Theorem 2.10 is the Fundamental Theorem of Arithmetic: "unique prime factorization" for integers greater than one. The prime factorization in Theorem 2.10 allows repetition of primes rather than prime powers.

Example. $480 \;=\; 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 5.$

Corollary 2.11 rewrites the unique prime factorization using positive integer powers of distinct primes instead of repeating primes.

Example. $480 \;=\; 2^5\cdot 3^1\cdot 5^1.$

As is discussed in the paragraphs between Corollary 2.11 and Lemma 2.12, it is often helpful to allow the exponents of the primes in a prime factorization to be zero. When we allow this, we lose the *uniqueness* of the prime factorization.

Example. $480 \;=\; 2^5\cdot 3^1\cdot 5^1 \;=\; 2^5\cdot 3^1\cdot 5^1\cdot 7^0.$

Notice that the number one does not have a prime factorization as described in Theorem 2.10 or Corollary 2.11. However, once we allow the primes in the factorization to have zero as an exponent, we can write a trivial sort of prime factorization for one: for any list of primes $p_1,\dots,p_n$ that we choose, $1 = p_1^0\cdot\dots\cdot p_n^0$.

Fact. (Simple consequence of Corollary 2.11.) *For an integer $a \ge 1$, if*

$$a = p_1^{e_1}\dots p_n^{e_n}\ ,$$

for distinct primes $p_1,\dots,p_n$ and nonnegative (so, possibly zero) integer exponents $e_1,\dots,e_n$, and if

$$a = p_1^{f_1}\dots p_n^{f_n}\ ,$$

for some nonnegative integer exponents $f_1,\dots,f_n$, then $e_i = f_i$ for all $1 \le i \le n$.

In this prime factorization, we allow zero as an exponent for a prime, to allow primes that are not divisors of a to appear in the factorization. In particular, this means that, as long as a list of primes includes all the prime factors of a, we can write a prime factorization for a in terms of the primes in our list, and the exponents for the primes are uniquely determined.

Definition/Fact. For a positive integer a and a prime p, the exponent of the highest power of p dividing a is called the **p-adic order** of a and denoted $\mathcal{O}_p(a)$. In other words $\mathcal{O}_p(a) = e$ means $p^e|a$ but $p^{e+1}\nmid a$. If we write a in the form

$$a = p_1^{e_1}\dots p_n^{e_n}\ ,$$

where $p_1,\dots,p_n$ are distinct primes and $e_1,\dots,e_n$ are nonnegative integers (possibly zero), and if $p = p_i$ for some i, then $\mathcal{O}_p(a) = \mathcal{O}_{p_i}(a) = e_i$.

Example. $480 \;=\; 2^5\cdot 3^1\cdot 5^1\cdot 7^0.$

- $2^0|480,\ \ 2^1|480,\ \ 2^2|480,\ \ 2^3|480,\ \ 2^4|480,$ and $2^5|480,$ but $2^6\nmid 480$, so $\mathcal{O}_2(480) = 5$.
- $3^0|480$, and $3^1|480$, but $3^2\nmid 480$, so $\mathcal{O}_3(480) = 1$.
- $5^0|480$, and $5^1|480$, but $5^2\nmid 480$, so $\mathcal{O}_5(480) = 1$.
- $7^0|480$, but $7^1\nmid 480$, so $\mathcal{O}_7(480) = 0$.
- Similarly, for any prime $p > 7$, $\mathcal{O}_p(480) = 0$.