The Unique Prime Factorization Theorem  For every positive integer there is a unique bag of primes whose product equals that integer. The fact that there is a bag of primes corresponding to every positive integer is readily proven using induction. We prove the uniqueness part in this note.

Notation  Henceforth, lower case letters like $p$ and $q$ denote primes, and upper case ones, such as, $S$ and $T$ denote finite bags of primes. We write $\overline{S}$ for the product of the elements of $S$, and $(p \mid S)$ for “$p$ divides $S$”. By convention, $\phi = 1$; thus the unique bag corresponding to 1 is $\phi$.

Lemma  $p \mid \overline{S} \Rightarrow p \in S$.
Proof: Proof is by induction on the size of $S$.

- $S = \phi$: Then, $p \mid \overline{S}$ does not hold for any prime $p$; hence, $p \mid \overline{S} \Rightarrow p \in S$ holds vacuously.

- $S = R \cup \{q\}$, for some $R$ and $q$: we have to show that for any prime $p$, $p \mid \overline{S} \Rightarrow p \in S$. This holds trivially if $p = q$. For $p \neq q$, i.e., if $p$ and $q$ are distinct primes, we employ Euclid’s theorem:

There exist integers $a$ and $b$ such that $ap + bq = 1$.

\[
\begin{align*}
  p & \mid apR, \text{ arithmetic} \\
  p & \mid bqR, \text{ $p \mid \overline{S}$ and $\overline{S} = qR$} \\
  p & \mid (ap + bq)R, \text{ from above two} \\
  p & \mid R, \text{ $ap + bq = 1$} \\
  p & \in R, \text{ induction hypothesis} \\
  p & \in S, \text{ $R \subseteq S$}
\end{align*}
\]

Theorem  $\overline{S} = \overline{T} \Rightarrow S = T$
Proof: For any $p$,

\[
\begin{align*}
  p & \in S \\
  \Rightarrow & \quad \{\text{definition of } \overline{S}\} \\
  p & \mid \overline{S} \\
  \Rightarrow & \quad \{\overline{S} = \overline{T}\} \\
  p & \mid \overline{T} \\
  \Rightarrow & \quad \{\text{from the Lemma}\} \\
  p & \in T
\end{align*}
\]

Therefore, $S \subseteq T$. Similarly, $T \subseteq S$. So, $S = T$. 

Alternate Proof due to J Moore Moore gives the following proof of

\[ p \mid ab \Rightarrow (p \mid a) \vee (p \mid b) \]

where \( a \) and \( b \) are positive integers, and \( p \) is prime.

Assume \( \neg(p \mid a) \). Since \( p \mid ab \), \( pc = ab \), for some \( c \).

\[
c = \begin{cases} 
\text{from } \neg(p \mid a) \text{ and } p \text{ prime, } \gcd(p,a) = 1 \\
\times \gcd(p,a) 
\end{cases}
\]

\[
= \begin{cases} 
\text{multiplication distributes over } \gcd \\
\gcd(pc, ac) 
\end{cases}
\]

\[
= \begin{cases} 
\text{identity} \\
\gcd(ab, ac) 
\end{cases}
\]

\[
= \begin{cases} 
\text{multiplication distributes over } \gcd \\
a \times \gcd(b, c) 
\end{cases}
\]

From \( c = a \times \gcd(b, c) \),

\[
\Rightarrow \begin{cases} 
pc = p \times a \times \gcd(b, c) \\
\text{Cancellation, } a \neq 0 \\
b = p \times \gcd(b, c) 
\end{cases}
\]

\[
\Rightarrow \begin{cases} 
\text{definition} \\
p \mid b 
\end{cases}
\]