Math 230 D **Fall 2012**
Homework 4 **Drew Armstrong**

Problem 1. Let $a, b, c \in \mathbb{Z}$ be integers. Prove the following.

(a) If $a|b$ and $b|c$, then $a|c$.
(b) If $a|b$ and $a|c$, then $a|(bx + cy)$ for any $x, y \in \mathbb{Z}$.
(c) If $a|b$ and $b|a$, then $a = \pm b$.

Problem 2. Given $a, b \in \mathbb{Z}$ not both zero, define the set of linear combinations

$$a\mathbb{Z} + b\mathbb{Z} := \{ax + by : x, y \in \mathbb{Z}\}.$$

What does this set look like? If $d = \gcd(a, b)$, **prove that**

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} := \{dk : k \in \mathbb{Z}\}.$$

This shows that "$\gcd(\mathrm{a}, \mathrm{b})$ is the smallest positive linear combination of a and b." [Hint: You must show that $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ and $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ **separately**. One direction requires Bézout's Identity.]

Problem 3. Let $a, b, r \in \mathbb{Z}$ be integers and define the set

$$V_r := \{(x, y) : ax + by = r\}.$$

Thus V_0 is the set of solutions (x, y) to the homogeneous equation $ax + by = 0$. If $ax_r + by_r = r$ (i.e. if (x_r, y_r) is any particular solution to the equation $ax + by = r$), **prove** that the general solution to the equation $ax + by = r$ is given by

$$\begin{aligned} V_r = (x_r, y_r) + V_0 &:= \{(x_r, y_r) + (x_0, y_0) : (x_0, y_0) \in V_0\} \\ &= \{(x_r + x_0, y_r + y_0) : ax_0 + by_0 = 0\}. \end{aligned}$$

That is, "the general solution equals the homogeneous solution shifted by any particular solution." [Hint: You must show that $V_r \subseteq ((x_r, y_r) + V_0)$ and $((x_r, y_r) + V_0) \subseteq V_r$ **separately**.]

The next problems use the notation "$a \equiv b \bmod n$," which means exactly that "n divides $a - b$."

Problem 4 (Generalization of Euclid's Lemma).

(a) Suppose that $d|ab$. If $\gcd(a, d) = 1$, prove that $d|b$.
(b) Let $\gcd(c, n) = 1$. If $ac \equiv bc \bmod n$, prove that $a \equiv b \bmod n$.

Problem 5 (Generalization of Euclid's Proof of Infinite Primes).

(a) Consider an integer $n > 1$. **Prove** that if $n \equiv 3 \bmod 4$ then n has a prime factor of the form $p \equiv 3 \bmod 4$. [Hint: You may assume Prop 2.51 from the text. There are three kinds of primes: the number 2, primes $p \equiv 1 \bmod 4$ and primes $p \equiv 3 \bmod 4$.]
(b) Prove that there are infinitely many prime numbers of the form $p \equiv 3 \bmod 4$. [Hint: Suppose there are only **finitely** many and call them $3 < p_1 < p_2 < \cdots < p_k$. Then consider the number $N = 4p_1p_2 \cdots p_k + 3$. Apply part (a).]