Solution for Math 301 Homework 4

2.2

6. Solve the equation $x^2 \oplus [8] \odot x = [0]$ in $\mathbb{Z}_9$.

In $\mathbb{Z}_9$, we have

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
$8x$	0	8	7	6	5	4	3	2	1
x^2+8x	0	0	2	6	3	2	3	6	2

Therefore, the solutions for $x^2 \oplus [8] \odot x = [0]$ in $\mathbb{Z}_9$ are $x = [0]$ and $x = [1]$.

8. Solve the equation $x^3 \oplus x^2 = [2]$ in $\mathbb{Z}_{10}$.

In $\mathbb{Z}_{10}$, we have

x	0	1	2	3	4	5	6	7	8	9
x^2	0	1	4	9	6	5	6	9	4	1
x^3	0	1	8	7	4	5	6	3	2	9
x^3+x^2	0	2	2	6	0	0	2	2	6	0

Therefore, the solutions for $x^3 \oplus x^2 = [2]$ in $\mathbb{Z}_{10}$ are $x = [1],\ [2],\ [6],\ [7]$.

12. Prove or disprove: If $[a] \odot [b] = [0]$ in $\mathbb{Z}_n$, then $[a] = [0]$ or $[b] = [0]$.

The statement is not true. Let $a = 2,\ b = 3,\ n = 6$. In $\mathbb{Z}_6$, we have $[2] \odot [3] = [6] = [0]$ but $[2],\ [3] \neq [0]$.

14 c). If p is a positive prime, show that the only solutions of $x^2 \oplus x = [0]$ in $\mathbb{Z}_p$ are $[0]$ and $[p-1]$.

Suppose p is prime and $x^2 \oplus x = [0]$ in $\mathbb{Z}_p$ for $x = [a]$. We have

$$p|(a^2+a) \Rightarrow p|a(a+1) \Rightarrow p|a \text{ or } p|(a+1).$$

Therefore, we have $[a] = [0]$ or $[a+1] = [0]$.

$$[a+1] = [0] \Rightarrow [a] = [-1] = [p-1].$$

Therefore, $x = [0]$ or $x = [p-1]$.

16. Find all $[a]$ in $\mathbb{Z}_n$ for which the equation $[a] \odot x = [1]$ has a solution, in the case when

(a) $n = 5$, (b) $n = 4$, (c) $n = 3$, (d) $n = 6$

For $[a] \odot x = [1]$ to have a solution, we must have $[a] \neq [0]$.

(a) In $\mathbb{Z}_5$, $[1] \odot [1] = [1]$, $[2] \odot [3] = [1]$, $[3] \odot [2] = [1]$, $[4] \odot [4] = [1]$. Therefore, $[a] \odot x = [1]$ has a solution for $[a] = [1],\ [2],\ [3],\ [4]$.

(b) In $\mathbb{Z}_4$, $[1] \odot [1] = [1]$, $[3] \odot [3] = [1]$ and $[2] \odot x \neq [1]$ for all $[x] \in \mathbb{Z}_4$. Therefore, $[a] \odot x = [1]$ has a solution for $[a] = [1],\ [3]$.

(c) In $\mathbb{Z}_3$, $[1] \odot [1] = [1]$, $[2] \odot [2] = [1]$. Therefore, $[a] \odot x = [1]$ has a solution for $[a] = [1],\ [2]$.

(d) In $\mathbb{Z}_6$, $[1] \odot [1] = [1]$, $[5] \odot [5] = [1]$. For $[a] = [2],\ [3],\ [4],\ [a] \odot x \neq [1]$ for all $[x] \in \mathbb{Z}_6$. Therefore, $[a] \odot x = [1]$ has a solution for $[a] = [1],\ [5]$.

2.3

2. Find all zero-divisors in

(a) $\mathbb{Z}_7$, (b) $\mathbb{Z}_8$, (c) $\mathbb{Z}_9$, (d) $\mathbb{Z}_{10}$

(a) In $\mathbb{Z}_7$, $[a] \odot [c] = [0] \Rightarrow 7|ac \Rightarrow 7|a$ or $7|c \Rightarrow [a]$ or $[c] = [0]$. Therefore, $\mathbb{Z}_7$ has no zero divisor.

(b) In $\mathbb{Z}_8$, $[2] \odot [4] = [4] \odot [6] = [0]$. Therefore, $[2],\ [4],\ [6]$ are zero divisors in $\mathbb{Z}_8$.

(c) In $\mathbb{Z}_9$, $[3] \odot [6] = [0]$. Therefore, $[3],\ [6]$ are zero divisors in $\mathbb{Z}_9$.

(d) In $\mathbb{Z}_{10}$, $[2] \odot [5] = [4] \odot [5] = [6] \odot [5] = [8] \odot [5] = [0]$. Therefore, $[2],\ [4],\ [5],\ [6],\ [8]$ are zero divisors in $\mathbb{Z}_{10}$.

6. If n is composite, prove that there is at least one zero-divisor in $\mathbb{Z}_n$. (See Exercise 2.)

Suppose $n > 1$ is composite. Then $n = ab$, where $1 < a,\ b < n$. Therefore, $[a],\ [b] \neq [0]$ in $\mathbb{Z}_n$ and $[a] \odot [b] = [0]$. Hence, $[a]$ and $[b]$ are zero divisors in $\mathbb{Z}_n$.

10. Prove that every nonzero element of $\mathbb{Z}_n$ is either a unit or a zero-divisor, but not both. [Hint: Exercise 9 provides the proof of "not both".]

Suppose $x \neq [0]$ in $\mathbb{Z}_n$. Then $x = [a]$ for some $1 \leqslant a < n$. Let $d = (a, n)$.
If $d = 1$, then by Theorem 2.10, $x = [a]$ is a unit in $\mathbb{Z}_n$.

If $d > 1$, let $a = a_1 d$ and $n = n_1 d$ for some $a_1,\ n_1 \in \mathbb{Z}$. Then $1 < n_1 < n$. We have $[a],\ [n_1] \neq [0]$ and $[a] \odot [n_1] = [a_1 d n_1] = [a_1 n] = [0]$. Therefore, $x = [a]$ is a zero divisor in $\mathbb{Z}_n$.

To show that x cannot be both a unit and zero-divisor, suppose x is a unit in $\mathbb{Z}_n$. Then there exists $u \in \mathbb{Z}_n$ such that $ux = [1]$. We are going to show that x cannot be a zero-divisor.

Let $y \neq [0]$ in Z_n, we have

$$u(xy) = (ux)y = [1]y = y \neq [0] \Rightarrow xy \neq [0]$$

Therefore, x cannot be a zero-divisor.

3.1

2. Let $R = \{0, e, b, c\}$ with addition and multiplication defined by the tables below. Assume associativity and distributivity and show that R is a ring with identity. Is R commutative? Is R a field?

+	0	e	b	c
0	0	e	b	c
e	e	0	c	b
b	b	c	0	e
c	c	b	e	0

·	0	e	b	c
0	0	0	0	0
e	0	e	b	c
b	0	b	b	0
c	0	c	0	c

(1) Closure for addition follows from the addition table.

(2) Under the assumption, addition is associative.

(3) Addition is commutative because the addition table is symmetric about the diagonal.

(4) From the tables, we have $a + 0 = a = 0 + a$ for every $a \in R \Rightarrow 0$ is the additive identity.

(5) $a + x = 0$ is solvable for every $a \in R$ because 0 appears in every row in the additive table.

(6) Closure for multiplication follows from the multiplication table.

(7) Under the assumption, multiplication is associative.

(8) Distributive laws hold under assumption.

(9) Multiplicationis are commutative because the multiplication table is symmetric about the diagonal.

(10) $a \cdot e = a = e \cdot a$ for every $a \in R \Rightarrow e$ is the multiplicative identity.

It follows from (1)-(10) that R is a commutative ring with identity.

(12) $b \neq 0$ but the row of b in the multiplication table does not contain e. Therefore, the equation $b \cdot x = e$ does not have a solution. Hence, R is not a field.

4. Find matrices A and C in $M(\mathbb{R})$ such that $AC = \mathbf{0}$ but $CA \neq \mathbf{0}$, where $\mathbf{0}$ is the zero matrix. [Hint: Example 6.]

Let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $C = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Then

$$AC = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ but } CA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$