Coprime

Continue proof of existence

We have constructed e_p for each prime number p so that $p^{e_p} \mid n$ and have seen that what remains to show is

$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

We have constructed e_p for each prime number p so that $p^{e_p} \mid n$ and have seen that what remains to show is

$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

For this, we need a lemma:

Lemma 2.2.4

Let a, b, n be integers. If $a \mid n$, $b \mid n$, and $\gcd(a, b) = 1$, then $ab \mid n$.

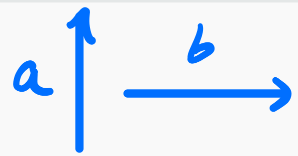
Proof. Since $a \mid n$, $b \mid n$, by the defining property of the least common multiple, $\operatorname{lcm}(a, b) \mid n$. We have $\operatorname{lcm}(a, b) = ab$ since $\gcd(a, b) = 1$. $\square$

Coprime

Definition 2.2.5

Two integers a, b are called *coprime* if $\gcd(a, b) = 1$.

Think this as analogy of being orthogonal.



Example 2.2.6

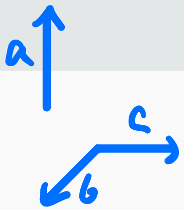
Two distinct primes p, q are coprime.

Proof. Indeed, since the divisors of p are $1, p$, while the divisors of q are $1, q$, the only common divisor of p, q is 1. $\square$

Coprime

Lemma 2.2.7

Let a, b, c be integers. If a, b are coprime and a, c are coprime, then a, bc are coprime.



Think this as analogy of "if $a \perp b$ and $a \perp c$, then $a \perp b + c$".

Proof. Suppose $\gcd(a, bc) = g$. Let p be the smallest divisor of g other than 1. Then p has to be a prime number, otherwise it will have another divisor $d > 1$, which is also a divisor of g by the transitivity, but this contradicts to the minimality of p. Now, since $p \mid bc$, by the fundamental property of prime, we have either $p \mid b$ or $p \mid c$. But we also have $p \mid a$. Hence, p is a common divisor of either a, b or a, c, which contradicts to $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. $\square$

We need to show
$$\prod_{p \text{ is prime}} p^{e_p} \mid n.$$

Let $p_1, \cdots, p_s$ be all the prime divisors of n. By example 2.2.6, any two of $p_1, \cdots, p_s$ are coprime to each other. Apply lemma 2.2.7 to them, we see that any two of $p_1^{e_{p_1}}, \cdots, p_s^{e_{p_s}}$ are coprime to each other.

By lemma 2.2.4, $p_1^{e_{p_1}} p_2^{e_{p_2}} \mid n$ and by lemma 2.2.7, $p_1^{e_{p_1}} p_2^{e_{p_2}}$ is coprime to $p_3^{e_{p_3}}$. Repeat this, we see that $p_1^{e_{p_1}} \cdots p_s^{e_{p_s}} \mid n$. $\square$