UNIVERSITY OF SOUTH CAROLINA

MATH-546 Algebraic Structures I Homework 1

Problem 1:

a. Find all congruence classes $[a]_{12} \in \mathbb{Z}_{12}$ such that $[2]_{12} \cdot [a]_{12} = [0]_{12}$

b. Prove that the only congruence class $[a]_{12} \in \mathbb{Z}_{12}$ that satisfies $[5]_{12} \cdot [a]_{12} = [0]_{12}$ is $[a]_{12} = [0]_{12}$.

Answer 1:

a. $[0]_{12}, [6]_{12}$

If $[2]_{12} \cdot [a]_{12} = [0]_{12}$ then $2a \in [0]_{12} = \{0, \pm 12, \pm 24, \pm 36, \cdots\}$ and $a \in \{0, \pm 6, \pm 12, \pm 18, \cdots\} = [0]_{12} \cup [6]_{12}$ and so $a \in [0]_{12}$ or $a \in [6]_{12}$.

b. Clearly $[5]_{12} \cdot [0]_{12} = [0]_{12}$ and $[0]_{12}$ is a solution.

First we note that $\gcd(5, 12) = 1$ and therefore $[5]_{12}$ has a multiplicative inverse. To show that it is unique we look at $[5]_{12} \cdot [a]_{12} = [0]_{12}$ and multiply on the left by that inverse:

$$\begin{aligned} [5]_{12} \cdot [a]_{12} &= [0]_{12} \\ ([5]_{12})^{-1} \cdot [5]_{12} \cdot [a]_{12} &= ([5]_{12})^{-1} \cdot [0]_{12} \\ [1]_{12} \cdot [a]_{12} &= [0]_{12} \\ [a]_{12} &= [0]_{12} \end{aligned}$$

and so it must be that $a \in [0]_{12}$.

Problem 2:

Without listing all the elements of $\mathbb{Z}_{144}$, find all congruence classes $[a]_{144} \in \mathbb{Z}_{144}$ that satisfy $[3]_{144} \cdot [a]_{144} = [0]_{144}$. Justify your answer.

Answer 2:

$[0]_{144}$,$[48]_{144}$,$[96]_{144}$

If $[3]_{144} \cdot [a]_{144} = [0]_{144}$ then $3a = 144k$ for some $k \in \mathbb{Z}$ therefore $a = 144 \cdot k/3 = 48 \cdot k$. So $k \in \{0, 1, 2\}$ are different solutions and any other k is one of those solutions.

Problem 3:

For each of the congruence classes below, find the multiplicative inverse or state that the multiplicative inverse does not exist:

$[5]_{12}$; $[18]_{22}$; $[19]_{22}$

Answer 3:

$[5]_{12}$: $[5]_{12}$ (self inverse)

$[18]_{22}$: no inverse ($\gcd(18, 22) \neq 1$)

$[19]_{22}$: $[7]_{12}$ ($7 \cdot 19 = 133$, $6 \cdot 22 = 132$)

Problem 4:

Without listing all the elements of $\mathbb{Z}_{125}$, list all congruence classes $[a]_{125} \in \mathbb{Z}_{125}$ that satisfy $[a]^2 = [a]$. Justify your answer. Make sure to explain why your list is complete (there are no other congruence classes with the required property).

Answer 4:

$[0]_{125}$ and $[1]_{125}$; these work as they are solutions to $a^2 - a = 0$.

Any other solution implies there must be some $a \in \{2, 3, \cdots, 123, 124\}$ such that $a(a-1) = 125k = 5^3 k$ for some $k \in \mathbb{Z}$. But one of a or $a-1$ must be a multiple of 5 and the other can't be. $a \equiv 0 (\text{mod } 5)$ means $(a-1) \equiv 4 (\text{mod } 5)$. And $(a-1) \equiv 0 (\text{mod } 5) \Rightarrow a \equiv 1 (\text{mod } 5)$. Therefore a or $a-1$ must be a non-zero integral multiple of 125 and not in $\{2, 3, \cdots, 123, 124\}$. A contradiction.

Problem Quiz 1.1:

Prove that addition of congruence classes is well defined.

Answer Quiz 1.1:

Problem Quiz 1.2:

Prove that multiplication of congruence classes is well defined.

Answer Quiz 1.2:

Problem Quiz 1.3:

Prove that a congruence class $[a]_n \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$.

Answer Quiz 1.3:

Problem Quiz 1.4:

List all the elements of $\mathbb{Z}_{12}^*$. Verify that each element $[a] \in \mathbb{Z}_{12}^*$ satisfies $[a]^2 = [1]$.

Answer Quiz 1.4:

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ (i.e. all $p \in \mathbb{Z}_{12}$ relatively prime to 12.

$$[1][1] = [1 \cdot 1] = [1]$$

$$[5] = [5 \cdot 5] = [25] = [2 \cdot 12 + 1] = [1]$$

$$[7] = [7 \cdot 7] = [49] = [4 \cdot 12 + 1] = [1]$$

$$[11] = [-1][-1] = [1]$$