Homework 6 - Solutions

MAT 200, Instructor: Alena Erchenko

1. *Proof.* If $x = 0$, then take $q = 0$ and $r = 0$.

   If x is a natural number, then we proved it in class.

   If x is an integer number which is not 0 and not a natural number, then $-x$ is a natural number. By the theorem in class, there exist $a, b \in \mathbb{N} \cup \{0\}$ such that $-x = da + b$ and $b < d$.

   If $b = 0$, i.e., $-x$ is divisible by d, then x is also divisible by d by Exercise 4 of Homework 1, i.e., there exists $q \in \mathbb{Z}$ such that $x = dq$. Take $r = 0 < d$, then we have $x = dq + r$ where $q \in \mathbb{Z}$, $r \in \mathbb{N} \cup \{0\}$ and $r < d$.

   If $-x$ is not divisible by d, then $b \in (0, d)$. Notice that $0 < d - b < d$. We have $x = -da - b = d(-a - 1) + (d - b)$. Let $q = -a - 1$ and $r = d - b$. Then, $q \in \mathbb{Z}$, $r \in \mathbb{N} \cup \{0\}$, $r < d$, and $x = dq + r$. □

2. *Proof.* Let X be a non-empty collection of positive integers. Notice that X is bounded below, because $0 \in \mathbb{Z}$ and $\forall x \in X$ we have $0 \leq x$. By the Well Ordering Principle, we have that there exists $m \in X$ such that $\forall x \in X$ we have $m \leq x$. Therefore, we showed that there exists a smallest element in X.

   Now we want to show that a smallest element in X is unique. Assume we have $m_1, m_2 \in X$ such that $\forall x \in X$ we have $m_1 \leq x$ and $m_2 \leq x$. Since $m_1 \in X$, we have that $m_2 \leq m_1$. Since $m_2 \in X$, we have that $m_1 \leq m_2$. Therefore, $m_2 = m_1$ because $m_2 \leq m_1$ and $m_1 \leq m_2$. As a result, we obtain that a smallest element in X is unique. □

3. *Proof.* Assume there are $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \mathbb{N} \cup \{0\}$ such that $x = dq_1 + r_1$, $x = dq_2 + r_2$, $r_1 < d$, and $r_2 < d$. To prove the uniquness, we need to show that $q_1 = q_2$ and $r_1 = r_2$. Since $x = dq_1 + r_1$ and $x = dq_2 + r_2$, we have that $dq_1 + r_1 = dq_2 + r_2$, so $d(q_1 - q_2) = r_2 - r_1$.

   Case 1: If $r_2 - r_1 \geq 0$, then $0 \leq r_2 - r_1 \leq r_2 < d$, where in the last inequality we used the information that $r_2 < d$. Moreover, since $d(q_1 - q_2) = r_2 - r_1$, we have that d divides $r_2 - r_1$ since $q_1 - q_2$ is an integer. If $r_2 - r_1 = 0$, i.e. $r_2 = r_1$, then $q_1 - q_2 = 0$ because $d \neq 0$, i.e., $q_1 = q_2$. If $r_2 - r_1 \neq 0$, i.e., $(r_2 - r_1) \in \mathbb{N}$, then by the lemma in class we have that $d \leq r_2 - r_1$ because d divides $r_2 - r_1$. But $r_2 - r_1 < d$, so we obtain contradiction, and we should have $r_2 = r_1$ what implies that $q_1 = q_2$.

   Case 2:If $r_2 - r_1 \leq 0$, then $0 \leq r_1 - r_2 \leq r_1 < d$, where in the last inequality we used the information that $r_1 < d$. Moreover, since $d(q_2 - q_1) = r_1 - r_2$, we have that d divides $r_1 - r_2$ since $q_2 - q_1$ is an integer. If $r_1 - r_2 = 0$, i.e. $r_1 = r_2$, then $q_2 - q_1 = 0$ because $d \neq 0$, i.e., $q_2 = q_1$. If $r_1 - r_2 \neq 0$, i.e., $(r_1 - r_2) \in \mathbb{N}$, then by the lemma in class we have that $d \leq r_1 - r_2$ because d divides $r_1 - r_2$. But $r_1 - r_2 < d$, so we obtain contradiction, and we should have $r_1 = r_2$ what implies that $q_1 = q_2$.

   Therefore, we obtain that q and r in the statement of the exercise are unique. □

4. *Proof.* Let $X = \{ax + by | x, y \in \mathbb{Z} \quad \text{and} \quad ax + by > 0\}$. If $a > 0$, then $a \in X$ because we can take $x = 1 \in \mathbb{Z}$ and $y = 0 \in \mathbb{Z}$, and we have $a \cdot 1 + b \cdot 0 = a > 0$. If $a < 0$, then $-a > 0$ and $-a \in X$ because we can take $x = -1 \in \mathbb{Z}$ and $y = 0 \in \mathbb{Z}$, and we have $a \cdot (-1) + b \cdot 0 = -a > 0$. Therefore, X is not empty. Moreover, since X is a collection of positive integers, we have $\forall c \in X$ we have $0 \leq c$ and $0 \in \mathbb{Z}$, so X is bounded below. Since X is non-empty subset of integer numbers that is bounded below, by Well Ordering Principle, there exists $d \in X$ such that $\forall c \in X$ we have $d \leq c$. There exists $s, t \in \mathbb{Z}$ such that $d = as + bt$ and $d > 0$ because $d \in X$.

   We show that d divides a. By the theorem in class, $\exists q, r \in \mathbb{N} \cup \{0\}$ such that $a = dq + r$ and $r < d$. Since $d = as + bt$, we have $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq)$. If $r \neq 0$, then $r \in X$ because $(1 - sq) \in \mathbb{Z}$, $(-tq) \in \mathbb{Z}$, and $r > 0$. Notice that $r < d$ and $r \in X$ if $r \neq 0$, what contradicts the fact that d is a smallest element in X. Therefore, $r = 0$, so $a = dq$, where $q \in \mathbb{Z}$, so d divides a.

   Similarly to d divides a, it can be shown that d divides b.

   Now we show that if $c \in \mathbb{N}$, c divides a, and c divides b, then c divides d. Recall that $d = as + bt$, where $s, t \in \mathbb{Z}$. Since c divides a and c divides b, we have $a = ck$ and $b = cn$, where $k, n \in \mathbb{Z}$. Therefore, we obtain that $d = as + bt = cks + cnt = c(ks + nt)$ where $(ks + nt) \in \mathbb{Z}$, so c divides d. □

5. *Solution.* Let u, v, and w be rational numbers. Then, $u = \frac{p}{q}$, $v = \frac{a}{b}$, and $w = \frac{c}{d}$, where $p, q, a, b, c, d \in \mathbb{Z}$ and $q, b, d \neq 0$.

   (a) We have $u - 2v = \frac{p}{q} - 2\frac{a}{b} = \frac{pb - 2aq}{qb}$. If $q \neq 0$ and $b \neq 0$, then $qb \neq 0$. Since $p, q, a, b, c, d \in \mathbb{Z}$, $pb - 2aq$ and qb are integers. Therefore, since $u - 2v = \frac{pb-2aq}{qb}$, we have $u - 2v$ is a rational number.

   (b) If $w \neq 0$, then $\frac{uv}{w}$ is well defined. In particular, if $w = \frac{c}{d}$ and $w \neq 0$, then $c \neq 0$. We have $\frac{uv}{w} = \frac{pad}{qbc}$. If $q, b, c \neq 0$, then $qbc \neq 0$. Since $p, q, a, b, c, d \in \mathbb{Z}$, pad and qbc are integers. Therefore, since $\frac{uv}{w} = \frac{pad}{qbc}$, we have $\frac{uv}{w}$ is a rational number.

□