MTH 4441 HW - Working in $\mathbb{Z}_n$ - Solutions

FALL 2017

Pat Rossi Name _____

1. Perform the following computations in $\mathbb{Z}_{12}$

   Remark: In each of the following exercises, our strategy will be to compute the value of each of the expressions, modulo 12, *using the proper remainders modulo 12.* The resulting value, modulo 12, will also be *proper remainder modulo 12.*

   a. $8 + 7$

   $$8 + 7 = 15 = (1)(12) + 3 \equiv 3 \pmod{12}$$

   i.e., $8 + 7 \equiv 3 \pmod{12}$

   $\boxed{\Rightarrow 8 + 7 = 3 \text{ in } \mathbb{Z}_{12}}$

   b. $10 + 9$

   $$10 + 9 = 19 = (1)(12) + 7 \equiv 7 \pmod{12}$$

   i.e., $10 + 9 \equiv 7 \pmod{12}$

   $\boxed{\Rightarrow 10 + 9 = 7 \text{ in } \mathbb{Z}_{12}}$

   c. $8 \cdot 11$

   $$8 \cdot 11 = 88 = 7 \cdot \mathbf{12} + 4 \equiv 4 \pmod{12}$$

   i.e., $8 \cdot 11 \equiv 4 \pmod{12}$

   $\boxed{\Rightarrow 8 \cdot 11 = 4 \text{ in } \mathbb{Z}_{12}}$

   d. $6 \cdot 9$

   $$6 \cdot 9 = 54 = 4 \cdot \mathbf{12} + 6 \equiv 6 \pmod{12}$$

   i.e., $6 \cdot 9 \equiv 6 \pmod{12}$

   $\boxed{\text{i.e., } 6 \cdot 9 = 6 \text{ in } \mathbb{Z}_{12}}$

e. $6 \cdot (9 + 11)$

$6 \cdot (9 + 11) = 120 = 10 \cdot \mathbf{12} + 0 \equiv 0 \pmod{12}$

i.e., $6 \cdot (9 + 11) \equiv 0 \pmod{12}$

$\boxed{\Rightarrow 6 \cdot (9 + 11) = 0 \text{ in } \mathbb{Z}_{12}}$

f. $5 \cdot (8 + 11)$

$5 \cdot (8 + 11) = 95 = 7 \cdot \mathbf{12} + 11 \equiv 11 \pmod{12}$

i.e., $5 \cdot (8 + 11) \equiv 11 \pmod{12}$

$\boxed{\Rightarrow 5 \cdot (8 + 11) = 11 \text{ in } \mathbb{Z}_{12}}$

g. $6 \cdot 9 + 6 \cdot 7$

$6 \cdot 9 + 6 \cdot 7 = 54 + 42 = 96 = 8 \cdot \mathbf{12} + 0 \equiv 0 \pmod{12}$

i.e., $6 \cdot 9 + 6 \cdot 7 \equiv 0 \pmod{12}$

$\boxed{\Rightarrow 6 \cdot 9 + 6 \cdot 7 = 0 \text{ in } \mathbb{Z}_{12}}$

h. $5 \cdot 8 + 5 \cdot 11$

$5 \cdot 8 + 5 \cdot 11 = 40 + 55 = 95 = 7 \cdot \mathbf{12} + 11 \equiv 11 \pmod{12}$

i.e., $5 \cdot 8 + 5 \cdot 11 \equiv 11 \pmod{12}$

$\boxed{\Rightarrow 5 \cdot 8 + 5 \cdot 11 = 11 \text{ in } \mathbb{Z}_{12}}$

i. $3 \cdot 7 + 4 \cdot 9$

$3 \cdot 7 + 4 \cdot 9 = 21 + 36 = 57 = 4 \cdot \mathbf{12} + 9 \equiv 9 \pmod{12}$

i.e., $3 \cdot 7 + 4 \cdot 9 \equiv 9 \pmod{12}$

$\boxed{\Rightarrow 3 \cdot 7 + 4 \cdot 9 = 9 \text{ in } \mathbb{Z}_{12}}$

j. $8 \cdot 5 - 2 \cdot 10$

$8 \cdot 5 - 2 \cdot 10 = 40 - 20 = 20 = 1 \cdot \mathbf{12} + 8 \equiv 8 \pmod{12}$

i.e., $85 - 2 \cdot 10 \equiv 8 \pmod{12}$

$\boxed{\Rightarrow 8 \cdot 5 - 2 \cdot 10 = 8 \text{ in } \mathbb{Z}_{12}}$

k. 2^9

Observe: $2^4 = 16 \equiv 4 \pmod{12}$

$2^9 = 2^{2(4)+1} = 2^{2(4)}2^1 = (4)^2\, 2 \equiv 4 \cdot 2 \pmod{12} \equiv 8 \pmod{12}$

i.e., $2^9 \equiv 8 \pmod{12}$

$\boxed{\Rightarrow 2^9 = 8 \text{ in } \mathbb{Z}_{12}}$

l. 3^4

$3^4 = 81 = 6 \cdot \mathbf{12} + 9 \equiv 9 \pmod{12}$

i.e., $3^4 \equiv 9 \pmod{12}$

$\boxed{\Rightarrow 3^4 = 9 \text{ in } \mathbb{Z}_{12}}$

2. ~

a. Verify that $1 \cdot 2 \cdot 3 \cdot 4 = 4$ in $\mathbb{Z}_5$

Observe: $1 \cdot 2 \cdot 3 \cdot 4 = 24 = (4)(\mathbf{5}) + 4 \equiv 4 \pmod 5$

i.e., $1 \cdot 2 \cdot 3 \cdot 4 \equiv 4 \pmod 5$

$\boxed{\Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 = 4 \text{ in } \mathbb{Z}_5}$

b. $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6$ in $\mathbb{Z}_7$

Observe: $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720 = (102)(\mathbf{7}) + 6 \equiv 6 \pmod 7$

i.e., $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 6 \pmod 7$

$\boxed{\Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6 \text{ in } \mathbb{Z}_7}$

c. Evaluate $1 \cdot 2 \cdot 3$ in $\mathbb{Z}_4$

Observe: $1 \cdot 2 \cdot 3 = 6 = (1)(\mathbf{4}) + 2 \equiv 2 \pmod 4$

i.e., $1 \cdot 2 \cdot 3 \equiv 2 \pmod 4$

$\boxed{\Rightarrow 1 \cdot 2 \cdot 3 = 2 \text{ in } \mathbb{Z}_4}$

d. Evaluate $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ in $\mathbb{Z}_6$

Observe: $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120 = (20)(\mathbf{6}) + 0 \equiv 0 \pmod 6$

i.e., $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \equiv 0 \pmod 6$

$\boxed{\Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 0 \text{ in } \mathbb{Z}_6}$

e. Evaluate $4 \cdot 3$ in $\mathbb{Z}_4$

Observe: $4 \cdot 3 = 12 = (3)\,(\mathbf{4}) + 0 \equiv 0 \,(\mathrm{mod}\, 4)$

i.e., $4 \cdot 3 \equiv 0 \,(\mathrm{mod}\, 4)$

$\boxed{\Rightarrow 4 \cdot 3 = 0 \text{ in } \mathbb{Z}_4}$

f. Evaluate $4 \cdot 2$ in $\mathbb{Z}_4$

Observe: $4 \equiv 0 \,(\mathrm{mod}\, 4)$

$\Rightarrow 4 \cdot 2 \equiv 0 \cdot 2 \,(\mathrm{mod}\, 4) \equiv 0 \,(\mathrm{mod}\, 4)$

$\boxed{\Rightarrow 4 \cdot 2 = 0 \text{ in } \mathbb{Z}_4}$

g. Evaluate $5 \cdot 2$ in $\mathbb{Z}_5$

Observe: $5 \equiv 0 \,(\mathrm{mod}\, 5)$

$\Rightarrow 5 \cdot 2 \equiv 0 \cdot 2 \,(\mathrm{mod}\, 5) \equiv 0 \,(\mathrm{mod}\, 5)$

$\boxed{\Rightarrow 5 \cdot 2 = 0 \text{ in } \mathbb{Z}_5}$

h. Evaluate $5 \cdot 4$ in $\mathbb{Z}_5$

Observe: $5 \equiv 0 \,(\mathrm{mod}\, 5)$

$\Rightarrow 5 \cdot 4 \equiv 0 \cdot 4 \,(\mathrm{mod}\, 5) \equiv 0 \,(\mathrm{mod}\, 5)$

$\boxed{\Rightarrow 5 \cdot 4 = 0 \text{ in } \mathbb{Z}_5}$

3. Make Addition Tables for each of the following:

Remark: Note that in the addition tables for $\mathbb{Z}_n$, the element 0 is the identity. Also, each element of the group must appear exactly once in each row and each column.

a. $\mathbb{Z}_2$

+	0	1
0	0	1
1	1	0

b. $\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	0	2	1

c. $\mathbb{Z}_5$

+	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

d. $\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

e. $\mathbb{Z}_7$

+	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

f. $\mathbb{Z}_8$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

4. Make multiplication tables for each of the following

Remark: Note that in the multiplication tables for $\mathbb{Z}_n$, the element 1 is the identity. Also, a set which contains the element 0 under the the binary operation of multiplication is **not a group.** There will be a row and a column of zeros.

a. $\mathbb{Z}_2$

+	0	1
0	0	0
1	0	1

b. $\mathbb{Z}_3$

+	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

c. $\mathbb{Z}_5$

+	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

d. $\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

e. $\mathbb{Z}_7$

+	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

f. $\mathbb{Z}_8$

+	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

5. For each of the following $\mathbb{Z}_n$, list all of the elements of $\mathbb{Z}_n$ that have multiplicative inverses in $\mathbb{Z}_n$.

   Remark: The elements of $\mathbb{Z}_n$ that have multiplicative inverse, are exactly those **non-zero** elements of $\mathbb{Z}_n$ that are **relatively prime to** n.

   a. $\mathbb{Z}_6$ $1, 5$

   b. $\mathbb{Z}_8$ $1, 3, 5, 7$

   c. $\mathbb{Z}_{10}$ $1, 3, 7, 9$

   d. $\mathbb{Z}_{12}$ $1, 5, 7, 11$

   e. $\mathbb{Z}_{18}$ $1, 5, 7, 11, 13, 17$

   f. $\mathbb{Z}_{20}$ $1, 3, 7, 9, 11, 13, 17, 19$

6. Find all zero divisors in each of the following $\mathbb{Z}_n$

   Remark: The zero divisors in $\mathbb{Z}_n$ are exactly those **non-zero** elements of $\mathbb{Z}_n$ that are NOT relatively prime to n.

   a. $\mathbb{Z}_6$ $2, 3, 4$

   b. $\mathbb{Z}_8$ $2, 4, 6$

   c. $\mathbb{Z}_{10}$ $2, 4, 5, 6, 8$

   d. $\mathbb{Z}_{12}$ $2, 3, 4, 6, 8, 9, 10$

   e. $\mathbb{Z}_{18}$ $2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16$

   f. $\mathbb{Z}_{20}$ $2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18$

In exercises -, decide whether each of the given sets is a group with respect to the indicated operation. State all of the group axioms that fail to hold. If it is a group, state its order.

25. The set $\{1, 3\} \subseteq \mathbb{Z}_8$ with operation multiplication

    This IS a group of order 2

    Observe:

    $1 \cdot 1 = 1$

    $1 \cdot 3 = 3$

    $3 \cdot 1 = 3$

    $3 \cdot 3 = 1$

    From this we can see that:

    i. the operation is **closed**

    ii. the element 1 is the **identity**

    iii. each element is its own **inverse**

    Also, associativity is inherited from the "parent group" $\mathbb{Z}_8$

26. The set $\{1, 3, 5\} \subseteq \mathbb{Z}_8$ with operation multiplication

    This is **NOT a group.**

    Observe: $3 \cdot 5 = 7 = 5 \cdot 3$

    i.e., the operation is **NOT closed** on the set $\{1, 3, 5\}$

    All other axioms hold, as 1 is the identity and each element is its own inverse.

27. The set $\{1, 2, 3\} \subseteq \mathbb{Z}_4$ with operation multiplication

    This is **NOT a group.**

    Observe: $2 \cdot 2 = 0$

    i.e., the operation is **NOT closed** on the set $\{1, 2, 3\}$

    Also, since $2 \cdot 2 = 0$, **the element 2 has no multiplicative inverse.**

28. The set $\{1, 2, 3, 4\} \subseteq \mathbb{Z}_5$ with operation multiplication

This IS a group of order 4

Consider the "group table"**:**

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From this we can see that:

i. the operation is **closed**

ii. the element 1 is the **identity**

iii. each element has an **inverse**

Also, associativity is inherited from the "parent group" $\mathbb{Z}_8$

29. The set $\{0, 2, 4\} \subseteq \mathbb{Z}_8$ with operation multiplication

This is NOT a group

The multiplicative identity 1 is not and element of $\{0, 2, 4\}$, so the set $\{0, 2, 4\}$ **has no identity.**

Also, **none of the elements** $0, 2, 4$ **have an inverse,** as there is no element of $\mathbb{Z}_8$ that we can multiply them by to get the multiplicative identity 1.

30. The set $\{0, 2, 4, 6, 8\} \subseteq \mathbb{Z}_{10}$ with operation multiplication

This is NOT a group

The multiplicative identity 1 is not and element of $\{0, 2, 4, 6, 8\}$, so the set $\{0, 2, 4, 6, 8\}$ **has no identity.**

Also, **none of the elements** $0, 2, 4, 6, 8$ **have an inverse,** as there is no element of $\mathbb{Z}_{10}$ that we can multiply them by to get the multiplicative identity 1.

31. The set $\{0, 2, 4, 6, 8\} \subseteq \mathbb{Z}_{10}$ with operation addition

This IS a group of order 5

Consider the "group table":

$+$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

From this we can see that:

i. the operation is **closed**

ii. the element 0 is the **identity**

iii. each element has an **inverse**

Also, associativity is inherited from the "parent group" $\mathbb{Z}_{10}$

32. The set $\{0, 2, 4, 6\} \subseteq \mathbb{Z}_8$ with operation addition

This IS a group of order 4

Consider the "group table":

$+$	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

From this we can see that:

i. the operation is **closed**

ii. the element 0 is the **identity**

iii. each element has an **inverse**

Also, associativity is inherited from the "parent group" $\mathbb{Z}_8$