MAT 108 Homework 19 Solutions

Problems are from A Transition to Advanced Mathematics 8th edition by Smith, Eggen, and Andre.

Section 3.4 #1hjkl, 2hjkl, 3, 4, 5, 12abc

1. Perform each of these calculations in $\mathbb{Z}_7$

(h) $(4+5)\cdot(5+6)$

Solution: $(4+5)\cdot(5+6) = 2\cdot 4 = 1 \bmod 7$

(j) 5^{23}

Solution: $5^{23} = 5^{18}\cdot 5^5 = 1\cdot(-2^5) = -32 = 3 \bmod 7$

Note: you can check and verify that $5^{18} = 5^{6^3} = 1 \bmod 7$.

(k) 4^{44}

Solution: $4^{44} = 4^2 = 2 \bmod 7$

(l) 2^{26}

Solution: $2^{26} = 2^2 = 4 \bmod 7$

2. Repeat Exercise 1 with calculations in $\mathbb{Z}_9$.

(h) $(4+5)\cdot(5+6)$

Solution: $(4+5)\cdot(5+6) = 0\cdot 2 = 0 \bmod 9$

(j) 5^{23}

Solution: We compute

- $5^2 = 7 \bmod 9$
- $5^3 = 8 \bmod 9$
- $5^4 = 4 \bmod 9$
- $5^5 = 2 \bmod 9$
- $5^6 = 1 \bmod 9$

So we have $5^{23} = 5^{18}\cdot 5^5 = 2 \bmod 9$.

(k) 4^{44}

Solution: We compute

- $4^2 = 7 \bmod 9$
- $4^3 = 1 \bmod 9$

So $4^{44} = 4^{42}\cdot 4^2 = 7 \bmod 9$

(l) 2^{26}

Solution: We compute We compute

- $2^2 = 4 \bmod 9$
- $2^3 = 8 \bmod 9$
- $2^4 = 7 \bmod 9$
- $2^5 = 5 \bmod 9$
- $2^6 = 1 \bmod 9$

So $2^{26} = 2^{24} \cdot 2^2 = 4 \bmod 9$.

3. Prove Theorem 3.4.2: If $a, b, c,$ and d are integers, $a = c \bmod m$, and $b = d \bmod m$, then $a \cdot b = c \cdot d \bmod m$.

Solution: Let $a, b, c, d \in \mathbb{Z}$ and suppose that $a = c \bmod m$, and $b = d \bmod m$. Then, by definition, we have $m|a - c$ and $m|b - d$. In order to conclude $a \cdot b = c \cdot d \bmod m$, we must show $m|ab - cd$. We first rewrite $ab - cd$ as

$$ab - cd = ab - bc + bc - cd = b(a - c) + c(b - d).$$

Since m divides both $a - c$ and $b - d$, it follows that m divides $b(a - c) + c(b - d) = ab - cd$. Thus, $ab = cd \bmod m$.

4. (a) For $\overline{x}, \overline{y}$ in $\mathbb{Z}_m$, give a definition of subtraction: $\overline{x} - \overline{y}$.

Solution: For $\overline{x}, \overline{y}$ in $\mathbb{Z}_m$ we define $\overline{x} - \overline{y} := \overline{x - y}$. Note that this matches our definition of addition of negative representatives of equivalence classes.

(b) Prove that subtraction is well defined.

Solution: Let $\overline{x}, \overline{y}, \overline{c}, \overline{d} \in \mathbb{Z}_m$ with $\overline{x} = \overline{c}, \overline{y} = \overline{d} \bmod m$. We wish to show that $\overline{x} - \overline{y} = \overline{c} - \overline{d}$. Since $\overline{x}$ is congruent to $\overline{c}$ and y is congruent to $\overline{d}$ in $\mathbb{Z}_m$, we know that $m|x - c$ and $m|y - d$. Therefore, $m|(x - c) - (y - d)$. But

$$(x - c) - (y - d) = (x - y) - (c - d),$$

so $m|(x - y) - (c - d)$, which tells us that $\overline{x} - \overline{y} = \overline{c} - \overline{d} \bmod m$.

(c) Find the results of

(i) 8-6 in $\mathbb{Z}_9$
(ii) 5-8 in $\mathbb{Z}_9$
(iii) 3-5 in $\mathbb{Z}_7$
(iv) 1-4 in $\mathbb{Z}_7$.

Solution:

(i) $8 - 6 = 2 \bmod 9$
(ii) $5 - 8 = 6 \bmod 9$
(iii) $3 - 5 = 5 \bmod 7$
(iv) $1 - 4 = 4 \bmod 7$

5. Suppose we try to define $\leq$ on $\mathbb{Z}_m$ by saying that for $\overline{x}, \overline{y}$ in $\mathbb{Z}_m$, $\overline{x} \leq \overline{y}$ if $x \leq y$. What is wrong with this definition.

Solution: This relation is not well defined on $\mathbb{Z}_m$. For example, we can take $m = 4$. Then $2, -2 \in \overline{2}$ but we have $-2 < 1$ and $2 > 1$.

12. 'Grade' the following proofs:

(a) (see textbook for proof)

Solution: C. The claim is true, but the proof has a lot of gaps and does not use the definitions of congruence to justify their assertions.

(b) (see textbook for proof)

Solution: F. The claim is false and the last step in the proof is not true in $\mathbb{Z}_8$.

(c) (see textbook for proof)

Solution: A. Proof is good