Math 230 **Spring 2019**
Homework 3 **Drew Armstrong**

Problem 1. Let $a, b \in \mathbb{Z}$. Use the axioms of $\mathbb{Z}$ to prove the following properties:

(a) $-(-a) = a$.
(b) $a(-b) = (-a)b = -(ab)$. [Hint: Multiply both sides of $b - b = 0$ by a.]
(c) $(-a)(-b) = ab$. [Hint: Combine parts (a) and (b).]

(a) By definition of negatives we have

$$\left\{ \begin{array}{c} a + (-a) = 0 \\ (-a) + (-(-a)) = 0 \end{array} \right\} \quad \Longrightarrow \quad a + (-a) = (-a) + (-(-a)).$$

Then cancelling $(-a)$ from both sides gives $a = -(-a)$.

(b) For all $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} b + (-b) &= 0 \\ a(b + (-b)) &= a0 \\ ab + a(-b) &= 0 && a0 = 0 \text{ from class} \\ ab + a(-b) &= ab + (-(ab)). \end{aligned}$$

Then cancelling ab from both sides gives $a(-b) = -(ab)$. It also follows that

$$(-a)b = b(-a) = -(ba) = -(ab).$$

(c) Finally, combining 1(a) and 1(b) gives

$$\begin{aligned} (-a)(-b) &= -(a(-b)) && 1(b) \\ &= -(-(ab)) && 1(b) \\ &= ab. && 1(a) \end{aligned}$$

□

Problem 2. Use the axioms of $\mathbb{Z}$ to prove the following properties:

(a) $\forall a \in \mathbb{Z}, (0 < a) \Leftrightarrow (-a < 0)$. [Hint: Add something to both sides.]
(b) $\forall a, b, c \in \mathbb{Z}, (a < b \wedge c < 0) \Rightarrow (bc < ac)$. [Hint: Use 2(a) and 1(b).]
(c) $\forall a, b \in \mathbb{Z}, (a \neq 0 \wedge b \neq 0) \Rightarrow (ab \neq 0)$. [Hint: There are 4 cases.]
(d) **Multiplicative Cancellation.** $\forall a, b, c \in \mathbb{Z}, (ab = ac \wedge a \neq 0) \Rightarrow (b = c)$. [Hint: If $ab = ac$ then $a(b - c) = 0$. Use the contrapositive of 2(c).]

(a) First suppose that $0 < a$. Then adding $-a$ to both sides gives

$$\begin{aligned} 0 &< a \\ 0 + (-a) &< a + (-a) && \text{axiom (O1)} \\ -a &< 0. \end{aligned}$$

Conversely, suppose that $-a < 0$. Then adding a to both sides gives

$$\begin{aligned} -a &< 0 \\ -a + a &< 0 + a && \text{axiom (O1)} \\ 0 &< a. \end{aligned}$$

(b) We want to prove that $(a < b \wedge c < 0) \Rightarrow (bc < ac)$. So suppose that $a < b$ and $c < 0$. From 2(a) this implies that $0 < -c$ and then axiom (O2) and Problem 1(c) give

$$\begin{aligned} a(-c) &< b(-c) && \text{axiom (O2)} \\ -(ac) &< -(bc) && \text{1(c)} \end{aligned}$$

Finally, we add $ac + bc$ to both sides to obtain

$$\begin{aligned} -(ac) &< -(bc) \\ \cancel{-(ac) + ac} + bc &< \cancel{-(bc) + bc} + ac \\ 0 + bc &< 0 + ac \\ bc &< ac. \end{aligned}$$

(c) We want to prove that $(a \neq 0 \wedge b \neq 0) \Rightarrow (ab \neq 0)$. So assume that $a \neq 0$ and $b \neq 0$. From the law of trichotomy there are four cases:

- **Case 1.** If $0 < a$ and $0 < b$ then (O2) gives $0 < ab$, hence $ab \neq 0$.
- **Case 2.** If $0 < a$ and $b < 0$ then (O2) gives $ab < 0$, hence $ab \neq 0$.
- **Case 3.** If $a < 0$ and $0 < b$ then (O2) gives $ab < 0$, hence $ab \neq 0$.
- **Case 4.** If $a < 0$ and $b < 0$ then 2(b) gives $0 < ab$, hence $ab \neq 0$.

In any case we conclude that $ab \neq 0$. For the purpose of 2(d) below, let me state this result in a logically equivalent form:

$$(ab = 0 \wedge a \neq 0) \Rightarrow (b = 0).$$

(d) We want to prove that $(ab = ac \wedge a \neq 0) \Rightarrow (b = c)$. So assume that $ab = ac$ and $a \neq 0$. Then we have

$$\begin{aligned} ab &= ab \\ ab - ac &= 0 \\ a(b - c) &= 0. \end{aligned}$$

Finally, since $a \neq 0$, part 2(c) implies that $(b - c) = 0$ and hence $b = c$. $\square$

Problem 3. For all $a \in \mathbb{Z}$ we assume that $\sqrt{a} \in \mathbb{R}$ exists. In this problem you will show that

$$\sqrt{a} \notin \mathbb{Z} \Rightarrow \sqrt{a} \notin \mathbb{Q}.$$

(a) Assume that $\sqrt{a} \notin \mathbb{Z}$. Prove that there exists $m \in \mathbb{Z}$ such that $m - 1 < \sqrt{a} < m$. [Hint: Let $S = \{n \in \mathbb{Z} : \sqrt{a} < n\}$ and use Well-Ordering.]

(b) Now assume for contradiction that $\sqrt{a} \in \mathbb{Q}$ and consider the set $T := \{n \geq 1 : n\sqrt{a} \in \mathbb{Z}\}$. Use Well-Ordering to show that this set has a least element $d \in T$. But then show that $d(\sqrt{a} - m + 1)$ is a smaller element of T. Contradiction.

Proof. (a) Assume that $\sqrt{a} \notin \mathbb{Z}$ and consider the set $S = \{n \in \mathbb{Z} : \sqrt{a} < n\}$. This set is non-empty (we don't really have an axiom to prove this because we never defined the real numbers) and bounded below (by the number 0; again we can't really prove this), so the Well-Ordering Principle says that there exists a smallest element $m \in S$. By minimality of m we must have $m - 1 \notin S$, which implies that $\sqrt{a} \not< m - 1$, or in other words $m - 1 \leq \sqrt{a}$. But since $\sqrt{a} \notin \mathbb{Z}$ we know that $m - 1 \neq \sqrt{a}$ and hence $m - 1 < \sqrt{a}$.

(b) Now consider the set $T = \{n \geq 1 : n\sqrt{a} \in \mathbb{Z}\}$ and assume for contradiction that $\sqrt{a} \in \mathbb{Q}$. This means that $\sqrt{a} = p/q$ for some integers $p, q \in \mathbb{Z}$ with $q \geq 1$. But then $q\sqrt{a} = p \in \mathbb{Z}$ and we conclude that $q \in T$. Since T is non-empty (it contains q) and is bounded below (by 1), the Well-Ordering Principle says that there exists a smallest element $d \in T$.

Now we will obtain a contradiction by producing a strictly smaller element of T. Recall from part (a) that there exists an integer $m \in \mathbb{Z}$ with $m - 1 < \sqrt{a} < m$. Applying axioms (O1) and (O2) gives

$$\begin{array}{rcccl} m-1 & < & \sqrt{a} & < & m \\ 0 & < & \sqrt{a} - m + 1 & < & 1 \\ 0 & < & d(\sqrt{a} - m + 1) & < & d. \end{array}$$

But note that

$$d(\sqrt{a} - m + 1) = d\sqrt{a} - d(m-1) \in \mathbb{Z} \quad \text{because} \quad d\sqrt{a} \in \mathbb{Z}.$$

Hence $d(\sqrt{a} - m + 1)$ is a positive integer that is strictly smaller than d. Finally, to show that $d(\sqrt{a} - m + 1)$ is an element of T we observe that

$$d(\sqrt{a} - m + 1)\sqrt{a} = da - (m-1)d\sqrt{a} \in \mathbb{Z} \quad \text{because} \quad d\sqrt{a} \in \mathbb{Z}.$$

□

Problem 4. Let $a, b, c \in \mathbb{Z}$. Prove the following properties of divisibility:

(a) If $a|b$ and $b|c$ then $a|c$.
(b) If $a|b$ and $a|c$ then for all $x, y \in \mathbb{Z}$ we have $a|(bx + cy)$.
(c) If $a|b$ and $b|a$ then $a = \pm b$. [Hint: Use 2(d).]
(d) **Bonus Material.** If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.

(a) Suppose that $a|b$ and $b|c$. By definition this means that $ak = b$ and $b\ell = c$ for some integers $k, \ell \in \mathbb{Z}$. But then we have

$$c = b\ell = (ak)\ell = a(k\ell),$$

which implies that $a|c$ because $k\ell \in \mathbb{Z}$.

(b) Suppose that $a|b$ and $a|c$. By definition this means that $ak = b$ and $a\ell = c$ for some integers $k, \ell \in \mathbb{Z}$. Then for all integers $x, y \in \mathbb{Z}$ we have

$$bx + cy = (ak)x + (a\ell)y = a(kx) + a(\ell y) = a(kx + \ell y),$$

which implies that $a|(bx + cy)$ becuase $kx + \ell y \in \mathbb{Z}$.

(c) Suppose that $a|b$ and $b|a$. By definition this means that $ak = b$ and $b\ell = a$ for some integers $k, \ell \in \mathbb{Z}$. If $a = 0$ then there is nothing to prove, so suppose that $a \neq 0$. Then from

Problem 2(d) we have

$$\begin{aligned}
a &= b\ell \\
a &= (ak)\ell \\
a &= a(k\ell) \\
\cancel{a}1 &= \cancel{a}(k\ell) \\
1 &= k\ell.
\end{aligned}$$

Finally, I claim that the only solutions are $k = \ell = 1$ (hence $a = b$) and $k = \ell = -1$ (hence $a = -b$). You don't need to prove this, but I'll provide a proof. The proof will use the absolute value notation to save space. Recall that the absolute value is defined by

$$|a| := \begin{cases} a & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -a & \text{if } a < 0, \end{cases}$$

and satisfies $|ab| = |a| \cdot |b|$ for all $a, b \in \mathbb{Z}$. [This result follows from the proof of 2(c).]

Proof. If $1 = k\ell$ then $1 = |1| = |k\ell| = |k| \cdot |\ell|$. I claim that $|k| = 1$ and hence also $|\ell| = 1$. To prove this, assume for contradiction that $|k| \neq 1$. Then there are two cases:

- **Case 1.** If $|k| < 1$ then since $|k| > 0$ we obtain a contradiction to the fact proved in class that there are no integers strictly between 0 and 1.
- **Case 2.** If $|k| > 1$ then multiplying both sides by the positive number $|\ell|$ gives $1 = |k| \cdot |\ell| > |\ell|$. But now $|\ell|$ is an integer strictly between 0 and 1. Contradiction.

$\square$

(d) **Bonus Material.** Let $a|b$ and $b \neq 0$. By definition we have $ak = b$ for some $k \in \mathbb{Z}$ and since $b \neq 0$ we must have $a \neq 0$ and $k \neq 0$. Since there are no integers between 0 and 1 this implies that $|k| \geq 1$ and then multiplying both sides by the positive integer $|a|$ gives

$$\begin{aligned}
1 &\leq |k| \\
|a| &\leq |a| \cdot |k| \\
|a| &\leq |ak| \\
|a| &\leq |b|.
\end{aligned}$$

$\square$

[Remark: We already used this result in class when we proved the uniqueness of quotients and remainders.]