Math 446 - Homework # 4

1. Are the following statements true or false?

   (a) $3 \equiv 5 (\text{mod } 2)$
   Solution: $3 - 5 = -2 = 2 \cdot (-1)$ is divisible by 2. Hence $2 \equiv 5 (\text{mod } 2)$.

   (b) $11 \equiv -5 (\text{mod } 5)$
   Solution: $11 - (-5) = 16$ is NOT divisible by 5. Hence $11 \not\equiv -5 (\text{mod } 5)$.

   (c) $-31 \not\equiv 10 (\text{mod } 3)$
   Solution: $-31 - 10 = -41$ is NOT divisible by 3. Hence $-31 \not\equiv 10 (\text{mod } 3)$.

   (d) $100 \equiv 12 (\text{mod } 4)$
   Solution: $100 - 12 = 88 = 4 \cdot 44$ is divisible by 4. Hence $100 \equiv 12 (\text{mod } 4)$.

2. Prove the following: If x, y, z, a, b, n are integers with $n \geq 2$ then the following are true:

   (a) $x \equiv x (\text{mod } n)$
   Solution: Note that $x - x = 0 = n \cdot 0$. Hence n divides $x - x$. Thus $x \equiv x (\text{mod } n)$.

   (b) If $x \equiv y (\text{mod } n)$, then and $y \equiv x (\text{mod } n)$.
   Solution: Since $x \equiv y (\text{mod } n)$ we have that $ns = x - y$ for some integer s. Multiplying by -1 gives $n(-s) = y - x$. Hence n divides $y - x$. Thus $y \equiv x (\text{mod } n)$.

   (c) If $x \equiv y (\text{mod } n)$ and $y \equiv z (\text{mod } n)$, then $x \equiv z (\text{mod } n)$.
   Solution: Since $x \equiv y (\text{mod } n)$ we have that $ns = x - y$ for some integer s. Since $y \equiv z (\text{mod } n)$ we have that $nt = y - z$ for some integer t. Adding the equations $ns = x - y$ and $nt = y - z$ gives the equation $n(s + t) = x - z$. Hence n divides $x - z$. Therefore $x \equiv z (\text{mod } n)$.

   (d) If $a \equiv b (\text{mod } n)$ and $x \equiv y (\text{mod } n)$, then $a + x \equiv b + y (\text{mod } n)$.

Solution: Since $a \equiv b(\text{mod } n)$ we have that $ns = a - b$ for some integer s. Since $x \equiv y(\text{mod } n)$ we have that $nt = x - y$ for some integer t. Therefore

$$(a + x) - (b + y) = (a - b) + (x - y) = ns + nt = n(s + t).$$

Therefore n divides $(a+x)-(b+y)$. Hence $a+x \equiv b+y(\text{mod } n)$.

(e) If $a \equiv b(\text{mod } n)$ and $x \equiv y(\text{mod } n)$, then $ax \equiv by(\text{mod } n)$.

Solution: Since $a \equiv b(\text{mod } n)$ we have that $ns = a - b$ for some integer s. Since $x \equiv y(\text{mod } n)$ we have that $nt = x - y$ for some integer t. Therefore

$$ax = (b + ns)(y + nt) = by + nbt + nsy + n^2st.$$

So,

$$ax - by = n(bt + sy + nst).$$

Therefore n divides $ax - by$. Hence $ax \equiv by(\text{mod } n)$.

(f) We have that $x \equiv y(\text{mod } n)$ if and only if $x = y + kn$ for some integer k.

Solution: Suppose that $x \equiv y(\text{mod } n)$. Then n divides $x - y$. Hence $nk = x - y$ for some integer k. Thus, $x = y + nk$.

Conversely suppose that $x = y + nk$. Then $x - y = nk$. Hence n divides $x - y$. Thus $x \equiv y(\text{mod } n)$.

3. In $\mathbb{Z}_4$, list ten elements from each of the following equivalence classes: $\overline{0}$, $\overline{-3}$, $\overline{2}$, $\overline{5}$.

Solution:

$$\begin{aligned}
\overline{0} &= \{\ldots, -20, -16, -12, -8, -4, 0, 4, 8, 12, 16, 20, \ldots\} \\
\overline{-3} &= \{\ldots, -23, -19, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\} \\
\overline{2} &= \{\ldots, -18, -14, -10, -6, -2, 2, 6, 10, 14, 18, 22, \ldots\} \\
\overline{5} &= \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, 21, 25, \ldots\}
\end{aligned}$$

4. Answer the following questions.

(a) Is $\overline{0} = \overline{8}$ in $\mathbb{Z}_4$?

Solution: Note that $0 - 8 = -8 = 4 \cdot (-2)$. Hence 4 divides $0 - 8$. Thus $0 \equiv 8(\text{mod } 4)$. Therefore $\overline{0} = \overline{8}$.

(b) Is $\overline{-10} = \overline{-2}$ in $\mathbb{Z}_5$?

Solution: Note that $-10 - (-2) = -8$ which is not divisible by 5. Thus $-10 \not\equiv -2 (\text{mod } 5)$. Therefore $\overline{-10} \neq \overline{-2}$.

(c) Is $\overline{1} = \overline{13}$ in $\mathbb{Z}_6$?

Solution: Note that $1 - 13 = -12 = 6 \cdot (-2)$. Hence 6 divides $1 - 13$. Thus $1 \equiv 13 (\text{mod } 6)$. Therefore $\overline{1} = \overline{13}$ in $\mathbb{Z}_6$.

(d) Is $\overline{2} = \overline{52}$ in $\mathbb{Z}_4$?

Solution: Note that $2 - 52 = -50$ which is not divisible by 4. Therefore $\overline{2} \neq \overline{52}$ in $\mathbb{Z}_4$.

(e) Is $\overline{-5} = \overline{19}$ in $\mathbb{Z}_4$?

Solution: Note that $-5 - 19 = -24 = 4 \cdot (-6)$ is divisible by 4. Therefore $\overline{-5} = \overline{19}$ in $\mathbb{Z}_4$.

5. Answer the following questions where the elements are from $\mathbb{Z}_8$.

(a) Is $\overline{0} = \overline{12}$?

Solution: No, because $0 - 12 = -12$ is not a multiple of 8.

(b) Is $\overline{-2} = \overline{14}$?

Solution: Yes, because $-2 - 14 = -16$ is a multiple of 8.

(c) Is $\overline{-51} = \overline{-109}$?

Solution: No, because $-51 - (-109) = 58$ is not a multiple of 8.

(d) Is $\overline{3} = \overline{43}$?

Solution: Yes, because $3 - 43 = -40$ is a multiple of 8.

6. Consider $\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Calculate the following. For each answer $\overline{x}$ that you calculate, reduce it so that $0 \leq x \leq 6$.

(a) $\overline{2} + \overline{6}$

Solution: $\overline{2} + \overline{6} = \overline{8} = \overline{1}$.

(b) $\overline{3} + \overline{4}$

Solution: $\overline{3} + \overline{4} = \overline{7} = \overline{0}$.

(c) $\overline{1473}$

Solution: To reduce 1473 number modulo 7 we use the division algorithm. Dividing 7 into 1473 we get that $1473 = 210 \cdot 7 + 3$. Now we use the fact that $\overline{7} = \overline{0}$ in $\mathbb{Z}_7$ to get that

$$\overline{1473} = \overline{210} \cdot \overline{7} + \overline{3} = \overline{210} \cdot \overline{0} + \overline{3} = \overline{3}$$

(d) $\overline{3} \cdot \overline{5}$

Solution: $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$.

(e) $\overline{2} \cdot \overline{3} + \overline{4} \cdot \overline{6}$

Solution: $\overline{2} \cdot \overline{3} + \overline{4} \cdot \overline{6} = \overline{30} = \overline{2}$.

(f) $\overline{5} \cdot \overline{2} + \overline{1} + \overline{2} \cdot \overline{4} \cdot \overline{6}$

Solution: $\overline{5} \cdot \overline{2} + \overline{1} + \overline{2} \cdot \overline{4} \cdot \overline{6} = \overline{10} + \overline{1} + \overline{48} = \overline{3} + \overline{1} + \overline{6} = \overline{10} = \overline{3}$.

7. Consider $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Calculate the following. For each answer $\overline{x}$ that you calculate, reduce it so that $0 \leq x \leq 3$.

(a) $\overline{2} + \overline{3}$

Solution: $\overline{2} + \overline{3} = \overline{5} = \overline{1}$.

(b) $\overline{1} + \overline{3}$

Solution: $\overline{1} + \overline{3} = \overline{4} = \overline{0}$.

(c) 4630

Solution: To reduce 4630 number modulo 4 we use the division algorithm. Dividing 4 into 4630 we get that $4630 = 1157 \cdot 4 + 2$. Now we use the fact that $\overline{4} = \overline{0}$ in $\mathbb{Z}_4$ to get that

$$\overline{4630} = \overline{1157} \cdot \overline{4} + \overline{2} = \overline{1157} \cdot \overline{0} + \overline{2} = \overline{2}$$

(d) $\overline{3} \cdot \overline{2}$

Solution: $\overline{3} \cdot \overline{2} = \overline{6} = \overline{2}$.

(e) $\overline{2} \cdot \overline{2} + \overline{3} \cdot \overline{3}$

Solution: $\overline{2} \cdot \overline{2} + \overline{3} \cdot \overline{3} = \overline{4} + \overline{9} = \overline{0} + \overline{1} = \overline{1}$.

(f) $\overline{3} \cdot \overline{2} + \overline{1} + \overline{2} + \overline{2} \cdot \overline{2} \cdot \overline{2}$

Solution: $\overline{3} \cdot \overline{2} + \overline{1} + \overline{2} + \overline{2} \cdot \overline{2} \cdot \overline{2} = \overline{6} + \overline{3} + \overline{8} = \overline{17} = \overline{1}$.

8. Suppose that x is an odd integer.

(a) Prove that $\overline{x} = \overline{1}$ or $\overline{x} = \overline{3}$ in $\mathbb{Z}_4$.

Solution: Let x be an integer. Dividing x by 4 we have that $x = 4q + r$ where q and r are integers and $0 \leq r < 4$.

Any integer of the form $4q + 0 = 2(2q)$ or $4q + 2 = 2(2q + 1)$ is an even integer. Since x is assumed to be odd we must have that either $x = 4q+1$ or $x = 4q+3$. So, $x-1 = 4q$ or $x-3 = 4q$. Thus, either $x \equiv 1 (\text{mod } 4)$ or $x \equiv 3 (\text{mod } 4)$. Therefore either $\overline{x} = \overline{1}$ or $\overline{x} = \overline{3}$.

(b) Prove that $\overline{x}^2 = \overline{1}$ in $\mathbb{Z}_4$.

Solution: Since x is odd, by exercise (8a) we have that either $\overline{x} = \overline{1}$ or $\overline{x} = \overline{3}$. Thus either $\overline{x}^2 = \overline{1}$ or $\overline{x}^2 = \overline{3}^2 = \overline{9} = \overline{1}$.

9. (a) Let p be a prime and x and y be integers. Suppose that $\overline{xy} = \overline{0}$ in $\mathbb{Z}_p$. Prove that either $\overline{x} = \overline{0}$ or $\overline{y} = \overline{0}$.

   Solution: Suppose that $\overline{xy} = \overline{0}$ in $\mathbb{Z}_p$. Then $xy \equiv 0(\text{mod } p)$. Thus p divides xy. Since p is a prime we must have that either $p|x$ or $p|y$. Thus either $x \equiv 0(\text{mod } p)$ or $y \equiv 0(\text{mod } p)$. So either $\overline{x} = \overline{0}$ or $\overline{y} = \overline{0}$.

   (b) Give an example where n is not prime with $\overline{xy} = \overline{0}$ but $\overline{x} \neq \overline{0}$ and $\overline{y} \neq \overline{0}$.

   Solution: In $\mathbb{Z}_6$ we have that $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$ but $\overline{2} \neq \overline{0}$ and $\overline{3} \neq \overline{0}$.

10. Let p be a prime. Suppose that $x^2 \equiv y^2(\text{mod } p)$. Prove that either $p|(x+y)$ or $p|(x-y)$.

    Solution: Suppose that $x^2 \equiv y^2(\text{mod } p)$. Then p divides $x^2 - y^2$. Hence p divides the product $(x-y)(x+y)$. Since p is prime, either $p|(x-y)$ or $p|(x+y)$.

11. Let n be an integer with $n \geq 2$. Let $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$. Prove the following. (You will need to use the corresponding properties of the integers.)

    (a) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$.

    Solution: Since a and b are integers we have that $a \cdot b = b \cdot a$. Thus
    $$\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{b \cdot a} = \overline{b} \cdot \overline{a}.$$

    (b) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$.

    Solution: Since a and b are integers we have that $a + b = b + a$. Thus
    $$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}.$$

    (c) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

    Solution: Since a, b, c are integers we have that $a \cdot (b + c) = a \cdot b + a \cdot c$. Thus
    $$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b + c} = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}.$$

(d) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

Solution: Since a, b, c are integers we have that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Thus

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{b \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}.$$

(e) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$.

Solution: Since a, b, c are integers we have that $a + (b + c) = (a + b) + c$. Thus

$$\overline{a}+(\overline{b}+\overline{c}) = \overline{a}+\overline{b+c} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{a + b}+\overline{c} = (\overline{a}+\overline{b})+\overline{c}.$$

12. Prove that 4 does not divide $n^2 + 2$ for any integer n.

Solution: We prove this by contradiction. Suppose that there exists an integer n where 4 divides $n^2 + 2$. Then $n^2 + 2 = 4k$ for some integer k. Therefore

$$\overline{n^2 + 2} = \overline{4k}$$

in $\mathbb{Z}_4$. Hence

$$\overline{n}^2 + \overline{2} = \overline{4} \cdot \overline{k}$$

in $\mathbb{Z}_4$. Since $\overline{4} = \overline{0}$ we have that

$$\overline{n}^2 + \overline{2} = \overline{0}.$$

Adding $\overline{2}$ to both sides and using the fact that $\overline{2} + \overline{2} = \overline{0}$ we have that

$$\overline{n}^2 = \overline{2}$$

in $\mathbb{Z}_4$. However, this equation is not possible in $\mathbb{Z}_4$ since

$$\begin{array}{rcl} \overline{0}^2 & = & \overline{0} \\ \overline{1}^2 & = & \overline{1} \\ \overline{2}^2 & = & \overline{0} \\ \overline{3}^2 & = & \overline{1}. \end{array}$$

13. Prove that $15x^2 - 7y^2 = 1$ has no integer solutions.

Solution: We prove this by contradiction. Suppose that x and y are integers with $15x^2 - 7y^2 = 1$. Then

$$\overline{15}\overline{x}^2 + \overline{-7}\overline{y}^2 = \overline{1}$$

in $\mathbb{Z}_3$. Since $\overline{15} = \overline{0}$ and $\overline{-7} = \overline{2}$ in $\mathbb{Z}_3$ we have that

$$\overline{2}\overline{y}^2 = \overline{1}.$$

Multiplying by $\overline{2}$ on both sides and using the fact that $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$ we have that

$$\overline{y}^2 = \overline{2}.$$

However this equation has no solutions in $\mathbb{Z}_3$ since

$$\begin{aligned} \overline{0}^2 &= \overline{0} \\ \overline{1}^2 &= \overline{1} \\ \overline{2}^2 &= \overline{1}. \end{aligned}$$

14. Prove that $x^2 - 5y^2 = 2$ has no integer solutions.

    Solution: We prove this by contradiction. Suppose that x and y are integers with $x^2 - 5y^2 = 2$. Then in $\mathbb{Z}_5$ we have that

    $$\overline{x}^2 + \overline{-5} \cdot \overline{y}^2 = \overline{2}.$$

    Since $\overline{-5} = \overline{0}$ in $\mathbb{Z}_5$ we have that

    $$\overline{x}^2 = \overline{2}.$$

    However, this equation has no solutions in $\mathbb{Z}_5$ since

    $$\begin{aligned} \overline{0}^2 &= \overline{0} \\ \overline{1}^2 &= \overline{1} \\ \overline{2}^2 &= \overline{4} \\ \overline{3}^2 &= \overline{4} \\ \overline{4}^2 &= \overline{1}. \end{aligned}$$

15. Let $n, x, y \in \mathbb{Z}$ with $n \geq 2$. Consider the elements $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_n$. Prove:

    (a) $\overline{x} = \overline{y}$ if and only if $x \equiv y (\text{mod } n)$.
    Solution: Suppose that $\overline{x} = \overline{y}$. By definition

    $$\overline{x} = \{t \in \mathbb{Z} \mid t \equiv x (\text{mod } n)\}.$$

Since $x \equiv x(\text{mod } n)$ we have that $x \in \overline{x}$. Therefore, $x \in \overline{y}$ because $\overline{x} = \overline{y}$. By definition

$$\overline{y} = \{z \in \mathbb{Z} \mid z \equiv y(\text{mod } n)\}.$$

Hence $x \equiv y(\text{mod } n)$.

Conversely, suppose that $x \equiv y(\text{mod } n)$. We now show that $\overline{x} = \overline{y}$. Let us begin by showing that $\overline{x} \subseteq \overline{y}$. Let $z \in \overline{x}$. By definition

$$\overline{x} = \{t \in \mathbb{Z} \mid t \equiv x(\text{mod } n)\}.$$

Thus, $z \equiv x(\text{mod } n)$. Since $z \equiv x(\text{mod } n)$ and $x \equiv y(\text{mod } n)$ we have that $z \equiv y(\text{mod } n)$. Thus $z \in \overline{y}$. Therefore $\overline{x} \subseteq \overline{y}$. A similar argument shows that $\overline{y} \subseteq \overline{x}$. Therefore, $\overline{x} = \overline{y}$.

(b) Either $\overline{x} \cap \overline{y} = \emptyset$ or $\overline{x} = \overline{y}$.

Solution: If $\overline{x} \cap \overline{y} = \emptyset$, then we are done. Suppose that $\overline{x} \cap \overline{y} \neq \emptyset$. Then there exists $z \in \overline{x} \cap \overline{y}$. Since $z \in \overline{x}$ we have that $z \equiv x(\text{mod } n)$. Since $z \in \overline{y}$ we have that $z \equiv y(\text{mod } n)$. Therefore, $x \equiv z(\text{mod } n)$ and $z \equiv y(\text{mod } n)$ which gives us that $x \equiv y(\text{mod } n)$. By exercise (15a) we have that $\overline{x} = \overline{y}$.