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 $f : Z_n \to Z_n$ be:

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

We want to show that f is a bijection.

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

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

  Thus,

  $$[i_1] = [i_2]$$

  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)

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