Math 230 D **Fall 2015**
Homework 4 **Drew Armstrong**

Problem 1. Rational Numbers. We have used the rational numbers a lot but we never defined them. Now we will. For all integers $a, b \in \mathbb{Z}$ with $b \neq 0$ we define an abstract symbol $[a, b]$. Let $\mathbb{Q}$ be the set of all these symbols:

$$\mathbb{Q} := \{[a, b] : a, b \in \mathbb{Z} \text{ with } b \neq 0\}.$$

We will "multiply" and "add" abstract symbols as follows:

$$[a, b] \cdot [c, d] = [ac, bd] \quad \text{and} \quad [a, b] + [c, d] = [ad + bc, bd].$$

Finally, we declare that $[a, b] = [c, d]$ if and only if $ad = bc$.

(a) Prove that the sum and product of abstract symbols is well-defined. That is, if $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$, prove that we have

$$[a_1, b_1] \cdot [c_1, d_1] = [a_2, b_2] \cdot [c_2, d_2] \quad \text{and} \quad [a_1, b_1] + [c_1, d_1] = [a_2, b_2] + [c_2, d_2].$$

(b) One can check that $\mathbb{Q}$ satisfies all of the axioms of $\mathbb{Z}$ except for the Well-Ordering Axiom (please don't check this), with additive identity $[0, 1] \in \mathbb{Q}$ and multiplicative identity $[1, 1] \in \mathbb{Q}$. But $\mathbb{Q}$ has one crucial advantage over $\mathbb{Z}$: **Prove** that every nonzero element of $\mathbb{Q}$ has a multiplicative inverse.

Problem 2. Generalizations of Euclid's Lemma.

(a) Let $a, b, d \in \mathbb{Z}$. Prove that if $d|ab$ and $\gcd(a, d) = 1$ then we have $d|b$. [Hint: Since $\gcd(a, d) = 1$ there exist $x, y \in \mathbb{Z}$ such that $ax + dy = 1$.]

(b) Consider $a_1, a_2, \ldots, a_n, p \in \mathbb{Z}$ with p prime. Prove that if $p|(a_1 a_2 \cdots a_n)$ then there exists $1 \leq i \leq n$ such that $p|a_i$. [Hint: Use induction or well-ordering. You can assume that the result is true when $n = 2$ (it follows from part (a)).]

Problem 3. Linear Diophantine Equations I. Consider $a, b \in \mathbb{Z}$, not both zero.

(a) Suppose that $d = \gcd(a, b)$ with $a = da'$ and $b = db'$. Prove that $\gcd(a', b') = 1$

(b) Use part (a) and Problem 2(a) to find **all integer solutions** $x, y \in \mathbb{Z}$ to the equation $ax + by = 0$.

Problem 4. Linear Diophantine Equations II. Let $a, b, c \in \mathbb{Z}$ be integers, where a and b are not both zero. We are interested in finding all integer solutions $x, y \in \mathbb{Z}$ to the equation $ax + by = c$. Consider the **set** of solutions

$$V_c := \{(x, y) : ax + by = c\}.$$

(a) If $\gcd(a, b)$ does not divide c, prove that $V_c = \emptyset$.

(b) If $ax' + by' = c$ is **one particular solution**, prove that

$$V_c = ((x', y') + V_0) := \{(x' + x, y' + y) : ax + by = 0\}.$$

[Hint: You have to show $V_c \subseteq ((x', y') + V_0)$ and $((x', y') + V_0) \subseteq V_c$ separately.]

(c) Let $d = \gcd(a, b)$. Suppose that $c = dc'$ and suppose that $ax' + by' = c$. Use everything you have learned to find **all integer solutions** $x, y \in \mathbb{Z}$ to the equation $ax + by = c$. [Hint: You know what V_0 is from Problem 3. Now use part (b).]