

# Mathematics Homework Sheet 2

Authors: Abdullah Oguz Topcuoglu & Ahmed Waleed Ahmed  
Badawy Shora

## Problem 1

(a)

$Z_5$ :

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$Z_7$ :

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b)

$Z_4$ :

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

  

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(Z_4, \oplus, \times)$  is not a field because  $[2]$  does not have a multiplicative inverse.

## Problem 2

(a)

Let  $f : Z_n \rightarrow Z_n$  be:

$$f([i]) = [i] + [m], \quad [m] \in Z_n$$

We want to show that  $f$  is a bijection.

- **Injective:** Suppose  $f([i_1]) = f([i_2])$ :

$$[i_1] + [m] = [i_2] + [m]$$

$$[i_1 + m] = [i_2 + m]$$

Thus, we have that  $n$  divides  $(i_1 + m) - (i_2 + m)$ .

Equivalently,  $n$  divides  $(i_1 - i_2)$

$$\therefore [i_1] = [i_2]$$

Thus,  $f$  is injective.

- **Surjective:** Let  $[j] \in Z_n$ . We want to show that there exists an  $[x]$  such that  $f([x]) = [j]$ :

$$f([j - m]) = [j - m] + [m] = [j]$$

Thus,  $f$  is surjective.

Thus,  $f$  is a bijection.

(b)

$[i] \rightarrow [i] + [1]: (01234567)$   
 $[i] \rightarrow [i] + [2]: (0246)(1357)$   
 $[i] \rightarrow [i] + [3]: (03614725)$   
 $[i] \rightarrow [i] + [4]: (04)(15)(26)(37)$

### Problem 3

(a)

Let  $f : Z_p \setminus \{[0]\} \rightarrow Z_p \setminus \{[0]\}$  be:

$$f([i]) = [m] \cdot [i], \quad [m] \in Z_p \setminus \{[0]\}$$

We want to show that  $f$  is a bijection.

- **Injective:** Suppose  $f([i_1]) = f([i_2])$ :

$$[m] \cdot [i_1] = [m] \cdot [i_2], [m \cdot i_1] = [m \cdot i_2]$$

Thus,  $P$  divides  $(m \cdot i_1 - m \cdot i_2)$ .

Equivalently,  $P$  divides  $(m \cdot (i_1 - i_2))$ .

Since  $P$  is a prime number,  $P$  divides either  $m$  or  $(i_1 - i_2)$ .

Since  $m \in \mathbb{Z} \setminus \{[0]\}$ ,  $P$  divides  $(i_1 - i_2)$ .

$$\therefore [i_1] = [i_2]$$

Thus,  $f$  is injective.

- **Surjective:** Let  $[j] \in Z_p \setminus \{[0]\}$ . We want to show that there exists an  $[x]$  such that  $f([x]) = [j]$ :

$$f([j \cdot m^{-1}]) = [j \cdot m^{-1}] \cdot [m] = [j]$$

Thus,  $f$  is surjective.

Thus,  $f$  is a bijection.

(b)

$[i] \rightarrow [6] \cdot [i]: (16)(25)(34)$   
 $[i] \rightarrow [2] \cdot [i]: (124)(365)$

### Problem 4

Let  $I$  be an arbitrary interval. We will show that  $I$  and  $\mathbb{R}$  have the same cardinality by constructing a bijection between them.

## Problem 5

(a)

Let  $(p, n), (q, m) \in N_0 \times N_0$ . We want to show that  $\sim$  is an equivalence relation on  $N_0 \times N_0$ :

- **Reflexive:** We want to show that  $(p, n) \sim (p, n)$ :

$$p + n = p + n$$

Thus,  $\sim$  is reflexive.

- **Symmetric:** We want to show that if  $(p, n) \sim (q, m)$ , then  $(q, m) \sim (p, n)$ :

$$p + m = q + n$$

Thus,

$$q + n = p + m$$

Thus,  $\sim$  is symmetric.

- **Transitive:** We want to show that if  $(p, n) \sim (q, m)$  and  $(q, m) \sim (r, s)$ , then  $(p, n) \sim (r, s)$ :

$$p + m = q + n$$

and

$$q + s = r + m$$

Thus,

$$p + s = r + n$$

Thus,  $\sim$  is transitive.

Thus,  $\sim$  is an equivalence relation on  $N_0 \times N_0$ .

(b)

Let  $k \in N_0$ . We want to show that  $(p, n) \sim (k + p, k + n)$ :

$$p + (k + n) = (k + p) + n$$

Thus,  $(p, n) \sim (k + p, k + n)$ .

(c)

Let  $[(k, 0)]$  be the equivalence class of  $(k, 0)$ . We want to find an equivalence class  $-[(k, 0)]$  such that

$$-[(k, 0)] + [(k, 0)] = [(0, 0)]$$

Define  $-\lceil(k, 0)\rceil$  as  $\lceil(0, k)\rceil$ . Then,

$$\lceil(0, k)\rceil + \lceil(k, 0)\rceil = \lceil(0 + k, k + 0)\rceil = \lceil(k, k)\rceil = \lceil(0, 0)\rceil$$

Thus, we have

$$-\lceil(k, 0)\rceil + \lceil(k, 0)\rceil = \lceil(0, 0)\rceil$$

Thus,  $-\lceil(k, 0)\rceil$  is the equivalence class with the property that  $-\lceil(k, 0)\rceil + \lceil(k, 0)\rceil = \lceil(0, 0)\rceil$ .