CSE 150 Lectures

Jeffrey Jiang

Fall Semester 2023

Contents

Lecture 1

Based on work by Eduardo L., edited by Jeffrey J.

1.1 Modular Arithmetic

Theorem 1.1. ***Quotient-Remainder Theorem*** *states that given integers $a, b \in \mathbb{Z}$ that there exists integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. [1] Consider the set of integers in the form $a - xb \in \mathbb{Z}$. Since this is the set of integers, it contains the positive integers. Therefore, there exists a minimal positive number denoted by $a - qb$. Define $r = a - qb$. This is equivalent to $a = qb + r$ meaning such q, r exists. Now to prove that $0 \leq r < b$. Assume that $r = a - qb \geq b$. Thus, an additional b can be subtracted from both sides, $r - b = a - qb - b = a - (q + 1)b \geq 0$. However, $r - b < r$ and it is positive. This contradicts the claim that $r = a - qb$ is the smallest possible positive integer in the set (minimality of r is contradicted). In conclusion, $q, r \in \mathbb{Z}$ exists and $0 \leq r < b$. □

q is often called the quotient, and r is called the remainder. The process of finding such q, r is called *Euclidean division*.

Definition. *Modulo* is a binary operation accepting a pair of integers $\mathbb{Z} \times \mathbb{Z}$ and outputs one integer $\mathbb{Z}$. It is denoted typically with the operator by "mod." The output of a mod b is the remainder when performing Euclidean division with a and b.[2] Here, b is often called the *modulus*.

In class, we described a process of calculating the result of a modulo operation. Given a mod b, consecutively add or subtract b from a until $0 \leq a < b$. This is the same process described in the proof the quotient-remainder theorem to prove that such r exists in that range.

Examples:

- $42 \bmod 8 = 2$
- $(3 + 5) \bmod 4 = 8 \bmod 4 = 0$

[1] This is not my proof. This proof comes from Ireland, K., Rosen, M. (1982). *A Classical Introduction to Modern Number Theory*, Bogden and Quigley, Inc. Publishers. All credit goes to them.

[2] Typically in modular arithmetic, mathematicians do not define a modulo operator. They instead define modular congruences.

- $-3 \bmod 7 = 4$

As an aside, this definition of modulo is not universal. For example, different programming languages can output different results from modulo. Some preserve the sign of the modulus while others require the result to be nonnegative. These cases can arise when either operand is negative.

With these definitions, it can be useful to define some operations:

$$\begin{aligned} +_n : \quad & \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\ & (a, b) \longrightarrow (a + b) \bmod n \end{aligned}$$

Similar operations can be defined for $-_n$, and $\times_n$. It is not defined for division since integers are not closed under division. When there is no ambiguity surrounding the modulus, it may not be stated.

Examples:

- $5 +_7 5 = 3$
- $-3 -_8 16 = 5$
- $7 \times_5 4 = 3$

Lecture 2

Written by Jeffrey J.

2.2 Introduction to Set Theory

2.2.1 Basic Definitions and Examples

Definition. A *set* is a grouping of mathematical objects.

A set is an unordered collection where the multiplicity,i.e. number of times the element occurs, of elements does not matter.

Some important common sets:

- The set of natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$[1]
- The set of integers, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
  - Sometimes, positive and negative integers are denoted as $\mathbb{Z}^+$ and $\mathbb{Z}^-$ respectively.
  - Nonnegative integers can be denoted as $\mathbb{Z}_{\geq 0}$.
- The set of rational numbers, $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
- The set of irrational numbers, $\mathbb{R} - \mathbb{Q}$
- The set of complex numbers, $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$

Some more uncommon sets:

- The set of Gaussian integers, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$
- Complete set of residue classes modulo n, $\mathbb{Z}/n\mathbb{Z}$.
  - The element of $\mathbb{Z}/n\mathbb{Z}$ is the set of integers $\mathbb{Z}$ whose remainders are the same when divided by n.
  - e.g. $\mathbb{Z}/\not{=}\mathbb{Z}$ is the set containing the set of even numbers and odd numbers.
  - This is an example of a set containing sets.
- The set of integer polynomials, i.e. polynomials with integer coefficients and variable x, $\mathbb{Z}[x]$
  - Likewise, the set of real and complex polynomials are $\mathbb{R}[x]$ and $\mathbb{C}[x]$ respec-

[1] Some include 0 as part of the natural numbers.

tively.

  - These are examples of sets containing polynomials.
- The set of invertible $n \times n$ matrices with real entries, $\mathrm{GL}_n(\mathbb{R})$
  - This is an example of a set containing matrices.
- The set of permutations on set S, Sym_S
  - A permutation is a function that "rearranges" the order of the set.
  - This is an example of a set containing functions.

Sets are flexible, and they can contain many more mathematical constructs than listed above.

Definition. The *empty set* $\emptyset$ is the set without any elements.

2.2.2 Set Operations

Definition. Two sets are *equal* if they contain the same elements. Likewise, two sets are *not equal* if they do not contain the same elements. Set equality and inequality is denoted by $=$ and $\neq$ respectively.

Definition. If set S *contains* element x, then $x \in S$.

Definition. Set A is a *subset* of set B if set B contains all elements of A, i.e. $a \in B \,\forall\, a \in A$. This is denoted as $A \subseteq B$.

Examples:

- $\{1, 2\} \subseteq \{1, 2, 3\}$
- $\{2, 4\} \not\subseteq \{1, 2, 3\}$
- $2 \not\subseteq \{1, 2, 3\}$ but $2 \in \{1, 2, 3\}$
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\mathbb{R} - \mathbb{Q} \subseteq \mathbb{R}$
- $\mathbb{Z}[i] \subseteq \mathbb{C}$
- $\emptyset \subseteq \{-2, 4, 7, 0\}$

Proposition 2.1. *The empty set $\emptyset$ is a subset of any set S.*

Proof. Since the empty set does not contain any elements, by definition, S contains all of its elements. Therefore, $\emptyset \subseteq S$. □

Proposition 2.2. *Given sets A, B, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof. Given $A = B$. Then, by definition, all elements in A is contained in element B. Therefore, $A \subseteq B$. Additionally, all elements of B are contained in A. So, $B \subseteq A$.

Now to prove the converse. Given $A \subseteq B$ and $B \subseteq A$, assume that $A \neq B$. This means that there exists an element in A or B which is not contained in the other set. Consider the case where this element x is in A but not B, i.e. $x \in A$, $x \notin B$. By definition, the statement $A \subseteq B$ implies that all elements of A are contained in B. This is a contradiction. The same contradiction is reached if $x \in B$ and $x \notin A$. Therefore, if $A \subseteq B$ and $B \subseteq A$, then $A = B$. □

Definition. Set A is a *proper subset* of set B if A is a subset of B and A is not equal to B. This is denoted as $A \subset B$.

A corollary of proposition 2.1 is the empty set $\emptyset$ is a proper subset of any set S as long as $S \neq \emptyset$.

Lecture 3

Index