CSE 150 Lectures

Jeffrey Jiang

Fall Semester 2023

Contents

Lecture 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:

- $42 \bmod 8 = 2$
- $(3 + 5) \bmod 4 = 8 \bmod 4 = 0$
- $-3 \bmod 7 = 4$

[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.

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

Lemma 1. *test 2*

Lecture 3