Solutions to example assignment

Adam Sheffer

1. We first prove by induction that there are infinitely many primes. Specifically, we prove by induction on $k$ that there are more than $k$ prime numbers. The induction basis is straightforward for $k = 1$ since 2 and 3 are primes. For the induction step, consider any $k > 1$. By the induction hypothesis, there exist at least $k$ prime numbers. Denote the $k$ smallest primes as $p_1, p_2, \ldots, p_k$, and set $m = p_1 p_2 \cdots p_k + 1$. By definition, we see that $m$ is not divisible by any of $p_1, p_2, \ldots, p_k$. Thus, either $p_{k+1}$ is prime or there exists a number $m'$ divides $m$ and is not divisible by any of $p_1, p_2, \ldots, p_k$. Either way, there exists an additional prime number which completes the proof of the induction step.

Next, we prove by contradiction the prime decomposition property. Assume for contradiction that there exists an integer that is neither a prime nor a product of primes (and is larger than 1). Let $m$ be the smallest integer with these properties. Since $p$ is not prime, by definition it has divisors $q$ and $r$ with $p = qr$. By the minimality of $p$, each of $q$ and $r$ are either primes or are products of primes. This in turn implies that $p$ can be written as a product of primes, which is a contradiction.

2. Following the hint we write $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$. where $p_1, \ldots, p_k$ are distinct primes and $a_1, \ldots, a_k, b_1, \ldots, b_k$ are non-negative integers. 

We have $GCD(a, b) = p_1^{\min\{a_1, b_1\}} \cdots p_k^{\min\{a_k, b_k\}}$. This is indeed the $GCD$ since taking a higher power of some $p_i$ or multiplying by a new prime $q$ will result in a number that is no longer a divisor of both $a$ and $b$. Similarly, we have $LCM(a, b) = p_1^{\max\{a_1, b_1\}} \cdots p_k^{\max\{a_k, b_k\}}$. This is indeed the $LCM$ since taking a smaller power of some $p_i$ will result in a number that is no longer divisible both $a$ and $b$.

By the above, we have

$$a \cdot b = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}$$

$$= \left( p_1^{\max\{a_1, b_1\}} \cdots p_k^{\max\{a_k, b_k\}} \right) \left( p_1^{\min\{a_1, b_1\}} \cdots p_k^{\min\{a_k, b_k\}} \right) = LCM(a, b) \cdot GCD(a, b).$$