# Homework 1 Solutions

MTH 310

3. - Let $x \in A \cup (B \cup C)$. Then either $x \in A$ or $x \in B \cup C$. In the first case, we see that since $x \in A$, it follows that $x$ is also an element of $A \cup B$ and $A \cup C$, so $x \in (A \cup B) \cup (A \cup C)$. In the second case, ic $x \in B \cup C$, then either $x \in B$ or $x \in C$. If $x \in B$, $x \in A \cup B$; similarly if $x \in C$, $x \in A \cup C$. So $x$ is an element of at least one of $A \cup B$ and $A \cup C$, implying that $x \in (A \cup B) \cup (A \cup C)$. As $x$ as arbitary, $A \cup (B \cup C) \subseteq (A \cup B) \cup (A \cup C)$.

     Conversely suppose $x \in (A \cup B) \cup (A \cup C)$. Then either $x \in A \cup B$ or $x \in A \cup C$. There are two possibilities, $x \in A$ and $x \notin A$. If $x \in A$, then $x \in A \cup (B \cup C)$. If $x \notin A$, then if $x \in A \cup B$, we must have $x \in B$, and if $x \in A \cup C$, we must have $x \in C$. So we perceive that $x$ is an element of at least one of $B$ and $C$, implying that $x \in B \cup C$. Hence $x \in A \cup (B \cup C)$. Since $x$ was arbitrary, $(A \cup B) \cup (A \cup C) \subseteq A \cup (B \cup C)$. We conclude that the two sets are equal.

   - Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$, implying that either $x \in B$ or $x \in C$. If $x \in B$, then $x \in A \cap B$; if $x \in C$, then $x \in A \cap C$. In either eventuality $x \in (A \cap B) \cup (A \cap C)$. Since $x$ was arbitrary, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

     Conversely let $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. If $x \in A \cap B$, then $x \in A$ and $x \in B$, implying that in particular $x \in A$ and $x \in B \cup C$, so $x \in A \cap (B \cup C)$. Similarly if $x \in A \cap C$ then $x \in A \cap (B \cup C)$. Since $x$ was arbitrary, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. We conclude that the two sets are equal.

4. Let

$$A = \{2x : x \in \mathbb{Z}\} \qquad A' = \{x \in \mathbb{Z} : 4|x^2\} \qquad A'' = \{x \in \mathbb{Z} : (-1)^x = 1\}$$

First we show $A = A'$. Now if $y \in A$, $y = 2x$ for some integer $x$, so $y^2 = 4x^2$ is divisible by 4. Hence $y \in A'$. So $A \subset A'$. In the other direction, suppose $y \notin A$. Then by the Division Algorithm, $y = 2k + 1$ for some $k \in \mathbb{Z}$. Then $y^2 = 4k^2 + 4k + 1$, which is certainly not divisible by 4. So any element which is not in $A$ is also not in $A'$, implying that $A' \subset A$. Hence $A = A'$.

Next we show that $A = A''$. First, if $y \in A$, then $y = 2x$ for some integer $x$, so $(-1)^y = (-1)^{2x} = ((-1)^2)^x = 1^x = 1$, so $y \in A'$. Hence $A \subset A'$.

Conversely if $y$ is not in $A$, then as previously $y = 2k + 1$ for some integer $k$, and $(-1)^y = (-1)^{2k+1} = (-1)^{2k}(-1) = (1)(-1) = -1$, so $y$ is not in $A''$. Hence $A'' \subset A$. So $A = A''$.

It follows that $A = A' = A''$.

5. (a) $241 = 17(13) + 3$.
   (b) $-241 = 17(-14) + 14$.
   (c) $0 = 17(0) + 0$.

6. We observe that by the Division Algorithm any integer $a$ can be written as on of $3q$, $3q + 1$, or $3q + 2$. We look at each of these cases separately.

$$(3q)^2 = 9q^2 = 3(3q^2) = 3k$$

$$(3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1 = 3k + 1$$

$$(3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1 = 3k + 1$$

So we see that any integer square $a^2$ may be written in the form $3k$ or $3k + 1$.

7. First, suppose $a$ and $c$ leave the same remainder when divided by $n$. Then we have $a = nq_1 + r$ and $c = nq_2 + r$. In particular $a - c = nq_1 + r - (nq_2 + r) = n(q_1 - q_2)$. So $n|(a - c)$.

   Conversely, suppose that $n|(a - c)$. Let $a - c = nk$. Use the Division Algorithm to write $a = nq_1 + r_1$ and $c = nq_2 + r_2$ for $0 \leq r_1, r_2 < n$. Then we see that

$$\begin{aligned} nk &= (nq_1 + r_1) - (nq_2 - r_2) \\ nk &= n(q_1 - q_2) + (r_1 - r_2) \\ n(k + q_2 - q_1) &= r_1 - r_2 \end{aligned}$$

   But $0 \leq r_1 < n$ and $-n < -r_2 \leq 0$, so in fact $-n < r_1 - r_2 < n$. But the only integer divisible by $n$ in that range is 0. So $r_1 = r_2$ as desired.

8. We prove an extended version of the Division Algorithm. If $b > 0$, this is just the actual Division Algorithm. So let $b < 0$. Given $a$, use the ordinary Division Algorithm to divide $-a$ by $|b|$, obtaining $-a = |b|q + r$ for some $0 \leq r < 0$. Multiplying by $-1$ we see that $a = bq - r$. If $r = 0$ we are done. Otherwise we observe that $a = bq - r = b(q + 1) + (|b| - r)$. We observe that since $b < -r \leq 0$, we have $|b| + b = 0 < |b| - r < |b|$. So setting $q' = q + 1$, we have written $a = bq' + r$ for $0 \leq r < |b|$ as desired. Uniqueness follows by the proof of uniqueness in the Division Algorithm (which did not importantly use the sign of $b$).