Prime Number.

has possible number of factor.

1. Definition: A prime number is a natural number greater than 1 whose only natural number divisors are 1 and itself.

1). A composite number is a number $m>1$ and has divisors other than 1 and m.

2. Theorem:

1). 1.1.3: Let m be a natural number other than 1. If m does not have a natural number divisor that is greater than 1 and no larger than the square root of m, then it's prime.

$\forall m \in \mathbb{N}.\ m>1,\ (\forall k \in \mathbb{N}.\ 1<k\le\sqrt{m},\ k \nmid m) \Rightarrow m$ is prime.

proof: $\neg Q \Rightarrow \neg P$, which. Assume m is not prime.

WTS: $\exists k \in \mathbb{N}.\ 1<k\le\sqrt{m},\ k \mid m$.

Since $m \in \mathbb{N}.\ m>1$, m has a prime divisor. from 1.1.4.

Since m is not a prime. $\exists q_1, q_2 \in \mathbb{N}.\ q_1 \neq 1.\ q_1 \neq m,\ q_2 \neq 1,\ q_2 \neq m.$

$q_1 \cdot q_2 = m$.

Since $q_1 \mid m$, $q_2 \mid m$. gives $q_1 \le m$, $q_2 \le m$.

Since $q_1 \neq m$. $q_2 \neq m$. gives. $q_1 < m$, $q_2 < m$.

① $q_1 > \sqrt{m}$.

Since $q_2 \in \mathbb{N}$. $q_1 \cdot q_2 > \sqrt{m} \cdot q_2$, and $q_1 \cdot q_2 = m$. gives. $m > \sqrt{m} q_2$.

From cancellation. gives. $\sqrt{m} > q_2$. where $q_2 \mid m$.

② $q_2 > \sqrt{m}$.

.....

2). 1.1.4.: Every natural number greater than 1 has a prime divisor.

Three Proof.

① $\mathbb{N}>1$ $\begin{cases} \text{prime: factor} = 1 \text{ or } n \\ \text{composite} \end{cases}$ → prime.

composite: prime factorization → n = product form of primes

② Given $n>1$, the smallest number $k>1$ that divides n must be a prime.

Let $n>1$. Let k be the smallest number $k>1$ that $k|n$.
WTP. k is a prime. Assume contradiction k is a composite.
Since $k|n$. gives. $\exists q \in \mathbb{N}.\ k \cdot q = n$.
Since k is a composite num. $\exists q_1, q_2 \in \mathbb{N}$, s.t. $q_1 \neq 1, q_1 \neq k. q_2 \neq 1. q_2 \neq k.$
$q_1 \cdot q_2 = k$.
Since $q_1 | k$, from the property of divisibility, $q_1 \leq k$.
Since $q_1 \neq k$, $q_1 < k$.
$\exists q' = q_2 \cdot q.\ q' \in \mathbb{N}$, $k \cdot q = q_1 \cdot q_2 \cdot q = q_1 \cdot q' = n$. gives $q_1 | n$.
which $q_1 < k$, contradicts. to k is the smallest number that divides n.

③ Given $n>1$, consider the set $A = \{m \in \mathbb{N}.\ 1<m$ and $m|n\}$.
WTS: the smallest element of A, if exists, must be a prime divisor of n.

Since for any $n \in \mathbb{N}$, $n>1$, gives $1|n$ and $n|n$, which.
n must be in A, A is non-empty and $A \subseteq \mathbb{N}$.
From WOP. gives. $\exists m' \in A, \forall m'' \in A, m' \leq m''$, which $m'>1$ and $m'|n$.
(follows the similar procedure as ②).

3).1.1.5.: There is no largest prime number.

★4).2.2.4.: Every natural number other than 1 is a product of prime numbers.

WTS: $\forall n \in \mathbb{N}.\ n > 1 \Rightarrow n = p_1 \cdot p_2 \cdots p_k$ where $k \in \mathbb{N}$, p_i are prime $\forall i \in \{1, 2, \ldots, k\}$

$P(n)$: $n = p_1 \cdot p_2 \cdots p_k$ where $k \in \mathbb{N}$, p_i are prime $\forall i \in \{1, 2, \ldots, k\}$

$S = \{x \in \mathbb{N} \mid P(n)\}$.

Base Case: $n = 2$.

Since 2 is a prime number, I've proved B.C is T.

Induction Step. Let $n \in \mathbb{N}$. $n \geq 2$.

Induction Hypothesis. $\forall t \in \mathbb{N}.\ 2 \leq t \leq n.\ P(k)$.

WTS: $P(n+1)$.

① $n+1$ is prime.

Since $n+1$ is a prime, it's a product of prime numbers.

② $n+1$ is composite.

From definition of composite number, $\exists x, y \in \mathbb{N}.\ 1 < x, y < n+1$.

$n+1 = x \cdot y$.

Since $x, y \in \mathbb{N}.\ 1 < x, y < n+1$. gives $2 \leq x \cdot y \leq n$. which. from I.H.

$x = p_1 \cdot p_2 \cdots p_k$, $y = q_1 \cdot q_2 \cdots q_e$, where $q_1, q_2, \ldots, q_e, p_1, p_2, \ldots, p_k$ are prime.

$n+1 = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot q_2 \cdots q_e$, which is a product of prime.

$\therefore n+1 \in S$.

■