**Unique Prime Factorization Theorem**
**Jayadev Misra**
2/4/2006, corrected 4/3/2022

**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. I 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 $\Pi\ S$ for the product of the elements of $S$, and $(p \mid \Pi\ S)$ for "$p$ divides $\Pi\ S$ ". By convention, $\Pi\phi = 1$; thus the unique bag corresponding to 1 is $\phi$.

**Lemma 1** $p \mid \Pi\ S \ \equiv\ p \in S$.
Proof: It is easy to see the proof in one direction: $p \in S \Rightarrow p \mid \Pi\ S$. I prove $p \mid \Pi\ S \ \Rightarrow\ p \in S$, i.e. every prime divisor of a positive integer is in every factorization bag of it, by induction on the size of $S$.

- $S = \{\}$: Then, $p \mid \Pi\ S$ is *false* for every prime $p$, and the hypothesis is true vacuously.
- $S = T \cup \{q\}$, for some bag of primes $T$ and prime $q$: If $p = q$ then $p \in S$, so the result holds trivially. For $p \neq q$ employ Bézout's identity: for any pair of positive integers $m$ and $n$ there exist integers $a$ and $b$ such that $a.m + b.n = \gcd(m, n)$. Using $p$ and $q$ for $m$ and $n$, respectively, and noting that $\gcd(p, q) = 1$ for distinct primes, we have $a.p + b.q = 1$ for some $a$ and $b$.

$$
\begin{array}{ll}
 & p \mid \Pi\ S \\
\Rightarrow & \{p \mid a.p.\Pi\ T \text{ and } p \mid \Pi\ S.\ \text{So, } p \mid (a.p.\Pi\ T + b.\Pi\ S)\} \\
 & p \mid (a.p.\Pi\ T + b.\Pi\ S) \\
\Rightarrow & \{S = T \cup \{q\}.\ \text{So, } \Pi\ S = q.\Pi\ T\} \\
 & p \mid \Pi\ T(a.p + b.q) \\
\Rightarrow & \{a.p + b.q = 1\} \\
 & p \mid \Pi\ T \\
\Rightarrow & \{\text{inductive hypothesis}\} \\
 & p \in T \\
\Rightarrow & \{T \subseteq S\} \\
 & p \in S
\end{array}
$$

**Theorem 1** (Unique prime factorization) $(R = S)\ \equiv\ (\Pi\ R = \Pi\ S)$.
Proof: We can argue inductively, based on Lemma 1, that the bag corresponding to a number $x$ is unique: if $p \mid x$ then $p$ is in the bag and $x/p$ has a unique bag, by induction; and if $p$ does not divide $x$ then $p$ is not in the bag. So, the bag corresponding to $x$ is unique. I show a formal proof next.

Obviously $(R = S) \Rightarrow (\Pi\ R = \Pi\ S)$. I prove that if $(\Pi\ R = \Pi\ S)$ then $R$ and $S$ are equal as bags. It is easy to show that for any $p$, $(p \in R) \ \equiv\ (p \in S)$. This only proves that $R$ and $S$ have the same *set* of elements, as in $R = \{2, 2, 3\}$ and $S = \{2, 3, 3\}$, not the same *bag* of elements [1]. The following proof uses induction on $n$, the size of $R$.

• $n = 0$: Then $R$ is the empty bag, so $\Pi\ R = 1 = \Pi\ S$. Then $S$ is the empty bag.

• $n > 0$: $R$, being non-empty, has an element $p$.

$$
\begin{array}{cl}
 & p \in R \\
\equiv & \{\text{from Lemma 1}\} \\
 & p \mid \Pi\ R \\
\equiv & \{\Pi\ R = \Pi\ S\} \\
 & p \mid \Pi\ S \\
\equiv & \{\text{from Lemma 1}\} \\
 & p \in S
\end{array}
$$

Let $R' = R - \{p\}$ and $S' = S - \{p\}$. Inductively, $R' = S'$ as bags. So, $R = S$ as bags because $R = R' \cup \{p\}$ and $S = S' \cup \{p\}$.

**Alternate Proof shown to me by 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 $c$.

$$
\begin{array}{cl}
 & c \\
= & \{\text{from } \neg(p \mid a) \text{ and } p \text{ prime, } \gcd(p, a) = 1\} \\
 & c \times \gcd(p, a) \\
= & \{\text{multiplication distributes over gcd}\} \\
 & \gcd(pc, ac) \\
= & \{pc = ab\} \\
 & \gcd(ab, ac) \\
= & \{\text{multiplication distributes over gcd}\} \\
 & a \times \gcd(b, c)
\end{array}
$$

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

$$
\begin{array}{cl}
 & pc = p \times a \times \gcd(b, c) \\
\Rightarrow & \{pc = ab\} \\
 & ab = p \times a \times \gcd(b, c) \\
\Rightarrow & \{\text{Cancellation, } a \neq 0\}
\end{array}
$$

[1] This mistake in my original proof was spotted by Rutger Dijkstra.

$$
\begin{array}{ll}
 & b = p \times \gcd(b, c) \\
\Rightarrow & \{\text{definition}\} \\
 & p \mid b
\end{array}
$$