

Notes on sets of equivalence classes and  $\mathbb{Z}_n$ 1. The Definition of  $\mathbb{Z}_n$ 

If  $R$  is an equivalence relation on a set  $A$ , we denote the set of all equivalence classes by  $A/R$  (read “ $A$  modulo  $R$ ” or “ $A \bmod R$ ”). [Recall that  $A/R$  forms a partition of the set  $A$ .]

**Example:** If  $\equiv$  is the relation of “congruence mod 2”, on  $\mathbb{Z}$ , then

$$\mathbb{Z}/\equiv = \{\bar{0}, \bar{1}\}$$

where

$$\begin{aligned} \bar{0} &= \{n \in \mathbb{Z} : n \equiv 0 \pmod{2}\} \\ &= \{n \in \mathbb{Z} : n = 2q \text{ for some } q \in \mathbb{Z}\} \\ &= \text{the set of even integers} \end{aligned}$$

and

$$\begin{aligned} \bar{1} &= \{n \in \mathbb{Z} : n \equiv 1 \pmod{2}\} \\ &= \{n \in \mathbb{Z} : n = 2q + 1 \text{ for some } q \in \mathbb{Z}\} \\ &= \text{the set of odd integers} \end{aligned}$$

In these notes, we will only look at  $\mathbb{Z}/R$  where  $R$  is “congruence mod  $n$ ” for some natural number  $n \geq 2$ :

$$\begin{aligned} a \equiv b \pmod{n} &\text{ iff } n \mid (a - b) \\ &\text{ iff } a - b = nk \text{ for some } k \in \mathbb{Z} \end{aligned}$$

This important class of examples gets a special notation:

We denote by  $\mathbb{Z}_n$  the set of all equivalence classes under the relation of “congruence mod  $n$ ”.

By the Division Algorithm, for every  $a \in \mathbb{Z}$ ,  $a = nq + r$ , where  $r$  is uniquely determined by  $0 \leq r < n$ , so that  $a \equiv r \pmod{n}$ , or  $\bar{a} = \bar{r}$ , for exactly one  $r \in \{0, 1, 2, \dots, n-1\}$ . This tells us that:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

## 2. Arithmetic in $\mathbb{Z}_n$

We can define addition and multiplication in  $\mathbb{Z}_n$  by:

$$\bar{a} + \bar{b} = \overline{a + b}$$

and

$$\bar{a} \bar{b} = \overline{ab}$$

The main question here is whether these are “well-defined” functions ( $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ). That is:

If  $\bar{a} = \bar{a}'$  and  $\bar{b} = \bar{b}'$ , does it follow that  $\overline{a + b} = \overline{a' + b'}$  and  $\overline{ab} = \overline{a'b'}$ ? Yes!

**Proof (for addition):** Let  $\bar{a}, \bar{b}, \bar{a}', \bar{b}' \in \mathbb{Z}_n$  and assume that  $\bar{a} = \bar{a}'$  and  $\bar{b} = \bar{b}'$ .

Then  $a - a' = nk$  and  $b - b' = nl$  for some  $k, l \in \mathbb{Z}$

$$\implies (a + b) - (a' + b') = (a - a') + (b - b') = nk + nl = n(k + l) \in n\mathbb{Z}.$$

Therefore,  $a + b \equiv a' + b' \pmod{n}$ , or  $\overline{a + b} = \overline{a' + b'}$ .

The proof for multiplication is similar (and left as an exercise). □

### **Example:** “clock arithmetic”

“Clock arithmetic”, if we disregard the distinction between **am** and **pm**, is arithmetic mod 12 (to account for the difference between **am** and **pm**, use arithmetic mod 24):

$$\begin{aligned} \bar{1} + \bar{12} &= \bar{13} = \bar{1} \text{ (since } 13 \equiv 1 \pmod{12}\text{)} \\ \bar{6} + \bar{8} &= \bar{14} = \bar{2} \text{ (that is, 8 hours from 6:00 is 2:00)} \end{aligned}$$

**Example:** Check the addition and multiplication tables given here for  $\mathbb{Z}_3$ :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Is addition in  $\mathbb{Z}_3$  commutative? associative?

Is multiplication commutative? associative?

Does addition distribute over multiplication? Does multiplication distribute over addition?

Is there an additive identity in  $\mathbb{Z}_3$ ? a multiplicative identity?

Are there additive inverses? multiplicative inverses?

**Theorem:** Let  $n \in \mathbb{N}$ ,  $n \geq 2$ . For all  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ :

(i)  $\bar{a} + \bar{b} = \bar{b} + \bar{a}$  and  $\bar{a} \bar{b} = \bar{b} \bar{a}$

(ii)  $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$  and  $(\bar{a} \bar{b}) \bar{c} = \bar{a} (\bar{b} \bar{c})$

(iii)  $\bar{a} (\bar{b} + \bar{c}) = \bar{a} \bar{b} + \bar{a} \bar{c}$

(iv)  $\exists!$  element  $\bar{0} \in \mathbb{Z}_n$  satisfying  $\bar{a} + \bar{0} = \bar{a}$  for all  $\bar{a} \in \mathbb{Z}_n$   
 $\exists!$  element  $\bar{1} \in \mathbb{Z}_n$  satisfying  $\bar{a} \bar{1} = \bar{a}$  for all  $\bar{a} \in \mathbb{Z}_n$

(v) For all  $\bar{a} \in \mathbb{Z}_n$ ,  $\exists!$   $\bar{x} \in \mathbb{Z}_n$  satisfying  $\bar{a} + \bar{x} = \bar{0}$ .

### 3. Well-Defined Functions

When defining functions on sets of equivalence classes, we have to be particularly careful that our functions are “well-defined”, since the defining rule for the function might apparently depend on the choice of representative of an equivalence class.

**Note:** It is convenient to introduce a notation to distinguish equivalence classes corresponding to different relations. We denote by  $[x]_n$  the equivalence class of  $x$  with respect to the relation of congruence mod  $n$ .

**Example:** Define  $f : \mathbb{Z}_2 \rightarrow \mathbb{Z}_3$  by  $f([n]_2) = [2n + 1]_3$ .

Is this function well-defined? That is, does  $f$  actually define a function? In other words, if  $[a]_2 = [b]_2$ , does it follow that  $f([a]_2) = f([b]_2)$ ?

**Check it:** If  $[a]_2 = [b]_2$ , then  $a - b = 2k$  for some  $k \in \mathbb{Z}$ .

(We need to check whether  $[2a + 1]_3 = [2b + 1]_3$ , that is, whether  $(2a + 1) - (2b + 1) \in 3\mathbb{Z}$ )

$$(2a + 1) - (2b + 1) = 2(a - b) = 2(2k) = 3k + k \equiv k \pmod{3}$$

It seems to depend on  $k$  whether or not  $[2a + 1]_3 = [2b + 1]_3$ . So, we can look for a counterexample (to the statement that  $f$  is well-defined).

$[1]_2 = [3]_2$ , and by the definition of  $f$  given,  $f([1]_2) = [3]_3 = [0]_3$  but  $f([3]_2) = [7]_3 = [1]_3$ . Since  $[0]_3 \neq [1]_3$ ,  $f$  is **not** well-defined.  $\square$