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

In-class Problem 11

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

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

In-class Problem 12 [1] *Let p be prime.*

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

Solution: *If $(a, b) = p$, then there exist $j, k \in \mathbb{Z}$ such that $a = pj, b = pk$, and $p \nmid j$ or $p \nmid k$ (otherwise $(a, b) = p^2$).*

$$a^2 = p^2 j^2, \quad a^3 = p^3 j^3, \quad b^3 = p^3 k^3$$

Then (a^2, b) is p if $p \nmid k$ or p^2 if $p \mid k$; and (a^3, b) is p if $p \nmid k$, p^2 if $p \mid k$ and $p^2 \nmid k$, or p^3 if $p^2 \mid k$.

If $p \mid j$, then $p \nmid k$ and $(a^2, b^3) = p^3$. If $p \nmid j$, then $(a^2, b^3) = p^2$.

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

Solution: *There exists $j, k \in \mathbb{Z}$ such that $a = pj, b = p^2 k$, and $p \nmid k, p \nmid k$. Then $ab = p^3 jk$ and $a + b = pj + p^2 k = p(j + pk)$. Thus, $(ab, p^4) = p^3$ and $(a + b, p^4) = p$.*

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 $a_1 x_1 + \cdots + a_k x_k = c$. .

Read Strayer, Section 6.1

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

[1] Not done 2024

Quiz (10 minutes)

More greatest common divisor

Lemma 10. *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 $d = e$.

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

Lemma 11. *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 12. *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. *Let $a_1, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Then*

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

Proof Let $k = 2$. The since $((a_1, a_2)) = (a_1, a_2)$ by the definition of greatest common divisor of one integer, $(a_1, a_2) = ((a_1, a_2))$. The $k = 3$ case is Lemma 10 in this section.

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

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

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

Note that $e \mid (a_1, a_2, a_3, \ldots, a_k)$ and $e \mid a_{k+1}$ by definition. Since $(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k)$ by the induction hypothesis, $e \mid (a_1, a_2, a_3, \ldots, a_{k-1})$ and $e \mid a_k$ by Lemma 12. Again, by the induction hypothesis, $(a_1, a_2, a_3, \ldots, a_{k-1}) = ((a_1, a_2, a_3, \ldots, a_{k-2}), a_{k-1})$, so $e \mid a_{k-1}$ and $e \mid (a_1, a_2, a_3, \ldots, a_{k-2})$ by Lemma 12. 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 12. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of Lemma 12. By the generalized version of the Lemma 11 on Homework 3, $e \mid f$.

To show that $f \mid e$, we note that $f \mid a_1, a_2, \ldots, a_k, a_{k+1}$ by definition. Then $f \mid d$ by the generalized version of the Lemma 11 on Homework 3. Since $e = (d, a_k)$, we have that $f \mid e$ by Lemma 11. ■

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 $\gcd(a, b)\,\mathrm{lcm}[a, b] = ab$. Since $\gcd(a, b), \mathrm{lcm}[a, b]$, and ab are all positive, $\mathrm{lcm}[a, b] = \dfrac{ab}{\gcd(a, b)}$ 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 13. *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 13 *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*

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

(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*

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

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

Proof (Proof of Proposition 13) Let $a, b, c, d \in \mathbb{Z}$ and let $ax + by + cz = d$ be a linear Diophantine equation. If $(a, b, c) \mid d$, let $e = (a, b)$. Then

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

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

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

has infinitely many solutions by Theorem 6.2, since $(e, c) = (a, b, c)$ by the Lemma 10 and $(a, b, c) \mid d$ by assumption. These solutions have the form

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

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

$$ax + by = ew_0.$$

Then the general solution is

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

To verify that these formulas for x, y, and z give solutions to $ax + by + cz = d$, we substitute into equation 2 then 1

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

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 14 *(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 $87 = \boxed{3(29)}$. To ensure that $(x, y) = 3$, not just $3 \mid x$ and $3 \mid y$, let $x = 3n$ where $\boxed{29} \nmid n$.

Proof *Let $x \in \mathbb{Z}$ with* $\boxed{\text{On Homework 3}}$. *Let $y = \square$. Then $3 \mid y$ by* $\boxed{\text{On Homework 3}}$. *Then $(x, y) = 3$ since* $\boxed{\text{On Homework 3}}$. *Thus, there are infinitely many $x, y \in \mathbb{Z}$* $\boxed{\text{On Homework 3}}$.

■

In-class Problem 15 *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* $\boxed{\text{linear combination}}$ $\boxed{\text{On Homework 3}}$ ■

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 14 (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 15 (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 16 (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 17 (Proposition 1.22)**.** *There are infinitely may prime numbers expressible in the form $4n + 3$ where n is a nonnegative integer.*

Proof (Similar to the proof that there are infinitely many prime numbers). Assume, by way of contradiction, that there are only finitely many prime numbers of the form $4n + 3$, say $p_0 = 3, p_1, p_2, \dots, p_r$, 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 Lemma 1.23. 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 16 *Prove that*

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

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

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

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

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

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 $\pmod m$ (20 minutes)

Definition. 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. 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 $-10 \equiv 4 \pmod 7$.

Think-Pair-Share 0.1. Prove that these two definitions are equivalent. That is, prove that 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.

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 $\pmod 2$**.** *Note that* $0^2 \equiv 0 \pmod 2$ *and* $1^2 \equiv 1 \pmod 2$.

> **Case 1:** $c^2 \equiv 0 \pmod 2$ *In this case,* $c \equiv 0 \pmod 2$ *and either* $1^2 + 1^2 \equiv 0 \pmod 2$ *or* $0^2 + 0^2 \equiv 0 \pmod 2$*. So, we know* $a \equiv b \pmod 2$. (Note: $\pmod 4$ will eliminate the $a \equiv b \equiv 1 \pmod 2$ case)
>
> **Case 2:** $c^2 \equiv 1 \pmod 2$ *In this case,* $c \equiv 1 \pmod 2$ *and either* $0^2 + 1^2 \equiv 1 \pmod 2$*. So, we know* $a \not\equiv b \pmod 2$.

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

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

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

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

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

We can use the idea of congruences to simplify divisibility arguments

In-class Problem 17 *Let a, b, c, d denote integers, 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* $c > 0$.

Let’s look at the various parts of this Lemma and see what they tell us about how congruences and moduli work.

The first two parts tell us that congruences behave a lot like equality.

The last two parts tell us how we can manipulate the modulus m. We can replace the modulus with a divisor of it at any time. We can replace the modulus with a multiple of it, provided we multiply a and b by the same multiple.

The remaining two parts are perhaps the most useful: they let us do arithmetic with congruences. In particular, they imply that whenever I’m adding or multiplying numbers, I can replace the numbers I have with any equivalent number that is more convenient to use. So for example, $37 * 210 \equiv 1 * 0 \pmod 2$ or $651262 * 697016 \equiv 2 * 6 \pmod{10}$.

Note that this doesn't work for powers. It is not the case that $2^{20} \equiv 2^0 \pmod{2}$. Also, unlike for regular equality, we cannot cancel a common factor of both sides unless it is relatively prime to m. That is to say $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{m}$ if $gcd(c, m) = 1$. (If $gcd(c, m) > 1$ we'll talk more on this later.)

Practice with Modular arithmetic (20 minutes)

In-class Problem 18 *List all integers in the range 1 to 100 that are congruent to 7 mod 17.*

Go over this as a class.