Number Theory

MAT-255 Davidson College

Claire Merriman

Spring 2024

Contents

Part I

Course Notes

These notes served as course notes for the Spring 2024 Number Theory course at Davidson College. This course can also serve as an introduction to proofs course. In addition to the course notes, worksheet versions of the in class assignments are provided in Appendix B and final project topics are provided in Appendix C

The official textbook for the course was *Elementary Number Theory* by James K. Strayer [Strayer, 2001]. Some topics that are not covered in these notes were assigned as reading before class. In order to reference these results in the notes, they are provided in Appendix A. The reading assignments are visible by using the `instructornote` option in the TEX file.

The introduction to proofs used An Introduction to Proof via Inquiry-Based Learning by Dana C. Ernst [Ernst, 2022], an open source textbook. My best effort has been made to link directly to this resource, although some standard staments and exercies are included in the notes.

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

These notes are also based on my notes teaching the Elementary Number Theory at The Ohio State University. Those courses use *An Introduction to the Theory of Numbers* by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery [Niven et al., 1991] and *Elementary Number Theory* by Gareth A. Jones and J. Mary Jones [Jones and Jones, 1998]. These notes were also influenced by *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by James Pommersheim, Tim Marks, Erica Flapan. I am thankful to Pommersheim and Marks' number theory course at the Johns Hopkins Center for Talented Youth for introducing me to proofs and number theory.

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

1 Introduction

What is number theory?

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

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

1.1 Mathematical definitions and notation

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

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

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

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

We will also use the following notation:

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

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

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

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

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

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

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

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

In-class Problem 1 Prove this theorem.

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

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

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

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

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

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

2 Divisibility, primes, and greatest common divisors

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

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

2.1 Divisibility

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

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

Reading assignment:

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

Turn in: From Ernst: Problem 2.6 and 2.8

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

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

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

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

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

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

so $a \mid c$. ■

This means that division is *transitive*.

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

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

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

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

Definition. The expression $ma + nb$ in Proposition 3 is called *an (integral) linear combination of* a *and* b.

Proposition 3 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 Proposition 2 and Proposition 3 as examples, prove the following facts. Each group will prove one part.

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

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

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

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

Solution: Problem on Homework.

2.2 Symbolic logic

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

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

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

Reading assignment:

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

Turn in: From Ernst: Problem 2.6 and 2.8

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

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

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

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

Solution:

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

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

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

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

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

2.3 The Division Algorithm

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

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

Reading assignment:

Read: Ernst Section 2.2 and Section 2.4

Turn in: Ernst, Problem 2.59 and 2.64

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

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

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

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

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

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

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

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

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

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

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

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

Multiplying all terms by $-b$, we get

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

Adding a to every term gives

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

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

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

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

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

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

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

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

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

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

In-class Problem 5 Use the 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 1. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exists a unique $q, r \in \mathbb{Z}$ such that

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

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

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

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

(a) Use the 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 $a = p|b| + s$ and $0 \leq s < |b|$.

(ii) There are two cases:

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

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

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

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

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

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

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

2.4 Greatest Common Divisors

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

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

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

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

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

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

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

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

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

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

This proof brings together definitions (of greatest common divisor), previous results (Division Algorithm, 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 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 $a \neq 0$.

2.5 Induction

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

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

- Construct a proof by induction .

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

In-class Problem 7 Theorems in Ernst Section 4.1

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

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

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

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

By the definition of *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.

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

(a) If n is a positive integer, then

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

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

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

2.6 The Euclidean Algorithm

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

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

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

Theorem 4 (Euclidean algorithm)**.** Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the 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 16 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 16, 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.

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

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

(a) $(21, 28)$

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

Using the Euclidean algorithm: $a = 28, b = 21$

$$\begin{array}{lll} 28 = 21(1) + 7 & q_1 = 1, r_1 = 7 & 7 = 21(1) + 28(-1) \\ 21 = 7(3) + 0 & q_2 = 3, r_2 = 0 & \end{array}$$

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

(b) $(32, 56)$

Solution: Using the Euclidean algorithm: $a = 56, b = 32$

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

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

(c) $(0, 113)$

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

(a) $(78, 708)$

Solution: Using the Euclidean algorithm: $a = 708, b = 78$

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

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

2.7 Primes

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

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

Reading assignment:

Read Strayer, Section 1.2

Turn in

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

  Solution: Summaries will vary

- Identify any other new proof methods in this section

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

  – Introducing a variable to aid in proof

  – Without loss of generality

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

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

Why is 1 not prime?

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

Proof Assume by contradiction that there exists $n \in \mathbb{Z}$ greater than 1 with no prime divisor. By the 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. ■

We will not go over this proof in class.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In-class Problem 11 Prove or disprove the following conjecture, which is similar to Twin Prime Conjecture:

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

2.8 The Fundamental Theorem of Arithmetic

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

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

Reading assignment:

Read Strayer, Section 1.5 through Proposition 1.17

Turn in

- Answer these questions about the proof of the Fundamental Theorem of Arithmetic (taken from Helping Undergraduates Learn to Read Mathematics):
  - Can you write a brief outline (maybe 1/10 as long as the theorem) giving the logic of the argument – proof by contradiction, induction on n, etc.? (This is KEY.)
  - What mathematical raw materials are used in the proof? (Do we need a lemma? Do we need a new definition? A powerful theorem? and do you recall how to prove it? Is the full generality of that theorem needed, or just a weak version?)
  - What does the proof tell you about why the theorem holds?
  - Where is each of the hypotheses used in the proof?
  - Can you think of other questions to ask yourself?
- Strayer states that the proof of Proposition 29 is "obvious from the Fundamental Theorem of Arithmetic and the definitions of (a, b) and $[a, b]$." Is this true? If so, why? If not, fill in the gaps.

Solution: Answers to both questions will vary between students.

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

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

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

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

■

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

In-class Problem 12

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

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

Put the following steps in order:

10 Therefore, $\sqrt{2}$ is not rational. 2 Assume that $\sqrt{2}$ is rational, ie, there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = \frac{p}{q}$.
6 Therefore there exists $k \in \mathbb{Z}$ such that $p = 2k$ by definition of $2 \mid p$
4 Then (include to remove fractions and the radical) $2q^2 = p^2$.
5 Then $2 \mid p^2$ by definition of divisibility and $2 \mid p$ by Lemma 1.14
9 This contradicts our assumption that $(p, q) = 1$ 7 Then (more algebraic manipulations) $2q^2 = 4k^2$ and $q^2 = 2k^2$.
1 We proceed by contradiction.
8 Then $2 \mid q^2$ and $2 \mid q$ by Lemma 1.14 and definition of $2 \mid q$
3 Without loss of generality, we may assume $(p, q) = 1$, since

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

In-class Problem 13 Let p be prime.

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

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

2.9 Arithmetic Progressions

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

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

Reading assignment:

Reading Strayer, Appendix B

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

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

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

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

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

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

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

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

Prime factorizations

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

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

A note on "if and only if" proofs:

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

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

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

contains infinitely many primes.

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

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

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

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

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

■

We will not go over the proof in class.

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

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

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

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

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

3 Linear Diophantine Equations

3.1 Linear Diophantine Equations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rearranging, we get

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

Dividing both sides by d gives

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

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

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

Multiple Choice:

(a) Yes

(b) No ✓

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

Using the Euclidean Algorithm, we find:

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

Thus

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

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

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

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

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

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

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

3.2 Greatest common divisors and Diophantine equations

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

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

Reading assignment:

Read: Strayer, Section 6.1

Turn in: Exercise 2a.

Greatest Common Divisors of three or more integers

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

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

Since $d = (a, b, c)$, we know $d \mid a, d \mid b$, and $d \mid c$. By Lemma 5, 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 5. Thus, e is a common divides of a, b and c ■

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

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

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

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

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

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

Proof Let $k = 2$. The since $((a_1, a_2)) = (a_1, a_2)$ by the definition of 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 (4).

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 1. 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 1. Repeat this

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

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 1. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of Lemma 1. By the generalized version of the Lemma 5 (Proposition 28), $e \mid f$.

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 Proposition 28. Since $e = (d, a_k)$, we have that $f \mid e$ by Lemma 5. ■

Linear Diophanitine equations in three variables

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

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

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

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

(b) The linear Diophantine equation $8x_1 - 4x_2 = 4y$ has infinitely many solutions for all $y \in \mathbb{Z}$ by Theorem 9. Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by Theorem 9, since $(4, 6) = 2 \mid 6$. Find them.

Solution: By inspection, $y = 0, x_3 = 1$ is a particular solution. Then by Theorem 9, the solutions have the form

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

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

Solution: By inspection, $x_1 = 1, x_2 = 2$ is a particular solution. Then by Theorem 9, the solutions have the form

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

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

Proof of Proposition 9 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 9. Similarly, the linear Diophantine equation

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

has infinitely many solutions by Theorem 9, since $(e, c) = (a, b, c)$ by the Lemma 4 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 4 then 3

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

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

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

■

§3.3 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. .

Proposition 9. 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 15 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 9. Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by Theorem 9, since $(4, 6) = 2 \mid 6$. Find them.

Solution: By inspection, $y = 0, x_3 = 1$ is a particular solution. Then by Theorem 9, the solutions have the form

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

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

Solution: By inspection, $x_1 = 1, x_2 = 2$ is a particular solution. Then by Theorem 9, the solutions have the form

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

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

Proof of Proposition 9 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

$$ax + by = ew \tag{3}$$

has a solution for all $w \in \mathbb{Z}$ by Theorem 9. Similarly, the linear Diophantine equation

$$ew + cz = d \tag{4}$$

has infinitely many solutions by Theorem 9, since $(e, c) = (a, b, c)$ by the Lemma 4 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 4 then 3

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

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

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

■

4 Modular arithmetic

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

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

4.1 Introduction to modular arithmetic

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

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

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

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

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

Proposition 10 (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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2 Practice with modular arithmetic

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

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

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

Proposition 11. Let m be a positive integer. Then equivalence modulo m partition the integers. That is, every integer is in exactly one equivalence class modulo m.

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

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

Proposition 12. The set $\{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proof Let $a, m \in \mathbb{Z}$ with $m > 0$. By the 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 $r = 0, 1, \ldots, m-2$, or $m-1$. Therefore, every integer is in the equivalence class of $0, 1, \ldots, m-2$ or $m-1$ modulo m. Since every integer is in exactly one equivalence class modulo m, and the remainder from the division algorithm is unique, it is not possible for a to be equivalent to any other element of $\{0, 1, \ldots, m-1\}$. ■

In-class Problem 16 Practice: addition and multiplication tables modulo $3, 4, 5, 6, 7$. I am adding 9 to include an odd composite.

Solution: **Modulo** 3

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

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

Modulo 4

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

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

Modulo 5

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

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

Modulo 6

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

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

Modulo 7

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

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

Modulo 8

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

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

Modulo 9

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

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

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

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

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

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

Different statements of the definition will be useful in different situations

Proposition 13. Let $a, b, c, d, m \in \mathbb{Z}$ with $m > 0$, then:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■

Example 5. Note that $2 \equiv 5 \pmod{3}$. Then $4 \equiv 10 \pmod{3}$ by Proposition 13(c), since $2 \equiv 2 \pmod{3}$. From part (e), $4 \equiv 10 \pmod{6}$, but $2 \not\equiv 5 \pmod{6}$.

[2] all definitions are if and only if

4.3 Equivalence Relations

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

- Prove a given set is an equivalence relation .

Reading assignment:

Read: Strayer, Appendix B

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

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

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

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

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

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

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

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

In-class Problem 17 Prove that

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

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

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

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

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

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

4.4 Linear congruences in one variable

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

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

Reading assignment:

Paper 1 due

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

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

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

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

Proof Let $a, b, m \in \mathbb{Z}$ with $m > 0$, and $d = (a, m)$. From the definition of congruence modulo m, $ax \equiv b \pmod{m}$ if and only if $m \mid (ax - b)$. That is, $ax \equiv b \pmod{m}$ if and only if $my = ax - b$ for some $y \in \mathbb{Z}$ from the definition of divisibility. Sine $ax - my = b$ is a linear Diophantine equation, Theorem 9 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 9, all solutions have the from $x = x_0 + \frac{mn}{d}$ for all $n \in \mathbb{Z}$. We need to show that these solutions are in exactly d distinct congruence classes modulo m.

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

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

■

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

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

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

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

Corollary 3. [Corollary of Theorem 10] Let $a, m \in \mathbb{Z}$ with $m > 0$. The linear congruence in one variable $ax \equiv 1 \pmod{m}$ has a solution if and only if $(a, m) = 1$. If $(a, m) = 1$, then the solution is unique modulo m.

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

Example 7. Examples of multiplicative inverses:

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

Example using multiplicative inverses:

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

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

Solution:

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

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

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

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

4.5 Chinese Remainder Theorem

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

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

Example 8. Consider the system of linear equations

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

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

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

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

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

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

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

Note that

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

Thus,

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

is a solution to all three congruences.

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

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

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

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

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

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

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

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

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

4.6 Wilson's Theorem

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

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

Reading assignment:

Read: Strayer, Section 2.4

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

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

Proof Let p be a prime number and $a \in \mathbb{Z}$. Then a is its own inverse modulo m if and only if $a^2 \equiv 1 \pmod{p}$ if and only if $p \mid a^2 - 1 = (a-1)(a+1)$. Since p is prime, $p \mid a-1$ or $a+1$ by Lemma 1.14. Thus, $a \equiv \pm 1 \pmod{p}$. ■

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

Remark 3. It is important to note why we require p is prime. 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 12 (Wilson's Theorem)**.** Let p be a prime number. Then

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

Proof When $p = 2$, $(2-1)! = 1 \equiv -1 \pmod{2}$. Now consider p an odd prime. By Corollary 3, each $a = 1, 2, \ldots, p-1$ has a unique multiplicative inverse modulo p. Lemma 7 says the only elements that are their own multiplicative inverse are 1 and $p-1$. Thus $(p-2)!$ is the product of 1 and $\dfrac{p-3}{2}$ pairs of a, a' where $aa' \equiv 1 \pmod{p}$. Therefore,

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

■

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

Proposition 14 (Converse of Wilson's Theorem)**.** Let n be a positive integer. If $(n-1)! \equiv 1 \pmod{n}$, then n is prime.

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

In-class Problem 18 (Part of Strayer, Chapter 2 Exercise 47) Let p be an odd prime. Use (a) $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ to show

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

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

4.7 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 .

Reading assignment:

Read Strayer, Section 2.5

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

> **Solution:** Consider the 10 integers given by $9, 2(9), 3(9), \ldots, 9(10)$. Note that $11 \mid 9i$ for $i = 1, 2, \ldots, 10$ since 11 is prime and $11 \nmid 10$ and $11 \nmid i$. By Corollary 3, since $(9, 11) = 1$ if $9i \equiv 9j \pmod{11}$ implies $i \equiv j \pmod{11}$. Therefore, no two of $9, 2(9), 3(9), \ldots, 9(10)$ are congruent modulo 11. So the least nonnegative residues modulo 11 of the integers $9, 2(9), 3(9), \ldots, 9(10)$, taken in some order, must be $1, 2, \ldots, p-1$. 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 Wilson's Theorem, the congruence above becomes $-9^{10} \equiv -1 \pmod{11}$, which is equivalent to $9^{10} \equiv 1 \pmod{11}$.

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

- $(r_i, m) = 1$ for all $i = 1, 2, \ldots, k$,
- $r_i \not\equiv r_j \pmod{m}$ when $i \neq j$,
- for all $a \in \mathbb{Z}$ with $(a, m) = 1$, $a \equiv r_1 \pmod{p}$ for some $i = 1, 2, \ldots, k$.

Example 9.

- 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 $\{1, 2, \ldots, p-1\}$ is a complete residue system modulo p. If $p \neq 5$, $\{5, 10, \ldots, 5(p-1)\}$ 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 8. Let m be a positive integer and let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system modulo m. If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \ldots, ar_k\}$ is a reduced residue system modulo m.

This result is also implicitly used in the proof of Fermat's Little Theorem since $\{1, 2, \ldots, p-1\}$ is a reduced residue system.

Proof Let $\{r_1, r_2, \ldots, r_k\}$ be a reduced residue system modulo m and $a \in \mathbb{Z}$ with $(a, m) = 1$. Since $\{r_1, r_2, \ldots, r_k\}$ and $\{ar_1, ar_2, \ldots, ar_k\}$ 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 of 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 Proposition 2.5, $ar_i \equiv ar_j \pmod{m}$ if and only $r_i \equiv r_j \pmod{\frac{m}{(a,m)}}$. 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

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

Remark 4. For a positive integer m, $\phi(m)$ is the number of reduced residues modulo m

Example 10.
- $\phi(7) = 6$
- If p is prime, $\phi(p) = p - 1$
- $\phi(12) = 4$

Theorem 13 (Euler's Generalization of Fermat's Little Theorem)**.** Let $a, m \in \mathbb{Z}$ with $m > 0$. If $(a, m) = 1$, then

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

Corollary 5 (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 Euler's Generalization of Fermat's Little Theorem Let m be a positive integer and let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced residue system modulo m. If $a \in \mathbb{Z}$ with $(a, m) = 1$, then $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ is a reduced residue system modulo m by Lemma 8. Thus, for all $i = 1, 2, \ldots, \phi(m)$, then $r_i \equiv ar_j \pmod{m}$ for some $j = 1, 2, \ldots, \phi(m)$. Thus

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

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

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

■

4.8 Calculations with Fermat's Little Theorem and Euler's Theorem

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

- Use Fermat's Little Theorem to find the least nonnegative residue modulo a prime
- Use Euler's Theorem to find the least nonnegative residue modulo a composite .

Finding least nonnegative residue Fermat's Little Theorem

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 6. 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 0.2. 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

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

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

Multiplicative inverses using Euler's Extension of Fermat's Little Theorem

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 mulod 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 7. 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 $(9^{19})21 = (3^2)^1 9(21)$. From here there are two options:

Factor 21**:**

$$(9^{19})21 \equiv (3^2)^1 9(3)(7) \equiv (3^{39})(7) \equiv (3^{20})(3^{19})(7) \pmod{25}$$

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 moddulo 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 $21 \equiv -4 \pmod{25}$**:**

$$(9^{19})21 \equiv (3^2)^1 9(-4) \equiv (3^{38})(-4) \equiv (3^{20})(3^{18})(-4) \pmod{25}$$

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 19 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 $q^{p-1} \equiv 1 \pmod{p}$ and $p^{q-1} \equiv 1 \pmod{q}$ by Fermat's Little Theorem, and $p^{q-1} \equiv 1 \equiv 0 \pmod{p}$ and $q^{p-1} \equiv 1 \equiv 0 \pmod{q}$ by *definition.*

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

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

5 The Euler ϕ-function

Recall from Section Part I, Euler ϕ-function

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

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

This section will explore the $\phi-$function in more depth.

5.1 The Euler ϕ-function

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

- Prove $\phi(4)\phi(5) = \phi(20)$ using an outline that mirrors the proof that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

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

Theorem 14. Let m and n be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

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

(a) A number a is relatively prime to 20 if and only if a is relatively prime to 4 and 5. The first blank should be smaller than second blank for the automatic grading to work.

Hint: *The number in each blank should be relevant to what we are trying to show.*

(b) We can partition the positive integers less that or equal to 20 into

$$\begin{aligned} 1 &\equiv 5 \equiv 9 \equiv 13 \equiv 17 \pmod 4 \\ 2 &\equiv 6 \equiv 10 \equiv 14 \equiv 18 \pmod 4 \\ 3 &\equiv 7 \equiv 11 \equiv 15 \equiv 19 \pmod 4 \\ 4 &\equiv 8 \equiv 12 \equiv 16 \equiv 20 \pmod 4 \end{aligned}$$

For any b in the range $1, 2, 3, 4$, define s_b to be the number of integers a in the range $1, 2, \ldots, 20$ such that $a \equiv b \pmod 4$ and $\gcd(a, 20) = 1$. Thus, $s_1 = 4, s_2 = 0, s_3 = 4$, and $s_4 = 0$.

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

(c) $\phi(20) = s_1 + s_2 + s_3 + s_4$. Why?

Free Response: Every positive integers less that or equal to 20 is counted by exactly one s_b.

(d) We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b = \phi(5)$, This blank is asking for a function, not a number. and that when $(b, 4) > 1$, $s_b = 0$. To finish the "proof" we show that there are $\phi(4)$ integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) = \phi(4)\phi(5)$.

In-class Problem 21 Repeat the same proof for m and n where $(m, n) = 1$.

Proof Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to m and n.

We can partition the positive integers less that or equal to mn into

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

For any b in the range $1, 2, 3, \ldots, m$, define s_b to be the number of integers a in the range $1, 2, \ldots, mn$ such that $a \equiv b \pmod m$ and $\gcd(a, mn) = 1$. Thus, when $(b, m) = 1$, $s_b = \phi(m)$ and when $(b, m) > 1$, $s_b = 0$.

Free Response: Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn) = s_1 + s_2 + \cdots + s_m$.

We have seen that $\phi(mn) = s_1 + s_2 + \cdots + s_m$, that when $(b, m) = 1$, $s_b = \phi(n)$, This blank is asking for a function, not a value. and that when $(b, m) > 1$, $s_b = 0$. Since there are $\phi(m)$ integers b where $(b, m) = 1$. Thus, we can say that $\phi(mn) = \phi(m)\phi(n)$. ■

In-class Problem 22 Complete the proof of Theorem 1 by proving that, if m, n, and i are positive integers with $(m, n) = (m, i) = 1$, then the integers $i, m + i, 2m + i, ..., (n - 1)m + i$ form a complete system of residues modulo n.

5.2 The Euler $\phi-$ function

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 assignment:

Reading None

Turn In Paper 2

6 Primitive Roots

6.1 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.

Review of ϕ-function

Remark 5. From before break, Theorem 1 states if $(m, n) = 1$ for positive integers m and n, then $\phi(mn) = \phi(m)\phi(n)$.

Thus, $\phi(63) = \phi(9(7)) = \phi(9)\phi(7) = 6(6)$.

In-class Problem 23 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,

$$\begin{aligned} x &\equiv n^7 \pmod 7 \\ x &\equiv n^7 \pmod 9 \end{aligned}$$

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 6. Reviewing the proof of part (a): 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

Definition 3 (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 $\operatorname{ord}_m a$, 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	$\operatorname{ord}_7 a$
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 $\operatorname{ord}_m a \mid \phi(m)$.

Proposition 15. 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 $\operatorname{ord}_m a \mid n$. In particular, $\operatorname{ord}_m a \mid \phi(m)$.

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

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

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

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

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

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

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

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

by definition of order of a modulo m.

■

Proposition 16. 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 and only if $i \equiv j \pmod{\operatorname{ord}_m a}$.

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

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

(⇒) Assume that $2^i \equiv 2^j \pmod{7}$. Then by exponent rules, $2^j 2^{i-j} \equiv 2^j \pmod{7}$. Since $(2^i, 7) = 1$, there exists a multiplicative inverse of 2^i modulo 7 by Corollary 3, 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 Proposition 1, $\operatorname{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\operatorname{ord}_m a}$ by definition.

(⇐) Assume that $i \equiv j \pmod{3}$. Then $3 \mid i - j$ by definition. Since $\operatorname{ord}_7 2 = 3$, Proposition 1 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 Proposition 16 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.

(⇒) Assume that $a^i \equiv a^j \pmod{m}$. Then by exponent rules, $a^j a^{i-j} \equiv a^j \pmod{m}$. Since $(a^i, m) = 1$ by assumption, there exists a multiplicative inverse of a^i modulo m by Corollary 3, 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 Proposition 1, $\operatorname{ord}_m a \mid i - j$. Thus, $i \equiv j \pmod{\operatorname{ord}_m a}$ by definition.

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

■

6.2 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 assignment:

Read: Uploaded notes, [Flapan et al., 2010, Pommersheim-Marks-Flapan, Chapter 10: Primitive Roots, Section 10.3: Primitive Roots]

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.

Definition 4 (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 $\operatorname{ord}_m r = \phi(r)$.

We saw in the reading that primitive roots always exist modulo a prime.

Theorem 15 (Primitive Root Theorem)**.** Let p be prime. Then there exists a primitive root modulo p.

What about composites?

Example 18.

- Since $\phi(6) = \phi(3)\phi(2) = 2$ and $\operatorname{ord}_6 5 = 2$, 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, $\operatorname{ord}_8 1 = 1$ and $\operatorname{ord}_8 3 = \operatorname{ord}_8 5 = \operatorname{ord}_8 7 = 2$.
- Since $\phi(9) = 3^1(3-1) = 6$ by Theorem 3.3, we check:

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

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

$$4^1 = 4, \qquad 4^2 = 2^4 \equiv 7 \pmod 9, \qquad 4^3 = 2^6 \equiv 1 \pmod 9$$

We can also use exponent rules and Proposition 16 to simplify some calculuations. For example, $5 \equiv 2^5 \pmod 9$, so $5^i \equiv 2^{5i} \equiv 2^j \pmod 9$ if and only if $5i \equiv j \pmod 6$.

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

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

$$\operatorname{ord}_9(1) = 1$$
$$\operatorname{ord}_9(2) = \operatorname{ord}_9(5) = 6$$
$$\operatorname{ord}_9(4) = \operatorname{ord}_9(7) = 3$$
$$\operatorname{ord}_9(8) = 2$$

Proposition 17. Let r be a primitive root modulo m. Then

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

is a set of reduced residues modulo m.

This is the general version of Reading Proposition 10.3.2, using exponents $1, 2, \ldots, \phi(m)$ instead of $0, 1, \ldots, \phi(m) - 1$. 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 18. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If i is a positive integer, then

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

In-class Problem 24 Use only the results through Proposition 17/Reading Lemma 10.3.5 to prove the primitive root version:

Proposition 19. Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m. If i is a positive integer, then

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

Proof Let $i, r, m \in \mathbb{Z}$ with $i, m > 0$ and r a primitive root modulo m. Then $\operatorname{ord}_m r = \phi(m)$ 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 proceding 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. Proposition 5.1 says that $\operatorname{ord}_p(a^i) \mid j$.

Since $a^{i \operatorname{ord}_p(a^i)} \equiv (a^i)^{\operatorname{ord}_p(a^i)} \equiv 1 \pmod{p}$ by definition of order, Proposition 5.1 says that $\operatorname{ord}_p a \mid i \operatorname{ord}_p(a^i)$. Since $\operatorname{ord}_p a = \phi(m) = dj$ and $i = dk$, we have $dj \mid dk \operatorname{ord}_p(a^i)$ which simplifies to $j \mid k \operatorname{ord}_p(a^i)$. Since $(j, k) = 1$, we can conclude $j \mid \operatorname{ord}_p(a^i)$.

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

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

■

Exercises cited in the reading, also on Homework 6:

In-class Problem 25 Prove the following statement, which is the converse of Reading 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 26 Prove the following generalization of Reading Lemma 10.3.5

Lemma 9. Let $n \in \mathbb{Z}$ and let $x_1, x_2, \ldots, x_m$ be reduced residues modulo n. Suppose that for all $i \neq j$, $\operatorname{ord}_n(x_i)$ and $\operatorname{ord}_n(x_j)$ are relatively prime. Then

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

6.3 Lagrange's Theorem

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

- Prove Lagrange's Theorem .

Reading assignment:

Read: Strayer Section 5.2

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

Solution: Since 41 is prime, **??** 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 Proposition 5.4, 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:

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

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

The goal is to finish proving the Primitive Root Theorem with a look at polynomials.

Theorem 16 (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 $a_0, a_1, \ldots, a_n$. Let d be the greatest integer such that $a_d \not\equiv 0 \pmod{p} t$ 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 3, there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.

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 $r_1, r_2, \ldots, r_d, r_{d+1}$. 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 Proposition 31 gives that one of $a_d, r_{d+1} - r_1, r_{d+1} - r_2, \ldots, r_{d+1} - r_d$ 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 $r_1, r_2, \ldots, r_d$ 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 $f(x) \equiv a_1 x + a_0 \pmod{p}$. Since $a_1 \not\equiv 0 \pmod{p}$ by assumption, $p \nmid a_1$. Since p is prime, $(a_1, p) = 1$. Thus, by , there is a unique solution modulo p to $a_1 \not\equiv 0 \pmod{p}$.

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.

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 20. 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 $1, 2, \ldots, p-1$. 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 Lagrange, 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 Lagrange, there are exactly m incongruent solutions to $x^m - 1 \equiv 0 \pmod{p}$ and thus $x^m \equiv 1 \pmod{p}$. ■

Definition 5 (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.

In-class Problem 27 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 1, $a^m \equiv 1 \pmod{p}$ if and only if $\operatorname{ord}_p a \mid m$. Similarly, $a^{p-1} \equiv 1 \pmod{p}$ if and only if $\operatorname{ord}_p a \mid p-1$. Thus, $\operatorname{ord}_p a$ is a common divisor of m and $p-1$. Combining Lemma 5 and Lemma 1 gives $\operatorname{ord}_p a$ is a common divisor of m and $p-1$ if and only if $\operatorname{ord}_p a \mid d$. One final application of Proposition 1 gives $\operatorname{ord}_p a \mid d$ if and only if $a^d \equiv 1 \pmod{p}$.

In-class Problem 28 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 27, $x^m \equiv 1 \pmod{p}$ if and only if $x^d \equiv 1 \pmod{p}$. By Proposition 20 there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, there are exactly d solutions to $x^m \equiv 1 \pmod{p}$. ■

6.4 Existence of primitive roots modulo a prime

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 .

We will now prove the existence of primivitive 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 Reading Lemma 10.3.4 instead of results from Chapter 3.

Theorem 17. 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 20, there are exactly q^s incongruent solutions to

$$x^{q^s} \equiv 1 \pmod{p} \tag{5}$$

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

$$x^{q^{s-1}} \equiv 1 \pmod{p}. \tag{6}$$

Since $(x^{q^{s-1}})^q = x^{q^s}$, all solutions to (6) are solutions to (5). 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 1, $\operatorname{ord}_p a \mid q^s$ and $\operatorname{ord}_p a \nmid q^{s-1}$. Since q is prime, $\operatorname{ord}_p a = q^s$. 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 $q_1, q_2, \ldots, q_k$ and positive integers $s_1, s_2, \ldots, s_k$. Let $a_1, a_2, \ldots, a_k$ be elements of order $q_1^{s_1}, q_2^{s_2}, \ldots, q_k^{s_k}$ respectively. Consider $a = a_1 a_2 \cdots a_k$ and $a^2, a^3, \ldots, a^d$. By Homework 6, Problem 6, a has order $q_1^{s_1} q_2^{s_2} \cdots q_k^{s_k} = d$. By Proposition 20, there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, $a, a^2, \ldots, a^d$ are all incongruent solutions to $x^d \equiv 1 \pmod{p}$ by Proposition 1. By Proposition 1, $\operatorname{ord}_p a^i = \dfrac{d}{(d,i)} = d$ 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 8. Let p be prime. There are exactly $\phi(p-1)$ primitive roots modulo p.

7 Introduction to quadratic residues

Definition 6 (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 7. When finding squares modulo m, we only need to check up to $\frac{m}{2}$, since $(-a)^2 = a^2$ and $m - a \equiv -a \pmod{m}$

7.1 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 .

Definition (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 8. 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 29 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 nonresidues
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 10. 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 9. 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 21. Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \mid a$. 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 $p \mid a$. 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 Lemma 10 says that there are at least two solutions, since $p > 2$. 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 22. Let p be an odd prime number. Then there are exactly $\dfrac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\dfrac{p-1}{2}$ 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 Proposition 21, and no integer is a solution to more than one of the congruences, exactly half are solvable. Therefore, there are exactly $\dfrac{p-1}{2}$ incongruent quadratic residues modulo p and exactly $\dfrac{p-1}{2}$ incongruent quadratic nonresidues modulo p. ■

7.2 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 assignment:

Read: 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

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

Definition 7 (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 18 (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 23. Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then

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

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

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

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, Euler's Criterion gives

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

■

Remark 10. 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 $a^{(p-1)/2} \equiv 0^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Theorem 19. 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

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

■

7.3 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 assignment:

Reading None

Proof of Euler's Criterion

We will prove Euler's Criterion.

Theorem 20 (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 $\{1, 2, \ldots, p-1\}$. 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 $\dfrac{p-1}{2}$ 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, $\left(\frac{a}{p}\right) = -1 \equiv a^{(p-1)/2} \pmod{p}$. ■

7.4 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 assignment:

Reading: Scanned notes, [Flapan et al., 2010, 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 Theorem 4.6, $\left(\frac{-1}{71}\right) = -1$, and from quadratic reciprocity $\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right)$. 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

Theorem 21 (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 (Quadratic Reciprocity (first statement)) is more useful in calculations and proofs, but the proof involves proving an equivalent statement (Law of Quadratic Reciprocity).

Theorem 22 (Law of Quadratic Reciprocity)**.** (Theorem 4.9) Let p and q be distinct primes. Then

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

Remark 11. We can quickly prove the second equality,

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

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

Proposition 24. Quadratic Reciprocity (first statement) is equivalent to Law of Quadratic Reciprocity. That is, Quadratic Reciprocity (first statement) implies Law of Quadratic Reciprocity and Law of Quadratic Reciprocity implies Quadratic Reciprocity (first statement) .

Proof We will first show that Law of Quadratic Reciprocity implies Quadratic Reciprocity (first statement).

Let p and q be distinct primes. Then Law of Quadratic Reciprocity 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 Quadratic Reciprocity (first statement):

Corollary 9. 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

In-class Problem 30 (Strayer Chapter 4, Exercise 35) 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 $3 \equiv 3 \pmod 4$,[3] we need two cases for Quadratic Reciprocity (first statement).

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

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

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

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 $\left(\frac{-1}{p}\right) = 1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. Then $p \equiv 1 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. Then $p \equiv 7 \pmod{12}$, 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 $p \equiv 1, 7 \pmod{12}$, which is equivalent to $p \equiv 1 \pmod 6$.

■

In-class Problem 31 (Strayer Chapter 4, Exercise 36) 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 $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by Quadratic Reciprocity (first statement). Then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 5$.

(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 Quadratic Reciprocity (first statement). Again, we have two cases.

(i) If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ by Theorem 4.6 and $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 5$. When $p \equiv 1 \pmod 5$, we have $p \equiv 1 \pmod{20}$ and when $p \equiv -1 \pmod 5$, we have $p \equiv 9 \pmod{20}$. In each case, there is a unique equivalence class modulo 20 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ by Theorem 4.6 and $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by Quadratic Reciprocity (first statement). Thus, $\left(\frac{-5}{p}\right) = -\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \pm 2 \pmod 5$. When $p \equiv 2 \pmod 5$, we have $p \equiv 7 \pmod{20}$ and when $p \equiv 3 \pmod 5$, we have $p \equiv 3 \pmod{20}$. In each case, there is a unique equivalence class modulo 20 by the Chinese Remainder Theorem.

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

7.5 Gauss's Lemma

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

- Find the Legendre symbol using Gauss's Lemma
- Find the Legendre symbol using several different methods .

Reading assignment:

Reading None

Statement of Guass's Lemma

Lemma 11 (Gauss's Lemma)**.** Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, 3a, \ldots, \dfrac{p-1}{a}$ modulo p that are greater than $\dfrac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Example 19. Find $\left(\dfrac{6}{11}\right)$

(a) Using Gauss's Lemma

Solution: Note that $\dfrac{11-1}{2} = 5$.

First, we list $6, 2(6), 3(6), 4(6), 5(6)$ and find the least nonnegative residues modulo 11 :

$$6,\ 2(6) \equiv 1 \pmod{11},\ 3(6) \equiv 7 \pmod{11},\ 4(6) \equiv 2 \pmod{11},\ 5(6) \equiv 8 \pmod{11}.$$

Now we count $n = 3$ of the least nonnegative residues modulo 11 are greater than $\dfrac{11}{2} = 5.5$

Thus, $\left(\dfrac{6}{11}\right) = (-1)^3 = -1$.

(b) Factoring and using quadratic reciprocity

Solution: Using Theorem 2 and the fact that $2 \equiv -9 \pmod{11}$,

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-9}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{9}{11}\right)\left(\frac{3}{11}\right) = \left(\frac{-1}{11}\right)(1)\left(\frac{3}{11}\right)$$

Since $11 \equiv 3 \pmod 4$, $\left(\dfrac{-1}{11}\right) = -1$ by Theorem 4.6 and $\left(\dfrac{3}{11}\right) = -\left(\dfrac{11}{3}\right)$. Thus,

$$\left(\frac{6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right) = (-1)(-1)\left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Example 20. Find $\left(\dfrac{-11}{7}\right)$

(a) Using Gauss's Lemma

Solution: Since $\frac{7-1}{2} = 3$, we need to find the least nonnegative residues of $-11, 2(-11), 3(-11)$ modulo 7. These are

$$-11 \equiv 3 \pmod 7,\ 2(-11) \equiv 6 \pmod 7,\ 3(-11) \equiv 2 \pmod 7.$$

Then $n = 1$ is greater than $\frac{7}{2} = 3.5$ and $\left(\frac{-11}{7}\right) = (-1)^1 = -1$.

(b) By reducing modulo 7 then using Gauss's Lemma

Solution: By Theorem 4.5(b) $\left(\frac{-11}{7}\right) = \left(\frac{3}{11}\right)$. Since $\frac{7-1}{2} = 3$, we need to find the least nonnegative residues of $3, 2(3), 3(3)$ modulo 7. These are

$$3 \pmod 7,\ 6 \pmod 7,\ 3(3) \equiv 2 \pmod 7.$$

Then $n = 1$ is greater than $\frac{7}{2} = 3.5$ and $\left(\frac{-11}{7}\right) = (-1)^1 = -1$.

(c) By reducing modulo 7 and using quadratic reciprocity

Solution: By Theorem 4.5(b) $\left(\frac{-11}{7}\right) = \left(\frac{3}{11}\right)$. Since $11 \equiv 3 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right)$ By Theorem 4.5(b) $-\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1$ using Theorem 4.6.

Practice Problems

We can combine these results to find the Legendre symbol many different ways.

In-class Problem 32 Use the following methods to find $\left(\frac{-6}{11}\right)$:

(a) Euler's Criterion, from March 22:

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

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

(b) Factor into $\left(\frac{-6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. From here, we will explore the various was to find $\left(\frac{2}{11}\right)$ and $\left(\frac{3}{11}\right)$.

(i) Find $\left(\frac{2}{11}\right)$ using the specified method:

- Using Euler's Criterion.

  Solution: From Euler's Criterion,

$$\left(\frac{2}{11}\right) \equiv 2^{(11-1)/2} \equiv 32 \equiv -1 \pmod{11}.$$

- Using Gauss's Lemma.

  Solution: First, find the least nonnegative residues of $2, 2(2), 3(2), 4(2), 5(2)$ modulo 11. These are

  $$2, 4, 6, 8, 10,$$

  and $n = 3$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

  $$\left(\frac{2}{11}\right) = (-1)^3 = 3.$$

(ii) Find $\left(\frac{3}{11}\right)$ using the specified method:

- Using Euler's Criterion.

  Solution: From Euler's Criterion,

  $$\left(\frac{3}{11}\right) \equiv 3^{(11-1)/2} \equiv (-2)^2(3) \equiv 1 \pmod{11}.$$

- Using Quadratic reciprocity

  Solution: Since $11 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$.

- Using Gauss's Lemma.

  Solution: First, find the least nonnegative residues of $3, 2(3), 3(3), 4(3), 5(3)$ modulo 11. These are

  $$3, 6, 9, 1, 4$$

  and $n = 2$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

  $$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

Thus, $\left(\frac{-6}{11}\right) = 1$

(c) Use that $-6 \equiv 5 \pmod{11}$, so $\left(\frac{-6}{11}\right) = \left(\frac{5}{11}\right)$. Then find $\left(\frac{5}{11}\right)$ the specified method:

(i) Using Euler's Criterion.

Solution: From Euler's Criterion,

$$\left(\frac{5}{11}\right) \equiv 5^{(11-1)/2} \equiv (3)^2(5) \equiv 1 \pmod{11}.$$

(ii) Using Quadratic reciprocity

Solution: Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$.

(iii) Using Gauss's Lemma.

Solution: First, find the least nonnegative residues of $5, 2(5), 3(5), 4(5), 5(5)$ modulo 11. These are

$$5, 10, 4, 9, 2,$$

and $n = 2$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

$$\left(\frac{5}{11}\right) = (-1)^2 = 1.$$

In-class Problem 33 Now we will examine the Legendre symbol of 2 using Gauss's Lemma. First, note that $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are already least nonnegative residues modulo p. It will be slightly easier to count how many are *less than* $\frac{p}{2}$, then subtract from the total number, $\frac{p-1}{2}$.

Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \left\lfloor \frac{p}{4} \right\rfloor$. Thus, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are greater than $\frac{p}{2}$.

Hint: *The two blanks should be the same, and also go in the blanks below*

Now complete this table

p	$\left\lfloor \frac{p}{4} \right\rfloor$	$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3	0	1	Less than $\frac{3}{2}$: N/A Greater than $\frac{3}{2}$: 2	$(-1)^1 = -1$
5	1	1	Less than $\frac{5}{2}$: 2 Greater than $\frac{5}{2}$: 4	$(-1)^1 = -1$
7	1	2	Less than $\frac{7}{2}$: 2 Greater than $\frac{7}{2}$: 4, 6	$(-1)^2 = 1$
11	2	3	Less than $\frac{11}{2}$: 2, 4 Greater than $\frac{11}{2}$: 6, 8, 10	$(-1)^3 = -1$
13	3	3	Less than $\frac{13}{2}$: 2, 4, 6 Greater than $\frac{13}{2}$: 8, 10, 12	$(-1)^3 = -1$
17	4	4	Less than $\frac{17}{2}$: 2, 4, 6, 8 Greater than $\frac{17}{2}$: 10, 12, 14, 16	$(-1)^4 = 1$
19	4	5	Less than $\frac{19}{2}$: 2, 4, 6, 8 Greater than $\frac{17}{2}$: 10, 12, 14, 16, 18	$(-1)^5 = -1$
p	5	6	Less than $\frac{17}{2}$: 2, 4, 6, 8, 10 Greater than $\frac{17}{2}$: 12, 14, 16, 18, 20, 22	$(-1)^6 = 1$

7.6 Proving Gauss's Lemma and the Quadratic Residue of 2

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

- Prove Gauss's Lemma
- Classify when 2 is a quadratic residue modulo a prime. .

Reading assignment:

Read: The remainder of Strayer Section 4.2. is on Moodle.

Turn in The $p \equiv 3 \pmod 9$ case of Strayer Theorem 4.8 (scanned notes Theorem 11.4.3/Theorem 11.4.4)

Solution: Mirroring Strayer's argument for $p \equiv 1 \pmod 8$:

If $p \equiv 3 \pmod 8$, then there exists $k \in \mathbb{Z}$ such that $p = 8k + 3$. Then

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{8k+3-1}{2} - \left\lfloor \frac{8k+3}{4} \right\rfloor = 4k + 1 - (2k) = 2k + 1 \equiv 1 \pmod 2,$$

and

$$\frac{p^2-1}{8} = \frac{(8k+3)^2 - 1}{8} = \frac{64k^2 + 48k + 9 - 1}{8} = 8k^2 + 6k + 1 \equiv 1 \pmod 2.$$

Thus, $\dfrac{p-1}{2} - \left\lfloor \dfrac{p}{4} \right\rfloor \equiv \dfrac{p^2-1}{8} \pmod 8$.

Remark 12. Gauss's Lemma is often stated as:

Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least absolute residues of the integers $a, 2a, 3a, \ldots, \dfrac{p-1}{2}$ modulo p that are negative. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Lemma 12. Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a.$$

The least absolute residues of ak and $a(p-k)$ differ by a negative sign. In other words,

$$ak \equiv -a(p-k) \pmod p.$$

Furthermore, for each $k = 1, 2, \ldots, \dfrac{p-1}{2}$, the exactly one of k and $-k$ is a least absolute residue of $\{a, 2a, 3a, \ldots, \dfrac{p-1}{2}a\}$.

Proof Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$ak \equiv -ap + ak \equiv -a(p-k) \pmod p.$$

Then

$$\{a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a\}$$

is a reduced residue system modulo p by . From Chapter 2, **??**,

$$\left\{\frac{-(p-1)}{2}, \frac{-(p-3)}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-2}{2}, \frac{p-1}{2}\right\}$$

is a reduced residue system modulo p. Thus, every element of $\{a, 2a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a\}$ is congruent to exactly one of $\left\{\frac{-(p-1)}{2}, \ldots, -1, 1, \ldots, \frac{p-2}{2}, \frac{p-1}{2}\right\}$. That is, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, both k and $-k$ are least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a\}$.

If k is the least absolute remainder of aj modulo p for some $j = 1, 2, \ldots, \frac{p-1}{2}$, then $-k$ is the absolute least residue of $a(p-j)$ modulo p and $p-j = \frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-1$. Thus, $-k$ is not an absolute least residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. Since there are $\frac{p-1}{2}$ elements of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, there must be $\frac{p-1}{2}$ distinct absolute least residues modulo p. Thus, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, exactly on of k and $-k$ is an absolute least residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$. ■

In-class Problem 34 Check Lemma 1 for

(a) $a = 3, p = 7$

(b) $a = 5, p = 11$

(c) $a = 6, p = 11$

Solution: (a) $a = 3, p = 7$

$$\begin{aligned} 3 \pmod 7,\ 3(2) \equiv -1 \pmod 7,\ 3(3) \equiv 2 \pmod 7,\\ 3(4) \equiv -2 \pmod 7,\ 3(5) \equiv 1 \pmod 7,\ 3(6) \equiv -3 \pmod 7, \end{aligned}$$

(b) $a = 5, p = 11$

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

(c) $a = 11, p = 23$

$$\begin{aligned} 11 \pmod{23},\ 11(2) \equiv -1 \pmod{23},\ 11(3) \equiv 10 \pmod{23},\\ 11(4) \equiv -2 \pmod{23},\ 11(5) \equiv 9 \pmod{23},\ 11(6) \equiv -3 \pmod{23},\\ 11(7) \equiv 8 \pmod{23},\ 11(8) \equiv -4 \pmod{23},\ 11(9) \equiv 7 \pmod{23},\\ 11(10) \equiv -5 \pmod{23},\ 11(11) \equiv 6 \pmod{23},\\ 11(12) \equiv -6 \pmod{23},\ 11(13) \equiv 5 \pmod{23},\\ 11(14) \equiv -7 \pmod{23},\ 11(15) \equiv 4 \pmod{23},\ 11(16) \equiv -8 \pmod{23},\\ 11(17) \equiv 3 \pmod{23},\ 11(18) \equiv -9 \pmod{23},\ 11(19) \equiv 2 \pmod{23},\\ 11(20) \equiv -10 \pmod{23},\ 11(21) \equiv 1 \pmod{23},\ 11(22) \equiv -11 \pmod{23}, \end{aligned}$$

We now prove Gauss's Lemma.

Proof Let $r_1, r_2, \ldots r_n$ be the least nonnegative residues of the integers $a, 2a, \ldots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$ and $s_1, s_2, \ldots, s_m$ be the least nonnegative residues that are less that $\frac{p}{2}$. Note that no r_i or s_j is 0, since p does not divide any of $a, 2a, \ldots \frac{p-1}{2}$. Consider the $\frac{p-1}{2}$ integers given by

$$p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m.$$

We want to show that these integers are the integers from 1 to $\frac{p-1}{2}$, inclusive, in some order. Since each integer is less than or equal to $\frac{p-1}{2}$, it suffices to show that no two of these integers are congruent modulo p.

If $p - r_i \equiv p - r_j \pmod{p}$ for some $i \neq j$, then $r_i \equiv r_j \pmod{p}$, but this implies that there exists some $k_i, k_j \in \mathbb{Z}$ such that $r_i = k_i a \equiv k_j a = r_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since

Multiple Choice:

(a) $p \nmid a$ ✓

(b) $p \mid a$

we know that the multiplicative inverse of a modulo p

Multiple Choice:

(a) exists ✓

(b) does not exist

and thus $k_i \equiv k_j \pmod{p}$, a contradiction. Thus, no two of the first n integers are congruent modulo p.

Similarly, no two of the second m integers are congruent. Now, if $p - r_i j \pmod{p}$, for some i and j, then $-r_i j \pmod{p}$. Thus, there exists $k_i, k_j \in \mathbb{Z}$ such that $-r_i = -k_i a \equiv k_j a = s_j \pmod{p}$ with $k_i \neq k_j$ and $1 \leq k_i, k_j \leq \frac{p-1}{2}$. Since $p \nmid a$, we know that the multiplicative inverse of a modulo p exists, and thus $-k_i \equiv k_j \pmod{p}$, a contradiction. Thus, the $\frac{p-1}{2}$ integers $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$ are the integers $1, 2, \ldots, \frac{p-1}{2}$ in some order.

Then,

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}$$

implies that

$$(-1)^n r_1 r_2 \cdots r_n s - 1 s_2 \cdots s_m \equiv \frac{p-1}{2}! \pmod{p}.$$

By the definition of r_i and s_j, we have

$$(-1)^n a(2a)(3a) \cdots (\frac{p-1}{2}a) \equiv \frac{p-1}{2}! \pmod{p}.$$

By reordering, we have

$$(-1)^n a^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv \frac{p-1}{2}! \pmod{p}.$$

Thus, $(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$. By Euler's criterion, we get that $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$. Since both sides of the congruence must be ± 1, we have $\left(\frac{a}{p}\right) = (-1)^n$. ■

We are going to prove a result about $\left(\frac{2}{p}\right)$ before our next technical lemma.

Theorem 23. Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & if\ p \equiv 1, 7 \pmod 8 \\ -1 & if\ p \equiv 3, 5 \pmod 8. \end{cases}$$

Proof By Gauss's Lemma, we have that $\left(\frac{2}{p}\right) = (-1)^n$, where n is the number of least positive residues of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are greater than $\frac{p}{2}$. Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \frac{p}{4}$; so $\left\lfloor \frac{p}{4} \right\rfloor$ of the integers $2, 2*2, 2*3, \ldots, \frac{p-1}{2}$ that are less than $\frac{p}{2}$, where $\lfloor \cdot \rfloor$ is the greatest integer (or floor) function. So, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of these integers are greater than $\frac{p}{2}$, from which

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor}$$

by Gauss's Lemma. For the first equality, it suffices to show that

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2.$$

If $p \equiv 1 \pmod 8$, the $p = 8k+1$ for some $k \in \mathbb{Z}$. That gives us

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{(8k+1)-1}{2} - \left\lfloor \frac{8k+1}{4} \right\rfloor = 4k - 2k = 2k \equiv 0 \pmod 2$$

and

$$\frac{p^2-1}{8} = \frac{(8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0 \pmod 2.$$

Thus, holds when $p \equiv 1 \pmod 8$. The rest of the cases are left as homework. ■

7.7 Geometric Lemma for Quadratic reciprocity

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

- Count lattice point in a rectangle with side lengths $\frac{p-1}{2}$ and $\frac{q-1}{2}$ two different ways
- Use the two counting methods to prove quadratic reciprocity .

Reading assignment:

Read: None

Theorem 24 (Quadratic Reciprocity)**.** Let p and a be odd primes with $p \neq q$. Then

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

Definition 8. A *lattice point* is a point $(x, y) \in \mathbb{R}^2$ where $x, y \in \mathbb{Z}$. We can write this as $(x, y) \in \mathbb{Z}^2$.

We will use two different methods to count the number of lattice points in the rectangle with vertices $(0,0)$, $\left(\frac{p-1}{2}\right)$, $\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, $\left(0, \frac{q-}{2}\right.$ other than the axes. The easy method is multiplication: there are $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ lattice points. The other method involves counting the lattice points (in the same rectangle) with $y > \frac{q}{p}$, call this number N_1, and those with $y < \frac{q}{p}$, call this number N_2. Then there are a total of $N_1 + N_2$ lattice points.

This changes the statement of quadratic reciprocity to

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_1}(-1)^{N_2}$$

Access GeoGebra at https://www.geogebra.org/m/tuf7y6sh.

Two stills from the GeoGebra interactive are in Figure 3 and Figure 4.

Geogebra link: `https://www.geogebra.org/m/tuf7y6sh`

In-class Problem 35 The steps below outline the proof in the general case, when $p = 7$ and $q = 5$. This case is in Figure 3. Move the sliders to $p = 7$ and $q = 5$.

(a) The line segment between the origin and $(7, 5)$ has slope $\frac{5}{7}$. Since $p = 7$ and $q = 5$ are distinct primes, there are no lattice points on line segment except the endpoints.

(b) First, we will count the number of points N_1 where $\frac{5-1}{2} \geq y > \frac{5}{7}x > 0$. This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines $j = 1, 2$. Let's just check the numbers we should get:

- When $j = 1$, there are 1 lattice points.
- When $j = 2$, there are 2 lattice points.

For each j, we are counting positive integers $x < \frac{7}{5}j$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$ ✓ .

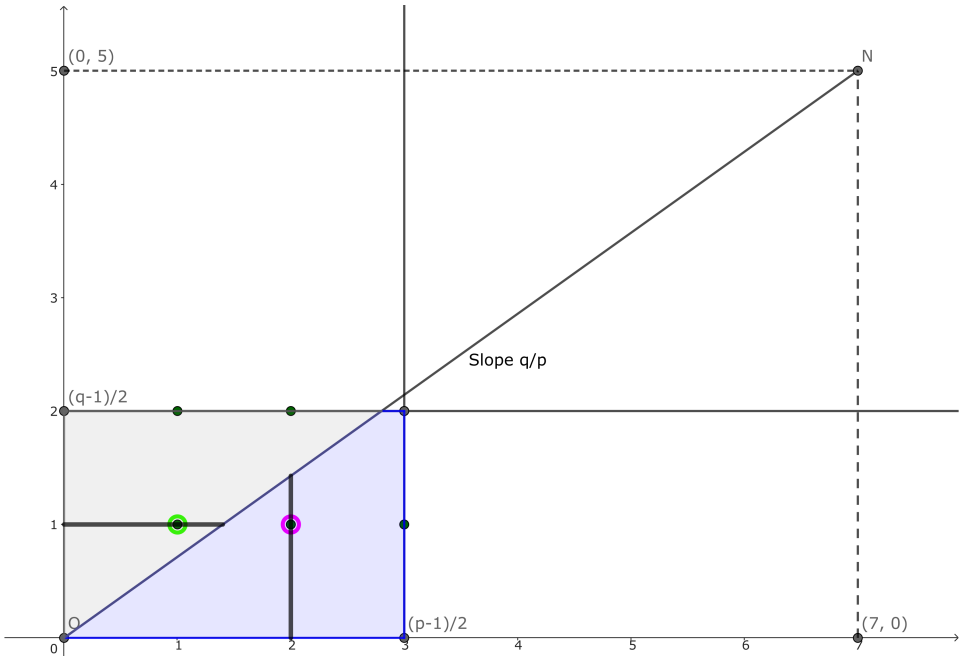


Figure 1: The lattice for the $p = 7, q = 5$ problem, with the $j = 1$ and $k = 2$ cases highlighted

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$.

Thus, the total number of lattice points in this triangle, N_1, is

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{5j}{7} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{7j}{5} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{5j}{7} \right\rfloor$

(c) Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number N_2.

The region is bounded by $0 < x \leq \frac{7-1}{2}$, $0 < y < \frac{5}{7}x$, and $y \leq \frac{5-1}{2}$. Now, the point A where $y = \frac{5}{7}x$ intersects $y = \frac{5-1}{2}$ is between two consecutive lattice points, with coordinates $x = 2, y = 2$ and $x = 3, y = 2$. Similarly, the point B where $y = \frac{5}{7}x$ intersects $x = \frac{7-1}{2}$ is between two consecutive lattice points, with coordinates $x = 3, y = 2$ and $x = 3, y = 3$. Thus, the only lattice point in the triangle A, B and $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$ is $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$. Therefore, there are also N_2 lattice points in the triangle with vertices $(0, 0), \left(\frac{7-1}{2}, 0\right), \left(\frac{7-1}{2}, \frac{5-1}{2}\right)$.

(d) We use the same method as N_1 to find N_2. We will count how many lattice points on each vertical lines $k = 1, 2, 3$. Let's just check the numbers we should get:

- When $k = 1$, there are 0 lattice points.
- When $k = 2$, there are 1 lattice points.
- When $k = 3$, there are 2 lattice points.

For each k, we are counting positive integers $y < \frac{5}{7}k$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$.

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{7k}{5} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{5k}{7} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{7k}{5} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{5k}{7} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 =$ (3)(2).

In-class Problem 36 The steps below outline the proof in the general case, when $p = 23$ and $q = 13$. Move the sliders to $p = 23$ and $q = 13$.

(a) The line segment between the origin and $(23, 13)$ has slope $\frac{13}{23}$. Since $p = 23$ and $q = 13$ are distinct primes, there are no lattice points on line segment except the endpoints.

(b) First, we will count the number of points N_1 where $\frac{13-1}{2} \geq y > \frac{13}{23}x > 0$. This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines $j = 1, 2, \ldots, 6$. Let's just check one case, we should get:

- When $j = 3$, as in Figure 4, there are 5 lattice points.

For each j, we are counting positive integers $x < \frac{23}{13}j$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$ ✓ .

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$.

Thus, the total number of lattice points in this triangle is

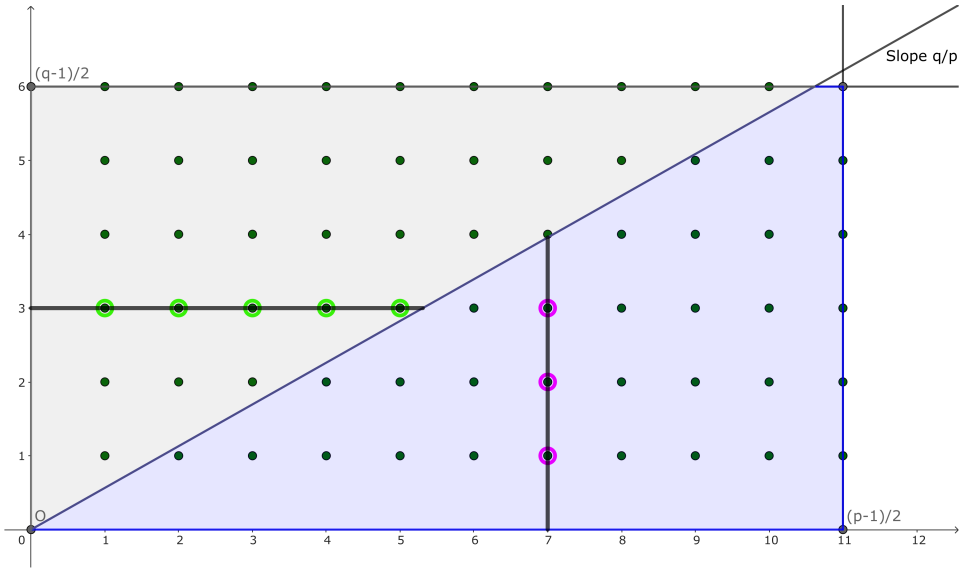


Figure 2: The lattice for the $p = 23, q = 13$, with the $j = 3$ and $k = 7$ cases highlighted

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{23j}{13} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{13j}{23} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{23j}{13} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{13j}{23} \right\rfloor$

(c) Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number N_2.

The region is bounded by $0 < x \leq \frac{23-1}{2}$, $0 < y < \frac{13}{23}x$, and $y \leq \frac{13-1}{2}$. Now, the point A where $y = \frac{13}{23}x$ intersects $y = \frac{13-1}{2}$ is between two consecutive lattice points, with coordinates $x = 10, y = 6$ and $x = 11, y = 6$. Similarly, the point B where $y = \frac{13}{23}x$ intersects $x = \frac{23-1}{2}$ is between two consecutive lattice points, with coordinates $x = 11, y = 6$ and $x = 11, y = 7$. Thus, the only lattice point in the triangle A, B and $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$ is $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$. Therefore, there are also N_2 lattice points in the triangle with vertices $(0, 0), \left(\frac{23-1}{2}, 0\right), \left(\frac{23-1}{2}, \frac{13-1}{2}\right)$.

(d) We use the same method as N_1 to find N_2. We will count how many lattice points on each vertical lines $k = 1, 2, \ldots, 11$. Let's just check the numbers we should get:

- When $k = 7$, as in Figure 4, there are 3 lattice points.

For each k, we are counting positive integers $y < \frac{13}{23}k$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$.

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{23k}{13} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{13k}{23} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{23k}{13} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{13k}{23} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 =$ (11)(6).

Now we will use without proof that

Lemma 13. Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$ and a odd. If

$$N = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor,$$

then

$$\left(\frac{a}{p}\right) = (-1)^N.$$

Proof of Law of Quadratic Reciprocity Let p and q be distinct odd primes. Then from ,

$$\left(\frac{p}{q}\right) = (-1)^{N_1}, \quad \left(\frac{q}{p}\right) = (-1)^{N_2}, \qquad \text{where} \quad N_1 = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{p}{q} j \right\rfloor \quad \text{and} \quad N_2 = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{q}{p} j \right\rfloor.$$

Thus, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_1+N_2}$. It remains to show that $N_1 + N_2 = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

Without loss of generality, assume that $p > q$. We draw the rectangle $(0,0), \left(\frac{p-1}{2}, 0\right), \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$, and $\left(0, \frac{q-1}{2}\right)$, as in the GeoGebra example. Then there are $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ lattice points in this rectangle, excluding the axes.

The line segment between the origin and (p, q) has slope $\frac{q}{p}$. Since p and q are distinct primes, there are no lattice points on line segment except the endpoints.

For each j, we are counting positive integers $x < \frac{p}{q} j$. Which is,

Multiple Choice:

(a) $\left\lfloor \frac{pj}{q} \right\rfloor$ ✓ .

(b) $\left\lfloor \frac{qj}{p} \right\rfloor$.

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(a) $N_1 = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor$ ✓

(b) $N_1 = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{qj}{p} \right\rfloor$

(c) $N_1 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{pj}{q} \right\rfloor$

(d) $N_1 = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{qj}{p} \right\rfloor$

Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number N_2. The region is bounded by $0 < x \leq \frac{p-1}{2}$, $0 < y < \frac{q}{p}x$, and $y \leq \frac{q-1}{2}$. Now, the point A where $y = \frac{q}{p}x$ intersects $y = \frac{q-1}{2}$ is between two consecutive lattice points, with coordinates $x = 10, y = (q-1)/2$ and $x = (p-1)/2, y = (q-1)/2$. Similarly, the point B where $y = \frac{q}{p}x$ intersects $x = \frac{p-1}{2}$ is between two consecutive lattice points, with coordinates $x = (p-1)/2, y = (q-1)/2$ and $x = (p-1)/2, y = 7$. Thus, the only lattice point in the triangle A, B and $\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$ is $\left(\frac{p-1}{2}, \frac{q-1}{2}\right)$. Therefore, there are also N_2 lattice points in the triangle with vertices $(0,0), \left(\frac{p-1}{2}, 0\right), \left(\frac{p-1}{2}, \frac{q-1}{2}\right)$.

We use the same method as N_1 to find N_2. We will count how many lattice points on each vertical lines $k = 1, 2, \ldots, \frac{p-1}{2}$. For each k, we are counting positive integers $y < \frac{q}{p}k$. Which is,

Multiple Choice:

(a) $\left\lfloor \frac{pj}{q} \right\rfloor$.

(b) $\left\lfloor \frac{qj}{p} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(a) $N_2 = \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$

(b) $N_2 = \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor$

(c) $N_2 = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor$

(d) $N_2 = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 = \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{pk}{q} \right\rfloor + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ ■

8 Nonlinear Diophantine Equations

8.1 Nonlinear Diophantine equations

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

- Define a nonlinear Diophantine equation .

Reading assignment:

Reading None

Definition 9. A Diophantine equation is *nonlinear* if it is not linear.

Example 21. (a) The Diophantine equation $x^2 + y^2 = z^2$ is our next section. Solutions are called Pythagorean triples.

(b) Let $n \in \mathbb{Z}$ with $n \geq 3$. The Diophantine equation $x^n + y^n = z^n$ is the subject of the famous Fermat's Last Theorem. We will also prove one case of this.

(c) Let $n \in \mathbb{Z}$. The Diophantine equation $x^2 + y^2 = n$ tells us which integers can be represented as the sum of two squares.

(d) Let $d, n \in \mathbb{Z}$. The Diophantine equation $x^2 - dy^2 = n$ is known as Pell's equation.

Sometimes we can use congruences to show that a particular nonlinear Diophantine equation has no solutions.

Example 22. Prove that $3x^2 + 2 = y^2$ is not solvable.

Solution: Assume that there is a solution. Then any solution to the Diophantine equation is also a solution to the congruence $3x^2 + 2 \equiv y^2 \mod 3$, which implies $2 \equiv y^2 \mod 3$, which we know is false. Thus there are no integer solutions to $3x^2 + 2 = y^2$.

Note: viewing the same equation modulo 2 says $x^2 \equiv y^2 \mod 2$, which does not give us enough information to prove a solution does not exist–it also is not enough information to conclude a solution exists.

8.2 Pythagorean triples

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

- Define a nonlinear Diophantine equation
- Define a primitive Pythagorean triple
- Prove the formula for generating primitive Pythagorean triples .

One of the most famous math equations is $x^2 + y^2 = z^2$, probably because we learn it in high school. We are going to classify all integer solutions to the equation.

Definition 10. A triple (x, y, z) of positive integers satisfying the Diophantine equation $x^2 + y^2 = z^2$ is called *Pythagorean triple*.

Select the Pythagorean triples:

Select All Correct Answers:

(a) 3,4,5 ✓

(b) 5,12,13 ✓

(c) -3,4,5

(d) 6,8,10 ✓

(e) 0,1,1

It is actually possible to classify all Pythagorean triples, just like we did for linear Diophantine equations in two variables. To simplify this process, we will work with $x, y, z > 0$, and $(x, y, z) = 1$. For any given solution of this form, we have that $(-x, y, z), (x, -y, z), (x, y, -z), (-x, -y, z), (x, -y, -z), (-x, y, -z)$, and $(-x, -y, -z)$ are also solutions to the Diophantine equation, as is (nx, ny, nz) for any integer n. Thus, we call such a solution a *primitive Pythagorean triple*. We call $(0, n, \pm n)$ and $(n, 0, \pm n)$ the *trival solutions*.

Theorem 25. For a primitive Pythagorean triple (x, y, z), exactly one of x and y is even.

Proof If x and y are both even, then z must also be even, contradicting that $(x, y, z) = 1$.

If x and y are both odd, then z is even. Now we can work modulo 4 to get a contradiction. Since x and y are odd, we have that $x^2 \equiv y^2 \equiv 1 \pmod 4$. Since z is even, we have that $z^2 \equiv 0 \pmod 4$, but $x^2 + y^2 \equiv 2 \pmod 4$.

Thus, the only remaining option is exactly one of x and y is even. ■

Theorem 26 (Theorem 6.3)**.** There are infinitely many primitive Pythagorean triples x, y, z with y even. Furthermore, they are given precisely by the equations

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2 \end{aligned}$$

where $m, n \in \mathbb{Z}, m > n > 0, (m, n) = 1$ and exactly one of m and n is even.

Example 23. (a) $m = 2$ and $n = 1$ satisfy the conditions of m and n in the theorem. This gives $x = 3, y = 4, z = 5$.

(b) $m = 3$ and $n = 2$ gives $x = 5, y = 12, z = 13$.

(c) Try with your own values of m and n.

Proof We first show that given a primitive Pythagorean triple with y even, there exist m and n as described. Since y is even, y and z are both odd. Moreover, $(x, y) = 1, (y, z) = 1$, and $(x, z) = 1$. Now,

$$y^2 = z^2 - x^2 = (x + z)(z - x)$$

implies that

$$\left(\frac{y}{2}\right)^2 = \frac{(x+z)}{2}\frac{(z-x)}{2}.$$

To show, $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = 1$, let $\left(\frac{(x+z)}{2}, \frac{(z-x)}{2}\right) = d$. Then $d \mid \frac{z+x}{2}$ and $d \mid \frac{z-x}{2}$. Thus, $d \mid \frac{z+x}{2} + \frac{z-x}{2} = z$ and $d \mid \frac{z+x}{2} - \frac{z-x}{2} = x$. Since $(x, z) = 1$, we have that $d = 1$. Thus, $\frac{(x+z)}{2}$ and $\frac{(z-x)}{2}$ are perfect squares. Let

$$m^2 = \frac{(x+z)}{2}, \quad n^2 = \frac{(z-x)}{2}.$$

Then $m > n > 0, (m, n) = 1, m^2 - n^2 = x, 2mn = y$, and $m^2 + n^2 = z$. Also, $(m, n) = 1$ implies that not both m and n are both even. If both m and n are odd, we have that z and x are both even, but $(x, z) = 1$. This proves that every primitive Pythagorean triple has this form.

Now we prove that given any such m and n, we have a primitive Pythagorean triple. First, $(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. We need to show that $(x, y, z) = 1$. Let $(x, y, z) = d$. Since exactly one of m and n is even, we have that x and z are both odd. Then d is odd, and thus $d = 1$ or d is divisible by some odd prime p. Assume that $p \mid d$. Thus, $p \mid x$ and $p \mid z$. Thus, $p \mid z + x$ and $p \mid z - x$. Thus, $p \mid (m^2 + n^2) + (m^2 - n^2) = 2m^2$ and $p \mid (m^2 + n^2) - (m^2 - n^2) = 2n^2$. Since p is odd, we have that $p \mid m^2$ and $p \mid n^2$, but $(m, n) = 1$, so $d = 1$. ■

8.3 Sums of squares

Reading assignment:

Reading None

The first result will prove which primes can be written as the sum of two squares. Note $1^2 + 1^2 = 2$, and if a is a positive integer such that $a \equiv 3 \pmod 4$, then a cannot be written as the sum of two squares.

Proposition 25. Let $m, n \in \mathbb{Z}$ with $m, n > 0$. If m and n can be written as the sums of two squares of integers, then mn can be written as the sum of two squares of integers.

Proof Let $m, n \in \mathbb{Z}$ with $m, n > 0$ and assume that there exists $a, b, c, d \in \mathbb{Z}$ such that $m = a^2 + b^2$ and $n = c^2 + d^2$. Then

$$\begin{aligned} mn = (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

■

We need two lemmas to prove

Theorem 27. Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.

Lemma 14. If p is a prime such that $p \equiv 1 \pmod 4$, then there are integers x, y such that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.

Proof Since $p \equiv 1 \pmod 4$, we have that $\left(\dfrac{-1}{p}\right) = 1$. Thus, there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 1$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + y^2 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

Proposition 26. A prime p can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof If $p \equiv 3 \pmod 4$, then p cannot be written as the sum of two squares. Since the squares modulo 4 are 0 and 1, the integers that can be written as a sum of two squares are congruent to $0^2 + 0^2 \equiv 0 \pmod 4$, $1^2 + 0^2 \equiv 1 \pmod 4$ or $1^2 + 1^2 \equiv 2 \pmod 4$, so no integer that is congruent to $3 \pmod 4$ can be written as the sum of two squares. Thus, if p can be written as the sum of two squares, $p \not\equiv 3 \pmod 4$. That is, $p = 2$ or $p \equiv 1 \pmod 4$.

We will prove the other direction with two cases. When $p = 2$, then $1^2 + 1^2 = 2$. It remains to show that every prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

Let $p \equiv 1 \pmod 4$, and let m be the least integer such that there exists $x, y \in \mathbb{Z}$ with $x^2 + y^2 = mp$ and $0 < m < p$ as in the previous theorem. We show that $m = 1$. Assume, by way of contradiction, that $m > 1$. Let $a, b \in \mathbb{Z}$ such that

$$a \equiv x \pmod m, \quad \frac{-m}{2} < a \leq \frac{m}{2}$$

and

$$b \equiv y \pmod m, \quad \frac{-m}{2} < b \leq \frac{m}{2}.$$

Then

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{m},$$

and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 = km$. (Why?)

Now,

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By , $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$, so $(ax + by)^2 + (ay - bx)^2 = km^2p$. Since $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$,

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

and

$$ay - bx \equiv xy - yx \equiv 0 \pmod{m}$$

so $\dfrac{ax + by}{m}, \dfrac{ay - bx}{m} \in \mathbb{Z}$ and

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp.$$

Now, $\dfrac{-m}{2} < a \leq \dfrac{m}{2}$ and $\dfrac{-m}{2} < b \leq \dfrac{m}{2}$ imply that $a^2 \leq \dfrac{m^2}{4}$ and $b^2 \leq \dfrac{m^2}{4}$. Thus, $km = a^2 + b^2 \leq \dfrac{m^2}{2}$. Thus, $k \leq \dfrac{m}{2} < m$, but this contradicts that m is the smallest such integer.

Thus, $m = 1$ and p can be written as the sum of two squares of integers. ■

8.4 Sum of Two Squares

Reading assignment:

Reading None

Theorem 28. Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.

Proof ($\Leftarrow$) Assume that every prime factor of n congruent to 3 modulo 4 occurs to an even power in the prime factorization of n. Then n can be written as $n = m^2 p_1 p_2 \dots p_r$ where $m \in \mathbb{Z}$ and $p_1, p_2, \dots, p_r$ are distinct prime numbers equal to 2 or equivalent to 1 modulo 4. Now, $m^2 = m^2 + 0^2$, so is expressible as the sum of two squares, and each p_1 is also expressible as the sum of two squares by the theorem labeled Primes as Sums of Squares. Thus, by the first theorem of the day, n is expressible as the sum of two squares.

($\Rightarrow$) Assume that p is an odd prime number and that $p^{2i+1}, i \in \mathbb{Z}$ occurs in the prime factorization of n. We will show that $p \equiv 1 \pmod 4$. Since n is expressible as the sum of two squares of integers, there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. Let $(x, y) = d, a = \dfrac{x}{d}, b = \dfrac{y}{d}$ and $m = \dfrac{n}{d^2}$. Then $(a, b) = 1$ and $a^2 + b^2 = m$. Let $p^j, j \in \mathbb{Z}$ be the largest power of p dividing d. Then $p^{(2i-1)-2j} \mid m$; since $(2i + 1) - 2j) \geq 1$, we have $p \mid m$. Now, $p \nmid a$ since $(a, b) = 1$. Thus, there exists $z \in \mathbb{Z}$ such that $az \equiv b \pmod p$. Then $m = a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \pmod p$.

Since $p \mid m$, we have

$$a^2(1 + z^2) \equiv 0 \pmod p$$

or $p \mid a^2(1 + z^2)$ or $z \equiv -1 \pmod p$. Thus, -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. By contrapositive, any prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n as desired.

■

8.5 Sums of three squares

We prove which integers cannot be written as the sum of four squares.

We finish out the sums of squares section by classifying which integers can be written as the sum of three squares and sum of four squares. These cases are more difficult than the sum of two squares since there is no formula analogous to the April 8 participation assignment.

Theorem 29 (Sum of three squares necessary condition)**.** Let $m, n \in \mathbb{Z}$ with $m, n \geq 0$. If $N = 4^m(8n + 7)$, then N can not be written as the sum of 3 squares.

Proof We start by proving the $m = 0$ case. In order to get a contradiction, assume that $N = 8n + 7$ can be written as the sum of three squares. Thus, there exists $x, y, z \in \mathbb{Z}$ such that

$$8n + 7 = x^2 + y^2 + z^2.$$

Now, $8n + 7 \equiv 7 \pmod 8$ and $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$ (by participation assignment), which gives the contradiction we are looking for.

Now we assume $m > 0$. and again assume $N = 4^m(8n + 7)$ can be written as the sum of three squares. As before, there exist $x, y, z \in \mathbb{Z}$ such that

$$4^m(8n + 7) = x^2 + y^2 + z^2$$

and x, y, z are even (by participation assignment). So there exists x', y' and z' such that $x = 2x', y = 2y'$, and $z = 2z'$. Substituting into our definition of N, we get

$$4^{m-1}(8n + 7) = (x')^2 + (y')^2 + (z')^2.$$

Repeating this process $m - 1$ times, we find $8n + 7$ is expressible as a sum of three squares, a contradiction. Thus, $N = 4^m(8n + 7)$ cannot be written as the sum of three squares. ■

Now, the converse is true. Legendre proved this in 1798, but is much harder to prove, due to the lack of formula like the one from April 8 participation assignment. Note that any integer that cannot be written as the sum of three squares cannot be written as the sum of two squares.

Example 24. Determine whether 1584 is expressible as the sum of three squares.

The highest power of 4 that divides 1584 evenly is 16, leaving $99 \equiv 3 \pmod 8$. Thus, 1584 can be written as the sum of three squares:

Multiple Choice:

(a) True ✓

(b) False

(c) Not enough information

Since this also allows us to factor 1584, we also know 1584 can be written as the sum of two squares:

Multiple Choice:

(a) True

(b) False ✓

(c) Not enough information

8.6 Sums of four squares

We prove that all integers can be written as the sum of four squares.

We now prove that all positive integers can be written as the sum of four squares. The new few results are similar to the proof of the sum of two squares. Some of these calculations are even more involved, but still use multiplication and factoring. I will upload a scan of the sums of squares section from *Elementary Number Theory* by James K. Strayer. All of the missing calculations are expanding and refactoring polynomial expression.

Theorem 30 (Euler)**.** Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of four squares, then so is $n_1 n_2$.

Proof Let $a, b, c, d, w, x, y, u \in \mathbb{Z}$ such that

$$n_1 = a^2 + b^2 + c^2 + d^2$$

and

$$n_1 = w^2 + x^2 + y^2 + z^2.$$

Then

$$n_1 n_2 = (aw + bx + cy + dz)^2 + (-ax + bw - cz + dy)^2 + (-ay + bz + cw - dx)^2 + (-az - by + cx + dw)^2$$

as desired. ■

Theorem 31 (Also Euler)**.** If p is an odd prime number, then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.

Proof We consider two cases.

Case 1: $p \equiv 1 \pmod 4$. Then $\left(\dfrac{-1}{p}\right) = 1$, so there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 0$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + 1 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$.

Case 2: $p \equiv 3 \pmod 4$. Let a be the least positive quadratic nonresidue modulo p. Note that $a \geq 2$. Then

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1$$

and so there exists $x \in \mathbb{Z}$ with $0 < x \leq \dfrac{p-1}{2}$ such that $x^2 \equiv -a \pmod p$. Now, $a - 1$ is positive and less than a, then $a - 1$ is a quadratic residue modulo p. Thus, there exists $y \in \mathbb{Z}$ with $0 < y \leq \dfrac{p-1}{2}$ such that $y^2 \equiv a - 1 \pmod p$. Thus,

$$x^2 + y^2 + 1 \equiv (-a) + (a - 1) + 1 \equiv 0 \pmod p$$

or, equivalently, $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Again, $k > 0$. Furthermore,

$$kp = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

We will prove that every prime number can be written as the sum of four squares.

Theorem 32 (Lagrange, 1770)**.** All prime numbers can be written as the sum of four squares.

Proof When $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, we are done. In fact, we can also writes a prime p where $p \equiv 1 \pmod 4$ as $p = x^2 + y^2 + 0^2 + 0^2$, but the following method works for all odd primes.

Let m be the least positive integer where $x^2 + y^2 + z^2 + w^2 = mp$ and $0 < m < p$. We want to show that $m = 1$. To get a contradiction, assume $m > 1$. We consider two cases.

Case 1: m even. There are three posibilities: w, x, y, z are all even; w, x, y, z are all odd; two of w, x, y, z are odd and the other two are even. In all three cases, we can assume $w \equiv x \pmod 2$ and $y \equiv z \pmod 2$. Then $\frac{w+x}{2}, \frac{w-x}{2}, \frac{y+z}{2}, \frac{y-z}{2}$ are integers and

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{mp}{2}$$

which contradicts the fact that m is minimal.

Case 2: m is odd.

Then $m \geq 3$. Let $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned}
a &\equiv w \pmod m, \frac{-m}{2} < a < \frac{m}{2} \\
b &\equiv x \pmod m, \frac{-m}{2} < b < \frac{m}{2} \\
c &\equiv y \pmod m, \frac{-m}{2} < c < \frac{m}{2} \\
d &\equiv z \pmod m, \frac{-m}{2} < d < \frac{m}{2}.
\end{aligned}$$

Then $a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv mp \equiv 0 \pmod m$ and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 + c^2 + d^2 = km$. Now

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (km)(mp) = km^2p.$$

By theorem 2 from today, we can rewrite $a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)$ as the sum of four squares $(aw+bx+cy+dz)^2 + (-ax+bw-cz+dy)^2 + (-ay+bz+cw-dx)^2 + (-az-by+cx+dw)^2 = km^2p$. Since $a \equiv w \pmod m, b \equiv x \pmod m, c \equiv y \pmod m, \frac{-m}{2} < c < \frac{m}{2}, d \equiv z \pmod m, \frac{-m}{2} < d < \frac{m}{2}$, we have

$$\begin{aligned}
aw + bx + cy + dz \equiv w^2 + x^2 + y^2 + z^2 &\equiv 0 \pmod m \\
-ax + bw - cz + dy \equiv -wx + xw - yz + zy &\equiv 0 \pmod m \\
-ay + bz + cw - dx \equiv -wy + yw + xz - zx &\equiv 0 \pmod m \\
-az - by + cx + dw \equiv -wx + zw - xy + yx &\equiv 0 \pmod m
\end{aligned}$$

Let $W = \frac{w^2 + x^2 + y^2 + z^2}{m}, X = \frac{-wx + xw - yz + zy}{m}, Y = \frac{-wy + yw + xz - zx}{m}, Z = \frac{-wx + zw - xy + yx}{m}$. Then $W^2 + X^2 + Y^2 + Z^2 = \frac{km^2p}{m^2} = kp$. Since $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$, then $a^2, b^2, c^2, d^2 < \frac{m^2}{4}$. Thus,

$$km = a^2 + b^2 + c^2 + d^2 < \frac{4m^2}{4}$$

and $k < m$. This contradicts that m is the smallest such integers.

Thus, $m = 1, w^2 + x^2 + y^2 + z^2 = p$. ■

Theorem 33 (Lagrange)**.** All positive integers can be written as the sum of four squares.

Proof Let $n \in \mathbb{Z}$ with $n > 1$. If $n = 1 = 1^2 + 0^2 + 0^2 + 0^2$. If $n > 1$, then n is the product of primes by the Fundamental Theorem of Arithmetic. By the previous theorem, every prime number can be written as the sum of four squares. By theorem 2 from today, n is can be written by the sum of four squares. ■

We finish this section with a few famous problems.

Example 25 (Waring's Problem, 1770)**.** Let $k \in \mathbb{Z}$ with $k > 0$. Does there exist a minimum integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power?

For example, $g(1) = 1$. Today we showed that $g(2) = 4$. The next step would be to find if $g(3)$ exists and what it equals.

Theorem 34 (Hilbert, 1906)**.** Let $k \in \mathbb{Z}$ with $k > 0$. There exists a minimal integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power.

The proof of Hilbert's theorem does not provide a formula for $g(k)$, merely proves it exists. Numerical evidence suggests $g(k) = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2$. It's been proven that there are only finitely many (or 0) k where the formula does not hold, and the formula holds when $k \leq 471,600,000$. Thus, $g(3) = 9, g(4) = 19$, and $g(5) = 37$. Proofs of these facts come from analytic number theory.

8.7 Sums and Differences of Squares

Reading assignment:

Reading and Turn in: This fill-in-the-blank version of the proof of Sum of Three Squares

In-class Problem 37 (Chapter 6, Exercise 34) Prove that a positive integer can be written as the difference of two squares of integers if and only if it is not of the form $4n+2$ for some $n \in \mathbb{Z}$.

Solution: ($\Rightarrow$) We will show that if a positive integer can be written as the difference of two squares of integers, then it is not of the form $4n+2$ for some $n \in \mathbb{Z}$.

(Proof)

($\Leftarrow$) We will show that any positive integer not of the form $4n+2$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers.

First, we will show that if a and b are positive integers that can be written as the difference of two squares of integers, then so can ab.

(Proof)

Now we will show that every odd prime can be written as the difference of two squares of integers. Let p be an odd prime. Then $p = x^2 - y^2 = (x-y)(x+y)$ when $x = \frac{p+1}{2}$ and $y = \frac{p-1}{2}$. Therefore every odd number can be written as the difference of two squares since _____.

It remains to show that every positive integer of the form $4n$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers. Why is this the only remaining case?

Similar to the odd prime case, $4n = x^2 - y^2 = (x-y)(x+y)$ when $x = n+1$ and $y = n-1$ or when $x = \frac{n}{2} - 2$ and $y = \frac{n}{2} + 2$ (solutions are not unique).

If there is time

In-class Problem 38 (Chapter 6, Exercise 14d) Let x, y, z be a primitive Pythagorean triple with y even. Prove that $x + y \equiv x - y \equiv 1, 7 \pmod 8$.

Hint: *First show that* $x + y \equiv x - y \pmod 8$.

Solution: Let x, y, z be a primitive Pythagorean triple with y even. Then from Theorem 6.3, there exist positive integers m, n with $m > n, (m, n) = 1$ and exactly one of m, n even such that

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ z &= m^2 + n^2. \end{aligned}$$

Thus, $4 \mid y$ and $y \equiv -y \pmod 8$. Adding x to both sides of the congruence gives $x + y \equiv x - y \pmod 8$.

Since exactly one of m, n even, $x \equiv 0 - 1, 4 - 1, 1 - 0, 1 - 4 \pmod 8$. When $x \equiv \pm 1 \pmod 8$, $4 \mid mn$ and thus $y = 2mn \equiv 0 \pmod 8$. Thus, $x + y \equiv x - y \equiv \pm 1 \pmod 8$. When $x \equiv \pm 3 \pmod 8$, $4 \nmid mn$ and thus $y = 2mn \equiv 4 \pmod 8$. Thus, $x + y \equiv x - y \equiv \pm 1 \pmod 8$.

8.8 Fermat's Last Theorem

Reading assignment:

Read Section 6.4

Turn in Explain the method of decent in your own words

After the Diophantine equation $x^2+y^2=z^2$, one generalization is $x^n+y^n=z^n$ for $n \geq 3$. Fermat's Last Theorem was first conjectured in 1637 and proven in 1995 by Andrew Wiles. Attempts to solve this problem through the centuries have created new branches of mathematics.

Theorem 35 (Fermat's Last Theorem)**.** The Diophantine equation $x^n+y^n=z^n$ has no nonzero integer solutions for $n \geq 3$.

We will show that it suffices to prove Fermat's Last Theorem for the cases of n and odd prime and $n=4$.

Theorem 36. The Diophantine equation $x^n+y^n=z^n$ has a solution no solutions for $n \geq 3$ if and only if there are no solutions for n an odd prime or $n=4$.

Proof Let $n \in \mathbb{Z}$ and $n \geq 3$. Let $n=ab$ where $a, b \in \mathbb{Z}$ and b is either an odd prime or 4. If x, y, z is a solution to $x^n+y^n=z^n$, then x^a, y^a, z^a is a solution to $x^b+y^b=z^b$. By contraposition, if $x^b+y^b=z^b$ has no solutions, then $x^n+y^n=z^n$ has no solutions. ■

We will prove the case where $n=4$ using the *method of decent.* This is the only case that Fermat proved. The next 400+ years were spent proving the theorem for odd primes. We will go through the decent arguement slowly on Monday. However, we can prove other facts about solutions to $x^n+y^n=z^n$. We can also use a similar decent arguement to show $x^4-y^4=z^2$ has no nontrivial integer solutions.

In-class Problem 39 (Chapter 6, Exercise 20) Let $x, y, z \in \mathbb{Z}$ and let p be a prime number.

(a) Prove that if $x^{p-1}+y^{p-1}=z^{p-1}$, then $p \mid xyz$.

(b) Prove that if $x^p+y^p=z^p$, then $p \mid (x+y-z)$.

Hint: *Recall Fermat's Little Theorem and Corollary 2.15.*

Hint: *For the first, try contradiction.*

Theorem 37 (Fermat's Right Triangle Theorem)**.** There are no right triangles with integer side lengths whose area is a perfect square.

Proof For a contradiction, assume that there exists a right triangle with integer side lengths a, b, c and area n^2 for some integer n. Then $a^2+b^2=c^2$ from the Pythagorean Theorem and $\frac{ab}{2}=n^2$ from the triangle area formula. Multiplying the second equation by 4 gives $2ab=4n^2$. Thus,

$$(a+b)^2=a^2+b^2+2ab=c^2+(2n)^2$$
$$(a-b)^2=a^2+b^2-2ab=c^2-(2n)^2.$$

Multiplying these two equations together gives

$$(a+b)^2(a-b)^2=c^4-(2n^2)^4.$$

Thus, $x=c, y=2n^2$, and $z=(a+b)(a-b)$ is a solution to $x^4-y^4=z^2$, which we will prove has no solutions. ■

The idea of the method of decent for proving no solution exists for a Diophantine equation is to assume a solution exists. Then use this solution to construct one that has one component that is strictly smaller than the original solution. This process could be repeated indefinitely, but it is not possible to construct an infinitely decreasing list of positive integers. Thus, no solution exists.

Theorem 38. The Diophantine equation $x^4 + y^4 = z^2$ has not solutions in nonzero integers x, y, z.

Note: If x, y, z is a solution to $x^4 + y^4 = z^4$, then

Multiple Choice:

(a) x, y, z

(b) x, y, z^2 ✓

x, y, z^2 is a solution to $x^4 + y^4 = z^4$. By contraposition, if $x^4 + y^4 = z^2$ has no solutions, then $x^4 + y^4 = z^4$ has no solutions.

Proof Assume by way of contradiction, that $x^4 + y^4 = z^2$ has a solution x_1, y_1, z_1 nonzero integers. Without loss of generality, we may assume $x_1, y_1, z_1 > 0$ and $(x_1, y_1) = 1$. We will show that there is another solution x_2, y_2, z_2 positive integers such that $(x_2, y_2) = 1$ and $0 < z_2 < z_1$. Now, $(x_1)^2, (y_1)^2, z_1$ is a Pythagorean triple with $(x_1^2, y_1^2, z_1) = 1$, and without loss of generality, y_1^2 is even. Thus, by Theorem 6.3 says that there exists $m, n \in \mathbb{Z}$ such that $(m, n) = 1, m > n > 0$, and exactly one of m and n is even such that $x_1^2 = m^2 - n^2, y_1^2 = 2mn, z_1 = m^2 + n^2$. Now, $x_1^2 = m^2 - n^2$ implies $x_1^2 + n^2 = m^2$ and x_1, m, n is a Pythagorean triple with $(x_1, m, n) = 1$ and n is even.

Applying the Theorem 6.3 again, we get that there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1, a > b > 0$, exactly one of a and b is even, with $x_1 = a^2 - b^2, n = 2ab, m = a^2 + b^2$.

We want to show that m, a and b are perfect squares. Now, $y_1^2 = 2mn = m(2n)$ and $(m, 2n) = 1$, we have that

Select All Correct Answers:

(a) m ✓

(b) n

(c) 2n ✓

are perfect squares. Thus, there exists $c \in \mathbb{Z}$ such that $2n = 4c^2$ or, equivalently, $n = 2c^2$. Now, $n = 2ab$ and $(a, b) = 1$, we have that

Select All Correct Answers:

(a) a ✓

(b) b ✓

(c) 2b

are perfect squares.

There exists x_2, y_2, z_2 such that

Multiple Choice:

(a) $m = x_2^2$

(b) $m = y_2^2$

(c) $m = z_2^2$ ✓

Multiple Choice:

(a) $a = x_2^2$ ✓

(b) $a = y_2^2$

(c) $a = z_2^2$

and

Multiple Choice:

(a) $b = x_2^2$

(b) $b = y_2^2$ ✓

(c) $b = z_2^2$.

There exists x_2, y_2, z_2 such that $m = z_2^2$, $a = x_2^2$ and $b = y_2^2$.

Without loss of generality, we may assume $x_2, y_2, z_2 > 0$. Then $m^2 = a^2 + b^2$ implies $z_2^2 = x_2^4 + y_2^4$, so that x_2, y_2, z_2 is a solution with positive integers to $x^4 + y^4 = z^2$. Also $(x_2, y_2) = 1$ and $0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1$.

Thus, we have constructed another solution as desired. That is, we assumed the existence of a solution to $x^4 + y^4 = z^2$ in the positive integers, we can construct another solution with a strictly smaller value of z. This is a contradiction since there are only finitely many positive integers between a given positive integer and zero. So $x^4 + y^4 = z^2$ has no solutions on nonzero x, y, z. ■

Part II

Appendix

A Other Results from Strayer and Homework Assignments

Most of these results are covered in the readings from Elementary Number Theory *by James K. Strayer in Spring 2024, and referenced in these notes. Additionally, some results were proved on homework assignments and not listed in other places in the notes. All of the results in this section are standard elementary number theory and presented without proof.*

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

0.1 Divisibility facts

Lemma 15 (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 27 (Proposition 1.10)**.** Let $a, b \in \mathbb{Z}$ with $(a, b) = d$. Then $(\frac{a}{d}, \frac{b}{d}) = 1$.

Lemma 16 (Lemma 1.12)**.** If $a, b \in \mathbb{Z}$, $a \geq b > 0$, and $a = bq + r$ with $q, r \in |Z$, then $(a, b) = (b, r)$.

Proposition 28 (Homework 3, Problem 4)**.** Let $a_1, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$ and let $d = (a_1, \ldots, a_n)$. Then $c \in \mathbb{Z}$ is a common divisor of $a_1, \ldots, a_n$ if and only if $c \mid d$.

0.2 Prime facts

Lemma 17 (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 10 (Corollary 1.15)**.** Let $a_1, a_2, \ldots, a_n, p \in \mathbb{Z}$ with p prime. If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

Proposition 29 (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 $p_1, p_2, \ldots, p_n$ are distinct primes and $a_1, a_2 \cdots, a_n, b_1, b_2, \cdots, b_n$ 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 39 (Theorem 1.19)**.** Let $a, b \in \mathbb{Z}$ with $a, b > 0$. Then $(a, b)[a, b] = ab$.

0.3 Congruences

Proposition 30 (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 18 (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 $c > 0$.

Proposition 31 (Homework 4, Problem 9)**.** Let p be prime, then $ax \equiv 0 \pmod{p}$ implies $a \equiv 0 \pmod{p}$ or $x \equiv 0 \pmod{p}$.

Furthermore, for a composite integer m, $ax \equiv 0 \pmod{m}$ does *not* imply either $a \equiv 0 \pmod{m}$ or $x \equiv 0 \pmod{m}$.

Corollary 11 (Corollary 2.15)**.** Let p be a prime number and let $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.

0.4 The Euler Phi-Function

Theorem 40 (Theorem 3.3)**.** Let p be prime and let $a \in \mathbb{Z}$ with $a > 0$. Then $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

B In Class Assignments

This section contains worksheet versions of the in class assignments from Spring 2024 and is only included with instructornotes.

Most of these problems can also be found throughout the course notes, often with less scaffolding. Since the Davidson College Number Theory course can serve as an introduction to proofs, many of the worksheets focus on proof solving skills, including using other proofs as a model, fill-in-the-blank reminders to justify reasoning, and examples of multiple proof methods for the same statement.

Since I anticipate these files would be highly modified by anyone teaching the course, I have also included references to *Elementary Number Theory* by James K. Strayer throughout the worksheets.

In-class Problem 1 Prove

Theorem 1 (Ernst, Theorem 2.2). If n is an even integer, then n^2 is even.

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.

In-class Problem 2 Prove

Theorem 2 (Strayer, Proposition 1.2). Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.

Use the proofs of the following propositions as a guide.

Proposition 1. Let $a, b \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

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 $a \mid c$. ■

Proposition 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. ■

In-class Problem 1 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 $a \nmid c$.

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

In-class Problem 3 Prove that our two definitions of even are equivalent using the following outline:

Proposition 3. Let $n \in \mathbb{Z}$. Then there is some $k \in \mathbb{Z}$ such that $n = 2k$ if and only if $2 \mid n$.

Proof ($\Rightarrow$) Let $n \in \mathbb{Z}$. Assume that there is some $k \in \mathbb{Z}$ such that $n = 2k$. Thus, $2 \mid n$

Free Response: by definition of divides.

($\Leftarrow$) Let $n \in \mathbb{Z}$. Assume that $2 \mid n$. Then, there is some $k \in \mathbb{Z}$ such that $n = 2k$

Free Response: by definition of divides.

■

In-class Problem 4 Prove that our two definitions of odd are equivalent using the following outline:

Proposition 4. Let $n \in \mathbb{Z}$. Then there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$ if and only if $2 \nmid k$.

Proof ($\Rightarrow$) Let $n \in \mathbb{Z}$. Assume that there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$. Then

Free Response: by the division algorithm, there exists unique $q, r \in \mathbb{Z}$ such that $n = 2q + r$ and $0 \leq r < 2$.

Thus, $2 \nmid k$.

($\Leftarrow$) Let $n \in \mathbb{Z}$. Assume that $2 \nmid k$. Then

Free Response: by the division algorithm, there exists unique $q, r \in \mathbb{Z}$ such that $n = 2q + r$ and $0 < r < 2$. Thus, $r = 1.1$

Thus, there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$. ■

MAT-255– Number Theory Spring 2024 In Class Work January 22

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Use the division algorithm on $a = 47, b = 6$ and $a = 281, b = 13$.

Solution: When $a = 47, b = 6$, we have $q = 7$, and $r = 5$ since

$$47 = 6(7) + 5 \quad \textit{and} \quad 0 \leq 5 < 6.$$

When $a = 281, b = 13$, we have $q = 21$, and $r = 8$ since

$$47 = 13(21) + 8 \quad \textit{and} \quad 0 \leq 8 < 13.$$

In-class Problem 2 Let a and b be nonzero integers. Prove that there exists a unique $q, r \in \mathbb{Z}$ such that

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

(a) Use the 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 $a = p|b| + s$ and $0 \leq s < |b|$.

(ii) There are two cases:

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

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

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

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

Hint: *The TEXcode for the floor function is* `\lfloor ... \rfloor`

as in the proof of the division algorithm.

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

(ii) Summarizing these statements, rewrite q, r in terms of a and b, as in the original proof of the division algorithm.

(iii) Now use your scratch work and follow the outline of the proof of the division algorithm to provide a new proof *without referencing the division algorithm.*

MAT-255– Number Theory Spring 2024 In Class Work January 24

Your Name: _____ Group Members: _____ _____

In-class Problem 1 (Chapter 1, Exercise 29) 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 $k \in \mathbb{Z}$.

Hint: *Try showing the statement is true for all odd integers greater than* 1.

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 2 (Chapter 1, Exercise 33) Prove or disprove the following conjecture, which is similar to the Twin Prime Conjecture:

Conjecture 3. There are infinitely many prime number p for which $p + 2$ and $p + 4$ are also prime numbers.

Hint: *Show that the only prime where $p + 2$ and $p + 4$ are also prime is $p = 3$.*

In-class Problem 3 Without looking up the proof, prove Proposition 1.10: Let $a, b \in \mathbb{Z}$ with $(a, b) = d$. Then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

MAT-255– Number Theory Spring 2024 In Class Work January 26

Your Name: _____ Group Members:_____ _____

Use the first principle of mathematical induction to prove each statement.

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

Proof We proceed by induction. The base case is $n = 1$. Since $3 \mid 4^1 - 1$, we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then $3 \mid 4^k - 1$. We want to show that $3 \mid 4^{k+1} - 1$.

Free Response: Then by the definition of divides, there exists m such that $3m = 4^k - 1$. Rewriting this equation, we get $3m + 1 = 4^k$. Multiplying both sides by 4 gives $4(3m) + 4 = 4^{k+1}$, or $3(4m + 1) = 4^{k+1} - 1$. Therefore, $3 \mid 4^{k+1} - 1$.

■

In-class Problem 2 (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 $\dfrac{n^2 - n}{2}$.

Proof We proceed by induction. The base case is $n = 1$. Since

Free Response: There are $6\dfrac{1^2 - 1}{2} = 0$ line segments connecting the only point

we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then

Free Response: there are $\dfrac{k^2 - k}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k$ arranged on a circle.

We want to show that

Free Response: there are $\dfrac{(k+1)^2 - (k+1)}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k, p_{k+1}$ arranged on a circle.

Free Response: Adding a $k+1^{st}$ point adds an additional k pairs of points. Then there are $\dfrac{k^2 - k}{2} + k = \dfrac{k^2 + k}{2} = \dfrac{(k+1)^2 - (k+1)}{2}$ line segments joining all pairs of distinct points $p_1, p_2, \ldots, p_k, p_{k+1}$ arranged on a circle.

■

In-class Problem 3 If n is a positive integer, then

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

Proof We proceed by induction. The base case is $n = 1$. Since $1^3 = \dfrac{1^2(1+1)^2}{4}$, we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then

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

We want to show that

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

Free Response:

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

■

In-class Problem 4 If n is an integer with $n \geq 5$, then

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

Proof We proceed by induction. The base case is $n = 5$. Since $2^5 > 5^2$, we are done.

The induction hypothesis is that if $k \geq 5$ and $n = k$, then $2^k > k^2$. We want to show that $2^{k+1} > (k+1)^2$.

Free Response: Multiplying both sides by k gives $k2^k > 2^{k+1} > k^2$.

■

Recall the notation $\gcd(a, b) = (a, b)$.

In-class Problem 5 Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $a_1 \neq 0$. Prove that

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

Hint: *Try solving the $k = 3$ case as part of your scratch work.*

Proof We proceed by induction. The base case is $n = 2$, since the statement we are trying to prove requires at least two inputs. Since

$$(a_1, a_2) = ((a_1, a_2))$$

we are done.

The induction hypothesis is that if $k \geq 2$ and $n = k$, then

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

We want to prove that

$$(a_1, a_2, \ldots, a_{k+1}) = ((a_1, a_2, a_k), a_{k+1})$$

Free Response: Let $d_k = (a_1, a_2, a_3, \ldots, a_k)$, $e = ((a_1, a_2, a_3, \ldots, a_k), a_{k+1}) = (d_k, a_{k+1})$, 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 $(a_1, \ldots, a_k) = ((a_1, a_2, a_3, \ldots, a_{k-1}), a_k) = (d_{k-1}, a_k)$ by the induction hypothesis, $e \mid d_{k-1}$ and $e \mid a_k$ by defintion of (d_{k-1}, a_k). Again, by the induction hypothesis, $d_{k-1} = (a_1, a_2, a_3, \ldots, a_{k-1}) = ((a_1, a_2, a_3, \ldots, a_{k-2}), a_{k-1}) = (d_{k-2}, a_{k-1})$, so $e \mid a_{k-1}$ and $e \mid d_{k-2}$ by defintion of (d_{k-2}, a_{k-1}). 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 definition of $((a_1, a_2), a_3)$. Thus $e \mid a_1, a_2, \ldots, a_{k+1}$ by repeated applications of the induction hypothesis and the definition of greatest common divisor. By Problem 4 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 $f \mid d_k$ by Problem 4 on Homework 3. Since $e = (d_k, a_k)$, we have that $f \mid e$ by Problem 4 on Homework 3.

■

In-class Problem 6 Redo the following proofs using induction:

In-class Problem 7 Let $n \in \mathbb{Z}$. Prove that $3 \mid n^3 - n$.

Proof We proceed by induction. The base case is $n = 1$. Since $3 \mid 1^3 - 1 = 3$, we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then $3 \mid k^3 - k$. We want to show that $3 \mid (k+1)^3 - (k+1)$.

Free Response: Since $3 \mid 3(k^2 + k)$ by the definition of divides, and $3 \mid k^3 - k$ by the induction hypothesis, $k^3 - k + 3(k^2 + k)$ by linear combination. Note that

$$\begin{aligned} k^3 - k + 3(k^2 + k) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= (k+1)^3 - (k+1). \end{aligned}$$

Thus, $3 \mid (k+1)^3 - (k+1)$.

■

In-class Problem 8 Let $n \in \mathbb{Z}$. Prove that $5 \mid n^5 - n$.

Proof We proceed by induction. The base case is $n = 1$. Since $5 \mid 1^5 - 1 = 0$, we are done.

The induction hypothesis is that if $k \geq 1$ and $n = k$, then $5 \mid k^5 - k$. We want to show that $5 \mid (k+1)^5 - (k+1)$.

Free Response: Since $5 \mid 5(k^4 + 2k^3 + 2k^2 + k)$ by the definition of divides, and $5 \mid k^5 - k$ by the induction hypothesis, $k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k)$ by linear combination. Note that

$$\begin{aligned} k^5 - k + 5(k^4 + 2k^3 + 2k^2 + k) &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\ &= (k+1)^5 - (k+1). \end{aligned}$$

Thus, $5 \mid (k+1)^5 - (k+1)$.

■

MAT-255– Number Theory Spring 2024 In Class Work January 31

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Find the greatest common divisors of the pairs of integers below and write the greatest common divisor as a linear combination of the integers.

(a) $(21, 28)$

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

Using the Euclidean Algorithm: $a = 28, b = 21$

$$\begin{array}{lll} 28 = 21(1) + 7 & q_1 = 1, r_1 = 7 & 7 = 21(1) + 28(-1) \\ 21 = 7(3) + 0 & q_2 = 3, r_2 = 0 & \end{array}$$

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

(b) $(32, 56)$

Solution: Using the Euclidean Algorithm: $a = 56, b = 32$

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

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

(c) $(0, 113)$

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

(d) $(78, 708)$

Solution: Using the Euclidean Algorithm: $a = 708, b = 78$

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

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

In-class Problem 2 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 $a = pj, b = p^2k$, and $p \nmid k, p \nmid k$. Then $ab = p^3jk$ and $a + b = pj + p^2k = p(j + pk)$. Thus, $(ab, p^4) = p^3$ and $(a + b, p^4) = p$.

MAT-255– Number Theory Spring 2024 In Class Work February 5

Your Name: _____ Group Members: _____ _____

In-class Problem 1 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

Free Response: Theorem 6.2.

Substituting into the original Diophantine equation gives $4y + 6x_3 = 6$, which has infinitely many solutions by

Free Response: 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

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

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

(d) By inspection, $x_1 = 1, x_2 = 2$ is a particular solution. Then by Theorem 6.2, the solutions have the form

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

The first row should not have reduced fractions. Then simplify your answer for the second row.

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

MAT-255– Number Theory Spring 2024 In Class Work February 7

Your Name: _____ Group Members:_____ _____

In-class Problem 1 (a) Do there exist integers x and y such that $x + y = 100$ and $(x, y) = 8$?

Solution: No. By linear combination, $(x, y) \mid x + y$. Since $8 \nmid 100$, there does not exist integers x and y such that $x + y = 100$ and $(x, y) = 8$

(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

Free Response: $x = 3n$ for some $n \in \mathbb{Z}$ where $29 \nmid n$.

Let $y = 87 - 3n$. Then $3 \mid y$ by *linear combination*. Then $(x, y) = 3$ since $29 \nmid n$. Thus, there are infinitely many $x, y \in \mathbb{Z}$

Free Response: where $x + y = 87$ and $(x, y) = 3$.

■

In-class Problem 2 (Strayer Chapter 1, Exercise 38) Let a and b be relatively prime integers. Prove that $(a + b, a - b)$ is either 1 or 2.

Hint: *From the back of Strayer: Let* $(a + b, a - b) = d$ *and note that* $d \mid (a + b) + (a - b)$ *and* $d \mid (a + b) - (a - b)$.

Hint: *Use Homework 3, Problem 2 which states* $(ca, cb) = |c|(a, b)$ *for all* $a, b \in \mathbb{Z}$, *not both* 0.

Solution: 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. Since $d \mid 2a$ and $d \mid 2b$, $d \mid (2a, 2b) = 2(a, b)$. Since $(a, b) = 1$ by assumption, $d \mid 2$. Thus, $d = 1, 2$.

MAT-255– Number Theory Spring 2024 In Class Work February 9

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Prove that

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

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

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

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

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

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

Since the relation is reflexive, symmetric, and transitive, it is an equivalence relation.

MAT-255– Number Theory Spring 2024 In Class Work February 14

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Find the addition and multiplication tables modulo $3, 4, 5, 6, 7, 8$ and 9.

Solution: **Modulo** 3

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

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

Modulo 4

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

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

Modulo 5

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

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

Modulo 6

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

*	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Modulo 7

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

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

Modulo 8

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

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

Modulo 9

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

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

MAT-255– Number Theory Spring 2024 In Class Work February 21

Your Name: _____ Group Members: _____ _____

In-class Problem 1 Let p be an odd prime. Use that $\left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{(p+1)/2} \pmod{p}$ to show

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

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

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

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

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

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

Your Name: _____ Group Members: _____ _____

In-class Problem 1 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 $q^{p-1} \equiv 1 \pmod{p}$ and $p^{q-1} \equiv 1 \pmod{q}$ by Fermat's Little Theorem, and $p^{q-1} \equiv 0 \pmod{p}$ and $p^{q-1} \equiv 0 \pmod{q}$ by *definition*.

Free Response: Thus, $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$ and $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$ by modular addition. Thus, $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ and this is the unique congruence class modulo pq by the Chinese Remainder Theorem.

■

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

(a) A number a is relatively prime to 20 if and only if a is relatively prime to 4 and 5. The first blank should be smaller than second blank for the automatic grading to work.

Hint: *The number in each blank should be relevant to what we are trying to show.*

(b) We can partition the positive integers less that or equal to 20 into

$$\begin{aligned} 1 \equiv 5 \equiv 9 \equiv 13 \equiv 17 \pmod 4 \\ 2 \equiv 6 \equiv 10 \equiv 14 \equiv 18 \pmod 4 \\ 3 \equiv 7 \equiv 11 \equiv 15 \equiv 19 \pmod 4 \\ 4 \equiv 8 \equiv 12 \equiv 16 \equiv 20 \pmod 4 \end{aligned}$$

For any b in the range $1, 2, 3, 4$, define s_b to be the number of integers a in the range $1, 2, \ldots, 20$ such that $a \equiv b \pmod 4$ and $\gcd(a, 20) = 1$. Thus, $s_1 = 4, s_2 = 0, s_3 = 4$, and $s_4 = 0$.

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

(c) $\phi(20) = s_1 + s_2 + s_3 + s_4$. Why?

Free Response: Every positive integers less that or equal to 20 is counted by exactly one s_b.

(d) We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b = \phi(5)$, This blank is asking for a function, not a number. and that when $(b, 4) > 1$, $s_b = 0$. To finish the "proof" we show that there are $\phi(4)$ integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) = \phi(4)\phi(5)$.

In-class Problem 3 Repeat the same proof for m and n where $(m, n) = 1$.

Solution: Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to m and n.

We can partition the positive integers less that or equal to mn into

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

For any b in the range $1, 2, 3, \ldots, m$, define s_b to be the number of integers a in the range $1, 2, \ldots, mn$ such that $a \equiv b \pmod m$ and $\gcd(a, mn) = 1$. Thus, when $(b, m) = 1$, $s_b = \phi(m)$ and when $(b, m) > 1$, $s_b = 0$.

Free Response: Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn) = s_1 + s_2 + \cdots + s_m$.

We have seen that $\phi(mn) = s_1 + s_2 + \cdots + s_m$, that when $(b, m) = 1$, $s_b = \phi(n)$, This blank is asking for a function, not a value. and that when $(b, m) > 1$, $s_b = 0$. Since there are $\phi(m)$ integers b where $(b, m) = 1$. Thus, we can say that $\phi(mn) = \phi(m)\phi(n)$.

MAT-255– Number Theory Spring 2024 In Class Work March 1

Your Name: _____ Group Members:_____ _____

In-class Problem 1 Repeat the proof from last class to prove

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

Proof Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to m and n.

We can partition the positive integers less that or equal to mn into

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

For any b in the range $1,2,3,\ldots,m$, define s_b to be the number of integers a in the range $1,2,\ldots,mn$ such that $a\equiv b \pmod{m}$ and $\gcd(a,mn)=1$. Thus, when $(b,m)=1$, $s_b=\phi(m)$ and when $(b,m)>1$, $s_b=0$.

Free Response: Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn)=s_1+s_2+\cdots+s_m$.

We have seen that $\phi(mn)=s_1+s_2+\cdots+s_m$, that when $(b,m)=1$, $s_b=\phi(n)$, This blank is asking for a function, not a value. and that when $(b,m)>1$, $s_b=0$. Since there are $\phi(m)$ integers b where $(b,m)=1$. Thus, we can say that $\phi(mn)=\phi(m)\phi(n)$. ■

In-class Problem 2 Complete the proof of Theorem 3.2 by proving

Proposition 1. If m,n, and i are positive integers with $(m,n)=(m,i)=1$, then the integers

$$i, m+i, 2m+i, \ldots, (n-1)m+i$$

form a complete system of residues modulo n.

MAT-255– Number Theory Spring 2024 In Class Work March 13

Your Name: _____ Group Members:_____ _____

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

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

In-class Problem 1 Use only the results through Proposition 5.3/Reading Lemma 10.3.5 (ie, not Proposition 5.4) to prove the primitive root version:

Proposition 2. Let $r, m \in \mathbb{Z}$ with $m > 0$ and r a primitive root modulo m. If i is a positive integer, then

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

Solution: Let r be a primitive root modulo m. Then by Proposition 5.3, $\{r, r^2, \ldots, r^{\phi(m)}\}$ is a complete residue system modulo m. By Proposition 5.1, $\operatorname{ord}_m(r^i) \mid \phi(m)$ and by Proposition 5.3, $r, r^2, \ldots, r^{\phi(m)}$ is a complete residue system modulo m

---

In-class Problem 2 Prove

Proposition 3 (Proposition 10.2.2). Let p be prime, and let m be a positive integer. Consider

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

(a) If $m \mid p - 1$, then there are exactly m incongruent solutions modulo p.

(b) For any positive integer m, there are $\gcd(m, p - 1)$ incongruent solutions modulo p.

Solution: Let p be prime, and let m be a positive integer. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$.

(a) If $m \mid p - 1$, then there exists $k \in \mathbb{Z}$ such that $mk = p - 1$. If $a^m \equiv 1 \pmod{p}$

In-class Problem 3 Prove the following statement, which is the converse of Reading 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.

Solution: Let p be prime, and let $a \in \mathbb{Z}$ such that every integer $b \in \mathbb{Z}$ where $p \nmid b$ is congruent to a^i modulo p for some positive integer i. Thus, $(a, p) = 1$, otherwise 1 would not be congruent to a power of a. ByProposition 5.2, $a^i \equiv a^j \pmod{p}$ if and only if $i \equiv j \pmod{p - 1}$. Thus, $a^1, a^2, \ldots, a^{p-1}$ are distinct congruence classes and only one of $a^1, a^2, \ldots, a^{p-1}$ is congruent to 1 modulo p. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $\operatorname{ord}_p a = p - 1$.

In-class Problem 4 Prove the following generalization of Reading Lemma 10.3.5

Lemma 1. Let $n \in \mathbb{Z}$ and let $x_1, x_2, \ldots, x_m$ be reduced residues modulo n. Suppose that for all $i \neq j$, $\operatorname{ord}_n(x_i)$ and $\operatorname{ord}_n(x_j)$ are relatively prime. Then

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

Your Name: _____

Lemma 1. Let $a, b \in \mathbb{Z}$, not both zero. Then any divisor of (a, b) is a common divisor of a and b.

Proposition 1 (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, $\text{ord}_m a \mid \phi(m)$.

Problems

In-class Problem 1 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 $a^d \equiv 1 \pmod{p}$.

Proof 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. 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 Lemmas 5 and 1 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 2 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 $d = (m, p-1)$. From Problem 1,

Free Response: $x^m \equiv 1 \pmod{p}$ if and only if $x^d \equiv 1 \pmod{p}$.

Now find a result that allows you to finish the proof in 1-2 sentences.

Free Response: By Proposition 5.8 there are exactly d solutions to $x^d \equiv 1 \pmod{p}$. Thus, there are exactly d solutions to $x^m \equiv 1 \pmod{p}$.

■

In-class Problem 3 Prove the following statement, which is the converse of Proposition 5.4 (for a prime):

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.

Solution: Let p be prime, and let $a \in \mathbb{Z}$ such that every integer $b \in \mathbb{Z}$ where $p \nmid b$ is congruent to a^i modulo p for some positive integer i. Thus, $(a, p) = 1$, otherwise 1 would not be congruent to a power of a. By Proposition 5.2, $a^i \equiv a^j \pmod{p}$ if and only if $i \equiv j \pmod{p-1}$. Thus, $a^1, a^2, \ldots, a^{p-1}$ are distinct congruence classes and only one of $a^1, a^2, \ldots, a^{p-1}$ is congruent to 1 modulo p. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $\text{ord}_p a = p-1$.

MAT-255– Number Theory Spring 2024 In Class Work March 27

Your Name: _____ Group Members: _____ _____

From class March 20:

Modulus	Quadratic residues	Quadratic nonresidues
2	1	None
3	1	2
5	1, 4	2, 3
7	1, 2, 4	3, 5, 6

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

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

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

Theorem 1 (Theorem 4.6)**.** Let p be an odd prime number. Then

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

Theorem 2 (Quadratic reciprocity)**.** 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 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

In-class Problem 1 (Strayer Chapter 4, Exercise 35) Let p be an odd prime number. Prove the following statements the following provided outlines, which will help solve the next problem, as well.

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

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

Proof (a) Since $3 \equiv 3 \pmod 4$,[4] we need two cases for Quadratic reciprocity.

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

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

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

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

(b) 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 $\left(\frac{-1}{p}\right) = 1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ by Quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. Then $p \equiv 1 \pmod{12}$, and this is the unique equivalence class modulo 12 by the Chinese Remainder Theorem.

(ii) If $p \equiv 3 \equiv -1 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ by Theorem 4.6 and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ by Quadratic reciprocity. Thus, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. Then $p \equiv 7 \pmod{12}$, 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 $p \equiv 1, 7 \pmod{12}$, which is equivalent to $p \equiv 1 \pmod 6$.

■

In-class Problem 2 (Strayer Chapter 4, Exercise 36) 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.

(a) 5

(b) -5

(c) 7

(d) -7

Proof (a) Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by Quadratic reciprocity. Then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$.

■

MAT-255– Number Theory Spring 2024 In Class Work April 1

Your Name: _____ Group Members: _____ _____

Results

Theorem 1 (Euler's Criterion)**.** Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

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

Theorem 2 (Theorem 4.6)**.** Let p be an odd prime number. Then

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

Theorem 3 (Quadratic reciprocity)**.** 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 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Lemma 1 (Gauss's Lemma)**.** Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Let n be the number of least positive residues of the integers $a, 2a, 3a, \ldots, \frac{p-1}{a}$ modulo p that are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Problems

We can combine these results to find the Legendre symbol many different ways.

In-class Problem 1 Use the following methods to find $\left(\frac{-6}{11}\right)$:

(a) Euler's Criterion, from March 22:

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

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

(b) Factor into $\left(\frac{-6}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$. From here, we will explore the various was to find $\left(\frac{2}{11}\right)$ and $\left(\frac{3}{11}\right)$.

(i) Find $\left(\frac{2}{11}\right)$ using the specified method:

- Using Euler's Criterion.

Solution: From Euler's Criterion,

$$\left(\frac{2}{11}\right) \equiv 2^{(11-1)/2} \equiv 32 \equiv -1 \pmod{11}.$$

- Using Gauss's Lemma.

  Solution: First, find the least nonnegative residues of $2, 2(2), 3(2), 4(2), 5(2)$ modulo 11. These are

  $$2, 4, 6, 8, 10,$$

  and $n = 3$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

  $$\left(\frac{2}{11}\right) = (-1)^3 = 3.$$

(ii) Find $\left(\frac{3}{11}\right)$ using the specified method:

- Using Euler's Criterion.

  Solution: From Euler's Criterion,

  $$\left(\frac{3}{11}\right) \equiv 3^{(11-1)/2} \equiv (-2)^2(3) \equiv 1 \pmod{11}.$$

- Using Quadratic reciprocity

  Solution: Since $11 \equiv 3 \pmod 4$, $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$.

- Using Gauss's Lemma.

  Solution: First, find the least nonnegative residues of $3, 2(3), 3(3), 4(3), 5(3)$ modulo 11. These are

  $$3, 6, 9, 1, 4$$

  and $n = 2$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

  $$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

Thus, $\left(\frac{-6}{11}\right) = 1$

(c) Use that $-6 \equiv 5 \pmod{11}$, so $\left(\frac{-6}{11}\right) = \left(\frac{5}{11}\right)$. Then find $\left(\frac{5}{11}\right)$ the specified method:

(i) Using Euler's Criterion.

Solution: From Euler's Criterion,

$$\left(\frac{5}{11}\right) \equiv 5^{(11-1)/2} \equiv (3)^2(5) \equiv 1 \pmod{11}.$$

(ii) Using Quadratic reciprocity

Solution: Since $5 \equiv 1 \pmod 4$, $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$.

(iii) Using Gauss's Lemma.

Solution: First, find the least nonnegative residues of $5, 2(5), 3(5), 4(5), 5(5)$ modulo 11. These are

$$5, 10, 4, 9, 2,$$

and $n = 2$ are greater than $\frac{11}{2}$. Thus, by Gauss's Lemma,

$$\left(\frac{5}{11}\right) = (-1)^2 = 1.$$

In-class Problem 2 Now we will examine the Legendre symbol of 2 using Gauss's Lemma. First, note that $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are already least nonnegative residues modulo p. It will be slightly easier to count how many are *less than* $\frac{p}{2}$, then subtract from the total number, $\frac{p-1}{2}$.

Let $k \in \mathbb{Z}$ with $1 \leq k \leq \frac{p-1}{2}$. Then $2k < \frac{p}{2}$ if and only if $k < \left\lfloor \frac{p}{4} \right\rfloor$. Thus, $\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$ of $2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$ are greater than $\frac{p}{2}$.

Hint: *The two blanks should be the same, and also go in the blanks below*

Now complete this table

p	$\left\lfloor \frac{p}{4} \right\rfloor$	$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$	$2, 2(2), 3(2), \ldots, 2(\frac{p-1}{2})$	$\left(\frac{2}{p}\right)$
3	0	1	Less than $\frac{3}{2}$: N/A Greater than $\frac{3}{2}$: 2	$(-1)^1 = -1$
5	1	1	Less than $\frac{5}{2}$: 2 Greater than $\frac{5}{2}$: 4	$(-1)^1 = -1$
7	1	2	Less than $\frac{7}{2}$: 2 Greater than $\frac{7}{2}$: 4, 6	$(-1)^2 = 1$
11	2	3	Less than $\frac{11}{2}$: 2, 4 Greater than $\frac{11}{2}$: 6, 8, 10	$(-1)^3 = -1$
13	3	3	Less than $\frac{13}{2}$: 2, 4, 6 Greater than $\frac{13}{2}$: 8, 10, 12	$(-1)^3 = -1$
17	4	4	Less than $\frac{17}{2}$: 2, 4, 6, 8 Greater than $\frac{17}{2}$: 10, 12, 14, 16	$(-1)^4 = 1$
19	4	5	Less than $\frac{19}{2}$: 2, 4, 6, 8 Greater than $\frac{17}{2}$: 10, 12, 14, 16, 18	$(-1)^5 = -1$
p	5	6	Less than $\frac{17}{2}$: 2, 4, 6, 8, 10 Greater than $\frac{17}{2}$: 12, 14, 16, 18, 20, 22	$(-1)^6 = 1$

MAT-255– Number Theory Spring 2024 In Class Work April 3

Your Name: _____ Group Members: _____ _____

Lemma 1. Let p be an odd prime number and like $a \in \mathbb{Z}$ with $p \nmid a$. Consider

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a, \frac{p+1}{2}a, \ldots, (p-1)a.$$

The least absolute residues of ak and $a(p-k)$ differ by a negative sign. In other words,

$$ak \equiv -a(p-k) \pmod{p}.$$

Furthermore, for each $k = 1, 2, \ldots, \frac{p-1}{2}$, the exactly one of k and $-k$ is a least absolute residue of $\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$.

In-class Problem 1 Check Lemma 1 for

(a) $a = 3, p = 7$

(b) $a = 5, p = 11$

(c) $a = 6, p = 11$

Solution: (a) $a = 3, p = 7$

$$\begin{aligned} 3 \pmod 7,\ 3(2) \equiv -1 \pmod 7,\ 3(3) \equiv 2 \pmod 7,\\ 3(4) \equiv -2 \pmod 7,\ 3(5) \equiv 1 \pmod 7,\ 3(6) \equiv -3 \pmod 7, \end{aligned}$$

(b) $a = 5, p = 11$

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

(c) $a = 11, p = 23$

$$\begin{aligned} 11 \pmod{23},\ 11(2) \equiv -1 \pmod{23},\ 11(3) \equiv 10 \pmod{23},\\ 11(4) \equiv -2 \pmod{23},\ 11(5) \equiv 9 \pmod{23},\ 11(6) \equiv -3 \pmod{23},\\ 11(7) \equiv 8 \pmod{23},\ 11(8) \equiv -4 \pmod{23},\ 11(9) \equiv 7 \pmod{23},\\ 11(10) \equiv -5 \pmod{23},\ 11(11) \equiv 6 \pmod{23},\\ 11(12) \equiv -6 \pmod{23},\ 11(13) \equiv 5 \pmod{23},\\ 11(14) \equiv -7 \pmod{23},\ 11(15) \equiv 4 \pmod{23},\ 11(16) \equiv -8 \pmod{23},\\ 11(17) \equiv 3 \pmod{23},\ 11(18) \equiv -9 \pmod{23},\ 11(19) \equiv 2 \pmod{23},\\ 11(20) \equiv -10 \pmod{23},\ 11(21) \equiv 1 \pmod{23},\ 11(22) \equiv -11 \pmod{23}, \end{aligned}$$

Access GeoGebra at https://www.geogebra.org/m/tuf7y6sh.

Two stills from the GeoGebra interactive are in Figure 3 and Figure 4.

Geogebra link: `https://www.geogebra.org/m/tuf7y6sh`

In-class Problem 1 The steps below outline the proof in the general case, when $p = 7$ and $q = 5$. This case is in Figure 3. Move the sliders to $p = 7$ and $q = 5$.

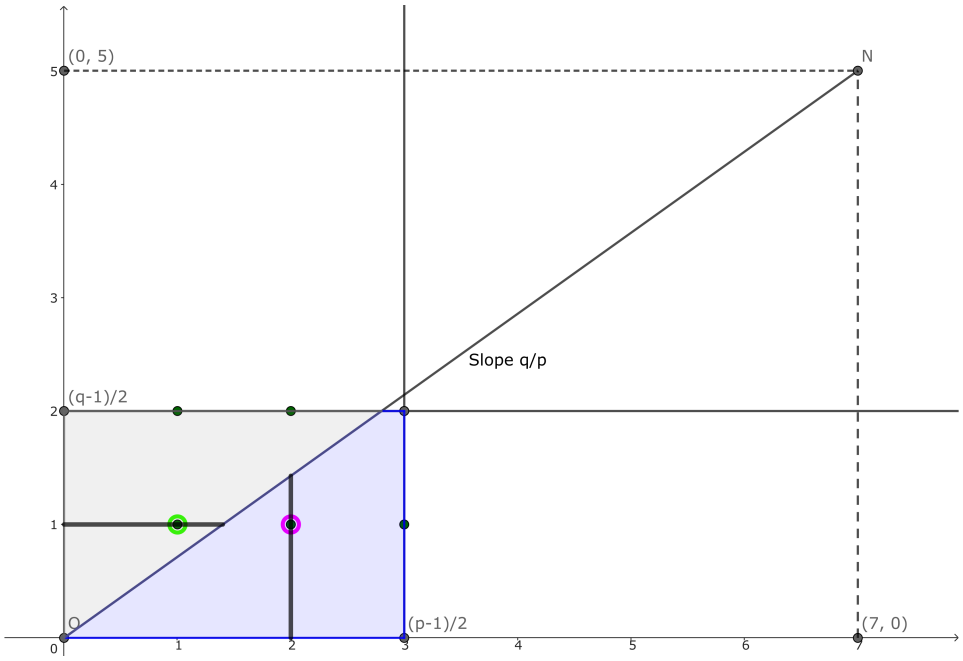


Figure 3: The lattice for the $p = 7, q = 5$ problem, with the $j = 1$ and $k = 2$ cases highlighted

(a) The line segment between the origin and $(7, 5)$ has slope $\frac{5}{7}$. Since $p = 7$ and $q = 5$ are distinct primes, there are no lattice points on line segment except the endpoints.

(b) First, we will count the number of points N_1 where $\frac{5-1}{2} \geq y > \frac{5}{7}x > 0$. This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines $j = 1, 2$. Let's just check the numbers we should get:

- When $j = 1$, there are 1 lattice points.
- When $j = 2$, there are 2 lattice points.

For each j, we are counting positive integers $x < \frac{7}{5}j$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$ ✓ .

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$.

Thus, the total number of lattice points in this triangle, N_1, is

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{7j}{5} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{2} \left\lfloor \frac{5j}{7} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{7j}{5} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{3} \left\lfloor \frac{5j}{7} \right\rfloor$

(c) Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number N_2.

The region is bounded by $0 < x \leq \frac{7-1}{2}$, $0 < y < \frac{5}{7}x$, and $y \leq \frac{5-1}{2}$. Now, the point A where $y = \frac{5}{7}x$ intersects $y = \frac{5-1}{2}$ is between two consecutive lattice points, with coordinates $x = 2, y = 2$ and $x = 3, y = 2$. Similarly, the point B where $y = \frac{5}{7}x$ intersects $x = \frac{7-1}{2}$ is between two consecutive lattice points, with coordinates $x = 3, y = 2$ and $x = 3, y = 3$. Thus, the only lattice point in the triangle A, B and $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$ is $\left(\frac{7-1}{2}, \frac{5-1}{2}\right)$. Therefore, there are also N_2 lattice points in the triangle with vertices $(0,0), \left(\frac{7-1}{2}, 0\right), \left(\frac{7-1}{2}, \frac{5-1}{2}\right)$.

(d) We use the same method as N_1 to find N_2. We will count how many lattice points on each vertical lines $k = 1, 2, 3$. Let's just check the numbers we should get:

- When $k = 1$, there are 0 lattice points.
- When $k = 2$, there are 1 lattice points.
- When $k = 3$, there are 2 lattice points.

For each k, we are counting positive integers $y < \frac{5}{7}k$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{7j}{5} \right\rfloor$.

(ii) $\left\lfloor \frac{5j}{7} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{7k}{5} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{2} \left\lfloor \frac{5k}{7} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{7k}{5} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{3} \left\lfloor \frac{5k}{7} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 = (3)(2)$.

In-class Problem 2 The steps below outline the proof in the general case, when $p = 23$ and $q = 13$. Move

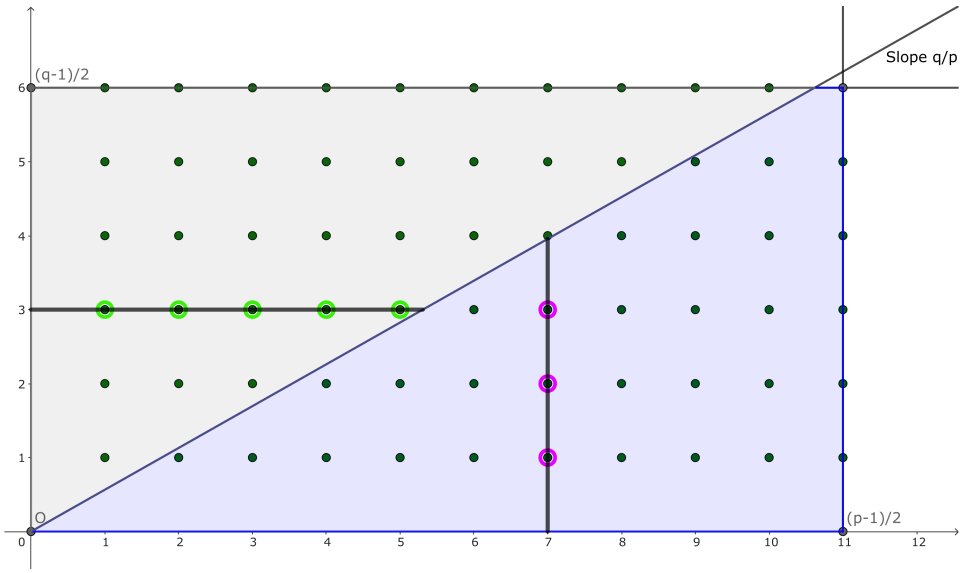


Figure 4: The lattice for the $p = 23, q = 13$, with the $j = 3$ and $k = 7$ cases highlighted

the sliders to $p = 23$ and $q = 13$.

(a) The line segment between the origin and $(23, 13)$ has slope $\frac{13}{23}$. Since $p = 23$ and $q = 13$ are distinct primes, there are no lattice points on line segment except the endpoints.

(b) First, we will count the number of points N_1 where $\frac{13-1}{2} \geq y > \frac{13}{23}x > 0$. This triangle is grey in the GeoGebra. We will count how many lattice points on each horizontal lines $j = 1, 2, \ldots, 6$. Let's just check one case, we should get:

- When $j = 3$, as in Figure 4, there are 5 lattice points.

For each j, we are counting positive integers $x < \frac{23}{13}j$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$ ✓ .

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$.

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{23j}{13} \right\rfloor$ ✓

(ii) $N_1 = \sum_{j=1}^{6} \left\lfloor \frac{13j}{23} \right\rfloor$

(iii) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{23j}{13} \right\rfloor$

(iv) $N_1 = \sum_{j=1}^{11} \left\lfloor \frac{13j}{23} \right\rfloor$

(c) Next we will count the rest of the lattice points in the rectangle, the blue region in the GeoGebra. We willl call this number N_2.

The region is bounded by $0 < x \leq \frac{23-1}{2}$, $0 < y < \frac{13}{23}x$, and $y \leq \frac{13-1}{2}$. Now, the point A where $y = \frac{13}{23}x$ intersects $y = \frac{13-1}{2}$ is between two consecutive lattice points, with coordinates $x = 10, y = 6$ and $x = 11, y = 6$. Similarly, the point B where $y = \frac{13}{23}x$ intersects $x = \frac{23-1}{2}$ is between two consecutive lattice points, with coordinates $x = 11, y = 6$ and $x = 11, y = 7$. Thus, the only lattice point in the triangle A, B and $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$ is $\left(\frac{23-1}{2}, \frac{13-1}{2}\right)$. Therefore, there are also N_2 lattice points in the triangle with vertices $(0,0), \left(\frac{23-1}{2}, 0\right), \left(\frac{23-1}{2}, \frac{13-1}{2}\right)$.

(d) We use the same method as N_1 to find N_2. We will count how many lattice points on each vertical lines $k = 1, 2, \ldots, 11$. Let's just check the numbers we should get:

- When $k = 7$, as in Figure 4, there are 3 lattice points.

For each k, we are counting positive integers $y < \frac{13}{23}k$. Which is,

Multiple Choice:

(i) $\left\lfloor \frac{23j}{13} \right\rfloor$.

(ii) $\left\lfloor \frac{13j}{23} \right\rfloor$ ✓ .

Thus, the total number of lattice points in this triangle is

Multiple Choice:

(i) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{23k}{13} \right\rfloor$

(ii) $N_2 = \sum_{k=1}^{6} \left\lfloor \frac{13k}{23} \right\rfloor$

(iii) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{23k}{13} \right\rfloor$

(iv) $N_2 = \sum_{k=1}^{11} \left\lfloor \frac{13k}{23} \right\rfloor$ ✓

Thus, the total number of lattice points is $N_1 + N_2 = (11)(6)$.

MAT-255– Number Theory Spring 2024 In Class Work April 17

Your Name: _____ Group Members: _____ _____

In-class Problem 1 (Chapter 6, Exercise 34) Prove that a positive integer can be written as the difference of two squares of integers if and only if it is not of the form $4n+2$ for some $n \in \mathbb{Z}$.

Proof ($\Rightarrow$) We will show that if a positive integer can be written as the difference of two squares of integers, then it is not of the form $4n+2$ for some $n \in \mathbb{Z}$.

Free Response:

($\Leftarrow$) We will show that any positive integer not of the form $4n+2$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers.

First, we will show that if a and b are positive integers that can be written as the difference of two squares of integers, then so can ab.

Free Response:

Now we will show that every odd prime can be written as the difference of two squares of integers. Let p be an odd prime. Then $p = x^2 - y^2 = (x-y)(x+y)$ when $x = \frac{p+1}{2}$ and $y = \frac{p-1}{2}$. Therefore every odd number can be written as the difference of two squares since

Free Response: every odd number is a product of odd primes, and we proved that the product of integers that can be written as the difference of two squares can also be written as the difference of two squares.

It remains to show that every positive integer of the form $4n$ for some $n \in \mathbb{Z}$ can be written as the difference of two squares of integers. Why is this the only remaining case?

Free Response: Every even integer has the form $4n$ or $4n + 2$.

Similar to the odd prime case, $4n = x^2 - y^2 = (x - y)(x + y)$ when $x = n + 1$ and $y = n - 1$.

■

Your Name: _____ Group Members:_____ _____

In-class Problem 1 (Chapter 6, Exercise 20) Let $x, y, z \in \mathbb{Z}$ and let p be a prime number.

(a) Prove that if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.

(b) Prove that if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.

Hint: *Recall Fermat's Little Theorem and its corrollaries.*

Solution: Let p be a prime number.

(a) Let $x, y, z \in \mathbb{Z}$ such that $x^{p-1} + y^{p-1} = z^{p-1}$.

By Fermat's Little Theorem, if $p \nmid x$, then $x^{p-1} \equiv 1 \pmod{p}$. If $p \mid x$, then $x^{p-1} \equiv 0 \pmod{p}$. Similarly for y and z. Thus,

$$x^{p-1} + y^{p-1} \equiv \begin{cases} 0+0 \pmod{p} \\ 0+1 \pmod{p} \\ 1+1 \pmod{p} \end{cases}$$

has a solution if andd only if p divides at least one of x, y. Thus, $p \mid xyz$.

(b) Let $x, y, z \in \mathbb{Z}$ such that $x^p + y^p = z^p$.

By Corollary 5.8, $x^p \equiv x \pmod{p}, y^p \equiv y \pmod{p}$, and $z^p \equiv z \pmod{p}$. Thus,

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{p} \\ x + y &\equiv z \pmod{p}. \end{aligned}$$

In otherwords, $p \mid (x + y - z)$.

C Final Projects

C.1 Instructions

Topics for final presentation in MAT-255 Number Theory, Spring 2024.

Attendance for each of the presentations is mandatory.

You may present individually or in pairs. Individual presentations should be 15-20 minutes and pair presentations should be 20-30 minutes. All presentations are on the whiteboard, although you may write on a tablet/slides if you check the technology ahead of time (and be prepared for it to not cooperate). You can have notes with you, and you may rely on them similar to how reliant I am on mine during lectures. But you should prepare this presentation enough that you aren't always directly copying your notes.

Submit your ranking of choices by the start of class on April 24. If you choose to work with a partner, only one person has to submit the rankings. I will send out the project assignments after class on Wednesday.

I encourage you to ask for help leading up to the presentation practice your presentation for time and accuracy, including presenting on the board.

Rubrics:

Content (20 points) Accuracy of proof, correct usage of terms, appropriate for the audience and within the scope of this class. The number of points per problem is on the individual topic assignments.

Organization (10 points) Overall information is presented in a logical sequence, including any necessary background information or examples without extraneous information.

Presentation (5 points) Well-prepared and well-rehearsed, spoken loud enough to hear easily, spoken and not read, good boardwork

Pacing (5 points) Slowing down and being more detailed in tougher to understand portions of the presentation, following the time guidelines, if presenting in a pair splitting time and content equally with your partner

Overall topic fluency (5 points) Able to answer 1-2 questions pertaining to presentation or clarification questions from classmates

Peer-feedback (5 points) Attends all presentations and fills out feedback and question forms

C.2 Fibonacci Sequence

Project on Fibonacci and Lucas sequence.

Exploration 1 *Start by reviewing the Fibonacci Sequence from Strayer Appendix A.2:* $F_1 = 1, F_2 = 1, F_{k+1} = F_k + F_{k-1}$ *for* $k \geq 3$.

Problem 1.1 *Prove that* $\lim_{k\to\infty} \frac{F_{k+1}}{F_k} = \phi$ *where* $\phi = \frac{1+\sqrt{5}}{2}$.

Rubric. 5 points if individual project, 3 points if presenting as a pair.

Problem 1.2 *Prove that for every positive integer* k,

$$F_1 + F_2 + \cdots + F_k = F_{k+2} - 1.$$

Rubric. 5 points if individual project, 3 points if presenting as a pair.

Problem 1.3 *(If presenting as a pair) Strayer Exercise Set A, Exercise 2.*

Rubric. 6 points.

The following problems are from *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by Erica Flapan, Tim Marks, and James Pommersheim, Chapter 2: Mathematical Induction, Section 2.3 The Fibonacci Sequence and the Golden Ratio [Flapan et al., 2010].

Exploration 2 *The following problems are from* Number Theory: A Lively Introduction with Proofs, Applications, and Stories *by Erica Flapan, Tim Marks, and James Pommersheim.*

The Lucas numbers are similar to the Fibonacci numbers, where $L_1 = 1, L_2 = 3, L_{k+1} = L_k + L_{k-1}$ *for* $k \geq 3$.

Problem 2.1 (a) *Make a table of the first* 12 *Lucas numbers.* You do not need to present this part

(b) *Use your results from part (a) to calculate the ratios of pairs of consecutive Lucas numbers.* You do not need to present this part

(c) *Make a conjecture about the value of* $\lim_{k\to\infty} \frac{L_{k+1}}{L_k}$. You do not need to present this part

(d) *Prove your conjecture is correct.* You **do** need to present this part

Rubric. 5 points if individual project, 3 points if presenting as a pair.

Problem 2.2 *(If presenting as a pair)*

(a) *Calculate* $L_1, L_1 + L_2, L_1 + L_2 + L_3, L_1 + L_2 + L_3 + L_4$. You do not need to present this part

(b) *Make a conjecture about the relationship between* $L_1 + L_2 + L_3 + \cdots + L_n$ *and the number* L_{n+2}. You do not need to present this part

(c) *Prove your conjecture is correct.* You **do** need to present this part

Rubric. 5 points if individual project, 3 points if presenting as a pair.

C.3 Geometry Pythagorean Triples

Project on geometry and Pythagorean Triples.

Definition 11. A *rational point* is a point (x, y) whose coordinates x and y are both rational numbers.

Use rational points on the unit circle and trigonometry to derive the formula for generating Pythagorean triples.

Problem 3.1 *Let (x, y) be a rational point on the unit circle. That is, there exists $a, b, c \in \mathbb{Z}$ such that $x = \frac{a}{c}$ and $y = \frac{b}{c}$.*

Explain why we can write x and y with the same denominator.

Rubric. 2 points.

Problem 3.2 *Let (x, y) be any point on the unit circle, ie $x^2 + y^2 = 1$. Consider the line segment between $(0, 0)$ and (x, y). As long as (x, y) is not $(-1, 0)$, the slope of this line is*

$$t = \frac{y}{1 + x} = \tan\theta$$

where θ is the angle between the line segment and the x-axis.

(a) *Show that*

$$x = \frac{1 - t^2}{1 + t^2}, y = \frac{2t}{1 + t^2}$$

either using algebra or trig identities.

(b) *Show that (x, y) is a rational point not equal to $(-1, 0)$*[5] *if and only if t is rational.*

(c) *Let $t = \frac{m}{n}$. Prove that if $x, y > 0$, then $m > n, (m, n) = 1$, exactly one of m, n is even, and all nontrivial Pythagorean triples have the form $a = k(m^2 - n^2), b = k(2mn), c = k(m^+n^2)$, for some $k \in \mathbb{Z}$.*

Hint: *Use that $k = \frac{c}{m^2 + n^2}$.*

Rubric. 4 points if individual, 3 if presenting as a pair.

Exploration 4 *The following problems are from* Number Theory: A Lively Introduction with Proofs, Applications, and Stories *by Erica Flapan, Tim Marks, and James Pommersheim Chapter 15, Some Nonlinear Diophantine Equations,15.5 A Geometric look at the Equation $x^4 + y^4 = z^2$ [Flapan et al., 2010].*

Theorem 1 (Fermat's Right Triangle Theorem)**.** The does not exist a right triangle with rational side lengths and area a perfect square.

Problem 4.1 *Let x, y, z be positive integers be the side lengths of a triangle with hypotenuse z and the area of the triangle is a perfect square. Prove that if z is the smallest such integer, then (x, y, z) is a primitive Pythagorean triple.*

Rubric. 4 points if individual, 3 if presenting as a pair.

[5] $x = -1$ and $y = 0$ is the limit as $t \to \infty$

Problem 4.2 *Let x, y, z as in the previous problem. Then there exists $m, n \in \mathbb{Z}$ with $m > n > 0, (m, n) = 1$ and exactly one of m and n even such that $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$. Furthermore, m, n, $m + n$ and $m - n$ are perfect squares.*

(a) *Prove that if $c, d \in \mathbb{Z}$ such that $c^2 = m + n$, and $d^2 = m - n$, then exactly one of $c + d$ and $c - d$ is divisible by 4.*

(b) *If $4 \mid c + d$, prove that $\frac{b^2}{4} = \frac{c+d}{4}\frac{c-d}{2}$, where the two factors on the right side of the equation are relatively prime.*

(c) *Show that there exists $s, t \in \mathbb{Z}$ such that $\frac{c+d}{4} = s^2$ and $\frac{c-d}{2} = t^2$*

(d) *Show that $(2s^2, t^2, a)$ is a Pythagorean triple and finish the proof of the right triangle theorem for this case.*

(e) *Repeat parts (b)-(d) for $4 \mid c - d$.*

Rubric. Part (a) 4 points if individual, 3 if presenting as a pair. Parts (b)-(d) 3 points per case if individual, 2 points per case if presenting as a pair.

Problem total: 10 points if individual, 7 points if pair.

Exploration 5 *(If presenting as a pair)*

Definition 12. A positive integer n is a *congruent number* if there exists a right triangle whose sides are all rational numbers and whose area is n.

Problem 5.1 *Show that the following are congruent numbers:*

- 6.
- 5.

Rubric. 2 points.

Problem 5.2 *Prove that there is no right triangle with* integer *sides whose area is* 5. *There is no right triangle with* integer *sides whose area is* 1.

Rubric. 3 points.

C.4 Gaussian Integers

Project on Gaussian Integers.

The following problems are from *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by Erica Flapan, Tim Marks, and James Pommersheim Chapter 13, Gaussian Integers.

Read the scanned notes on Moodle. Present as much as necessarily for classmates to follow.

Rubric. Present as much as necessarily for classmates to follow: 4 points if individual, 3 points if pair.

Exploration 6 *Here I will use slightly more standard notation, which will match iwth the $\mathbb{Z}[\sqrt{d}]$ topic and complex analysis.*

Definition 13. The set of *Gaussian integers*, denoted $\mathbb{Z}[i]$ (read "$\mathbb{Z}$ adjoin i") is defined by

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

where $i^2 = -1$.

Let $z = a + bi$ be a Gaussian integer. The *complex conjugate of* z is $\overline{z} = a - bi$. Define the *norm of* z, as

$$N(z) = |z| = z\overline{z} = (a + bi)(a - bi) = a^2 + b^2.$$

Lemma (Lemma 13.1.4)**.** Let r and s be Gaussian integers. Then

$$N(rs) = N(r)N(s).$$

Problem 6.1 *Prove Lemma 13.1.4*

Rubric. 4 points if individual, 3 points if pair.

Problem 6.2 *Let d and z be Gaussian integers.*

(a) *Prove that if $d \mid z$, then $|d| \mid |z|$.*

(b) *Prove or provide a counterexample for if $|d| \mid |z|$, then $d \mid z$.*

Rubric. 4 points if individual, 3 points if pair.

Definition 14. Let $p \in \mathbb{Z}[i]$ such that p is not a unit. We say p is *prime* if for every $a, b \in \mathbb{Z}[i]$, $p = ab$ implies that a is a unit or b is a unit.

Lemma (Lemma 13.2.6)**.** Let z be a Gaussian integer. If $N(z)$ is a prime in the (regular) integers, then z is a prime as a Gaussian integer.

Problem 6.3 *Prove Lemma 13.2.6.*

Rubric. 4 points if individual, 3 points if pair.

Definition 15. Let $a, d \in \mathbb{Z}[i]$. We say a and b are *relatively prime* if for all $d \in \mathbb{Z}[i]$, $d \mid a$ and $d \mid b$ implies that d is a unit.

Theorem 2 (Division Theorem for Gaussian Integers)**.** Let $a, d \in \mathbb{Z}[i]$ with $b \neq 0$. Then there exist Gaussian integers q and r such that $a = qb + r$ with $N(r) < N(b)$

Problem 6.4 *(If presenting as a pair) Prove Division Theorem for Gaussian Integers using Exercises 15-17 in the scanned notes.*

Rubric. 5 points.

Theorem 3 (Theorem 13.5.4)**.** Suppose $p \in \mathbb{Z}$ is prime. Then p is a prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$.

Theorem 4 (Theorem 13.5.5)**.** Let $z \in \mathbb{Z}[i]$. Then z is a prime Gaussian integer if and only if one of the following conditions holds:

- $N(z) = 2$,
- $N(z)$ is a prime integer congruent to 1 modulo 4,
- z is a unit times a prime integer congruent to 3 modulo 4.

Problem 6.5 *Prove Theorem 13.5.5*

Rubric. 4 points if individual, 3 points if pair.

C.5 Other number systems: $\mathbb{Z}[\sqrt{d}]$

Project on $\mathbb{Z}[\sqrt{d}]$.

Definition 16. Let $d \in \mathbb{Z}$ such that d is not a perfect square. Define $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$, pronounced "$Z$ adjoin square-root d" If $d < 0$, then $\mathbb{Z}[\sqrt{d}]$ is a set of complex numbers. We will use the regular definition of addition and multiplication.

Definition 17. Let $d \in \mathbb{Z}$ such that d is not a perfect square, and let $z \in \mathbb{Z}[\sqrt{d}]$ where $z = a + b\sqrt{d}$. The *conjugate of* z is $\overline{z} = a - b\sqrt{d}$, and the *norm of* z is $|z| = z\overline{z} = a^2 - db^2$.

Strayer uses the notation z' for the conjugate.

Exploration 7 Problem 7.1 *Strayer Chapter 1, Exercise 77 explores the case* $d = -10$. *Then* $\mathbb{Z}[\sqrt{d}]$ *is not have unique factorization. Do this problem.*

Rubric. Parts (a) and (b): 3 points each if individual, 2 points each if pair. Part (c): 2 points.

Problem total: 8 points if individual, 6 points if pair.

Problem 7.2 *If* $x, y \in \mathbb{Z}[\sqrt{d}]$, *prove that* $|xy| = |x||y|$. *If* $\dfrac{x}{y} \in \mathbb{Z}[\sqrt{d}]$, *prove that* $\left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$.

Rubric. 2 points.

Problem 7.3 *(If presenting as a pair)*

(a) *Prove that the norm of any nonzero element (ie,* $a \neq 0$ *or* $b \neq 0$ *of* $\mathbb{Z}[\sqrt{-5}]$ *is positive.*

(b) *When, if ever, does* $|a + b\sqrt{-5}| = 1$*?*

(c) *When, if ever, does* $|a + b\sqrt{-5}| = 13$*?*

Rubric. 4 points.

Problem 7.4 *Strayer Chapter 8, Student Project 6.*

Rubric. Part (a): 2 points. Parts (b) and (c): 4 points each if individual, 3 points each if pair.

Problem total: 10 points if individual, 8 points if pair.

C.6 Farey Fractions

Project on Farey Fractions.

The following problems are based on *The Theory of Number* by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery [Niven et al., 1991].

The subject of *Diophantine Approximation* concerns approximating real numbers with rational numbers. One way to do this is with *Farey fractions*–which we can generate by adding "wrong." However, there is a much simpler way to generate Farey fractions. One goal is to show these two methods give the same sequences.

Exploration 8

Definition 18. The N^{th} *Farey sequence* is the list of all fractions, written from smallest to largest, between 0 and 1 where the denominator is less than or equal to N when written as a reduced fraction. We write this sequence as $\mathcal{F}_N$.

The first three Farey sequences are:

$$\mathcal{F}_1 = \left\{\frac{0}{1}, \frac{1}{1}\right\},$$
$$\mathcal{F}_2 = \left\{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\right\},$$
$$\mathcal{F}_3 = \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\}$$

Problem 8.1 *Prove that for a positive integer $N \geq 2$, the number of elements of $\mathcal{F}_N$ with denominator N is equal to $\phi(N)$.*

Rubric. 5 points if individual, 4 points if pair.

Exploration 9 *Another way to generate the Farey sequence is using a table. In the first row, write $\frac{0}{1}$ and $\frac{1}{1}$.*

To form the second row, copy the first row. Then insert $\frac{0+1}{1+1}$ between $\frac{0}{1}$ and $\frac{1}{1}$.

To form the n^{th} row, copy the $(n-1)^{st}$ row. Then for each $\frac{a}{b}, \frac{c}{d}$ in the $(n-1)$ row, if $b+d \leq n$, insert $\frac{a+c}{b+d}$ between $\frac{a}{b}$ and $\frac{c}{d}$.

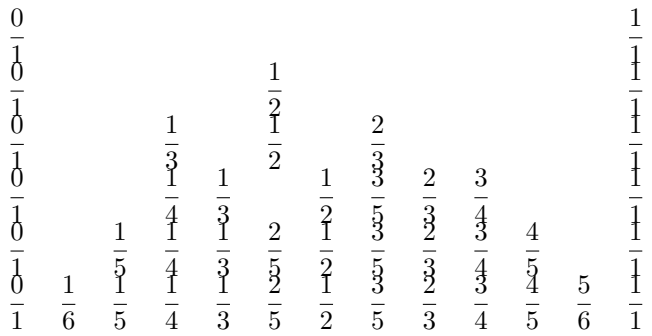
Lemma 1 (Niven-Zukerman-Montgomery, Theorem 6.1)**.** If $\frac{a}{b}$ and $\frac{c}{d}$ are consecutive fractions in the n^{th} row of the table, with $\frac{a}{b}$ to the left of $\frac{c}{d}$, then $bc - ad = 1$.

This lemma matches with the definition of a Farey pair *from Strayer Chapter 7, Student Project 2.*

Problem 9.1 *Prove this lemma.*

Rubric. 5 points if individual, 4 points if pair.

Problem 9.2 *(If presenting as a pair) Strayer Chapter 7, Student Project 2.*



Rubric. Parts (a)-(c): 4 points. Part (d): 4 points.

Problem 9.3 *(If presenting as an individual) Prove*

Corollary 12 (Niven-Zukerman-Montgomery, Corollary 6.2)**.** Every $\frac{a}{b}$ in the table is in reduced form.

Corollary 13 (Niven-Zukerman-Montgomery, Corollary 6.3)**.** The fractions in each row are listed in order from smallest to largest.

Rubric. 5 points.

Problem 9.4 *Prove that if* $0 \leq m \leq n$ *and* $(m, n) = 1$*, then fraction* $\frac{m}{n}$ *is in the* n^{th} *row of the table. Therefore, algorithmic definition of the* n^{th} *Farey sequence equivalent to the definition: The* N^{th} Farey sequence *is the list of all fractions, written from smallest to largest, between* 0 *and* 1 *where the denominator is less than or equal to* N *when written as a reduced fraction.*

Rubric. 5 points if individual, 4 points if pair.

C.7 Decimal expansions

Project on decimal expansions.

In this project, you will classify decimal (and duadecimal) expansions are finite, periodic, or aperiodic.

Read Strayer Section 7.1.

Rubric. Introducing topic, definitions, and any necessary results: 4 points

Exploration 10 *We say that the decimal expansion of a real number is* finite *if it terminates after a finite number of digits. If the pattern of digits eventually repeats, such as* $\frac{1}{3} = 0.33333\cdots = 0.\overline{3}$ *or* $\frac{1}{28} = 0.03571428571428\cdots = 0.03\overline{571428}$*, we say the decimal is* periodic*. We could also say that finite decimal expansions are periodic, where the periodic part is* $\overline{0}$*. Otherwise, we say the decimal is* aperiodic*.*

Problem 10.1 (a) *Find the decimal expansions of* $\frac{3}{2}, \frac{2}{3}, \frac{7}{25}, \frac{2}{7}, \frac{3}{20}, \frac{2}{15}$ *using WolframAlpha or another resource or method that will tell you if the decimal is periodic. These particular examples should be fine with a regular calculator.* You do not need to present these answers, they are to help with the next part.

(b) *Complete and prove the statement:*

Conjecture 4. Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and $(a, b) = 1$. Then $\frac{a}{b}$ has a finite decimal expansion if and only if b has no prime factors other than $2, 5$.

Rubric. 4 points if individual, 3 points if pair.

Problem 10.2 *Prove that if a real number has terminating decimal expansion, then it must be rational. Prove that if a real number has a periodic decimal expansion, then it must be rational.*

Hint: *Generalize the idea in Example 4 and the proof of Proposition 7.4.*

Rubric. 6 points if individual, 4 points if pair.

Exploration 11

Definition 19. Let $x \in \mathbb{R}$ with $0 < x < 1$. Then the *base 12* expansion of x is

$$\sum_{n=1}^{\infty} \frac{d_n}{12^n} = 0.d_1 d_2 \ldots, \quad d_i \in \{1, 2, \ldots, 11, 12\}.$$

If there exist a positive integer r and N such that $d_n = d_{n+r}$ for all $n \geq N$, then x is *periodic* and $d_N d_{N+1} \ldots d_{N+r}$ is the periodic part of the base 12 expansion. The base 12 expansion of x is finite if the periodic part is 0.

If m is a positive integer, then the base 12 expansion of m is

$$\sum_{k=1}^{n} a_k 12^k, \quad a_i \in \{1, 2, \ldots, 11, 12\}.$$

Combining these definitions gives the base 12 expansion of any positive real number (the only reason to separate the definitions is dealing with the indices of the summation)

Example 26. (a) To find the base 12 expansion of $\frac{3}{2}$, first write $\frac{3}{2} = 1 + \frac{1}{2}$. Since $1 \in \{1, 2, \ldots, 12\}$ the base 12 expansion of 1 is still 1. Then we find the base 12 expansion of $\frac{1}{2}$:

$$\frac{1}{2} = \frac{a_1}{12} + \frac{a_2}{12^2} + \cdots$$
$$6(1) = a_1 + \frac{a_2}{12} + \cdots$$

Then we can make $a_1 = 6$ and the rest of the $a_i = 0$. So the base 12 expansion of $\frac{3}{2}$ is 1.6

(b) To find the base 12 expansion of $\frac{1}{10}$,

$$\frac{1}{11} = \frac{a_1}{12} + \frac{a_2}{12^2} + \cdots$$
$$12\left(\frac{1}{11}\right) = a_1 + \frac{a_2}{12} + \cdots$$
$$1 + \frac{1}{11} = a_1 + \frac{a_2}{12} + \cdots$$

So $a_1 = 1$, and we are back to where we started, finding the base 12 expansion of $\frac{1}{11}$. Thus $\frac{1}{11} = 0.\overline{1}$.

(c) Often a is used to represent 10 and b is used to represent 11. The base 12 expansion of

$$\frac{10}{11} = b\frac{1}{11} = b\left(\frac{1}{12} + \frac{1}{12^2} + \cdots +\right) = 0.\overline{b}.$$

Problem 11.1 *Adjust the technique from Example 26 or check with WolframAlpha to find the base 12 expansions of the fractions from Problem 1.1(a). Present some of these in class: you do not need to present the work, only the expansion.*

Rubric. 2 points.

Problem 11.2 *Complete and prove the statement:*

Conjecture 5. Let $a, b \in \mathbb{Z}$ with $b \neq 0$ and $(a, b) = 1$. Then $\frac{a}{b}$ has a finite base 12 expansion if and only if b has no prime factors other than 2, 3.

Rubric. 4 points if individual, 3 points if pair.

Problem 11.3 *(If presenting as a pair) Prove that if a real number has terminating base 12 expansion, then it must be rational.*

Hint: *Generalize the idea in Example 4 and the proof of Proposition 7.4.*

Rubric. 4 points.

C.8 Circle of fifths

Project on frequency ratios for musical cords and continued fractions.

Read Strayer Sections 7.2 and 7.3, paying particular attention to the examples. I will use more standard notation than Strayer.

Exploration 12 *Give an introduction to continued fraction expansions, with enough detail for classmates to follow the presented problems.*

Rubric. Present as much as necessarily for classmates to follow: 4 points if individual, 3 points if pair.

Definition 20. Let x be a positive real number. Then the *continued fraction expansion of* x is

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}} = [a_0; a_1, a_2, \dots]$$

where $a_1, a_2, \dots$ are positive integers and a_0 is a nonnegative integer.

Define the *convergents of* x to be the sequence of $\dfrac{p_n}{q_n}$ where

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots + \cfrac{1}{a_n}}}}$$

Problem 12.1 *Use induction to show that* $p_n = a_n p_{n-1} + p_{n-2}, q_n = a_n q_{n-1} + q_{n-2}$.

Hint: *Consider* $\dfrac{1}{a_n + \dfrac{1}{a_{n+1}}}$ *and use* $a_n + \dfrac{1}{a_{n+1}}$ *in the induction step.*

Rubric. 4 points if individual, 3 points if pair.

Problem 12.2 *(If presenting as a pair) Chapter 7, Exercise 18*

Rubric. 3 points.

Exploration 13 *The following problems are from* Number Theory: A Lively Introduction with Proofs, Applications, and Stories *by Erica Flapan, Tim Marks, and James Pommersheim Chapter 14, Continued Fractions, Section 14.3 Approximating Irrational Numbers Using Continued Fractions [Flapan et al., 2010].*

Read the scanned notes on Moodle. Present as much as necessarily for classmates to follow.

Rubric. Present as much as necessarily for classmates to follow: 4 points if individual, 3 points if pair.

Problem 13.1 *An acoustically correct major third has frequency ratio* $5 : 4$

(a) *Show that there do not exist natural numbers m and n such that*

$$\left(\frac{5}{4}\right)^m = 2^n.$$

Thus, no number of acoustically correct major thirds that can make up a. whole number of octaves.

(b) *Find the first four convergents of* $\log_2\left(\frac{5}{4}\right)$

(c) *For each of your answer to part (b), find a pair of integers m and n for which* $\left(\frac{5}{4}\right)^m = 2^n$ *is approximately correct.*

(d) *In the equal-tempered scale, and octave consists of exactly 3 major thirds. To which convergent of* $\log_2\left(\frac{5}{4}\right)$ *does this correspond?*

Rubric. Each part: 2 points.

C.9 Jacobi Symbol

Project on the Jacobi Symbol, the composite analogue of the Legendre Symbol.

Exploration 14 Problem 14.1 *Strayer Chapter 4, Exercise 37.*

Rubric. 4 points if individual, 3 points if pair.

Problem 14.2 *Strayer Chapter 4, Student Project 6.*

Rubric. 4 points if individual, 3 points if pair.

Problem 14.3 *Strayer Chapter 4, Exercise 38 parts (a) through (e)*

For part (e) in addition to the hints in Strayer, it may help to use that

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

Rubric. Parts (a)-(c) 4 points if individual, 3 points if pair. Part (d) 4 points if individual, 3 points if pair. Part (e) 4 points.

Problem 14.4 *(If presenting as a pair) Strayer Chapter 4, Exercise 38 part (f)*

Rubric. 4 points.

C.10 Perfect Numbers

Project on perfect numbers.

Read Strayer Sections 3.4 and 3.5.

Rubric. Present as much as necessarily introduction for classmates to follow: 4 points.

Present the proof of Theorem 3.9 and the proof of the "only if" direction of Theorem 3.12.

Pick several problems in Exercise Set 3.5 to solve and present. Check with me that you have chosen a reasonable number of problems, but all are interesting (in similar ways).

Rubric. Proofs from the text: 4 points each.

References

[Ernst, 2022] Ernst, D. C. (2022). *An introduction to proof via inquiry-based learning*. MAA Press.

[Flapan et al., 2010] Flapan, E., Marks, T., and Pommersheim, J. (2010). *Number Theory: A Lively Introduction with Proofs, Applications, and Stories*. John Wiley & Sons, Hoboken, NJ.

[Jones and Jones, 1998] Jones, G. A. and Jones, J. M. (1998). *Elementary Number Theory*. Springer Science & Business Media.

[Niven et al., 1991] Niven, I., Zuckerman, H. S., and Montgomery, H. L. (1991). *An introduction = ,ntroduction to the Theory of Numbers*. John Wiley & Sons.

[Strayer, 2001] Strayer, J. K. (2001). *Elementary Number Theory*. Waveland Press.