Math 230 D **Fall 2015**
Exam 2 — Fri Oct 30 **Drew Armstrong**

There are 4 problems, worth 6 points each. This is a closed book test. Anyone caught cheating will receive a score of **zero**.

Problem 1. Division Theorem.

(a) Accurately state the Division Theorem.

Given integers $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique integers $q, r \in \mathbb{Z}$ satisfying
- $a = bq + r$,
- $0 \leq r < |b|$.

(b) Use the Division Theorem to prove that there is **no** integer $n \in \mathbb{Z}$ satisfying the property $3n = 4$.

Proof. Assume for contradiction that there exists $n \in \mathbb{Z}$ such that $3n = 4$. Applying the Division Theorem to 4 mod 3 gives

$$4 = 3 \cdot 1 + 1 \text{ with } 0 \leq 1 < 3,$$

so the quotient is 1 and the remainder is 1. But by assumption we also have

$$4 = 3 \cdot n + 0 \text{ with } 0 \leq 0 < 3,$$

so the quotient is n and the remainder is 0. Since $0 \neq 1$, this contradicts the uniqueness part of the Division Theorem. □

Problem 2. Axioms of $\mathbb{Z}$. Consider the following three axioms:

(1) $\forall a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.
(2) $\exists 0 \in \mathbb{Z}$, $\forall a \in \mathbb{Z}$, $a + 0 = 0 + a = a$.
(3) $\forall a \in \mathbb{Z}$, $\exists -a \in \mathbb{Z}$, $a + (-a) = (-a) + a = 0$.

(a) Explicitly use the axioms to prove the following Cancellation Lemma:

$$\forall a, b, c \in \mathbb{Z}, (a + b = a + c) \Rightarrow (b = c).$$

Proof. Consider $a, b, c \in \mathbb{Z}$ and assume that $a + b = a + c$. Then we have

$$\begin{aligned}
b &= 0 + b && (2) \\
&= ((-a) + a) + b && (3) \\
&= (-a) + (a + b) && (1) \\
&= (-a) + (a + c) && \text{assumption} \\
&= ((-a) + a) + c && (1) \\
&= 0 + c && (2) \\
&= c, && (3)
\end{aligned}$$

as desired. □

(b) Let $a \in \mathbb{Z}$ and suppose there exists $a' \in \mathbb{Z}$ such that $a + a' = 0$. In this case prove that $a' = (-a)$. [Hint: You can quote the Cancellation Lemma from part (a).]

Proof. By assumption we have $a + a' = 0$ and by axiom (3) we have $a + (-a) = 0$, hence $a + a' = a + (-a)$. Now the Cancellation Lemma implies $a' = (-a)$. □

Problem 3. Linear Diophantine Equations.

(a) Use the Extended Euclidean Algorithm to find **one particular solution** $x', y' \in \mathbb{Z}$ to the equation $22x' + 16y' = 2$.

Consider triples of integers (x, y, z) such that $22x + 16y = z$. Applying the Euclidean Algorithm to the two obvious triples $(1, 0, 22)$ and $(0, 1, 16)$ gives

x	y	z
1	0	22
0	1	16
1	−1	6
−2	3	4
3	−4	2
−8	11	0

The second last row says $22(3) + 16(-4) = 2$, so we can take $(x', y') = (3, -4)$.

(b) Write down the **complete solution** $x, y \in \mathbb{Z}$ to the equation $22x + 16y = 0$.

If $d = \gcd(a, b)$ with $a = da'$ and $b = db'$, you proved on the homework that the general solution to $ax + by = 0$ is $(x, y) = (-b'k, a'k)$ for all $k \in \mathbb{Z}$. In this case we have $a = 22$, $b = 16$, $d = 2$, $a' = 11$, and $b' = 8$, so the general solution to $22x + 16y = 0$ is

$$(x, y) = (-8k, 11k) \text{ for all } k \in \mathbb{Z}.$$

We could also read this solution from the last row of the table in part (a).

(c) Write down the **complete solution** $x, y \in \mathbb{Z}$ to the equation $22x + 16y = 2$.

Given the particular solution $(3, -4)$ and the general homogeneous solution $(-8k, 11k)$, the general solution is given by

$$(x, y) = (3 - 8k, -4 + 11k) \text{ for all } k \in \mathbb{Z}.$$

Problem 4. Well-Ordering.

(a) Accurately state some version of the Well-Ordering Axiom.

Every nonempty set of positive integers contains a least element.

(b) Use Well-Ordering to prove that **every** integer $n > 1$ is divisible by a prime number. [Hint: Assume for contradiction that **there exists** an integer $n > 1$ such that n is **not** divisible by a prime number.]

Proof. Assume for contradiction that there exists an integer $n > 1$ that is **not** divisible by a prime number, and let S be the set of these integers. Since $S \neq \emptyset$, well-ordering says that S has a least element; call it $m \in S$. Since m is not divisible by a prime number it is not prime, so by definition m has a proper factor, i.e., there exists $d \in \mathbb{Z}$ such that $d|m$ and $1 < d < m$. Now I claim that d has a prime factor. If not, then since $d > 1$ we would have $d \in S$. But then since $d < m$ this would contradict the minimality of m. Thus there exists a prime p such that $p|d$. Since $d|m$ this implies that $p|m$, contradicting the fact that $m \in S$. □