Math 230 E **Fall 2013**
Homework 2 **Drew Armstrong**

Problem 1. Practice with the axioms of $\mathbb{Z}$. For the following exercises I want you to give Euclidean style proofs using the axioms of $\mathbb{Z}$ from the handout. That is, *don't assume anything* and *justify every tiny little step*.

(a) Given integers $a, b, c \in \mathbb{Z}$ with $a + b = a + c$, prove that $b = c$. This is called the cancellation property of $\mathbb{Z}$. [Hint: First apply axiom (A4) to the integer a.]

(b) Axiom (A3) says that for each integer $a \in \mathbb{Z}$ there exists another integer $b \in \mathbb{Z}$ such that $a + b = 0$ (and we call this b an "additive inverse" of a). Prove that additive inverses are **unique**. That is, show that if $a + b = 0$ and $a + c = 0$ then $b = c$. [Hint: Use part (a).]

Proof. To prove (a), consider integers $a, b, c \in \mathbb{Z}$ such that $a + b = a + c$. By (A4) there exists some $d \in \mathbb{Z}$ such that $a + d = 0$. Then we have

$$
\begin{aligned}
a + b &= a + c, && \\
b + a &= c + a, && \text{(A1)}\\
(b + a) + d &= (c + a) + d, && \text{(don't worry about it)}\\
b + (a + d) &= c + (a + d), && \text{(A2)}\\
b + 0 &= c + 0, && \text{(property of } d\text{)}\\
0 + b &= 0 + c, && \text{(A1)}\\
b &= c. && \text{(A3)}
\end{aligned}
$$

[Oops. The second step there was actually a bit tricky. Don't worry about it.] To prove (b), consider an integer $a \in \mathbb{Z}$ and suppose that there exist $b, c \in \mathbb{Z}$ such that $a + b = 0 = a + c$. Since $a + b = a + c$, the cancellation proprty from part (a) says that $b = c$. $\square$

[Since the additive inverse of a is unique, we might as well give it a name. How about "$-a$"?]

Problem 2. For each integer $a \in \mathbb{Z}$ we define the absolute value:

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

(a) Prove that for all integers $a, b \in \mathbb{Z}$ we have $|ab| = |a||b|$. [Hint: You may assume the properties $(-a)(-b) = ab$ and $(-a)b = -(ab)$ without proof. We'll prove them later.]

(b) Given integers $a, b \in \mathbb{Z}$ we say that a divides b (and we write $a|b$) if there exists $q \in \mathbb{Z}$ such that $b = qa$. If $a|b$ and $b \neq 0$, prove that $|a| \leq |b|$. [Hint: If $q \neq 0$ note that $|q| \geq 1$. Now use part (a).]

Proof. To prove (a), consider two integers $a, b \in \mathbb{Z}$. If a or b is zero then we have $|ab| = 0 = |a||b|$, so assume that a and b are both nonzero. Now there are four cases:

- If $a > 0$ and $b > 0$ then we have $ab > 0$, hence

$$
|ab| = ab = |a||b|.
$$

- If $a < 0$ and $b > 0$ then we have $ab < 0$, hence
$$|ab| = -(ab) = (-a)b = |a||b|.$$
- If $a > 0$ and $b < 0$ then we have $ab < 0$, hence
$$|ab| = -(ab) = a(-b) = |a||b|.$$
- If $a < 0$ and $b < 0$ then we have $ab > 0$, hence
$$|ab| = (-a)(-b) = ab = |a||b|.$$

To prove (b) suppose that $a|b$ (say, $b = qa$) with $b \neq 0$. Since $b \neq 0$ we also have $q \neq 0$, and since q is an integer this implies $|q| \geq 1$. (Strictly speaking, we probably need the Well-Ordering Axiom to prove that, but we won't bother.) Multiplying both sides of the inequality $|q| \geq 1$ by the non-negative $|a|$ gives $|q||a| \geq |a|$. Finally, use part (a) to conclude that
$$|b| = |q||a| \geq |a|.$$
□

Problem 3. Prove that $\sqrt{3}$ is not a ratio of whole numbers, in two steps.

(a) First prove the following **lemma**: Given a whole number n, if n^2 is a multiple of 3, then so is n. [Hint: Use the contrapositive, and note that there are two different ways for n to be not a multiple of 3. Treat each separately.]

(b) Use the method of contradiction to prove that $\sqrt{3}$ is not a ratio of whole numbers. Quote your lemma in the proof. [Hint: Mimic the proof for $\sqrt{2}$ as closely as possible.]

Lemma: If n^2 is a multiple of 3 then so is n.

Proof. We will prove the contrapositive statement — that if n is **not** a multiple of 3 then **neither** is n^2 — which is logically equivalent. So suppose that n is not a multiple of 3. There are two cases: **(1)** If $n = 3k+1$ for some k, then $n^2 = (3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$ is not a multiple of 3. (It leaves remainder 1 when divided by 3.) **(2)** If $n = 3k+2$ for some k, then $n^2 = (3k+2)^2 = 9k^2+12k+4 = 9k^2+12k+3+1 = 3(3k^2+4k+1)+1$ is also not a multiple of 3. □

[Here we implicitly used the Division Algorithm to conclude that every integer $n \in \mathbb{Z}$ is of the form $3k+0$, $3k+1$, or $3k+2$ for some $k \in \mathbb{Z}$.]

Theorem: $\sqrt{3}$ is not a ratio of whole numbers.

Proof. **Suppose for contradiction** that $\sqrt{3} = a/b$ for whole numbers a, b. After dividing out common factors we may assume that a and b have no common factor (other than ± 1). Square both sides to get $3 = a^2/b^2$ and then multiply by b^2 to get $a^2 = 3b^2$. Since a^2 is a multiple of 3 the Lemma implies that $a = 3k$ for some k. But then $3b^2 = a^2 = 9k^2$ and dividing by 3 gives $b^2 = 3k^2$. The Lemma now implies that b is a multiple of 3. To summarize, we have shown that a and b are both divisible by 3, but this **contradicts** the fact that a, b have no common factor. Hence our original assumption — that $\sqrt{3}$ is a ratio of whole numbers — must be false. □

[When we assumed that we could write a/b in "lowest terms", we were implicitly using the Well-Ordering Axiom to tell us that the process of dividing out common factors would stop in finite time.]

Problem 4. In this exercise you will show that all of Boolean logic can be expressed using only the concepts NOT and $\Rightarrow$. We use the symbol $\equiv$ to denote logical equivalence.

(a) Use a truth table to show that "P OR Q" $\equiv$ "(NOT P) $\Rightarrow Q$".
(b) Use a truth table to show that "P AND Q" $\equiv$ "NOT($P \Rightarrow$ (NOT Q))".
(c) Write the statement $P \Leftrightarrow Q$ using **only the symbols** P, Q, NOT and $\Rightarrow$ (and, of course, parentheses).

Proof. For part (a) we have the following truth table:

P	Q	P OR Q	NOT P	(NOT P) $\Rightarrow Q$
T	T	T	F	T
T	F	T	F	T
F	T	T	T	T
F	F	F	T	F

For part (b) we have the following truth table:

P	Q	P AND Q	NOT Q	$P \Rightarrow$ (NOT Q)	NOT ($P \Rightarrow$ (NOT Q))
T	T	T	F	F	T
T	F	F	T	T	F
F	T	F	F	T	F
F	F	F	T	T	F

Now we turn to part (c). By definition we have "$P \Leftrightarrow Q$" $\equiv$ "($P \Rightarrow Q$) AND ($Q \Rightarrow P$)". Finally, applying part (b) gives

$$\begin{aligned}\text{``}P \Leftrightarrow Q\text{''} &\equiv \text{``}(P \Rightarrow Q) \text{ AND } (Q \Rightarrow P)\text{''}\\ &\equiv \text{``NOT}\,((P \Rightarrow Q) \Rightarrow (\text{NOT}\,(Q \Rightarrow P)))\text{''}.\end{aligned}$$

$\square$

[This problem shows that it's possible to discuss logic without ever using the words OR or AND. It doesn't mean that we *want* to; it just means that it's *possible*.]