| CS250: | D7 Answers: The Unique Factorization Theorem | Fall 2016 |
|---|---|---|

Recall that in the R21 Quiz we proved

**Fact 21:** Every natural number $n > 1$ is divisible by a prime number.

**Prop. 1:** Every positive natural number greater than 1 is equal to a product of primes:

$\forall n > 1\ \exists k, p_1, \ldots, p_k, i_1, \ldots, i_k \in \mathbf{Z}^+$ s.t., $p_1 < p_2 < \cdots < p_k$ are prime and $n = p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_k^{i_k}$.

**Proof:** Let $S = \{n \in \mathbf{N} \mid n > 1 \wedge$ n is not equal to a product of primes$\}$.

Assume for the sake of a contradiction that $S \neq \emptyset$. By the well-ordering of **N**, $S$ has a minimum element, $m = \min(S)$.

By Fact 21, $m$ is divisible by some prime number, $p$. Furthermore, since $m \in S$, we know that $m \neq p$. Thus, $1 < m/p < m$. Since $m$ was the least element of $S$, we have that $m/p \notin S$. Thus, $m/p$ is a product of primes. Thus, so is $m$. Thus, $m \notin S$. This is a contradiction. Thus, our assuption that $S \neq \emptyset$ is false. $\square$

**Lemma 1:** If $a|(b \cdot c)$ and $\gcd(a, b) = 1$ then $a|c$.

**Proof:** Assume that $a|(b \cdot c)$ and $\gcd(a, b) = 1$. Let $x, y \in \mathbf{Z}$ be s.t. $ax + by = 1$.

Let $d \in \mathbf{Z}$ be s.t. $ad = bc$. Thus, $ady = byc$. But $by = 1 - ax$.

Thus, $ady = (1 - ax) \cdot c$. Thus, $a(dy + xc) = c$, i.e,. $a|c$. $\square$

**Lemma 2:** If $p$ is prime and $p|(a \cdot b)$ then $p|a$ or $p|b$.

**Proof:** Suppose that $p|(a \cdot b)$. If $p \not| a$, then $\gcd(p, a) = 1$ and thus by Lemma 1, $p|b$. $\square$

**Unique Factorization Thm.** Every natural number $n > 1$ can be written in a unique way as a product of primes.

**Proof:** Suppose for the sake of a contradiction that there is a natural number greater than 1 which can be written in two different ways, and let $m$ be the minimum such number.

Thus $m = p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_k^{i_k} = p_1^{j_1} \cdot p_2^{j_2} \cdot \cdots \cdot p_k^{j_k}$ where $(1_1, \ldots, i_k) \neq (j_1, \ldots, j_k)$ and $p_1, \ldots, p_k$ are distinct primes. If for some $\ell$, $i_\ell$ and $j_\ell$ are both greater than 0, then $m/p_\ell$ is also expressible as a product of primes in two different ways, so $m$ was not the minimum. Thus $m = q_1 \cdots q_r$ is a product of primes not including $p_1$, and $p_1|m$.

By Lemma 2, since $p_1 \not| q_1$ we know that $p_1|(m/q_1)$. Thus, $(m/q_1) < m$ and can be written as a product of primes in two different ways – one involving $p_1$ and one not. This contradicts the fact that $m$ was the least such number. $\square$