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.

"induction hypothesis"

Principle of Induction

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

If

- the statement $P(0)$ holds, and "Basis" or "Base case".
- the statement

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

  "Induction step"

  also holds

then

- the statement

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

  holds.

Binomial Theorem

$\binom{n}{k} =_{df} \frac{n!}{(n-k)!\,k!}$

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: Let $P(n)$ be the statement

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

We prove $\forall m \in \mathbb{N}.\ P(m)$ by mathematical induction.

Basis: i.e. $P(0)$ holds by the following argum^t.

l.h.s $= (x+y)^0 = 1$ r.h.s $= 1$.

Induction step. Assume $P(n)$ holds. RTP. $P(n+1)$.

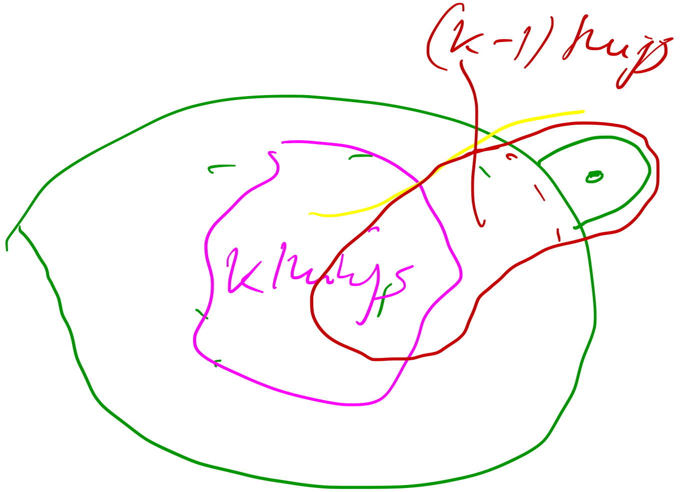
Here $(x+y)(x+y)^n = (x+y)\cdot \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

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

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

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

Exercise by Math'l Ind.



Definition by Mathematical Induction (Recursion)

To define a function on $\mathbb{N}$, specifying

$$f(0) = k \quad \text{and}$$

$$f(n+1) = B(n, f(n)) \text{ for } n \in \mathbb{N}$$

suffices. Eg.

$$!0 = 1$$

$$!(n+1) = (n+1) \cdot !n$$

defines the factorial function.

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

- $P(\ell)$ 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.

(a.k.a. course-of-values induction)

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

- $P(\ell)$ 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.

An alternative formulation of Strong Induction.

If

when $n = l$
true

$$\forall n \geq l \text{ in } \mathbb{N}.\ \left(\forall k,\ l \leq k < n.\ P(k)\right) \Rightarrow P(n)$$

then $\forall m \geq l \text{ in } \mathbb{N}.\ P(m)$.

Where's the basis case gone?

Consider $n = l$.

$$\left(\forall k,\ l \leq k < l.\ P(k)\right) \Leftrightarrow \underbrace{\forall k.\ \left(\underbrace{\overbrace{l \leq k < l}^{\text{false}} \Rightarrow P(k)}_{\text{true}}\right)}_{\text{true}}$$

is "vacuously true".

So $\left(\forall k,\ l \leq k < l.\ P(k)\right) \Rightarrow P(n)$

reduces to $\text{true} \Rightarrow P(n)$, so to $P(n)$.

Fundamental Theorem of Arithmetic

Proposition 76 *Every positive integer greater than or equal 2 is a prime or a product of primes.* $p_1 \cdot p_2 \cdots p_k$

PROOF: Let $P(m)$ be the statement

m is prime or a product of primes.

We prove

$$\forall m \geq 2 \text{ in } \mathbb{N}.\ P(m)$$

by Strong Induction with basis 2.

Basis. $P(2)$ as 2 is a prime.

Induction step Assume $\forall k \in [2, \dots, n]$. $P(k)$. RTP $P(n+1)$.

Case 1 $n+1$ is a prime. Then $P(n+1)$ directly.

Case 2 $n+1$ is composite, i.e. $n+1 = x \cdot y$

where $x, y \in [2, \dots, n]$

Have $P(x)$ and $P(y)$ from ind. hyp.

$\therefore$ $P(x \cdot y)$ i.e. $P(n+1)$.

This completes the proof by strong induction $\boxtimes$

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*

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

aka "smallest counterexample"

PROOF: Use the least number principle:

A non-empty subset of $\mathbb{N}$ has a least element.

(The least number principle is equivalent to math. ind.)