

Math 310

Introduction to Modern Algebra

Worksheets

Contents

1	The Integers, Proof Techniques	1
1.1	The integers	1
1.2	Divisibility of integers	2
1.3	Proof techniques	3
1.3.1	Direct proofs	3
1.3.2	Proofs by contradiction	4
2	Sets and Logic	5
2.1	Sets	5
2.2	Logic	6
2.3	Quantifiers	8
3	Division Algorithm	9
3.1	The Well Ordering Principle	9
3.2	The Division Algorithm	9
4	Greatest common divisor, the Euclidean algorithm	13
4.1	Greatest Common Divisor	13
4.2	The Euclidean Algorithm	14
5	Primes and the Fundamental Theorem of Arithmetic	18
5.1	Primes	18
5.2	The Fundamental Theorem of Arithmetic	21
6	Proofs by Induction	24
6.1	Mathematical Induction	24
6.2	Strong induction	27

7	Equivalence Relations and Equivalence Classes	29
7.1	Equivalence relations	29
7.2	Equivalence classes	30
8	Congruence and Congruence Classes	33
8.1	Congruence	33
8.2	Congruence classes	35
9	Modular Arithmetic	37
9.1	The set $\mathbb{Z}_N$ of congruence classes	37
9.2	Adding congruence classes	37
9.3	Multiplying congruence classes	39
9.4	Units	40
10	Rings	42
10.1	Binary operations	42
10.2	Rings	45
11	Properties of Rings, Subrings, Domains, and Fields	47
11.1	Properties of rings	47
11.2	Subrings	49
11.3	Domains and fields	51
11.4	Product rings	53
12	Polynomial Rings	54
12.1	Polynomials and their degree	54
12.2	The Division Algorithm and GCDs	57
12.3	Irreducible polynomials and irreducible factorizations	59
13	Functions	61
13.1	Injective functions	61
13.2	Surjective functions	62
13.3	Bijjective functions	63
14	Homomorphisms and Isomorphisms	67
14.1	Isomorphisms	67
14.2	Homomorphisms	70
14.3	Properties of homomorphisms	72
15	RSA Cryptography	73
15.1	How RSA works	73
15.2	The mathematics behind RSA	73
15.3	Challenge Example	75

1 The Integers, Proof Techniques

1.1 The integers

The word “integer” refers to a whole number, either negative, positive, or zero. So, the set of all integers consists of:

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

We write this more formally in *set notation* as

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

We write that a is an integer in symbols as $a \in \mathbb{Z}$.

Integers have many nice mathematical properties one could ask for: they have operations of addition, subtraction, and multiplication. These operations follow several rules which we will take for granted. We call these facts that we take for granted “axioms”.

Axioms (Properties of integers)

1. **Closure under addition:** If a, b are integers, then $a + b$ is an integer.
2. **Associativity of addition:** If a, b, c are integers, then $(a + b) + c = a + (b + c)$.
3. **Commutativity of addition:** If a, b are integers, then $a + b = b + a$.
4. **Additive identity:** 0 is an integer; if a is an integer, then $a + 0 = a = 0 + a$.
5. **Additive inverses:** If a is an integer, then $-a$ is an integer and $a + (-a) = 0 = (-a) + a$.
6. **Closure under multiplication:** If a, b are integers, then ab is an integer.
7. **Associativity of multiplication:** If a, b, c are integers, then $(ab)c = a(bc)$.
8. **Commutativity of multiplication:** If a, b are integers, then $ab = ba$.
9. **Multiplicative identity:** If a is an integer, then $a \cdot 1 = a = 1 \cdot a$.
10. **Distributivity:** If a, b, c are integers, then $a(b + c) = ab + ac = (b + c)a$.

Now let’s think about the natural numbers, which are the positive integers:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Exercise 1.1. Which of the 10 axioms listed above remain true if we replace the word integer (or integers) by natural number (or natural numbers)?

1.2 Divisibility of integers

We all have a notion of what it means for one integer to divide another.

◁ **Example:** For example, 3 divides 12 and 5 divides 75, but 7 does not divide 20. ▷

Exercise 1.2. Formulate a *precise* definition of what it means for one integer to divide another integer. Your definition should start as follows

An integer a divides an integer b if . . .

After a few minutes, we'll compare suggested definitions. Record the definition we agreed upon as a class here:

Definition 1.1. An integer a divides an integer b , written $a \mid b$, if

◁ **Notation:** We write $a \mid b$ for a divides b . This should not be confused with the fraction a/b which indicates division of a by b . ▷

Exercise 1.3. List all the integers that divide 12.

Exercise 1.4. Which integers divide 0? Which integers does 0 divide?

Exercise 1.5. Which integers divide 1? Which integers does 1 divide?

Exercise 1.6. Which integers divide -1 ? Which integers does -1 divide?

Exercise 1.7. Define what it means for an integer a to be *even* and define what it means for an integer b to be *odd*.

An integer a is even if . . .

An integer a is odd if . . .

Record the definitions we agreed upon as a class here:

Definition 1.2. An integer a is even if

Definition 1.3. An integer a is odd if

Important remark: only use the definitions 1.1, 1.2 and 1.3 we agreed upon in the following proofs. Do not use any alternate definitions you came up with in your groups.

1.3 Proof techniques

A *mathematical statement* is a sentence that is either true or false.

- “Go Huskers!” is not a mathematical statement.
- “8 is an odd number” is a mathematical statement – it happens to be false.

Conditional statements form the backbone of mathematical reasoning. A conditional statement takes the form “If P , then Q ”, denoted $P \Rightarrow Q$. It is true whenever P is false or both P and Q are true. We call P the *hypothesis* and Q the *conclusion*.

1.3.1 Direct proofs

A direct proof is a proof technique for conditional statements $P \Rightarrow Q$ where one supposes P to be true and shows by utilizing P together with definitions, axioms, and algebraic manipulations, that Q is true.

Exercise 1.8. Rewrite the following statement: “The sum of two even integers is even” in if-then form.

Here is a sample direct proof.

Proposition 1.9. *If a and b are even integers then $a + b$ is an even integer.*

Proof.

□

Now try your hand at this:

Proposition 1.10. *If a, b, c, m, n are integers such that a divides b and a divides c , then a divides $b \cdot n + c \cdot m$.*

Proof.

□

1.3.2 Proofs by contradiction

A proof by contradiction is a proof technique for statements of the form “If P , then Q .” which works by assuming P to be true and Q to be false and deriving a contradiction.

Exercise 1.11. Rewrite the following statement: “The sum of an even integer and an odd integer is odd.” in the form “If ..., then ...”

Exercise 1.12. Prove: The sum of an even integer and an odd integer is odd.

2 Sets and Logic

2.1 Sets

Sets are just collections of objects. the objects in a set are called *elements* of that set.

◁ **Notation:** We write $x \in A$ to mean that x is an *element of* a set A . ▷

◁ **Example:** Writing $A = \{1, 2, 3\}$ means A is the set with elements 1, 2, and 3. ▷

◁ **Example:** The empty set, denoted $\emptyset$ is the set with no elements. ▷

◁ **Notation:** We can describe the elements of a set by writing down the properties they satisfy. This is called *set-builder* notation. ▷

◁ **Example:** For example, the set of all even integers is $E = \{a \mid a \in \mathbb{Z}, a \text{ is even}\}$ and the set of all odd integers is $O = \{a \mid a \in \mathbb{Z}, a \text{ is odd}\}$. The vertical line in set builder notation is read "such that". It does not mean divides, although it is the same symbol. ▷

New sets can be obtained from old by means of several set operations.

Definition 2.1. Given two sets A and B , we can form new sets by

- *union* $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- *intersection* $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- *set difference* $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

Exercise 2.1. What are $E \cup O, E \cap O, \mathbb{Z} \setminus E, \mathbb{Z} \setminus O$?

Exercise 2.2. Let a and b be integers and let $C = \{x \in \mathbb{Z} \mid x \text{ divides both } a \text{ and } b\}$.

- Can C be the empty set? If so, give examples of a and b for which this is true. If not provide justification.
- Can C be a set with only one element? If so, give examples of a and b for which this is true. If not provide justification.
- Can $C = \mathbb{Z}$? If so, give examples of a and b for which this is true. If not provide justification.

2.2 Logic

We can form *compound statements* as listed below:

- P **and** Q is a true statement whenever both P and Q are true statements
- P **or** Q is a true statement whenever either one of P or Q (or both) are true statements
- **Not** P is a true statement whenever P is a false statement.
- **If** P **then** Q (written $P \Rightarrow Q$) is true whenever P is false or Q is true.

Exercise 2.3. Which of the following statements are true?

- (a) “If pigs could fly then they would be purple.”
- (b) “If 12 is even, then 5 divides 12.”
- (c) “For an integer n , if n is even then -2 divides n ”.

Exercise 2.4. What is the negation of the statement “ P and Q ”?

Exercise 2.5. What is the negation of the statement “ P or Q ”?

Exercise 2.6. Fill out the following table with T and F for when the compound statements are true or false respectively. – Record this in your notebook.

P	Q	P and Q	P or Q	not P	$P \Rightarrow Q$	$(\text{not } P) \Rightarrow Q$	$(\text{not } Q) \Rightarrow (\text{not } P)$
T	T						
T	F						
F	T						
F	F						

Two statements are **logically equivalent** if they have the same truth value for all possible truth values of the inputs P, Q . If statements S and T are logically equivalent and we want to prove S is true, we can prove T is true instead!

Exercise 2.7. Explain why when we want to prove “ P or Q ” we could instead prove “ $(\text{not } P) \Rightarrow Q$ ”.

Definition 2.2. The **contrapositive** of " $P \Rightarrow Q$ " is $(\text{not } Q) \Rightarrow (\text{not } P)$.

Exercise 2.8. Explain why when we want to prove " $P \Rightarrow Q$ " we could instead prove " $(\text{not } Q) \Rightarrow (\text{not } P)$ ", the contrapositive.

Exercise 2.9. Consider the statement "For an integer a , if a^2 is odd, then a is odd."

Prove this statement by following these steps (all steps should be included in your proof):

- Write down carefully the contrapositive of this statement.
- Prove the contrapositive.
- Conclude the original statement is true.

Proof.

□

Definition 2.3. The **converse** of the if-then statement "If P then Q " is "If Q then P ".

Exercise 2.10. Show by means of an example that the converse of an if-then statement is **not** logically equivalent to the statement itself.

Exercise 2.11. Show using a truth table that the **negation** of $P \Rightarrow Q$ is " P and $(\text{not } Q)$ ".

2.3 Quantifiers

In mathematics we use two quantifiers

- the **universal quantifier** “for every” (or “for any” or “for all”), in symbols $\forall$ and
- the **existential quantifier** “there exists”, in symbols $\exists$.

An important difference

- To prove an existentially quantified statement “There exists x such that P holds.” it suffices to give an **example** of an x for which P holds.
- To disprove a universally quantified statement “For all x , P holds.” it suffices to give a **counterexample** of an x for which P is false.

Exercise 2.12. Consider the following statement: “The sum of two odd integers is odd.”

- Note that the statement involves *implicit* universal quantifiers. Rewrite the statement using notation (letters) for the two integers and the appropriate universal quantifiers.
- Disprove the statement.

Negating statements containing quantifiers:

- the negation of “For every x , P holds” is “There exists x such that not P holds”.
- the negation of “There exists x such that P holds” is “For every x , not P holds”.

Exercise 2.13. Negate the following statements. Is the second one true or false?

- The sum of two odd integers is odd.
- There exists an odd integers a so that a^2 is even.

3 Division Algorithm

3.1 The Well Ordering Principle

Axiom 3.1 (The Well-Ordering Principle).

Every non-empty set of non-negative integers has a smallest element.

UNDERSTANDING THE WELL-ORDERING PRINCIPLE.

Exercise 3.2. Give some examples of non-empty sets of non-negative integers and their smallest elements.

Exercise 3.3. Is the Well-Ordering Principle still true if we drop the word *non-empty*?

Exercise 3.4. Is the well-ordering principle still true if we drop the word *non-negative*?

Exercise 3.5. Explain why the smallest element of a non-empty set of non-negative integers must be a non-negative integer.

3.2 The Division Algorithm

Theorem 3.6 (Division Algorithm Theorem:). *Let $n, d \in \mathbb{Z}$ with $d > 0$. There exists unique $q, r \in \mathbb{Z}$ such that*

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Exercise 3.7. Suppose we take $n = 25$ and $d = 4$ in the statement of the Division Algorithm. What values of q and r that make the conclusion hold true?

Exercise 3.8. Suppose we take $n = -25$ and $d = 4$ in the statement of the Division Algorithm. What values of q and r that make the conclusion hold true?

Exercise 3.9. If we were to allow d to be negative, would the conclusion of the Division Algorithm Theorem remain true? For example, think of the case when $d = -1$.

Exercise 3.10. If we were to drop the phrase " $0 \leq r < d$ " from the Division Algorithm Theorem, would it still be true?

◁ **Example:** If we wish to find the quotient and remainder of 692 and 17, $692 = 17 \cdot 40 + 12$, we can really think of division as repeated subtraction. That is,

$$\begin{aligned} 692 - 17 &= 675 \\ 675 - 17 &= 658 \\ &\vdots \\ 29 - 17 &= 12 \end{aligned} \tag{3.1}$$

The set of results of these repeated subtractions can be written as

$$\mathcal{S} = \{692 - 17x \mid x \in \mathbb{Z} \text{ and } 692 - 17x \geq 0\} = \{12, 29, \dots, 658, 675, 692, 709, \dots\}.$$

Note that the remainder, 12, is the smallest element of $\mathcal{S}$. ▷

For $n, d \in \mathbb{Z}$ with $d > 0$ define a set $\mathcal{S}$ as follows:

$$\mathcal{S} = \{y \mid y = n - dx \text{ for some } x \in \mathbb{Z} \text{ and } y \geq 0\}.$$

Exercise 3.11. If $n = 17, d = 5$, write out some explicit elements of $\mathcal{S}$. Do the same for $n = -33$ and $d = 8$.

Exercise 3.12. Prove that $\mathcal{S}$ is **non-empty**. *Hint:* often, the easiest way to show a set is non-empty is to give an explicit element in it. Consider two cases: $n \geq 0$ and $n < 0$.

Exercise 3.13. Explain why $\mathcal{S}$ has a **smallest element**.

Exercise 3.14. Let r be the smallest element of $\mathcal{S}$. Prove that $0 \leq r < d$.

EXISTENCE AND UNIQUENESS. The Division Algorithm Theorem has two parts: an **existence** statement and an **uniqueness** statement.

Theorem 3.15 (Existence portion of the division algorithm theorem). *Let $n, d \in \mathbb{Z}$ with $d > 0$. There exists $q, r \in \mathbb{Z}$ such that $n = dq + r$ and $0 \leq r < d$.*

Explain how the previous exercises prove Theorem 3.15.

Theorem 3.16 (Uniqueness portion of the division algorithm theorem). *Let $n, d \in \mathbb{Z}$ with $d > 0$. If $q, r, q', r' \in \mathbb{Z}$ are such that $n = dq + r$ and $0 \leq r < d$ and also $n = dq' + r'$ and $0 \leq r' < d$ then $q = q'$ and $r = r'$.*

Exercise 3.17. Prove Theorem 3.16. *Hint:* show that $d \mid (r - r')$ and that $-d < r - r' < d$.

THE CONNECTION BETWEEN “DIVIDES” AND THE “DIVISION ALGORITHM”.

Exercise 3.18. Let $n, d \in \mathbb{Z}$ with $d > 0$, and (using the division algorithm) write $n = qd + r$ where $0 \leq r < d$. Prove that d divides n if and only if $r = 0$.

A statement of the form “P if and only if Q” is called a **biconditional** statement. It consists of two if-then statements “If P, then Q” and “If Q, then P”. To prove the biconditional statement, you must prove both.

Proof. Suppose $n, d \in \mathbb{Z}$ with $d > 0$, and $n = qd + r, 0 \leq r < d$.
($\Rightarrow$) If d divides n then $r = 0$.

($\Leftarrow$) If $r = 0$ then d divides n .

□

4 Greatest common divisor, the Euclidean algorithm

4.1 Greatest Common Divisor

Definition 4.1. Let a be an integer. A **divisor** of a is an integer d so that $d \mid a$.

Definition 4.2. Let a and b be two integers, not both of which are 0.

The **greatest common divisor** or **GCD** of a, b is the largest integer d such that d divides a and d divides b . We often write $\gcd(a, b)$ for the GCD of a and b .

Important note: The definition says that the GCD of a and b has the following properties:

- $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. (“common divisor” property)
- If n is an integer, $n \mid a$ and $n \mid b$, then $\gcd(a, b) \geq n$. (“greatest” common divisor)

Exercise 4.1. List all divisors of 18. List all divisors of 24. Find $\gcd(18, 24)$.

Exercise 4.2. Why does the definition of $\gcd$ stipulate that not both of a and b are 0?

Exercise 4.3. Show that if a and b are integers not both equal to zero, then $\gcd(a, b) \geq 1$.

Exercise 4.4. For $a > 0$, what is $\gcd(a, a)$? For $a < 0$, what is $\gcd(a, a)$?

Exercise 4.5. What is $\gcd(a, 7a)$ when $a > 0$? What is $\gcd(a, 7a)$ when $a < 0$?

Exercise 4.6. What is $\gcd(a, 0)$ for $a \neq 0$?

Exercise 4.7. Let a be an integer. Show that a and $-a$ have the same divisors.

Exercise 4.8. Let a, b be integers not both equal to 0.

Let $A = \{d \in \mathbb{Z} \mid d \mid a \text{ and } d \mid b\}$ and $B = \{n \in \mathbb{Z} \mid n \mid a \text{ and } n \mid (-b)\}$.

How are the sets A and B related? How are $\gcd(a, b)$ and $\gcd(a, -b)$ related?

4.2 The Euclidean Algorithm

We now discuss the **Euclidean algorithm**, a method to find the GCD of two integers.

Exercise 4.9. Suppose a, b, q, r are integers and $a = bq + r$.

Prove that if d is a common divisor of b and r , then d is a common divisor of a and b .

What does this say about the relationship between the sets

$$A = \{d \in \mathbb{Z} \mid d \mid a \text{ and } d \mid b\} \text{ and } B = \{d \in \mathbb{Z} \mid d \mid b \text{ and } d \mid r\}?$$

Exercise 4.10. Suppose a, b, q, r are integers and $a = bq + r$.

Prove that if d is a common divisor of a and b , then d is a common divisor of b and r .

What does this say about the relationship between the sets

$$A = \{d \in \mathbb{Z} \mid d \mid a \text{ and } d \mid b\} \text{ and } B = \{d \in \mathbb{Z} \mid d \mid b \text{ and } d \mid r\}?$$

Exercise 4.11. Explain how the work above proves the following

Lemma 4.12. *Suppose a, b, q, r are integers and $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.*

AN EXAMPLE OF EUCLIDEAN ALGORITHM

Consider the following computation, which you can assume is accurate:

$$\begin{array}{lll}
 524 = 148 \cdot 3 + 80 & 0 \leq 80 < 148 & \text{(i)} \\
 148 = 80 \cdot 1 + 68 & 0 \leq 68 < 80 & \text{(ii)} \\
 80 = 68 \cdot 1 + 12 & 0 \leq 12 < 68 & \text{(iii)} \\
 68 = 12 \cdot 5 + 8 & 0 \leq 8 < 12 & \text{(iv)} \\
 12 = 8 \cdot 1 + 4 & 0 \leq 4 < 8 & \text{(v)} \\
 8 = 4 \cdot 2 + 0 & & \text{(vi)}
 \end{array}$$

Exercise 4.13.

- What is going on on each individual line?
- How does each line relate to the previous one?
- Justify, using previous results from this worksheet, that $\gcd(524, 148) = \gcd(148, 80) = \gcd(80, 68) = \gcd(68, 12) = \gcd(12, 8) = \gcd(8, 4) = \gcd(4, 0) = 4$.

AN EXAMPLE OF THE EXTENDED EUCLIDEAN ALGORITHM

The Euclidean algorithm can also be used to find integers x and y such that

$$\gcd(a, b) = xa + by.$$

An expression of the form $xa + yb$ is known as a *linear combination* of a and b . Let's see how to find x and y by back-tracing the work previous example:

Exercise 4.14.

- Use equation (i) to express 80 as a linear combination of 524 and 148.
- Use equation (ii) to express 68 as a linear combination of 148 and 80. Use this and the previous part to express 68 as a linear combination of 524 and 148.
- Starting with equation (iii), express 12 as a linear combination of 68 and 80. Use this and the previous parts to express 12 as a linear combination of 524 and 148.
- Continue in this way to eventually express $4 = \gcd(524, 148)$ as a linear combination of 524 and 148.

HANDLING $\gcd(a, b)$ WHEN $b < 0$

Exercise 4.15. How would you use the work above to determine $\gcd(524, -148)$? (1-line answer)

Exercise 4.16. How would you use the work above to express $\gcd(524, -148)$ as a linear combination of 524 and -148 ? (1-line answer)

Here is a formal statement of the **Euclidean Algorithm**. The last sentence is called the **extended Euclidean Algorithm**.

Theorem 4.17 (The Euclidean Algorithm). *Let a and b be integers such that $b > 0$. Define a list of integers $r_1, r_2, \dots, r_m$ by repeatedly applying the division algorithm as follows:*

- r_1 is the unique integer such that $a = b \cdot q_1 + r_1$ and $0 \leq r_1 < b$ for some $q_1 \in \mathbb{Z}$.
- If $r_1 = 0$, then set $m = 1$ and stop. If $r_1 > 0$, define r_2 to be the unique integer such that $b = r_1 \cdot q_2 + r_2$ and $0 \leq r_2 < r_1$ for some integer q_2 .
- If $r_2 = 0$, then set $m = 2$ and stop. If $r_2 > 0$, define r_3 to be the unique integer such that $r_1 = r_2 \cdot q_3 + r_3$ and $0 \leq r_3 < r_2$ for some integer q_3 .
- Continue in this fashion until one arrives at a remainder $r_m = 0$.

Then $\gcd(a, b) = r_{m-1}$.

PROOF OF THE EUCLIDEAN ALGORITHM

Exercise 4.18. Verify that the consecutive remainders in the Euclidean algorithm satisfy $b > r_1 > r_2 > \dots > r_m = 0$.

Exercise 4.19. Use the previous exercise to explain why the procedure described in the Euclidean Algorithm must stop after a finite number of steps.

Exercise 4.20. Use facts from this worksheet to explain why

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \gcd(r_3, r_4) = \cdots = \gcd(r_{m-1}, r_m).$$

Exercise 4.21. Use facts from this worksheet and the previous exercise to explain why $\gcd(a, b) = r_{m-1}$.

Exercise 4.22. Use the Extended Euclidean Algorithm to prove the following theorem.

Theorem 4.23. *If a and b are integers such that $a \neq 0$ and $b \neq 0$, then there exist integers x and y so that*

$$\gcd(a, b) = ax + by.$$

5 Primes and the Fundamental Theorem of Arithmetic

5.1 Primes

Definition 5.1. A integer p is called **prime** if

- $p \neq 0$, $p \neq 1$, $p \neq -1$ and
- the only divisors of p are 1 , -1 , p and $-p$.

Definition 5.2. An integer n is **composite** if it is not prime.

Exercise 5.1. List all integers n such that $|n| \leq 10$ and n is prime.

Exercise 5.2. If p is prime, show that $|p|$ is also prime.

Exercise 5.3. If p and q are both prime integers and p divides q , what can you conclude? Prove your claim.

Exercise 5.4. If p is a prime integer and a is any integer, what are the possible values of $\gcd(p, a)$? Write your answer in the form below and prove it.

Lemma 5.5. *If p is a prime integer and a is any integer, then*

$$\gcd(p, a) = \begin{cases} \underline{\hspace{2cm}} & \text{if } \underline{\hspace{2cm}} \\ \underline{\hspace{2cm}} & \text{if } \underline{\hspace{2cm}} \end{cases}$$

Proof. Case 1:

Case 2:

□

Next we will prove a very important theorem.

Theorem 5.6. *Let a, b, c be integers. If $a \mid (bc)$ and $\gcd(a, b) = 1$, then $a \mid c$.*

To prove Theorem 5.6 we will use Lemma 5.7, a statement that can be proven using the extended Euclidean algorithm.

Lemma 5.7. *If a, b are integers and $\gcd(a, b) = 1$ then there exist $x, y \in \mathbb{Z}$ so that*

$$xa + yb = 1.$$

Exercise 5.8. Prove Theorem 5.6 using Lemma 5.7.

Exercise 5.9. Give an example to show Theorem 5.6 is no longer true if we remove the hypothesis $\gcd(a, b) = 1$.

A corollary is a mathematical statement that can be proven using a previously proven theorem. We will prove the following corollary of Theorem 5.6¹:

Corollary 5.10 (Euclid's lemma). *Let a, b, p be integers. If p is prime and $p \mid (ab)$, then $p \mid a$ or $p \mid b$.*

Exercise 5.11. Prove Corollary 5.10 using Lemma 5.5 and Theorem 5.6. You will want to follow a proof method called *case analysis*. A template for it follows:

Proof. Suppose

Consider two cases:

Case 1: if $p \mid a$ then

Case 2: if $p \nmid a$ then we must prove

□

Exercise 5.12. Suppose p is a prime integer, $a_1, a_2, \dots, a_n$ are arbitrary integers, and $p \mid (a_1 a_2 \cdots a_n)$. What can you conclude from the Corollary? How?

Exercise 5.13. Suppose p and $q_1, q_2, \dots, q_n$ are all prime integers and $p \mid (q_1 q_2 \cdots q_n)$. What can you conclude? How?

¹This appears in the ninth book of Euclid's Elements.

5.2 The Fundamental Theorem of Arithmetic

The Fundamental theorem of arithmetic says that every integer can be factored into primes in an essentially unique way. More precisely, it says the following:

Theorem 5.14 (The Fundamental Theorem of Arithmetic). *If n is an integer and $n \neq 0$, $n \neq 1$, $n \neq -1$, then there exist prime integers $p_1, \dots, p_s$ such that*

$$n = p_1 \cdots p_s.$$

Moreover, given two prime factorizations for the same integer n

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

where $p_1, \dots, p_s$ and $q_1, \dots, q_t$ are primes, then the number of factors must be the same, that is, $s = t$, and there exists a reordering of the factors $q_1, \dots, q_t$ such that we have

$$q_1 = p_1 \text{ or } q_1 = -p_1, \quad q_2 = p_2 \text{ or } q_2 = -p_2, \quad \dots, \quad q_s = p_s \text{ or } q_s = -p_s.$$

Exercise 5.15. Find two different factorizations of -24 into primes, and note that your factorizations are the same up to reordering.

Exercise 5.16. How do we factor -17 into an (essentially unique) product of primes?

Exercise 5.17. Suppose you knew the existence part (first sentence) of the Fundamental Theorem of Arithmetic is true for **positive** n . How would you use this to prove that the same statement is true for **negative** n ?

Exercise 5.18. Suppose you know the Fundamental Theorem of Arithmetic is true. Prove that if $n \neq 1$ is a **positive** integer then there exist **positive** prime integers $p_1, \dots, p_s$ such that $n = p_1 \cdots p_s$.

We will prove the Fundamental Theorem of Arithmetic soon. For now let's use it.

Exercise 5.19. Are there primes p_1, p_2, p_3 and q_1, q_2 so that $p_1 \neq p_2, p_1 \neq p_3, p_2 \neq p_3, q_1 \neq q_2$ and $p_1 p_2 p_3 = q_1^2 q_2$? If so, give an example of such primes. If not, prove it!

Exercise 5.20. Are there **positive** primes p_1, p_2, p_3 and q_1, q_2 so that $p_1 \neq p_2, p_1 \neq p_3, p_2 \neq p_3, q_1 \neq q_2$ and $p_1 p_2 p_3 = q_1^2 q_2$? If so, give an example of such primes. If not, prove it!

The examples above illustrate that we can give a stronger form of the Fundamental Theorem of Arithmetic if we restrict to positive prime integers.

We can also write the prime factorization from the FTA in a shorter way, using powers of primes. For example instead of $24 = 2 \cdot 2 \cdot 2 \cdot 3$ we write $24 = 2^3 \cdot 3^1$.

Theorem 5.21 (Fundamental Theorem of Arithmetic in exponential notation). *If n is an integer and $n \neq 0, n \neq 1, n \neq -1$, then there exist positive integers $e_1, \dots, e_s$ and **distinct positive prime integers** $p_1, \dots, p_s$ and such that*

$$n = \pm p_1^{e_1} \cdots p_s^{e_s}.$$

Moreover, given two prime factorizations for the same integer n

$$\pm p_1^{e_1} \cdots p_s^{e_s} = \pm q_1^{f_1} \cdots q_t^{f_t}$$

*where $p_1, \dots, p_s$ are distinct positive primes, $q_1, \dots, q_t$ are distinct positive primes, and $e_1, \dots, e_s, f_1, \dots, f_t$ are **positive integers**, then there exists a reordering of the factors $q_1, \dots, q_s$ so that the prime factors as well as their exponents agree, that is,*

$$s = t, p_1 = q_1, \dots, p_s = q_s, \text{ and } e_1 = f_1, \dots, e_s = f_s.$$

Exercise 5.22. Give an example that shows the word distinct is needed for the primes $p_1, \dots, p_s$ in the uniqueness (moreover) part of the strong Fundamental Theorem of Arithmetic above.

Exercise 5.23. Give an example that shows the word positive is needed for the exponents $e_1, \dots, e_s$ in the uniqueness (moreover) part of the strong Fundamental Theorem of Arithmetic above.

The Return of the Greatest Common Divisor

Even though we have seen above that the exponents in the strong Fundamental Theorem of Arithmetic should be positive for the uniqueness statement to hold, if we are interested in comparing two prime factorizations it helps if we make the prime factors be the same at the expense of possibly allowing zero exponents.

For example, to compare $a = 2^{10} \cdot 5^7 \cdot 11$ and $b = 2^5 \cdot 3 \cdot 7^2$ we can instead write them as

$$\begin{aligned}a &= 2^{10} \cdot 3^0 \cdot 5^7 \cdot 7^0 \cdot 11^1 \\b &= 2^5 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0.\end{aligned}\tag{5.1}$$

Exercise 5.24. Consider integers a, b and their prime factorizations

$$a = \pm p_1^{a_1} \cdots p_k^{a_k} \quad \text{and} \quad b = \pm p_1^{b_1} \cdots p_k^{b_k}$$

where $a_1, \dots, a_k, b_1, \dots, b_k \geq 0$ and $p_1, \dots, p_k > 0$ are *distinct positive* primes.

- (a) Can you list all the divisors of a and of b (separately) using their prime decompositions?
- (b) Can you list all the common divisors of a and b ?
- (c) Find a formula for $\gcd(a, b)$ in terms of $p_1, \dots, p_k, a_1, \dots, a_k, b_1, \dots, b_k$.

6 Proofs by Induction

6.1 Mathematical Induction

Induction is a very helpful proof technique for showing results about all positive integers, or where the statement depends on a positive integer. Proofs by induction go as follows:

We have a statement we want to prove that depends on a positive integer n ; let's refer to that statement as $P(n)$. To prove $P(n)$ for all n , we follow two steps:

- **Base Case:** Prove that $P(n)$ holds for the smallest value of n we are considering. Usually this is $P(0)$ or $P(1)$.
- **Induction Step:** Assume that $P(n)$ is true for some n , and prove that this implies $P(n+1)$ is true.

Example A statement that can be proven by the Principle of Mathematical Induction:

Recall that $n! = 1 \cdot 2 \cdots n$. For every integer $n \geq 1$ we have $2^{n-1} \leq n!$.

Proof. We give a proof by induction. Let $P(n)$ be the statement " $2^{n-1} \leq n!$ ".

- **Base case:** $P(1)$ is the statement $2^0 \leq 1!$. This is true since $2^0 = 1 = 1!$.
- **Induction Step:** Assume $P(n)$ is true for some $n \geq 1$, that is, $2^{n-1} \leq n!$.
 $P(n+1)$ is the statement $2^{n+1-1} \leq (n+1)!$
 Observe that

$$2^n = 2^{n-1} \cdot 2 \leq n! \cdot (n+1) = 1 \cdot 2 \cdots n \cdot (n+1) = (n+1)!,$$

where the middle inequality follows by multiplying the inequalities $2^{n-1} \leq n$ (the inductive hypothesis) and $2 \leq n+1$ (which follows from $n \geq 1$).

This shows $P(n+1)$ is true.

By the Principle of Mathematical Induction, $2^{n-1} \leq n!$ for every integer $n \geq 1$. □

Important features of a proof by induction:

1. always start by stating you will do a proof by induction
2. next state clearly what your $P(n)$ statement is
3. a frequent mistake is to include the words "for all/every/any n " in the $P(n)$ statement. This is incorrect. The $P(n)$ statement applies just to the n which is named inside the $P(n)$ notation.
4. label your base case and induction step clearly
5. state what $P(n+1)$ is clearly before you prove it.
6. finish the proof saying "By the Principle of Mathematical Induction ... is true for all $n \geq \dots$ "

It is a *theorem* that once you prove both the base case and the induction step, $P(n)$ must hold for all integers $n \geq r$, where r is the value of n in your base case. Most often $r = 1$.

Here is the formal statement:

Theorem 6.1 (The Principle of Mathematical Induction). *Suppose $r \geq 1$ is an integer and $P(n)$ is a statement that applies to an integer $n \geq r$. If*

- *$P(r)$ is true and*
- *if $P(n)$ is true, then $P(n + 1)$ is true,*

then $P(n)$ is true for all $n \geq r$.

Proof. Suppose $P(r)$ is true and $P(n)$ implies $P(n + 1)$ for all $n \geq 1$.

Assume towards a contradiction it is not the case that $P(n)$ is true for all $n \geq r$. Then the set $S := \{k \in \mathbb{Z} \mid k \geq r, P(k) \text{ is false}\}$ is a non-empty set of positive integers. By the Well-Ordering Axiom, S has a least element, call it j . In words, j is an integer such that $P(j)$ is true but $P(i)$ is false for all i such that $r \leq i < j$.

Since we assumed $P(r)$ is true, $j \neq r$. So $j > r$ and hence $j - 1 \geq r$. Since $j - 1 < j$, $j - 1$ must not be in the set S . That is, $P(j - 1)$ is true. But we are assuming $P(j - 1)$ implies $P(j)$, and thus $P(j)$ must be true. We have concluded that $P(j)$ is both true and false, which is a contradiction.

Since we reached a contradiction, it must be that the set S is empty — that is, $P(n)$ is true for all positive integers n . $\square$

Now it is your turn. Prove the following using the Principle of Mathematical Induction.

Exercise 6.2. For every integer $n \geq 1$, 5 divides $11^n - 6$.

Exercise 6.3. Prove the following theorem using induction on $n \geq 1$:

Theorem 6.4 (Generalized Euclid's Lemma). *Let $a_1, \dots, a_n$ be integers. If p is a prime and $p \mid (a_1 \cdots a_n)$, then $p \mid a_i$ for some $i \in \{1, \dots, n\}$.*

Exercise 6.5. Prove the **uniqueness part of the Fundamental Theorem of Arithmetic** using induction on $n = \max\{s, t\}$ (the largest among s and t) and Theorem 6.4.

Theorem 6.6. *Let $p_1, \dots, p_s$ and $q_1, \dots, q_t$ be prime integers. If $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ then $s = t$ and after reordering the factors we have $p_1 = \pm q_1, p_2 = \pm q_2, \dots, p_s = \pm q_s$.*

6.2 Strong induction

Sometimes we need a stronger form of induction where in the induction step we assume not only $P(n)$, but also $P(k)$ for all $k \leq n$, where k should also satisfy $k \geq 1$ or whatever else is our base case. This is called Strong Induction or Complete Induction.

Theorem 6.7 (The Principle of Strong Mathematical Induction). *Suppose $P(n)$ is a statement that refers to an integer n . Suppose that there exist integers r, b so that*

- $P(r), P(r+1), \dots, P(b)$ are true and
- for all integers $n > b$, if $P(k)$ is true for all $1 \leq k < n$, then $P(n)$ is true.

Then $P(n)$ is true for all n .

Less formally, to prove $P(n)$ for all n using strong induction, we follow two steps:

- **Base Case:** Prove that $P(n)$ holds for some small values that you cannot account for in your induction step.
- **Induction Step:** Assume that $P(k)$ is true for all $k < n$, and prove that $P(n)$ is true.

Exercise 6.8. Use strong induction to prove that every class with at least 6 students in it can be divided up into groups each of size 3 or 4. Here are some tips:

- Let $P(n)$ be the statement “A class with n students can be divided up into groups each of size 3 or 4”
- Check that $P(n)$ holds for $n = 6, 7$ or 8 by just explicitly showing how this is possible.
- Let $n \geq 9$. Assume $P(k)$ holds for all $6 \leq k < n$, and deduce that $P(n)$ holds. (Imagine starting with a class of n students, pick any three students and put them in a group. What can you say about the remaining $n - 3$ students?)

Exercise 6.9. Use strong induction to prove the **existence part of the Fundamental Theorem of Arithmetic**.

Theorem 6.10. *Every integer $n \geq 2$ is a product of primes.*

7 Equivalence Relations and Equivalence Classes

7.1 Equivalence relations

Definition 7.1. An **equivalence relation** on a set X is a binary relation $\sim$ (meaning $a \sim b$ expresses a relationship between elements $a, b \in X$) satisfying three properties:

1. For every $a \in X$, $a \sim a$. This is known as the *reflexive* property.
2. If $a \sim b$, then $b \sim a$. This is known as the *symmetric* property.
3. If $a \sim b$ and $b \sim c$, then $a \sim c$. This is known as the *transitive* property.

The symbol “ $\sim$ ” is read as “is equivalent to”; $a \sim b$ is read as “ a is equivalent to b ”.

Here is an example of equivalence relation:

Example.

Exercise 7.1. Let X denote the set of all points in the plane. Given two such points P and Q , declare $P \sim Q$ to mean that P and Q have the same distance to the origin. For instance the point $P = (3, 4)$ has distance 5 to the origin and the point $Q = (0, -5)$ also has distance 5 to the origin, and hence $P \sim Q$. But $R = (3, 0)$ is at distance 3 from the origin, so that $P \not\sim R$ and $Q \not\sim R$.

Check that the three properties of an equivalence relation are satisfied by $\sim$.

- *The reflexive property:*
- *The symmetric property:*
- *The transitive property:*

7.2 Equivalence classes

Definition 7.2. Let $\sim$ be an equivalence relation on some set X . For $a \in X$, the *equivalence class* of a , written $[a]$, is the set of elements that are equivalent to a :

$$[a] = \{b \in X \mid a \sim b\}$$

Exercise 7.2. Let X and $\sim$ be as in Example 7.1. Given a point $P \in X$, describe the equivalence class $[P]$ geometrically.

Exercise 7.3. For $\sim$ as in Example 7.1 and points $P \sim Q$ in the plane, what can you say about how $[P]$ and $[Q]$ relate?

Exercise 7.4. For $\sim$ as in Example 7.1 and points $P \not\sim Q$ in the plane what can you say about how $[P]$ and $[Q]$ relate?

Above you have discovered some sets that are equal. Let us say formally what it means that two sets are equal.

Definition 7.3. Two sets A and B are equal provided that they have the same elements. In other words $A = B$ provided $x \in A$ if and only if $x \in B$.

To prove that two sets A and B are equal ($A = B$) according to the definition (which involves a biconditional) we must prove two statements:

- if $x \in A$ then $x \in B$. This property is known as $A \subseteq B$, read A is *contained in* B .
- If $x \in B$ then $x \in A$. This property is known as $B \subseteq A$, read B is *contained in* A .

Exercise 7.5. Prove the following theorem.

Theorem 7.6. *Let X be any set and $\sim$ be any equivalence relation on X . For elements $a, b \in X$ we have $a \sim b$ if and only if $[a] = [b]$.*

- *Proof notes.* Recall that to prove a biconditional statement you have to prove two separate statements. Write each of these statements down fully before proving them.
- To prove an equality of sets $[a] = [b]$, use the guidelines on the previous page.

Exercise 7.7. Prove the following corollary.

Corollary 7.8. *Let X be a set and $\sim$ an equivalence relation on X . Any two equivalence classes are either disjoint (have no common elements) or equal. In other words, for all $a, b \in X$, either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.*

- *Proof notes.* Recall that " P or Q " is logically equivalent to " $(\text{not } P) \Rightarrow Q$ ".
- Recall that $[a] \cap [b]$ is notation for the intersection of sets $[a]$ and $[b]$, that is, the set of common elements of $[a]$ and $[b]$. More formally, this is defined as

$$[a] \cap [b] = \{x \in X \mid x \in [a] \text{ and } x \in [b]\}.$$

Recall that $\emptyset$ is the notation for the empty set, that is, the set that has no elements. Therefore $[a] \cap [b] \neq \emptyset$ means that there exists $x \in X$ so that $x \in [a] \cap [b]$.

8 Congruence and Congruence Classes

8.1 Congruence

Definition 8.1. Fix a nonzero integer N . We say that $a, b \in \mathbb{Z}$ are **congruent modulo N** if $N \mid (a - b)$ and we denote this by write $a \equiv b \pmod{N}$.

In this notation, the a and b are the two inputs, and $\equiv \pmod{N}$ is one piece, like a complicated equal sign.

Exercise 8.1. True or False? Justify your answers using the definition of congruence 8.1 or by providing a counterexample.

- (a) $5 \equiv 19 \pmod{7}$
- (b) $-5 \equiv 20 \pmod{10}$
- (c) $-11 \equiv -26 \pmod{5}$
- (d) Any two odd integers are congruent modulo 2.
- (e) Any two odd integers are congruent modulo 3.

Exercise 8.2. Suppose I tell you that $7 \equiv 27 \pmod{N}$ for some integer N . What are the possible values of N ?

Exercise 8.3. Congruence modulo 10.

- (a) There is a unique integer r such that $0 \leq r \leq 9$ and r is congruent to the year of your birth modulo 10. Find r . (The answer will vary from one student to another.)
- (b) In general, given an integer a , how does one quickly and easily find r such $0 \leq r \leq 9$ and $r \equiv a \pmod{10}$?

Exercise 8.4. Prove the following theorem.

Theorem 8.5. *If $N > 0$ is an integer then for every $a \in \mathbb{Z}$ there exists a unique $r \in \mathbb{Z}$ such that $a \equiv r \pmod{N}$ and $0 \leq r < N$.*

Exercise 8.6. Prove the following theorem.

Theorem 8.7. *If $N > 0$ is an integer then congruence modulo N is an equivalence relation.*

Proof. Suppose $N > 0$ is an integer.

- *The reflexive property:*

- *The symmetric property:*

- *The transitive property:*

□

Exercise 8.8. A nice feature is that we may add and multiply congruences. Prove the following.

Theorem 8.9. *If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then*

$$a + c \equiv b + d \pmod{N} \quad \text{and} \quad ac \equiv bd \pmod{N}.$$

8.2 Congruence classes

Definition 8.2. Fix a nonzero integer N . For $a \in \mathbb{Z}$, the **congruence class of a modulo N** is the set

$$[a]_N = \{b \in \mathbb{Z} \mid b \equiv a \pmod{N}\}.$$

Note and keep in mind that $[a]_N$, the congruence class of a , **is a set not a number**.

Exercise 8.10. Describe the set $[7]_2$. Describe the set $[-8]_2$.

Exercise 8.11. True or False? Justify your answer.

(a) $47 \in [17]_5$.

(c) $[17]_6 \cap [19]_7 = \emptyset$.

(b) $[17]_7 \cap [23]_7 = \emptyset$.

(d) For all integers a , $[a]_{60} \subseteq [a]_{10}$.

Exercise 8.12. How many different congruence classes are there modulo 3? That is, how many different subsets of $\mathbb{Z}$ are there of the form $[a]_3$ for various a ? What are these sets?

Exercise 8.13. The following theorem is a particular case of a theorem you proved before.

Theorem 8.14. *For any positive integer N and any pair of integers a, b exactly one of the following possibilities is true:*

1. $[a]_N = [b]_N$ or
2. $[a]_N \cap [b]_N = \emptyset$

Expand on the previous theorem by filling in the blanks with words that make the following statements true. You may use theorems from previous worksheets.

Theorem 8.15. *For any positive integer N and any pair of integers a, b we have*

1. $[a]_N = [b]_N$ if and only if _____
2. $[a]_N \cap [b]_N = \emptyset$ if and only if _____

Exercise 8.16. Fill in the blank with words that make the following theorem true and prove it. Record the theorem and its proof in your notebook.

Theorem 8.17. *For any positive integer N , there are exactly ____ congruence classes modulo N , namely _____.*

Hint: use some theorems from this worksheet.

9 Modular Arithmetic

9.1 The set $\mathbb{Z}_N$ of congruence classes

Recall from the previous worksheet the following

Definition 9.1. Fix a nonzero integer N . For $a \in \mathbb{Z}$, the **congruence class of a modulo N** is the subset of $\mathbb{Z}$ consisting of all integers congruent to a modulo N ; that is, the **congruence class of a modulo N** is the set

$$[a]_N := \{b \in \mathbb{Z} \mid b \equiv a \pmod{N}\}.$$

Let's now consider the set of all congruence classes modulo a fixed integer N .

Definition 9.2. For a positive integer N , $\mathbb{Z}_N$ is the set of congruence classes of integers modulo N . By Theorem 8.17 we know all the congruence classes of integers modulo N , thus

$$\mathbb{Z}_N = \{[0]_N, [1]_N, \dots, [N-1]_N\}.$$

Exercise 9.1. What are the elements of $\mathbb{Z}_2$? What are the elements of the elements of $\mathbb{Z}_2$?

Exercise 9.2. What are the elements of $\mathbb{Z}_3$? What are the elements of the elements of $\mathbb{Z}_3$?

9.2 Adding congruence classes

Using the fact that congruences can be added and multiplied, we may introduce rules for adding and multiplying congruence classes.

Definition 9.3. Fix a non-zero integer N . Let a, b be integers. Define $[a]_N + [b]_N$ to be the congruence class modulo N given by the following rule:

Pick any $x \in [a]_N$ and pick any $y \in [b]_N$, and define $[a]_N + [b]_N = [x + y]_N$.

Perhaps you notice a troubling aspect of the definition for adding congruence classes: the construction of $[a]_N + [b]_N$ seems to depend on choices of representative elements $x \in [a]_N$ and $y \in [b]_N$. What if one pair of choices leads to a different outcome than another pair of choices? That would be non-sensical.

◁ **Example:** Let us compute $[17]_5 + [11]_5$. The rule says that we start by picking any elements $x \in [17]_5$ and $y \in [11]_5$. I'll choose $x = 2$ (since $2 \equiv 17 \pmod{5}$) and $y = 1$ (since $6 \equiv 1 \pmod{5}$). Next we add our choices for x and y as ordinary integers to get 8, and conclude that $[17]_5 + [11]_5 = [3]_5$.

I could have also chosen $x' = 17$ and $y' = 11$ in which case we conclude that $[17]_5 + [11]_5 = [28]_5$. Note that $[3]_5 = [28]_5$ by Theorem 8.15 (since $3 \equiv 28 \pmod{5}$), so either way we got the same result. ▷

Now we see that the addition given in Definition 9.3 is **well defined**, that is, does not depend on our choice of x and y .

Theorem 9.3. *The definition of adding congruence classes is independent of the choices made. In more detail, if $[a]_N$ and $[b]_N$ are two congruence classes modulo N , and we pick $x_1, x_2 \in [a]_N$, and $y_1, y_2 \in [b]_N$, then $[x_1 + y_1]_N = [x_2 + y_2]_N$.*

Proof. Suppose $a, b, N \in \mathbb{Z}$ and $x_1, x_2 \in [a]_N$ and $y_1, y_2 \in [b]_N$.

Since x_1 and x_2 belong to $[a]_N$ we have $x_1 \equiv a \pmod{N}$ and $x_2 \equiv a \pmod{N}$ which, by using the symmetric and transitive properties, yield that $x_1 \equiv x_2 \pmod{N}$. Similarly, since y_1 and y_2 both belong to $[b]_N$, we deduce that $y_1 \equiv y_2 \pmod{N}$. By Theorem 8.9 we may add these two congruences to conclude $x_1 + y_1 \equiv x_2 + y_2 \pmod{N}$. Using Theorem 8.15 it follows that $[x_1 + y_1]_N = [x_2 + y_2]_N$. □

Definition 9.4 (More convenient definition for adding congruence classes). Since $a \in [a]_N$ and $b \in [b]_N$, we can write the rule for addition in Definition 9.3 as

$$[a]_N + [b]_N = [a + b]_N.$$

Exercise 9.4. Have each member of your group compute $[120]_6 + [13]_6$ using a different pair of representatives. Then compare your answers. Are they equal?

9.3 Multiplying congruence classes

Exercise 9.5. Give a rule for *multiplying* congruence classes similar to Definition 9.3.

Definition 9.5. Fix a non-zero integer N . Let a, b be integers. Define $[a]_N \cdot [b]_N$ to be the congruence class modulo N given by the following rule:

Pick any $x \in [a]_N$ and pick any $y \in [b]_N$, and define $[a]_N \cdot [b]_N = \underline{\hspace{2cm}}$.

Exercise 9.6. Have each member of your group compute $[120]_6 \cdot [13]_6$ using a different pair of representatives. Then compare your answers. Are they equal?

Exercise 9.7. State and prove a theorem which shows that your general rule for $[x]_N \cdot [y]_N$ in $\mathbb{Z}_N$ is well defined. This should be similar to Theorem 9.3.

Theorem 9.8. *The definition of multiplying congruence classes is independent of the choices made. In more detail, if $[a]_N$ and $[b]_N$ are two congruence classes modulo N , and we pick $x_1, x_2 \in [a]_N$, and $y_1, y_2 \in [b]_N$, then*

$\underline{\hspace{2cm}}$.

9.4 Units

Definition 9.6. A congruence class $[a]_N$ in $\mathbb{Z}_N$ is called a **unit** if there exists a congruence class $[b]_N$ in $\mathbb{Z}_N$ such that $[b]_N \cdot [a]_N = [1]_N$. In this case $[b]_N$ is called a **multiplicative inverse** of $[a]_N$.

Exercise 9.9. List all of the congruence classes in $\mathbb{Z}_6$ that are units, and for each that is, give its multiplicative inverse. (Figure this out just by trial and error.)

Exercise 9.10. Prove the following Theorem.

Theorem 9.11. *Suppose a, N are integers with $N \neq 0$. Then there exists $b \in \mathbb{Z}$ such that $b \cdot a \equiv 1 \pmod{N}$ if and only if $\gcd(a, N) = 1$.*

Exercise 9.12. Let's translate the previous theorem into a statement about congruence classes. Fill in the following theorem.

Theorem 9.13. *Given integers a, N with $N > 0$, the congruence class $[a]_N \in \mathbb{Z}_N$ is a unit if and only if _____.*

Exercise 9.14. If p is a positive prime integer, what are all the units in $\mathbb{Z}_p$?

Exercise 9.15. Since $\gcd(131, 260) = 1$ we have that $[131]_{260}$ is a unit by Theorem 9.13. Find the multiplicative inverse of $[131]_{260}$ using the extended Euclidean algorithm.

10 Rings

10.1 Binary operations

Definition 10.1. A **binary operation** on a set S is a rule that assigns to two inputs taken from S one output which also belongs to S .

We write $x \star y$ to indicate the result of applying operation $\star$ to the pair of inputs (x, y) .

◁ **Example:** Addition and multiplication are binary operations on the set of integers. ▷

◁ **Remark:** In defining a binary operation $\star$ on a set S , we are implicitly requiring that the set S is **closed under the operation**, meaning that for all $x, y \in S$ we have $x \star y \in S$. ▷

Exercise 10.1. Which of the following rules $\star$ are binary operations on the indicated set S ?

- (a) Let S be all non-zero real numbers and let $a \star b = \frac{a}{b}$.
- (b) Let S be the set of all even integers and $a \star b = a + b$
- (c) Let S be the set of all odd integers and $a \star b = a + b$

Here are some special abstract properties a binary operation can have.

Definition 10.2.

- *Commutativity.* A binary operation $\star$ is **commutative** if $x \star y = y \star x$ for any $x, y \in S$.
- *Associativity.* By definition, binary operations only take two inputs. If we wanted to operate on three things, we would have to choose two to pair first, then throw in the third. A binary operation $\star$ is **associative** if we get the same result with either grouping:

$$(x \star y) \star z = x \star (y \star z) \text{ for any } x, y, z \text{ in } S.$$

- *Identity.* An element $e \in S$ is an **identity** for a binary operation $\star$ if $e \star x = x$ and $x \star e = x$ for all $x \in S$.
- *Inverses.* If $\star$ is a binary operation with an identity e , then an **inverse** for an element x is another element y such that $x \star y = e$ and $y \star x = e$.

Exercise 10.2. For each of the following binary operations, determine if they are associative or commutative:

- (a) the set of all non-zero real numbers with the operation of division: $a \star b = a/b$.
- (b) the real numbers $\mathbb{R}$ with the operation of subtraction: $a \star b = a - b$.
- (c) $\mathbb{R}$ with the operation of addition.
- (d) $\mathbb{R}$ with the operation being taking the maximum, that is, $a \star b = \max\{a, b\}$.

Exercise 10.3. Recall that 2×2 is an array of real numbers of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and that one may add 2×2 matrices using the rule

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} a+r & b+s \\ c+t & d+u \end{bmatrix}$$

Addition is a binary operation on the set of all 2×2 matrices and it turns out is it associative. Is it commutative?

Exercise 10.4. One can also multiply 2×2 matrices by the rule

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} r & s \\ t & u \end{bmatrix} = \begin{bmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{bmatrix}$$

Multiplication is a binary operation on the set of all 2×2 matrices and it turns out is it associative. Is it commutative?

Exercise 10.5. We can also describe operations by tables: the entry in row x and column y for operation $\star$ means $x \star y$. Below are some operation tables for operations on the set $\{a, b, c, d\}$. Decide for each whether the operation is commutative.

	a	b	c	d
a	a	b	c	d
b	b	b	c	d
c	c	c	c	d
d	d	d	d	d

	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Exercise 10.6. Which of these four tables has an identity? What is the identity element?

Exercise 10.7. For each of the operations above that has an identity, which elements have a inverse and what is the inverse?

Exercise 10.8. Two of these tables correspond to the operations of $+$ and $\cdot$ that we have defined on $\mathbb{Z}_4$. Can you spot them?

Exercise 10.9. Which of the following operations have an identity? If so, what is it?

- (a) multiplication of 2×2 matrices.
- (b) division of positive real numbers $a \star b = \frac{a}{b}$.
- (c) averaging two real numbers, that is $a \star b = \frac{a+b}{2}$.
- (d) maximum of two real numbers: that is $a \star b = \max\{a, b\}$.

10.2 Rings

Definition 10.3. A **ring** is a set R with two binary operations written as $+$ and $\cdot$ and called addition and multiplication, such that the following properties all hold:

1. **Closure under addition:** If a, b are elements of R , then $a + b \in R$.
2. **Associativity of addition:** If a, b, c are elements of R , then $(a + b) + c = a + (b + c)$.
3. **Commutativity of addition:** If a, b are elements of R , then $a + b = b + a$.
4. **Additive identity:** There exists an element $0 \in R$ so that for any $a \in R$ we have $a + 0 = a = 0 + a$.
5. **Additive inverses:** For every $a \in R$ there is an element denoted $-a \in R$ so that $a + (-a) = 0 = (-a) + a$.
6. **Closure under multiplication:** If a, b are elements of R , then $ab \in R$.
7. **Associativity of multiplication:** If a, b, c are elements of R , then $(ab)c = a(bc)$.
8. **Multiplicative identity:** There exists an element $1 \in R$ so that for any $a \in R$ we have $a \cdot 1 = a = 1 \cdot a$.
9. **Distributivity:** If a, b, c are elements of R , then $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Warning: our definition of ring differs from that of the (optional) textbook! Whenever we say ring, we mean a “ring with identity” in the notation of the book.

Definition 10.4. A ring R is called a **commutative ring** if in addition to all the properties in Definition 10.3 it satisfies

10. **Commutativity of multiplication:** If a, b are elements of R , then $ab = ba$.

◁ **Example:** Since it satisfies the axioms on our worksheet 1, $\mathbb{Z}$ is a commutative ring.▷

Our second example of a ring is a set we have recently encountered.

Theorem 10.10. *The set $\mathbb{Z}_N$ of congruence classes modulo N is a commutative ring with respect to the addition and multiplication defined on worksheet 9.*

We will not check all required properties for $\mathbb{Z}_N$ for the sake of time. We’ll just check two.

Exercise 10.11. Prove that $\mathbb{Z}_N$ satisfies commutativity of multiplication.

Exercise 10.12. Prove that $\mathbb{Z}_N$ satisfies the distributive property. (In view of 10.11 it suffices to check a single equality.)

Exercise 10.13. For each of the following sets and pairs of binary operators, determine if they form a ring. If not, list which axioms fail.

- (a) The set of all even integers under the usual rules for adding and multiplying.
- (b) The set of all positive real numbers under the usual rules for adding and multiplying.
- (c) The set of all 2×2 matrices with entries in $\mathbb{R}$ under the rules for adding and multiplying matrices introduced in 10.3 and 10.4.
- (d) The set $\mathcal{F}(\mathbb{R}) = \{ \text{functions } f : \mathbb{R} \rightarrow \mathbb{R} \}$ with the usual rules for adding and multiplying functions, namely $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x) \cdot g(x)$
- (e) The set of $\mathcal{I}(\mathbb{R}) = \{ \text{increasing functions } f : \mathbb{R} \rightarrow \mathbb{R} \}$ (increasing means if $x \leq y$ then $f(x) \leq f(y)$) with the same addition and multiplication as in part (d) above.

11 Properties of Rings, Subrings, Domains, and Fields

11.1 Properties of rings

Recall that we defined rings in the following way. In this worksheet we shall denote 0_R and 1_R the additive identity and multiplicative identity of a ring R to distinguish them from the additive identity and multiplicative identity of another ring.

Definition 11.1. A **ring** is a set R with two binary operations, written as $+$ and $\cdot$, and called *addition* and *multiplication*, respectively, such that the following properties all hold:

1. **Closure under addition:** If a, b are elements of R , then $a + b \in R$.
2. **Associativity of addition:** If a, b, c are elements of R , then $(a + b) + c = a + (b + c)$.
3. **Commutativity of addition:** If a, b are elements of R , then $a + b = b + a$.
4. **Additive identity:** There exists an element $0_R \in R$ so that for any $a \in R$ we have $a + 0_R = a = 0_R + a$.
5. **Additive inverses:** For every $a \in R$ there is an element denoted $-a \in R$ so that $a + (-a) = 0_R = (-a) + a$.
6. **Closure under multiplication:** If a, b are elements of R , then $ab \in R$.
7. **Associativity of multiplication:** If a, b, c are elements of R , then $(ab)c = a(bc)$.
8. **Multiplicative identity:** There exists an element $1_R \in R$ so that for any $a \in R$ we have $a \cdot 1_R = a = 1_R \cdot a$.
9. **Distributivity:** If a, b, c are elements of R , then $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

In this worksheet we will be simultaneously discussing several different rings, thus we will need to be able to work with several different additive and multiplicative elements and keep track of what ring each belongs to. For this purpose we use the notations 0_R and 1_R to mean the additive and multiplicative elements of the ring R .

Definition 11.2. A ring R is called a **commutative ring** if in addition to all the properties in Definition 11.1 it satisfies

10. **Commutativity of multiplication:** If a, b are elements of R , then $ab = ba$.

Definition 11.3. Let R be a ring. An element $r \in R$ is a **unit** in R if it has a **two-sided multiplicative inverse** s , that is, if there exists $s \in R$ such that $rs = 1 = sr$.

Note: In an arbitrary ring to check that an element r is a unit you must check **both** that $rs = 1$ and that $sr = 1$. If the ring is known to be commutative, then it suffices to check $rs = 1$. This is why in the case of $\mathbb{Z}_N$ we defined units using only one such equality.

Exercise 11.1. Using only the ring axioms 1–9 listed above prove the following theorem.

Theorem 11.2. *Let $(R, +, \cdot)$ be a ring.*

- (a) For all $a \in R$ we have $0 \cdot a = 0$ and $a \cdot 0 = 0$.*
- (b) The zero element 0_R and the one element 1_R of R are unique.*
- (c) Every element $x \in R$ has a unique additive inverse.*
- (d) For any elements $a, b \in R$ we have $(-a) \cdot b = -(a \cdot b)$.*
- (e) For any element $a \in R$ we have $(-1) \cdot a = -a$.*
- (f) For every element $x \in R$, if x is a unit, that is, if x has a two-sided multiplicative inverse, then that inverse is unique.*

Exercise 11.3. Verify that the one-element set $\{0\}$ equipped with binary the operations $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a ring. You may go quickly through most of the axioms, but do carefully prove the existence of a multiplicative identity. This ring is called the **zero ring**.

Exercise 11.4. Suppose R is any ring such that $0_R = 1_R$. Prove that R has only one element.

Hint: Recall from Theorem 11.2 that $0 \cdot a = 0$ holds for any ring element a .

11.2 Subrings

Definition 11.4. A nonempty subset S of a ring R is a **subring** of R if S is a ring with respect to the same operations $+$, $\times$ from R .

Exercise 11.5. Find a subring of $\mathbb{R}$.

Exercise 11.6. Find a subring of $\mathcal{F} = \{f : \mathbb{R} \rightarrow \mathbb{R}\}$, the set of all functions from $\mathbb{R}$ to itself with the operations $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$.

Exercise 11.7. Every ring always contains at least two *trivial* subrings. Explain what they are.

Exercise 11.8. Prove the following theorem.

Theorem 11.9. *If R is a ring and $S \subseteq R$ is nonempty and satisfies*

- $0_R, 1_R \in S$,
- S is closed under addition: *for all $s_1, s_2 \in S$ we have $s_1 + s_2 \in S$,*
- S is closed under additive inverses: *for any $s_1 \in S$ we have $-s_1 \in S$, and*
- S is closed under multiplication: *for all $s_1, s_2 \in S$ we have $s_1 s_2 \in S$.*

then S is a subring of R .

Exercise 11.10. Is the converse of Theorem 11.9 true?

11.3 Domains and fields

Notation: Recall that you proved before in Theorem 11.2 that if an element r has a multiplicative inverse, then it has only one such inverse. In other words, inverses are unique when they exist.

If r is a ring element with a multiplicative inverse, we write its unique inverse as r^{-1} .

Exercise 11.11. What are the units in $\mathbb{Z}$. What is the inverse of each?

Definition 11.5. Let R be a commutative ring. A element $r \in R, r \neq 0$ is a **zero divisor** in R if there exists $s \in R, s \neq 0$ such that $rs = 0$.

Definition 11.6. A ring R is a **integral domain**, or simply a **domain**, if R is commutative, $0_R \neq 1_R$, and R has no zero divisors.

Definition 11.7. A ring R is a **field** if R is commutative, $1_R \neq 0_R$, and every nonzero element is a unit.

Exercise 11.12. Prove

Proposition 11.13. *A ring R is an integral domain if and only if R satisfies the following properties:*

- R is commutative,
- $0_R \neq 1_R$, and
- if $ab = 0_R$ for elements $a, b \in R$, we have $a = 0_R$ or $b = 0_R$.

Exercise 11.14. Verify that $\mathbb{Z}$ is a domain.

Exercise 11.15. Is $\mathbb{Z}$ a field?

Exercise 11.16. Give an example of a field.

Exercise 11.17. For which values of N is $\mathbb{Z}_N$ a field?

Exercise 11.18. For which values of N is $\mathbb{Z}_N$ a domain?

Exercise 11.19. Let R be a commutative ring. Prove that if $r \in R$ is a unit, then it is not a zero divisor.

Exercise 11.20. Prove that every field is a domain.

Exercise 11.21. Give an example of an integral domain that is not a field.

Exercise 11.22. Prove the following **cancelation property for non zero divisors**:

Proposition 11.23. *Suppose R is a commutative ring and $r \in R$ is a non-zero element that is not a zero divisor. Prove that if $ra = rb$ for some elements $a, b \in R$, then $a = b$.*

11.4 Product rings

Definition 11.8. Let R and S be sets. The **cartesian product** of R and S is the set of ordered pairs

$$R \times S = \{(r, s) \mid r \in R, s \in S\}.$$

Exercise 11.24. Let R and S be rings. Define an operation called $+$ on $R \times S$ by $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$. The three different plus signs in the preceding sentence have three different meanings; explain.

Exercise 11.25. Is this operation on $R \times S$ associative and commutative? Does it have an identity? Does every $(r, s) \in R \times S$ have an inverse under $+$?

Exercise 11.26. Define a multiplication on $R \times S$ so that, together with the addition defined in (1), the set $R \times S$ becomes a ring. (You do not have to check all the properties.)

Exercise 11.27. How many elements are in the ring $\mathbb{Z}_N \times \mathbb{Z}_M$?

Exercise 11.28. Make tables for the addition and multiplication in $\mathbb{Z}_2 \times \mathbb{Z}_2$. Identify the multiplicative and additive identity elements. Which elements have a multiplicative inverse?

12 Polynomial Rings

12.1 Polynomials and their degree

We now define polynomials. This will match the notion of polynomials with coefficients in the real numbers that you have encountered in high school or in calculus, but we extend it to create polynomials with coefficients in any ring, for example, $\mathbb{Z}_N$.

Theorem 12.1. *If R is a commutative ring, then there exists a **polynomial ring** denoted $R[x]$, containing an element x that is not in R , which has these properties:*

(i) *The set $R[x]$ consists of all expressions of the form*

$$a_0 + a_1x + \dots + a_nx^n \text{ (where } n \geq 0 \text{ and } a_i \in R \text{ for } 0 \leq i \leq n).$$

(ii) *The representation of elements in $R[x]$ is unique, that is,*

$$a_0 + a_1x + \dots + a_nx^n = b_0 + b_1x + \dots + b_nx^n \text{ if and only if } a_0 = b_0, \dots, a_n = b_n.$$

In particular, $a_0 + a_1x + \dots + a_nx^n = 0_R$ if and only if $a_i = 0_R$ for $0 \leq i \leq n$.

(iii) *Addition in $R[x]$ is given by*

$$(a_0 + a_1x + \dots + a_nx^n) + (b_0 + b_1x + \dots + b_nx^n) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n.$$

(iv) *Multiplication in $R[x]$ is given by*

$$\begin{aligned} (a_0 + a_1x + \dots + a_nx^n) \cdot (b_0 + b_1x + \dots + b_mx^m) = \\ (a_0 \cdot b_0) + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \dots + (a_nb_m)x^{n+m}. \end{aligned} \quad (12.1)$$

More precisely, the coefficient of x^j in the product is $\sum_{i=0}^j a_{j-i}b_i$.

(v) *R is a subring of $R[x]$ by viewing elements $a_0 \in R$ as polynomials.*

(vi) *$xa = ax$ for every $a \in R$ and, more generally, $R[x]$ is a commutative ring.*

We will not prove this theorem as checking the ring axioms can get slightly tedious.

Exercise 12.2. Match each polynomial with the smallest ring to which it belongs.

1. $\mathbb{Z}_9[x]$

4. $\mathbb{R}[x]$

2. $\mathbb{Z}[x]$

(i) $x^2 + 3x + 7$

3. $\mathbb{Q}[x]$

(ii) $\pi x^3 + ex + \sqrt{2}$

(iii) $2x^2 + \frac{3}{2}x + 1$

(iv) $[1]_9 + [3]_9x$

Definition 12.1. The **degree** of a polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is the largest $d \geq 0$ so that $a_d \neq 0$. So, the degree is n provided $a_n \neq 0$. We write $\deg p(x)$ for the degree of $p(x)$.

Exercise 12.3. Fill in the correct degrees of the following polynomials in $\mathbb{R}[x]$

1. $\deg(3 - 7x^2 + \sqrt{2}x^7) =$

1. $\deg(5.7) =$

2. $\deg(\pi x^5 + \sqrt[7]{128}x^{12}) =$

2. $\deg(0) =$

Proposition 12.4. Given a ring R and non-zero polynomials $p(x)$ and $q(x)$ in $R[x]$

$$\begin{aligned} \deg(p(x) + q(x)) &\leq \max\{\deg p(x), \deg q(x)\} \\ \deg(p(x) \cdot q(x)) &\leq \deg p(x) + \deg q(x). \end{aligned} \tag{12.2}$$

Exercise 12.5. Give examples of polynomials $p(x)$ and $q(x)$ so that

(a) $\deg(p(x) + q(x)) = \max\{\deg p(x), \deg q(x)\}$

(b) $\deg(p(x) + q(x)) < \max\{\deg p(x), \deg q(x)\}$

(c) $\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$

(d) $\deg(p(x) \cdot q(x)) < \deg p(x) + \deg q(x)$

Exercise 12.6. Prove the following

Proposition 12.7. If R is a domain then

(a) for non-zero polynomials $p(x)$ and $q(x)$ in $R[x]$, $\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$

(b) $R[x]$ is a domain.

12.2 The Division Algorithm and GCDs

Theorem 12.8 (Division Algorithm). *Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exists unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = g(x)q(x) + r(x) \text{ and either } r(x) = 0_F \text{ or } \deg r(x) < \deg g(x)$$

We will not worry about proving this theorem. Instead let's recall that there is an algorithm (long division) that gives us the $q(x)$ and $r(x)$ in the Division Algorithm Theorem.

◁ **Example:** Divide $f(x) = x^3 + x^2 - 1$ by $g(x) = x - 1$

$$\begin{array}{r}
 x^2 + 2x + 2 \\
 x - 1 \overline{) \begin{array}{r} x^3 + x^2 - 1 \\ - x^3 + x^2 \\ \hline 2x^2 \\ - 2x^2 + 2x \\ \hline 2x - 1 \\ - 2x + 2 \\ \hline 1 \end{array}}
 \end{array}$$

▷

Exercise 12.9. Divide $f(x) = 3x^5 + 2x^4 + 2x^3 + 4x^2 + x - 2$ by $g(x) = 2x^3 + 1$ in $\mathbb{R}[x]$.

Exercise 12.10. Divide $f(x) = x^3 + [2]_5x^2 + x + [2]_5$ by $g(x) = [2]_5x + [1]_5$ in $\mathbb{Z}_5[x]$.

Definition 12.2. Let F be a field and $a(x), b(x) \in F[x]$ with $b(x) \neq 0$. We say that $a(x)$ divides $b(x)$, and write $a(x)|b(x)$ if $b(x) = a(x)h(x)$ for some $h(x) \in F[x]$.

Definition 12.3. Let F be a field and $a(x), b(x) \in F[x]$, not both zero. The **greatest common divisor** of $a(x)$ and $b(x)$ is the polynomial of highest degree that divides both $a(x)$ and $b(x)$ and that has leading coefficient 1_F .

Exercise 12.11. Find the GCD of $a(x) = 2x^4 + 5x^3 - 5x - 2$ and $b(x) = 2x^3 - 3x^2 - 2x$.
Hint: $2x^4 + 5x^3 - 5x - 2 = (2x+1)(x+2)(x+1)(x-1)$ and $2x^3 - 3x^2 - 2x = (2x+1)(x-2)x$.

Theorem 12.12 (Euclidean Algorithm). *Let F be a field and $a(x), b(x) \in F[x]$, not both zero. Then there is a unique GCD $d(x)$ of $a(x)$ and $b(x)$ which can be found using the Euclidean algorithm followed by dividing the last non-zero remainder polynomial by its leading coefficient. Furthermore, there are polynomials $u(x)$ and $v(x)$ such that $d(x) = a(x)u(x) + b(x)v(x)$.*

Exercise 12.13. Find the GCD of $a(x) = 2x^4 + 5x^3 - 5x - 2$ and $b(x) = 2x^3 - 3x^2 - 2x$ using the Euclidean algorithm.

12.3 Irreducible polynomials and irreducible factorizations

Definition 12.4. Let R be a commutative ring with identity. An element $a \in R$ is said to be an **associate** of an element $b \in R$ if there is a unit $u \in R$ such that $au = b$.

Exercise 12.14. Find an associate to

- (a) the number 4 in $\mathbb{Z}$
- (b) the polynomial $x^2 + 3x + 2$ in $\mathbb{Q}[x]$.

Definition 12.5. Let F be a field. A non-constant polynomial $p(x) \in F[x]$ is said to be **irreducible** if its only divisors are its associates and the nonzero constant polynomials (units).

Exercise 12.15. Prove that every polynomial of degree 1 in $F[x]$ is irreducible in $F[x]$.

Exercise 12.16. The following theorems are reminiscent of facts proven for integers. What are these facts?

Theorem 12.17. *Let F be a field. A non-zero polynomial $f(x)$ is reducible in $F[x]$ if and only if $f(x)$ can be written as the product of two polynomials of lower degree.*

Theorem 12.18. *Let F be a field and $p(x)$ a non-constant polynomial in $F[x]$. Then the following are equivalent:*

1. *The polynomial $p(x)$ is irreducible.*
2. *If $b(x)$ and $c(x)$ are polynomials and $p(x)|b(x)c(x)$, then $p(x)|b(x)$ or $p(x)|c(x)$.*
3. *If $r(x)$ and $s(x)$ are any polynomials such that $p(x) = r(x)s(x)$, then $r(x)$ is a non-zero constant polynomial or $s(x)$ is a non-zero constant polynomial.*

Theorem 12.19. *Let F be a field. Every non-constant polynomial $f(x) \in F[x]$ is a product of irreducible polynomials in $F[x]$. This factorization is unique in the following sense: If*

$$p_1(x)p_2(x)\dots p_n(x) = q_1(x)q_2(x)\dots q_m(x)$$

with each $p_i(x)$ and $q_i(x)$ irreducible, then $n = m$ and up to some relabeling, $p_i(x)$ and $q_i(x)$ are associates.

13 Functions

Definition 13.1. A **function** f from a set A to a set B denoted $f : A \rightarrow B$ is a rule that assigns to every element $a \in A$ an element denoted $f(a) \in B$.
The set A is called the **domain** of f and the set B is called the **codomain** of f .

When working with functions between finite sets it helps to represent them pictorially with arrows as given below. Every arrow connects an element $a \in A$ (the source of the arrow) to $f(a)$ (the target of the arrow).

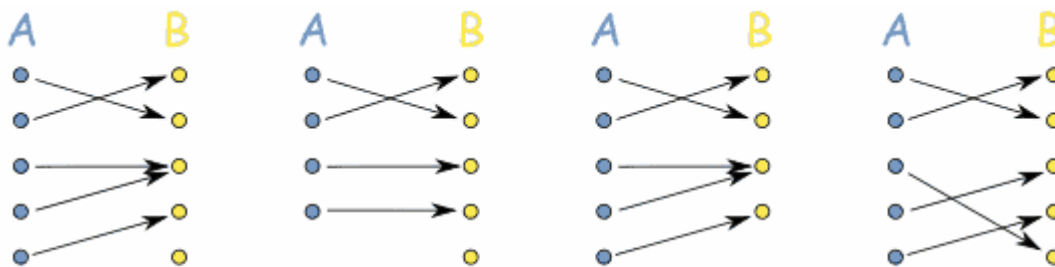


Figure 1: Pictures of functions

In other situations it is better to represent functions by giving a formula or rule for $f(x)$.

Example 13.1. Here are some functions you know:

- (a) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2$
- (b) $f : \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = 2x$
- (c) $f : \mathbb{R} \rightarrow \mathbb{Z}, f(x) = \lfloor x \rfloor$, where $\lfloor x \rfloor$ is the largest integer that is smaller or equal to x and some that you will get to know
- (d) $f : \mathbb{Z} \rightarrow \mathbb{Z}_N, f(x) = [x]_N$
- (e) $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_N, f([x]_N) = [-x]_N$

13.1 Injective functions

Notice that in Figure 1 sometimes there can be multiple arrows reaching the same element in B . When this does not happen we say f is injective.

Definition 13.2. A function $f : A \rightarrow B$ is **injective** or **one-to-one** if whenever $x, y \in A$ are such that $f(x) = f(y)$ then $x = y$.

Key tips for proving/ disproving that a function is injective

- To prove a function f is injective, suppose $f(x) = f(y)$ and prove that $x = y$.
- To prove a function f is not injective find x, y so that $f(x) = f(y)$ but $x \neq y$.

Exercise 13.2. For each of the functions in Figure 1 decide whether it is injective or not.

Exercise 13.3. For each of the functions in Example 13.1 decide whether it is injective or not with justification.

13.2 Surjective functions

Notice that in Figure 1 there is arrow leaving from every element (dot) in A . This is because a function associates to every $a \in A$ some element of B . However there may be some elements in B which do not receive arrows, so they are not outputs of the function f . To distinguish those elements of B which are outputs of f we introduce the following notion.

Definition 13.3. The **image** of a function $f : A \rightarrow B$ is the set

$$\text{Im}(f) = \{f(a) \mid a \in A\}.$$

The image is a subset of the codomain, $\text{Im}(f) \subseteq B$, but they need not be equal.

Exercise 13.4. For each of the functions in Example 13.1 find the image.

Definition 13.4. A function $f : A \rightarrow B$ is **surjective** or **onto** if for every $b \in B$ there exists $a \in A$ so that $f(a) = b$.
Equivalently, f is surjective if and only if $\text{Im}(f) = B$.

Exercise 13.5. For each of the functions in Figure 1 decide whether it is surjective or not.

Exercise 13.6. For each of the functions in Example 13.1 decide whether it is surjective or not with justification.

13.3 Bijective functions

Now we can combine the notions of injective and surjective.

Definition 13.5. A function $f : A \rightarrow B$ is **bijective** if f is both injective and surjective.

Exercise 13.7. Which of the functions in Figure 1 and Example 13.1 are bijective?

Exercise 13.8. Prove the following theorem:

Theorem 13.9. *If $f : A \rightarrow B$ is a bijective functions and A and B are finite sets then A and B must have the same number of elements.*

Exercise 13.10. Prove the following theorem:

Theorem 13.11. *If A and B are finite sets which have the same number of elements and $f : A \rightarrow B$ is a function, then the following are equivalent:
(a) f is injective, (b) f is surjective, (c) f is bijective.*

Note: a “**the following are equivalent**” statement as above means three if and only if statements: (a) if and only if (b); (b) if and only if (c); (c) if and only of (a). However, to prove all of this it suffice to prove only 3 if – then statements, namely

1. $(a) \Rightarrow (b)$: if (a) then (b)
2. $(b) \Rightarrow (c)$: if (b) then (c)
3. $(c) \Rightarrow (a)$: if (c) then (a)

Exercise 13.12. Prove the following theorem.

Theorem 13.13. *If R is a domain which has finitely many elements, then R is a field.*

Hint: Consider $r \in R, r \neq 0_R$ and the function $f : R \rightarrow R, f(x) = rx$. What properties among injective/ surjective/ bijective does this function have?

Exercise 13.14. Prove the following

Theorem 13.15 (Fermat's Little Theorem). *If $b, p \in \mathbb{Z}$ are such that p is a prime integer and p does not divide b then $b^{p-1} \equiv 1 \pmod{p}$.*

Hints: consider the set $A = \{[1]_p, [2]_p, \dots, [p-1]_p\} \subset \mathbb{Z}_p$. Define a function

$$f : A \rightarrow A, f([a]_p) = [b]_p[a]_p.$$

- Prove that f is injective and conclude that f is bijective.
- Enumerate the set $\text{Im}(f)$ in two different ways.
- Compute the product of the elements in $\text{Im}(f)$ in two different ways.

14 Homomorphisms and Isomorphisms

14.1 Isomorphisms

Two rings R and S are **isomorphic** if they are the same after relabelling. Here is the formal definition:

Definition 14.1. Let R and S be rings. An **isomorphism** from R to S is a function $f: R \rightarrow S$ such that the following properties hold:

- For all $a, b \in R$ if $f(a) = f(b)$ then $a = b$. (f is injective)
- For all $s \in S$ there exists $r \in R$ so that $f(r) = s$. (f is surjective)
- For all $a, b \in R$ we have $f(a + b) = f(a) + f(b)$. (f preserves addition.)
- For all $a, b \in R$ we have $f(a \cdot b) = f(a) \cdot f(b)$. (f preserves multiplication.)
- $f(1_R) = 1_S$. (f preserves multiplicative identities.)

We say R is *isomorphic* to S if there exists an isomorphism from R to S , and we write $R \cong S$ to signify that R and S are isomorphic.

Note: The reason we do not include $f(0_R) = 0_S$ in the definition of “isomorphism” is that it is a consequence of the other parts of the definition. You will prove this below.

Exercise 14.1. Write out the $+$ and $\times$ tables for $\mathbb{Z}_4$. There is a way to relabel the elements of $\mathbb{Z}_4$ with the names a, b, c , and d , so that the $+$ and $\times$ tables each become identical to one of the tables for the operations $\clubsuit$, $\diamond$, $\heartsuit$, and $\spadesuit$ from below. More formally, give an explicit isomorphism $f: \mathbb{Z}_4 \rightarrow S$, that is, say what $f([0]_4)$, $f([1]_4)$, $f([2]_4)$, $f([3]_4)$ are.

$\clubsuit$	a	b	c	d
a	a	b	c	d
b	b	b	c	d
c	c	c	c	d
d	d	d	d	d

$\diamond$	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

$\heartsuit$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	a	c
d	a	d	c	b

$\spadesuit$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Exercise 14.2. Consider the set $S = \{a, b, c, d\}$ and the binary operations $\oplus$ and $\otimes$ given by the following tables:

$\oplus$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\otimes$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

Take it on faith that the operations $\oplus$ and $\otimes$ make S into a ring. Find an **explicit** isomorphism $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow (S, \oplus, \otimes)$, that is, find

$$\begin{aligned}
 f([0]_2, [0]_2) &= \\
 f([0]_2, [1]_2) &= \\
 f([1]_2, [0]_2) &= \\
 f([1]_2, [1]_2) &=
 \end{aligned} \tag{14.1}$$

Can you find a *different* isomorphism $\mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow (S, \oplus, \otimes)$?

$$\begin{aligned}
 f([0]_2, [0]_2) &= \\
 f([0]_2, [1]_2) &= \\
 f([1]_2, [0]_2) &= \\
 f([1]_2, [1]_2) &=
 \end{aligned} \tag{14.2}$$

Exercise 14.3. Consider the ring $R = \text{Mat}_{2 \times 2}(\mathbb{R})$ of all 2×2 matrices with real entries. The subring

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{Z} \right\}$$

is isomorphic to $\mathbb{Z}$. Describe an explicit isomorphism from $\mathbb{Z}$ to S (or vice versa) and check that it satisfies the definition of isomorphism.

Here is what you need to do:

- (a) Define a function that you think might be an isomorphism $f : \mathbb{Z} \rightarrow S$ by $f(a) = ??$ where ?? is an element of S involving a .

$$f(a) =$$

- (b) Prove that f is injective, that is, prove that if $f(a) = f(b)$ then $a = b$.

(c) Prove that f is surjective, that is, given an element $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in S$ find $x \in \mathbb{Z}$ so that

$$f(x) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}.$$

(d) Prove that $f(a + b) = f(a) + f(b)$.

(e) Prove that $f(a \cdot b) = f(a) \cdot f(b)$

(f) Prove that $f(1_{\mathbb{Z}}) = 1_S$.

Exercise 14.4. Prove

Proposition 14.5. *If $f: R \rightarrow S$ is an isomorphism and $r \in R$ is a unit then $f(r)$ is also a unit. If $s \in S$ is a unit then there exists a unique $r \in R$ so that $f(r) = s$ and r is a unit of R . Thus there is a bijection between the units of R and the units of S .*

Exercise 14.6. Use Exercise 14.4 to prove that $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic.

Exercise 14.7. Prove

Proposition 14.8. *If $f : R \rightarrow S$ is an isomorphism and $r \in R$ is a zero divisor then $f(r)$ is a zero divisor. If $s \in S$ is a zero divisor, then there exists a unique $r \in R$ so that $f(r) = s$ and r is a zero divisor in R . Thus there is a bijection between the zero divisors of R and the zero divisors of S .*

Exercise 14.9. Use Exercise 14.7 to give yet another proof that $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic.

14.2 Homomorphisms

Definition 14.2. A **ring homomorphism** between two rings R and S is a function $\phi : R \rightarrow S$ that satisfies the following properties:

1. $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in R$. (ϕ preserves addition.)
2. $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ for all $x, y \in R$. (ϕ preserves multiplication.)
3. $\phi(1_R) = 1_S$. (ϕ preserves multiplicative identities.)

Exercise 14.10. Which of the following functions between rings is a **homomorphism**? Which are **isomorphisms**? If the function is not a homomorphism or an isomorphism say which property fails. No proofs are required for those functions that are homomorphisms or isomorphisms.

- (a) The inclusion function $i: \mathbb{Z} \hookrightarrow \mathbb{Q}$ given by $i(n) = \frac{n}{1}$.
- (b) The doubling function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(n) = 2n$.
- (c) The function $\pi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ sending each integer a to its congruence class $\pi(a) = [a]_n$.
- (d) The “evaluation at 0” function $Z: \mathbb{R}[x] \rightarrow \mathbb{R}$ sending $f(x)$ to $Z(f(x)) = f(0)$.
- (e) The differentiation function $D: \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ sending each polynomial f to $D(f) = \frac{df}{dx}$.
- (f) The function $F: \mathbb{R} \rightarrow \text{Mat}_{2 \times 2}(\mathbb{R})$ sending λ to $F(\lambda) = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$.
- (g) The function $D: \mathbb{R} \rightarrow \text{Mat}_{2 \times 2}(\mathbb{R})$ sending λ to $D(\lambda) = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$.
- (h) The function $\det: \text{Mat}_{2 \times 2}(\mathbb{Z}) \rightarrow \mathbb{R}$ sending each 2×2 matrix to its determinant.
- (i) The function $\pi: \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_2$ defined by $\pi([a]_2, [b]_3) = [a]_2$.
- (j) More generally, for rings R and S , the function $\pi: R \times S \rightarrow R$ defined by $\pi(r, s) = r$.

14.3 Properties of homomorphisms

Exercise 14.11. Prove

Theorem 14.12. *Let $\phi : R \rightarrow S$ be a ring homomorphism. Then*

- (a) $\phi(0_R) = 0_S$.
- (b) for all $x \in S$, $-\phi(x) = \phi(-x)$.

Hint: what is $\phi(0_R + 0_R)$?

Definition 14.3. The **kernel** of a ring homomorphism $\phi : R \rightarrow S$ is the set of elements in the source that map to the zero of the target; that is,

$$\ker \phi = \{r \in R \mid \phi(r) = 0_S\}.$$

Exercise 14.13. Prove

Theorem 14.14. *A homomorphism $\phi : R \rightarrow S$ is injective if and only $\ker \phi = \{0_R\}$.*

Hint: Given elements $a, b \in R$ such that $f(a) = f(b)$, what can you say about $f(a - b)$?

15 RSA Cryptography

15.1 How RSA works

We can replace any letter in the alphabet by a number with two digits as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

We can then represent words by numbers: HELLO=0805121215.

How RSA works

Secret: Bob picks 2 primes p, q and computes $n = pq$	$p = 29, q = 101$ $n = 2929$
Secret: Bob chooses an encrypting exponent e that is coprime with $(p-1)(q-1)$, that is, $\gcd(e, (p-1)(q-1)) = 1$ (sometimes e itself is taken to be a prime; that works, but is not necessary)	$e = 17$
Public: Bob announces n and e . This is Bob's public key .	$n = 2929, e = 17$
Secret: Alice writes her message as a sequence of numbers. If n is an $r+1$ -digit number she will split her message into r -digit blocks. Her message will look like $b_1 \ b_2 \ \dots \ b_m$	HELLO 0 805 121 215
Secret: Alice computes $b_1^e \pmod{n}, b_2^e \pmod{n}, \dots, b_m^e \pmod{n}$	$0^{17} = 0$ $805^{17} \equiv 962 \pmod{2929}$ $121^{17} \equiv 1053 \pmod{2929}$ $215^{17} \equiv 1491 \pmod{2929}$
Public: Alice sends the results of her computations to Bob. This is the encrypted message	0 962 1053 1491
Secret: Bob computes $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ using the Euclidean algorithm Bob computes $(b_1^e)^d \pmod{n}, (b_2^e)^d \pmod{n}, \dots, (b_m^e)^d \pmod{n}$, recovering the original message $b_1 \ b_2 \ \dots \ b_m$. This is the decryption phase.	$d = 1153$ $962^{1153} \equiv 805 \pmod{2929}$ $1053^{1153} \equiv 121 \pmod{2929}$ $1491^{1153} \equiv 215 \pmod{2929}$

The RSA decryption is based on Theorem 15.6.

15.2 The mathematics behind RSA

Recall the following theorem.

Theorem 15.1 (Fermat's Little Theorem). *If $b, p \in \mathbb{Z}$ are such that p is a prime integer and p does not divide b then $b^{p-1} \equiv 1 \pmod{p}$.*

Exercise 15.2. Prove:

Lemma 15.3. *If $b, c, p \in \mathbb{Z}$ are such that p is a prime integer and $c \equiv 1 \pmod{p-1}$, then $b^c \equiv b \pmod{p}$.*

Exercise 15.4. Prove: if p and q are positive prime integers such $p \neq q$ and a is an integer which satisfies $p \mid a$ and $q \mid a$, then $(pq) \mid a$.

Exercise 15.5. Prove the following

Theorem 15.6. *If p, q are positive primes, $c \equiv 1 \pmod{(p-1)(q-1)}$ and b is an integer, then $b^c \equiv b \pmod{pq}$.*

15.3 Challenge Example

1. I have encrypted a message using Bob's public key from above $n = 2929, 3 = 17$. It reads

0 0876 2753 2095 1698 0835 0076 0885 0581 1865 0672 0612 0128 1282 0128 2311

Can you decrypt my message? You may use a computer program which can compute with modular arithmetic. For example google "Wolfram Alpha mod calculator".

2. Now suppose that Bob's public key was $n = 00071151151044511411597000310100141105900164614953131181600135601007229419223712775518982103014624262359480648127533339110476675929546676148994202136112137775146436093786329234224308648775144851838454788951454019331894962103495323569873087949110089541073341437136926387315720915581301061468328506421776242736895943798848997261371665116063864239010347124141261196388661588618893604009512727286113134485865497632411137772258274566471625091446479821017638436378874928609431161098191567710910431277064261287255531237181190460145565741502115182811426093455895257646602259657961239115169414662110180344284929653014399726397831021010031121137717331052475543035581434933570364734343226685506453325008883471033436611039, e = 84096$

Would you be able to decode a message sent to Bob? Why (not)?