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.

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: We prove it by induction on $n \in \mathbb{N}$.

(1) BASE CASE:

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

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

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

(2) INDUCTIVE STEP

Let $n \in \mathbb{N}$ s.t. $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ (IH)

RTP: $(x+y)^{n+1} \stackrel{?}{=} \sum_{i=0}^{n+1} \binom{n+1}{i} x^i y^{n+1-i}$

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

$\parallel$

$(x+y)\cdot(x+y)^n$

$\parallel$ by (IH)

$(x+y) \cdot \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} = \sum_{i=0}^{n} \binom{n}{i} x^{i+1} y^{n-i} + \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i+1}$

$$\sum_{i=0}^{n} \binom{n}{i} x^{i+1} y^{n-i} + \sum_{i=0}^{n} \binom{n}{i} x^{i} y^{n-i+1}$$

$$= x^{n+1} + \underbrace{\sum_{i=0}^{n-1} \binom{n}{i} x^{i+1} y^{n-i} + \sum_{i=1}^{n} \binom{n}{i} x^{i} y^{n-i+1}}_{\stackrel{?}{=} \sum_{i=1}^{n} \binom{n+1}{i} x^{i} y^{n+1-i}} + y^{n+1}$$

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

$$\sum_{i=0}^{n-1}\binom{n}{i}x^{i+1}y^{n-i}+\sum_{i=1}^{n}\binom{n}{i}x^{i}y^{n-i+1}$$

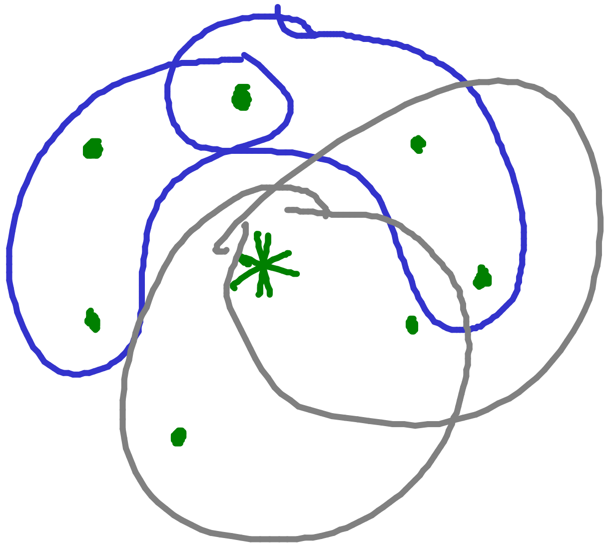
$$=\sum_{k=1}^{n}\binom{n}{k-1}x^{k}y^{n-(k-1)}+\sum_{i=1}^{n}\binom{n}{i}x^{i}y^{n-i+1}$$

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

Lemma:

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

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



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

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

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.

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

INDUCTION 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 95 *Every positive integer greater than or equal 2 is a prime or a product of primes.*

PROOF: Show

$\forall n \geq 2$ in $\mathbb{N}$. n is prime or a product of primes.

By strong induction from basis 2 we show:

(1) BASE CASE: Since 2 is prime, we are done.

(2) INDUCTIVE STEP:

Let $n \geq 2$ in $\mathbb{N}$. Assume: for all $2 \leq i \leq n$, i is prime or a product of primes. (SIH)

RTP: $n+1$ is prime or a product of primes.

CASES:

(1) if $n+1$ is prime, we are done,

(2) if $n+1$ is composite.

Then, $n+1 = a \cdot b$ with $a \geq 2$, $b \geq 2$ and also

$a \leq n$, $b \leq n$

So by (SIH), a is a prime or a product of primes

and b is a prime or product of primes.

In either case, $a \cdot b$ is a product of primes,

and we are done.

$\boxtimes$

Theorem 96 (Fundamental Theorem of Arithmetic) *For every positive integer n there is a unique finite ordered sequence of primes $(p_1 \le \cdots \le p_\ell)$ with $\ell \in \mathbb{N}$ such that*

$$\prod() \stackrel{\text{def}}{=} 1$$

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

$$\prod(p_1, \ldots, p_\ell) = p_1 \cdot p_2 \cdot \cdots \cdot p_\ell$$

PROOF:

For uniqueness,

$$n = \prod(p_1, p_2, \ldots, p_\ell)$$
$$p_1 \le p_2 \le \cdots \le p_\ell$$

and

$$n = \prod(q_1, q_2, \ldots, q_k)$$
$$q_1 \le q_2 \le \cdots \le q_k$$

$$\stackrel{?}{\Longrightarrow} \ \ell = k \text{ and } p_1 = q_1, p_2 = q_2, \ldots, p_\ell = q_k$$

① $\prod(p_1 \cdots p_\ell) = \prod(q_1 \cdots q_k)$

$p_1 \leq \cdots \leq p_\ell$ $\qquad$ $q_1 \leq \cdots \leq q_k$

① $\Rightarrow p_1 \mid \prod(q_1 \cdots q_k) \Rightarrow p_1 = q_i$ for some i

$\Rightarrow q_1 \leq p_1$

① $\Rightarrow q_1 \mid \prod(p_1 \cdots p_\ell) \Rightarrow q_1 = p_j$ for some j

$\Rightarrow p_1 \leq q_1$

$\Rightarrow$ ② $p_1 = q_1$

① & ② $\Rightarrow \prod(p_2, \ldots, p_\ell) = \prod(q_2, \ldots, q_k)$

Proceed iteratively; That is, formally by induction $\boxtimes$

Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF: Assume by contradiction that there are a finite number of primes, say

$$p_1, p_2, \ldots, p_N \quad \text{for } N \in \mathbb{N}$$

Consider,

$$(p_1 \cdot p_2 \cdot \cdots p_N) + 1$$

Then, by assumption, $(p_1 \cdots p_N)+1$ is not a prime and there is p_j that divides it for some j

Thus, 1 is an int. lin. comb of $(p_1 \cdots p_N)$ and p_j

$$p_j = \underline{\gcd}((p_1 \cdots p_N), p_j) = 1$$

$\lightning$

contradiction.

$\boxtimes$