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)** $0 < 1$.

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 $a = \pm b$.

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 $k, \ell \in \mathbb{Z}$.]

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 $\gcd(\mathrm{c}, \mathrm{n}) = 1$. 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 $\gcd(c, n) \neq 1$.

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 $p|a_1 a_2 \cdots a_n$, 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 $p|a_1 a_2 \cdots a_{k+1}$.”)]