where the p_is and q_is are all prime, $p_1 \le p_2 \le \ldots \le p_k$ and $q_1 \le q_2 \le \ldots \le q_l$, then

$$k = l \quad \textit{and} \quad p_i = q_i \quad \textit{for all } i = 1, \ldots, k \ .$$

The point about specifying that $p_1 \le p_2 \le \ldots \le p_k$ is that this condition determines the order in which we write down the primes in the factorization of n. For example, 28 can be written as a product of primes in several ways: $2 \times 7 \times 2$, $7 \times 2 \times 2$ and $2 \times 2 \times 7$. But if we specify that the prime factors have to increase or stay the same, then the only factorization is $28 = 2 \times 2 \times 7$.

PROOF Part (I) is just Proposition 8.1.

Now for the uniqueness part (II). We prove this by contradiction. So suppose there is some integer n which has two different prime factorizations, say

$$n = p_1 \ldots p_k = q_1 \ldots q_l$$

where $p_1 \le p_2 \le \ldots \le p_k$, $q_1 \le q_2 \le \ldots \le q_l$, and the list of primes $p_1, \ldots, p_k$ is not the same list as $q_1, \ldots, q_l$.

Now in the equation $p_1 \ldots p_k = q_1 \ldots q_l$, cancel any primes that are common to both sides. Since we are assuming the two factorizations are different, not all the primes cancel, and we end up with an equation

$$r_1 \ldots r_a = s_1 \ldots s_b \ ,$$

where each $r_i \in \{p_1, \ldots, p_k\}$, each $s_i \in \{q_1, \ldots, q_l\}$, and none of the r_is is equal to any of the s_is (i.e., $r_i \ne s_j$ for all i, j).

Now we obtain a contradiction. Certainly r_1 divides $r_1 \ldots r_a$, hence r_1 divides $s_1 \ldots s_b$. By Proposition 11.6, this implies that $r_1 | s_j$ for some j. However, s_j is prime, so its only divisors are 1 and s_j, and hence $r_1 = s_j$. But we know that none of the r_is is equal to any of the s_is, so this is a contradiction. This completes the proof of (II). ∎

Of course, in the prime factorization given above in part (I) of Theorem 12.1, some of the p_is may be equal to each other. If we collect these up, we obtain a unique prime factorization of the form

$$n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} \ ,$$

where $p_1 < p_2 < \ldots < p_m$ and the a_is are positive integers.

Some Consequences of the Fundamental Theorem

First, here is an application of the Fundamental Theorem of Arithmetic that looks rather more obvious than it really is.

PROPOSITION 12.1

Let $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, where the p_is are prime, $p_1 < p_2 < \ldots < p_m$ and the a_is are positive integers. If m divides n, then

$$m = p_1^{b_1} p_2^{b_2} \ldots p_m^{b_m} \quad \textit{with} \quad 0 \le b_i \le a_i \quad \textit{for all } i \ .$$

For example, the only divisors of $2^{100}3^2$ are the numbers $2^a 3^b$, where $0 \le a \le 100, 0 \le b \le 2$.

PROOF If $m|n$, then $n = mc$ for some integer c. Let $m = q_1^{e_1} \ldots q_k^{e_k}$, $c = r_1^{d_1} \ldots r_l^{d_l}$ be the prime factorizations of m, c. Then $n = mc$ gives the equation

$$p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} = q_1^{e_1} \ldots q_k^{e_k} r_1^{d_1} \ldots r_l^{d_l} \ .$$

By the Fundamental Theorem 12.1, the primes, and the powers to which they occur, must be identical on both sides. Hence, each q_i is equal to some p_j, and its power e_i is at most a_j. In other words, the conclusion of the proposition holds. ∎

We can use this to prove some further obvious-looking facts about integers. Define the *least common multiple* of two positive integers a and b, denoted by $lcm(a,b)$, to be the smallest positive integer that is divisible by both a and b. For example, $lcm(15,21) = 105$.

PROPOSITION 12.2

Let $a, b \ge 2$ be integers with prime factorizations

$$a = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}, \quad b = p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$$

where the p_i are distinct primes and all $r_i, s_i \ge 0$ (we allow some of the r_i and s_i to be 0). Then

(i) $hcf(a,b) = p_1^{\min(r_1,s_1)} \ldots p_m^{\min(r_m,s_m)}$

(ii) $lcm(a,b) = p_1^{\max(r_1,s_1)} \ldots p_m^{\max(r_m,s_m)}$

(iii) $lcm(a,b) = ab/hcf(a,b)$.