Math 230 D **Fall 2015**
Homework 3 **Drew Armstrong**

Problem 1. How do $-$ and $\times$ interact? For the following exercises I want you to give Euclidean style proofs using the axioms of $\mathbb{Z}$ from the handout. You can also use the results we proved in class, such as: uniqueness of "$-a$", $0a = 0$ for all $a \in \mathbb{Z}$, and the Cancellation Lemma $(a + b = a + c) \Rightarrow (b = c)$.

(a) Recall that $-n$ is the **unique** integer satisfying $n + (-n) = 0$. Prove that for all $n \in \mathbb{Z}$ we have $-(-n) = n$.

(b) Prove that for all $a, b \in \mathbb{Z}$ we have $(-a)b = a(-b) = -(ab)$. [Hint: Use the fact that $0a = 0$ for all $a \in \mathbb{Z}$, which we proved in class.]

(c) Recall that for all $m, n \in \mathbb{Z}$ we define $m - n := m + (-n)$. Prove that for all $a, b, c \in \mathbb{Z}$ we have $a(b - c) = ab - ac$. [Hint: Use (b).]

(d) Prove that for all $a, b \in \mathbb{Z}$ we have $(-a)(-b) = ab$. [Hint: Use parts (a) and (b).]

Proof. For part (a) consider any $n \in \mathbb{Z}$ and note that $n + (-n) = 0$ by definition. On the other hand, we have $(-n) + (-(-n)) = 0$ by definition. Combining the two equations gives $(-n) + (-(-n)) = (-n) + n$, and then we can cancel $(-n)$ from both sides (using the Cancellation Lemma) to get $-(-n) = n$.

For part (b) consider any $a, b \in \mathbb{Z}$. Then we have

$$\begin{aligned} ab + a(-b) &= a(b + (-b)) && \text{(D)} \\ &= a0 && \text{(A4)} \\ &= 0 && \text{from class.} \end{aligned}$$

In other words, $a(-b)$ is an additive inverse of ab. By the uniqueness of additive inverses (proved in class), we have $a(-b) = -(ab)$. Similarly, we have

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{(D)} \\ &= 0b && \text{(A4)} \\ &= 0 && \text{from class,} \end{aligned}$$

which implies that $(-a)b = -(ab)$.

For part (c), consider any $a, b, c \in \mathbb{Z}$. Then we have

$$\begin{aligned} a(b - c) &= a(b + (-c)) && \text{by definition} \\ &= ab + a(-c) && \text{(D)} \\ &= ab + (-(ac)) && \text{by part (b)} \\ &= ab - ac && \text{by definition.} \end{aligned}$$

For part (d), consider any $a, b \in \mathbb{Z}$. Then we have

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

$\square$

Problem 2. First Look at Induction.

(a) Prove that 3^n is an odd number **for all** natural numbers $n \in \mathbb{N}$. [Hint: Assume for contradiction that **there exists** a natural number such that 3^n is **even**. In this case, the Well-Ordering Axiom tells us that there is a **smallest** such integer. Call it $m \in \mathbb{N}$. Now try to find a contradiction.]

(b) Assume that there exists a real number $x \in \mathbb{R}$ such that $2^x = 3$ (we call it $x = \log_2(3)$). Use part (a) to prove that $x \notin \mathbb{Q}$.

Proof. For part (a), let $S = \{n \in \mathbb{N} : 3^n \text{ is even}\}$. We wish to show that S is the empty set. To show this, assume for contradiction that S is **not** empty. Then the Well-Ordering Axiom says that there exists a smallest element, say $m \in S$. We know that $3^1 = 3$ is odd, so that $1 \notin S$, and hence $1 < m$. Now consider the natural number $m-1 \in \mathbb{N}$. Since m is the smallest element of S we must have $m - 1 \notin S$, and hence 3^{m-1} is odd. But then $3^m = 3 \cdot 3^{m-1}$, being the product of two odd numbers, is odd. This contradicts the fact that $m \in S$. We conclude that S is the empty set; in other words, 3^n is odd for all $n \in \mathbb{N}$.

For part (b), let $x = \log_2(3)$ and assume for contradiction that $x = m/n$ for some integers $m, n \in \mathbb{Z}$ with $n \in \mathbb{N}$. By definition we have

$$\begin{aligned} 2^x &= 3 \\ 2^{m/n} &= 3 \\ (2^{m/n})^n &= 3^n \\ 2^m &= 3^n. \end{aligned}$$

Since $n \in \mathbb{N}$ we know from part (a) that 3^n is an odd number. But since $2^m = 3^n > 1$ we know that $m \geq 1$ and hence $2^m = 2 \cdot 2^{m-1}$ is even. Contradiction. $\square$

Problem 3. Square root of $a \in \mathbb{Z}$.

(a) Suppose that $\alpha \in \mathbb{R}$ and $\alpha \notin \mathbb{Z}$. In this case, use the Well-Ordering Axiom to prove that there exists an integer $b \in \mathbb{Z}$ such that

$$b < \alpha < b + 1.$$

[Hint: Let $S = \{n \in \mathbb{Z} : \alpha < n\}$. Since this set is nonempty and bounded below, the Well-Ordering Axiom says it has a least element, say $m \in S$.]

(b) Prove that for all $a \in \mathbb{Z}$ we have

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

[Hint: Assume that $\sqrt{a} \notin \mathbb{Z}$, so we have $b < \sqrt{a} < b + 1$ for some $b \in \mathbb{Z}$ by part (a). Now assume for contradiction that $\sqrt{a} \in \mathbb{Q}$. Consider the set $T = \{n \in \mathbb{N} : n\sqrt{a} \in \mathbb{Z}\}$. Show that T is not empty, so by Well-Ordering it has a smallest element, say $m \in T$. Now show that $m(\sqrt{a} - b)$ is a **smaller** element of T. Contradiction.]

Proof. For part (a), let $\alpha \in \mathbb{R}$ and $\alpha \notin \mathbb{Z}$. Define the set $S = \{n \in \mathbb{Z} : \alpha < n\}$. By Well-Ordering, this set has a least element, say $m \in S$. Since $m \in S$ we have $\alpha < m$ by definition. And since $m - 1 \notin S$ we have $\alpha \not< m - 1$ by definition. Finally, since $\alpha \neq m - 1$ (because $\alpha \notin \mathbb{Z}$) this implies that $m - 1 < \alpha$. The desired integer is $b = m - 1$.

For part (b), consider $a \in \mathbb{Z}$ and suppose that $\sqrt{a} \notin \mathbb{Z}$. In this case we want to show that $\sqrt{a} \notin \mathbb{Q}$. To do this, assume for contradiction that $\sqrt{a} \in \mathbb{Q}$, so we can write $\sqrt{a} = p/q$ with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Now consider the set $T = \{n \in \mathbb{N} : n\sqrt{a} \in \mathbb{Z}\}$. We know that T is not empty because $q \in \mathbb{N}$ and $q\sqrt{a} = p \in \mathbb{Z}$ imply that $q \in T$. Thus, by Well-Ordering there is a smallest element, say $m \in T$.

Since $\sqrt{a} \notin \mathbb{Z}$ by assumption, part (a) implies that there exists an integer $b \in \mathbb{Z}$ such that $b < \sqrt{a} < b+1$. Subtracting b and then multiplying by m gives

$$\begin{aligned} b < \sqrt{a} &< b+1 \\ 0 < \sqrt{a} - b &< 1 \\ 0 < m(\sqrt{a}-b) &< m. \end{aligned}$$

If we can show that $m(\sqrt{a}-b) \in T$ then this will be the desired contradiction, because m is supposed to be the **smallest** element of T. To show that $m(\sqrt{a}-b) \in T$ first note that since $m\sqrt{a} \in \mathbb{Z}$ and $mb \in \mathbb{Z}$ we have

$$m(\sqrt{a}-b) = m\sqrt{a} - mb \in \mathbb{Z},$$

and since $0 < m(\sqrt{a}-b)$ this implies that $m(\sqrt{a}-b) \in \mathbb{N}$. Finally, we have

$$m(\sqrt{a}-b)\sqrt{a} = ma - b(m\sqrt{a}) \in \mathbb{Z},$$

and hence $m(\sqrt{a}-b) \in T$ as desired. $\square$

Problem 4. Greatest Common Divisor. Consider two integers $a, b \in \mathbb{Z}$ that are not both zero. Now consider the set of "common divisors"

$$D = \{d \in \mathbb{Z} : d|a \wedge d|b\}.$$

Show that this set is bounded above, so by Well-Ordering it has a largest element. Call the largest element $\gcd(a,b)$. Now show that $1 \leq \gcd(a,b)$. [Hint: Use Problem 3(d) from HW2.]

Proof. Recall from HW2 Problem 3(d) that for $x, y \in \mathbb{Z}$ with $y \neq 0$ we have $x|y \Rightarrow |x| \leq |y|$. Now consider integers $a, b \in \mathbb{Z}$ not both zero and define ther set of common divisors $D = \{d \in \mathbb{Z} : d|a \wedge d|b\}$. Without loss of generality, let's assume that $a \neq 0$ (otherwise we can switch the names of a and b and the argument will be the same). Then for all $d \in D$ we have $d|a$ and $a \neq 0$, hence $d \leq |d| \leq |a|$ by the above the remark. Since the set D is bounded above (by $|a|$), it follows from Well-Ordering that D has greatest element. We will denote this element by $\gcd(a,b) \in D$, and call it the "greatest common divisor" of a and b.

Finally, note that $1|a$ and $1|b$, so that $1 \in D$. Since $\gcd(a,b)$ is the **greatest** element of D it follows that $1 \leq \gcd(a,b)$, as desired.

$\square$