Math 295. Homework 5 (Due October 22)

The purpose of this homework set is to prove the fundamental theorem of arithmetic: Every integer greater than one factors uniquely into primes, up to reordering. That is,

Theorem: *If $n \in \mathbb{Z}$ with $n \geq 2$, then n can be written as the product*

$$n = p_1^{a_1} \cdots p_t^{a_t}$$

where the p_i are distinct prime (positive) numbers. If

$$n = q_1^{b_1} \cdots q_s^{b_s}$$

is another prime factorization, with the q_i distinct primes, then $s = t$, and for each i there exists a unique j such that $p_i = q_j$ and $a_i = b_j$.

Recall that a positive integer p greater than one is prime if, whenever we write $p = ab$, either $|a| = p$ or $|b| = p$. We have already shown in class the *existence* of a prime factorization. By the way, our proof was the same as Euclid's orginal proof, over 2300 years ago. You may want to review this: we used strong induction. It remains to show that the factorization is *unique up to reordering.* That is what you will be doing on this problem set, in steps.

Definition: For $a, w \in \mathbb{Z}$ we say "a divides w" and write $a|w$ provided that there exists $c \in \mathbb{Z}$ so that $w = ac$. For x, y in $\mathbb{Z}$ we say that $a \in \mathbb{Z}$ is a *common divisor* of x and y provided that $a|x$ and $a|y$. The greatest common divisor of x and y, should it exist, is denoted $\gcd(x, y)$.

CAUTION: In all problems below, be very careful not to assume the fundamental theorem of arithmetic. You are trying to prove it! If needed, you may use the division algorithm[1] which we proved in class: *if a and b are integers, with $b \neq 0$, then there are unique integers q and r satisfying*

$$a = bq + r$$

where $0 \leq r < b$. It may also be helpful to remember the well-ordering principle of $\mathbb{N}$.

(1) Let x, y and n be integers. Show that if n divides both x and y, then n divides $(x + y)$.
(2) For non-zero $x, y \in \mathbb{Z}$, show that $\gcd(x, y)$ exists and can be written as $m'x + n'y$ for some $m', n' \in \mathbb{Z}$. [Hint: consider the set
$$S := \{mx + ny \,|\, m \in \mathbb{Z}, n \in \mathbb{Z}, \text{ and } mx + ny \in \mathbb{N}\}.]$$
(3) Show that if a prime number p does not divide an integer a, then the greatest common divisor of a and p is 1.
(4) Show that if a and b are positive integers, and a prime number p divides then product ab, then p divides a or p divides b. [Hint: if p does not divide a, write an equation which can be cleverly multiplied by b in order to see that p must divide b.]
(5) Prove the fundamental theorem of arithmetic.

[1] Actually, at least one proof I know, not the one outlined here, makes heavy use of this algorithm.