"Every no $n > 1$ can be expressed as a product of primes in one & only way (except for order).

$4 = 2 \cdot 2 = 2^2$
$12 = 4 \cdot 3 = 2^2 \cdot 3^1$.
product of primes.

Proof

Let n be any natural number > 1.

So n must have atleast one prime factor (p_1).

$\exists$ n_1 such that $n = p_1 n_1$ where $n > n_1$. — (1)

If $n_1 = 1$, $n = p_1$. ($n_1 \in \mathbb{N}$)
↳ prime factor.
Hence proved if $n_1 = 1$.

If $n_1 > 1$, So n_1 has atleast one prime factor p_2.
$\exists$ n_2 such that $n_1 = p_2 \cdot n_2$ where $n_1 > n_2$ — (2)

Put (2) in (1).

$n = p_1 \cdot p_2 \cdot n_2$. — (3)

If $n_2 = 1$, $n = p_1 \cdot p_2$.
product of primes.
Hence proved if $n_2 = 1$.

If $n_2 > 1$, So n_2 has atleast one prime factor (p_3)
$\exists$ n_3 such that $n_2 = n_3 \cdot p_3$ where $n_2 > n_3$ — (4)

$\therefore n = p_1 \cdot p_2 \cdot p_3 \cdot n_3$ where $n > n_1 > n_2 > n_3$.

As n is finite & $n > n_1 > n_2 > n_3$, this process ends after a finite no. of steps.

$\therefore n = p_1 \cdot p_2 \cdot p_3 \cdots p_k \cdot n_k$.
where $n_k = 1$.
$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$.
product of primes.

Uniqueness

$n = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_k$ — (1).

If possible $\exists$ a set of primes
$q_1, q_2, q_3 \cdots q_l$ such that —
$n = q_1 \cdot q_2 \cdot q_3 \cdots q_l$ — (2)

To. $k = l$ & each p_i = some q_j

from ① & ②

$P_1 \cdot P_2 \cdot P_3 \cdots P_k = q_1 q_2 q_3 \cdots q_l$.

Sol—

$P_1 (P_2 \cdot P_3 \cdots P_k) = q_1 q_2 q_3 \cdots q_l$

by defn of divisibility,

by defn of divisibility

$a \mid b$ Then $b = ac$

$P_1 \mid q_1 q_2 q_3 \cdots q_l$

$\Rightarrow$ Either $P_1 = 1$ (or) $P_1 = q_j$'s.

P_1 divides atleast one q_j's.

Without loss of Generality $P_1 \mid q_1$.

either $P_1 \neq 1$ (or) $P_1 = q_1$.

$P_1 \neq 1$ (prime)

Hence $P_1 = q_1$.

Hence.

$P_1 P_2 \cdots P_k = P_1 q_2 q_3 \cdots q_l$.

$P_2 P_3 \cdots P_k = q_2 q_3 \cdots q_l$.

Similarly

$P_2 (P_3 \cdots P_k) = q_2 q_3 \cdots q_l$

By defn of divisibility.

$P_2 \mid q_2 q_3 \cdots q_l$.

$\Rightarrow$ P_2 divides atleast one q_j

Without loss of Generality $P_2 \mid q_2$.

Then. $P_2 = 1$ or $P_2 = q_2$.

$P_2 \neq 1 \Rightarrow P_2 = q_2$.

Then

$P_3 \cdots P_k = q_3 \cdots q_l$.

Continuing, $P_1 = q_1$ $P_2 = q_2$ $P_3 = q_3 \cdots P_k = q_k$.

Let $k < s$

Then $1 = q_k$

upto q_k, $p_1 \cdot q_2 \ldots\ldots$

$1 = \underbrace{q_{k+1} q_{k+2} \ldots\ldots q_s}_{(s-k)}$.

Hence 1 is product of $(s-k)$ prime numbers

A Contradiction

not possible.

Thus $k \nless t$

Hence similarly $k > t$. not possible.

Thus $\boxed{k > t}$.

Lemma 1 (Euclids) If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Lemma 2 Let p be a prime and $p \mid a_1 a_2 \cdots a_n$ where $a_1, a_2, \ldots, a_n$ are +ve integers then $p \mid a_i$ for some i when $1 \le i \le n$.

Proof (week induction)

When $n = 1$ Result follows

So assume it is true for an arbitrary positive integer k.

If $p \mid a_1 a_2 \cdots a_k$ then $p \mid a_i$ for some i.

Suppose $p \mid a_1 a_2 \cdots a_{k+1}$ that is $p \mid (a_1 a_2 \cdots a_k) a_{k+1}$

Then by Euclid's lemma,

$p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$

If $p \mid a_1 a_2 \cdots a_k$ then $p \mid a_i$ for some i

$1 \le i \le k$.

Thus $p \mid a_i$ when $1 \le i \le k$ or $p \mid a_{k+1}$.