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

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

  also holds

then

- the statement

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

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \quad .$$

PROOF: Consider the property

$$P(n) \stackrel{\text{def}}{=} \left[(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \right]$$

<u>RTP</u>

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

We proceed by induction.

BASE CASE: RTP $P(0)$

$$(x+y)^0 \stackrel{?}{=} \sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k$$

$$(x+y)^0 = 1$$

$$\sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k = \binom{0}{0} x^0 y^0 = 1$$

INDUCTIVE STEP:

Let $n \in \mathbb{N}$ be arbitrary.

Assume THE INDUCTION HYPOTHESIS.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

RTP: $(x+y)^{n+1} = \sum_{k}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$.

We have:

$$(x+y)^{n+1} = (x+y)^n \cdot (x+y)$$

$$\overset{\text{by (IH)}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right) \cdot (x+y)$$

$$= \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k\right) + \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}\right)$$

$$= x^{n+1} + \left[\sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k\right] + y^{n+1}$$

$$\overset{?}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

$$= x^{n+1} + \left(\sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^{k}\right)$$

$$+ y^{n+1} + \left(\sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1}\right)$$

<u>Aim</u>

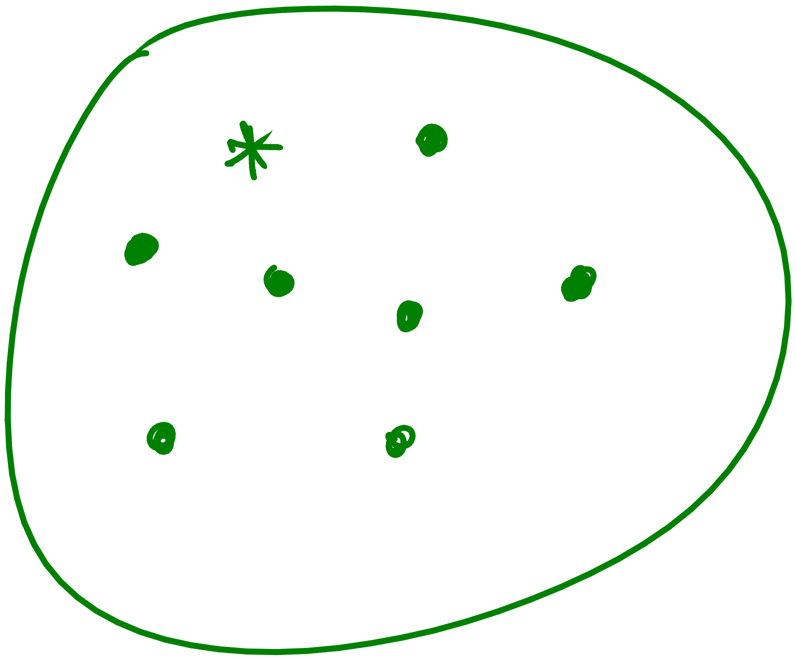
$$\sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^{k}$$

$$+ \sum_{k=1}^{n} \binom{n}{k-1} x^{n-k+1} y^{k}$$

<u>Lemma</u>: $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

$$\stackrel{?}{=} \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^{k}$$

$\binom{n+1}{k}$ = the number of ways in which we can select k objects from a set of $n+1$ objects.



selecting k objects without selecting $*$

$\binom{n}{k}$

selecting k objects incorporating $*$

$\binom{n}{k-1}$

Principle of Induction

from basis ℓ

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

If

BASE CASE

- $P(\ell)$ holds, and

INDUCTIVE 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.

Principle of Strong Induction

from basis ℓ 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 ℓ.

If both

BASE CASE

- $P(\ell)$ and

INDUCTIVE STEP

- $\forall\, n \geq \ell$ 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.

Fundamental Theorem of Arithmetic

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

$\Pi() = 1$

$\Pi(p) = p$

...

PROOF: We prove

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

where

$P(n) \stackrel{def}{=}$ There exists a finite sequence of primes $(p_1, \dots, p_\ell)$ with $\ell \in \mathbb{N}$ such that $n = \Pi(p_1, \dots, p_\ell)$.

by strong induction.

BASE CASE $P(1)$

Since $1 = \Pi()$ we are done.

INDUCTIVE STEP: Let n be a positive int.

Assume (IH) that for all $1 \leq l \leq n$, l = product of a finite sequence of primes.

RTP $n+1$ = product of a finite sequence of primes.

Case 1: If $n+1$ is a prime, say p, then $n+1 = \Pi(p)$ and we are done.

Case 2: If $n+1$ is composite, that is, $n+1 = i \cdot j$ for some $1 \leq i, j \leq n$.

Then, by strong induction,

$$i = \prod (p_1 \cdots p_k) \quad \text{for primes } p_1 \cdots p_k$$

$$j = \prod (q_1 \cdots q_l) \quad \text{for primes } q_1 \cdots q_l$$

So

$$n+1 = \prod (p_1 \cdots p_k q_1 \cdots q_k)$$

and we are done. $\boxtimes$

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: $P(0)$

That is, $\left(1 = \prod_{j=1}^{m} q_j\right) \overset{?}{\Longrightarrow} m = 0$

Assume $1 = \prod_{j=1}^{m} q_j \geq 2^m$

Then $1 \geq 2^m$

Hence $m = 0$.

INDUCTIVE STEP:

Assume (IH) for $m \in \mathbb{N}$.

$P(m) =^{def}$ for all $(p_1 \leq \dots \leq p_m)$ primes

for all $(q_1 \leq \dots \leq q_n)$ primes.

$\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j$

$\Rightarrow$ $m = n$ and $p_k = q_k$ $(k = 1 - m)$

RTP: $P(m+1)$

Consider $(s_1 \leq s_2 \leq \dots \leq s_m \leq s_{m+1})$ primes.

$(t_1 \leq \dots \leq t_\ell)$ primes.

such that $\prod(s_1, \dots, s_m, s_{m+1}) = \prod(t_1, \dots, t_\ell)$

RTP: $\ell = m+1$ and $s_k = t_k$ $k = 1 — m+1$.

$s_1 \mid \pi(t_1 \cdots t_\ell)$

So $s_1 = t_{j_0}$ for some j_0 and $t_1 \leq s_1$

Analogously $s_1 \leq t_1$ and hence $s_1 = t_1$

Since $s_1 s_2 \cdots s_m s_{m+1} = t_1 t_2 \cdots t_\ell$

we have $\underbrace{s_2 \cdots s_m s_{m+1}}_{\text{a sequence of length } m} = t_2 \cdots t_\ell$

So, by (IH), $m = \ell - 1 \Rightarrow \ell = m+1$

and $s_k = t_k$ for all $k = 2, \ldots, m+1$

$\boxtimes$

Euclid's infinitude of primes

Theorem 80 *The set of primes is infinite.*

PROOF: By contradiction assume it is not.
Let $p_1, p_2, \ldots, p_N$ be the "finite" set of primes.

Consider $c = \prod(p_1, \ldots, p_N) + 1$

Since $c \neq p_i$ for all $i = 1, \ldots, N$. There is some k such that $p_k \mid c$; that is, $c = p_k \cdot l$ for some l.

$1 = c - \prod(p_1 \ldots p_N) = p_k \cdot l - \prod(p_1 - p_N)$

$\Rightarrow 1 = \underline{gcd}(p_k, \prod(p_1 - p_N)) = p_k$ a contradiction $\boxtimes$