Claim:

Any integer $n$ can be factored into a product of primes, possibly trivial, i.e. $n$ is itself prime.

Proof: by induction on $n$.

Base case: Show true when $n=1$.

- $N=1$: yes - is prime
- $N=2$: yes - is prime
- $N=3$: yes - is prime
- $N=4$: yes - 2, 2 product of primes
- $N=5$: yes
- $N=6$: yes - 2, 3
So the hypothesis is true if \( n \) with 
\[ \forall \, n \leq 6. \]

So now assume true 
\[ \forall \, n \leq N - 1 \]

\[ \text{ie } n \text{ can be written as a product of primes} \]
and look at \( N \).

if \( N \) is prime, we're done.

otherwise \( N = ab \) for integers \( 1 < a, b \) (hence \( a, b \leq N-1 \))

by induction hypothesis

\( a \) and \( b \) are both products of primes

Thus \( N \) is a product of primes.
Side note: two "flavors" of induction

Both start with a base case

Flavor 1

assume true for \( N - 1 \)

\* show true for \( N \)

Flavor 2

assume true for all \( n \leq N - 1 \)

and show true for \( n = N \)
Claim:

If \( n = p_1 \cdots p_r \) is a factorization of \( n \) into primes, then any other factorization is just a reordering.
Proof:
suppose \( n = g_1 \cdot g_2 \cdots \cdot g_s \)

for primes \( g_i \).

Then
\[
T_{g_2} \cdots T_{g_s} = g_1 \cdot \cdots \cdot g_s
\]

so since \( p_i \mid \) left-hand side

Then \( p_i \mid g_1 \cdot \cdots \cdot g_s \)

\[\therefore p_i \mid g_i \text{ for some } i\]

but the \( g_i \)'s are prime, \( \therefore p_i = g_i \text{ for some } i \).

So reorder the \( g_i \)'s to make it the first one.
Thus

\[ \Phi_1 \Phi_2 \Phi_3 \ldots \Phi_r = \Phi_{\Phi_2 \Phi_3 \ldots \Phi_r} \]

so \[ \Phi_2 \ldots \Phi_r = \Phi_{\Phi_2 \Phi_3 \ldots \Phi_r} \]

\[ p_2 \mid \Phi_2 \ldots \Phi_r \]

so \[ p_2 \mid \Phi_{\Phi_2 \Phi_3 \ldots \Phi_r} \]

\[ p_2 \mid \Phi_{\Phi_2 \Phi_3 \ldots \Phi_r} \] for some

Assume the first
Thus

\[ p_2 \ p_3 \ \cdots \ p_r = p_2 \ q_3 \ \cdots \ q_s \]

\[ p_3 \ \cdots \ p_r = q_3 \ \cdots \ q_s \]

\text{etc.}

Thus \[ p_1 \ \cdots \ p_r = q_1 \ \cdots \ q_s \]

\((r \text{ must }= s)\) \(\text{ up to reordering.}\)
This means that any

\[ N = \prod_i \alpha_i \]

Right now -

Suppose \( M = \prod_i \beta_i \), \( N = \prod_i \alpha_i \)

What is \( \gcd(M, N) \), \( \text{lcm}(M, N) \)