

Unique Prime Factorization Theorem

Jayadev Misra

2/4/2006

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 $(p \mid \overline{S})$ for “ p divides \overline{S} ”. By convention, $\overline{\phi} = 1$; thus the unique bag corresponding to 1 is ϕ .

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 $ap + bq = 1$.

$p \mid ap\overline{R}$, arithmetic
$p \mid bq\overline{R}$, $p \mid \overline{S}$ and $\overline{S} = q\overline{R}$
$p \mid (ap + bq)\overline{R}$, from above two
$p \mid \overline{R}$, $ap + bq = 1$
$p \in R$, induction hypothesis
$p \in S$, $R \subseteq S$

Theorem $\overline{S} = \overline{T} \Rightarrow S = T$

Proof: Proof is by induction on the value of \overline{S} .

- $\overline{S} = 1$: Then, $\overline{T} = 1$ and $S = \phi = T$.
- $\overline{S} > 1$: Then, $\overline{T} > 1$. Let $S = R \cup \{q\}$ and $T = U \cup \{p\}$.
 If $p = q$, then from $\overline{S} = \overline{T}$, we have $\overline{R} = \overline{U}$. Inductively, $R = U$, or $S = T$.
 If $p \neq q$, then

$q \in S$	
\Rightarrow	{definition of \overline{S} }
	$q \mid \overline{S}$
\Rightarrow	{ $\overline{S} = \overline{T}$ }

$$\Rightarrow \begin{array}{l} q \mid \bar{T} \\ \{\text{from the Lemma}\} \\ q \in T \end{array}$$

That is, $T = V \cup \{q\}$, for some V . Given that $S = R \cup \{q\}$, apply Case (1) to conclude $S = T$.

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 .

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

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

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