Math 230 **Fall 2018**
Homework 4 **Drew Armstrong**

Problem 1. Prove the following properties for all integers $a, b, c \in \mathbb{Z}$.

(a) If $a|b$ and $b|c$ then $a|c$.
(b) If $a|b$ and $a|c$ then $a|(bx + cy)$ for all integers $x, y \in \mathbb{Z}$.
(c) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$. [Hint: Absolute value is multiplicative.]
(d) If $a|b$ and $b|a$ then $a = \pm b$. [Hint: Use the fact that $uv = 0$ implies $u = 0$ or $v = 0$.]

Problem 2. Euclid's Lemma. For all integers $a, b, c \in \mathbb{Z}$ prove that

$$a|(bc) \text{ and } \gcd(a,b) = 1 \text{ imply that } a|c.$$

[Hint: If $\gcd(a, b) = 1$ then the Extended Euclidean Algorithm tells us that there exist (non-unique) integers $x, y \in \mathbb{Z}$ satisfying $ax + by = 1$.]

Problem 3. Let $a, b, c \in \mathbb{Z}$, with a and b not both zero, and consider the sets

$$V = \{(x, y) \in \mathbb{Z}^2 : ax + by = c\},$$
$$V_0 = \{(x, y) \in \mathbb{Z}^2 : ax + by = 0\}.$$

(a) If $(x', y') \in V$ is one particular solution, prove that V is equal to the set

$$(x', y') + V_0 := \{(x' + x, y' + y) : (x, y) \in V_0\}.$$

(b) Let $d = \gcd(a, b)$ with $a = da'$ and $b = db'$ and assume that $c = dc'$ for some $a', b', c' \in \mathbb{Z}$. Prove that V is equal to the set

$$V' := \{(x, y) \in \mathbb{Z}^2 : a'x + b'y = c'\}.$$

(c) Now let $(a, b, c) = (3094, 2513, 21)$. Use the Extended Euclidean Algorithm to find one particular element $(x', y') \in V$. [Hint: From part (b) it is enough to find one particular element of $(x', y') \in V'$.]
(d) Continuing from (c), use Problem 2 to find **all elements** of the set V_0. [Hint: From part (b) we know that $V_0 = V_0' = \{(x, y) \in \mathbb{Z}^2 : a'x + b'y = 0\}$.]

Problem 4. Consider an integer $n \geq 2$. We say that d is a *proper divisor* of n if $d|n$ and $1 < d < n$. We say that $p \geq 2$ is *prime* if it has no proper divisor. Prove that

$$\text{every integer } n \geq 2 \text{ has a prime divisor } p|n.$$

[Hint: Let S be the set of integers $n \geq 2$ that have no prime divisor. If this set is not empty then it must have a smallest element $m \in S$. You will need 1(c).]