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

INDUCTIVE 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: By induction we show:

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

<u>BASE CASE</u> $(n=0)$: That is,

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

INDUCTIVE STEP: Let $n \in \mathbb{N}$.

Assume:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \quad \left(\text{INDUCTION HYPOTHESIS}\right)$$

RTP:

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

We have:

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

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

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

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

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

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

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

$$\left[\binom{n}{k}+\binom{n}{k-1}\right]\overset{?}{=}\binom{n+1}{k}$$

$\boxtimes$

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

PROOF: We show

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

by strong induction from basis 2.

BASE CASE: Holds because 2 is prime.

INDUCTIVE STEP: Let $n \geq 2$ in $\mathbb{N}$.

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

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

CASE: $n+1$ is prime — Then we are done

CASE: $n+1$ is composite

$$n+1 = a \cdot b \text{ for } 2 \leq a, b \leq n$$

By (IH), a is a prime or a product of primes and b is a prime or a product of primes.

So, $n+1 = a \cdot b$ is a product of primes.

$\boxtimes$

Theorem 96 (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*

$$n = \underbrace{\prod(p_1, \ldots, p_\ell)}_{\text{The product of } p_1, \ldots, p_\ell} \; .$$

In particular, $\prod() = 1$

PROOF:

We want to show that

$$\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k) \overset{?}{\Longrightarrow} \ell = k \text{ and } p_i = q_i \text{ for all } 1 \leq i \leq \ell$$

$\underbrace{p_1 \leq p_2 \leq \cdots \leq p_\ell}_{\text{primes}}$ $\qquad$ $\underbrace{q_1 \leq q_2 \leq \cdots \leq q_k}_{\text{primes}}$

Assume

$$\prod(p_1,\dots,p_\ell) = \prod(q_1,\dots,q_k)$$

$p_1 \le p_2 \le \dots \le p_\ell$ primes $\qquad q_1 \le q_2 \le \dots \le q_k$ primes

$$p_1 \mid \prod(q_1 - q_k) \Rightarrow p_1 = q_i \text{ for some } i$$
$$\Rightarrow q_1 \le p_1$$

$$q_1 \mid \prod(p_1 - p_\ell) \Rightarrow q_1 = p_j \text{ for some } j$$
$$\Rightarrow p_1 \le q_1$$

$$\Rightarrow q_1 = p_1$$

Therefore

$$\prod(p_2,\dots,p_\ell) = \prod(q_2, - q_k)$$

and iterating the argument we are done. $\boxtimes$

Euclid's infinitude of primes

Theorem 99 *The set of primes is infinite.*

PROOF: Proceed by contradiction.

Let

$p_1, p_2, \cdots, p_N$

be the finite number of primes.

Consider $\prod(p_1, p_2, \cdots, p_N) + 1$

which is not a prime.

Then there is some $p_i \mid \prod(p_1 - p_N) + 1$

And 1 is an int. linear of p_i and $\prod(p_1 - p_N)$.

Therefore

$$\gcd\left(p_i, \prod(p_1 \cdots p_N)\right) = 1$$

$$\| \qquad \qquad \lightning \text{ contradiction}$$

$$p_i$$

$\boxtimes$