Mathematical structure

Objectives

- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

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
- 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.

Base case

&

Inductive step

$\Downarrow$

Goal

Binomial Theorem

Theorem 28 *For all* $n \in \mathbb{N}$,

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

PROOF: We proceed by induction on $n \in \mathbb{N}$.

<u>Base case</u>: We need show $P(0)$; That is, that $(x+y)^0$ equals $\sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k$. We calculate

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

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

And we are done.

Inductive step: Assume $\underbrace{P(n)}$ for $n \geq 0$. and show $P(n+1)$.

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

$P(n+1) \Updownarrow$

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

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

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

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

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

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

$$= x^{n+1} + \sum_{k=1}^{n} \underbrace{\left[\binom{n}{k} + \binom{n}{k-1} \right]}_{\overset{?}{=} \binom{n+1}{k}} \cdot x^{n-k+1} y^{k} + y^{n+1}$$

<u>Lemma</u>

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

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

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

Base case & Inductive step $\Downarrow$ Goal

then

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

Strong induction for a property P is nothing but induction for a property $P^{\#}$ defined as $P^{\#}(n) \Leftrightarrow [\forall k \in [\ell..n] \cdot P(k)]$

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 $\mathbb{N}$. $\Big(\big(\forall\, k \in \underbrace{[\ell..n]}_{\text{integer interval from } \ell \text{ to } n}.\, P(k)\big) \implies P(n+1) \Big)$

Base case & Strong Inductive step

hold, then

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

Goal

Fundamental Theorem of Arithmetic

Proposition 67 *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

PROOF: Consider

$P(n) \iff$ [n is prime or a product of primes]

Want to show $\forall n \geq 2.\ P(n)$.

Base case: $P(2) \iff$ [2 is prime or a product of primes]

holds because 2 is prime.

Inductive step: Assume $P(k)$ for $2 \le k \le n$, and show it for $n+1$; That is, show $n+1$ is prime or a product of primes.

Case 1: $n+1$ is a prime, in which case we are done

Case 2: $n+1$ is composite say $n+1 = k \cdot l$ with $k, l \geq 2$. Since $k, l \le n$ they are primes or products of primes. Hence $k \cdot l$ is a product of primes and we are done.

by induction hypothesis.

Theorem 68 (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*

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

PROOF: We know from the previous proposition that every positive integer is 1 or prime or a product of primes. Now we want to show this is unique.

That is, $\forall \ell \in \mathbb{N}, \forall k \in \mathbb{N},$ $\Longleftrightarrow P(\ell)$

$\forall \underbrace{p_1 \leq \cdots \leq p_\ell}_{\text{primes}}, \underbrace{q_1 \leq \cdots \leq q_k}_{\text{primes}},$

$\prod(p_1 - p_\ell) = \prod(q_1 - q_k) \Rightarrow \ell = k \ \& \ \forall i \ p_i = q_i$

Base case: $P(0) \Leftrightarrow \left[\forall k \in \mathbb{N}.\ \forall \underbrace{q_1 \le \cdots \le q_k}_{\text{primes}} \right.$

$$\Pi() = \Pi(q_1 \cdots q_k)$$

This holds because

$$\left. \Rightarrow k = 0 \right]$$

any non-empty product of primes is greater than $1 = \Pi()$.

Inductive step: ~ EXERCISE

Use Euclid's Theorem.

Euclid's infinitude of primes

Theorem 69 *The set of primes is infinite.*

PROOF: By contradiction assume the set of primes is finite, say $p_1, p_2, \ldots, p_N$.

Consider

$$q = \Pi(p_1 - p_N) + 1$$

It is not in the list of p_i's, so not a prime. Then by the fundamental thm is a product of primes. Let p_i be a prime factor of q. Then p_i divides both q and $\Pi(p_1 - p_N)$ and hence $q - \Pi(p_1 - p_N) = 1$ ↯ □