Theorem. *Every composite number has a prime divisor not greater than its square root.*

Proof. Let n be a composite number. We can write $n = ab$ for some integers a and b with $1 < a \leq b < n$. Suppose $a > \sqrt{n}$, then we would have $b > \sqrt{n}$ making $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$, a contradiction. Hence we must have $a \leq \sqrt{n}$.

Now, by the Lemma below, a is divisible by some prime, p, and therefore p divides a. Since $p \leq a \leq \sqrt{n}$, it follows that n has a prime divisor not greater than $\sqrt{n}$. □

Lemma. *Every integer greater than 1 is divisible by some prime.*

Proof. We use strong mathematical induction. The basis of the induction holds because 2 is divisible by 2 and 2 is a prime.

Let the induction hypothesis be the assumption that every number in the set $\{2, 3, 4, \ldots, n\}$ is divisible by some prime. Now consider the next integer $n + 1$. We want to show that $n + 1$ is also divisible by some prime.

If $n + 1$ is prime then we are done as it is divisible by the prime $n + 1$. Otherwise $n + 1$ is composite and $n + 1 = r \cdot s$ for some integers r and s with $2 \leq r \leq n$. By the induction hypothesis, r is divisible by some prime, p, and since p divides r and r divides $n + 1$, then p divides $n + 1$. In either case, $n + 1$ is divisible by some prime and the result follows. □

This work is licensed under Creative Commons Attribution-NoDerivatives 4.0 International. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/4.0/

©David Ireland DI Management https://di-mgt.com.au/ (July 17, 2026).