

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, p and q denote primes, and S , T and R 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 .

Observation $p \in S \Rightarrow p \mid \overline{S}$

Lemma $p \mid \overline{S} \Rightarrow p \in S$

Proof: proof is by induction on the size of S .

$S = \phi$: Then $\overline{S} = 1$ and the antecedent is false.

$S = R \cup \{q\}$: If $p = q$ then the result holds trivially. Otherwise, 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
$p \in S$, $R \subseteq S$

Corollary $p \mid \overline{S} \equiv p \in S$, from Observation and Lemma.

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

Proof:

$p \in S$
\equiv {from the corollary}
$p \mid \overline{S}$
\equiv $\{\overline{S} = \overline{T}\}$
$p \mid \overline{T}$
\equiv {from the corollary}
$p \in T$

Therefore, $S = T$.

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

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