# Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

# Principle of Induction

Let $P(m)$ be a statement for $m$ ranging over the set of natural numbers $\mathbb{N}$.

If

BASE CASE

- the statement $P(0)$ holds, and

INDUCTION STEP

- the statement

  $$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

  also holds

then

- the statement

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

  holds.

**Proposition** $\forall n \in \mathbb{N}.\ \underline{Even}(n) \text{ or } \underline{Odd}(n).$

where $\underline{Even}(n) = (\exists k \in \mathbb{N}.\ n = 2k)$

and $\underline{Odd}(n) = (\exists k \in \mathbb{N}.\ n = 2k+1)$

**PROOF**: We proceed by induction for

$$P(n) = \underline{Even}(n) \text{ or } \underline{Odd}(n)$$

Base case: $n = 0$

RTP: $\underline{Even}(0)$ or $\underline{Odd}(0)$

In fact $Even(0)$ holds, as $0 = 2 \cdot 0$, hence we are done.

<u>Induction step:</u> Let n be an arbitrary natural number

<u>Assume</u>: Even(n) (1) or Odd(n) (2)

<u>RTP</u>: Even(n+1) or Odd(n+1)

<u>We proceed by cases</u>:

(1) Even(n) holds, that is $n = 2k$ for an integer k
Then, $n+1 = 2k+1$ and hence Odd(n+1) holds
and we are done.

(2) Odd(n) holds, that is $n = 2k+1$ for an integer k
Then $n+1 = 2(k+1)$ and hence Even(n+1) holds
and we are done.

$\square$

NB: Induction from basis $\ell$ for a property $P$ is in fact equivalent to Induction (from basis 0) for the property

# Principle of Induction

from basis $\ell$  $Q(n) = P(\ell + n)$

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

If

BASE CASE

- $P(\ell)$ holds, and

INDUCTION STEP

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

then

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

NB: The principle of Strong Induction from basis $\ell$ for a property P is the principle of Induction from basis $\ell$ for the property $P^{\#}$ of the supervision exercises.

Exercise

# 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

BASE CASE

INDUCTION STEP

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

$\big(\forall k.\ \ell \leq k \leq n \Rightarrow P(k)\big)$

hold, then

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

# Fundamental Theorem of Arithmetic

**Proposition 76** *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

PROOF: We proceed by induction from basis 2 for the predicate

$P(n) = (n$ is a prime or $n$ is a product of primes$)$

<u>Base case</u>: $n=2$

Since 2 is a prime, we are done.

<u>Inductive step</u>: Let $n \geq 2$ be arbitrary.

(IH) <u>Assume</u>: $\forall\, k \in [2..n].\ k$ is prime or $k$ is a product of primes.

<u>RTP</u> : $P(n+1)$ holds, that is,

$n+1$ is a prime or $(n+1)$ is a product of primes.

<u>Case 1</u> : $n+1$ is a prime, then we are done.

<u>Case 2</u> : $n+1$ is not a prime, then $n+1 = k \cdot l$ for some $k$ and $l$ greater than or equal 2 and less than or equal $n$.

Hence, by Induction Hypothesis (IH),

$k$ is prime or a product of primes

and

$l$ is prime or a product of primes.

Therefore

$n+1 = k \cdot l$ is a product of primes.

and we are done $\square$

**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*

$$n = \underbrace{\prod(p_1, \ldots, p_\ell)}_{\text{notation for } p_1 \cdot p_2 \cdot \ldots \cdot p_\ell} .$$

PROOF:

N.B. For $\ell = 0$, $\prod(\,) = 1$

Since we know that a number $\geq 2$ is prime or a product of primes we need only prove the uniqueness of prime decomposition.

We show that for all $n \geq 1$,

$$\left.\begin{array}{l}
\text{If} \\
\qquad n = \prod(p_1 \dots p_\ell) \text{ for } p_i \text{ primes} \\
\quad \text{and} \\
\qquad n = \prod(q_1 \dots q_k) \text{ for } q_j \text{ primes.} \\
\text{Then} \\
\qquad \ell = k,\ p_1 = q_1, \dots, p_\ell = q_\ell,
\end{array}\right\} P(n)$$

We proceed by induction:

BASE CASE: $n = 1$, $n = \prod(p_1 \dots p_\ell) = \prod(q_1 \dots q_k)$

with $\ell = k = 0$. Therefore we are done.

INDUCTIVE STEP Consider $n \geq 1$

(STRONG INDUCTION)

Assume $P(m)$ for all $1 \leq m \leq n$

RTP : $P(n+1)$

primes

i.e if $n+1 = \Pi(p_1 \cdots p_l) = \Pi(q_1 \cdots q_k)$

Then $l = k$, $p_1 = q_1$ ---- $p_l = q_l$.

Assume $n+1 = \Pi(p_1 — p_l) = \Pi(q_1 — q_k)$.

RTP: $l = k$, $p_1 = q_1, \ldots, p_l = q_l$.

We know

$$p_1 \mid n+1 = \Pi(q_1 \dots q_k)$$

So

$$p_1 \mid q_j \quad \text{for some } j.$$

EUCLID'S THEOREM

By the ordering assumption on the sequence, we have

$$q_j = q_1$$

and so $p_1 \mid q_1$. Analogously, we show that $q_1 \mid p_1$

Hence $p_1 = q_1$.

Consider then $\Pi(p_2, \dots p_\ell) = \Pi(q_2 \dots q_k)$.

By Induction Hypothesis applied to

$$\prod (p_2 \cdots p_l) = \prod (q_2 \cdots q_k) \qquad (\leq n)$$

we get

$$l = k, \; p_2 = q_2, \ldots, p_l = q_l$$

Hence we are done. $\square$