Supplement: Proving the uniqueness of prime factorizations

This supplement completes the proof of the FTA (Thm 1.13)

Proof (Uniqueness of prime factorization: Direct) Fix $n$ a natural. Let $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} = n = q_1^{l_1} q_2^{l_2} \ldots q_s^{l_s}$ be factorizations of $n$ with all of the notation as per the statement of the FTA. To prove the uniqueness of the factorization, we prove two things (in order) about these factorizations:

1. the lists of primes $p_1 < p_2 < \ldots < p_r$ and $q_1 < q_2 < \ldots < q_s$ associated with each of the factorizations agree; and
2. $k_1 = l_1, k_2 = l_2, \ldots, k_r = l_r$ (that is, the exponents attached to the primes are the same in each).

To prove (1), just assume that the two lists of primes differ somewhere (and we’ll try to reach a contradiction). We then have two cases to consider: either some $p_i$ is not in the list $q_1 < q_2 < \ldots < q_s$ or some $q_i$ is not in the list $p_1 < p_2 < \ldots < p_r$.

Case 1: $p_i$ is not in the list $q_1 < q_2 < \ldots < q_s$. But $p_i | n$, and so $p_i | q_1^{l_1} q_2^{l_2} \ldots q_s^{l_s}$. However, by exercises 1.5.1 and 1.4.5, $(p_i, q_i) = 1$. Thus $p_i | q_2^{l_2} \ldots q_s^{l_s}$ by exercise 1.2.4. Continuing in this way, we eventually get $p_i | q_r^{l_r}$. With this $(p_i, q_r^{l_r}) = p_i$ by the definition of the greatest common divisor. However, we know $(p_i, q_r^{l_r}) = 1$ by exercises 1.5.1 and 1.4.5. Thus $p_i = 1$, which is not prime.

Case 2: $q_i$ is not on the list $p_1 < p_2 < \ldots < p_r$. But $q_i | p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. As in the last case, this gives rise to another contradiction concerning $q_i$.

Since both cases give rise to contradictions, it must be that every prime on the list $p_1 < p_2 < \ldots < p_r$ is also on the list $q_1 < q_2 < \ldots < q_s$, and, conversely, every prime on the list $q_1 < q_2 < \ldots < q_s$ is on the list $p_1 < p_2 < \ldots < p_r$. This tells us that the two lists of primes are really the same. In particular this means $r = s$. That is, we now know our factorizations are $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} = n = p_1^{l_1} p_2^{l_2} \ldots p_r^{l_r}$.
We can now turn to part (2) of the proof. Just suppose that the exponents attached to the individual primes don’t all agree. As above, let \( i \) denote the first time they fail to agree. That is, let

\[ k_1 = l_1, \quad k_2 = l_2, \ldots \quad \text{and} \quad k_{i} = l_{i} \quad \text{but} \quad k_{i} \neq l_{i}. \]

**Case 1:** \( k_{i} < l_{i} \). So \( 1 \leq l_{i} - k_{i} \). Using some common rules of exponential notation we have

\[ p_{i}^{k_{1}} p_{2}^{k_{2}} \cdots p_{r}^{k_{r}} = p_{i}^{l_{1}} p_{2}^{l_{2}} \cdots \]

canceling common factors from both sides of these expressions (don’t forget, \( k_{1} = l_{1}, \quad k_{2} = l_{2}, \ldots \quad \text{and} \quad k_{i} = l_{i} \) we have

\[ p_{i}^{k_{i}} \cdots p_{r}^{k_{r}} = p_{i}^{l_{i}} \cdots p_{r}^{l_{r}} \]. So \( p_{i} | p_{i}^{k_{i}} \cdots p_{r}^{k_{r}} \). As we have seen in part (1) of the proof, this will lead us to the statement \( p_{i} | p_{r}^{k_{r}} \). The only way to avoid a contradiction is to have \( i = r \) (that is, all the exponents agree until the last one). However, if this is true then we have

\[ p_{1}^{k_{1}} p_{2}^{k_{2}} \cdots p_{r}^{k_{r}} = n = p_{1}^{l_{1}} p_{2}^{l_{2}} \cdots p_{r}^{l_{r}} \].

Canceling under this condition would give \( 1 = p_{r}^{l_{r}} \). So \( p_{r} > 1 \). But \( p_{r} \) is prime, and thus \( p_{r} > 1 \). This final contradiction tells us that \( k_{i} \) cannot be less than \( l_{i} \).

**Case 2:** \( l_{i} < k_{i} \). See the last case.

Since both cases give rise to contradictions, it must be that all of the exponents agree. This uniqueness argument completes the proof of the FTA (Thm 1.13).