Section 2.5

In this section, all variables are integers. Find a solution $x \in \mathbb{Z}, 0 \leq x < n$, for each of the congruences $ax = b \pmod{n}$ in Exercises 4, 6, 22, and 24.

Problem # 4

$2x \equiv 3 \pmod{5}$

Solution

$$\begin{aligned} 2x &\equiv 3 \pmod{5} \\ 2x &\equiv 8 \pmod{5} \\ x &\equiv 4 \pmod{5} \end{aligned} \tag{1}$$

Problem # 6

$3x \equiv 4 \pmod{13}$

Solution

$$\begin{aligned} 3x &\equiv 4 \pmod{13} \\ 3x &\equiv 30 \pmod{13} \\ x &\equiv 10 \pmod{13} \end{aligned} \tag{2}$$

Problem # 22

$57x + 7 \equiv 78 \pmod{58}$

Solution

$$\begin{aligned} 57x + 7 &\equiv 78 \pmod{58} \\ 58x + 7 &\equiv 78 + x \pmod{58} \\ 7 &\equiv 78 + x \pmod{58} \\ 7 &\equiv 20 + x \pmod{58} \\ x &\equiv -13 \pmod{58} \\ x &\equiv 45 \pmod{58} \end{aligned} \tag{3}$$

Problem # 24

$82x + 23 \equiv 2 \pmod{47}$

Solution

$$\begin{aligned}
35x + 23 &\equiv 2 \pmod{47} \\
35x + 23 &\equiv 49 \pmod{47} \\
5x + 23 &\equiv 7 \pmod{47} \\
82x &\equiv -16 \pmod{47} \\
5x &\equiv 125 \pmod{47} \\
x &\equiv 25 \pmod{47}
\end{aligned} \tag{4}$$

Use the results in Exercises 38 and 39 to determine whether there are solutions. If there are, find d incongruent solutions modulo n.

Problem # 40

$4x \equiv 18 \pmod{28}$

Solution

Let $d = (4, 28) = 4$. $b = 18$. From Exercise 38 we know that if there is a solution to $ax = b$ then $d \mid b$. $4 \nmid 18$. Therefore there are no solutions.

Problem #42

$18x \equiv 33 \pmod{15}$

Solution

Let $d = (18, 15) = 3$. $3 \mid 33$ so by Exercise we know there are solutions.

$$\begin{aligned}
18x &\equiv 33 \pmod{15} \\
18x &\equiv 18 \pmod{15} \\
x &\equiv 1 \pmod{15}
\end{aligned} \tag{5}$$

Let $x_1 = 1$, then by Exercise 39 we know the set of discongruent solutions is given by

$$x_1, x_1 + n_0, x_1 + 2n_0, \ldots x_1 + (d-1)n_0$$

For n_0 such that $dn_0 = 15$. So the solutions are $x = 1, 6, 11$.

Problem #44

$35x \equiv 10 \pmod{20}$

Solution

Let $d = (35, 20) = 5$. $5 \mid 20$ so by Exercise 38 we know there are solutions.

$$\begin{aligned} 35x &\equiv 10 \pmod{20} \\ 15x &\equiv 10 \pmod{20} \\ 15x &\equiv 30 \pmod{20} \\ x &\equiv 2 \pmod{20} \end{aligned} \tag{6}$$

Let $x_1 = 2$, then by Exercise 39 we know the set of discongruent solutions is given by

$$x_1, x_1 + n_0, x_1 + 2n_0, \ldots x_1 + (d-1)n_0$$

For n_0 such that $dn_0 = 20$. So the solutions are $x = 2, 6, 10, 14, 18$.

Section 2.6

Problem #4b

Make a multiplication table for $\mathbb{Z}_3$.

Solution

	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[0]

Problem #5

Find the multiplicative inverse of each given element.

- [7] in $\mathbb{Z}_{11}$
- [16] in $\mathbb{Z}_{27}$

Solution

b)

$$\begin{aligned} [7][x] &= [1] \\ 7x &\equiv 1 \pmod{11} \\ 7x &\equiv 56 \pmod{11} \\ x &\equiv 8 \pmod{11} \end{aligned} \tag{7}$$

So $[7]^{-1}$ in $\mathbb{Z}_{11}$ is [8].

d)

$$\begin{aligned} [16][x] &= [1] \\ 16x &\equiv 1 \pmod{27} \\ 16x &\equiv 28 \pmod{27} \\ 4x &\equiv 7 \pmod{27} \\ 4x &\equiv 88 \pmod{27} \\ x &\equiv 22 \pmod{27} \end{aligned} \tag{8}$$

So $[16]^{-1}$ in $\mathbb{Z}_{27}$ is [22].

Problem #6

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

- $\mathbb{Z}_8$
- $\mathbb{Z}_{12}$

b)

$$[1], [3], [5], [7]$$

d)

$$[1], [5], [7], [11]$$

Problem #9

Let $[a]$ be an element of $\mathbb{Z}_n$ that has a multiplicative inverse $[a]^{-1}$ in $\mathbb{Z}_n$. Prove that $[x] = [a]^{-1}[b]$ is the unique solution in $\mathbb{Z}_n$ to the equation $[a][x] = [b]$.

Solution

1. For $[x] = [a]^{-1}[b]$

$$\begin{aligned} [a][x] &= [a][a]^{-1}[b] \\ &= [1][b] \\ &= [b] \end{aligned} \tag{9}$$

So $[x] = [a]^{-1}[b]$ is a solution.
2. Assume there is another solution $[y]$. Then

$$\begin{aligned} [a][y] &= [b] \\ [a]^{-1}[a][y] &= [a]^{-1}[b] \\ [1][y] &= [a]^{-1}[b] \\ [y] &= [a]^{-1}[b] \\ [y] &= [x] \end{aligned} \tag{10}$$

Therefore [x] is a unique solution.

Problem #10

Solve each of the following equations by finding $[a]^{-1}$ and using the result in Exercise 9.

- $[8][x] = [7]$ in $\mathbb{Z}_{11}$
- $[8][x] = [11]$ in $\mathbb{Z}_{15}$

Problem #22

Let p be a prime integer. Prove that $[1]$ and $[p-1]$ are the only elements in $\mathbb{Z}_p$ that are their own multiplicative inverses.

Solution

Assume that $[a]$ is an element of $\mathbb{Z}_p$ such that $[a][a] = [1]$. Then

$$\begin{aligned} a^2 &\equiv 1 \pmod{p} \\ a^2 - 1 &\equiv 0 \pmod{p} \\ (a+1)(a-1) &\equiv 0 \pmod{p} \end{aligned} \tag{11}$$

If there were zero divisors $[x], [y]$ in $\mathbb{Z}_p$ that would imply that $xy \equiv p \mod p$. We know that this is not the case because p is prime. Therefore there are no zero divisors and either $(x-1) \equiv 0$ or $(x+1) \equiv 0$. In the first case $x \equiv 1$ and in the second $x \equiv p-1$. There are no other cases so these are the only elements in $\mathbb{Z}_p$ that are their own multiplicative inverses.

Problem #38

Let G be the set of all matrices in $M_3(R)$ that have the form

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$$

with all three numbers a, b, and c nonzero. Prove or disprove that G is a group with respect to multiplication.

Solution

Part (a)

$$\begin{bmatrix} a_1 & 0 & 0 \\ 0 & b_1 & 0 \\ 0 & 0 & c_1 \end{bmatrix}\begin{bmatrix} a_2 & 0 & 0 \\ 0 & b_2 & 0 \\ 0 & 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & 0 & 0 \\ 0 & b_1b_2 & 0 \\ 0 & 0 & c_1c_2 \end{bmatrix}$$

The products a_1a_2, b_1b_2, and c_1c_2 are not zero because none of their components are zero and there are no zero divisors in $\mathbb{Z}$. So the set G is closed under multiplication.

Part (b)

$$\left(\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}\begin{bmatrix} d & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & f \end{bmatrix}\right)\begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{bmatrix} = \begin{bmatrix} adx & 0 & 0 \\ 0 & bey & 0 \\ 0 & 0 & cfz \end{bmatrix}$$

and

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}\left(\begin{bmatrix} d & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & f \end{bmatrix}\begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{bmatrix}\right) = \begin{bmatrix} adx & 0 & 0 \\ 0 & bey & 0 \\ 0 & 0 & cfz \end{bmatrix}$$

Therefore multiplication is associative in G.

Part (c)

$$\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$$

Therefore $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is the identity element in G.

Part (d)

For all matrices A in G there exists an inverse A^{-1} so that

$$AA^{-1} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \begin{bmatrix} \frac{1}{a} & 0 & 0 \\ 0 & \frac{1}{b} & 0 \\ 0 & 0 & \frac{1}{c} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = e$$

Having satisfied the four conditions above, it can be concluded that G is a group with respect to multiplication.

Problem #39

Let G be the set of all matrices in $M_3(R)$ that have the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

for arbitrary real numbers a, b, and c. Prove or disprove that G is a group with respect to multiplication.

Solution

Part (a)

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix}$$

The real numbers are closed under addition so the resulting matrix is also a member of set G.

Part (b)

Matrix multiplication is associative. That means it is also associative for all subsets of matrices. G is such a matrix.

Part (c)

For all matrices A in G

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

So $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is the identity element in G under multiplication.

Problem #40

Prove or disprove that the set G in Exercise 38 is a group with respect to addition.

Solution

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The matrix $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ is not a member of G. So G is not closed under addition. G is not a group with respect to addition.

Problem #41

Prove or disprove that the set G in Exercise 39 is a group with respect to addition.

Solution

Part (a)

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{bmatrix}$$

The resulting matrix is not a member of G. Therefore G is not closed under addition. G is not a group with respect to addition.

Problem #42a

For an arbitrary set A, the power set $\mathcal{P}(A)$ was defined in Section 1.1 by $\mathcal{P}(A) = \{X | X \subseteq A\}$, and addition in $\mathcal{P}(A)$ was defined by

$$\begin{aligned} X + Y &= (X \cup Y) - (X \cap Y) \\ &= (X - Y) \cup (Y - X) \end{aligned} \tag{12}$$

Prove that $\mathcal{P}(A)$ is a group with respect to this operation of addition.

Solution

Part (a)

Addition as defined here can be summarized as taking every element that is a member of either X or Y but not both. Being members of the set $\mathcal{P}(A)$, every element of both X and Y must also be an element of A. This means that the result of their addition is composed entirely of elements from X and Y. The result is a subset of A, and is contained in $\mathcal{P}(A)$. So $\mathcal{P}(A)$ is closed with respect to this operation of addition.

Part (b)

$$(Y + Z) = (Y - Z) \cup (Z - Y) \tag{13}$$
$$= (Y \cap Z') \cup (Y' \cap Z) \tag{14}$$

We can then use this substitution

$$\begin{aligned}
X + (Y + Z) &= (X - (Y + Z)) \cup ((Y + Z) - X) \\
&= (X \cap (Y + Z)') \cup ((Y + Z) \cap X') \\
&= (X \cap ((Y \cap Z') \cup (Y' \cap Z))' \cup (((Y \cap Z') \cup (Y' \cap Z)) \cap X') \\
&= (X \cap ((Y \cup Z) \cap (Y' \cup Z'))' \cup (((Y \cap Z') \cup (Y' \cap Z)) \cap X') \\
&= (X \cap ((Y \cup Z)' \cup (Y' \cup Z)') \cup (((Y \cap Z') \cup (Y' \cap Z)) \cap X') \\
&= (X \cap ((Y' \cap Z') \cup (Y \cap Z)) \cup (((Y \cap Z') \cup (Y' \cap Z)) \cap X') \\
&= ((X \cap Y' \cap Z') \cup (X \cap Y \cap Z)) \cup ((X' \cap Y \cap Z') \cup (X' \cap Y' \cap Z)) \\
&= (X \cap Y' \cap Z') \cup (X \cap Y \cap Z) \cup (X' \cap Y \cap Z') \cup (X' \cap Y' \cap Z) \\
&= (X \cap Y' \cap Z') \cup (X' \cap Y \cap Z') \cup (X' \cap Y' \cap Z) \cup (X \cap Y \cap Z) \\
&= (X \cap Y' \cap Z') \cup (X' \cap Y \cap Z') \cup (((X' \cap Y') \cup (X \cap Y)) \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup (((X' \cap Y') \cup (X \cap Y)) \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup (((X \cup Y)' \cup (X' \cup Y')') \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup (((X \cup Y) \cap (X' \cup Y'))' \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup (((X \cup Y) \cap (X' \cup Y'))' \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup (((X \cap Y') \cup (X' \cap Y))' \cap Z) \\
&= (((X \cap Y') \cup (X' \cap Y)) \cap Z') \cup ((X + Y)' \cap Z) \\
&= ((X + Y) \cap Z') \cup ((X + Y)' \cap Z) \\
&= (X + Y) + Z
\end{aligned} \tag{15}$$

So this operation of addition is associative in $\mathcal{P}(A)$.

Part (c)

For any set X in $\mathcal{P}(A)$ it can be seen that $X + \emptyset = X$. Thus $\emptyset$ is the identity element for addition in $\mathcal{P}(A)$.

Part (d)

For any set X in $\mathcal{P}(A)$ it can be seen that

$$\begin{aligned} X + X &= (X \cap X') \cup (X' \cap X) \\ &= \emptyset \end{aligned} \tag{16}$$

So every set in $\mathcal{P}(A)$ is its own inverse.

Having satisfied the four necessary conditions, we can conclude that $\mathcal{P}(A)$ is a group with respect to the addition operation defined above.