# Principle of Induction

from basis $\ell$

Let $P(m)$ be a statement for $m$ ranging over the natural numbers greater than or equal a fixed natural number $\ell$.

If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\big( P(n) \implies P(n+1) \big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}$. $P(m)$ holds.

## Principle of Strong Induction

from basis $\ell$ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for $m$ ranging over the natural numbers greater than or equal a fixed natural number $\ell$.

If both

- $P(\ell)$ and
- $\forall\, n \geq \ell$ in $\mathbb{N}$. $\Big( \big(\forall\, k \in [\ell..n].\, P(k)\big) \implies P(n+1) \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.

NB. $k \in [\ell..n] \iff \ell \leq k \leq n$

# Fundamental Theorem of Arithmetic

**Proposition** For every positive integer $n$ there exists a finite sequence of primes $(p_1, \ldots, p_\ell)$ with $\ell \in \mathbb{N}$ such that $n = \pi(p_1, \ldots, p_\ell)$.

**PROOF:** We prove

$$\forall n \geq 1 \text{ in } \mathbb{N}.\ P(n)$$

where

$$P(n) \stackrel{\text{def}}{=} \begin{array}{l}\text{There exists a finite sequence of primes} \\ (p_1, \ldots, p_\ell) \text{ with } \ell \in \mathbb{N} \text{ such that} \\ n = \pi(p_1, \ldots, p_\ell).\end{array}$$

by strong induction.

Base case: We need prove that

There exists a finite sequence of primes $(p_1, \dots, p_\ell)$ with $\ell \in \mathbb{N}$ such that

$1 = \pi(p_1, \dots, p_\ell)$.

Indeed, the product of the empty sequence of length 0 is 1.

Inductive step: Let $n \geq 1$ in $\mathbb{N}$.

Assume the strong Induction Hypothesis

(SIH) For every $1 \leq k \leq n$ there exists a finite sequence of primes $(p_1, \dots, p_{\ell_k})$ with $\ell_k \in \mathbb{N}$ such that $k = \pi(p_1, \dots, p_{\ell_k})$.

RTP: There exists a finite sequence of primes $(p_1, \dots, p_\ell)$ with $\ell \in \mathbb{N}$ such that

$$n+1 = \Pi(p_1, \dots, p_\ell).$$

- CASE $n+1$ is a prime, say $p$.

  Then, $n+1$ is the product of the singleton sequence $(p)$.

- CASE $n+1$ is composite, say $n+1 = i \cdot j$ with $1 \leq i \leq n$ and $1 \leq j \leq n$.

By (SIH): $i = \Pi(p_1, \dots, p_{\ell_i})$ and $j = \Pi(q_1, \dots, q_{\ell_j})$

for finite sequences of primes $(p_1, \dots p_{l_i})$ and $(q_1, \dots, q_{l_j})$ with $l_i$ and $l_j$ in $\mathbb{N}$.

Therefore

$$n+1 = \prod (p_1 \cdots p_{l_i}, q_1 \cdots q_{l_j})$$

as required. $\boxtimes$

**Theorem 77 (Fundamental Theorem of Arithmetic)** *For every positive integer* $n$ *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \quad .$$

PROOF: We prove

$$\forall m \in \mathbb{N} . P(m)$$

where

$P(m) \stackrel{\text{def}}{=}$ for all primes $(p_1 \leq \cdots \leq p_m)$ and for all $n \in \mathbb{N}$ and primes $(q_1 \leq \cdots \leq q_n)$ if $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$ then $m = n$ and $\forall 1 \leq k \leq m . \, p_k = q_k$.

by induction.

BASE CASE:

RTP: for all $n \in \mathbb{N}$ and primes $(q_1 \leq \cdots \leq q_n)$
if $1 = \prod_{j=1}^{n} q_j$ then $0 = n$.

Let $n$ be a natural number and let $q_1 \leq \cdots \leq q_n$ be primes.
Assume that $1 = \prod_{j=1}^{n} q_j$.

Then
$$1 = q_1 \cdot \cdots \cdot q_n \geq 2^n$$

Therefore
$$n = 0$$

**INDUCTIVE STEP**: Let $m$ be a natural number and assume the Induction Hypothesis

(IH) for all primes $(p_1 \leq \cdots \leq p_m)$ and for all $n \in \mathbb{N}$ and primes $(q_1 \leq \cdots \leq q_n)$, if $\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$ then $m = n$ and $\forall\, 1 \leq k \leq m .\ p_k = q_k$.

**RTP**: for all primes $(s_1 \leq \cdots \leq s_m \leq s_{m+1})$ and for all $l \in \mathbb{N}$ and $(t_1 \leq \cdots \leq t_l)$, if $\prod_{i=1}^{m+1} s_i = \prod_{j=1}^{l} t_j$ then $m+1 = l$ and $\forall\, 1 \leq k \leq m+1,\ s_k = t_k$.

Let $(s_1 \leq \cdots \leq s_m \leq s_{m+1})$ be primes, and let $\ell$ be a natural number and $(t_1 \leq \cdots \leq t_\ell)$ be primes.

Assume: $\prod_{i=1}^{m+1} s_i = \prod_{j=1}^{\ell} t_j$. $(*)$

RTP: $m+1 = \ell$ and $\forall\, 1 \leq k \leq m+1.\ s_k = t_k$.

By $(*)$, $s_1 \mid \prod_{j=1}^{\ell} t_j$. Therefore $\ell \neq 0$ and, by Euclid's Thm $s_1 \mid t_{j_0}$ for some $1 \leq j_0 \leq \ell$.

So, ① $s_1 = t_{j_0} \geq t_1$. Analogously, by $(*)$, $t_1 \mid \prod_{i=1}^{m+1} s_i$, and therefore $t_1 \mid s_{i_0}$ for some $1 \leq i_0 \leq m+1$.

Again, ② $t_1 = s_{i_0} \geq s_1$. By ① and ②, $s_1 = t_1$.

Moreover from

$$\prod_{i=1}^{m+1} s_i = \prod_{j=1}^{l} t_j \quad \text{and} \quad s_1 = t_1$$

we have

$$\prod_{i=2}^{m+1} s_i = \prod_{j=2}^{l} t_j$$

$$\prod_{i=1}^{m} s_{i+1} \qquad\qquad \prod_{j=1}^{l-1} t_{j+1}$$

By (IH), it follows that

$$m = l-1 \text{ and } \forall 1 \leq k \leq m.\, s_{k+1} = t_{k+1}. \qquad \boxtimes$$