Math 230 E **Fall 2013**
Homework 4 **Drew Armstrong**

Problem 1. Prove that for all integers $a, b \in \mathbb{Z}$ we have

$$(ab = 0) \implies (a = 0 \text{ or } b = 0).$$

You may assume the following axioms: **(1)** For all $x, y, z \in \mathbb{Z}$, if $x < y$ and $z > 0$ then $xz < yz$. **(2)** For all $x, y, z \in \mathbb{Z}$, if $x < y$ and $z < 0$ then $xz > yz$. **(3)** $0 < 1$.

Proof. We will prove the contrapositive statement, that

$$(a \neq 0 \text{ and } b \neq 0) \implies (ab \neq 0).$$

So assume that $a \neq 0$ and $b \neq 0$. There are four cases:

- **Case** $a > 0$ **and** $b > 0$. If we multiply both sides of $a > 0$ by b then axiom **(1)** says that $ab > 0b = 0$, hence $ab \neq 0$.
- **Case** $a > 0$ **and** $b < 0$. If we multiply both sides of $a > 0$ by b then axiom **(2)** says that $ab < 0b = 0$, hence $ab \neq 0$.
- **Case** $a < 0$ **and** $b > 0$. If we multiply both sides of $a < 0$ by b then axiom **(1)** says that $ab < 0b = 0$, hence $ab \neq 0$.
- **Case** $a < 0$ **and** $b < 0$. If we multiply both sides of $a < 0$ by b then axiom **(2)** says that $ab > 0b = 0$, hence $ab \neq 0$.

□

Problem 2. (Multiplicative Cancellation)

(a) Given $a, b, c \in \mathbb{Z}$ with $c \neq 0$, prove that $(ac = bc) \Rightarrow (a = b)$.
(b) Given $a, b \in \mathbb{Z}$ with $a|b$ and $b|a$, prove that $a = \pm b$.

Proof. For part (a), assume that $ac = bc$ with $c \neq 0$. Then we have

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

Since $c \neq 0$, Problem 1 tells us that $a - b = 0$, hence $a = b$. For part (b), assume that $a|b$ and $b|a$, i.e. we have $a = kb$ and $b = \ell a$ for some integers $k, \ell \in \mathbb{Z}$. Then we have

$$\begin{aligned} a &= kb \\ a &= k\ell a \\ a - k\ell a &= 0 \\ (1 - k\ell)a &= 0. \end{aligned}$$

If $a = 0$ then we also have $b = 0$ and there is nothing to show, so assume that $a \neq 0$. Then Problem 1 implies that $1 - k\ell = 0$, or $k\ell = 1$. From this it follows that $k = \ell = 1$ (in which case $a = b$) or $k = \ell = -1$ (in which case $a = -b$). □

The remaining problems will use the following notation. Fix a nonzero integer $0 \neq n \in \mathbb{Z}$. Then for all integers $a, b \in \mathbb{Z}$ we define

$$\text{“}a \equiv b \pmod{n}\text{”} \iff n|(a-b).$$

Problem 3. Given $0 \neq n \in \mathbb{Z}$, prove that is it safe to “add” and “multiply” numbers modulo n. That is, given $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, prove that

(a) $a + b \equiv a' + b' \pmod{n}$
(b) $ab \equiv a'b' \pmod{n}$

[Hint: We have $a = a' + kn$ and $b = b' + \ell n$ for some $k, \ell \in \mathbb{Z}$.]

Proof. Assume that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. By definition this means that $n|(a - a')$ and $n|(b - b')$ and so we can write $a = a' + kn$ and $b = b' + \ell n$ for some $k, \ell \in \mathbb{Z}$.

For part (a), note that

$$\begin{aligned} a + b &= (a' + kn) + (b' + \ell n) \\ a + b &= (a' + b') + (k + \ell)n \\ (a + b) - (a' + b') &= (k + \ell)n. \end{aligned}$$

We conclude that $n|((a + b) - (a' + b'))$ and hence $a + b \equiv a' + b' \pmod{n}$.

For part (b), note that

$$\begin{aligned} ab &= (a' + kn)(b' + \ell n) \\ ab &= a'b' + b'kn + a'\ell n + k\ell n^2 \\ ab &= a'b' + (b'k + a'\ell + k\ell n)n \\ ab - a'b' &= (b'k + a'\ell + k\ell n)n. \end{aligned}$$

We conclude that $n|(ab - a'b')$ and hence $ab \equiv a'b' \pmod{n}$. $\square$

Problem 4.

(a) Consider $a, b, d \in \mathbb{Z}$ with $d|ab$. If $\gcd(d, a) = 1$ prove that $d|b$.
(b) Consider $a, b, c, n \in \mathbb{Z}$ with $0 \neq n$ and gcd(c, n) = 1. Prove that

$$ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}.$$

(c) Give a specific example to show that the result of part (b) **fails** when $\gcd(c, n) \neq 1$.

Proof. For part (a), assume that $d|ab$ (say $ab = dk$ for $k \in \mathbb{Z}$) and $\gcd(d, a) = 1$. Since $\gcd(d, a) = 1$, by Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $1 = dx + ay$. Multiplying both sides by b then gives

$$\begin{aligned} 1 &= dx + ay \\ b &= dbx + aby \\ b &= dbx + dky \\ b &= d(bx + ky). \end{aligned}$$

We conclude that $d|b$.

For part (b) assume that $ac \equiv bc \pmod{n}$ for some $0 \neq n$ and assume that $\gcd(c, n) = 1$. Then by definition we have $n|(ac - bc)$ hence $n|(a - b)c$. Since $\gcd(c, n) = 1$ we use part (a) to conclude that $n|(a - b)$, hence $a \equiv b \pmod{n}$.

For part (c) we will give an example in which cancellation does **not** work. Consider $(a, b, c, n) = (1, 3, 2, 4)$. Then we have a true statement

$$1 \cdot 2 \equiv 3 \cdot 2 \pmod 4,$$

but if we try to cancel the 2 from both sides we get

$$1 \equiv 3 \pmod 4,$$

which is false. The reason we can't cancel the 2 is because $\gcd(2, 4) \neq 1$. $\square$

Problem 5. (Generalization of Euclid's Lemma) Let $p \in \mathbb{Z}$ be prime. Use **induction** to prove that for all integers $n \geq 2$ the following holds: "Given any set of n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that $p|a_1a_2 \cdots a_n$, there exists some $1 \leq i \leq n$ such that $p|a_i$." [Hint: Call the statement $P(n)$. Prove that (or say why) $P(2) = T$. Prove that for all $k \geq 2$ we have $P(k) \Rightarrow P(k + 1)$. (Your proof will begin: "Fix $k \geq 2$ and assume for induction that $P(k) = T$. In this case we want to show that $P(k + 1) = T$. So consider any $k + 1$ integers $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$ such that $p|a_1a_2 \cdots a_{k+1}$.")]

Proof. For all $n \geq 2$ we define the statement $P(n) :=$ "Given any set of n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that $p|a_1a_2 \cdots a_n$, there exists some $1 \leq i \leq n$ such that $p|a_i$." We want to show that $P(n) = T$ for all $n \geq 2$.

First we note that the base case $P(2)$ is just the statement of Euclid's Lemma, which we know is true.

Now fix an arbitrary $k \geq 2$ and **assume for induction** that $P(k) = T$. In this case we want to show that $P(k + 1)$ is also true. So consider any collection $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$ of $k+1$ integers and assume that $p|a_1a_2 \cdots a_{k+1}$. In this case we want to show that $p|a_i$ for some $1 \leq i \leq k + 1$. First note that

$$p|(a_1a_2 \cdots a_k)a_{k+1},$$

hence Euclid's Lemma (the statement $P(2)$) implies that $p|a_{k+1}$, in which case we're done, or $p|a_1a_2 \cdots a_k$. But in this second case, the true statement $P(k)$ implies that $p|a_i$ for some $1 \leq i \leq k$. Putting these together we conclude that $p|a_i$ for some $1 \leq i \leq k + 1$. Hence $P(k + 1) = T$.

By induction, we conclude that $P(n) = T$ for all $n \geq 2$. $\square$