Lecture 4

Reference: Judson, Chapter 2

Congruence relations and $\mathbb{Z}_n$.

Throughout this section let us fix a positive integer $n \in \mathbb{Z}$ (to get reasonable examples further on it is natural to assume also that $n > 1$).

Definition 1: Congruence relation modulo n

Given fixed nonzero n, let us introduce an equivalence relation on $\mathbb{Z}$ as follows:

$$a \sim b \Longleftrightarrow n|(a-b),$$

i.e., a is equivalent to b if and only if their difference if divisible by n. In this case we will write

$$a \equiv b \mod n$$

'a is equivalent to b modulo n'.

Problem 1: Verify that this is an equivalence relation.

The equivalence class modulo this equivalence relation is called a *congruence class*. Clearly numbers a and b are in the same congruence class if and only if a and b have the same remainder under division by b, so that the set of equivalence classes is

$$(\mathbb{Z}/\sim) = \Big\{[0],[1],\dots,[n-1]\Big\},$$

where

$$[a] = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

We will use a special notation for the set of equivalence classes $\mathbb{Z}/\sim$ and denote it

$$\mathbb{Z}_n := \Big\{[0],[1],\dots,[n-1]\Big\}$$

to keep track of our choice of n. Another commonly used notation is $\mathbb{Z}/n\mathbb{Z}$.

Arithmetics in $\mathbb{Z}_n$

So far $\mathbb{Z}_n$ is only a set consisting of n elements. Our next goal is to introduce addition and multiplication operations on $\mathbb{Z}_n$. To this end we will need a simple lemma.

Lemma 1

If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

$$(a+b) \equiv (a'+b') \mod n$$

$$ab \equiv a'b' \mod n.$$

Proof. We will prove the claim about multiplication. The claim about addition is proved similarly (and is a good exercise).
From the assumptions of the lemma, of know that

$$a' = a + kn \quad b' = b + ln$$

for some $k, l \in \mathbb{Z}$. Therefore the difference

$$a'b' - ab = (a+kn)(b+ln) - ab = knb + lna + kln^2 = n(ab + la + kln)$$

is clearly divisible by n, so that $a'b' \equiv ab \mod n$. □

This lemma allows us introduce addition and multiplication on $\mathbb{Z}_n$ as follows.

Definition 2

Given two congruence classes $[a]$ and $[b]$ in $\mathbb{Z}_n$ we choose *representatives* $a \in [a]$ and $b \in [b]$ and introduce an operation $\oplus$

$$[a] \oplus [b] := [a + b]$$

and an operation $\odot$

$$[a] \odot [b] := [ab].$$

The above lemma ensures that this definition is *correct*, i.e., if we had chosen different representatives $a' \in [a]$ and $b' \in [b]$, we would get the same congruence classes as the results of $\oplus$ and $\odot$ operations. Operations $\oplus$ and $\odot$ satisfy all the axioms **G1, G2, G3, GC, R1, R2, R3**, i.e.:

G1 $\oplus$ is associative

G2 $\oplus$ has neutral element $[0]$

G3 $[a]$ has additive inverse $[-a]$

GC $\oplus$ is commutative

R1 $\odot$ is associative

R2 $\odot$ is distributive with respect to $\oplus$

R3 $\odot$ has neutral element $[1]$,

which means that the pair $(\mathbb{Z}_n, \oplus)$ is a *commutative group* and the triple $(Z_n, \oplus, \odot)$ is a *ring*.

For this lecture we will keep notations $[a]$ to denote an element of $\mathbb{Z}_n$ and write $\oplus$ and $\odot$ for addition and multiplication to underline that these are new elements and new operations. However, from the next lecture on, we will write just $a, +$, and simply add (mod n), if we are considering those in $\mathbb{Z}_n$.

Example 1

In $\mathbb{Z}_5$ we have

$$[1] \oplus [4] = [0]$$

and

$$[4] \odot [4] = [1].$$

Problem 2: Find all elements in $\mathbb{Z}_{16}$ such that $[a] \odot [a] = [1]$.

Multiplication in $\mathbb{Z}_n$ has several new features, which are not present in $\mathbb{Z}$.

Example 2

In $\mathbb{Z}_7$ we have $[3] \odot [5] = [1]$. For this reason, $[5]$ plays the same role as the number $1/3$ in $\mathbb{Q}$, i.e., it is multiplicative inverse for 3.
For instance, if we want to solve equation

$$[3] \odot y = [5]$$

in $\mathbb{Z}_7$, we can multiply both sides with $[5]$ (which will have the same effect as division by $[3]$), and get

$$[5] \odot [3] \odot y = [5] \odot [5].$$

Using the fact that $[5] \odot [3] = [1]$ and $[5] \odot [5] = [25] = [4]$ in $\mathbb{Z}_7$ we conclude

$$y = [4].$$

Example 3

In $\mathbb{Z}_6$ the product of two nonzero elements might be zero:

$$[2]\odot[3]=[6]=[0] \quad \text{in } \mathbb{Z}_6.$$

The above example motivates us to introduce the following notion.

Definition 3

Congruence class $[a]$ in $\mathbb{Z}_n$ is called a *unit* (or *multiplicatively invertible*), if there exists a congruence class $[b]$ such that

$$[a]\odot[b]=[1].$$

Problem 3: Prove that multiplicative inverse, if exists, unique.

Example 4

In $\mathbb{Z}_6$ congruence classes $[1],[5]$ are invertible

$$[1]\odot[1]=[1], \quad [5]\odot[5]=[1]$$

while the remaining classes are not invertible (why?).

NB 1: Caution! In general in $\mathbb{Z}_n$ one can not cancel nonzero factors from both sides of an identity, for example in $\mathbb{Z}_6$

$$[2]\odot[3]=[0]=[2]\odot[0]$$

while

$$[3]\neq[0].$$

In the next lecture we will give necessary and sufficient condition under which we can cancel factor $[a]$ in $\mathbb{Z}_n$.