Math 310 Chapter 6 Review

Divisibility/GCD/Primality

- **divisibility**: For $a, b \in \mathbb{Z}$ and $a \neq 0$, if there exists $k \in \mathbb{Z}$ such that $b = ka$, then we say a *divides* b (or b is *divisible* by a. We write $a|b$.
- **prime**: If $n \in \mathbb{N}$ with $n > 1$ and the only divisors of n are 1 and n, then we say n is a *prime*.
- **greatest common divisor**: If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\gcd(a, b)$='the largest positive integer that divides both a and b'. And we define $\gcd(0, 0) = 0$.
- **relatively prime**: If $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, then we say that a and b are *relatively prime*.

Basic Proof Tips:

1. When proving facts involving divisibility always write out the definition of $a|b$.
2. When proving facts about the $\gcd(a, b)$ it is often useful to consider the set $D(a, b) = \{d \in \mathbb{N} \ : \ d|a \text{ and } d|b\}$. Note that $\gcd(a, b)$=the largest element of $D(a, b)$. And if $D(a, b) = D(c, d)$ (*i.e.* if these sets are equal), then $\gcd(a, b) = \gcd(c, d)$.
3. The fundamental theorem of arithmetic says that for any $n \in \mathbb{N}$ with $n > 1$, you are allowed to write: $n = \prod_{i=1}^{k} p_i^{e_i}$, where p_i are all primes and e_i are positive exponents and this can be done in a unique way.
   (a) Here are a couple examples: $52 = 2 \cdot 2 \cdot 13 = 2^2 \cdot 13$ and $150 = 2 \cdot 3 \cdot 5^2$.
   (b) You can use this in proofs as well. If $n \in \mathbb{N}$ and $n > 1$, then in a proof you can write: $n = \prod_{i=1}^{k} p_i^{e_i}$.
4. (*Facts about relative primality*) If a and b are relatively prime (that is, $\gcd(a, b) = 1$, then
   (a) there exist integers x and y such that $ax + by = 1$, and
   (b) if $a = \prod_{i=1}^{k} p_i^{e_i}$ and $b = \prod_{j=1}^{k'} q_j^{f_j}$, then every prime p_i is different from every prime q_j for each i and j.

Important Results:

1. If $d|a$ and $d|b$, then $d|(a + b)$. (Proof given in lecture.)
2. If $\gcd(a, b) = 1$ and $a|qb$, then $a|q$. (Proof given in lecture.)
3. If $p|ab$ and p is a prime, then $p|a$ or $p|b$. (Proof given in lecture.)
4. (*Division Algorithm*) If $a, b \in \mathbb{N}$ and $a > b$, then there exists $q, r \in \mathbb{N}$ such that $a = qb + r$ where $0 \leq r < b$.
5. (*Euclidean Algorithm*) Let $a, b \in \mathbb{N}$ and $a > b$ and define $r_0 = a$, $r_1 = b$ and
$$r_i = q_{i+1} r_{i+1} + r_{i+2}, \quad \text{where } 0 \leq r_{i+2} < r_{i+1}.$$
   If $r_n \neq 0$ and $r_{n+1} = 0$, then $\gcd(a, b) = r_n$. (That is, $\gcd(a, b)$ is the last nonzero remainder using the given process).
6. (*Linear Diophantine Equations*) If $a, b \in \mathbb{Z}$, then there exist solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ to the equation $ax + by = c$ if and only if $\gcd(a, b)|c$. NOTE: We can get one solution to $ax + by = d$ where $d = \gcd(a, b)$ by back substituting in the Euclidean algorithm.
7. (*Fundamental Theorem of Arithmetic*) If $n \in \mathbb{N}$ and $n > 1$, then n can be expressed as the product of primes in a unique way (up to ordering).