## LECTURE 20 EXCERCISE SOLUTIONS

**Problem.** 1: Prove that if $p, q$ are primes, and $p$ divides $q$, then $p = q$. (4 Points)

**Solution.** Consider $q$. Being prime, its divisors are only 1 and $q$. Since $p$ divides $q$, $p$ is a divisor of $q$. Therefore, either $p = 1$ or $p = q$. Since 1 is not prime, $p$ cannot equal 1, so we must have that $p = q$.

**Common Problems.** No serious complaints here. Again, clarity suffered from time to time. Some people are also still mixing up the definition of divides. If $a$ divides $b$, then there exists some number $k$ such that $b = ak$. *Not* that $a = bk$. Small issue, though, and everyone mostly had the right idea.

**Problem.** 2: Suppose that $p_1 \leq p_2 \leq ... \leq p_n$, and $q_1 \leq q_2 \leq ... \leq q_m$ are all prime numbers, such that $p_1p_2...p_n = q_1q_2...q_m$. Then prove that $p_n = q_m$, and hence that $p_1p_2...p_{n-1} = q_1q_2...q_{m-1}$. (4 Points)

**Solution.** Note that $p_n$ divides $q_1q_2...q_m$. Therefore, by Euclid's Lemma, $p_n$ divides one of the factors, so you know that $p_n$ divides $q_i$ *for some* $i$. You don't know which $i$, but you know that for some $i$, $p_n$ divides $q_i$. By the first problem, we therefore have that $p_n = q_i$, for that $i$. Since $q_i \leq q_m$, we have that $p_n \leq q_m$.

Applying the same argument on the other side, $q_m$ divides $p_1p_2...p_n$. Therefore, $q_m$ divides $p_r$ for some $r$. By the first problem, we have that $q_m = p_r$ for some $r$. $p_r \leq p_n$, therefore, $q_m \leq p_n$.

Combining the two, we have that $p_n = q_m$. Therefore, dividing each side appropriately, we have that $p_1p_2...p_{n-1} = q_1q_2...q_{m-1}$.

**Common Problems.** The biggest problem people had here was in the application of Euclid's Lemma. Many people applied Euclid's Lemma to say that since $p_n$ divides the product of the $q$'s, $p_n$ divides $q_m$. This is too bold. You know that $p_n$ divides one of the factors of the product of the $q$'s, but the lemma does not tell you which one. Variants of this included people asserting by similar means, that $p_1 = q_1$, and working their way up from there. Again, it's not something that you can conclude directly, without making some kind of size comparison as in the above proof.

Another very common approach was the following. Divide each side by the product of the $q$'s, and you get

$$\frac{p_1}{q_1}\frac{p_2}{q_2}...\frac{p_n}{q_m} = 1$$

Thus, each factor of $p_i/q_i$ had to be one, thus $p_i = q_i$ for all $i$. There are two main problems with this approach. Firstly, there is no justification as to why each of the $p_i/q_i$ had to be an integer, much less 1. (2/3)*(3/2) = 1, for instance. Again, you have to make a size argument, using what you're given about the orderings of the factors. The other problem with this is that it implicitly assumes that there are the same number of q's as there are p's - otherwise, you couldn't factor the whole thing into just terms of $p_i/q_i$. And you have no reason at all to imagine that $m = n$. It does, in fact, but it is something that needs to be proved itself.

**Problem.** 3: Prove that, for any number $a \geq 2$, the decomposition of $a$ into increasing prime factors is unique. Use WOP. (4 Points)

**Solution.** Let $S = \{a \in \mathbb{N} | a \geq 2$ and $a$ has at least two prime decompositions$\}$. This is clearly bound from below, so assume it is non-empty. By the WOP, we have that it has some smallest element $a$, with at least two distinct prime decompositions. Let $a = p_1p_2...p_n = q_1q_2...q_m$, such that the $p_i$ and the $q_i$ are increasing.

Note, however, by the previous problem, that we have that $p_n = q_m$, hence that $p_1p_2...p_{n-1} = q_1q_2...q_{m-1}$. If we then define $b = p_1p_2...p_{n-1} = q_1q_2...q_{m-1}$, we have that $b$ divides $a$, and $b < a$.

Since $b < a$, $b$ cannot be in $S$, since $a$ was the smallest element of $S$. Therefore, $b$ has a unique prime decomposition. Given that we have two decompositions of $b$, on in $p$, the other in $q$, the decompositions must in fact be equal. $m = n$, and $p_1 = q_1, p_2 = q_2, ...p_{n-1} = q_{n-1}$. However, going back to the decomposition of $a$, we also have that $p_n = q_m$. Hence, the decompositions of $a$ are equal - this is a contradiction!

Therefore, $S$ can have no smallest element, and every integer greater than or equal to 2 has a unique prime decomposition in this way.

**Common Problems.** Most people seemed to get the right idea about this problem. An altenative approach would be to apply the previous problem in some kind of inductive or iterative sort of way - take a number $a$ with two prime decompositions, apply problem 2 to say that $p_n = q_m$, and then apply it again to say that $p_{n-1} = q_{m-1}$, etc down the line. The problem is that you need to be more rigorous than 'etc down the line', and that is all the justification that was given by people who attempted this approach. Note the way that the approach taken here, using the smallest element of $S$, sort of short circuits any kind of itteration you might need.