CS250: D7: The Unique Factorization Theorem 11/2/16

As usual, you will join random groups of 4 according to the card you are given. Please work together in your groups to understand and solve today's problems. There will be a D7 moodle quiz for you to fill in your answers by Thursday night, 11 p.m.

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

Today, in your group, you will try to prove the The Unique Factorization Thm. Recall that in the R21 Quiz we proved that every natural number $n > 1$ is divisible by a prime number.

1. **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 $n = p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_k^{i_k}$.

   Prove Prop. 1. Hint: Let $S = \{n \in \mathbf{N} \mid n > 1 \wedge \text{ n is not equal to a product of primes}\}$. Assume for the sake of a contradiction that $S \neq \emptyset$. By the well-ordering of **N**, S has a minimum element, $m = \min(S)$. Derive a contradiction.

2. We know from Prop. 1, that every number greater than 1 can be written as a product of primes. We want to show that this can only be done in a unique way. So the problem, intuitively, is how do I know that $5 \cdot 13 \cdot 17 \cdot 23 \neq 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 19$?

   In order to prove that factorization is unique, the following lemma is helpful:

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

   The best way I know to prove Lemma 2 is to first prove:

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

   Prove Lemma 1. Hint: use Euclid's Algorithm: recall that $\gcd(a, b) = 1 \rightarrow \exists x, y \in \mathbf{Z}\ ax + by = 1$. Substitute $(1 - ax)$ for $b \cdot y$ in equation $a \cdot d \cdot y = b \cdot y \cdot c$.

3. Use Lemma 1 to prove Lemma 2.

4. Use Lemma 2 to prove the Unique Factorization Thm. Hint: let m be the least counterexample.