Prime Factorization

Tilmann, Olaf, Arka

July 2023

Definition 1 (prime)**.** *Let $p \in \mathbf{N}$, $p \geq 2$. p is called prime, if:*

$$\forall d \in \mathbf{N} : d|p \implies d = 1 \vee d = p$$

Lemma 1 (prime is fact)**.** *Let $p \in \mathbf{N}$ prim.*
$s = \{p\}$ Multiset. Then:

$$p \in s \implies p \text{ prim} \tag{1}$$

$$\prod_{q \in s} q = p \tag{2}$$

Lemma 2 (exists factor)**.** *Let $n \in \mathbf{N}$, $n \geq 2$ $\neg n$* prim.
Then exists $p, q \in \mathbf{N}$, such that $n = p * q \wedge p, q < n \wedge p, q \neq 1$

Proof. Let $n \in \mathbf{N}$, $n \geq 2$ $\neg n$ prime
According to negation of definition 1: $\exists d \in \mathbf{N}$ such that $d|n \wedge d \neq 1 \wedge d \neq n$.
Because $d|n$ $\exists c \in \mathbf{N}, c \neq 0$ with: $n = d * c$. $c \neq 0 \implies c \geq 1 \implies n \geq d$.
$d \neq n \implies d < n$
$d \neq 1 \implies d > 1$ □

Lemma 3 (prod solution)**.** *Let $p, q \in \mathbf{N}$, $n = p * q$. $s_p, s_q \subseteq \mathbf{N}$ are multisets, such that: $\prod_{e \in s_p} e = p$ and $\prod_{e \in s_q} e = q$. $s = s_p + s_q$. Then: $\prod_{e \in s} e = n$*

Theorem 1 (prime fact)**.** *Let $n \in \mathbf{N}$, $n \geq 2$ then exists Multiset $s \subseteq \mathbf{N}$, such that:*

$$\prod_{p \in s} p = n \tag{3}$$

$$p \in s \implies p \text{ prim} \tag{4}$$

Proof. Use strong induction in n:

Base Case: n=2 prime $\xRightarrow{Lemma1}$ Multiset $s = \{n\}$ is sufficient for (3) and (4).

Assumption: $\forall\ 2 \leq d \leq n\ \exists$ Multiset$s \subseteq \mathbf{N}$ such that $\prod_{p \in s} p = d$ and $p \in s \implies p$ prim

Induction Step:

1st case: $n+1$ prime

n+1 prime $\xRightarrow{Lemma1}$ Multiset $s = \{n+1\}$ is sufficient for (3) and (4)

2nd case $n+1$ not prime

$\xRightarrow{Lemma2} \exists\ 2 \leq p, q \leq n$, such that: $n+1 = p * q$.

$\xRightarrow{Assumption} \exists$ Multisetss_p, s_q such that: $x \in s_p, s_q \implies x$ prime and $\prod_{x \in s_p} = p$ and $\prod_{x \in s_q} = q$

$\xRightarrow{Lemma3} s = s_q + s_p$ is sufficient for (3) and (4).

$\square$