Math 580/780I Notes 3

The Fundamental Theorem of Arithmetic (Unique Factorization):

- **Theorem 6.** *Every integer $n > 1$ can be written uniquely as a product of primes in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where $p_1 < p_2 < \cdots < p_r$ are distinct primes and $e_1, e_2, \ldots, e_r$ and r are positive integers.

- **Comment:** In other words, every positive integer n can be written uniquely as a product of primes except for the order in which the prime factors occur.

- **Lemma.** *If p is a prime and a and b are integers such that $p|ab$, then either $p|a$ or $p|b$.*

- **Proof of Lemma.** Let k be an integer such that $ab = kp$, and suppose $p \nmid a$. We wish to show $p|b$. By Theorem 5, there are integers x and y such that $ax + py = 1$. Hence, $b = abx + pby = p(kx + by)$. Thus, $p|b$.

- **Proof of Theorem 6.** First, we prove that n is a product of primes by induction. The case $n = 2$ is clear. Suppose it is true for n less than some integer $m > 2$. If m is prime, then m is a product of primes. If m is not prime, then $m = ab$ with a and b integers in $(1, m)$. Since a and b are products of primes by the induction hypothesis, so is m.

Now, we prove uniqueness by induction. Again, one checks $n = 2$ directly. Suppose uniqueness of the representation of n as a product of primes as in the theorem holds for $n < m$. Let $p_1, \ldots, p_r$ (not necessarily distinct) and $q_1, \ldots, q_t$ (not necessarily distinct) denote primes such that $m = p_1 \cdots p_r = q_1 \cdots q_t$. Observe that $p_1 | q_1 \cdots q_t$. Hence, the lemma implies $p_1|q_1$ or $p_1|q_2 \cdots q_t$. This in turn implies $p_1|q_1$, $p_2|q_2$, or $p_1|q_3 \cdots q_t$. Continuing, we deduce that $p_1|q_j$ for some $j \in \{1, 2, \ldots, t\}$. As p_1 and q_j are primes, we obtain $p_1 = q_j$. Now, $p_2 \cdots p_r = m/p_1 = q_1 \cdots q_{j-1} q_{j+1} \cdots q_t$ and the induction hypothesis imply that the primes $p_2, \ldots, p_r$ are the same as the primes $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_t$ in some order. This implies the theorem.

Homework:

(1) Find the prime factorization described in Theorem 6 for 312 and for 2010.

(2) Find all integers k and ℓ such that $k \log_{10} 2 + \ell \log_{10} 3 = \log_{10} 24$. What does this have to do with Theorem 6?

(3) For n a positive integer, prove that n is a square if and only if each prime occurs an even number of times in the factorization of n as a product of primes.

(4) Prove that if n is an integer ≥ 2 which is composite (i.e., not prime), then n has a prime divisor which is $\leq \sqrt{n}$.