Homework 8 - Solutions

MAT 200, Instructor: Alena Erchenko

1. *Solution.* (a) Reflexive: We showed in class that for any $a \in \mathbb{Z}$ we have $a^2 \geq 0$. Thus, aRa for any $a \in \mathbb{Z}$.

   Symmetric: From the commutativity of the multiplication of integers, we have that for any $a, b \in \mathbb{Z}$ if $ab \geq 0$ then $ba \geq 0$. Thus, if aRb then bRa.

   Not Transitive: Let $a = 1$, $b = 0$, and $c = -1$. Then, $ab = 0$ and $bc = 0$, so aRb and bRc, but $ac = -1 < 0$, so a is not related to c.

   Not Equivalence: Since the relation is not transitive, it is not an equivalence relation.

   (b) Reflexive: We have for any $A \in \mathcal{P}(Y)$ that $A \subset A$, so ARA.

   Not Symmetric: Let $A = \emptyset$ and $B = Y$, then $A \subset B$ but $B \not\subset A$ because $B \neq \emptyset$. Thus, A is related to B, but B is not related to A.

   Transitive: Let $A, B, C \in \mathcal{P}(Y)$. Assume that $A \subset B$, $B \subset C$. Then, for any $a \in A$ we have that $a \in B$ because $A \subset B$, so $a \in C$ because $B \subset C$. Thus, $A \subset C$. As a result, if ARB and BRC, then ARC.

   Not Equivalence: Since the relation is not symmetric, it is not an equivalence relation.

   (c) Not reflexive: Let $n = 2 \in \mathbb{N}$. Then, $n + n = 4$ which is not prime, so n is not related to n.

   Symmetric: From the commutativity of the summation on $\mathbb{N}$, we have that for any $n, m \in \mathbb{N}$ if $n + m$ is a prime then $m + n$ is a prime. Thus, if nRm then mRn.

   Not Transitive: Let $n = 2$, $m = 3$, and $l = 4$. Then, $n + m = 5$ is a prime, $m + l = 7$ is a prime, but $n + l = 6 = 2 \cdot 3$ is not a prime. Thus, for chosen n, m, l we have that nRm and mRl, but n is not related to l.

   Not Equivalence: Since the relation is not reflexive, it is not an equivalence relation.

   $\square$

2. *Proof.* We show that the relation is reflexive, symmetric, and transitive, what implies that it is an equivalence relation.

   Reflexive: For any $x \in \mathbb{Z}$ we have that $x \equiv x \pmod{n}$ because $x - x = 0$ and n divides 0.

   Symmetric: Assume that $x, y \in \mathbb{Z}$ and $x \equiv y \pmod{n}$. Then, n divides $(x - y)$. By Exercise 4 in Homework 1, we obtain that n divides $-(x - y)$, i.e., n divides $(y - x)$, so $y \equiv x \pmod{n}$.

   Transitive: Let $x, y, z \in \mathbb{Z}$. Assume that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$. We want to show that $x \equiv z \pmod{n}$. Since $x \equiv y \pmod{n}$, we have that n divides $x - y$, so $x - y = nk$ for some $k \in \mathbb{Z}$, so $x = y + nk$. Since $y \equiv z \pmod{n}$, we have that n divides $y - z$, so $y - z = nl$ for some $l \in \mathbb{Z}$, so $y = z + nl$. Therefore, $x = z + nl + nk = z + n(l + k)$, so $x - z = n(l + k)$ where $(l + k) \in \mathbb{Z}$. Thus, n divides $x - z$, so $x \equiv z \pmod{n}$. $\square$

3. *Proof.* Assume that $a \equiv b \pmod{n}$. Then, n divides $(a-b)$, so $(a-b) = nk$ for some $k \in \mathbb{Z}$. We have $ca - cb = c(a-b) = cnk = n(ck)$ where $ck \in \mathbb{Z}$ because $c, k \in \mathbb{Z}$, so n divides $(ca - cb)$, i.e., $ca \equiv cb \pmod{n}$. $\square$

4. *Proof.* Since $a_1 \equiv b_1 \pmod{n}$, we have n divides $a_1 - b_1$, so $a_1 - b_1 = nk$ for some $k \in \mathbb{Z}$. Since $a_2 \equiv b_2 \pmod{n}$, we have n divides $a_2 - b_2$, so $a_2 - b_2 = nl$ for some $l \in \mathbb{Z}$. We have

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = nk - nl = n(k - l)$$

where $(k - l) \in \mathbb{Z}$, so n divides $(a_1 + a_2) - (b_1 + b_2)$, i.e., $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$. $\square$

5. *Solution.* (a) It is true. We can prove by induction that $9^n \equiv 1 \pmod{8}$ if $n \in \mathbb{N}$, in particular, $9^{73} \equiv 1 \pmod{8}$.

   Base case: $9^1 = 9$ and $9 \equiv 1 \pmod{8}$ because $9 - 1 = 8$ and 8 divides 8.

   Inductive step: Assume $9^n \equiv 1 \pmod{8}$. We show that $9^{n+1} \equiv 1 \pmod{8}$. We have $9^{n+1} = 9^n \cdot 9$, $9^n \equiv 1 \pmod{8}$ by inductive hypothesis, and $9 \equiv 1 \pmod{8}$ by base case, so $9^{n+1} \equiv 1 \pmod{9}$.

   Therefore, by the principle of mathematical induction, we have that $9^n \equiv 1 \pmod{8}$ for all $n \in \mathbb{N}$.

   (b) It is true. We have $14^{198} = 7 \cdot 7^{197} \cdot 2^{198}$, so $14^{198} \equiv 0 \pmod{7}$. Also, $-2 \equiv 5 \pmod{7}$ because $5 - (-2) = 7$ and 7 divides 7. Therefore, $14^{198} - 2 \equiv 0 + 5 \pmod{7}$, so $14^{198} - 2 \equiv 5 \pmod{7}$.

   $\square$

6. We have

$$\begin{aligned} n = a_3a_2a_1a_0 &= a_3 \cdot 1000 + a_2 \cdot 100 + a_1 \cdot 10 + a_0 \\ &= a_3(1001 - 1) + a_2(99 + 1) + a_1(11 - 1) + a_0 \\ &= (1001a_3 + 99a_2 + 11a_1) + (a_0 - a_1 + a_2 - a_3) \\ &= 11(91a_3 + 9a_2 + a_1) + (a_0 - a_1 + a_2 - a_3). \end{aligned}$$

Thus, since $(91a_3 + 9a_2 + a_1) \in \mathbb{Z}$, we obtain that

$$n \equiv a_0 - a_1 + a_2 - a_3 \pmod{11}.$$

Moreover, 11 divides n if and only if $n \equiv 0 \pmod{11}$ (using the theorem in one of the classes). Using transitivity of the congruence modulo 11, we have that $n \equiv 0 \pmod{11}$ if and only if $a_0 - a_1 + a_2 - a_3 \equiv 0 \pmod{11}$ which is if and only if 11 divides $a_0 - a_1 + a_2 - a_3$.