

MATH 2150: HIGHER ARITHMETIC



Pamini Thangarajah
Mount Royal University

00: Front Matter

This page was auto-generated because a user created a sub-page to this page.

Higher Arithmetic

Pamini Thangarajah, PhD.

Mount Royal University

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (<https://LibreTexts.org>) and like the thousands of other texts available within this powerful platform, it is freely available for reading, printing, and "consuming."

The LibreTexts mission is to bring together students, faculty, and scholars in a collaborative effort to provide an accessible, and comprehensive platform that empowers our community to develop, curate, adapt, and adopt openly licensed resources and technologies; through these efforts we can reduce the financial burden born from traditional educational resource costs, ensuring education is more accessible for students and communities worldwide.

Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects. Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.



LibreTexts is the adaptable, user-friendly non-profit open education resource platform that educators trust for creating, customizing, and sharing accessible, interactive textbooks, adaptive homework, and ancillary materials. We collaborate with individuals and organizations to champion open education initiatives, support institutional publishing programs, drive curriculum development projects, and more.

The LibreTexts libraries are Powered by [NICE CXone Expert](#) and was supported by the Department of Education Open Textbook Pilot Project, the California Education Learning Lab, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptations contact info@LibreTexts.org or visit our main website at <https://LibreTexts.org>.

This text was compiled on 05/02/2025

TABLE OF CONTENTS

00: Front Matter

- TitlePage
- InfoPage
- Table of Contents
- Licensing

Licensing

Preface

0: Preliminaries

- 0.1: Basics
- 0.2: Introduction to Proofs/Contradiction
- 0.3: Proof Do's and Dont's
- 0.4: Egyptian Multiplication and Division (optional)
- 0.E: Exercises

1: Binary operations

- 1.1: Binary operations
- 1.2: Exponents and Cancellation
- 1.E: Exercises

2: Binary relations

- 2.1: Binary Relations
- 2.2: Equivalence Relations, and Partial order
- 2.3: Arithmetic of inequality
- 2.4: Arithmetic of divisibility
- 2.5: Divisibility Rules
- 2.6: Division Algorithm
- 2.E: Exercises

3: Modular Arithmetic

- 3.1: Modulo Operation
- 3.2: Modulo Arithmetic
- 3.3: Divisibility rules revisited
- 3.E: Exercises

4: Greatest Common Divisor, least common multiple and Euclidean Algorithm

- 4.1: Greatest Common Divisor
- 4.2: Euclidean algorithm and Bezout's algorithm
- 4.3: Least Common Multiple
- 4.4: Relatively Prime numbers
- 4.5: Linear Congruences
- 4.E: Exercises

5: Diophantine Equations

- [5.1: Linear Diophantine Equations](#)
- [5.2 : Linear Congruences Revisted](#)
- [5.3: Non-Linear Diophantine Equations](#)
- [5.E: Exercises](#)

6: Prime numbers

- [6.1: Prime numbers](#)
- [6.2: GCD, LCM and Prime factorization](#)
- [6.3: Fermat Primes, Mersenne Primes and Primes of the other forms](#)
- [6.E: Prime Numbers \(Exercises\)](#)

7: Numeration Systems

- [7.1: Historical numeral systems](#)
- [7.2: Number Bases](#)
- [7.3: Unusual Number systems](#)
- [7.E: Exercises](#)
- [Index](#)
- [Glossary](#)
- [Detailed Licensing](#)

8: Rational numbers, Irrational Numbers, and Continued fractions

- [8.1: Rational numbers](#)
- [8.2: Irrational Numbers](#)
- [8.3: Continued fractions](#)
- [8.E: Exercises](#)

Mock exams

- [Sample Final](#)
- [Sample term test](#)

Notations

- [Notations](#)

[Index](#)

[Glossary](#)

[Detailed Licensing](#)

[Reference](#)

Licensing

A detailed breakdown of this resource's licensing can be found in [Back Matter/Detailed Licensing](#).

Preface

To those teaching this course:

Course Description:

This course explores elementary number theory, numeration systems, operations on integers and rational numbers, and elementary combinatorics, using both inductive and deductive methods. Emphasis will be placed on the development of clarity and understanding of mathematical processes and ideas, the application of these ideas to problem-solving and the communication of these ideas to other people.

This course is one of the required courses for the Minor in Mathematics for Elementary Education program at Mount Royal University (MRU) and was designed especially for elementary education students. The purpose of this course is to introduce future elementary (grades K-6) educators to elementary number theory. The relationship of concepts to the elementary mathematics curriculum is emphasized. We started offering this course in Winter 2014. I have been teaching this course since its inception. I have created these lecture notes to facilitate student learning. This course partially fulfills the need for mathematics to be taught as a language with reasoning and gives students number sense.

Course Learning Outcomes:

Upon successful completion of this course, students will be able to:

- show knowledge of fundamental concepts in mathematics,
- encourage mathematical investigations,
- demonstrate an understanding of elementary number theory,
- reflect major algebraic ideas such as algebra as a set of rules and procedures; algebra as the study of structures; algebra as the study of the relationship among quantities,
- do problem-solving by using number theory, and
- perform mathematical calculations that use modulo operations and different number bases.

Course topics and tentative schedule:

Week	Chapter(s)
1	1
2,3	2
3,4	3
4,5	4
7,8	5
9,10	6
11	7
12	8

To those taking this course:

A Note on Formatting:

Throughout this resource, practice exercises can be found at the end of each chapter. No answer key is provided. This is to encourage students to experience mathematics as a synthetic and creative field and also to attend class to ask questions. The "Thinking Out Loud" sections are to prompt discussion - take these up with your classmates and see if you can justify your position using what you know.

Acknowledgements:

The creation of this resource would not have been possible without significant help from a variety of sources. They are, in no particular order,

- Professor Delmar Larsen, LibreTexts, for his unconditional support,
- The Department of Mathematics and Computing, Mount Royal University,
- Faculty of Science and Technology, and
- Former students, who have taken this class in person, and who donated their class notes as reference material.
- Undergraduate research assistant Dallas Daniel.
- Undergraduate student James Bergeron.

Thank you all, so very much, for your help, insights, and resources.

Pamini Thangarajah, PhD

Calgary, Alberta

November 2017, edited in December 2019, April 2022

Contact:

If you find any error(s), please contact me via email: pthangarajah@mtroyal.ca.

CHAPTER OVERVIEW

0: Preliminaries

Some definitions, notation, and results that are used throughout this text are introduced in this chapter for convenience.

Topic hierarchy

[0.1: Basics](#)

[0.2: Introduction to Proofs/Contradiction](#)

[0.3: Proof Do's and Dont's](#)

[0.4: Egyptian Multiplication and Division \(optional\)](#)

[0.E: Exercises](#)

This page titled [0: Preliminaries](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

0.1: Basics

Mathematical objects come into existence by definitions. These definitions must give an absolutely clear picture of the object or concept. We don't need to prove them; we simply need to define them clearly. We are going to state some basic facts that are needed in this course:

Basic Facts on Sets:

- The collection of **counting numbers**, otherwise known as the collection of **natural numbers**, is usually denoted by $\mathbb{N}$. We write $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.
- The collection of the **integers** is usually denoted by $\mathbb{Z}$ and we write $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$.
- The collection of the positive **integers** is usually denoted by $\mathbb{Z}_+$ and we write $\mathbb{Z}_+ = \{1, 2, 3, 4, \dots\}$.
- The collection of the negative **integers** is usually denoted by $\mathbb{Z}_-$ and we write $\mathbb{Z}_- = \{-1, -2, -3, -4, \dots\}$.
- The collection of all **rational numbers** (fractions) is usually denoted by $\mathbb{Q}$, and we write $\mathbb{Q} = \{\frac{a}{b} : a \text{ and } b \text{ are integers, } b \neq 0\}$.
- The collection of all **irrational numbers** is denoted by $\mathbb{Q}^c$.
- The collection of all **real numbers** is denoted by $\mathbb{R}$. This set contains all of the rational numbers and all of the irrational numbers.

Basic Facts:

We shall assume the use of the usual addition, subtraction, multiplication, and division as operations and inequalities ($<$, $>$, $\leq$, $\geq$) and equality ($=$), are relations on $\mathbb{R}$.

1. The distributive law: If a, b and c are real numbers, then $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.
2. The commutative law: If a and b are real numbers, then $ab = ba$ and $a + b = b + a$.
3. The associative law: If a, b and c are real numbers, then $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$.
4. The existence of 0: The real number 0 exists so that, for any real number a , $a + 0 = 0 + a = a$.
5. The existence of 1: The real number 1 exists so that, for any real number a , $a \cdot 1 = 1 \cdot a = a$.
6. Subtraction: For each real number a , there exists a real number $-a$, so that $a + (-a) = 0 = (-a) + a$.
7. Division: For each nonzero real number a , there exists a real number $\frac{1}{a}$, so that $a(\frac{1}{a}) = (\frac{1}{a})a = 1$.

The laws above form the foundation of arithmetic and algebra of real numbers. They are the laws that we have accepted and used with no reserve. They are mentioned here to encourage the reader to develop an appreciation for them and an awareness that they must be respected in all calculations involving real numbers. Further, there are rules of precedence which help us to calculate any valid arithmetic expression. For example, if given the following $6 \div 2 \times 5 - \frac{7}{5} - 3$, we will apply the rule to calculate.

Example 0.1.1:

Evaluate $6 \div 2 \times 5 - \frac{7}{5} - 3$.

Solution

$$6 \div 2 \times 5 - \frac{7}{5} - 3 = ((6 \div (2 \times 5)) - (7 \div 5)) - 3 = -\frac{16}{5}.$$

Rules of Precedence

1. Functions are evaluated first.
2. Expressions inside parentheses or brackets are evaluated next.
3. Multiplication and division are next and evaluated left to right.
4. Addition and subtraction are last and are evaluated left to right.

In short form:

Order of Operations

B Brackets

E Exponents

D Division

M Multiplication

An Addition

S Subtraction

Recall that, if a and b are real numbers or $a, b \in \mathbb{R}$ as written in mathematical language, then

1. $a < b$ means that a is less than b .
2. $a > b$ means that a is greater than b .

Definitions:

1. A real number is positive if greater than 0.
2. A real number is called non-negative if it is greater than or equal to 0.
3. An integer n is an even number if there is an integer m such that $n = 2m$.
4. An integer n is an odd number if there is an integer m such that $n = 2m + 1$.
5. An integer a is said to be divisible by an integer b if there is an integer m such that $a = bm$. In this case, we can say that b divides a and is denoted $b|a$. Further, b is called a divisor (factor) of a .
6. A positive integer p is called prime if $p > 1$ and the only positive divisors of p are 1 and p .
7. A positive integer n is called composite if there is a positive integer m such that $1 < m < n$ and $m|n$.

Note

Note that 1 is neither prime nor composite.

Axioms for Inequalities

The following are axioms for inequalities:

- Trichotomy Law: if x and y are real numbers, then one and only one of the three statements $x < y$, $x = y$ and $y < x$ is true.
- Transitivity: if x, y and z are real numbers and if $x < y$ and $y < z$ then $x < z$.
- if x, y and z are real numbers and if $x < y$ then $x + z < y + z$.
- if x and y are real numbers which satisfy $0 < x$ and $0 < y$ then $0 < xy$.

Definition:

A theorem is a declarative statement about mathematics for which there is proof.

This page titled [0.1: Basics](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

0.2: Introduction to Proofs/Contradiction

In this section, we will explore different techniques of proving a mathematical statement "If p then q ." ($p \rightarrow q$).

0.2.1 From DR. THI DINH'S PROOF WRITING HANDBOOK THIS BIBLE:

0.2.1.0.1 In the beginning...

Let P and Q be statement variables. When needed, suppose that $P = P(x)$ depends on a variable x . The symbol " $\forall$ " means "for all" or "for any". The symbol $\exists$ means "there exists".

Type of statement	What must we do to prove that it is true
(1) If P , then Q	Suppose that P is true.
(2) $\forall P, Q$	Prove that Q is true.
(3) $\exists x P(x)$ such that Q	Choose x so that $P(x)$ is true. Prove that Q is true. Note: You need not explain how you find x .

0.2.1.0.1 The first (and only) commandment

To prove that a statement is **false**, thou shalt **write out the negation of the statement and prove that**.

0.2.1.0.1 The five cardinal sins

- When proving any of the types of statements (1), (2), or (3):
- Thou shalt not:** suppose that Q is true.
 - Thou shalt not:** overuse symbols and violate the rules of English grammar. You must write in full sentences and use symbols correctly.
- When proving a statement of the form (2) P, Q :
- Thou shalt not:** choose or exhibit an example in place of a proof.
- When proving a statement of the form (3) " $\forall x P(x)$ such that Q ":
- Thou shalt not:** attempt to construct all possible x so that $P(x)$ and Q are true.
- When proving a statement by contradiction:
- Thou shalt not:** claim a contradiction has been reached without explanation. You must clearly identify the contradiction being made by making a statement of the form " P and NOT P , which is a contradiction".

0.2.2 Direct Proof

In this technique, we shall assume p and show that q is true.

Theorem 0.2.1

Let n be an integer. If n is even then n^2 is even.

Proof

Assume that n is even. Then $n = 2m$ for some integer m .

Consider $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$. Since m is an integer, $(2m^2)$ is an integer.

Thus n^2 is even.

Example 0.2.1

Show that for all integers n , if n is odd then n^2 is odd.

Answer

Assume that n is odd. Then $n = 2m + 1$ for some integer m .

Consider $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.

Since m is an integer, $(2m^2 + 2m)$ is an integer.

Thus n^2 is odd.

0.2.3 Proof by Contrapositive

In this technique, we shall assume $\neg p$ and show that $\neg q$ is true.

Theorem 0.2.2

Let n be an integer. If n^2 is even then n is even.

Proof

We shall prove this statement by assuming n is odd. Then $n = 2m + 1$ for some integer m .

Consider $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.

Since m is an integer, $(2m^2 + 2m)$ is an integer.

Thus n^2 is odd.

Example 0.2.2

Show that for all integers n , if n^2 is odd then n is odd.

Answer

We shall prove this statement by assuming n is even. Then $n = 2m$ for some integer m .

Consider $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Since m is an integer, $(2m^2)$ is an integer. Thus n^2 is even.

0.2.4 Proof by Contradiction

In this technique, we shall assume the negation of the given statement is true and come to a contradiction.

Theorem 0.2.3

$\sqrt{2}$ is irrational.

Proof

Assume that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{b}{a}$, where $b \in \mathbb{Z}$, $a \in \mathbb{Z} \setminus \{0\}$, with no common factors between a and b . Now, $\sqrt{2}a = b$. Then $2a^2 = b^2$. Since 2 divides $2a^2$, 2 divides b^2 . Thus b^2 is even. Therefore, b is even (by theorem 2). Since b is even, 2 divides b . Therefore, 2^2 divides b^2 .

Since $2a^2 = b^2$, 2^2 divides $2a^2$. Therefore, 2 divides a^2 . Which implies a is even. This contradicts the fact that a and b have no common factors. Thus $\sqrt{2}$ is irrational.

0.2.5 Proof by Counterexample

Example 0.2.3:

Decide whether the statement is true or false and justify your answer:

For all integers a, b, u, v , and $u \neq 0, v \neq 0$, if $au + bv = 0$ then $a = b = 0$.

Solution: The statement is false.

Counterexample: Choose $a = 1, b = -1, u = 2, v = 2$, then $au + bv = 0$, but $a \neq 0, b \neq 0, a \neq b$.

0.2.6 Proof by induction

In mathematics, we use induction to prove mathematical statements involving integers. There are two types of induction: regular and strong. The steps start the same but vary at the end. Here are the steps. In mathematics, we start with a statement of our assumptions and intent:

Let $p(n) \forall n \geq n_0, n, n_0 \in \mathbb{Z}$ be a statement. We would show that $p(n)$ is true for all possible values of n .

1. Show that $p(n)$ is true for the smallest possible value of n : In our case $p(n_0)$. **AND**
2. **For Regular Induction:** Assume that the statement is true for $n = k$, for some integer $k \geq n_0$. Show that the statement is true for $n = k + 1$.

OR

For Strong Induction: Assume that the statement $p(r)$ is true for all integers r , where $n_0 \leq r \leq k$ for some $k \geq n_0$. Show that $p(k+1)$ is true.

If these steps are completed, and the statement holds, we are saying that, by mathematical induction, we can conclude that the statement is true for all values of $n \geq n_0$.

Example 0.2.4:

Prove that $1 + 2 + \dots + n = \frac{n(n+1)}{2}, \forall n \in \mathbb{Z}$.

Solution:

Base step: Choose $n = 1$. Then L.H.S = 1 and R.H.S = $\frac{(1)(1+1)}{2} = 1$

Induction Assumption: Assume that $1 + 2 + \dots + k = \frac{k(k+1)}{2}$, for $k \in \mathbb{Z}$.

We shall show that $1 + 2 + \dots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}$

Consider,

$$\begin{aligned} 1 + 2 + \dots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= (k+1) \left(\frac{k}{2} + 1 \right) \\ &= (k+1) \left(\frac{k+2}{2} \right) \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Thus, by induction we have $1 + 2 + \dots + n = \frac{n(n+1)}{2}, \forall n \in \mathbb{Z}$.

Example 0.2.5

Prove $2^n > n + 4$ for $n \geq 3, n \in \mathbb{N}$.

Solution

Let $n = 3$. Then $2^3 > 3 + 4$ is true, since clearly $8 > 7$. Thus, the statement is true for $n = 3$.

Assume that $2^n > n + 4$ is true for some $n = k$.

We will show that $2^{k+1} > (k + 1) + 4$.

Consider $2^{k+1} = 2 \cdot 2^k > 2 \cdot (k + 4) = 2k + 8$.

Since $2k > k + 1$ and $8 > 4$, we have $2k + 8 > (k + 1) + 4$.

Thus the statement is true for all $n = k$.

By induction, $2^n > n + 4$ for all $n \geq 3, n \in \mathbb{Z}$. $\square$

This page titled [0.2: Introduction to Proofs/Contradiction](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

- [Current page](#) by [Pamini Thangarajah](#) is licensed [CC BY-NC-SA 4.0](#).
- [3.1: Proof by Induction](#) by [Pamini Thangarajah](#) is licensed [CC BY-NC-SA 4.0](#).

0.3: Proof Do's and Dont's

Do's:

1. Write the statement to be proved. It should be clear what you are proving.
2. Clearly mark the beginning of your proof with the word "*Proof*".
3. Make your proof self-contained. In particular, identify all variables used in your proof in the body of your proof.
4. Write proof in complete English sentences.

Example 0.3.1: Acceptable

Proof: Let $n \in \mathbb{Z}$. Assume n is an even integer. Then $n = 2k$, for some $k \in \mathbb{Z}$.

Example 0.3.2: Unacceptable

Proof: n is even $\implies 2k$.

5. Indicate what method of proof you are using. (The default assumption is that it is a direct proof).
6. Learn the definitions and how they come into play when proving various types of statements.

Don'ts:

1. Argue from examples. A general statement can't be proved true by showing it is true for special cases.
2. Use the same letter to mean two different things within a proof.

Example 0.3.3:

Proof: Let $n \in \mathbb{Z}$. Assume n is an even integer. Then $n = 2k$, for some $k \in \mathbb{Z}$. So $n^2 = 4K^2 = 2(2k^2)$. Thus $n^2 = 2k, k \in \mathbb{Z}$ is even. (The reader asks, does $n = n^2$?)

3. Assume what you are trying to prove. This is also known as begging the question. You can do it inadvertently in the middle of proof if you are not careful.

This page titled [0.3: Proof Do's and Dont's](#) is shared under a [CC BY-NC-ND 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

0.4: Egyptian Multiplication and Division (optional)

Duplation is a multiplication strategy that students can learn to help further develop their number sense and ability to multiply numbers. Duplation or also referred to as mediation can be dated back to being one of the earliest records of multiplication used by the Egyptians (Ancient Multiplication Methods, n.d. para.1). The Duplation strategy is explained through the example of 14×12 shown below:

Example 0.4.1:

Evaluate 14×12 .

Solution

1. Start with 1 and the other number, and double them.
2. Keep doubling until the left-hand column is going to be bigger than the other number 14
3. Since 16 is bigger than 14, stop there. See the table below.

1	12
2	24
4	48
8	96
16	

4. Use the left column numbers to add to $14 = 8 + 4 + 2$ and add the corresponding numbers on the right $96 + 48 + 24 = 168$ to get the product

- Why does this work? What you're really doing is adding the appropriate doubles: 96 is eight 12s, 48 is four 12s, and 24 is two 12s. So when you add them you get 14 12s.

The division is similar - demonstrates Egyptian knowledge that division and multiplication are reciprocal operations, like addition and subtraction.

Example 0.4.2:

Evaluate $\frac{153}{21}$.

Solution

List the powers of 2 in a column. List the divisor beside the 1, and double it down the second column until the number approaches, but does not exceed the dividend.

1	21
2	42
4	84

- Subtract the largest possible right-column number from the dividend, noting which ones are used, until it is no longer possible: $153 - 84 = 69$, $69 - 42 = 27$, $27 - 21 = 6$.
- The quotient is the sum of the left-hand column numbers associated with the subtracted quantities: So, since we used 84, 42, and 21, the quotient is $4 + 2 + 1 = 7$.
- The remainder is the result of the subtractions: 7 remainder 6.

See [Egyptian fraction](#).

This page titled [0.4: Egyptian Multiplication and Division \(optional\)](#) is shared under a [not declared](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

0.E: Exercises

Exercise 0.E.1

Solve the following:

1. $\frac{2 \times 5}{2+3}$

Answer

2.

Exercise 0.E.2

Prove or disprove: There is a largest integer.

Answer

Hint: use proof by contradiction.

Exercise 0.E.3

Use Egyptian multiplication to calculate 12×13 .

Answer

- List powers of two in increasing order in a column without going over one chosen factor (12 in this exercise):
- List the other factor (13 in this exercise) next to the 1, and double for each cell underneath:
- Choose the rows that add up to the first, chosen, factor (12 in this exercise):

1	13
2	26
4	52
8	104

- Add the two numbers in the right-hand column to get the answer:
 - $52 + 104 = 156$. $12 \times 13 = 156$.
 - This is because of the distributive property of multiplication. Since $12 \times 13 = (4 + 8) \times 13 = (4 \times 13) + (8 \times 13)$, this all works out. Also, the right-hand column is just saving time: doubling a quantity is much easier than multiplying it by 4 or 8 or 16 etc.

This page titled 0.E: Exercises is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by [Pamini Thangarajah](https://math.libretexts.org/@go/page/18153).

CHAPTER OVERVIEW

1: Binary operations

In this chapter, we will explore binary operations and properties of binary operations. Most of the properties we have used already. However, we will study formally.

Topic hierarchy

[1.1: Binary operations](#)

[1.2: Exponents and Cancellation](#)

[1.E: Exercises](#)

Thumbnail By This vector image was created with Inkscape by Elembis, and then manually replaced. (Own work) [Public domain], via Wikimedia Commons

This page titled [1: Binary operations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

1.1: Binary operations

Binary operation

Definition: Binary operation

Let S be a non-empty set, and $\star$ said to be a binary operation on S , if $a \star b$ is defined for all $a, b \in S$. In other words, $\star$ is a rule for any two elements in the set S .

Example 1.1.1:

The following are binary operations on $\mathbb{Z}$:

1. The arithmetic operations, addition $+$, subtraction $-$, multiplication $\times$, and division $\div$.
2. Define an operation oplus on $\mathbb{Z}$ by $a \oplus b = ab + a + b, \forall a, b \in \mathbb{Z}$.
3. Define an operation ominus on $\mathbb{Z}$ by $a \ominus b = ab + a - b, \forall a, b \in \mathbb{Z}$.
4. Define an operation otimes on $\mathbb{Z}$ by $a \otimes b = (a + b)(a + b), \forall a, b \in \mathbb{Z}$.
5. Define an operation oslash on $\mathbb{Z}$ by $a \oslash b = (a + b)(a - b), \forall a, b \in \mathbb{Z}$.
6. Define an operation min on $\mathbb{Z}$ by $a \vee b = \min\{a, b\}, \forall a, b \in \mathbb{Z}$.
7. Define an operation max on $\mathbb{Z}$ by $a \wedge b = \max\{a, b\}, \forall a, b \in \mathbb{Z}$.
8. Define an operation defect on $\mathbb{Z}$ by $a *_3 b = a + b - 3, \forall a, b \in \mathbb{Z}$.

Lets explore the binary operations, before we proceed:

Example 1.1.2:

1. $2 \oplus 3 = (2)(3) + 2 + 3 = 11$.
2. $2 \otimes 3 = (2 + 3)(2 + 3) = 25$.
3. $2 \oslash 3 = (2 + 3)(2 - 3) = -5$.
4. $2 \ominus 3 = (2)(3) + 2 - 3 = 5$.
5. $2 \vee 3 = 2$.
6. $2 \wedge 3 = 3$.

Exercise 1.1.2

1. $-2 \oplus 3$.
2. $-2 \otimes 3$.
3. $-2 \oslash 3$.
4. $-2 \ominus 3$.
5. $-2 \vee 3$.
6. $-2 \wedge 3$.

Properties:

Closure property

Definition: Closure

Let S be a non-empty set. A binary operation $\star$ on S is said to be a closed binary operation on S , if $a \star b \in S, \forall a, b \in S$.

Below we shall give some examples of closed binary operations, that will be further explored in class.

Example 1.1.3: Closed binary operations

The following are closed binary operations on $\mathbb{Z}$.

1. The addition $+$, subtraction $-$, and multiplication $\times$.
2. Define an operation oplus on $\mathbb{Z}$ by $a \oplus b = ab + a + b, \forall a, b \in \mathbb{Z}$.

3. Define an operation ominus on $\mathbb{Z}$ by $a \ominus b = ab + a - b, \forall a, b \in \mathbb{Z}$.
4. Define an operation otimes on $\mathbb{Z}$ by $a \otimes b = (a + b)(a + b), \forall a, b \in \mathbb{Z}$.
5. Define an operation oslash on $\mathbb{Z}$ by $a \oslash b = (a + b)(a - b), \forall a, b \in \mathbb{Z}$.
6. Define an operation min on $\mathbb{Z}$ by $a \vee b = \min\{a, b\}, \forall a, b \in \mathbb{Z}$.
7. Define an operation max on $\mathbb{Z}$ by $a \wedge b = \max\{a, b\}, \forall a, b \in \mathbb{Z}$.
8. Define an operation defect on $\mathbb{Z}$ by $a *_3 b = a + b - 3, \forall a, b \in \mathbb{Z}$.

Exercise 1.1.1

Determine whether the operation ominus on $\mathbb{Z}_+$ is closed?

Example 1.1.4: Counter Example

Division ($\div$) is not a closed binary operations on $\mathbb{Z}$.

$2, 3 \in \mathbb{Z}$ but $\frac{2}{3} \notin \mathbb{Z}$.

Summary of arithmetic operations and corresponding sets:

	+	$\times$	-	$\div$
$\mathbb{Z}_+$	closed	closed	not closed	not closed
$\mathbb{Z}$	closed	closed	closed	not closed
$\mathbb{Q}$	closed	closed	closed	closed (only when 0 is not included)
$\mathbb{R}$	closed	closed	closed	closed (only when 0 is not included)

Associative property

Definition: Associative

Let S be a subset of $\mathbb{Z}$. A binary operation $\star$ on S is said to be associative, if $(a \star b) \star c = a \star (b \star c), \forall a, b, c \in S$.

We shall assume the fact that the addition (+) and the multiplication ($\times$) are associative on $\mathbb{Z}_+$. (**You don't need to prove them!**).

Below is an example of proof when the statement is True.

Example 1.1.5: Associative

Determine whether the binary operation oplus is associative on $\mathbb{Z}$.

We shall show that the binary operation oplus is associative on $\mathbb{Z}$.

Below is an example of how to disprove when a statement is False.

Example 1.1.6: Not Associative

Determine whether the binary operation subtraction ($-$) is associative on $\mathbb{Z}$.

Answer: The binary operation subtraction ($-$) is not associative on $\mathbb{Z}$.

Commutative property

Definition: Commutative property

Let S be a non-empty set. A binary operation $\star$ on S is said to be commutative, if $a \star b = b \star a, \forall a, b \in S$.

We shall assume the fact that the addition (+) and the multiplication($\times$) are commutative on $\mathbb{Z}_+$. (**You don't need to prove them!**).

Below is the proof of subtraction ($-$) NOT being commutative.

Example 1.1.7: NOT Commutative

Determine whether the binary operation subtraction $-$ is commutative on $\mathbb{Z}$.

Example 1.1.8: Commutative

Determine whether the binary operation oplus is commutative on $\mathbb{Z}$.

We shall show that the binary operation oplus is commutative on $\mathbb{Z}$.

Identity**Definition: Identity**

A non-empty set S with binary operation $\star$, is said to have an identity $e \in S$, if $e \star a = a \star e = a, \forall a \in S$.

Note that 0 is called additive identity on $(\mathbb{Z}, +)$, and 1 is called multiplicative identity on $(\mathbb{Z}, \times)$.

Example 1.1.9: Is identity unique?

Let S be a non-empty set and let $\star$ be a binary operation on S . If e_1 and e_2 are two identities in $(S, \star)$, then $e_1 = e_2$.

Proof:

Suppose that e_1 and e_2 are two identities in $(S, \star)$.

Then $e_1 = e_1 \star e_2 = e_2$.

Hence identity is unique. $\square$

Example 1.1.10: Identity

Does $(\mathbb{Z}, \oplus)$ have an identity?

Example 1.1.11:

Does $(\mathbb{Z}, \otimes)$ have an identity?

Distributive Property**Definition: Distributive property**

Let S be a non-empty set. Let $\star_1$ and $\star_2$ be two different binary operations on S .

Then $\star_1$ is said to be distributive over $\star_2$ on S if $a \star_1 (b \star_2 c) = (a \star_1 b) \star_2 (a \star_1 c), \forall a, b, c, \in S$.

Note that the multiplication distributes over the addition on $\mathbb{Z}$. That is, $4(10 + 6) = (4)(10) + (4)(6) = 40 + 24 = 64$.

Further, we extend to $(a + b)(c + d) = ac + ad + bc + bd$ (FOIL).

F-First

O-Outer

I-Inner

L-Last

This property is very useful to find $(26)(27)$ as shown below:

Example 1.1.12: Find $(26)(27)$

	20	6
20	400	120
7	140	42

Hence $(26)(27) = 400 + 120 + 140 + 42 = 702$.

Let's play a game!

Example 1.1.13:

Does multiplication distribute over subtraction?

Example 1.1.14:

Does division distribute over addition?

Example 1.1.15:

Does $\otimes$ distribute over $\oplus$ on $\mathbb{Z}$?

Summary

In this section, we have learned the following for a non-empty set S :

1. Binary operation,
2. Closure property,
3. Associative property,
4. Commutative property,
5. Distributive property, and
6. Identity.

This page titled [1.1: Binary operations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

1.2: Exponents and Cancellation

Definition: Inverse

Let S be a set with a binary operation $\star$, and with identity e . Let $a \in S$, then $b \in S$ is called an inverse of a if $a \star b = b \star a = e$.

Example 1.2.1:

1. For every $a \in \mathbb{Z}$, $-a$ is the inverse of a with the operation $+$.
2. For every $a \in \mathbb{R} \setminus \{0\}$, $a^{-1} = \frac{1}{a}$ is the inverse of a with the multiplication.

Cancellation law

Let S be a set with a binary operation $\star$. If for any $a, b, c \in S$, $a \star b = a \star c$ then $b = c$

Example 1.2.2:

$(1)(0) = (3)(0) = 0$, but $1 \neq 3$.

Example 1.2.3:

1. For any $a, b, c \in \mathbb{Z}$, $a + b = a + c$ then $b = c$.
2. For any $a, b, c \in \mathbb{Z}$ and $a \neq 0$, $ab = ac$ then $b = c$.

Example 1.2.4:

If $ab = 0$ then $a = 0$ or $b = 0$.

Theorem 1.2.1

For any integers a , and b , the following are true.

1. $-(-a) = a$.
2. $0(a) = 0$.
3. $(-a)b = -ab$.
4. $(-a)(-b) = ab$.

Proof

1. Let $a \in \mathbb{Z}$. Since $-a$ is the inverse of a , $a + (-a) = (-a) + a = 0$. Therefore the additive inverse of $-a$ is a .

Thus $-(-a) = a$.

2. Let $a \in \mathbb{Z}$. Then by distributive law, $0a + 0a = (0 + 0)a = 0a = 0a + 0$. Now by cancellations law, $0a = 0$.

3. Let $a, b \in \mathbb{Z}$. By distributive law, $((-a) + a)b = (-a)b + ab$. Since $-a$ is the additive inverse of a , $(-a) + a = 0$. By (2), $0 = (-a)b + ab$. Thus $(-a)b$ is the additive inverse of ab . Hence $-ab = (-a)b$.

4. Let $a, b \in \mathbb{Z}$. Since $(-a)(-b) + (-a)b = (-a)(-b + b) = (-a)(0) = 0$. Hence $(-a)(-b)$ is the additive inverse of $(-a)b$. But ab is the additive inverse of $-ab$. Thus by (3), we have $(-a)(-b) = ab$.

Definition: Exponentiation

For every a , $n \in \mathbb{Z}_+$, the binary operation exponentiation is denoted as a^n , defined as n copies of a .

Example 1.2.5:

$$2^3 = 8$$

Example 1.2.6:

1. Determine whether the exponentiation is associative?
2. Determine whether the exponentiation is commutative?

Solution

1. Since $(3^2)^3 = 9^3$ is not the same as $3^{2^3} = 3^8$, the exponentiation is not associative.
2. Since $3^2 = 9$ is not the same as $2^3 = 8$, the exponentiation is not commutative.

Theorem 1.2.2

The exponentiation is distributive over multiplication. That is $(ab)^n = a^n b^n, \forall a, b, n \in \mathbb{Z}$.

Proof

Since multiplication is associative, the result follows.

Example 1.2.7:

Prove that $a^m a^n = a^{m+n}, \forall a, m, n \in \mathbb{Z}$.

Example 1.2.8:

Prove that $(a^m)^n = a^{mn}, \forall a, m, n \in \mathbb{Z}$.

This page titled [1.2: Exponents and Cancellation](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

1.E: Exercises

Exercise 1.E.1: Binary operations

Evaluate the following:

1. $3 \oplus 4$
2. $3 \ominus 4$
3. $3 \oslash 4$
4. $3 \otimes 4$

Exercise 1.E.2: Ominus

For $a, b \in \mathbb{Z}$, define an operation $\ominus$, by $a \ominus b = ab + a - b$. Determine whether $\ominus$ on $\mathbb{Z}$,

1. is closed,

Answer

Proof:

Let $a, b \in \mathbb{Z}$.

Then consider $a \ominus b = ab + a - b$.

Since $\cdot$, $+$ and $-$ are closed on $\mathbb{Z}$, ab , $(ab) + a$, and $(ab + a) - b$ are in $\mathbb{Z}$.

Hence $a \ominus b \in \mathbb{Z}$.

Thus, the binary operation is closed on $\mathbb{Z}$. ☐

2. is commutative,

Answer

Counterexample:

Choose $a = 3$ and $b = 4$.

Then consider $3 \ominus 4 = (3)(4) + 3 - 4 = 12 + 3 - 4 = 15 - 4 = 11$.

Now consider $4 \ominus 3 = (4)(3) + 4 - 3 = 12 + 4 - 3 = 16 - 3 = 13$.

Since $11 \neq 13$, the binary operation $\ominus$ is not commutative on $\mathbb{Z}$.

3. is associative,

Answer

Counterexample:

Choose $a = 3$, $b = 4$, $c = 2$.

Then consider $(3 \ominus 4) \ominus 2 = [(3)(4) + 3 - 4] \ominus 2 = 11 \ominus 2 = (11)(2) + 11 - 2 = 22 + 11 - 2 = 31$.

Now consider, $3 \ominus (4 \ominus 2) = 3 \ominus [(4)(2) + 4 - 2] = 3 \ominus 10 = (3)(10) + 3 - 10 = 30 + 3 - 10 = 23$.

Since $31 \neq 23$, the binary operation is not associative on $\mathbb{Z}$. ☐

4. has an identity.

Answer

Let e be the identity on $\mathbb{Z}$. Then $a \ominus e = e \ominus a = a$, $a \in \mathbb{Z}$.

Now consider, $a \ominus e = e \ominus a$.

$$ae + a - e = ea + e - a.$$

$$ae - ea + 2a = 2e.$$

$$ae = ea \text{ since } \cdot \text{ is commutative on } \mathbb{Z}.$$

Thus, $e = a$.

Now consider $ae = ae + a - e = a$.

If $e = a$, then $a^2 = a$, $a \in \mathbb{Z}$.

This is a contradiction.

Thus, $(\mathbb{Z}, \ominus)$ has no identity.

Exercise 1.E.3: Oplus

For $a, b \in \mathbb{Z}$, define an operation $\oplus$, by $a \oplus b = ab + a + b$. Determine whether $\oplus$ on $\mathbb{Z}$,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

What happens to the result for the above questions, if we change the set to $\mathbb{Z} \setminus \{-1\}$?

Exercise 1.E.4: Oslash

For $a, b \in \mathbb{Z}$, define an operation $\oslash$, by $a \oslash b = (a + b)(a - b)$. Determine whether $\oslash$ on $\mathbb{Z}$,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Exercise 1.E.5: Otimes

For $a, b \in \mathbb{Z}$, define an operation $\otimes$, by $a \otimes b = (a + b)(a + b)$. Determine whether $\otimes$ on $\mathbb{Z}$,

1. is closed,

Answer

Proof:

Let $a, b \in \mathbb{Z}$. Then consider, $a \otimes b = (a + b)(a + b)$.

since $\cdot$ is commutative on $\mathbb{Z}$, $(a + b)(a + b) = a^2 + 2ab + b^2$. Since $\cdot$, $+$ are closed on $\mathbb{Z}$, $a^2, 2ab, b^2, a^2 + 2ab$, and $(a^2 + 2ab) + b^2 \in \mathbb{Z}$.

Hence, $a^2 + 2ab + b^2 \in \mathbb{Z}$. Thus $a \otimes b \in \mathbb{Z}$.

Therefore, the binary operation $\otimes$ is closed on $\mathbb{Z}$. ☐

2. is commutative,

Answer

Proof:

Let $a, b \in \mathbb{Z}$. Then consider, $a \otimes b = (a + b)(a + b) = a^2 + 2ab + b^2 = b^2 + 2ba + a^2 = (b + a)(b + a) = b \otimes a$.

Therefore, the binary operation $\otimes$ is commutative on $\mathbb{Z}$. ☐

3. is associative,

Answer**Counterexample:**

Choose $a = 2, b = 3, c = 4$.

Then consider, $(a \otimes b) \otimes c = ((2 + 3)(2 + 3)) \otimes 4 = 25 \otimes 4 = (25 + 4)(25 + 4) = 841$.

Now consider $a \otimes (b \otimes c) = 2 \otimes (3 + 4)(3 + 4) = 2 \otimes 49 = (2 + 49)(2 + 49) = 2601$.

Since $841 \neq 2601$, the binary operation $\otimes$ is not associative on $\mathbb{Z}$. ☐

4. has an identity.

Answer

Let e be the identity on $(\mathbb{Z}, \otimes)$.

Then consider, $a \otimes e = e \otimes a = a, \forall \mathbb{Z}$.

Now, $a = e \otimes a = (e + a)(e + a) = e(e + a) + a(e + a)$, since $\cdot$ is associative on $\mathbb{Z}$.

$a = e^2 + ea + ae + a^2 = e^2 + 2ae + a^2$. Then choose $a = 0$.

Thus, $e^2 = 0$, which implies $e = 0$.

Hence $a^2 = a, \forall \mathbb{Z}$. This is a contradiction.

Thus, $(\mathbb{Z}, \otimes)$ has no identity. ☐

Exercise 1.E. 6: Max

For $a, b \in \mathbb{Z}$, define an operation $\wedge$, by $a \wedge b = \max\{a, b\}$. Determine whether $\wedge$ on $\mathbb{Z}$,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Exercise 1.E. 7: Min

For $a, b \in \mathbb{Z}$, define an operation $\vee$, by $a \vee b = \min\{a, b\}$. Determine whether $\vee$ on $\mathbb{Z}$,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Exercise 1.E. 8: Defection

For $a, b \in \mathbb{Z}$, define an operation $\star_5$, by $a \star_5 b = a + b - 5$. Determine whether $\star_5$ on $\mathbb{Z}$,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Answer

is closed, is commutative, is associative, and has an identity.

Exercise 1.E.9: Distributive

Determine whether $\otimes$ is distributive over $\oplus$ on $\mathbb{Z}$.

Answer

Counterexample:

Choose $a = 2, b = 3, c = 4$.

Then consider $2 \otimes (3 \oplus 4) = 2 \otimes [(3)(4) + 3 + 4] = 2 \otimes 19 = (2 + 19)(2 + 19) = 441$.

Now consider $(2 \otimes 3) \oplus (2 \otimes 4) = [(2 + 3)(2 + 3)] \oplus [(2 + 4)(2 + 4)] = 25 \oplus 36 = (25)(36) + 25 + 36 = 961$.

Since $441 \neq 961$, the binary operation $\otimes$ is not distributive $\oplus$ over on $\mathbb{Z}$. ☐

Exercise 1.E.10: Distributive

Determine whether $\oslash$ is distributive over $\oplus$ on $\mathbb{Z}$.

Exercise 1.E.11: Even Multiplication

Let $S = \{1, 2, 4, 6, \dots\}$, that is S is the set of all even positive integers and 1. Use the multiplication $\times$ as the binary operation.

Determine whether the multiplication $\times$ on S ,

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Exercise 1.E.12: Arithmetic operations on Rationals and Irrationals

1. Is addition closed on $\mathbb{Q}$?
2. Is multiplication closed on $\mathbb{Q}$?
3. Is addition closed on $\mathbb{Q}^c$?
4. Is multiplication closed on $\mathbb{Q}^c$?

This page titled 1.E: Exercises is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

CHAPTER OVERVIEW

2: Binary relations

In this chapter, we will explore binary relation and the properties of binary relations.

Topic hierarchy

- 2.1: Binary Relations
- 2.2: Equivalence Relations, and Partial order
- 2.3: Arithmetic of inequality
- 2.4: Arithmetic of divisibility
- 2.5: Divisibility Rules
- 2.6: Division Algorithm
- 2.E: Exercises

Thumbnail picture By Function_color_example_3.gif: Wvbailey. The original uploader was Wvbailey at English Wikipedia derivative work: Zerodamage [CC BY-SA 3.0 (<https://creativecommons.org/licenses/by-sa/3.0>) or GFDL (<http://www.gnu.org/copyleft/fdl.html>)], via Wikimedia Commons

This page titled 2: Binary relations is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

2.1: Binary Relations

Definition: Binary Relation

Let S be a non-empty set. Then any subset R of $S \times S$ is said to be a relation over S . In other words, a relation is a rule that is defined between any two elements in S . Intuitively, if R is a relation over S , then the statement aRb is either **true** or **false** for all $a, b \in S$.

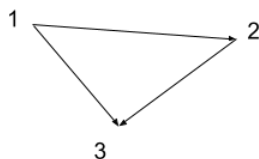
If the statement aRb is false, we denote this by $a \not R b$.

Example 2.1.1:

Let $S = \{1, 2, 3\}$. Define R by aRb if and only if $a < b$, for $a, b \in S$.

Then $1R2, 1R3, 2R3$ and $2 \not R 1$.

We can visualize the above binary relation as a graph, where the vertices are the elements of S , and there is an edge from a to b if and only if aRb , for $a, b \in S$.



The following are some examples of relations defined on $\mathbb{Z}$.

Example 2.1.2:

1. Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$.
2. Define R by aRb if and only if $a > b$, for $a, b \in \mathbb{Z}$.
3. Define R by aRb if and only if $a \leq b$, for $a, b \in \mathbb{Z}$.
4. Define R by aRb if and only if $a \geq b$, for $a, b \in \mathbb{Z}$.
5. Define R by aRb if and only if $a = b$, for $a, b \in \mathbb{Z}$.

Multiples and divisors

Next, we will introduce the notion of "divides."

Definition: Divisor/Divides

Let a and b be integers. We say that a divides b is denoted $a \mid b$, provided we have an integer m such that $b = am$. In this case we can also say the following:

- b is divisible by a
- a is a factor of b
- a is a divisor of b
- b is a multiple of a

If a does not divide b , then it is denoted by $a \nmid b$.

Example 2.1.3:

Find all positive integers divisible by 16.

Solution

Multiples of 16.

Example 2.1.4:

Find all positive integers divides 16.

Solution

1, 2, 4, 8, 16

Example 2.1.5:

$4 \mid 12$ and $12 \nmid 4$

Next, we will introduce the notion of "divides" for positive integers.

Definition: Divides

Let a and b be positive integers. We say that a divides b is denoted $a \mid b$, there exists a positive integer m such that $b = am$.

Theorem 2.1.1: Divisibility inequality theorem

If $a \mid b$, for $a, b \in \mathbb{Z}_+$ then $a \leq b$,

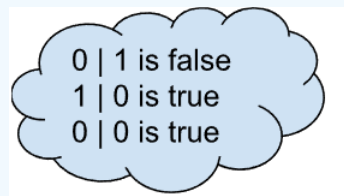
Proof

Let $a, b \in \mathbb{Z}_+$ such that $a \mid b$. Since $(a \mid b)$, there is a positive integer m such that $b = am$. Since $m \geq 1$ and a is a positive integer, $b = am \geq (a)(1) = a$.

Note that if $a \mid b$, for $a, b \in \mathbb{Z}_+$ then $a \leq b$, but the converse is not true. For example: $2 < 3$, but $2 \nmid 3$.

Example 2.1.6:

According to our definition $0 \mid 0$.



Definition: Even integer

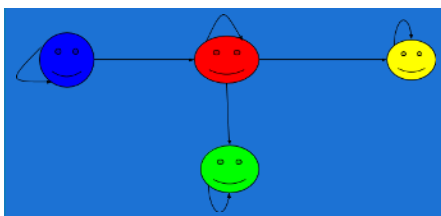
An integer is even provided that it is divisible by 2.

Properties of binary relation:

Definition: Reflexive

Let S be a set and R be a binary relation on S . Then R is said to be reflexive if $aRa, \forall a \in S$.

Example 2.1.5: Visually



$\forall a \in S, aRa$ holds.

We will follow the template below to answer the question about reflexive.

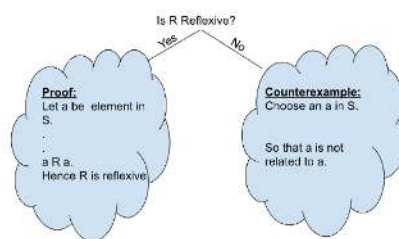


Figure 2.1.1: Reflexive.

Example 2.1.7:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R reflexive?

Counterexample:

Choose $a = 2$.

Since $2 \not< 2$, R is not reflexive.

Example 2.1.8:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}$. Is R reflexive?

Proof:

Let $a \in \mathbb{Z}$. Since $a = (1)(a)$, $a \mid a$.

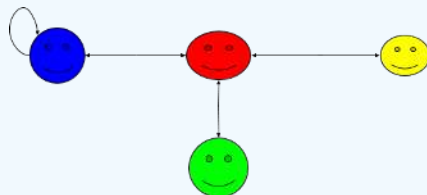
Thus R is reflexive. $\square$

Definition: Symmetric

Let S be a set and R be a binary relation on S . Then R is said to be symmetric if the following statement is true:

$\forall a, b \in S$, if aRb then bRa , in other words, $\forall a, b \in S, aRb \implies bRa$.

Example 2.1.8: Visually



$\forall a, b \in S, aRb \implies bRa$ holds!

We will follow the template below to answer the question about symmetric.

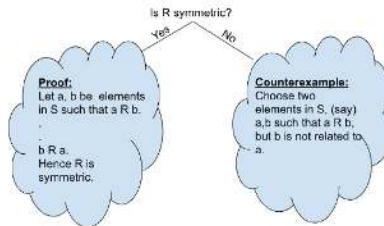


Figure 2.1.2: Symmetric.

Example 2.1.9:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R symmetric?

Counter Example:

$1 < 2$ but $2 \not< 1$.

Example 2.1.10:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}$. Is R symmetric?

Counterexample:

$2 \mid 4$ but $4 \nmid 2$.

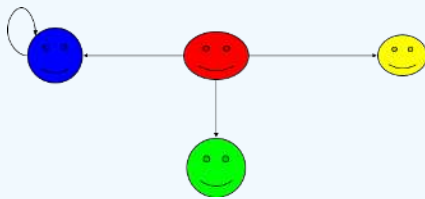
Definition: Antisymmetric

Let S be a set and R be a binary relation on S . Then R is said to be antisymmetric if the following statement is true:

$\forall a, b \in S$, if aRb and bRa , then $a = b$.

In other words, $\forall a, b \in S, aRb \wedge bRa \implies a = b$.

Example 2.1.11: VISUALLY



$\forall a, b \in S, aRb \wedge bRa \implies a = b$ holds!

We will follow the template below to answer the question about anti-symmetric.

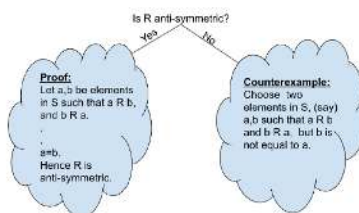


Figure 2.1.3: Anti-symmetric.

Example 2.1.12:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R antisymmetric?

Example 2.1.13:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}_+$. Is R antisymmetric?

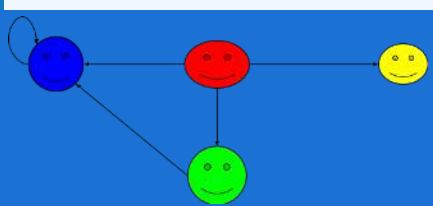
Definition: Transitive

Let S be a set and R be a binary relation on S . Then R is said to be transitive if the following statement is true

$\forall a, b, c \in S$, if aRb and bRc , then aRc .

In other words, $\forall a, b, c \in S, aRb \wedge bRc \implies aRc$.

Example 2.1.14: VISUALLY



$\forall a, b, c \in S, aRb \wedge bRc \implies aRc$ holds!

We will follow the template below to answer the question about transitive.

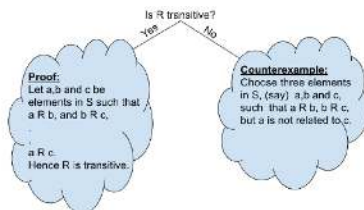


Figure 2.1.4: transitive.

Example 2.1.15:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R transitive?

Example 2.1.16:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}_+$. Is R transitive?

Summary:

In this section, we learned about binary relations and the following properties:

Reflexive

Symmetric

Antisymmetric

Transitive

This page titled [2.1: Binary Relations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

2.2: Equivalence Relations, and Partial order

Definition: Equivalence Relation

A binary relation is an equivalence relation on a nonempty set S if and only if the relation is reflexive(R), symmetric(S) and transitive(T).

Definition: Partial Order

A binary relation is a **partial order** if and only if the relation is reflexive(R), antisymmetric(A) and transitive(T).

Example 2.2.1: =

Let $S = \mathbb{R}$. Define a relation R on S by aRb if and only if $a = b$. Is the relation R on S ,

a) reflexive, b) symmetric, c) antisymmetric, d) transitive, e) an equivalence relation, f) a partial order.

Solution:

1. R is reflexive.

Proof:

Let $a \in \mathbb{R}$. Since $a = a$, R is reflexive. $\square$

2. R is symmetric.

Proof:

Let $a, b \in \mathbb{R}$ such that aRb . Now, $a = b \implies b = a$. Thus bRa . Hence R is symmetric. $\square$

3. R is antisymmetric.

Proof:

Let $a, b \in \mathbb{R}$ s.t. $a = b$ and $b = a$ then clearly $a = b \forall a, b \in \mathbb{R}$. $\square$

Yes R is transitive.

Proof:

Let $a, b, c \in \mathbb{R}$ s.t. $a = b$ and $b = c$.

We shall show that aRc .

Since $a = b$ and $b = c$ it follows that $a = c$

Thus aRc . $\square$

3. Yes R is an equivalence relation.

Proof:

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

4. Yes R is a partial order.

Proof:

R is a partial order, since R is reflexive, antisymmetric and transitive.

Example 2.2.2: Less than or equal to

Let $S = \mathbb{R}$ and R be $\leq$. Is the relation a) reflexive, b) symmetric, c) antisymmetric, d) transitive, e) an equivalence relation, f) a partial order.

Solution

1. Yes, R is reflexive.

Proof:

We will show that aRa is true.

Let $a \in S$ that is $a \in \mathbb{R}$.

Since $a < a$, R is reflexive. $\square$

2. No, R is not symmetric.

Counterexample:

Let $a = 2$ and $b = 3$ which are both $\in \mathbb{R}$.

It is true that $2 < 3$, but it is not true that $3 < 2$.

Thus R is not symmetric. $\square$

3. Yes, R is antisymmetric.

Proof:

We will show that given $a \leq b$ and $b \leq a$ that $a = b$.

Since $a \leq b$, $\exists \{x \in \mathbb{R} : x \geq 0\}$ s.t. $a + x = b$.

Further, since $b \leq a$, $\exists \{y \in \mathbb{R} : y \geq 0\}$, $b + y = a$.

Then $a + x = a + y$.

Thus, $x + y = 0$.

Since, $x, y \geq 0$, $x, y = 0$ thus $a = b$. $\square$

4. Yes, R is transitive.

Proof:

We will show that given $a \leq b$ and $b \leq c$ that $a \leq c$.

Since $a \leq b$, $\exists \{x \in \mathbb{R} : x \geq 0\}$ s.t. $a + x = b$.

Further, since $b \leq c$, $\exists \{y \in \mathbb{R} : y \geq 0\}$, $b + y = c$.

Then $a + x + y \leq c$.

Since, $x, y \geq 0$, thus $a \leq c$. $\square$

5. No, R is not an equivalence relation on S since it is not symmetric.

6. Yes, R is a partial order on S since it is reflexive, antisymmetric and transitive.

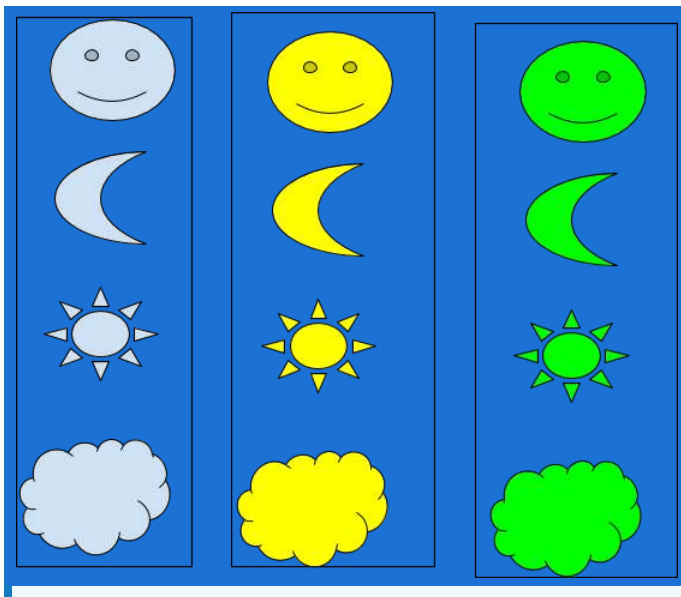
Definition: Equivalence Class

Given an equivalence relation R over a set S , for any $a \in S$ the equivalence class of a is the set $[a]_R = \{b \in S \mid aRb\}$, that is $[a]_R$ is the set of all elements of S that are related to a .

Example 2.2.3: Equivalence relation

Define a relation that two shapes are related iff they are the same color. Is this relation an equivalence relation?

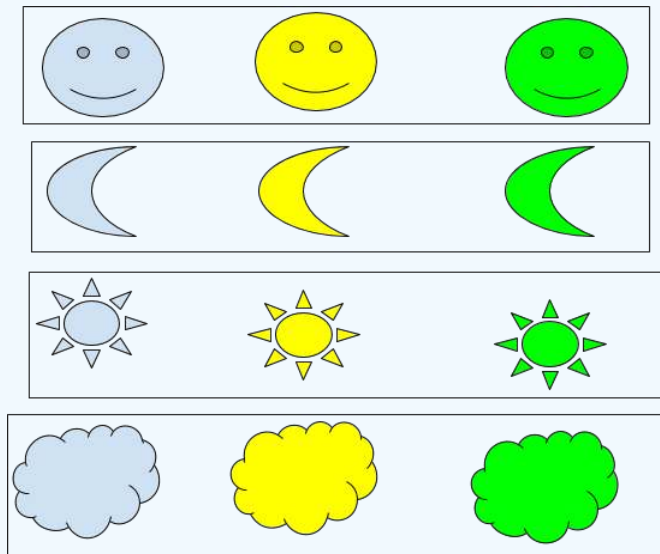
Equivalence classes are:



Example 2.2.4:

Define a relation that two shapes are related iff they are similar. Is this relation an equivalence relation?

Equivalence classes are:



Definition: Partition

Let A be a nonempty set. A partition of A is a set of nonempty pairwise disjoint sets whose union is A .

Note

For every equivalence relation over a nonempty set S , S has a partition.

Theorem 2.2.1

If $\sim$ is an equivalence relation over a non-empty set S . Then the set of all equivalence classes is denoted by $\{[a]_{\sim} | a \in S\}$ forms a partition of S .

This means

1. Either $[a] \cap [b] = \emptyset$ or $[a] = [b]$, for all $a, b \in S$.
2. $S = \cup_{a \in S} [a]$.

Proof

Assume $\sim$ is an equivalence relation on a nonempty set S .

Let $x, y \in S$. If $[x]_{\sim} \cap [y]_{\sim} = \emptyset$, then we are done. Otherwise, assume $[x]_{\sim} \cap [y]_{\sim} \neq \emptyset$.

Let a be the common element between them.

Let $a \in [x]_{\sim} \cap [y]_{\sim}$.

Then $a \in [x]_{\sim}$ and $a \in [y]_{\sim}$, which means that $a \sim x$ and $a \sim y$.

Since $\sim$ is an equivalence relation and $a \sim x, x \sim a$.

Since $x \sim a$ and $a \sim y$ (due to transitive property), $x \sim y$.

Thus $y \in [x]_{\sim}$ and $x \in [y]_{\sim}$.

Hence $[x]_{\sim} = [y]_{\sim}$.

Next, we will show that $S = \cup_{x \in S} [x]_{\sim}$.

First we shall show that $S \subseteq \cup_{x \in S} [x]_{\sim}$.

Let $m \in S$.

Then $[m]_{\sim}$ exists and $m \in [m]_{\sim}$.

Hence $m \in \cup_{x \in S} [x]_{\sim}$.

Thus $S \subseteq \cup_{x \in S} [x]_{\sim}$.

Conversely, we shall show that $\cup_{x \in S} [x]_{\sim} \subseteq S$.

Let $d \in \cup_{x \in S} [x]_{\sim}$.

Then $d \in [x]_{\sim}$ for some $x \in S$.

Thus $d \sim x \therefore d \in x$.

Thus $\cup_{x \in S} [x]_{\sim} \subseteq S$.

Since $S \subseteq \cup_{x \in S} [x]_{\sim}$ and $\cup_{x \in S} [x]_{\sim} \subseteq S$, then $S = \cup_{x \in S} [x]_{\sim}$. $\square$

For the following examples, determine whether or not each of the following binary relations R on the given set A is reflexive, symmetric, antisymmetric, or transitive. If a relation has a certain property, prove this is so; otherwise, provide a counterexample to show that it does not. If R is an equivalence relation, describe the equivalence classes of A .

Example 2.2.5:

Let $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Define a relation R on $A = S \times S$ by $(a, b)R(c, d)$ if and only if $10a + b \leq 10c + d$.

Solution

1. R is reflexive on S .

Proof:

Let $(a, b) \in A$.

We will show that $10a + b \leq 10a + b$.

Since $10a + b = 10a + b$, $10a + b \leq 10a + b$.

Since $(a, b)R(a, b)$, R is reflexive on S . $\square$

2. R is not symmetric on S .

Counter Example:

Let $a = 0, b = 1, c = 2, d = 3$.

Note $10(0) + 1 \leq 10(2) + 3$, specifically $(a, b)R(c, d)$, $1 < 23$ is true.

However, $(c, d)R(a, b)$, $23 < 1$ is false.

Since $b \not R a$, R is not symmetric on S . $\square$

3. R is antisymmetric on S .

Proof:

Let $a, b, c, d \in S$ s.t. $10a + b < 10c + d$ and $10c + d < 10a + b$.

Since $10a + b < 10c + d$ and $10c + d < 10a + b$, $10a + b = 10c + d$.

We will show that $a = c$ and $b = d$.

$0 \leq a, b, c, d \leq 9$ by definition.

Since $0 \leq b, d \leq 9$ and $0 \leq a, c \leq 9$, $10a = 10c$ thus $a = c$.

Since $a = c$, $b = d$.

Thus $(a, b)R(c, d)$ is antisymmetric on S . $\square$

5. R is transitive on S .

Proof:

Let $a, b, c, d, e, f \in S$ s.t. $10a + b < 10c + d$ and $10c + d < 10e + f$.

We will show that $10a + b < 10e + f$.

Since $10a + b < 10c + d$, $10a + b \leq 10c + d$.

Thus R is transitive on S . $\square$

6. R is not an equivalence relation since it is not reflexive, symmetric, and transitive.

Example 2.2.6:

Let $A = \mathbb{Z} \setminus \{0\}$. Define a relation R on A , by aRb if and only if $ab > 0$.

Solution

1. R is reflexive on A .

Proof:

Let $a \in \mathbb{Z} \setminus \{0\}$ we will show that $a \cdot a > 0$.

Clearly $a^2 > 0$ since $a \neq 0$ and a negative integer multiplied by a negative integer is a positive integer in $\mathbb{Z}$.

Since aRa , R is reflexive on A . $\square$

2. R is symmetric on A .

Proof:

We will show that if aRb , then bRa .

Let $a, b \in A$ s.t. aRb , that is $ab > 0$.

Since $ab = ba \in \mathbb{Z}$, $ba > 0$.

Since bRa , R is symmetric on A . $\square$

3. R is not antisymmetric on A .

Counter Example:

Let $a = 3$ and $b = 4$ then $3 \cdot 4 > 0$ and $4 \cdot 3 > 0$.

Since $3 \neq 4$, R is not antisymmetric on A . $\square$

4. R is transitive on A .

Proof:

Let $a, b \in A$ s.t. $ab > 0$ and $b, c \in A$ s.t. $bc > 0$.

There are two cases to be examined:

Case 1: $a > 0$ and $b > 0$.

Since $b > 0$, $c > 0$ thus $ac > 0$.

Case 2: $a < 0$ and $b < 0$.

Since $b < 0$, $c < 0$ thus $ac > 0$.

Since (aRb) in both possible cases R is transitive on A . $\square$

5. Since R is reflexive, symmetric and transitive, it is an equivalence relation. Equivalence classes are $[1]$ and $[-1]$.

Let $a \in A$, then $[a] = \{x \in A : x \sim a\}$

$= \{x \in A : xa > 0\}$.

Case 1: $a > 0$, then $x > 0$.

$[a] = \{x \in A : x > 0\}$.

$[1] = \{1, 2, 3, \dots\}$.

Case 2: $a < 0$, then $x < 0$.

$[a] = \{x \in A : x < 0\}$.

$[-1] = \{\dots, -3, -2, -1\}$.

Note this is a partition since $[x] \cap [y] = \emptyset$ or $[x] = [y]$, $\forall x, y \in S$. So we have all the intersections are empty.

$[1] \cap [-1] = \emptyset$.

Further, we have $S = \bigcup_{x \in S} [x]$. Note that 0 is excluded from S .

Hasse Diagram

Consider the set $S = \{1, 2, 3, 4, 5\}$. Then the relation $\leq$ is a partial order on S . Check!

Partial orders are often pictured using the Hasse diagram, named after mathematician Helmut Hasse (1898-1979).

Definition: Hasse Diagram

Let S be a nonempty set and let R be a partial order relation on S . Then Hasse diagram construction is as follows:

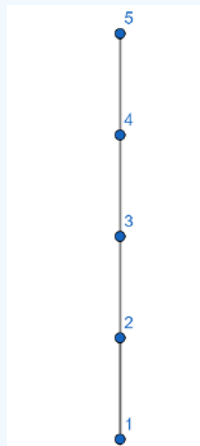
- there is a vertex (denoted by dots) associated with every element of S .
- if aRb , then the vertex b is positioned higher than vertex a .
- if aRb and there is no c such that aRc and cRb , then a line is drawn from a to b .

This diagram is called **the Hasse diagram**.

✓ Example 2.2.7:

Hasse diagram for $S = \{1, 2, 3, 4, 5\}$ with the relation $\leq$.

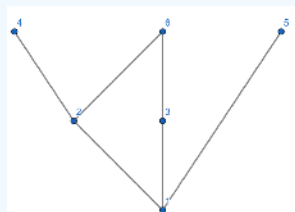
Solution



✓ Example 2.2.8:

Show that $\mathbb{Z}_+$ with the relation $|$ is a partial order. Draw a Hasse diagram for $S = \{1, 2, 3, 4, 5, 6\}$ with the relation $|$.

Solution



This page titled [2.2: Equivalence Relations, and Partial order](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

2.3: Arithmetic of inequality

Definition: Inequality

Let $a, b \in \mathbb{Z}$. Then

1. $a < b$ provided $b = a + k$, for some $k \in \mathbb{Z}_+$.
2. $a > b$ provided $a = b + h$, for some $h \in \mathbb{Z}_+$.

Theorem 2.3.1

Let $a, b \in \mathbb{Z}$.

1. If $a < b$ then $a + c < b + c$, $\forall c \in \mathbb{Z}$.
2. If $a < b$ then $ac < bc$, $\forall c \in \mathbb{Z}_+$.
3. If $a < b$ then $ac > bc$, $\forall c \in \mathbb{Z}_-$.
4. If $a < b$ and $c < d$ then $a + c < b + d$.

Proof

Let $a, b, c \in \mathbb{Z}$ such that $a < b$. Then $b = a + k$, for some $k \in \mathbb{Z}_+$.

1. Now consider, $b + c = (a + k) + c = (a + c) + k$, for some $k \in \mathbb{Z}_+$. Thus $a + c < b + c$.
- 2.

Example 2.3.1:

Determine all integers m that satisfy $-12m \geq 324$.

Solution

Since $-12m \geq 324$, $m \leq -\frac{324}{12} = -27$.

Example 2.3.2:

Determine all integers m that satisfy $14m \geq 635$.

Solution

Since $14m \geq 635$, $m \geq \frac{635}{14} = 45.35$. Thus the solutions are $\{m \in \mathbb{Z} | m \geq 46\}$.

Example 2.3.3:

Determine all integers k that satisfy $-165 + 98k \geq 0$, $-335 + 199k \geq 0$, $-165 + 98k < 100$ and $-335 + 199k < 100$.

Solution

Since $-165 + 98k \geq 0$, $k \geq 1.68$.

Since $-335 + 199k \geq 0$, $k \geq 1.68$.

Since $-165 + 98k < 100$, $98k < 265$, and $k < 2.70$.

Since $-335 + 199k < 100$, $199k < 435$, and $k < 2.18$.

Since $1.68 \leq k < 2.18$ and $k \in \mathbb{Z}$, $k = 2$.

2.4: Arithmetic of divisibility

Thinking out loud

If a teacher was able to share 6 apples among 6 boys and 8 oranges among 4 girls equally, is it possible for the teacher to share the 14 fruits with the 10 children equally?

Theorem: Divisibility theorem I (BASIC)

Let $a, b, c \in \mathbb{Z}$ such that $a + b = c$. If $d \in \mathbb{Z}_+$ divides any two of a, b and c , then d divides the third one.

Proof:

Proof:(by cases)

Case 1: Suppose $d \mid a$ and $d \mid b$. We shall show that $d \mid c$.

Since $d \mid a$ and $d \mid b$, $a = dm$ and $b = dk$, for some $m, k \in \mathbb{Z}$.

Consider, $c = a + b = dm + dk = d(m + k)$.

Since $(m + k) \in \mathbb{Z}$, $d \mid c$.

Case 2: Suppose $d \mid a$ and $d \mid c$. We shall show that $d \mid b$.

Since $d \mid a$ and $d \mid c$, $a = dm$ and $c = dk$, for some $m, k \in \mathbb{Z}$.

Consider, $b = c - a = d(k - m)$.

Since $(k - m) \in \mathbb{Z}$, $d \mid b$.

Case 3: Suppose $d \mid b$ and $d \mid c$. We shall show that $d \mid a$.

Since $d \mid b$ and $d \mid c$, $b = dm$ and $c = dk$, with $m, k \in \mathbb{Z}$.

Consider, $a = c - b = d(k - m)$.

Since $(k - m) \in \mathbb{Z}$, $d \mid a$.

Having examined all possible cases, given $a + b = c$, then if $d \in \mathbb{Z}_+$ divides any two of a, b and c , then d divides the third one. $\square$

Theorem: Divisibility theorem II (MULTIPLE)

Let $a, b, c \in \mathbb{Z}$ such that $a \mid b$. Then $a \mid bc$.

Proof:

Let $a, b, c \in \mathbb{Z}$ such that $a \mid b$.

We shall show that $a \mid bc$.

Consider that since $a \mid b$, $b = ak$, $k \in \mathbb{Z}$.

Further consider $bc = a(ck)$.

Since $ck \in \mathbb{Z}$, $a \mid bc$. $\square$

Theorem: Arithmetic of Divisibility

Let $a, b, c, d \in \mathbb{Z}$. Then

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
2. if $a \mid b$ and $a \mid c$ then $a \mid (bc)$.
3. if $a \mid b$ and $c \mid d$ then $(ac) \mid (bd)$.

Proof:

Proof of 1:

Let $a, b, c, d \in \mathbb{Z}$.

We shall show that if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.

Since $a \mid b$, $b = ak$, $k \in \mathbb{Z}$ and since $a \mid c$, $c = am$, $m \in \mathbb{Z}$.

Consider, $b + c = a(k + m)$.

Since $k + m \in \mathbb{Z}$, $a \mid (b + c)$. $\square$

Proof of 2:

Let $a, b, c, d \in \mathbb{Z}$.

We shall show that if $a \mid b$ and $a \mid c$ then $a \mid (bc)$.

Since $a \mid b$, $b = ak$, $k \in \mathbb{Z}$ and since $a \mid c$, $c = am$, $m \in \mathbb{Z}$.

Consider $bc = a(akm)$.

Since $akm \in \mathbb{Z}$, $a \mid (bc)$. $\square$

Proof of 3:

Let $a, b, c, d \in \mathbb{Z}$.

We shall show that if $a \mid b$ and $c \mid d$ then $(ac) \mid (bd)$.

Since $a \mid b$, $b = ak$, $k \in \mathbb{Z}$ and since $c \mid d$, $d = cm$, $m \in \mathbb{Z}$.

Consider $bd = (ak)(cm) = ac(km)$.

Since $km \in \mathbb{Z}$, $(ac) \mid (bd)$. $\square$

Example 2.4.1:

Let $a, b, c, d \in \mathbb{Z}$ such that $a \mid b$ and $c \mid d$. Is it always true that $(a + c) \mid (b + d)$?

In other words, if a teacher was able to share 6 apples among 6 boys and 8 oranges among 4 girls equally, is it possible for the teacher to share the 14 fruits with the 10 children equally?

Example 2.4.2:

Let a and b be positive integers such that $7 \mid (a + 2b + 5)$ and $7 \mid (b - 9)$. Prove that $7 \mid (a + b)$.

Solution

Let $a, b \in \mathbb{Z} + s$. $t. 7 \mid (a + 2b + 5)$ and $7 \mid (b - 9)$.

Consider $a + 2b + 5 = 7(m)$, $m \in \mathbb{Z}$.

Further consider $b - 9 = 7(k)$, $k \in \mathbb{Z}$.

Next consider $a + 2b + 5 - (b - 9) = 7m - 7k$.

$$a + b + 14 = 7(m - k).$$

$$a + b = 7(m - k - 2), m - k - 2 \in \mathbb{Z}.$$

Thus, $7|(a + b)$. $\square$

Example 2.4.3:

Let a and b be positive integers. Prove or disprove the following statements:

1. If $a|b$ then $a^2|b^3$.
2. If $a^2|b^3$ then $a|b$.

Solution

1. This statement is true.

Proof:

Let a and b be positive integers such that $a|b$. Then $b = am$, $m \in \mathbb{Z}_+$.

$$\text{Consider } b^3 = (am)^3 = a^3m^3 = a^2(am^3).$$

$$\text{Since } am^3 \in \mathbb{Z}_+, a^2|b^3.$$

2. This statement is false. Counterexample:

$$\text{Choose } a = 3^3, b = 3^2. \text{ Then } a^2 = 3^6 = b^3.$$

$$\text{Hence } a^2|b^3 \text{ but } a \nmid b.$$

2.5: Divisibility Rules

In this section, we will explore some rules of divisibility for some positive integers. These rules can be easily extended to all the integers by dropping the sign.

Let $x \in \mathbb{Z}_+$.

Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0, \quad (2.5.1)$$

which implies

$$x = 10(d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_2 10 + d_1) + d_0. \quad (2.5.2)$$

Thus we can express x as $10a + b$, where $b = d_0$ is the ones digit of x , and $a = d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_2 10 + d_1$.

Divisibility by $2 = 2^1$:

Let $x \in \mathbb{Z}_+$. $2 \mid x$ iff $2 \mid b$. In other words, 2 divides an integer iff the ones digit of the integer is either 0, 2, 4, 6, or 8.

Proof:

Since $2 \mid 10$, $x = 10a + b$, and by divisibility theorem I, $2 \mid x$ iff $2 \mid b$. $\square$

Divisibility by 5 :

$5 \mid x$ iff $5 \mid b$. In other words, 5 divides an integer iff the ones digit of the integer is either 0, or 5.

Proof:

Since $5 \mid 10$, $x = 10a + b$, and by divisibility theorem I, $5 \mid x$ iff $5 \mid b$. $\square$

Divisibility by 10 :

$10 \mid x$ iff $10 \mid b$. In other words, 10 divides an integer iff the ones digit of the integer is 0,.

Proof:

Since $10 \mid 10$, $x = 10a + b$, and by divisibility theorem I, $10 \mid x$ iff $10 \mid b$. $\square$

Divisibility by $4 = 2^2$:

$4 \mid x$ iff $4 \mid d_1 d_0$.

Proof:

Let x be an integer. Then

$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0$, which implies

$$x = 100(d_n 10^{n-2} + d_{n-1} 10^{n-3} + \cdots + d_2) + 10d_1 + d_0 = 100(d_n 10^{n-2} + d_{n-1} 10^{n-3} + \cdots + d_2) + d_1 d_0.$$

Since $4 \mid 100$, $x = 100a + d_1 d_0$, and by divisibility theorem I, $4 \mid x$ iff $4 \mid d_1 d_0$. $\square$

Divisibility by 4 of a two digit number

$$4 \mid d_1 d_0 \text{ iff } 4 \mid 2d_1 + d_0$$

Divisibility by $8 = 2^3$:

$$8 \mid x \text{ iff } 8 \mid d_2 d_1 d_0.$$

Proof:

Let x be an integer. Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0, \text{ which implies}$$

$$x = 10^3(d_n 10^{n-3} + d_{n-1} 10^{n-4} + \cdots + d_3) + 100d_2 + 10d_1 + d_0 = 10^3(d_n 10^{n-3} + d_{n-1} 10^{n-4} + \cdots + d_3) + d_2 d_1 d_0.$$

$$\text{Since } 8 \mid 1000, x = 1000a + d_2 d_1 d_0, \text{ and by divisibility theorem I, } 8 \mid x \text{ iff } 8 \mid d_2 d_1 d_0. \square$$

A similar argument can be made for divisibility by 2^n , for any positive integer n .

Example 2.5.1:

Using divisibility tests, check if the number 824112284 is divisible by:

1. 5
2. 4
3. 8

Solution:

1. 824112284 is **not divisible** by 5.

Rule: The one's digit of the number has to be either a 0 or a 5.

Since the last digit is not 0 or 5, 824112284 is **not divisible** by 5.

2. 824112284 is **divisible** by 4.

Rule: The last two digits of the number have to be divisible by 4.

The last two digits of 824112284 is $84 = (4)(21)$.

Since 84 is divisible by 4, 824112284 is **divisible** by 4 also.

3. 824112284 is **not divisible** by 8.

Rule: The last three digits of the number have to be divisible by 8.

The last three digits of 824112284 is 284. Since 284 is not divisible by 8, the original number, 824112284 is **not divisible** by 8 either.

Notice the following pattern $10 - 1 = 9, 100 - 1 = 99, 1000 - 1 = 999, \dots, 10^n - 1 = 999 \dots 9$

Divisibility by $3 = 3^1$:

$$3 \mid x \text{ iff } 3 \text{ divides sum of its digits.}$$

Proof:

Let $x \in \mathbb{Z}_+$.

Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0, \quad (2.5.3)$$

which implies

$$x = 9(d_n(10^{n-1} + d_{n-1}10^{n-2} + \cdots + d_2 10 + d_1) + (d_0). \quad (2.5.4)$$

Example 2.5.2:

Find the possible values for the missing digit x , if $1234x51234$ is divisible by 3.

Solution:

Consider the following:

The divisibility rule for the number 3 is as follows: If the sum of the digits in the whole number is a number divisible by 3, then the larger, original number is also.

The sum of the digits is $2(1 + 2 + 3 + 4) + 5 + x = 25 + x$. Since $3 \mid (25 + x)$, $25 + x = 27, 30$ or 33 . Hence $x = 2, 5$ or 8 .

Divisibility by $9 = 3^2$:

$9 \mid x$ iff 9 divides sum of its digits.

Divisibility by 7:

$7 \mid x$ iff 7 divides the absolute difference between $a - 2b$, where $x = 10a + b$, where $b = d_0$ is the ones digit of x , and $a = d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_2 10 + d_1$.

Proof:

Assume $7 \mid x$. Which implies $7 \mid 10a + b$.

Consider $x - 21b = (10a + b) - 21b = 10a - 20b = 10(a - 2b)$.

Thus $7 \mid x$ if and only if $7 \mid a - 2b$.

Divisibility by 11:

$11 \mid x$ iff 11 divides the absolute difference between the alternate sum.

Proof:

2.6: Division Algorithm

The absolute value

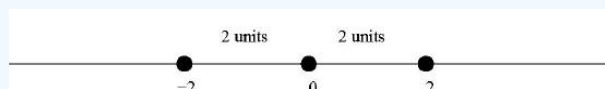
Definition: Absolute value

For any real number x the absolute value of x is denoted by $|x|$ and defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases} \quad (2.6.1)$$

Example 2.6.1 : Absolute Value

Consequently we see that $|-2| = |2| = 2$.



Theorem 2.6.1: Well ordering principle

Every non-empty subset of $\mathbb{N}$ has a smallest element.

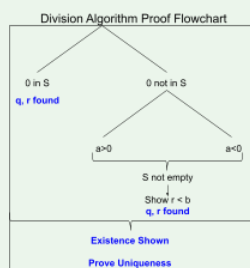
Theorem 2.6.2: Division Algorithm

Let a and b be integers. Then there exist unique integers q and r such that $a = bq + r$, $0 \leq r < |b|$, where q is the quotient and r is the remainder, and the absolute value of d is defined as:

$$|b| = \begin{cases} b, & \text{if } b \geq 0 \\ -b, & \text{if } b < 0. \end{cases} \quad (2.6.2)$$

Proof

We will show that $q, r \in \mathbb{Z}$ exist and that they are unique.



Let $a, b \in \mathbb{Z}$ s.t. $b > 0$.

Let S be a set defined by $S = \{a - bm : a - bm \geq 0, m \in \mathbb{Z}\}$.

We will show existence by examining the possible cases.

Case 1: $0 \in S$

If $0 \in S$, then $a - bm = 0$ for some $m \in \mathbb{Z}$.

Thus, $a = bm$

Since $b|a$, $q = m$ and $r = 0$.

Therefore, existence has been proved.

Case 2: $0 \notin S$.

Since $0 \notin S$, we will show that $S \neq \emptyset$ by examining the possible cases. Note: $S \subseteq \mathbb{N}$.

Case a: $a > 0$.

Since $a > 0$, $a = a - b(0) > 0$.

Therefore $a \in S$.

Case b: $a < 0$.

Consider $a - bm$, where $m = 2a$.

Thus $a - b(2a) = a(1 - 2b)$.

Consider $1 - 2b$ is always negative since $b > 0 \cap b \in \mathbb{N}$, thus greatest $1 - 2b$ can be in -1 .

Therefore $a(1 - 2b) \geq 0$ since $b \geq 1$.

Note: The $\geq$ could be $>$ without loss of generality.

Since both cases, a & b, are non-empty sets, $S \neq \emptyset \subseteq \mathbb{N}$.

Thus S has the smallest element by the well-ordering principle, and let's call it r .

That means $r = a - bm$, for some $m \in \mathbb{Z}$ where $r \geq 0$.

Thus the non-empty set is $r = a - bm \geq 0$.

We shall show that $r < b$ by proceeding with a proof by contradiction.

Assume that $r \geq b$.

Then $a - b(m + 1) = a - bm - b = r - b \geq 0$ for some $m \in \mathbb{Z}$.

Then $r - b \in S$ and $r - b < r$. Note ($b > 0$)

This contradicts that r is the smallest element of S .

Therefore $r < b$.

Having examined all possible cases, $a = bq + r$, $0 \leq r < b$ exists.

Next, we will show uniqueness.

Let r_1, r_2, q_1, q_2 s.t. $a = bq_1 + r_1$ and $a = bq_2 + r_2$ with $0 \leq r_1, r_2 < b$.

Consider $bq_1 + r_1 = bq_2 + r_2$, $0 \leq r_1 < b$.

Further since $b(q_1 - q_2) = r_2 - r_1$, $\boxed{b|(r_2 - r_1)}$, but b has to be $\leq r_1$.

Since, $r_2 - r_1 < b$, $r_2 - r_1 = 0$ and $r_1 = r_2$.

Hence $q_1 = q_2$.

Therefore, uniqueness has been shown.

Let n and d be integers. Then there exist unique integers q and r such that $n = dq + r$, $0 \leq r < |d|$, where q is the quotient and r is the remainder, and the absolute value of d is defined as:

$$|d| = \begin{cases} d, & \text{if } d \geq 0 \\ -d, & \text{if } d < 0. \end{cases} \quad (2.6.3)$$

Example 2.6.2:

Find the q is the quotient and r is the remainder for the following values of n and d .

1. $n = 2018$ and $d = 343$.

$$\begin{array}{r} 5 \\ 343 \overline{)2018} \\ \underline{-1715} \\ 303 \end{array}$$

Thus $2018 = (5)(343) + 303$.

2. $n = -2018$ and $d = 343$.

$$\begin{array}{r} -6 \\ 343 \overline{)-2018} \\ \underline{+2058} \\ 40 \end{array}$$

Thus $-2018 = (-6)(343) + 40$.

3. $n = 2018$ and $d = -343$.

Thus $2018 = (6)(-343) + 40$.

4.

$n = -2018$ and $d = -343$.

Thus $-2018 = (6)(-343) + 40$.

Example 2.6.3:

Today is March 3, 2018, and it is Friday. What day will it be on March 3, 2019?

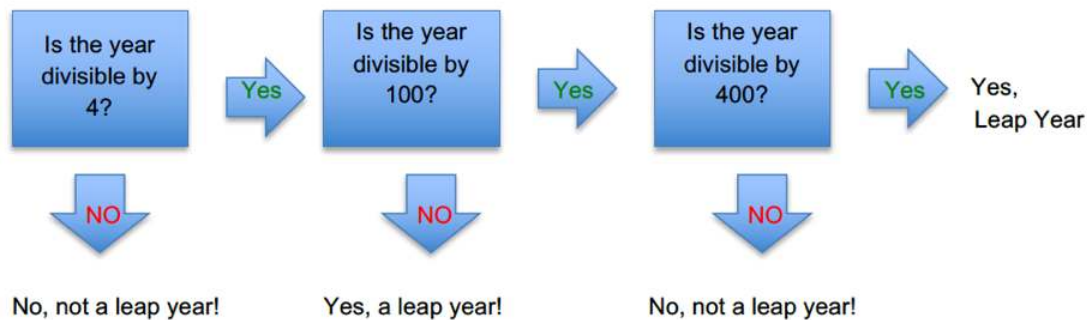
At first, note that 2019 is not a leap year. Therefore, there are 365 days between March 3, 2018, and March 3, 2019. Also $365 = (52)(7) + 1$. There are seven days in a week and keeping Friday as 0, we can conclude that March 3, 2019, will be a Saturday.

Leap Year

The Gregorian calendar is the calendar we most commonly use today throughout the world. The Gregorian calendar consists of both common years with 365 days and Leap years consisting of 366 days due to the intercalary day added on February 29th. Leap years are necessary in order to keep the Gregorian calendar aligned with the Earth's revolution around the sun.

Following our modern day Gregorian calendar there are three rules to take into consideration to identify leap years:

1. The year must be evenly divided by 4.
2. If the year is evenly divided by 100, it is not a leap year unless:
3. The year is also evenly divided by 400.



For example: the years 1600, 1800, 2000 are all leap years, but the years 1700 and 1900 aren't leap years.

Example 2.6.4:

Each day, Ms. Mary visits grocery stores A, B, C, D in that order. Further, she spends exactly \$27, \$35, \$12, \$40 in the stores A, B, C, D respectively. Her total expenditure, from the beginning of the month up to a certain day of the month, was \$924. Which store would she be visiting next?

Example 2.6.5

In a 101-digit multiple of 13, the first 50 digits are all 5s and the last 50 digits are all 8s. What is the middle digit?

Solution

Since $13 \mid 555555$ and $13 \mid 888888$, we need to consider what the value of $X \in \mathbb{Z}$ is such that $13 \mid 55X88$ since the first and last 48 digits of the number will produce multiples of 13. At this point (Solution 1), trial and error can be applied to this calculation, resulting in $X = 5$.

A more elegant solution (Solution 2) can be obtained by recognizing that any number $Q \in \mathbb{Z}^+$ can be written as:

$$Q = 10a + b, \text{ where } a, b \in \{0, 1, \dots, 8, 9\}.$$

Next find a multiple of 13 that has a 1 as the last digit. This condition is satisfied with 91. Next, rewrite the equation to be $Q - 91b = 10a + b - 91b$ and simplify to $Q - 91b = 10(a - 9b)$. Using this formula, $55X8 - 9(8)$ a number whose last digit is a 6, is divisible by 13 and the first two digits must be either 55 or 54 will satisfy the condition $13 \mid 55X88$. The only number that satisfies these conditions is 5486. Adding back 72, we obtain 5558, thus confirming that $X = 5$.

A more deductive solution (Solution 3) can be seen using long division as follows:

Steps to determine value of X

- 1: 55 divided by 13 is 4 remainder 3, yielding line (a).
- 2: Since $13 \nmid 55X88$, the remainder is zero (b).
- 3: The last digit of a multiple of 13 must be an eight (c).
- 4: The number used in (c) must be the same as in (d).
- 5: The last two digits of (e) must be 10 in order to obtain a 78 in line (d).
- 6: The first digit of (e) must be 9 since $13 \nmid 91$.
- 7: First two digits must be 26 in order be able to obtain a leading 9 in line (e).
- 8: Finally, X must be 5.

$$\begin{array}{r}
 4 \\
 13 \overline{) 55X88} \\
 \underline{52000} \\
 (a) \quad 3X88 \\
 (f) \quad 2600 \\
 \underline{988} \\
 910 \quad (e) \\
 \underline{78} \quad (d) \\
 78 \quad (c) \\
 \underline{0} \\
 (b) \quad 0
 \end{array}$$

This page titled [2.6: Division Algorithm](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

2.E: Exercises

Exercise 2.E.1: Equivalence relation

Determine whether or not each of the following binary relations R on the given set A is reflexive, symmetric, antisymmetric, or transitive. If a relation has a certain property, prove this is so; otherwise, provide a counterexample to show that it does not. If R is an equivalence relation, describe the equivalence classes of A .

1. Define a relation R on $A = \mathbb{Z}$ by $a R b$ if and only if $4 \mid (3a + b)$.
2. Define a relation R on $A = \mathbb{Z}$ by $a R b$ if and only if $3 \mid (a^2 - b^2)$.
3. Let $A = \mathbb{R}$, If $a, b \in \mathbb{R}$, define $a R b$ if and only if $a - b \in \mathbb{Z}$.
4. Define a relation R on the set $\mathbb{Z} \times \mathbb{Z}$ by: $(a, b) R (c, d)$ if and only if $ac = bd$.
5. Define a relation R on $\mathbb{Z}$ by: $a R b$ if and only if $5 \mid 2a + 3b$.
6. Define a relation R on $\mathbb{Z}$ by: $a R b$ if and only if $2 \mid a^2 + b$.

Answer

- i. We shall show that R is reflexive on A .

Proof:

Let $a \in \mathbb{Z}$.

Since $3a + a = 4a$, $4 \mid (3a + a)$. Thus aRa .

Hence R is reflexive on $\mathbb{Z}$.

- ii. We shall show that R is symmetric on A .

Proof:

Let $a, b \in \mathbb{Z}$, such that aRb .

Then $4 \mid (3a + b)$. Thus $3a + b = 4m$, for some integer m .

We shall show that bRa . That means $4 \mid (3b + a)$.

Consider $3a + b = 4m$

$$(3a + b) + (3b + a) = 4m + (3b + a)$$

$$(4b + 4a) = 4m + (3b + a)$$

$$3b + a = -4m + 4b + 4a = 4(-m + b + a).$$

Since $m + b + a \in \mathbb{Z}$, $4 \mid (3b + a)$.

Hence R is symmetric on $\mathbb{Z}$.

- iii. We shall show that R is not antisymmetric on $\mathbb{Z}$.

Counterexample:

Choose $a = 4$ and $b = 0$.

Then $3(4) + 0 = 12$ and $4 \mid 12$, so $4 \mid 3a + b$. Also $3(0) + 4 = 4$ and $4 \mid 4$, so $4 \mid 3b + a$.

However, $4 \neq 0$, so $a \neq b$.

Hence R is not antisymmetric on $\mathbb{Z}$.

- iv. We shall show that R is transitive on $\mathbb{Z}$.

Proof:

Let $a, b, c \in \mathbb{Z}$, such that aRb and bRc . That means $4 \mid 3a + b$ and $4 \mid 3b + c$.

Since $4 \mid 3a + b$, $3a + b = 4m$ for some integer m , and Since $4 \mid 3b + c$, $3b + c = 4n$, for some integer n .

We shall show that aRc . That is $4 \mid 3a + c$.

Consider $(3a + b) + (3b + c) = 4m + 4n \implies 3a + c + 4a + 4b = 4m + 4n \implies 3a + c = 4(m + n - a - b)$.

Since $m + n - a - b \in \mathbb{Z}$, $4 \mid 3a + c$. Thus, aRc .

Hence R is transitive on $\mathbb{Z}$.

v. Since R is reflexive, symmetric and reflexive, aRb is an equivalence relation on $\mathbb{Z}$.

Equivalence classes:

$$[0] = \{x \in \mathbb{Z} \mid x \sim 0\} = \{x \in \mathbb{Z} \mid 4 \mid (3x + 0)\} = \{x \in \mathbb{Z} \mid 4m = 3x, \text{ for some integer } m\} = \{0, \pm 4, \pm 8, \dots\}.$$

$$[1] = \{x \in \mathbb{Z} \mid x \sim 1\} = \{x \in \mathbb{Z} \mid 4 \mid (3x + 1)\} = \{x \in \mathbb{Z} \mid 4m = 3x + 1, \text{ for some integer } m\} = \{\dots, -3, 1, 5, \dots\}.$$

$$[2] = \{x \in \mathbb{Z} \mid x \sim 2\} = \{x \in \mathbb{Z} \mid 4 \mid (3x + 2)\} = \{x \in \mathbb{Z} \mid 4m = 3x + 2, \text{ for some integer } m\} = \{\dots, -2, 2, 6, \dots\}.$$

$$[3] = \{x \in \mathbb{Z} \mid x \sim 3\} = \{x \in \mathbb{Z} \mid 4 \mid (3x + 3)\} = \{x \in \mathbb{Z} \mid 4m = 3x + 3, \text{ for some integer } m\} = \{\dots, -1, 3, 7, \dots\}.$$

6.

Proof of Reflexivity:

Let $a \in \mathbb{Z}$.

We shall show that $a^2 + a = 2m, m \in \mathbb{Z}$. We can show this directly or using cases:

Directly:

Since $a^2 + a = a(a + 1)$, and $a, a + 1$ are consecutive integers,

$a^2 + a$ is even. Thus $\sim$ is reflexive on $\mathbb{Z}$.

Proof of Symmetry:

Let $a, b \in \mathbb{Z}$ s.t. $a^2 - b = 2m, m \in \mathbb{Z}$.

We will show that $b^2 + a = 2k, k \in \mathbb{Z}$.

Since

$$a^2 = 2m - b, \quad b^2 + a = (2m - a^2)^2 + a = 4m^2 - 4ma^2 + a^4 + a.$$

Thus

$$b^2 + a = 2(2m^2 - 2ma^2) + a(a^3 + 1) =$$

$$2(2m^2 - 2ma^2) + a(a + 1)(a^2 - a + 1).$$

Since $a(a+1)$ is even,

$b^2 + a$ is even.

Thus $\sim$ is symmetric on $\mathbb{Z}$.

Proof of Transitivity:

Let $a, b, c \in \mathbb{Z}$ s.t. $2 \mid a^2 + b$ and $2 \mid b^2 + c$.

We will show that $2 \mid a^2 + c$.

Consider $a^2 - b = 2m, m \in \mathbb{Z}$ and $b^2 + c = 2n, n \in \mathbb{Z}$.

Further, consider that $a^2 + c = 2m - b + 2n - b^2 = 2(m + n) - (b^2 + b)$.

Since $\sim$ is reflexive on $\mathbb{Z}$, $b^2 + b = 2q, q \in \mathbb{Z}$.

Thus $a^2 + c = 2(m - n - q), m, n, q \in \mathbb{Z}$.

Thus $\sim$ is transitive on $\mathbb{Z}$.

Having shown that $\sim$ is reflexive, symmetric and transitive on $\mathbb{Z}$, $\sim$ is an equivalence relation on $\mathbb{Z}$. $\square$

Let $a \in \mathbb{Z}$, then $[a] = \{x \in \mathbb{Z} : x \sim a\}$.

Case $a = 3$:

$$\begin{aligned} [3] &= \{x \in \mathbb{Z} : x \sim 3\} \\ &= \{x \in \mathbb{Z} : 2|(x^2 + 3)\} \\ &= \{x \in \mathbb{Z} : x^2 + 3 = 2m, m \in \mathbb{Z}\} \\ &= \{\pm 1, \pm 3, \dots\}. \end{aligned}$$

Case $a = 2$:

$$\begin{aligned} [2] &= \{x \in \mathbb{Z} : x \sim 2\} \\ &= \{x \in \mathbb{Z} : 2|(x^2 + 2)\} \\ &= \{x \in \mathbb{Z} : x^2 + 2 = 2m, m \in \mathbb{Z}\} \\ &= \{0, +2, +4, \dots\}. \end{aligned}$$

Exercise 2.E.2: Divides

Let $a, b, c, d \in \mathbf{Z}_+$.

1. If $a|b$ and $a|c$, is it necessarily true that $a|(b+c)$?
2. If $a|(b+c)$, is it necessarily true that $a|b$ and $a|c$?
3. If $a|bc$, is it necessarily true that $a|b$ and $a|c$?
4. If $(a+b)|c$, is it necessarily true that $a|c$ and $b|c$?
5. If $a|c$ and $b|c$, is it necessarily true that $(a+b)|c$?
6. If $a^3|b^4$, is it necessarily true that $a|b$?
7. If $a|b$, is it necessarily true that $a^3|b^5$?
8. If $c|a$ and $d|b$, is it necessarily true that $cd|ab$.

Exercise 2.E.3: Divisibility Rules

1. Find all possible values for the missing digit if 12345X51234 is divisible by 3.
2. Using divisibility tests, check if the number 355581 is divisible by 7
3. Using divisibility tests, check if the number 824112284 is divisible by 5, 4, and 8.

Answer

1. An integer (q) is divisible by 3 iff $\sum_{i=0}^n d_i$ is divisible by 3, where d_i is the i th digit of q . Thus, the sum of the digits of 12345X51234 must be divisible by 3.

Simplifying, $3 \mid (30 + X)$.

Since $3 \mid 30$, 3 must divide X in order to satisfy $3 \mid 12345X51234$.

Thus $X \in \{0, 3, 6, 9\}$.

2.

An integer (q) is divisible by 7 iff $7 \mid (a - 2b)$, where b is the last digit of q and a is the remaining digits.

Step 1: $a = 35558$, $b = 1$.

Thus, $a - 2b = 35556$.

Step 2: $a = 3555$, $b = 6$.

Thus, $a - 2b = 3543$.

Note at this point it is clear that $7 \nmid 355581$, since $7 \nmid 3543$. However, for practice, we will continue on.

Step 3: $a = 354$, $b = 3$.

Thus, $a - 2b = 348$.

Step 4: $a = 34$, $b = 8$.

Thus $a - 2b = 18$.

Since $7 \nmid 18$, $7 \nmid 355581$.

3.

Solution:

An integer (q), is divisible by 5 iff its last digits $\in \{0, 5\}$.

Since $4 \notin \{0, 5\}$, $5 \nmid 824112284$.

Solution:

An integer (q) is divisible by 8 iff q 's last three digits are divisible by 8.

Since $8 \nmid 284$, $8 \nmid 824112284$.

An integer (q) is divisible by 4 iff q 's last two digits are divisible by 4.

Since $4 \mid 84$, $4 \mid 824112284$.

Exercise 2.E.4: Divisibility

- Let a be a positive integer such that $3 \mid (a + 1)$. Show that $3 \mid (7a + 4)$.
- Let a and b be positive integers such that $7 \mid (a + 2b - 2)$ and $7 \mid (b - 9)$. Prove that $7 \mid (a + b)$.
- Let a, b, c and d be positive integers such that $4 \mid (abc + d)$, $4 \mid (adc + b)$, $4 \mid (abd + c)$ and $4 \mid (bcd + a)$. Prove that $4 \mid (a^2 + b^2 + c^2 + d^2)$.
- Let a, b, c and d be positive integers such that $ad - bc > 1$. Show that at least one of these four integers is not divisible by $ad - bc$.

Exercise 2.E.5: Middle digit

- In a 113-digit multiple of 13, the first 56 digits are all 5s and the last 56 digits are all 8s. What is the middle digit?
- In a 113-digit multiple of 7, the first 56 digits are all 8s and the last 56 digits are all 1s. What is the middle digit?

Exercise 2.E.6: True or False

Prove the statements that are true and give counterexamples to disprove those that are false.

Let a, b and c be integers.

1. If $a|b$ then $b|a$.
2. If $a|bc$ then $a|b$ and $a|c$.
3. If $a|b$ and $a|c$ then $a|bc$.
4. If $a|b$ and $a|c$ then $a|(b+c)$ and $a|(b-c)$.
5. If $a|(b+c)$ and $a|(b-c)$ then $a|b$ and $a|c$.
6. If $a|b$ and $a|c$ then $a|(b+c)$ and $a|(2b+c)$.
7. If $a|(b+c)$ and $a|(2b+c)$ then $a|b$ and $a|c$.

Exercise 2.E.7: Induction

Prove that for all integers $n \geq 1$, $5^{2n} - 2^{5n}$ is divisible by 7.

Answer

use induction to prove the statement.

Exercise 2.E.8: Induction or by cases

Prove that for all integer $n \geq 1$, 6 divides $n^3 - n$.

Answer

use induction to prove the statement.

Exercise 2.E.9: True or false

Which of the following statements are true. Prove the statement(s) that are true and give a counterexample for the statement(s) that are false.

If a, b, c and d are integers such that $a < b$ and $c < d$, then $ac < bd$.

If a, b, c and d are integers such that $a < 0 < b$ and $c < 0 < d$, then $ac < bd$.

If a, b, c and d are integers such that $0 < a < b$ and $c < 0 < d$, then $ac < bd$.

If a, b, c and d are integers such that $a < b$ and $c < d$, then $a - d < b - c$.

Answer

TBD

Exercise 2.E.10 Tip?

There are 9 waiters and 1 busboy working at a restaurant. The tips are always in whole number of dollars. At the end of the day, the waiters share the tips equally among themselves as far as possible, each getting a whole number of dollars. The busboy gets what is left. How much does he get on a day when the total amount of the tips is \$980.

Answer

$980 \pmod{9} \equiv 8 \pmod{9}$, thus, the busboy would receive \$ 8 when the total tip for the day was \$ 980.

Exercise 2.E.11 Day of the week

March 1 on some year is a Friday. On what day of the week will Christmas be that year?

Answer

Christmas falls on December 25th in any given year. The number of days from March 1 till Christmas $(430) + (631) - 7 = 299$. Note: We consider March 1 as day zero and there are 6 days from December 25 to December 31, thus seven days must be subtracted from the total number of days. Since $299 = 7(42) + 5$ and March 1 is a Friday, Christmas will fall five days after Friday, which is a Wednesday. Thus, if in a given year, March 1 is a Friday, Christmas will fall on a Wednesday that year.

Exercise 2.E.12: Inequality

Solve $0 < 199m - 335 < 100$ for all integers m .

Answer

$$m = 2.$$

This page titled [2.E: Exercises](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

CHAPTER OVERVIEW

3: Modular Arithmetic

Modular Arithmetic begins with a modulus " n ", n must be a member of $\mathbb{Z}_+$.

Modulus " n " divides all the integers into congruent or residue classes. These classes are determined by the remainder after division.

The modulus must always be set in advance; for example $n = 2, n = 5, n = 15$.

Remainders are always $0, \dots, n - 1$.

Topic hierarchy

[3.1: Modulo Operation](#)

[3.2: Modulo Arithmetic](#)

[3.3: Divisibility rules revisited](#)

[3.E: Exercises](#)

Thumbnail picture By Function_color_example_3.gif: Wvbailey. The original uploader was Wvbailey at English Wikipedia derivative work: Zerodamage [CC BY-SA 3.0 (<https://creativecommons.org/licenses/by-sa/3.0>) or GFDL (<http://www.gnu.org/copyleft/fdl.html>)], via Wikimedia Commons

3: Modular Arithmetic is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

3.1: Modulo Operation

Definition: Modulo

Let $m \in \mathbb{Z}_+$.

a is congruent to b modulo m denoted as $a \equiv b \pmod{m}$, if a and b have the remainder when they are divided by m , for $a, b \in \mathbb{Z}$.

Example 3.1.1:

Suppose $n = 5$, then the possible remainders are 0, 1, 2, 3, and 4, when we divide any integer by 5.

Is $6 \equiv 11 \pmod{5}$? Yes, because 6 and 11 both belong to the same congruent/residue class 1. That is to say when 6 and 11 are divided by 5 the remainder is 1.

Is $7 \equiv 15 \pmod{5}$? No, because 7 and 15 do not belong to the same congruent/residue class. Seven has a remainder of 2, while 15 has a remainder of 0, therefore 7 is not congruent to $15 \pmod{5}$. That is $7 \not\equiv 15 \pmod{5}$.

Example 3.1.2: Clock arithmetic

Find $18 : 00$, that is find $18 \pmod{12}$.

Solution

$18 \pmod{12} \equiv 6$. 6 pm.

Properties

Let $n \in \mathbb{Z}_+$. Then

Theorem 1 :

Two integers a and b are said to be congruent modulo n , $a \equiv b \pmod{n}$, if all of the following are true:

- a) $m \mid (a - b)$.
- b) both a and b have the same remainder when divided by n .
- c) $a - b = kn$, for some $k \in \mathbb{Z}$.

NOTE: Possible remainders of n are $0, \dots, n - 1$.

Reflexive Property

Theorem 2:

The relation " $\equiv$ " over $\mathbb{Z}$ is reflexive.

Proof: Let $a \in \mathbb{Z}$.

Then $a - a = 0 \pmod{n}$, and $0 \in \mathbb{Z}$.

Hence $a \equiv a \pmod{n}$.

Thus congruence modulo n is Reflexive.

Symmetric Property

Theorem 3:

The relation " $\equiv$ " over $\mathbb{Z}$ is symmetric.

Proof: Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$.

Then $a - b = kn$, for some $k \in \mathbb{Z}$.

Now $b - a = (-k)n$ and $-k \in \mathbb{Z}$.

Hence $b \equiv a \pmod{n}$.

Thus the relation is symmetric.

Antisymmetric Property

Is the relation " $\equiv$ " over $\mathbb{Z}$ antisymmetric?

Counter Example: n is fixed

choose: $a = n + 1, b = 2n + 1$, then

$a \equiv b \pmod{n}$ and $b \equiv a \pmod{n}$

but $a \neq b$.

Thus the relation " $\equiv$ " on $\mathbb{Z}$ is not antisymmetric.

Transitive Property

Theorem 4 :

The relation " $\equiv$ " over $\mathbb{Z}$ is transitive.

Proof: Let $a, b, c \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Then $a = b + kn, k \in \mathbb{Z}$ and $b = c + hn, h \in \mathbb{Z}$.

We shall show that $a \equiv c \pmod{n}$.

Consider $a = b + kn = (c + hn) + kn = c + (hn + kn) = c + (h + k)n, h + k \in \mathbb{Z}$.

Hence $a \equiv c \pmod{n}$.

Thus congruence modulo n is transitive.

Theorem 5:

The relation " $\equiv$ " over $\mathbb{Z}$ is an equivalence relation.

Modulo classes

Let $m \in \mathbb{Z}_+$. The relation $\equiv$ on $\mathbb{Z}$ by $a \equiv b$ if and only if $m | (a - b)$, is an equivalence relation. The Classes of $\pmod{m}$ have the following equivalence classes:

$[0], [1], [2], \dots, [m-1]$.

Example of writing equivalence classes:

Example 3.1.3:

The equivalence classes for $\pmod{3}$ are (need to show steps):

$[0] = \{x \in \mathbb{Z} : x \sim 0\} = \{x \in \mathbb{Z} : x \equiv 0 \pmod{3}\}$	$[1] = \{x \in \mathbb{Z} : x \sim 1\} = \{x \in \mathbb{Z} : x \equiv 1 \pmod{3}\}$	$[2] = \{x \in \mathbb{Z} : x \sim 2\} = \{x \in \mathbb{Z} : x \equiv 2 \pmod{3}\}$
$= \{x \in \mathbb{Z} : 3 \mid (x - 0)\} = \{x \in \mathbb{Z} : 3 \mid x\}$	$= \{x \in \mathbb{Z} : 3 \mid (x - 1)\} = \{x \in \mathbb{Z} : 3 \mid (x - 1)\}$	$= \{x \in \mathbb{Z} : 3 \mid (x - 2)\} = \{x \in \mathbb{Z} : 3 \mid (x - 2)\}$
$= \{x \in \mathbb{Z} : x = 3m, m \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$	$= \{x \in \mathbb{Z} : x = 3m + 1, m \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$	$= \{x \in \mathbb{Z} : x = 3m + 2, m \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$

Computational aspects:

Finding "mod 5"

```
%%python3
print( "integer integer mod 5")
for i in range(30):
    print(i, " ", i%5)
```

Code 3.1.1 (Python):

```
%%python3
```

This page titled [3.1: Modulo Operation](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

3.2: Modulo Arithmetic

In this section, we will explore arithmetic operations in a modulo world.

Let $n \in \mathbb{Z}_+$.

Theorem 5 :

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $(a + c) \equiv (b + d) \pmod{n}$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

We shall show that $(a + c) \equiv (b + d) \pmod{n}$.

Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, $n \mid (a - b)$ and $n \mid (c - d)$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(a + c) - (b + d) = a - b + c - d = n(k + l)$, $k + l \in \mathbb{Z}$.

Hence $(a + c) \equiv (b + d) \pmod{n}$. $\square$

Theorem 6:

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $(ac) \equiv (bd) \pmod{n}$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

We shall show that $(ac) \equiv (bd) \pmod{n}$.

Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, $n \mid (a - b)$ and $n \mid (c - d)$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(ac) - (bd) = (b + nk)(d + nl) - bd = bnl + dnk + n^2lk = n(bl + dk + nlk)$,
 $(bl + dk + nlk) \in \mathbb{Z}$.

where

Hence $(ac) \equiv (bd) \pmod{n}$. $\square$

Theorem 7:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$. Then $a^2 \equiv b^2 \pmod{n}$.

Proof:

Let $a, b \in \mathbb{Z}$, and $n \in \mathbb{Z}_+$, such that $a \equiv b \pmod{n}$.

We shall show that $a^2 \equiv b^2 \pmod{n}$.

Since $a \equiv b \pmod{n}$, $n \mid (a - b)$.

Thus $(a - b) = nx$, where $x \in \mathbb{Z}$.

Consider $(a^2 - b^2) = (a + b)(a - b) = (a + b)(nx) = n(ax + bx)$, $ax + bx \in \mathbb{Z}$.

Hence $n \mid a^2 - b^2$, therefore $a^2 \equiv b^2 \pmod{n}$. $\square$

Theorem 8:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$. Then $a^m \equiv b^m \pmod{n}$, $\forall m \in \mathbb{Z}$.

Proof:

Exercise.

By using the above result we can solve many problems. Some of them are discussed below:

Example 3.2.1: $\text{mod } 3$ Arithmetic

Let $n = 3$.

Addition

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

Multiplication

x	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Example 3.2.2: $\text{mod } 4$ Arithmetic

Let $n = 4$.

x	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Example 3.2.3:

Find the remainder when $(101)(103)(107)(109)$ is divided by 11.

Answer

$$101 \equiv 2(\text{mod } 11)$$

$$103 \equiv 4(\text{mod } 11)$$

$$107 \equiv 8(\text{mod } 11)$$

$$109 \equiv 10(\text{mod } 11)$$

Therefore,

$$(101)(103)(107)(109) \equiv (2)(4)(8)(10)(\text{mod } 11) \equiv 2(\text{mod } 11)$$

Example 3.2.4:

Find the remainder when 7^{1453} is divided by 8.

Answer

$$7^0 \equiv 1(\text{mod } 8)$$

$$7^1 \equiv 7(\text{mod } 8)$$

$$7^2 \equiv 1(\text{mod } 8)$$

$$7^3 \equiv 7(\text{mod } 8),$$

As there is a consistent pattern emerging and we know that 1453 is odd, then $7^{1453} \equiv 7(\text{mod } 8)$. Thus the remainder is 7.

Example 3.2.5:

Find the remainder when 7^{2020} is divided by 18.

Answer

$$7^0 \equiv 1(\text{mod } 18)$$

$$7^1 \equiv 7(\text{mod } 18)$$

$$7^2 \equiv 13(\text{mod } 18)$$

$$7^3 \equiv 1(\text{mod } 18),$$

As there is a consistent pattern emerging and we know that $2020 = (673)3 + 1$,
 $7^{2020} = 7^{(673)3+1} = (7^3)^{673}7^1 \equiv 7(\text{mod } 18)$. Thus the remainder is 7.

Example 3.2.6:

Find the remainder when 26^{1453} is divided by 3.

Odd and Even integers:

An integer n is even iff $n \equiv 0(\text{mod } 2)$.

An integer n is odd iff $n \equiv 1(\text{mod } 2)$.

Two integers a and b are said to have same parity if they are both even or both odd otherwise a and b are said to have different parity.

Example 3.2.6:

Show that the sum of an odd integer and an even integer is odd.

Answer

Proof: Let a be an odd integer and let b be an even integer. We shall show that $a + b$ is odd by using the language of congruency.

Since a is odd, $a \equiv 1(\text{mod } 2)$.

Since b is even, $b \equiv 0(\text{mod } 2)$.

Then $(a + b) \equiv (1 + 0)(\text{mod } 2)$,

$$(a + b) \equiv 1(\text{mod } 2).$$

Hence $a + b$ is odd. $\square$

Example 3.2.7:

Show that the product of an odd integer and an even integer is even.

Answer

Proof: Let a be an odd integer and let b be an even integer. We shall show that ab is even by using the language of congruency.

Since a is odd, $a \equiv 1 \pmod{2}$.

Since b is even, $b \equiv 0 \pmod{2}$.

Then $(ab) \equiv (1)(0) \pmod{2}$,

$$(ab) \equiv 0 \pmod{2}.$$

Hence ab is even. $\square$

Example 3.2.8:

Show that $n^2 + 1$ is not divisible by 3 for any integer n .

Answer

Proof: Let $n \in \mathbb{Z}$. We shall show that $(n^2 + 1)$ is not divisible by 3 using the language of congruency.

We shall show that $(n^2 + 1) \pmod{3} \neq 0$ by examining the possible cases.

Case 1: $n \equiv 0 \pmod{3}$.

$$n^2 \equiv 0^2 \pmod{3}.$$

$$(n^2 + 1) \equiv 1 \pmod{3}.$$

Hence $n^2 + 1$ is not divisible by 3.

Case 2: $n \equiv 1 \pmod{3}$.

$$n^2 \equiv 1^2 \pmod{3}.$$

$$(n^2 + 1) \equiv 1 \pmod{3}.$$

Hence $n^2 + 1$ is not divisible by 3.

Case 3: $n \equiv 2 \pmod{3}$.

$$n^2 \equiv 2^2 \pmod{3} \equiv 1 \pmod{3}.$$

$$(n^2 + 1) \equiv 2 \pmod{3}.$$

Hence $n^2 + 1$ is not divisible by 3.

Since none of the possible cases is congruent to $0 \pmod{3}$, $n^2 + 1$ is not divisible by 3. $\square$

Example 3.2.9:

Show that $5 \mid a^5 + 4a$ for any integer a .

Answer

Notice that $4 \equiv -1 \pmod{5}$. Therefore, $5 \mid a^5 + 4a$ iff $5 \mid a^5 - a$ for all integer a .

Let $a \in \mathbb{Z}$.

We shall show that $a^5 \equiv a \pmod{5}$, $\forall a \in \mathbb{Z}$.

Then $5 \mid (a^5 - a)$ and $a^5 - a \equiv 0 \pmod{5}$.

We will proceed by examining the 5 possible cases of $a \pmod{5}$. Specifically, $a \in \{0, 1, 2, 3, 4\}$.

Case $a = 0$: If $a = 0$ then $a^5 = 0^5$

$$\equiv 0 \pmod{5}.$$

Thus $a^5 - a \equiv 0 \pmod{5}$.

Case $a = 1$: If $a = 1$ then $a^5 = 1^5$

$$\equiv 1 \pmod{5}.$$

Thus $a^5 - a \equiv 0 \pmod{5}$.

Case $a = 2$: If $a = 2$ then $a^5 = 2^5$

$$= 5(6) + 2$$

$$\equiv 2 \pmod{5}.$$

Thus $a^5 - a \equiv 0 \pmod{5}$.

Case $a = 3$: If $a = 3$ then $a^5 = 3^5$

$$= 5(48) + 3$$

$$\equiv 3 \pmod{5}.$$

Thus $a^5 - a \equiv 0 \pmod{5}$.

Case $a = 4$: If $a = 4$ then $a^5 = 4^5$

$$= 5(204) + 4$$

$$\equiv 4 \pmod{5}.$$

Thus $a^5 - a \equiv 0 \pmod{5}$.

Having examined all possible cases, $a^5 \equiv a \pmod{5}$. $\square$

Answer

Let $a \equiv b \pmod{5}$ where $a \in \mathbb{Z}$ and $b \in \{0, 1, 2, 3, 4\}$.

Then $5 | (a - b)$.

Thus $a - b = 5m, m \in \mathbb{Z}$. Rearranging, we obtain $a = 5m + b$.

Consider $a^5 = (5m + b)^5$

$$= \sum_{k=0}^5 \binom{5}{k} (5m)^{5-k} \cdot b^k$$

$$= \left(\sum_{k=0}^4 \binom{5}{k} (5m)^{5-k} \cdot b^k \right) + b^5$$

$$= 5m \cdot \left(\sum_{k=0}^4 \binom{5}{k} (5m)^{4-k} \cdot b^k \right) + b^5.$$

$$\text{Let } q = m \cdot \left(\sum_{k=0}^4 \binom{5}{k} (5m)^{4-k} \cdot b^k \right).$$

Since $k, m, b \in \mathbb{Z}$, then $q \in \mathbb{Z}$.

Thus $a^5 = 5q + b^5$.

Clearly, $5 | 5q$. We shall examine the possible cases of b^5 .

Case $b=0$: If $b = 0$ then $a^5 = 5q + 0^5$. Thus $a^5 \equiv 0 \pmod{5}$.

Case $b=1$: If $b = 1$ then $a \equiv 1 \pmod{5}$ and $a^5 = 5q + 1$ where $q \in \mathbb{Z}$.

Thus $a^5 \equiv 5q + 1 \pmod{5} \equiv 1 \pmod{5}$.

Case $b=2$: If $b = 2$ then $a \equiv 2 \pmod{5}$ and $2^5 = 5(6) + 2$.

Thus $a^5 \equiv 5q + 5(6) + 2 \pmod{5} \equiv 5(q + 6) + 2 \equiv 2 \pmod{5}$.

Case $b=3$: If $b=3$ then $a \equiv 3 \pmod{5}$ and $3^5 = 5(48) + 3$.

Thus $a^5 \equiv 5q + 5(48) + 3 \pmod{5} \equiv 5(q + 48) + 3 \equiv a \pmod{5}$.

Case $b=4$: If $b=4$ then $a \equiv 4 \pmod{5}$ and $4^5 = 5(204) + 4$.

Thus $a^5 \equiv 5q + 5(204) + 4 \pmod{5} \equiv 5(q + 204) + 4 \equiv a \pmod{5}$.

Having examined all possible cases, $a^5 \equiv a \pmod{5}$. $\square$

Example 3.2.10

For every positive integer n , prove that $n^3 - n$ is divisible by 3.

Answer

Proof:

Let $S(n)$ be the statement $3 \mid (n^3 - n)$.

$S(n)$ says that $n^3 - n = 3m, m \in \mathbb{Z}$.

$S(1)$ says that $1^3 - 1 = 3m, m \in \mathbb{Z}$. Since $0 = 3(0)$ and $0 \in \mathbb{Z}$, $S(1)$ is true.

Assume $S(n)$ is true for some $k = n$.

We will show that $S(k+1)$ is true.

Specifically, we will show that $(k+1)^3 - (k+1) = 3l, l \in \mathbb{Z}$.

Consider that $(k+1)^3 - (k+1) = (k+1)^3 - (k+1)$

$$= k^3 + 3k^2 + 3k + 1 - k - 1$$

$$= (k^3 - k) + 3k^2 + 3k$$

$$= 3m + 3k^2 + 3k$$

$$= 3(m + k^2 + k).$$

Since $m, k \in \mathbb{Z}$, $m + k^2 + k \in \mathbb{Z}$.

Let $l = m + k^2 + k$.

Thus $(k+1)^3 - (k+1) = 3l, l \in \mathbb{Z}$.

Having shown the inductive step, for every positive integer n , $n^3 - n$ is divisible by 3.

ISBN Check Digit

ISBN is the abbreviation for the International Standard Book Number. ISBN numbers are 10 digits in length. In an ISBN of the form X-XX-XXXXXX-X:

- The first block of digits on the left represents the language of the book (0 is used to represent English).
- The second block of digits represents the publisher.
- The third block of digits represents is the number assigned to the book by the publishing company.
- The fourth block consists of the check digit.

Consider the ISBN 0-13-190190-?

To determine the check digit for this Book Number, follow the below steps.

Step 1: Multiply all nine assigned digits by weighted values. The weighted values are 1 for the first digit from the left, 2 for the second digit, three for the third digit, etc.

$$1 * 0 + 2 * 1 + 3 * 3 + 4 * 1 + 5 * 9 + 6 * 0 + 7 * 1 + 8 * 9 + 9 * 0 = 139 \quad .$$

Step 2: ISBN uses $(\text{mod } 11)$ to determine the check digit. So $139 = 11(11) + 7$ so $139 \equiv 7(\text{mod } 11)$. Hence the check digit is 7. Note that X is used for 10.

If someone orders a book by the ISBN number then the check digit is a way of ensuring that the number was reported and recorded correctly so that the correct book is obtained.

This page titled [3.2: Modulo Arithmetic](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

3.3: Divisibility rules revisited

Thinking out Loud

Can any integer n be written as a sum of distinct powers of 2?

Example 3.3.1:

Express 2019 as a sum of distinct powers of 2?

Note that, $10 \equiv 1 \pmod{3}$, $10 \equiv 1 \pmod{9}$, and $10 \equiv (-1) \pmod{11}$.

Let $x \in \mathbb{Z}_+$.

Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0, \quad (3.3.1)$$

which implies

$$x = 10(d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_2 10 + d_1) + d_0. \quad (3.3.2)$$

Thus we can express x as $10a + b$, where $b = d_0$ is the ones digit of x , and $a = d_n 10^{n-1} + d_{n-1} 10^{n-2} + \cdots + d_2 10 + d_1$.

Divisibility by $2 = 2^1$:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $2 \mid x$ iff $2 \mid d_0$. In other words, 2 divides an integer iff the ones digit of the integer is either 0, 2, 4, 6, or 8. That is, $x \equiv 0 \pmod{2}$ iff $d_0 \equiv 0 \pmod{2}$.

Proof:

Since $10 \equiv 0 \pmod{2}$ and $x = 10a + b$, $x \equiv 0 \pmod{2}$ iff $d_0 \equiv 0 \pmod{2}$. $\square$

Divisibility by 5:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $5 \mid x$ iff $5 \mid d_0$. In other words, 5 divides an integer iff the ones digit of the integer is either 0, or 5.

That is, $x \equiv 0 \pmod{5}$ iff $d_0 \equiv 0 \pmod{5}$.

Proof:

Since $10 \equiv 0 \pmod{5}$ and $x = 10a + b$, $x \equiv 0 \pmod{5}$ iff $d_0 \equiv 0 \pmod{5}$. $\square$

Divisibility by 10:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $10 \mid x$ iff $10 \mid d_0$. In other words, 10 divides an integer iff the ones digit of the integer is 0.

That is, $x \equiv 0 \pmod{10}$ iff $d_0 \equiv 0 \pmod{10}$.

Proof:

Since $10 \equiv 0 \pmod{10}$ and $x = 10a + b$, $x \equiv 0 \pmod{10}$ iff $d_0 \equiv 0 \pmod{10}$. $\square$

Divisibility by $4 = 2^2$:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $4 \mid x$ iff $4 \mid d_1 d_0$. That is, $x \equiv 0 \pmod{4}$ iff $d_1 d_0 \equiv 0 \pmod{4}$.

Proof:

Let x be an integer. Then

$x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_2 10^2 + d_1 10^1 + d_0$, which implies

$$x = 100(d_n 10^{n-2} + d_{n-1} 10^{n-3} + \cdots + d_2) + 10d_1 + d_0 = 100(d_n 10^{n-2} + d_{n-1} 10^{n-3} + \cdots + d_2) + d_1 d_0.$$

Since $100 \equiv 0 \pmod{4}$, $x = 100a + d_1 d_0$, $x \equiv 0 \pmod{4}$ iff $d_1 d_0 \equiv 0 \pmod{4}$. $\square$

Divisibility by $8 = 2^3$:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $8 \mid x$ iff $8 \mid d_2 d_1 d_0$. That is. $x \equiv 0 \pmod{8}$ iff $d_2 d_1 d_0 \equiv 0 \pmod{8}$.

Proof:

Let x be an integer. Then

$x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0$, which implies

$$x = 10^3(d_n 10^{n-3} + d_{n-1} 10^{n-4} + \dots + d_3) + 100d_2 + 10d_1 + d_0 = 10^3(d_n 10^{n-3} + d_{n-1} 10^{n-4} + \dots + d_3) + d_2 d_1 d_0 .$$

Since $1000 \equiv 0 \pmod{8}$, $x = 1000a + d_2 d_1 d_0$, $x \equiv 0 \pmod{8}$ iff $d_2 d_1 d_0 \equiv 0 \pmod{8}$. $\square$

A similar argument can be made for divisibility by 2^n , for any positive integer n . The following results follows from the fact that,

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 = d_n(10^n - 1) + d_{n-1}(10^{n-1} - 1) + \dots + d_2(10^2 - 1) + d_1(10^1 - 1) + (d_n + d_{n-1} + \dots + d_1 + d_0)$$

Divisibility by 3 :

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $3 \mid x$ iff 3 divides sum of its digits.

Proof:

Let x be an integer. Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 , \quad \text{which} \quad \text{implies}$$

$$x = d_n(10^n - 1) + d_{n-1}(10^{n-1} - 1) + \dots + d_2(10^2 - 1) + d_1(10^1 - 1) + (d_n + d_{n-1} + \dots + d_1 + d_0) .$$

Hence,

$$x \pmod{3} \equiv d_n(10^n - 1) + d_{n-1}(10^{n-1} - 1) + \dots + d_2(10^2 - 1) + d_1(10^1 - 1) \pmod{3} + (d_n + d_{n-1} + \dots + d_1 + d_0) \pmod{3} .$$

Notice that $(10^n - 1) \equiv 0 \pmod{3}$, for all positive integer n .

Therefore, $x \pmod{3} \equiv (d_n + d_{n-1} + \dots + d_1 + d_0) \pmod{3}$.

Thus, $3 \mid x$ iff 3 divides sum of its digits.

Divisibility by $9 = 3^2$:

Let $x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 \in \mathbb{Z}_+$, then $9 \mid x$ iff 9 divides sum of its digits.

Proof:

Let x be an integer. Then

$$x = d_n 10^n + d_{n-1} 10^{n-1} + \dots + d_2 10^2 + d_1 10^1 + d_0 , \quad \text{which} \quad \text{implies}$$

$$x = d_n(10^n - 1) + d_{n-1}(10^{n-1} - 1) + \dots + d_2(10^2 - 1) + d_1(10^1 - 1) + (d_n + d_{n-1} + \dots + d_1 + d_0) .$$

Hence,

$$x \pmod{9} \equiv d_n(10^n - 1) + d_{n-1}(10^{n-1} - 1) + \dots + d_2(10^2 - 1) + d_1(10^1 - 1) \pmod{9} + (d_n + d_{n-1} + \dots + d_1 + d_0) \pmod{9} .$$

Notice that $(10^n - 1) \equiv 0 \pmod{9}$, for all positive integer n .

Therefore, $x \pmod{9} \equiv (d_n + d_{n-1} + \dots + d_1 + d_0) \pmod{9}$.

Thus, $9 \mid x$ iff 9 divides sum of its digits.

Divisibility by 7 :

$7 \mid x$ iff 7 divides the absolute difference between $a - 2b$, where $x = 10a + b$, and, $b = d_0$ is the ones digit of x and $a = d_n 10^{n-1} + d_{n-1} 10^{n-2} + \dots + d_2 10 + d_1$.

Proof:

Divisibility by 11 :

$11 \mid x$ iff 11 divides the absolute difference between alternate sum.

Proof:

This page titled [3.3: Divisibility rules revisited](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

3.E: Exercises

Exercise 3.E.1:

Let $a, b, c \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$.

Show that $ac \equiv bc \pmod{n}$.

Exercise 3.E.2:

Find the remainder when $(201)(203)(205)(207)$ is divided by 13.

Exercise 3.E.3:

Show that the sum of 2 odd integers is even.

Exercise 3.E.4:

Given that February 14, 2018, is a Wednesday, what day of the week will February 14, 2090 be?

Exercise 3.E.5:

Find the remainder when 8^{1789} is divided by 28.

Exercise 3.E.6:

Find the remainder,

1. when 3^{1798} is divided by 28.
2. when 2^{1798} is divided by 28.
3. when 7^{5453} is divided by 8.
4. when $3^{135} + 15^2$ is divided by 7.

3.E.7 Exercise :

Given a positive integer x , rearrange its digits to form another integer y . Explain why $x - y$ is divisible by 9.

Exercise 3.E.8

Prove that for all integer $n \geq 1$, 6 divides $n^3 - n$.

Exercise 3.E.9

Compute the last two digits of 9^{1600} .

Exercise 3.E.10

Show that $a^2 + b^2 \not\equiv 3 \pmod{4}$ for any integers a and b .

Exercise 3.E.11

Let a be an odd integer. Show that $a^2 \equiv 1 \pmod{8}$.

3.E: Exercises is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by LibreTexts.

CHAPTER OVERVIEW

4: Greatest Common Divisor, least common multiple and Euclidean Algorithm

- 4.1: Greatest Common Divisor
- 4.2: Euclidean algorithm and Bezout's algorithm
- 4.3: Least Common Multiple
- 4.4: Relatively Prime numbers
- 4.5: Linear Congruences
- 4.E: Exercises

4: Greatest Common Divisor, least common multiple and Euclidean Algorithm is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

4.1: Greatest Common Divisor

Think out loud

We want to tile a 253 ft by 123 ft ($a = 253$ and $b = 123$, with $a, b \in \mathbb{Z}$) floor with identical square tiles. What is the largest square tile we can use?

Definition: Greatest Common Divisor

Let $a, b \in \mathbb{Z}$, where a, b not both zero.

Then, we say that an integer $d = \gcd(a, b) \in \mathbb{Z}_+$, greatest common divisor if it satisfies the following conditions:

1. $d|a$ and $d|b$, Note: d must divide both numbers

If $c \in \mathbb{Z}$, $c|a$ and $c|b$ then $c \leq d$. Note: d is the greatest number that divides both.

Thus the greatest common divisor of two integers a and b , also known as GCD of a and b , is the greatest positive integer that divides the two integers. This class will use the following notation: $\gcd(a, b)$.

Example 4.1.1:

What is the gcd of 15 and 20?

A process to find the solution:

List all positive divisors of 15 and 20.

The positive divisors of 15 are 1, 3, 5, and 15.

The positive divisors of 20 are 1, 2, 4, 5, 10, and 20.

The common positive divisors are 1, 5.

As you can see from the list the gcd of 15 and 20 is 5. That is, the $\gcd(15, 20) = 5$.

Example 4.1.2:

An elementary gym teacher has 3 grade 4 gym classes with 21, 35 and 28 students in them. The teacher wants to order equipment that equal-sized groups can use in each class. What is the largest group size that will work for all 3 classes?

Solution:

You will need to find the GCD of all 3 classes.

Firstly, you will find the GCD of 21 and 35.

The positive divisors of 21 are 1, 3, 7, and 21.

The positive divisors of 35 are 1, 5, 7, and 35.

The GCD of 21 and 35 is 7.

Since $7 | 28$ you will now find the GCD of 7 and 28, which turns out to be 7.

Therefore the GCD of 21, 35 and 28 is 7.

Thus, the largest number of students in a group for each class will be 7.

Properties:

Let $a, b, c \in \mathbb{Z}$. This section introduces a binary operation on $\mathbb{Z}$.

Then:

1. $\gcd(a, a) = |a|, a \neq 0$.
2. $\gcd(a, b) = \gcd(b, a)$.
3. $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.
4. $\gcd(a, 0) = a$.
5. $\gcd(0, 0)$ is undefined.

In the next section, we will learn an algorithm to calculate GCD.

Practical Uses:

There are many real-world applications for learning the greatest common divisor (gcd).

- Fractions
- Algebra
- Foundational word problem skills
- Ratios
- Recipes
- Group arrangements

This page titled [4.1: Greatest Common Divisor](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

4.2: Euclidean algorithm and Bezout's algorithm

Definition: Euclidean Algorithm

The *Euclidean Algorithm* is an efficient way of computing the GCD of two integers. It was discovered by the Greek mathematician Euclid, who determined that if n goes into x and y , it must go into $x-y$. Therefore, we can subtract the smaller integer from the larger integer until the remainder is less than the smaller integer. We continue using this process until the remainder is 0, thus leaving us with our GCD.

If $a, b \in \mathbb{Z} \setminus \{0\}$, then by using division algorithm iteratively, we obtain

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ r_0 &= r_1q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_n &= r_nq_{n+1} + 0 \end{aligned}$$

Notice that, the last non-zero remainder is r_n , such an r_n exists, since $|b| > |r_0| > |r_1| > \dots > |r_n|$. The $r_n = \gcd(a, b)$.

Example 4.2.1:

Find the GCD of 30 and 650 using the Euclidean Algorithm.

$650 / 30 = 21 \text{ R } 20$. Now take the remainder and divide that into the original divisor.

$30 / 20 = 1 \text{ R } 10$. Now take the remainder and divide that into the previous divisor.

$20 / 10 = 2 \text{ R } 0$. Since we have a remainder of 0, we know that the divisor is our GCD.

Therefore, the GCD of 30 and 650 is 10.

Example 4.2.2:

Find $\gcd(2420, 230)$

Note: Work from right to left to follow the steps shown in the image below.

$$\begin{array}{r} 11 \\ 10 \overline{) 110} \\ \underline{100} \\ 10 \\ \underline{10} \\ 0 \end{array} \quad \begin{array}{r} 1 \\ 110 \overline{) 120} \\ \underline{110} \\ 10 \end{array} \quad \begin{array}{r} 1 \\ 120 \overline{) 230} \\ \underline{120} \\ 110 \end{array} \quad \begin{array}{r} 10 \\ 230 \overline{) 2420} \\ \underline{2300} \\ 120 \end{array}$$

Hence, $\gcd(2420, 230) = 10$

Example 4.2.3:

Find $\gcd(3915, 825)$

Note: Work from right to left to follow the steps shown in the image below.

$$\begin{array}{r}
 13 \\
 15 \overline{)195} \\
 \underline{150} \\
 45 \\
 \underline{45} \\
 0
 \end{array}
 \quad
 \begin{array}{r}
 1 \\
 195 \overline{)210} \\
 \underline{195} \\
 15
 \end{array}
 \quad
 \begin{array}{r}
 2 \\
 210 \overline{)615} \\
 \underline{420} \\
 195
 \end{array}
 \quad
 \begin{array}{r}
 1 \\
 615 \overline{)825} \\
 \underline{615} \\
 210
 \end{array}
 \quad
 \begin{array}{r}
 4 \\
 825 \overline{)3915} \\
 \underline{3300} \\
 615
 \end{array}$$

Hence, $\gcd(3915, 825) = 15$

Example 4.2.4: Geometric GCD

We want to tile an a ft by b ft ($a, b \in \mathbb{Z}$) floor with identical square tiles. What is the largest square tile we can use? $\gcd(a, b)$. Consider the following example where $a = 100$ and $b = 44$.

The Euclidean algorithm:

$$100 = 2 \times 44 + 12$$

$$44 = 3 \times 12 + 8$$

$$12 = 1 \times 8 + 4$$

$$8 = 2 \times 4 + 0$$

So $GCD(100, 44) = 4$.



The largest square tile we can use to completely tile a 100 ft by 44 ft floor is a 4 ft by 4 ft tile.

BEZOUT'S IDENTITY

For integers a and b , let d be the greatest common divisor, $d = \gcd(a, b)$. Then there exists integers x and y such that $ax + by = d$. Any integer that is of the form $ax + by$, is a multiple of d .

Note

This condition will be a necessary and sufficient condition in the case of $d = 1$. We will prove this result in section 4.4, Relatively Prime numbers.

Bezout Algorithm

Use the Euclidean Algorithm to determine the GCD, then work backwards using substitution. WHEN DOING SUBSTITUTION BE VERY CAREFUL OF THE POSITIVES AND NEGATIVES.

Example 4.2.5

Find the Bezout Identity for $a=34$ and $b=19$.

Solution

First, find the $\gcd(34, 19)$.

$$34 = 19(1) + 15.$$

$$19 = 15(1) + 4.$$

$$15 = 4(3) + 3.$$

$$4 = 3(1) + 1.$$

$$3 = 1(3) + 0.$$

Thus, the $\gcd(34, 19) = 1$.

Next, work backwards to find x and y .

$$1 = 4 - 1(3).$$

$$= 4 - 1(15 - 4(3)) = 4(4) - 1(15).$$

$$= 4(19 - 15(1)) - 1(15) = 4(19) - 5(15).$$

$$= 4(19) - 5(34 - 19(1)) = 9(19) - 5(34).$$

Thus Bezout's Identity for $a=34$ and $b=19$ is $1 = 34(-5) + 19(9)$.

Example 4.2.6: Tabular Method, yielding GCD and Bezout's Coefficients

Find Bezout's Identity for $a = 237$ and $b = 13$.

Solution:

(1) Set up the initial table. This step is always the same regardless of which numbers you are trying to find the GCD of.	Iteration	Remainder	Quotient	Coefficients of Bezout's	
	i	r	q	s	t
	0			1	0
	1			0	1
	2				

(2) Insert numerator into R_0C_1 (3) Insert denominator into R_1C_1 (4) Integer divide R_0C_1 by R_1C_1 and place result into R_1C_2	i	r	q	s	t
	0	237		1	0
	1	13	18	0	1

(5) Place remainder from (4) into R_2C_1

Table at right shows completed steps 1 - 5 of $\text{GCD}(237,13)$.
Note: $237/13 = 18 \text{ R } 3$

2	3			
---	---	--	--	--

(6) add new line to table, increment i.

(7) R_iC_2 is integer division $R_{i-1}C_1/R_iC_1$

(8) Place remainder from (7) into $R_{i+1}C_1$

Note: $13/3 = 4$

R_1

(9) R_iC_3 is $R_{i-2}C_3 - (R_{i-1}C_2 * R_{i-1}C_3)$

(10) R_iC_4 is $R_{i-2}C_4 - (R_{i-1}C_2 * R_{i-1}C_4)$

i	r	q	s	t
0	237		1	0
1	13	18	0	1
2	3	4	1	-18
3	1			

Repeat steps 6 - 10 until $R_iC_1 = 0$
Completed table for $\text{GCD}(237,13)$ at right.

$\text{GCD}(237,13) = 1 =$ first non zero remainder.

Write answer as:

$$\text{GCD}(237,13) = 1 = -4(237) + 73(13)$$

Iteration	Remainder	Quotient	Coefficients of Bezout's	
i	r	q	s	t
0	237		1	0
1	13	18	0	1
2	3	4	1	-18
3	1	3	-4	73

Where $-4=s$ and $73=t$. The GCD = 1 indicates that the numbers are relatively prime.

4	0			
---	---	--	--	--

Thus, the Bezout's Identity for $a=237$ and $b=13$ is $1 = -4(237) + 73(13)$.

Example 4.2.7:

Find the GCD of 149553 and 177741:

First, use the Euclidean Algorithm to determine the GCD.

$$177741/149553 = 1 \text{ R } 28188$$

$$149553/28188 = 5 \text{ R } 8613$$

$$28188/8613 = 3 \text{ R } 2349$$

$$8613/2349 = 3 \text{ R } 1566$$

$$2349/1566 = 1 \text{ R } 783$$

$$1566/783 = 2 \text{ R } 0$$

Because we have a remainder of 0 we have now determined that 783 is the GCD.

Next, find $x, y \in \mathbb{Z}$ such that $783=149553(x)+177741(y)$.

Using the answers from the division in Euclidean Algorithm, work backwards.

$$783 = 2349 + 1566(-1).$$

$$1566 = 8613 + 2349(-3).$$

$$2349 = 28188 + 8613(-3).$$

$$8613 = 149553 + 28188(-5).$$

$$28188 = 177741 + 149553(-1).$$

Now substitute in,

$$783 = 2349 + 1566(-1).$$

$$= 2349 + (8613 + 2349(-3))(-1)$$

$$= 2349 + (8613(-1) + 2349(3))$$

$$= 2349(4) + 8613(-1)$$

$$= (28188 + 8613(-3))(4) + 8613(-1)$$

$$= 28188(4) + 8613(-13)$$

$$= 28188(4) + (149553 + 28188(-5))(-13)$$

$$= 28188(69) + 149553(-13)$$

$$= (177741 + 149553(-1))(69) + 149553(-13)$$

$$= 177741(69) + 149553(-82)$$

Thus, Bezout's Identity is $783=177741(69)+149553(-82)$.

Example 4.2.8:

Let $a, b \in \mathbb{Z}$. If $ax + by = 12$ for some integers x and y . Then what are the possible values for $\gcd(a, b)$. For these values find possible values for a, b, x and y .

Answer

a	b	x	y	d=gcd(a,b)

This page titled [4.2: Euclidean algorithm and Bezout's algorithm](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

4.3: Least Common Multiple

Definition: Least Common Multiples

Let a and b be integers. Then any integer that is a multiple of both a and b is called a common multiple of a and b . The least common multiple of integers a and b , denoted by $\text{lcm}(a, b)$, is the smallest positive common multiple of a and b .

Example 4.3.1:

Find

1. $\text{lcm}(5, 10)$
2. $\text{lcm}(-6, 18)$
3. $\text{lcm}(0, 5)$

Solution

1. 10, 2. 18 3. undefined.

Finding LCM using GCD

The least common multiple of integers a and b , also known as the LCM, is the smallest number that is divisible by both integers a and b . You can determine the LCM by dividing the absolute value of the product of a and b by the GCD of a and b .

That is

$$\text{lcm}(a, b) = \frac{|ab|}{\text{gcd}(a, b)} \quad (4.3.1)$$

Example 4.3.2:

What is the LCM of 24 and 35?

Solution:

We must first determine the GCD of 24 and 35.

Find the divisors of 24 and 35.

24 : 1, 2, 3, 4, 8, 12, 24

35 : 1, 5, 7, 35

Therefore the GCD of 24 and 35 is 1.

Now that we have determined the GCD, we can continue on to determine the least common multiple.

$$\frac{(24)(35)}{1} = 840.$$

Hence $\text{lcm}(24, 35) = 840$.

Properties:

Let $a, b, c \in \mathbb{Z}$.

Then:

1. $\text{lcm}(a, a) = a$.
2. $\text{lcm}(a, b) = \text{lcm}(b, a)$.
3. $\text{lcm}(a, b, c) = \text{lcm}(\text{lcm}(a, b), c) = \text{lcm}(a, \text{lcm}(b, c))$.
4. $\text{lcm}(a, 0) = \text{undefined}$.

Example 4.3.3:

A lady is carrying a grocery basket full of chocolate Easter bunnies. She drops the basket and all the chocolate bunnies break. When asked how many chocolate bunnies she had, she says that she is poor in arithmetic, but remembers that when she counted the chocolate bunnies by twos, threes, fours and fives she had remainders of 1, 2, 3, and 4 respectively. What is the smallest number of chocolate bunnies that she could have had in the basket?

Solution:

At First, this problem uses modular arithmetic and lcm together.

Let n = the number of chocolate bunnies. Then

$$n \pmod{2} \equiv 1$$

$$n \pmod{3} \equiv 2$$

$$n \pmod{4} \equiv 3$$

$$n \pmod{5} \equiv 4$$

This shows us that the lcm of 2, 3, 4, 5 = $n + 1$.

We need to subtract the 1 from either side to isolate n .

$$\text{Therefore } \text{lcm}(2, 3, 4, 5) - 1 = n.$$

We must now determine the lcm of 2, 3, 4, 5, which is $60 - 1 = 59$.

Therefore the smallest number of chocolate bunnies the lady could have had in her shopping basket was 59.

Example 4.3.3:

Find the smallest positive integer x with following condition: x has remainders 8, 10, 12, and 14 when divided by 11, 13, 15, and 17.

Solution:

We need to find smallest x such that

$$x \equiv 8 \pmod{11},$$

$$x \equiv 10 \pmod{13},$$

$$x \equiv 12 \pmod{15},$$

$$x \equiv 14 \pmod{17}.$$

Since $x \equiv 8 \pmod{11}$, possible values for x are 8, 19, 30, 41, 52, $\dots$, $8 + 11m$ where $m \in \mathbb{Z}$.

Since $x \equiv 10 \pmod{13}$, possible values for x are 10, 23, 46, 59, 72, $\dots$, $10 + 13k$ where $k \in \mathbb{Z}$.

Since $x \equiv 8 \pmod{11}$ and $x \equiv 10 \pmod{13}$, $x = \text{lcm}(11, 13) - 3$.

By similar argument, we can see that if $x \equiv 8 \pmod{11}$, $x \equiv 10 \pmod{13}$, $x \equiv 12 \pmod{15}$, and $x \equiv 14 \pmod{17}$.

$$\text{Then } x = \text{lcm}(11, 13, 15, 17) - 3 = 36465 - 3 = 36462.$$

PRACTICAL USES:

There are multiple real-world applications for using lowest common multiple.

- Fractions
- Ratios
- Recipes
- Algebra
- Distribution between packages
- Meal preparation

4.4: Relatively Prime numbers

Definition: Relatively prime or Coprime

Two integers are relatively prime or Coprime when there are no common factors other than 1. This means that no other integer could divide both numbers evenly. Two integers a, b are called relatively prime to each other if $\gcd(a, b) = 1$.

For example, 7 and 20 are relatively prime.

Theorem

Let $a, b \in \mathbb{Z}$. If there exist integers x and y such that $ax + by = 1$ then $\gcd(a, b) = 1$.

Proof:

Let $a, b \in \mathbb{Z}$, such that $d = \gcd(a, b)$. Then $d|a$ and $d|b$.

Hence $d|(ax + by)$, thus $d|1$. Which implies $d = \pm 1$, since $\gcd$ is the greatest, $d = 1$.

Example 4.4.1:

Suppose a and b are relatively prime integers. Prove that $\gcd(a + b, a - b) = 1$, or 2.

Solution

Let a and b be relatively prime integers. Then $\gcd(a, b) = 1$. Suppose $d = \gcd(a + b, a - b)$. Then $d|(a + b)$ and $d|(a - b)$. Then $a + b = dm$ and $a - b = dn$ for some $m, n \in \mathbb{Z}$. Now $2a = d(m + n)$ and $2b = d(m - n)$. Thus $d|2a$ and $d|2b$. Hence $d|\gcd(2a, 2b)$. Since $\gcd(2a, 2b) = 2\gcd(a, b)$, $d|2$. Thus $d = 1$ or 2.

Example 4.4.2:

Suppose a and c are relatively prime integers and b is an integer such that $b|c$. Prove that $\gcd(a, b) = 1$.

Solution

Let a and c be relatively prime integers. Then $\gcd(a, c) = 1$. Thus there exist integers x and y such that $ax + cy = 1$. Suppose b is an integer such that $b|c$. Then $c = bm$ for some $m \in \mathbb{Z}$. Now $ax + bmy = 1$. Therefore, $\gcd(a, b) = 1$.

Multiplicative inverse modulo m

Let $m \in \mathbb{Z}_+$. Let $a \in \mathbb{Z}$ such that a and m are relatively prime. Then there exist integers x and y such that $ax + my = 1$. Then $ax \equiv 1 \pmod{m}$. Note that 1 is the multiplicative identity on $\text{mod } m$. In this case, $x \pmod{m}$ is the inverse of $a \pmod{m}$.

✓ Example 4.4.3

If possible, find multiplicative inverse of 2 (mod 10).

Solution

Since $\gcd(2, 10) = 2 \neq 1$, 2 has no multiplicative inverse modulo 10.

✓ Example 4.4.4

If possible, find multiplicative inverse of 16 (mod 35).

Solution

By using Euclidean Algorithm, we will find $\gcd(16, 35)$.

$$35 = (16)(2) + 3$$

$$16 = (3)(5) + 1$$

$$3 = (1)(3) + 0$$

Thus $\gcd(16, 35) = 1$. Hence multiplicative inverse of $16 \pmod{35}$ exists.

By using Bezout's algorithm,

$$\begin{aligned} 1 &= 16 + (3)(-5) \\ &= 16 + (35 + (16)(-2))(-5) \\ &= (35)(-5) + (16)(11) \end{aligned}$$

Thus $\gcd(16, 35) = 1 = (35)(-5) + (16)(11)$. Hence the multiplicative inverse of $16 \pmod{35}$ is 11.

4.4: Relatively Prime numbers is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by LibreTexts.

4.5: Linear Congruences

Linear Congruences

Definition: Linear Congruences

A linear congruence in one variable has the form $ax \equiv b \pmod{m}$, where $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$ and $x \in \mathbb{Z}$ is a variable.

A linear congruence is similar to a linear equation, solving linear congruence means finding all integer x that makes, $ax \equiv b \pmod{m}$ true. In this case, we will have only a finite solution in the form of $x \equiv \text{something} \pmod{m}$. Thus there will be at most m solutions, namely $0, 1, \dots, m-1$.

Thus, a linear congruence in one variable x is of the form $ax \equiv b \pmod{m}$, where $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. This form of linear congruence has at most m solutions.) In this section, we shall assume $a(\neq 0) \in \mathbb{Z}$.

Method I: We can find the solutions to a linear congruence, by checking all possible $0, 1, \dots, m-1$.

Example 4.5.1:

Find all solutions to $x \equiv 6 \pmod{11}$, between 0 and 10 inclusive.

Solution

Possible solutions are $0, 1, 2, \dots, 10$ The only solution is 6.

Example 4.5.2:

Find all solutions to $2x \equiv 3 \pmod{7}$, between 0 and 6 inclusive.

Solution

Possible solutions are $0, 1, 2, \dots, 6$ The only solution is 5.

Example 4.5.3:

Solve $3x \equiv 1 \pmod{8}$.

Solution

Possible solutions are $0, 1, 2, \dots, 7$. The only solution is 3.

✓ Example 4.5.4

Find all solutions to $3x \equiv 1 \pmod{6}$, between 0 and 5 inclusive.

Solution

Possible solutions are $0, 1, 2, 3, 4, 5$ In this case $3x \pmod{6}$ is $0, 3, 0, 3, 0, 3$ Thus, $3x \equiv 1 \pmod{6}$ has no solutions.

Example 4.5.5:

Solve $2x \equiv 2 \pmod{4}$.

Solution

Possible solutions are $0, 1, 2, 3$ The solutions are 1 and 3.

The following theorems give a criterion for the solvability of $ax \equiv b \pmod{m}$.

Method II:

Theorem 4.5.1

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. If $\gcd(c, m) = 1$ and $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$

Proof

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. Assume that $\gcd(c, m) = 1$ and $ac \equiv bc \pmod{m}$. Since $ac \equiv bc \pmod{m}$, $ac - bc = mn$, for $n \in \mathbb{Z}$. Thus $(a - b)c = mn$. Thus $m \mid (a - b)c$. Since $\gcd(c, m) = 1$, $m \mid (a - b)$. Hence, $a \equiv b \pmod{m}$.

✓ Example 4.5.6

Solve $3x \equiv 1 \pmod{8}$.

Solution

We will solve using the above theorem. $3x \equiv 1 \equiv 9 \pmod{8}$. Hence, $x \equiv 3 \pmod{8}$.

🔗 Theorem 4.5.2

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. Then $ac \equiv bc \pmod{m}$ if and only if $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$

Proof

TBA

✓ Example 4.5.7

Solve $9x \equiv 6 \pmod{24}$.

Solution

Since $\gcd(3, 24) = 3$, $3x \equiv 2 \pmod{8}$. Thus $3x \equiv 2 \equiv 10 \equiv 18 \pmod{8}$. Hence $x \equiv 6 \pmod{8}$.

The above two methods are tedious when the numbers are large.

🔗 Theorem 4.5.3

Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Then

$ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$. Moreover, if $x = x_0$ is a particular solution to this congruence, then the set of all solutions is $\{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{m}\} = \left\{x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}\right\}$, where $d = \gcd(a, m)$.

Proof

TBA

We will see below how to find the solution for a particular case: Using Multiplicative inverse modulo m

Let $m \in \mathbb{Z}_+$. Let $a \in \mathbb{Z}$ such that a and m are relatively prime. Then there exist integers x and y such that $ax + my = 1$. Then $ax \equiv 1 \pmod{m}$. Note that 1 is the multiplicative identity on $\pmod{m}$. In this case, $x \pmod{m}$ is the inverse of $a \pmod{m}$.

Theorem 4.5.3

If $\gcd(a, m) = 1$ then $ax \equiv b \pmod{m}$ has a unique solution $x \equiv a^{-1}b \pmod{m}$. Thus, the set of all solutions is $\{x \in \mathbb{Z} \mid x \equiv a^{-1}b \pmod{m}\}$.

Proof

Since $\gcd(a, m) = 1$, therefore a has an inverse $a^{-1} \pmod{m}$. Hence $x \equiv a^{-1}b \pmod{m}$.

✓ Example 4.5.8

Solve $16x \equiv 11 \pmod{35}$.

Solution

Since $16x \equiv 11 \pmod{35}$, $x \equiv (16)^{-1}11 \pmod{35} \equiv (11)(11) \pmod{35} \equiv 16 \pmod{35}$.

The following theorem guides on solving linear congruence. However, we will discuss it after learning the linear Diophantine equations.

Theorem 4.5.4

Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Then, the linear congruence

$ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) | b$. Moreover, if $x = x_0$ is a particular solution to this congruence, then the set of all solutions is $\{x \in \mathbb{Z} | x \equiv x_0 \pmod{m}\} = \left\{x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}\right\}$, where $d = \gcd(a, m)$.

The Chinese Remainder Theorem

In this section, we will explore solving simultaneous linear congruences.

Theorem 4.5.5

Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then there exists $x \in \mathbb{Z}$ such that $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$. Moreover x is unique modulo mn .

Example 4.5.5:

Solve $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$.

Solution

Since $x \equiv 2 \pmod{3}$, the possible solutions are 2, 5, 8, 11, 15, ...

Since $x \equiv 3 \pmod{5}$, the possible solutions are 3, 8, 13, ...

Then $x = 8$. Since any y such that $y \equiv 8 \pmod{15}$ are also solutions, we have 23, 38, ...

Theorem 4.5.6: Chinese Remainder Theorem

Let $a_1, \dots, a_k \in \mathbb{Z}$ and $m_1, \dots, m_k \in \mathbb{N}$ such that $\gcd(m_i, m_j) = 1$, for all $i \neq j$. Then there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad (4.5.1)$$

Moreover x is unique modulo $m_1 \dots m_k$.

Note

Solving Congruences, using Chinese Remainder Theorem

Let

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad (4.5.2)$$

Then

Step 1: Calculate the product $M = m_1 \times m_2 \times \dots \times m_k$.

Step 2: Calculate the Modulus Factors. For each m_i , calculate $M_i = \frac{M}{m_i}$.

Step 3: Compute the Inverses. For each M_i , compute the modular inverse M_i^{-1} modulo m_i .

Step 4: Combine Solutions. Finally, the solution x to the system of congruences is given by:

$$x = \left(\sum_{i=1}^k a_i M_i M_i^{-1} \right) \pmod{M} \quad (4.5.3)$$

We can use the following table to compute all the listed variables.

a_i	m_i	M_i	M_i^{-1}	M

✓ Example 4.5.6

Solve

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{8} \end{cases} \quad (4.5.4)$$

Answer

a_i	m_i	M_i	M_i^{-1}	M
3	5	$\frac{280}{5} = 56$	1	280
1	7	$\frac{280}{7} = 40$	3	280
6	8	$\frac{280}{8} = 35$	3	280

First we calculate $M = (5)(7)(8)280$. Now we can calculate M_1 , M_2 and M_3 .

Next we calculate M_1^{-1} , M_2^{-1} and M_3^{-1} .

To calculate M_1^{-1} : we need to solve $56x_1 \equiv 1 \pmod{5}$. Place these values into the table.

Now, $x \equiv ((3)(56)(1) + (7)(40(3) + (8)(35)(3)) \pmod{280} \equiv 918 \pmod{280} \equiv 78 \pmod{280}$.

This page titled [4.5: Linear Congruences](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

4.E: Exercises

Exercise 4.E.1:

Find the gcd of:

- 10 and 75
- 48 and 360
- 9357 and 5864

Answer

	2	1		5		1		8		2		1		1		1
1	2	1	1	0	6	1	2	7	1	1	2	2	2	3	7	1
	2	1	1	0	5	1	0	6	1	0	1	6	2	2	4	4
	0			1		2	1		1	0	6		1	2	7	1

$$1 = (106) - 5(21).$$

$$21 = (127) - 1(106).$$

$$106 = (1122) - 8(127).$$

$$127 = (2371) - 2(1122).$$

$$1122 = (3493) - 1(2371).$$

$$2371 = (5864) - 1(3493).$$

$$3493 = (9357) - 1(5864).$$

$$1 = (106) - 5((127) - 1(106)) = 6(106) - 5(127).$$

$$1 = 6((1122) - 8(127)) - 5(127) = 6(1122) - 53(127).$$

$$1 = 6(1122) - 53((2371) - 2(1122)) = 112(1122) - 53(2371).$$

$$1 = 112((3493) - 1(2371)) - 53(2371) = 112(3493) - 165(2371).$$

$$1 = 112(3493) - 165((5864) - 1(3493)) = 277(3493) - 165(5864).$$

$$1 = 277((9357) - 1(5864)) - 165(5864) = 277(9357) - 442(5864).$$

$$\text{Then } 1 = 277(9357) - 442(5864).$$

Find the lcm of:

- 10 and 75
- 48 and 360
- 9357 and 5864

Exercise 4.E.2:

Using GCD determine how many packages of hotdogs and hotdog buns are needed to have an equal amount if the hotdog package contains 10 hotdogs, and the hotdog bun package contains 12 buns.

Exercise 4.E.3:

Using Euclidean Algorithm, find the gcd of 1716 and 1260, and the LCM of 1716 and 1260.

Exercise 4.E.4:

- Use the Euclidean algorithm to find $\gcd(270, 504)$. Find integers x and y such that

$$\gcd(270, 504) = 270x + 504y. \quad (4.E.1)$$

- Use the Euclidean algorithm to find $\gcd(-270, 504)$, Find integers x and y such that

$$\gcd(-270, 504) = -270x + 504y. \quad (4.E.2)$$

Exercise 4.E. 5:

Suppose a and b are relatively prime integers and c is an integer such that $a|c$ and $b|c$. Prove that $ab|c$.

Exercise 4.E. 6:

Suppose a and b are relatively prime integers and c is an integer such that $a|bc$. Prove that $a|c$.

Exercise 4.E. 7:

1. Let a and b be non-zero integers with least common multiple l . Let m be any common multiple of a and b . Prove that $l|m$.
2. Prove that if a, b and c are natural numbers, $\gcd(a, c) = 1$ and $b | c$, then $\gcd(a, b) = 1$.
3. Suppose a and c are relatively prime integers and b is an integer such that $b|c$. Prove that $\gcd(a, b) = 1$.

Exercise 4.E. 8:

Prove that for any positive integer k , $7k + 5$ and $4k + 3$ are relatively prime.

Exercise 4.E. 9:

Let a, b, c and d be non-zero integers. Then determine whether the following statements are true or false. Justify your answers.

1. If $\gcd(a, b) = \gcd(a, c)$, then $b = c$.
2. If $\text{lcm}(a, b) = \text{lcm}(a, c)$, then $b = c$.
3. $\text{lcm}(\gcd(a, b), c) = \gcd(\text{lcm}(a, b), c)$.
4. If $\gcd(a, b) = \gcd(c, d)$ and $\text{lcm}(a, b) = \text{lcm}(c, d)$, then $a = b$ and $c = d$.
5. $\gcd(c, a + b) = \gcd(c, a) + \gcd(c, b)$.
6. $\gcd(c, ab) = \gcd(c, a) \gcd(c, b)$.
7. $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

Exercise 4.E. 10:

Let a, b and c be non-zero integers. Prove the following statements:

1. $\gcd(a, b) = \gcd(a, b - a) = \gcd(a, a + b) = \gcd(\pm a, \pm b)$.
2. $\gcd(a, b) = \gcd(a, b - ac)$.
3. $\gcd(ac, bc) = \gcd(a, b)|c|$

Exercise 4.E. 11:

Solve the following linear congruence:

1. $3x \cong 1 \pmod{6}$.
2. $16x \cong 11 \pmod{35}$.
3. $2x \cong 13 \pmod{13}$.

CHAPTER OVERVIEW

5: Diophantine Equations

[5.1: Linear Diophantine Equations](#)

[5.2 : Linear Congruences Revisted](#)

[5.3: Non-Linear Diophantine Equations](#)

[5.E: Exercises](#)

This page titled [5: Diophantine Equations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

5.1: Linear Diophantine Equations

Thinking out loud

Mary went to a park and saw vehicles with 2 wheels and 4 wheels. She counted the wheels. When she came home she told her mom that the vehicles she had seen had a total of 28 wheels. Her mom asked how many vehicles had 2 wheels and how many vehicles had 4 wheels. What was Mary's response?

Diophantine Equation

A Diophantine equation is a polynomial equation with 2 or more integer unknowns.

A Linear Diophantine equation (LDE) is an equation with 2 or more integer unknowns and the integer unknowns are each to at most degree of 1.

Linear Diophantine equation in two variables takes the form of $ax + by = c$, where $x, y \in \mathbb{Z}$ and a, b, c are integer constants. x and y are unknown variables.

A **Homogeneous** Linear Diophantine equation (HLDE) is $ax + by = 0, x, y \in \mathbb{Z}$. Note that $x = 0$ and $y = 0$ is a solution, called the trivial solution for this equation.

Example 5.1.1:

Example of a homogeneous linear diophantine equation:

$$5x - 3y = 0, x, y \in \mathbb{Z}.$$

In this case $x = 3, y = 5$ is a solution as is $x = 6, y = 10$.

Hence $x = 3k$ and $y = 5k, k \in \mathbb{Z}$ represent all the solutions.

Check: $5(3k) - 3(5k) = 15k - 15k = 0$.

**** NOTE**** In a homogeneous linear diophantine equation, the minute the equation is an addition, one of the variable is required to be negative.

In the case of $5x + 3y = 0, x, y \in \mathbb{Z}$, $x = -3k$ and $y = 5k, k \in \mathbb{Z}$ are solutions.

THEOREM: Homogeneous Linear Diophantine Equation

Let $ax + by = 0, x, y \in \mathbb{Z}$ be a homogeneous linear Diophantine equation.

If $\gcd(a, b) = d$, then the complete family of solutions to the above equation is

$$x = \frac{b}{d}k, \text{ and } y = -\frac{a}{d}k, k \in \mathbb{Z}.$$

Example 5.1.2: Solve the Homogeneous linear Diophantine equation

$$6x + 9y = 0, x, y \in \mathbb{Z}.$$

Solution:

Note that GCD of 6 and 9 is 3. Hence the solutions are

$$x = \frac{9k}{3} = 3k \text{ and } y = \frac{-6k}{3} = -2k \text{ with } k \in \mathbb{Z}.$$

Use the following steps to solve a non-homogeneous linear Diophantine equation.

Solve the linear Diophantine Equations: $ax + by = c, x, y \in \mathbb{Z}$.

Use the following steps to solve a non-homogeneous linear Diophantine equation.

Step 1: Determine the GCD of a and b . Let suppose $\gcd(a, b) = d$.

Step 2: Check that the GCD of a and b divides c . NOTE: If YES, continue on to step 3. If NO, STOP as there are no solutions.

Step 3: Find a particular solution to $ax + by = c$ by first finding x_0, y_0 such that $ax + by = d$. Suppose $x = \frac{c}{d}x_0$ and $y = \frac{c}{d}y_0$.

Step 4: Use a change of variables: Let $u = x - \frac{c}{d}x_0$ and $v = y - \frac{c}{d}y_0$, then we will see that $au + bv = 0$ (important to check your result).

Step 5: Solve $au + bv = 0$. That is: $u = -\frac{b}{a}m$ and $v = \frac{a}{b}m, m \in \mathbb{Z}$.

Step 6: Substitute for u and v . Thus the general solutions are $x - \frac{c}{d}x_0 = -\frac{b}{a}m$ and $y - \frac{c}{d}y_0 = \frac{a}{b}m, m \in \mathbb{Z}$.

Example 5.1.3: Die hard Jug Problem

Solve the linear Diophantine Equations: $5x + 3y = 4, x, y \in \mathbb{Z}$.

Solution:

Step 1: Determine the GCD of 5 and 3 (a and b). Since $5(2) + 3(-3) = 1$, $\gcd(5, 3) = 1$.

Step 2: Since $1 \mid 4$, we will continue on to Step 3.

Step 3: Find a particular solution to $5x + 3y = 4, x, y \in \mathbb{Z}$.

Since $5(5) + 3(-7) = 4, x = 5$ and $y = -7$ is a particular solution.

Step 4: Let $u = x - 5$ and $v = y + 7$. Note: The opposite integer of Step 4, so if it's positive in step 4 it will be negative in step 5 and vice versa.

Then $5u + 3v = 5(x - 5) + 3(y + 7)$

$= 5x - 25 + 3y + 21$

$= 5x + 3y - 4$

$= 4 - 4$ (because the equation is $5x + 3y = 4$)

$= 0$.

Step 5: Solve $5u + 3v = 0$

The general solutions are $u = -3m$ and $v = 5m, m \in \mathbb{Z}$.

Step 6: $x - 5 = -3m$ and $y + 7 = 5m, m \in \mathbb{Z}$.

Hence the general solutions are $x = -3m + 5, y = 5m - 7, m \in \mathbb{Z}$.

Example 5.1.4:

Solve the linear Diophantine Equations: $2x + 4y = 21, x, y \in \mathbb{Z}$.

Solution:

Since $\gcd(2, 4) = 2$ and 2 does not divide 21, $2x + 4y = 21$ has no solution.

Example 5.1.5:

Solve the linear Diophantine Equation $20x + 16y = 500, x, y \in \mathbb{Z}_+$.

Solution

Both $x, y \geq 0. 500 = 20(x) + 16(y)$.

Step 1: $\gcd(20, 16) = 4$. Since $4 \mid 500$, we expect a solution.

Step 2: A solution is $4125 = 20(1)(125) + 16(-1)(125)$.

$500 = 20(125) + 16(-125)$

Hence, $x = 125$ and $y = -125$ is a solution to $500 = 20x + 16y$.

Step 3: Let $u = x - 125$ and $v = y + 125$.

Consider that $20u + 16v = 20x - (20)(125) + 16y + (16)(125)$

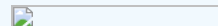
$= 20x + 16y - [(20)(125) - (16)(125)]$

$= 20x + 16y - 500$.

Thus, $20u + 16v = 0$.

Step 4: In general, the solution to $ax + by = 0$ is $x = bdk$ and $y = -adk, k \in \mathbb{Z} \setminus \{0\}$, $d = \gcd(a, b)$. Recall, $\gcd(20, 16) = 4$.

Thus $u = 16k/4 = 4k$ and $v = -20k/4 = -5k, k \in \mathbb{Z}$.



Step 5: Replace u and v .

Consider $4k = x - 125$ and $-5k = y + 125$.

Hence, $x = 4k + 125$ and $y = -5k - 125$.

Step 6: Both x and $y \geq 0$. $x \leq 25$ and $y \leq 31$ since total is 500.

$4k + 125 \geq 0$, $k \geq -125/4$, $\therefore k \geq -31.25$.

$4k + 125 \leq 25$, $4k \leq -100$, $\therefore k \leq -25$.

Thus, the possible solutions are:

Let $k = -25$ then $x = 25$, $y = 0$.

Let $k = -26$ then $x = 21$, $y = 5$.

Let $k = -27$ then $x = 17$, $y = 10$.

Let $k = -28$ then $x = 13$, $y = 15$.

Let $k = -29$ then $x = 9$, $y = 20$.

Let $k = -30$ then $x = 5$, $y = 25$.

Let $k = -31$ then $x = 1$, $y = 30$.

Thus the options of (x, y) that satisfy the given equation are:

$\{(25, 0), (21, 5), (17, 10), (13, 15), (9, 20), (5, 25), (1, 30)\}$

The following problem can be found in puzzle books.

Example 5.1.6:

When Mrs. Brown cashed her cheque, the absent minded teller gave her as many cents as she should have dollars, and as many dollars as she should have cents. Equally absent minded Mrs. Brown left with the cash without noticing the discrepancy. It was only after she spent 5 cents that she noticed now she had twice as much money as she should. What was the amount of her cheque?

Solution

Let x be the number of dollars Mrs Brown should have received and y be the number of cents she should have received.

Then $2(100x + y) = 100y + x - 5$

Note double original amount without spending a nickel.

$200x + 2y = 100y + x - 5$

$199x - 98y = -5$.

$5 = -199x + 98y$

Step 1: $\gcd(199, 98) = 1$. Since $1 \mid 5$, we can continue.

Step 2: A solution is $51 = -199(-33)(5) + (98)(-67)(5)$

$5 = -199(-165) + 98(-335)$.

Hence $x = -165$ and $y = -335$ is a solution to $5 = 98y - 199x$.

Step 3: Let $u = x + 165$ and $v = y + 335$.

Consider that $-199u + 98v = -199(x + 165) + 98(y + 335)$

$= -199x + 98y - [(199)(165) + (98)(335)]$

Thus $-199u + 98v = -199x + 98y - 5 = 0$.

Step 4: In general, the solution to $ax + by = 0$ is $x = bdk$ and $y = -adk$, $k \in \mathbb{Z} \setminus \{0\}$, $d = \gcd(a, b)$.

Recall, $\gcd(199, 98) = 1$.

Thus, $u = 98k$ and $v = 199k$, $k \in \mathbb{Z}$.

Step 5: Replace u and v .

$x + 165 = 98k$ and $y + 335 = 199k$, $k \in \mathbb{Z}$.

Hence $x = -165 + 98k$ and $y = -335 + 199k$.

Step 6: Both x & $y \geq 0$ and both $x, y < 100$

$-165 + 98k \geq 0$, so $k \geq 1.68$

$-335 + 199k \geq 0$, so $k \geq 1.68$

$-165 + 98k < 100$, $98k < 265$, $\therefore k < 2.70$

$-335 + 199k < 100$, $199k < 435$, $\therefore k < 2.18$

Since, $1.68 \leq k < 2.18$ and $k \in \mathbb{Z}$, $k = 2$.

Thus, $x = 98(2) - 165 = 31$ and $y = -335 + 199(2) = 63$.

Thus, the cheque was for \$31.63.

To verify, the teller gave Mrs. Brown \$63.31, she then spent 5 cents, leaving her with \$63.26 which is twice the check amount $(2)(\$31.63) = \$63.26$ ✓

PRACTICAL USES

- Cryptography
- Designing different combinations of a variety of elements.

This page titled [5.1: Linear Diophantine Equations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

5.2 : Linear Congruences Revisted

The following theorem we stated in Chapter 4:

Theorem 5.2.1

Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Then

$ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$. Moreover, if $x = x_0$ is a particular solution to this congruence, then the set of all solutions is $\{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{m}\} = \{x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}\}$, where $d = \gcd(a, m)$.

Let us learn how to use the theorem to solve linear congruence. Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Consider the linear congruence $ax \equiv b \pmod{m}$. Which is equivalent to $m \mid ax - b \implies ax - b = my$, for some $y \in \mathbb{Z}$. Thus solving linear congruence is equivalent to solving the linear Diophantine equation $ax + my = b$, for $x, y \in \mathbb{Z}$.

Example 5.2.1

If possible, solve $2x \equiv 2 \pmod{4}$.

Solution

Since $\gcd(2, 4) = 2$ and $2 \mid 2$, $2x \equiv 2 \pmod{4}$ has a solution. Moreover, the set of all solutions is given by $\{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{4}\}$. To find a particular solution we consider the corresponding Diophantine equation $2x + 4y = 2$. Since $2(-1) + 4(1) = 2$, one particular solution is given by $x_0 = -1$. Then all the solutions to the Diophantine equation $2x + 4y = 2$ are of the form $x = -1 + 2k, y = 1 - 4k, k \in \mathbb{Z}$.

Thus $x \pmod{4} = -1, 1$.

Since $(-1) \pmod{4} \equiv 3$ and $1 \pmod{4} \equiv 1$, the set of all solutions are all integers x such that $x \equiv 3 \pmod{4}$ or $x \equiv 1 \pmod{4}$.

This page titled [5.2 : Linear Congruences Revisted](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

- [4.5: Linear Congruences](#) by [Pamini Thangarajah](#) is licensed [CC BY-NC-SA 4.0](#).

5.3: Non-Linear Diophantine Equations

The following are some well-known examples of non-linear Diophantine equations:

Pythagorean Equation

Pythagorean Equation

Equations of the form $x^2 + y^2 = z^2$, where $x, y, z \in \mathbb{Z}$.

This equation arises out of geometric consideration, as Pythagoras was a geometer in ancient Greece.

Note that $3^2 + 4^2 = 5^2$ is a solution to the above equation. In this case, $4 + 5 = 3^2$.

This happens to be the first instance of a pattern.

Example 5.3.1

Let x be a positive odd integer. If x^2 is a sum of two consecutive positive integers y and z , then $x^2 + y^2 = z^2$.

Solution

Let $x, y, z \in \mathbb{Z}_+$ such that $x^2 = y + z$ and $z = y + 1$.

Consider, $x^2 + y^2 = (y + z) + y^2 = (y + y + 1) + y^2 = y^2 + 2y + 1 = (y + 1)^2 = z^2$.

Note that $5^2 = 12 + 13$ and $7^2 = 24 + 25$.

Example 5.3.2

Let x be a positive even integer. If $\frac{x^2}{2}$ is a sum two positive integers y and z differs by 2, then $x^2 + y^2 = z^2$.

Solution

Note that $\frac{6^2}{2} = 18 = 10 + 8$ and $10^2 = 8^2 + 6^2$.

Also, $\frac{8^2}{2} = 32 = 15 + 17$ and $17^2 = 15^2 + 8^2$.

Note that these patterns always generate solutions to the Pythagorean equations. Thus there are infinitely many solutions to the Pythagorean equations. Note that $\{x = 3, y = 4, z = 5\}$ and $\{x = 6, y = 8, z = 10\}$ are solutions to the Pythagorean equations.

However, these patterns do not generate all solutions.

Example 5.3.3

Not all the solutions to $x^2 + y^2 = z^2$, $x, y, z \in \mathbb{Z}_+$ can be obtained by doubling a solution.

Solution

Note that $\{x = 20, y = 21, z = 29\}$ can't be obtained from doubling a solution.

Pellian Equation

Pellian Equation

Equations of the form $x^2 - dy^2 = 1$, where $x, y \in \mathbb{Z}$, and d is a positive integer which is not a square of an integer.

Note that the solutions to $x^2 - 2y^2 = 1$, where $x, y \in \mathbb{Z}$, give rise to [square triangular numbers](#).

A square triangular numbers are of the form $\frac{t(t+1)}{2} = s^2$, for some $t, s \in \mathbb{Z}_+$.

Then $t^2 + t = 2s^2$. Now $4(t^2 + t) + 1 = 8s^2 + 1$.

Thus $(2t+1)^2 = 8s^2 + 1$. Let $x = 2t+1$ and $y = 2s$, then $x^2 - 2y^2 = 1$.

Example 5.3.4

Consider the Pellian equation $x^2 - 2y^2 = 1$.

1. Find a solution to the Pellian equation, by inspection.
2. Prove that if $x = a$ and $y = b$ is a solution, then $x = a^2 + 2b^2$ and $y = 2ab$ is also a solution.

Solution

1. $x = 3, y = 2$.

2. Assume that $a^2 - 2b^2 = 1$. Consider
 $(a^2 + 2b^2)^2 - 2(2ab)^2 = a^4 + 4a^2b^2 + 4b^4 - 8a^2b^2 = a^4 - 4a^2b^2 + 4b^4 = (a^2 - 2b^2)^2 = 1$. Hence the result.

This page titled [5.3: Non-Linear Diophantine Equations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

5.E: Exercises

Exercise 5.E.1

Decide whether the following homogeneous Diophantine equations are solvable if so find all the solutions.

1. $37x - 31y = 0$
2. $4x + 28y = 0$
3. $35x + 27y = 0$
4. $2058x - 1935y = 0$

Answer

TBC.

Exercise 5.E.2

Decide whether the following Diophantine equations are solvable if so find all the solutions.

1. $37x - 31y = 35$
2. $4x + 28y = 113$
3. $35x + 27y = 125$
4. $2058x - 1935y = 54$

Answer

TBC.

Exercise 5.E.3:

Goldfish cost \$8.00 Canadian and hamsters cost \$6.00 Canadian. How many of each animal can be bought for \$106.00 Canadian? Let x = number of Goldfish and y = number of hamsters. *Hint* there are 4 possible solutions.

Exercise 5.E.4:

Pencils can be purchased for 5 pesos, and erasers can be purchased for 4 pesos. How many of each can be purchased for 27 pesos? Let x = number of pencils and y = number of erasers. *Hint* there is only one possible answer.

Answer

Solution:

Let x be the number of pencils purchased and y be the number of erasers purchased. Thus $5x + 4y = 27$.

Step 1: The $\gcd(5, 4)$ was found to be 1.

Step 2: $1 \mid 27$, so we will continue.

Step 3: One solution is $x = \frac{27}{1}(1)$ and $y = \frac{27}{1}(-1)$.

Check: $5(27) + 4(-27) = 27 \checkmark$.

Step 4: Let $u = x - 27$ and $v = y + 27$.

Check: $0 = 5u + 5y$

$= 5(x - 27) + 4(y + 27)$

$= 5x + 4y - [5(27) - 4(27)]$

$= 5x + 4y - 27. \checkmark$

Step 5: The general solutions to $5u + 4y = 0$ are $u = -4m$ and $v = 5m$, $m \in \mathbb{Z}$.

Step 6: $x - 27 = -4m$ and $y + 27 = 5m$, $m \in \mathbb{Z}$.

Hence $x = -4m + 27$ and $y = 5m - 27$, $m \in \mathbb{Z}$.

Both $x, y \geq 0$. Thus $-4m + 27 \geq 0$ and $5m - 27 \geq 0$.
Solving for m in both equations we obtain $m \leq 6.75$ and $m \geq 5.2$.
Since $m \in \mathbb{Z}$, $m = 6$.
Hence $x = -4(6) + 27 = 3$ and $y = 5(6) - 27 = 3$.
Check: $5(3) + 4(3) = 15 + 12 = 27$. ✓
Thus with 27 pesos, we can purchase 3 pencils and 3 erasers.

Exercise 5.E. 5:

What combination of quarters and dimes will add to a sum of 88 cents?

Exercise 5.E. 6:

When Mary cashed her check, a teller accidentally gave her as many cents as she should have dollars and as many dollars as she should have cents. Mary left with the cash adding to the money \$27.60 in her bag, without noticing the discrepancy. It was after she spent one half of her money, she saw that now she had the exact amount of money on the check. What was the amount of check?

Exercise 5.E. 7:

Mary bought several sweaters at \$143 each and bought several tops at \$105 each. She spent \$1500. How many sweaters and how many tops did she buy?

This page titled [5.E: Exercises](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

CHAPTER OVERVIEW

6: Prime numbers

Topic hierarchy

- 6.1: Prime numbers
- 6.2: GCD, LCM and Prime factorization
- 6.3: Fermat Primes, Mersenne Primes and Primes of the other forms
- 6.E: Prime Numbers (Exercises)

This page titled [6: Prime numbers](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

6.1: Prime numbers

Definition:

Prime Numbers - integers greater than 1 with exactly 2 positive divisors: 1 and itself.

Let n be a positive integer greater than 1. Then n is called a prime number if n has exactly two positive divisors, 1 and n .

Composite Numbers - integers greater than 1 which are not prime.

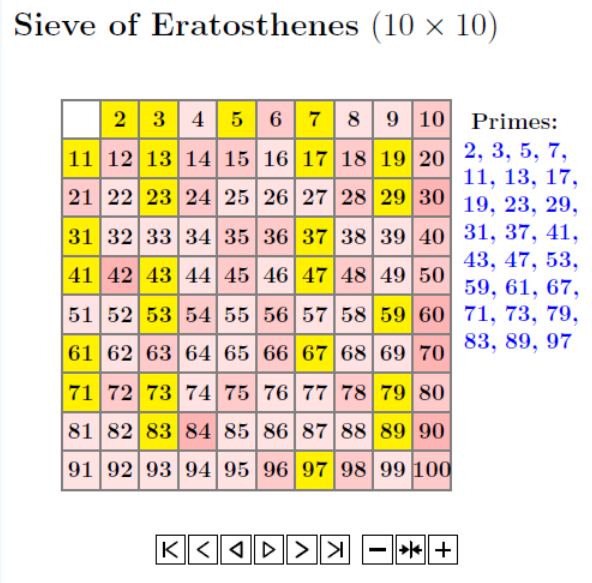
Note that: 1 is neither prime nor composite.

There are infinitely many primes, which was proved by Euclid in 100BC.

Example 6.1.1: Method of Sieve of Eratosthenes

Examples of prime numbers are 2 (this is the only even prime number), 3, 5, 7, 11, 13, 17, ...

Method of Sieve of Eratosthenes:



The following will provide us a way to decide given number is prime.

Theorem 6.1.1

Let n be a composite number with exactly 3 positive divisors. Then there exists a prime p such that $n = p^2$.

Proof

Let n be a positive integer with exactly 3 positive divisors. Then two of the positive divisors are 1 and n .

Let d be the third positive divisor. Then $1 < d < n$ and the only positive divisors of d are 1 and d .

Therefore d is prime.

Since $d \mid n$, $n = md$, $m \in \mathbb{Z}_+$.

Since $m \mid n$ and $1 < m < n$, $m = d$, $n = d^2$.

Thus, d is prime. $\square$

Theorem 6.1.2

Every composite number n has a prime divisor less than or equal to $\sqrt{n}$. If p is a prime number and $p \mid n$, then $1 < p \leq \sqrt{n}$.

Proof

Suppose p be the smallest prime divisor of n . Then there exists an integer m such that $n = pm$. Assume that $p > \sqrt{n}$. Then $m < \sqrt{n}$.

Let q be any prime divisor of m . Then q is also a prime divisor of n and $q < m < \sqrt{n} < p$. This is a contradiction.

Example 6.1.2:

Is 223 a prime number?

Solution:

The prime numbers $< \sqrt{223}$ are as follows: 2, 3, 5, 7, 11, and 13. Note that $17^2 > 223$.

Since 223 is not divisible by any of the prime numbers identified above, 223 is a prime number.

Exercise 6.1.3

Is 2011 a prime number?.

Answer

yes.

Theorem 6.1.3: Prime divisibility theorem

Let p be a prime number. If $p \mid ab$, $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Proof

Let p be a prime number and let $a, b \in \mathbb{Z}$. Assume that $p \mid ab$. If $p \mid a$, we are done. So we suppose that p does not divide a . Thus $\gcd(a, p) = 1$. Thus there exists $x, y \in \mathbb{Z}$ such that $1 = ax + py$. Hence $b = abx + pby$. Since $p \mid ab$, $ab = pm$, $m \in \mathbb{Z}$. Thus $b = pmx + pby = p(mx + by)$. Hence, $p \mid b$.

Theorem 6.1.5

There are infinitely many primes.

Proof

Proof by contradiction.

Suppose there are finitely many primes $p_1, p_2, \dots, p_n$, where n is a positive integer. Consider the integer Q such that

$$Q = p_1 p_2 \dots p_n + 1. \quad (6.1.1)$$

Notice that Q is not prime. Hence Q has at least a prime divisor, say q . If we prove that q is not one of the primes listed then we obtain a contradiction. Suppose now that $q = p_i$ for $1 \leq i \leq n$. Thus q divides $p_1 p_2 \dots p_n$ and as a result q divides $Q - p_1 p_2 \dots p_n$. Therefore q divides 1. But this is impossible since there is no prime that divides 1 and as a result q is not one of the primes listed.

The following theorem explains the gaps between prime numbers:

Theorem 6.1.5

Let n be an integer. Then there exists n consecutive composite integers.

Proof

Let n be an integer. Consider the sequence of integers

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n, (n+1)! + (n+1) \quad (6.1.2)$$

Notice that every integer in the above sequence is composite because k divides $(n+1)! + k$ if $2 \leq k \leq (n+1)$.

Example 6.1.4:

Does there exist a block of 1000000 consecutive integers without a prime number among them?

Solution

Use $1000001!$ and consider $1000001! + 2, \dots, 1000001! + 1000001$

Example 6.1.5:

Consider the formula $y = x^2 + x + 13$. Then

1. Find the values y for $x = 1, \dots, 12$. How many of these values are prime?
2. Can we conclude that this formula always generates a prime number?

Definition: Twin primes

Two prime numbers are called twin primes if they differ by 2.

Theorem 6.1.6 Fundamental Theorem of Arithmetic (FTA)

Let $n \in \mathbb{Z}_+$, then n can be expressed as a product of primes in a unique way. This means

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where $p_1 < p_2 < \dots < p_k$ are primes.

Neither the fundamental theorem nor the proof shows us how to find the prime factors. We can use tests for divisibility to find prime factors whenever possible.

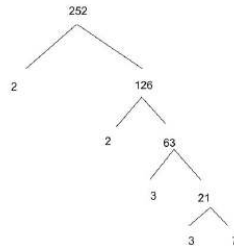
Example 6.1.6:

Find the prime factorization of

1. 252
2. 2018
3. 1000

Solution

1. Using divisibility tests, we can find that $252 = 2^2 3^2 7$



2. We can see that 2018 is divisible by 2, and $2018 = 2 \times 1009$. 1009 is prime (why?).

3. $1000 = 10^3 = ((2)(5))^3 = 2^3 5^3$

Example 6.1.7:

Find the prime factorization of 1000001.

Solution

Consider $1000001 = 1000000 + 1 = 10^6 + 1 = (10^2)^3 + 1^3 = (10^2 + 1^2)(10^4 - 10^2 + 1^2) = 101 \times 9901$. 101 and 9901 are prime (why?)

Note: Conjectures

Goldbach's Conjecture(1742)

Every even integer $n > 2$ is the sum of two primes.

Goldbach's Ternary Conjecture:

Every odd integer $n \geq 5$ is the sum of at most three primes.

This page titled [6.1: Prime numbers](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

6.2: GCD, LCM and Prime factorization

We have already discussed GCD and LCM in Chapter 4. This section will explore another method for finding GCD and LCM using prime factorization. In this method, we must first find the given integers' prime factorization.

Example 6.2.1:

Determine $\gcd(3^9, 3^8)$ and $\text{lcm}(3^9, 3^8)$

Solution

$\gcd(3^9, 3^8) = 3^8$ (the lowest powers of all prime factors that appear in both factorizations) and $\text{lcm}(3^9, 3^8) = 3^9$ (the largest powers of each prime factor that appear in factorizations).

Example 6.2.2:

Determine $\gcd(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2)$ and $\text{lcm}(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2)$.

Solution

$\gcd(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2) = 2^4 \times 3^8$ (the lowest powers of all prime factors that appear in both factorizations) and $\text{lcm}(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2) = 2^6 \times 3^9 \times 5^2$ (the largest powers of each prime factors that appear in factorizations).

Example 6.2.3:

Find $\gcd(3915, 825)$ and $\text{lcm}(3915, 825)$.

Solution

Since $3915 = 3^3 \times 5 \times 29$ and $825 = 3 \times 5^2 \times 11$, $\gcd(3915, 825) = 3 \times 5$ and $\text{lcm}(3915, 825) = 3^3 \times 5^2 \times 11 \times 29$.

Example 6.2.4:

Find $\gcd(2420, 230)$ and $\text{lcm}(2420, 230)$.

Solution

Since $2420 = 2^2 \times 5 \times 11^2$ and $230 = 2 \times 5 \times 23$, $\gcd(2420, 230) = 2 \times 5$ and $\text{lcm}(2420, 230) = 2^2 \times 5 \times 11^2 \times 23$.

Another use of Prime factorization is as follows:

Euler's totient function

Definition:

For $n \in \mathbb{N}$, the Euler's totient function $\phi(n)$ is defined to be the number of positive integers less than n that are relatively prime to n .

Euler's totient function has numerous applications in number theory, cryptography, and other branches of mathematics. It plays a vital role in RSA encryption, where it is used to compute the encryption and decryption keys.

✓ Example 6.2.5

Determine the value $\phi(n)$ for each integer $n \leq 30$. For $n \in \mathbb{N}$, $\phi(n)$ is defined to be the number of positive integers less than or equal to n that are relatively prime to n .

Number of $n \in \mathbb{N}$, Relatively Prime to n

n	$\phi(n)$	Set of $n \in \mathbb{N}$ that are relatively Prime to n .

1	1	{1}
2	1	{1}
3	2	{1,2}
4	2	{1,3}
5	4	{1,2,3,4}
6	2	{1,5}
7	6	{1,2,3,4,5,6}
8	4	{1,3,5,7}
9	6	{1,2,4,5,7,8}
10	4	{1,3,7,9}
11	10	{1,2,3, ... ,8,9,10}
12	4	{1,5,7,11}
13	12	{1,2,3, ... ,10,11,12}
14	6	{1,3,5,9,11,13}
15	8	{1,2,4,7,8,11,13,14}
16	8	{1,3,5,7,9,11,13,15}
17	16	{1,2,3, ... ,14,15,16}
18	6	{1,5,7,11,13,17}
19	18	{1,2,3, ... ,16,17,18}
20	8	{1,3,7,9,11,13,17,19}
21	12	{1,2,4,5,8,10,11,13,16,17,19,20}
22	10	{1,3,5,7,9,13,15,17,19,21}
23	22	{1,2,3, ... ,20,21,22}
24	8	{1,5,7,11,13,17,19,23}
25	20	{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24}
26	12	{1,3,5,7,9,11,15,17,19,21,23,25}
27	18	{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26}
28	12	{1,3,5,9,11,13,15,17,19,23,25,27}
29	28	{1,2,3, ... ,26,27,28}
30	8	{1,7,11,13,17,19,23,29}

The following results will help us find Euler's totient function $\phi(n)$ for $n \in \mathbb{N}$.

Wilson's Theorem

Theorem 6.2.7

Let p be a prime number. Then $(p-1)! + 1$ is divisible by p .

Proof:

Consider the product $P = 1 \cdot 2 \cdot 3 \cdots (p-1)$. Now, let's pair each number k from 1 to $p-1$ with its modular inverse k^{-1} modulo p .

We know that for every k such that $1 \leq k \leq p-1$, there exists a unique k^{-1} such that $kk^{-1} \equiv 1 \pmod{p}$. Moreover, these pairs will be distinct because if $kk^{-1} \equiv 1 \pmod{p}$ and $jj^{-1} \equiv 1 \pmod{p}$ for $k \neq j$, then $k = kj^{-1}$ and $j = jk^{-1}$, implying $k = j$, which contradicts the distinctness of the pairs.

Thus, we can pair each k with k^{-1} such that the product of these pairs is congruent to 1 (mod p). Therefore, $P \equiv (p-1)! \equiv -1 \pmod{p}$. Adding 1 to both sides gives $(p-1)! + 1 \equiv 0 \pmod{p}$, which means $(p-1)! + 1$ is divisible by p .

Fermat's Little Theorem

Theorem 6.2.8

For any prime number p and any positive integer a such that p does not divide a , we have $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem

Theorem 6.2.9

If a and n are relatively prime (i.e., $\gcd(a, n) = 1$), then

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad (6.2.1)$$

Theorem 6.2.10

1. If p is prime then $\phi(p) = p - 1$.
2. If p is prime and k is a positive integer then $\phi(p^k) = p^k - p^{k-1}$.
3. If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.
- 4.

$$\phi(n) = n \times \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad (6.2.2)$$

where the product is taken over distinct prime factors p of n .

✓ Example 6.2.6

Find $\phi(252)$.

Solution

Since $252 = 2^2 3^2 7$, $\phi(252) = (2^2 - 2)(3^2 - 3)(7 - 1) = 72$.

This page titled [6.2: GCD, LCM and Prime factorization](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

6.3: Fermat Primes, Mersenne Primes and Primes of the other forms

In this section, we consider special kinds of prime numbers.

Fermat Primes and Mersenne Primes

Definition:

1. The prime numbers of the form $2^k + 1$, where $k \in \mathbb{Z}_+$, are called Fermat primes.
 2. The prime numbers of the form $2^k - 1$, where $k \in \mathbb{Z}_+$, are called Mersenne primes.
- They are named after the French mathematicians Fermat and Mersenne.

Example 6.3.1:

1. $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$ are Fermat primes. Notice that $2^3 + 1 = 9$ is not prime.
2. $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ are Mersenne primes. Notice that $2^1 - 1 = 1$, $2^4 - 1 = 15$ are not prime.

Theorem 6.3.1

If $2^k + 1$ is a prime, $k \in \mathbb{Z}_+$, then k is a power of 2.

Proof

Left as an exercise.

Theorem 6.3.2

If $2^k - 1$ is a prime, $k \in \mathbb{Z}_+$, then k is also a prime.

Proof

Left as an exercise.

Primes of the form $4k - 1$

Example 6.3.2:

$(4)(1) - 1 = 3$, $(4)(2) - 1 = 7$, $(4)(3) - 1 = 11$, $4(5) - 1 = 19$, $(4)(6) - 1 = 23$ are primes of the form $4k - 1$. Notice that $(4)(4) - 1 = 15$ is not a prime.

How many are there?

Theorem 6.3.3

There are infinitely many primes of the form $4k - 1$, $k \in \mathbb{Z}_+$.

The proof of this theorem is beyond the scope of this class.

Primes of the form $6k - 1$

Example 6.3.3:

$(6)(1) - 1 = 5$, $(6)(2) - 1 = 11$, $(6)(3) - 1 = 17$, $6(5) - 1 = 29$ are primes of the form $6k - 1$. Notice that $(6)(6) - 1 = 35$ is not a prime.

This page titled 6.3: Fermat Primes, Mersenne Primes and Primes of the other forms is shared under a [not declared](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

6.E: Prime Numbers (Exercises)

Exercise 6.E.1:

Are 253 and 257 prime?

Exercise 6.E.2:

Using prime factorization find the GCD and LCM of 3920 and 820.

Exercise 6.E.3:

Using prime factorization find the GCD and LCM of 30030 and 165.

Exercise 6.E.4:

Find the prime factorization of 10101.

Answer

$$3 \times 7 \times 13 \times 37 .$$

Exercise 6.E.5:

1. Let a and b be positive integers such that $a^2 | b^2$. Show that $a | b$.
2. Let a and b be positive integers. Prove that $\gcd(a^2, b^2) = (\gcd(a, b))^2$.
3. Let a and b be positive integers such that $\gcd(a, b) = 1$. If ab is a perfect square then show that a and b are both perfect square.

Hint

Use the fundamental theorem of Arithmetic.

Exercise 6.E.6:

Describe in terms of the prime numbers all numbers with exactly four divisors.

Exercise 6.E.7:

1. Find a prime k such that $2^k - 1$ is not a prime.
2. Find an integer k , which is a power of 2 such that $2^k + 1$ is not a prime.

Answer

1. $k=29$, 2. $k = 32$

This page titled [6.E: Prime Numbers \(Exercises\)](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

CHAPTER OVERVIEW

7: Numeration Systems

Definition:

A *number* is a quantity.

A *numeral* is a symbol of representation.

A *system of numeration* is a set of numerals and a rule for combining them to make numbers.

There have been multiple *numeration* systems used throughout history and in various cultures.

[7.1: Historical numeral systems](#)

[7.2: Number Bases](#)

[7.3: Unusual Number systems](#)

[7.E: Exercises](#)

[Index](#)

[Glossary](#)

[Detailed Licensing](#)

This page titled [7: Numeration Systems](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

7.1: Historical numeral systems

Example 7.1.1:

Ciphered Number System

Names are given to 1, the powers of the base, as well as the multiples of the powers.

The first known Ciphered Number System was the Egyptian Hieratic Numerals. The Egyptians had no concept of a place value system, such as the decimal system. Therefore it required exact finite notation. It was based on multiples of 10, often being rounded off to the higher power.

Other ciphered number systems include Greek, Coptic, Hindu Brahmin, Hebrew, Syrian, and early Arabic.

Example 7.1.2:

Roman Number System

Numbers in the Roman number system are represented by combinations of letters from the Latin Alphabet.

Symbol	I	V	X	L	C	D	M
Base 10	1	5	10	50	100	500	1,000

So for example, 6 is VI, one more than 5 and 4 is IV, one less than 5. Similarly, 11 is XI, and 9 is IX. Thirty-three would be written as XXXIII.

What is this number represented in Roman Numerals MMMMDCCXXVII?

Example 7.1.3:

Addition in Roman Numerals:

Let's say we want to add 27 and 39 in Roman Numerals: XXVII + XXXIV

Simply line up XXVII and XXXIV, group, add and convert, yielding LXVI = 66.

Multiplication in Roman Numerals:

Suppose we wish to multiply 38 and 3. First, convert thirty-eight to roman numerals - XXXVIII. Then, they would have simply written it out 3 times and added as follows:

XXXVIII
XXXVIII
XXXVIII
=LXXXXXXIV
=LLXIV
=CXIV

Subtraction in Roman Numerals:

Suppose we wish to subtract 29 from 63. First, expand or do in parts

=LXIII - XXVIV
=XXXXXXXXIII - XXVIV
=XXXIV.

Example 7.1.4:

Hindu-Arabic Decimal System

This system came to western civilization from India in 1000 AD. In 1200 AD it was translated from Latin, 300 years later (15th and 16th century) we began using Arabic numerals commonly. This is the system that we use today, it uses only 10 digits, with 0 as a placeholder. It is a position based system.

10 Symbols - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

We need not create any other symbols as we have the positioning system which determines the quantity of the symbol.

For Example: 509 - can be expanded to $500 + 0 + 9$, or $5 \times 10^2 + 0 \times 10^1 + 9 \times 10^0$.

Base 10 columns explained using 24,962

10^4	10^3	10^2	10^1	10^0
2	4	9	6	2
2(10,000)	4(1000)	9(100)	6(10)	2(1)
20000	4000	900	60	2

The Babylonians began the idea for this positional system, however, they used base 60. They, however, had 2 oversights that were corrected with our current decimal system:

1. They did not create a 0 or such a symbol to represent a placeholder in the position that had no value such as in our 10's position in the above example, and
2. They did not create a decimal point, which made reading numbers very difficult. The decimal point in our current system is extremely important when reading number systems.

For example, we know that \$21.45, tells us the product cost 21 dollars and 45 cents, so there is a 2 in the 10's position, a 1 in the 1's position, and 4 in the tenths position, and 5 in the hundredths position. What if we were to simply write 2145, how much would the product cost?

Note

FOUR components that make up a good number system:

- positional notation
- multiplicative base
- abstract symbolization
- 0: very important to distinguish number position. For example 12 5 or 1205.

Interesting number system fact:

The Magical World of Harry Potter's currency system uses a non-decimal system:
1 Galleon = 17 sickles = 493 Knuts

This page titled [7.1: Historical numeral systems](#) is shared under a [not declared](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

7.2: Number Bases

Definition:

A number base is the number of digits or combination of digits that a system of counting uses to represent numbers. A base can be any whole number greater than 0. The most commonly used number system is the decimal system, commonly known as base 10. Its popularity as a system of counting is most likely due to the fact that we have 10 fingers.

Example 7.2.1:

The base of any number may be written beside the number. For example, 17_8 is read as 17 base 8, which is 15 in base 10.

Conversion from decimal to other bases

Example 7.2.2: Using positional notation

Binary is the most commonly used non-base 10 system. It is used for coding in computers. Binary is also known as Base 2. This means it is composed of only 0's and 1's. For example 9 in binary/base 2 is 1001. Let's see how this works.

Base 10	Base 2	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	1
9	1001	0	1	0	0	1
16	10000	1	0	0	0	0

Column 2 in the table above represents the binary representation of the decimal number shown in column 1. Columns 3-7 show the expansion of base 2. Note that leading zeros are not normally shown. The Binary system works similarly to the same way base 10 does, only smaller, therefore, requires more digits to make up the same number as in base 10. To illustrate, $16_{10} = 1(10^1) + 6(10^0) = 1(2^4) + 0(2^3) + 0(2^2) + 0(2^1) + 0(2^0)$.

Example 7.2.3: using positional notation

Look at Base 16, also known as the hexadecimal system, another common base when coding and using computer systems. In this case, we use the digits 0 – 9 and the letters representing two digits $A(10)$, $B(11)$, $C(12)$, $D(13)$, $E(14)$, $F(15)$.

Base 10	Base 16	16^2	16^1	16^0
100	064	0	6	4
42	02A	0	2	A (10)
124	07C	0	7	C (12)
269	10D	1	0	D (13)

✓ Example 7.2.4: Using division by base

Convert 1065 into base 12.

Solution

Notice that

$$1065 = (88)(12) + 9$$

$$88 = (7)(12) + 4$$

$$7 = (0)(12) + 7$$

We write the remainders from bottom to top, $1065 = 749_{12}$.

Conversion from binary to octal (base 8) and hexadecimal (base 16)

✓ Example 7.2.5

Convert 1010 into base 8 and 16.

Solution

12_8 and A_{16}

Arithmetic in other bases

Example 7.2.6:

Addition in Base 2:

Cheat Table to help with Addition:

$$0+0=0$$

$$0+1=1$$

$$1+0=1$$

$$1+1=10$$

Let's try it:

$$110$$

$$+ 101$$

$$1011$$

$$=====$$

$$\text{Check: } 110_2 = 6_{10}$$

$$101_2 = 5_{10}$$

$$1011_2 = 11_{10}$$

Therefore our addition is correct as $6 + 5 = 11$ in base 10.

Let's try another one:

$$10101_2$$

$$+ 11101_2$$

$$110010_2$$

$$=====$$

$$\text{Check: } 10101_2 = 21$$

$$11101_2 = 29$$

$$110010_2 = 50$$

Therefore our addition is correct as $21 + 29 = 50$ in base 10.

Example 7.2.7:**Subtraction in Base 2:**

Cheat table to help with subtraction:

$$1-1=0$$

$$0-0=0$$

$$1-0=1$$

$0-1=1$ * This requires a carry $10-1=1$. As you will remember, 10 in base 2 is 2.

Let's try it:

$$10111_2$$

$$- 10101_2$$

$$00010_2$$

$$=====$$

$$\text{Check: } 10111_2 = 23_{10}$$

$$10101_2 = 21_{10}$$

$$00010_2 = 2_{10}$$

Therefore, our subtraction is correct as $23 - 21 = 2$ in base 10.

Example 7.2.8:

Find $203_5 + 124_5$

$$\begin{array}{r} 2 \ 0 \ 3 \\ + \ 1 \ 2 \ 4 \\ \hline 3 \ 3 \ 2 \end{array} \quad (7.2.1)$$

Therefore,

$$203_5 + 124_5 = 332_5. \quad (7.2.2)$$

Practical Uses

- Coding
- Time (24 hours) or (60)
- Baking (Dozen)
- Imperial or Metric measurement systems

This page titled [7.2: Number Bases](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

7.3: Unusual Number systems

Dualtown Number System

The peoples of Dualtown use only numbers which are 1 and some of the multiples of 2 (even numbers). $E = \{1, 2, 4, 6, 8 \dots\}$. Notice that the set E is closed under multiplication.

Let's construct a 4×4 multiplication table E .

$\times$	1	2	4	6
1	1	2	4	6
2	2	4	8	12
4	4	8	16	24
6	6	12	24	36

The smallest ten prime numbers in Dualtown are 2, 6, 10, 14, 18, 22, 26, 30, 34, 38. Notice that $36 = (6)(6) = (2)(18)$. Thus 36 has two different Dualtown prime factorizations. Hence the Prime Divisibility Theorem does not hold for the Dualtown number system.

This page titled [7.3: Unusual Number systems](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

7.E: Exercises

Exercise 7.E. 1

Convert 101101101_2 to base 10.

Answer

TBD.

Exercise 7.E. 2

The tripletown number system use only numbers which are 1 more than some multiples of 3.

1. Construct a 5×5 tripletown number system of multiplication table with the numbers 1, 4, 7, 10 and 13.
2. Find the smallest ten prime numbers in the tripletown number system.
3. Find a number with two different tripletown number system prime factorizations.
4. Does the Prime divisibility Theorem hold for the tripletown number system? Explain.

Exercise 7.E. 3

The Quadritown number system use only numbers which are 1 more than some multiples of 4.

1. Construct a 5×5 Quadritown number system of multiplication table with the numbers 1, 5, 9, 13 and 17.
2. Find the smallest ten prime numbers in the Quadritown number system.
3. Find a number with two different Quadritown number system prime factorizations.
4. Does the Prime divisibility Theorem hold for the Quadritown number system? Explain.

Answer

1. Construct a 5×5 Quadritown multiplication table with the numbers 1, 5, 9, 13 and 17.

X	1	5	9	13	17
1	1	5	9	13	17
5	5	25	45	65	85
9	9	45	81	117	153
13	13	65	117	169	221
17	17	85	153	221	289

2. Find the smallest ten prime numbers in Quadritown.

Answer

5, 9, 13, 17, 21, 29, 33, 37, 41, 49

3. Find a number with two different Quadritown prime factorizations.

A solution: (found by trial and error)

Examples

Product	Prime Factorization #1	Prime Factorization #2

441	(21)(21)	(9)(49)
1089	(33)(33)	(9)(121)
2205	(5)(21)(21)	(5)(9)(49)
3249	(57)(57)	(9)(361)

Does the Prime divisibility Theorem hold for the Quadritown number system? Explain.

Prime divisibility is defined as follows:

Let p be a prime and let a and b be integers. If $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Thus, prime divisibility does not hold for the Quadritown number system since $21 \mid 441$ and $21 \mid (9)(49)$, but $21 \nmid 9$ nor does $21 \nmid 49$. Note, this argument could be modified for each of the examples identified in part c.

This page titled [7.E: Exercises](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

CHAPTER OVERVIEW

8: Rational numbers, Irrational Numbers, and Continued fractions

Topic hierarchy

- [8.1: Rational numbers](#)
- [8.2: Irrational Numbers](#)
- [8.3: Continued fractions](#)
- [8.E: Exercises](#)

This page titled [8: Rational numbers, Irrational Numbers, and Continued fractions](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

8.1: Rational numbers

This page is a draft and is under active development.

Definition: Rational

A real number x is called a rational number if $x = \frac{m}{n}$ for some $m, n \in \mathbb{Z}, n \neq 0$.

Example 8.1.1:

Write $2.\overline{13}$ as a fraction.

Solution

Let $x = 2.\overline{13}$. Then $100x = 213.\overline{13}$ Therefore $99x = 211$. which implies $x = \frac{211}{99}$.

8.1: Rational numbers is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

8.2: Irrational Numbers

This page is a draft and is under active development.

Definition: Irrational

A number that is not a rational number is called an irrational number.

Theorem 8.2.1

$\sqrt{3}$ is irrational.

Proof

Proof by contradiction.

Example 8.2.1:

Prove that $\sqrt{3 + \sqrt{6}}$ is irrational.

Solution

Proof by contradiction.

8.2: Irrational Numbers is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by LibreTexts.

8.3: Continued fractions

This page is a draft and is under active development.

Definition: Continued fractions

A simple continued fraction is of the form, denoted by $[a_0, a_1, \dots]$,

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}, \quad (8.3.1)$$

where $a_0, a_1, a_2, \dots \in \mathbb{Z}$. Continued fraction has been studied extensively, but we will only explore some of them in this class.

Example 8.3.1:

A simple finite continued fraction

$$\frac{1}{2} = [1, 1] = 0 + \frac{1}{1 + \frac{1}{1}} \quad (8.3.2)$$

A simple infinite continued fraction: Golden Ratio

$$\phi = \frac{1 + \sqrt{5}}{2} = [1, 1, \dots] = 1 + \frac{1}{1 + \frac{1}{1 + \dots}}, \quad (8.3.3)$$

which can be found using $x = 1 + \frac{1}{1 + x}$.

Note

Rational numbers have a simple finite continued fraction, and irrational numbers have an infinite continued fraction.

Writing Continued Fractions

Let's explore the process of writing continued fractions using two examples:

✓ Example 8.3.2

Starting with the fraction

$$\frac{47}{17} = 2 + \frac{13}{17} \quad (8.3.4)$$

This expression indicates that

$$\frac{47}{17} \text{ is equivalent to the whole number } 2 \text{ plus a fraction } \frac{13}{17}. \quad (8.3.5)$$

Next, we can express it as

$$\frac{47}{17} = 2 + \frac{1}{\frac{17}{13}} \quad (8.3.6)$$

Here, we've written

$$\frac{47}{17} \text{ as the whole number } 2 \text{ plus the reciprocal of the fraction } \frac{17}{13}. \quad (8.3.7)$$

Continuing, we have

$$\frac{47}{17} = 2 + \frac{1}{1 + \frac{4}{13}} \quad (8.3.8)$$

Now, the continued fraction form includes the whole number 2 and a fraction where the denominator is the sum of 1 and $\frac{4}{13}$.

$$\frac{47}{17} = 2 + \frac{1}{1 + \frac{1}{\frac{13}{4}}} \quad (8.3.9)$$

Here, we express

$$\frac{47}{17} \text{ as } 2 \text{ plus a fraction where the denominator itself is a continued fraction.} \quad (8.3.10)$$

We can further express it as

$$\frac{47}{17} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}} \quad (9)$$

The final form illustrates the continued fraction expansion of $\frac{47}{17}$ with multiple levels of nesting.

✓ Example 8.3.3

Now, let's consider the square root of 2:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) \quad (10)$$

Here, we expressed that the square root of 2 equals $1 + (\sqrt{2} - 1)$. Next, we write:

$$\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}} \quad (11)$$

In this form, the square root of 2 is written as 1 plus the reciprocal of the quantity $1 + \sqrt{2}$. Now replace $\sqrt{2}$ with what we proved it to equal in equation (11):

$$\sqrt{2} = 1 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}} \quad (12)$$

Simplifying gives us:

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}} \quad (13)$$

Continue with replacing $\sqrt{2}$ with what we proved it to equal in equation (11):

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{1 + 1 + \frac{1}{1 + \sqrt{2}}}} \quad (14)$$

This leads to:

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \sqrt{2}}}} \quad (15)$$

Finally, we have:

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\dots}}} \quad (16)$$

This final form illustrates the continued fraction expansion of the square root of 2 with repeated nesting. The ellipsis (...) represents an infinite continuation of the pattern.

✓ Example 8.3.4

Using the Euclidean algorithm to find a simple finite continued fraction

Let's explore the following example:

Consider $\frac{2520}{154}$.

By Euclidean algorithm we have,

$$2520 = (16)(154) + 56$$

$$154 = (2)(56) + 42$$

$$56 = (1)(42) + 14$$

$$42 = (3)(14) + 0.$$

The quotients give us the simple finite continued fraction $[16, 2, 1, 3]$ That is

$$\frac{2520}{154} = 16 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3}}} \quad (8.3.11)$$

Continued fractions are more structured and easier to manipulate for certain mathematical operations, especially in number theory problems. While familiar, decimals can be challenging for analysis and computation.

8.3: Continued fractions is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by LibreTexts.

8.E: Exercises

This page is a draft and is under active development.

? Exercise 8.E. 1

Prove that $\sqrt{3}$ is irrational.

Answer

Use Fundamental theorem of Arithmetic.

? Exercise 8.E. 2

Find the continued fractions for $\sqrt{5}$ and $\frac{17}{12}$.

8.E: Exercises is shared under a [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/) license and was authored, remixed, and/or curated by LibreTexts.

CHAPTER OVERVIEW

Mock exams

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them, will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

Topic hierarchy

[Sample Final](#)

[Sample term test](#)

[Mock exams](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

Sample Final

This page is a draft and is under active development.

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them, will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

Exercise 1

For $a, b \in \mathbb{Z}$, define an operation $\otimes$, by $a \otimes b = (a + b)(a + b)$. Determine whether $\otimes$ on $\mathbb{Z}$.

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Answer

1. is closed,

Proof:

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Then consider, $a \otimes b = (a + b)(a + b)$.

$((a + b)(a + b) = a^2 + 2ab + b^2)$, since $\cdot$ is commutative on $\mathbb{Z}$.

$(a^2, 2ab, b^2, a^2 + 2ab + b^2) \in \mathbb{Z}$, since $\cdot, +$ are closed on $\mathbb{Z}$.

Hence, $a^2 + 2ab + b^2 \in \mathbb{Z}$.

Hence, $a \otimes b \in \mathbb{Z}$.

Thus, the binary operation is closed on $\mathbb{Z}$. ☐

2. is commutative,

Proof:

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

Then consider, $a \otimes b = (a + b)(a + b)$

$= a^2 + 2ab + b^2$ (since $\cdot$ is commutative on $\mathbb{Z}$.)

$= b^2 + 2ba + a^2$ (since $\cdot, +$ are commutative on $\mathbb{Z}$.)

$= (b + a)(b + a)$.

Thus $ab = ba$.

Thus, the binary operation is commutative on $\mathbb{Z}$. ☐

1. is associative,

Counterexample:

Choose $a=2, b=3, c=4$.

Then consider, $(a \otimes b) \otimes c =$

$= [(2 + 3)(2 + 3)] \otimes 4$

$$= 25 \otimes 4$$

$$= (25 + 4)(25 + 4)$$

$$= 841.$$

$$\text{Now consider } a(bc) = 2(3 + 4)(3 + 4)$$

$$= 249$$

$$= (2 + 49)(2 + 49)$$

$$= 2601.$$

Since $841 \neq 2601$, the binary operation is not associative on $\mathbb{Z}$. ☐

has an identity.

Proof by Contradiction:

Let e be the identity on $(\mathbb{Z}, \cdot)$.

Then consider, $ae = ea = a, a \in \mathbb{Z}$.

Now, $a = ea$.

$$= (e + a)(e + a).$$

$$= e(e + a) + a(e + a), \text{ since } \cdot \text{ is associative on } \mathbb{Z}.$$

$$= e^2 + ea + ae + a^2.$$

$$a = e^2 + 2ae + a^2, a \in \mathbb{Z}, \text{ since } \cdot \text{ is commutative on } \mathbb{Z}.$$

Then choose $a=0$.

$$\text{Thus, } e^2 = 0 \text{ and } e = 0.$$

$$\text{Hence } a^2 = a, \text{ for all } a \in \mathbb{Z}$$

This is a contradiction.

Thus, $(\mathbb{Z}, \cdot)$ has no identity.



Exercise 2

For $a, b \in \mathbb{Z}$, the ominus of b from a is defined by $a \ominus b = ab + a - b$. The oplus of a by b is defined by $a \oplus b = a + b + ab$. The oslash of a by b is defined by $a \oslash b = (a + b)(a - b)$. Answer the following:

- (a) Determine whether $\oslash$ is distributive over $\oplus$.
 (b) Determine whether $\oslash$ is distributive over $\ominus$.

Answer

(a)

Counter Example:

Choose $a = 2$, $b = 3$, and $c = 4$.

$$\begin{aligned} \text{Consider } 2 \oslash (3 \oplus 4) &= 2 \oslash (3 + 4 + (3)(4)) \\ &= 2 \oslash 19 \\ &= (2 + 19)(2 - 19) \\ &= 357. \end{aligned}$$

$$\begin{aligned} \text{Now consider } (23) \oplus (24) &= [(2+3)(2-3)] \oplus [(2+4)(2-4)] \\ &= (-5) \oplus (-12) \\ &= (-5) + (-12) + [(-5)(-12)] \\ &= 41. \end{aligned}$$

Since $357 \neq 41$, $\oslash$ is not distributive over $\oplus$.

(b)

Counter Example:

Choose $a = 2$, $b = 3$, $c = 4$.

$$\begin{aligned} \text{Consider } 2 \oslash (3 \ominus 4) &= 2 \oslash [(34) + 3 - 4] \\ &= 2 \oslash 11 \\ &= (2 + 11)(2 - 11) \\ &= 117. \end{aligned}$$

$$\begin{aligned} \text{Next consider } (2 \oslash 3) \ominus (2 \oslash 4) &= [(2+3)(2-3)] \ominus [(2+4)(2-4)] \\ &= (-5) \ominus (-12) \\ &= (-5)(-12) + (-5)(-12) \\ &= 67. \end{aligned}$$

Since $117 \neq 67$, $\oslash$ is not distributive over $\ominus$.

Exercise 3

Let $a, b \in \mathbb{Z}$, define the relation aRb iff $4 \mid (3a + b)$.

Determine whether this relation

- (a) is reflexive,
 (b) is symmetric,
 (c) is antisymmetric,
 (d) is transitive.
 (e) If R is an equivalence relation, describe the equivalence classes of $\mathbb{Z}$.

Answer

TBA

Exercise 4

- (a) Prove that $n^2 + 1$ not divisible by 3 for any integer n .
(b) Let $a, b \in \mathbb{Z}^+$. If $a|b$, is it necessarily true that $a^3|b^5$?

Answer

TBA

Exercise 5

Find the remainder

- (a) when $201 \times 203 \times 207 \times 209$ is divided by 13.
(b) when 7^{3453} is divided by 8.

Answer

TBA

Exercise 6

- (a) In a 101-digit multiple of 7, the first 50 digits are all 8s and the last 50 digits are all 1s. What is the middle digit?
(b) Let a and b be positive integers such that $7|(a + 2b + 5)$ and $7|(b - 9)$. Prove that $7|(a + b)$.

Answer

Add texts here. Do not delete this text first.

Exercise 7

- (a) An elementary art teacher has 4 art classes with 21, 32, 35 and 29 students, respectively. The teacher wants to order some equipment that can be used by equal-sized groups in each class. What is the largest number of students in a group in each class so that each group has the same number of students?
(b) Given that April 11, 2018, is a Wednesday, what day of the week is Jan 1, 2025?

Answer

Add texts here. Do not delete this text first.

Exercise 8

- (a) Using Euclidean algorithm, find $\gcd(2017, 7021)$ and $\text{lcm}(2017, 7021)$.
(b) Using prime factorization, find $\gcd(2017, 7021)$ and $\text{lcm}(2017, 7021)$.

Answer

TBA

Exercise 9

- (a) Solve the Diophantine equation $2058x - 1935y = 54$
(b) When Mrs. Brown cashed her cheque, the absent-minded teller gave her as many cents as she should have dollars, and as many dollars as she should have cents. Equally absent-minded Mrs. Brown left with the cash without noticing the discrepancy.

It was only after she spent 25 cents that she noticed now she had twice as much money as she should. What was the amount of her cheque?

Answer

Add texts here. Do not delete this text first.

Exercise 10

The Quadripark town uses only numbers which are 1 more than some of the multiples of 4.

1. Construct a 5X5 Quadripark multiplication table with the numbers 1, 5, 9, 13 and 17.
2. Find the smallest ten prime numbers in Quadripark.
3. Find a number with two different Quadripark prime factorizations.
4. Does the Prime divisibility Theorem hold for the Quadripark number system? Explain

Answer

2.

5, 9, 13, 17, 21, 29, 33, 37, 41, 49

This page titled [Sample Final](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

Sample term test

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them, will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

? Exercise 1

For $a, b \in \mathbb{Z}$, define an operation $\otimes$, by $a \otimes b = (a + b)(a + b)$. Determine whether $\otimes$ on $\mathbb{Z}$.

1. is closed,
2. is commutative,
3. is associative, and
4. has an identity.

Answer

1. is closed,

Proof:

Let $a, b \in \mathbb{Z}$.

$$\text{Then } a \otimes b = (a + b)(a + b) = a^2 + 2ab + b^2.$$

Since $\cdot$ is commutative on $\mathbb{Z}$, $a^2, 2ab, b^2 \in \mathbb{Z}$. Thus $a^2 + 2ab + b^2 \in \mathbb{Z}$.

Hence, $a \otimes b \in \mathbb{Z}$.

Thus, the binary operation is closed on $\mathbb{Z}$. ☐

2. is commutative,

Proof:

Let $a, b \in \mathbb{Z}$.

Then

$$a \otimes b = (a + b)(a + b) = a^2 + 2ab + b^2 \text{ (since } \cdot \text{ is commutative on } \mathbb{Z}) = b^2 + 2ba + a^2 \text{ (since } \cdot, + \text{ are commutative on } \mathbb{Z}) = (b + a)(b + a).$$

$$\text{Thus } a \otimes b = b \otimes a.$$

Thus, the binary operation is commutative on $\mathbb{Z}$.

3. is not associative,

Counterexample:

Choose $a = 2, b = 3, c = 4$.

$$\text{Then consider, } (a \otimes b) \otimes c = [(2 + 3)(2 + 3)] \otimes 4 = 25 \otimes 4 = (25 + 4)(25 + 4) = 841.$$

$$\text{Now consider } a \otimes (b \otimes c) = 2 \otimes [(3 + 4)(3 + 4)] = 2 \otimes 49 = (2 + 49)(2 + 49) = 2601.$$

Since $841 \neq 2601$, the binary operation is not associative on $\mathbb{Z}$. ☐

4. Does not have an identity.

Proof by Contradiction:

Let e be the identity on $(\mathbb{Z}, \otimes)$.

$$\text{Then } a \otimes e = e \otimes a = a, a \in \mathbb{Z}.$$

$$\text{Now, } a = e \otimes a.$$

$$= (e + a)(e + a).$$

$$= e(e + a) + a(e + a), \text{ since } \cdot \text{ is associative on } \mathbb{Z}$$

$$= e^2 + ea + ae + a^2$$

$$a = e^2 + 2ae + a^2, a \in \mathbb{Z}, \text{ since } \cdot \text{ is commutative on } \mathbb{Z}.$$

Then choose $a = 0$.

$$\text{Thus, } e^2 = 0 \implies e = 0.$$

$$\text{Hence } a^2 = a, \text{ for all } a \in \mathbb{Z}$$

This is a contradiction.

Now choose, $e \neq 0$ then it won't work for $a = 0$.

Thus, $(\mathbb{Z}, \cdot)$ has no identity. ☐

? Exercise 2

For $a, b \in \mathbb{Z}$, the minus of b from a is defined by $a \ominus b = ab + a - b$. The plus of a by b is defined by $a \oplus b = a + b + ab$. The slash of a by b is defined by $a \oslash b = (a + b)(a - b)$. Answer the following:

(a) Determine whether $\oslash$ is distributive over $\oplus$.

(b) Determine whether $\oslash$ is distributive over $\ominus$.

Answer

(a)

Counter Example:

Choose $a = 2, b = 3$, and $c = 4$.

Consider $2 \oslash (3 \oplus 4) = 2 \oslash (3 + 4 + (3)(4)) = 2 \oslash 19 = (2 + 19)(2 - 19) = 357$.

Now consider $(2 \oslash 3) \oplus (2 \oslash 4) = [(2 + 3)(2 - 3)] \oplus [(2 + 4)(2 - 4)] = (-5) \oplus (-12) = (-5) + (-12) + [(-5)(-12)] = 41$.

Since $357 \neq 41$, $\oslash$ is not distributive over $\oplus$.

(b)

Counter Example:

Choose $a = 2, b = 3$, and $c = 4$.

Consider $2 \oslash (3 \ominus 4) = 2 \oslash [(3)(4) + 3 - 4] = 2 \oslash 11 = (2 + 11)(2 - 11) = 117$.

Next consider, $(2 \oslash 3) \ominus (2 \oslash 4) = [(2 + 3)(2 - 3)] \ominus [(2 + 4)(2 - 4)] = (-5) \ominus (-12) = (-5)(-12) + (-5) - (-12) = 67$.

Since $117 \neq 67$, $\oslash$ is not distributive over $\ominus$.

? Exercise 3

Let $m \in \mathbb{Z}_+$. Let $a, b \in \mathbb{Z}$, define the relation $a R b$ iff $m \mid (a - b)$.

1. Determine whether the relation is

a) reflexive,

b) symmetric

c) antisymmetric

d) transitive.

2. If R is an equivalence relation, describe the equivalence classes of $\mathbb{Z}$.

Answer

(a) is reflexive,

Proof:

Let $m \in \mathbb{Z}_+$.

Let $a \in \mathbb{Z}$.

Since $a - a = 0 = m(0), m \mid (a - a)$.

Hence, $a R a$. Thus R is reflexive. $\square$

(b) is symmetric,

Proof:

Let $a, b \in \mathbb{Z}$, such that $a R b$. Thus $m \mid (a - b)$.

We shall show that $b R a$.

Since $m \mid (a - b), a - b = m(k), k \in \mathbb{Z}$.

Now, $(b - a) = m(-k), -k \in \mathbb{Z}$.

Thus, $m \mid (b - a) \implies b R a$. , therefore, R is symmetric on $\mathbb{Z}$. $\square$

(c) is antisymmetric,

Counter Example:

We shall show that $m \mid (a - b)$ and $m \mid (b - a)$ but $a \neq b$.

Choose $m = 2$, $a = 5$ and $b = 7$.

Then $2 \mid (5 - 7)$ since $-2 = 2(-1)$ and $2 \mid (7 - 5)$ since $2 = 2(1)$.

But, $5 \neq 7$, thus $m \mid (a - b)$ is not antisymmetric on $\mathbb{Z}$. $\square$

(d) is transitive.

Proof:

Let $a, b, c, m \in \mathbb{Z}^+$ s.t. $m \mid (a - b)$ and $m \mid (b - c)$.

We shall show that $m \mid (a - c)$.

Since $m \mid (a - b)$, $(a - b) = m(k_1)$, $k_1 \in \mathbb{Z}$.

Since $m \mid (b - c)$, $(b - c) = m(k_2)$, $k_2 \in \mathbb{Z}$.

Now consider $(a - b) + (b - c) = mk_1 + mk_2$.

Thus $(a - c) = m(k_1 + k_2)$, $k_1 + k_2 \in \mathbb{Z}$.

Hence $m \mid (a - c)$, thus $a R c$, therefore R is transitive on $\mathbb{Z}$. $\square$

? Exercise 4

Find the remainder

(a) when $201 \times 203 \times 207 \times 209$ is divided by 13.

(b) when 7^{3453} is divided by 8.

Answer

(a) $201 \equiv 6 \pmod{13}$, $203 \equiv 8 \pmod{13}$, $207 \equiv 12 \pmod{13}$, $209 \equiv 1 \pmod{13}$

$6 \cdot 8 \cdot 12 \cdot 1 = 48 \cdot 12 \cdot 1 \equiv 9 \cdot 12 \cdot 1 \pmod{13}$

$9 \cdot 12 = 108 \equiv 4 \pmod{13}$

(b)

$7 \equiv 7 \pmod{8}$ Since 1453 is odd, $7^{1453} \equiv 7 \pmod{8}$

$7^2 \equiv 1 \pmod{8}$

$7^3 \equiv 7 \pmod{8}$

$7^4 \equiv 1 \pmod{8}$

? Exercise 5

(a) Let a and b be positive integers such that $7 \mid (a+2b+5)$ and $7 \mid (b-9)$. Prove that $7 \mid (a+b)$.

(b) Let $a, b \in \mathbb{Z}_+$. If $a \mid b$, is it necessarily true that $a^3 \mid b^4$?

Answer

a) Let $a, b \in \mathbb{Z}_+$ such that $7 \mid (a+2b+5)$, and $7 \mid (b-9)$,

Then $7 \mid ((a+2b+5)+(b-9))$, $7 \mid (a+3b-4)$

If $7 \mid (a+b)$ then $7 \mid (a+3b-4)-(a+b)$, $7 \mid (2b-4)$

$7 \mid (a+b)$, such that $a=7x+5$, $b=7x+9$

$$\begin{array}{lll}
 7|(a+2b+5) & 7|(b-9) & 7|(a+b) \\
 \Rightarrow 7|(7x+5 + 2(7x+9) +5) & \Rightarrow 7|(7x+9-9) & \Rightarrow 7|(7x+5+7x+9) \\
 \Rightarrow 7|(21x + 28) & \Rightarrow 7|(7x) & \Rightarrow 7|(14x+14)
 \end{array}$$

(Do not use equal sign for relations!!!!!!)

b) Proof:

Let $a, b \in \mathbb{Z}^+$ s.t. $a \mid b$.

Since $a \mid b$, $\exists k \in \mathbb{Z}^+$ such that $b=a(k)$.

Now consider $b^4 = (a(k))^4$,

$$= a^4(k^4).$$

Since $ak^4 \in \mathbb{Z}^+$, $a^4 \mid b^4$. $\square$

This page titled [Sample term test](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by [Pamini Thangarajah](#).

- [Sample Final](#) by [Pamini Thangarajah](#) is licensed [CC BY-NC-SA 4.0](#).

CHAPTER OVERVIEW

Notations

Topic hierarchy

[Notations](#)

[Notations](#) is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.

Notations

This page is a draft and is under active development.

[Notations](#) is shared under a [CC BY-NC-SA 4.0](#) license and was authored, remixed, and/or curated by LibreTexts.

Index

B

Bezout's algorithm

[4.2: Euclidean algorithm and Bezout's algorithm](#)

Binary Relations

[2.1: Binary Relations](#)

C

Composite Numbers

[6.1: Prime numbers](#)

D

Diophantine Equations

[5: Diophantine Equations](#)

[5.1: Linear Diophantine Equations](#)

E

Euclidean Algorithm

[4.2: Euclidean algorithm and Bezout's algorithm](#)

F

Fermat Primes

[6.3: Fermat Primes, Mersenne Primes and Primes of the other forms](#)

Fundamental Theorem of Arithmetic

[6.1: Prime numbers](#)

G

Gilblich's Conjecture

[6.1: Prime numbers](#)

Goldbach's Ternary

[6.1: Prime numbers](#)

greatest common divisor

[4.1: Greatest Common Divisor](#)

L

least common multiple

[4.3: Least Common Multiple](#)

Linear Diophantine equation

[5.1: Linear Diophantine Equations](#)

M

Mersenne primes

[6.3: Fermat Primes, Mersenne Primes and Primes of the other forms](#)

modular arithmetic

[3.2: Modulo Arithmetic](#)

modulo operation

[3.1: Modulo Operation](#)

modulus

[3.2: Modulo Arithmetic](#)

N

Non Linear Diophantine Equations

[5.3: Non-Linear Diophantine Equations](#)

P

prime factorization tree

[6.1: Prime numbers](#)

prime numbers

[6: Prime numbers](#)

[6.1: Prime numbers](#)

R

Reflexive Property

[3.2: Modulo Arithmetic](#)

remainder

[3.2: Modulo Arithmetic](#)

S

Symmetric Property

[3.2: Modulo Arithmetic](#)

Glossary

Sample Word 1 | Sample Definition 1

File failed to load: <https://cdnjs.cloudflare.com/ajax/libs/mathjax/2.7.5/jax/output/HTML-CSS/jax.js>

Detailed Licensing

Overview

Title: [Higher Arithmetic](#)

Webpages: 76

Applicable Restrictions: Noncommercial, No Derivatives

All licenses found:

- [CC BY-NC-SA 4.0](#): 69.7% (53 pages)
- [Undeclared](#): 28.9% (22 pages)
- [CC BY-NC-ND 4.0](#): 1.3% (1 page)

By Page

- [Higher Arithmetic](#) - [CC BY-NC-SA 4.0](#)
 - [Front Matter](#) - [Undeclared](#)
 - [00: Front Matter](#) - [Undeclared](#)
 - [TitlePage](#) - [Undeclared](#)
 - [InfoPage](#) - [Undeclared](#)
 - [Table of Contents](#) - [Undeclared](#)
 - [Licensing](#) - [Undeclared](#)
 - [TitlePage](#) - [Undeclared](#)
 - [InfoPage](#) - [Undeclared](#)
 - [Table of Contents](#) - [Undeclared](#)
 - [Licensing](#) - [CC BY-NC-SA 4.0](#)
 - [Preface](#) - [CC BY-NC-SA 4.0](#)
 - [0: Preliminaries](#) - [CC BY-NC-SA 4.0](#)
 - [0.1: Basics](#) - [CC BY-NC-SA 4.0](#)
 - [0.2: Introduction to Proofs/Contradiction](#) - [CC BY-NC-SA 4.0](#)
 - [0.3: Proof Do's and Dont's](#) - [CC BY-NC-ND 4.0](#)
 - [0.4: Egyptian Multiplication and Division \(optional\)](#) - [Undeclared](#)
 - [0.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [1: Binary operations](#) - [CC BY-NC-SA 4.0](#)
 - [1.1: Binary operations](#) - [CC BY-NC-SA 4.0](#)
 - [1.2: Exponents and Cancellation](#) - [CC BY-NC-SA 4.0](#)
 - [1.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [2: Binary relations](#) - [CC BY-NC-SA 4.0](#)
 - [2.1: Binary Relations](#) - [CC BY-NC-SA 4.0](#)
 - [2.2: Equivalence Relations, and Partial order](#) - [CC BY-NC-SA 4.0](#)
 - [2.3: Arithmetic of inequality](#) - [CC BY-NC-SA 4.0](#)
 - [2.4: Arithmetic of divisibility](#) - [CC BY-NC-SA 4.0](#)
 - [2.5: Divisibility Rules](#) - [CC BY-NC-SA 4.0](#)
 - [2.6: Division Algorithm](#) - [CC BY-NC-SA 4.0](#)
 - [2.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [3: Modular Arithmetic](#) - [CC BY-NC-SA 4.0](#)
 - [3.1: Modulo Operation](#) - [CC BY-NC-SA 4.0](#)
 - [3.2: Modulo Arithmetic](#) - [CC BY-NC-SA 4.0](#)
 - [3.3: Divisibility rules revisited](#) - [CC BY-NC-SA 4.0](#)
 - [3.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [4: Greatest Common Divisor, least common multiple and Euclidean Algorithm](#) - [CC BY-NC-SA 4.0](#)
 - [4.1: Greatest Common Divisor](#) - [CC BY-NC-SA 4.0](#)
 - [4.2: Euclidean algorithm and Bezout's algorithm](#) - [CC BY-NC-SA 4.0](#)
 - [4.3: Least Common Multiple](#) - [CC BY-NC-SA 4.0](#)
 - [4.4: Relatively Prime numbers](#) - [CC BY-NC-SA 4.0](#)
 - [4.5: Linear Congruences](#) - [CC BY-NC-SA 4.0](#)
 - [4.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [5: Diophantine Equations](#) - [CC BY-NC-SA 4.0](#)
 - [5.1: Linear Diophantine Equations](#) - [CC BY-NC-SA 4.0](#)
 - [5.2 : Linear Congruences Revisted](#) - [CC BY-NC-SA 4.0](#)
 - [5.3: Non-Linear Diophantine Equations](#) - [CC BY-NC-SA 4.0](#)
 - [5.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [6: Prime numbers](#) - [CC BY-NC-SA 4.0](#)
 - [6.1: Prime numbers](#) - [CC BY-NC-SA 4.0](#)
 - [6.2: GCD, LCM and Prime factorization](#) - [CC BY-NC-SA 4.0](#)
 - [6.3: Fermat Primes, Mersenne Primes and Primes of the other forms](#) - [Undeclared](#)
 - [6.E: Prime Numbers \(Exercises\)](#) - [CC BY-NC-SA 4.0](#)
 - [7: Numeration Systems](#) - [CC BY-NC-SA 4.0](#)
 - [7.1: Historical numeral systems](#) - [Undeclared](#)
 - [7.2: Number Bases](#) - [CC BY-NC-SA 4.0](#)
 - [7.3: Unusual Number systems](#) - [CC BY-NC-SA 4.0](#)
 - [7.E: Exercises](#) - [CC BY-NC-SA 4.0](#)
 - [Back Matter](#) - [Undeclared](#)
 - [Index](#) - [Undeclared](#)
 - [Glossary](#) - [Undeclared](#)
 - [Detailed Licensing](#) - [Undeclared](#)

- 8: Rational numbers, Irrational Numbers, and Continued fractions - *CC BY-NC-SA 4.0*
 - 8.1: Rational numbers - *CC BY-NC-SA 4.0*
 - 8.2: Irrational Numbers - *CC BY-NC-SA 4.0*
 - 8.3: Continued fractions - *CC BY-NC-SA 4.0*
 - 8.E: Exercises - *CC BY-NC-SA 4.0*
- Mock exams - *CC BY-NC-SA 4.0*
 - Sample Final - *CC BY-NC-SA 4.0*
 - Sample term test - *CC BY-NC-SA 4.0*
- Notations - *Undeclared*
 - Notations - *CC BY-NC-SA 4.0*
- Back Matter - *Undeclared*
 - Index - *Undeclared*
 - Glossary - *Undeclared*
 - Detailed Licensing - *Undeclared*
 - Reference - *Undeclared*

Reference

Arithmetical Wonderland, by Andy Liu

Elementary Number theory by Kenneth H. Rosen