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

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

BASE CASE

- the statement

INDUCTIVE STEP

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

also holds

then

- the statement

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

holds.

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

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

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

PROOF: We proceed by induction on x to prove $\forall n \in \mathbb{N} . P(n)$.

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

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

So we are done.

Note The $\sum_{k=0}^{n} f(k)$ is defined by induction on $n \in \mathbb{N}$

- **BASE CASE**: $\sum_{k=0}^{0} f(k) = f(0)$

- **Inductive step**:

$$\sum_{k=0}^{n+1} f(k) = \left(\sum_{k=0}^{n} f(k)\right) + f(n+1).$$

INDUCTIVE STEP:

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

Assume $n \in \mathbb{N}$. Assume $P(n)$, that is,

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

RTP:

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

Scratch work

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

by (IH)

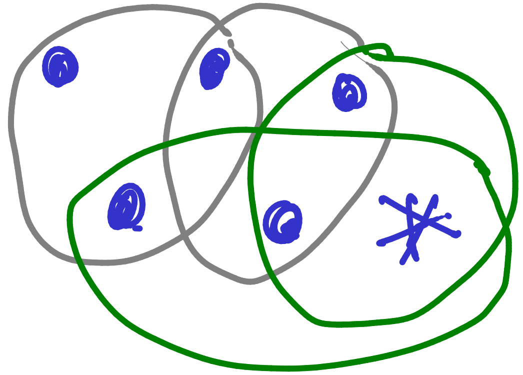
$$= \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right) \cdot (x+y)$$

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

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

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

n-element set



$\binom{n}{3}$

Consider $\binom{n+1}{k}$

conjecture $=$

Idea

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

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

$$= \sum_{k=0}^{n+1} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n+1-k} y^{k} = \cdots$$

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.

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.

Fundamental Theorem of Arithmetic

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

PROOF: $\forall\, n \geq 2.$ (n is prime) or (n is a product of primes)

By strong induction:

BASE CASE: (2 prime) or (2 a product of primes).

Trivially true.

INDUCTIVE STEP

Let $n \geq 2$ such that for all

(IH) $2 \leq k \leq n$, (k prime) or (k is a product of primes)

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

CASE (1) $n+1$ prime, then we are done.

CASE (2) $n+1$ not prime, say $n+1 = p \cdot q$ $(p, q \geq 2)$

The induction hypothesis holds for p and q, that is, they are prime or products of primes.

So $p \cdot q$ is a product of primes, 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*

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

~~Inductive def~~

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

$\prod(k_1, \ldots, k_{\ell+1}) \stackrel{\text{def}}{=} \prod(k_1, \ldots, k_\ell) \cdot k_{\ell+1}$

PROOF: Idea

$1 = \prod(\,)$

$n \geq 2$ so $n = \prod(p) = p$ n is prime

or $n = \prod(p_1, \ldots, p_\ell)$ n is a product of primes.

We want to show

$$\prod(p_1 \cdots p_l) = \prod(q_1 \cdots q_k)$$

for p_i and q_j primes

and written in increasing order

$$\Rightarrow l = k \text{ and } p_1 = q_1, p_2 = q_2, \ldots, p_l = q_k$$

We prove it by induction on the length of the sequence $(p_1 — p_l)$.

$P(\ell) \equiv \forall p_1, \ldots, p_\ell$ ordered primes

$\forall k \in \mathbb{N}.\ \forall q_1 \ldots q_k$ ordered primes

$\prod(p_1 - p_\ell) = \prod(q_1 - q_k)$

$\Rightarrow \ell = k \wedge p_i = q_i$

$\forall i = 1, \ldots, \ell$

Show by induction $\forall \ell \in \mathbb{N}.\ P(\ell)$.

idea

$$\prod(p_1 - p_\ell) = \prod(q_1 - q_k)$$

$$p_1 \mid \prod(p_1 - p_\ell) = \prod(q_1 - q_k)$$

$p_1 \mid q_j$ for some j.

$\overset{?}{\rightsquigarrow}$ show that $p_1 \mid q_1$

by cancellation $\prod(p_2 - p_\ell) = \prod(q_2 - q_k)$