2.9 Theorem (Fundamental Theorem of Arithmetic - Uniqueness Part). Let n be a natural number. Let $\{p_1, p_2, ..., p_m\}$ and $\{q_1, q_2, ..., q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, ..., r_m\}$ and $\{t_1, t_2, ..., t_s\}$ be sets of natural numbers such that

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} ... p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} ... q_s^{t_s}. \end{aligned}$$

Then $m = s$ and $\{p_1, p_2, ..., p_m\} = \{q_1, q_2, ..., q_s\}$. That is, the sets of primes are equal but their elements are not necessarily listed in the same order; that is, p_i may or may not equal q_i. Moreover, if $p_i = q_j$ then $r_i = t_j$.

Proof. Let n be a natural number. Let $\{p_1, p_2, ..., p_m\}$ and $\{q_1, q_2, ..., q_s\}$ be sets of primes with $p_i \neq p_j$ if $i \neq j$ and $q_i \neq q_j$ if $i \neq j$. Let $\{r_1, r_2, ..., r_m\}$ and $\{t_1, t_2, ..., t_s\}$ be sets of natural numbers be given such that

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} ... p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} ... q_s^{t_s}. \end{aligned}$$

Suppose not. That is, let the prime factorizations be different such that $m \neq s$. Suppose we canceled out all common prime factors by dividing. For simplicity, the naming convention will be the same but the two sets have no matching prime with each other such that

$$p_1^{r_1} p_2^{r_2} ... p_m^{r_m} = q_1^{t_1} q_2^{t_2} ... q_s^{t_s}.$$

Let k be the product of all but one of the primes on the left hand side and call that prime p such that

$$pk = q_1^{t_1} q_2^{t_2} ... q_s^{t_s}.$$

By Lemma 2.8, $p = q_i$. This means that all of the primes on one side have a matching prime on the other side, which contradicts our assumption above. Thus, $m = s$ such that every natural number has a unique prime factorization.

Moreover, since $p_i = q_j$, then $r_i = t_j$. By contradiction, suppose $p_i = q_j$ and $r_i \neq t_j$ with $r_i > t_j$. Since $r_i > t_j$, let $r_i = t_j + r_i$ such that $p_i^{r_i} = p_i^{t_j} p_i^{r_i - t_j}$. Thus,

$$p_1^{r_1} p_2^{r_2} ... p_i^{t_j} p_i^{r_i - t_j} ... p_m^{r_m} = q_1^{t_1} q_2^{t_2} ... q_j^{t_j} ... q_s^{t_s}.$$

Notice $p_i^{t_j}$ and $q_j^{t_j}$ have the same exponent. Since $p_i = q_j$, we can divide and cancel those factors from each side such that

$$p_1^{r_1} p_2^{r_2} ... p_i^{r_i - t_j} ... p_m^{r_m} = q_1^{t_1} q_2^{t_2} ... q_s^{t_s}.$$

Notice the left hand side has an extra factor. This contradicts the Fundamental Theorem of Arithmetic. Thus, if $p_i = q_j$, then $r_i = t_j$. $\square$