

Mathematical Induction

Original Notes adopted from September 11, 2001(Week 1)

© P. Rosenthal , MAT246Y1, University of Toronto, Department of Mathematics typed by A. Ku Ong

Natural Numbers

$1, 2, 3, 4, 5, 6 \dots n = \{ 1, 2, 3, 4, \dots \}$

Principle of Mathematical Induction

If $S \subset \mathbb{N}$ such that

- $1 \in S$
- $(k+1) \in S$ whenever $k \in S$, then $S = \mathbb{N}$.

Eg. Prove: $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Let $S = \{m : 1^2 + 2^2 + 3^2 + \dots + m^2 = \frac{m(m+1)(2m+1)}{6}\}$

To show: $S = \mathbb{N}$.

By Mathematical Induction, suffices to show

- $1 \in S$
- $(k+1) \in S$ whenever $k \in S$

Is $1 \in S$? $1^2 = \frac{1(1+1)(2+1)}{6}$

$$1 = 1$$

Suppose $k \in S$

$1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}$

Must show:

$1^2 + 2^2 + 3^2 + \dots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \dots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\ &= \frac{(k+1)[2k^2 + k + 6k + 6]}{6} \\ &= \frac{(k+1)[2k^2 + 7k + 6]}{6} \\ &= \frac{(k+1)[(2k+3)(k+2)]}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \end{aligned}$$

which is the formula for $n = k+1$, so $(k+1) \in S$. $\therefore S$ has properties a) & b), so $S = \mathbb{N}$.

	$n!$	3^n		$n!$	$3n$
$n = 1$	1	3	$n = 5$	120	243
$n = 2$	2	9	$n = 6$	720	729
$n = 3$	6	27	$n = 7$	5040	2187
$n = 4$	24	81			

Thm: $n! > 3^n$ for $n \geq 7$

Can start induction anywhere i.e.

For any $n_0 \in \mathbb{N}$, if $S \subset \mathbb{N}$ such that

a) $n_0 \in S$

b) $(k+1) \in S$ whenever $k \in S$ & $k \geq n_0$

then $S \supset \{n \in \mathbb{N} : n \geq n_0\}$

To prove $n! > 3^n$ for $n \geq 7$ use above.

Let $S = \{m \in \mathbb{N} : m! > 3^m\}$, $7 \in S$ (we checked).

Suppose $k! > 3^k$, Must show: $(k+1)! > 3^{k+1}$

We have $k! > 3^k$, Multiply both sides by $k+1$.

We get $(k+1)! > 3^{k+1} * (k+1)$

Since $k \geq 7$, $k+1 > 3$, so

$3^k(k+1) > 3^k * 3 = 3^{k+1}$

$\therefore (k+1)! > 3^{k+1}$, so $S \supset \{m : m \geq 7\}$

Well Ordering Principle: Every subset of \mathbb{N} other than \emptyset has a smallest element.

Assume Well-ordering Principle.

Thm: If $S \subset \mathbb{N}$ such that

a) $1 \in S$

b) $(k+1) \in S$ whenever $k \in S$, then $S = \mathbb{N}$.

Proof:

Let $T = \{n \in \mathbb{N} : n \notin S\}$ ("The complement of S ")

Show $T \neq \emptyset$, T would have a smallest element, say n_1 ,

$n_1 \neq 1$, since $1 \in S$.

$\therefore (n_1 - 1) \in \mathbb{N}$

$n_1 - 1 < n_1$ & n_1 least element of $T \Rightarrow n_1 - 1 \notin T$

$\therefore n_1 - 1 \in S$ By b), $(n_1 - 1) + 1 \in S$, So $n_1 \in S$.

In \mathbb{N} , a divides b (written $a|b$)

If $b = ac$ for some $c \in \mathbb{N}$.

Defn: $p \in \mathbb{N}$ is prime if only divisors of p are p & 1 , & $p \neq 1$. Prime: 2,3,4,7,11,13

Lemma: If n is a natural number & $n \neq 1$ & n is not a prime number, then n is a product of prime numbers.
 $180 = 9 \times 10 \times 2 = 3 \times 3 \times 5 \times 2 \times 2$.

Principle of Complete Mathematical Induction.

If $S \subset \mathbb{N}$ such that:

a) $1 \in S$

b) $(k + 1) \in S$ whenever $\{ 1, 2, 3, \dots, k \} \subset S$, then $S = \mathbb{N}$.

Proof of Lemma:

Let $S = \{ n : \text{Lemma holds for } n \}$. Show $S = \mathbb{N}$. Use Complete Induction.

Assume $\{ 1, 2, \dots, k \} \subset S$. Show $(k + 1) \in S$.

If $k + 1$ is prime, $k + 1 \in S$.

If $k + 1$ is not prime, then $k + 1 = m * n$ with m, n not 1 or $k+1$.

$m < k, n < k \implies m \in S, n \in S$.

Each of m & n is either prime or product of primes,
so $k + 1$ is the product of the primes that multiply to m and
the primes to n . $\therefore k + 1 \in S$, so $S = \mathbb{N}$.

Corollary: If $n \in \mathbb{N}$, & $n \neq 1$, then n is divisible by a prime.

Theorem: There is no largest prime number.

Proof: Let p be a prime number.

Multiply all the primes from 2 up to p together and then add 1.

Let $M = (2 * 3 * 5 * 7 * 11 \dots p) + 1$

$M > p$, so if M is prime, we're done.

$M > 1$. Suppose M is not prime, By corollary $q | M$ (q divides M) for some prime q .

We want to show: $q > p$ (that finishes the proof).

$q \neq 2$ since M leaves remainder 1 upon division by 2

For any prime $r \leq p$, M leaves remainder 1 upon division by r .

$\therefore q \neq r$ for any $r \leq p$. $\therefore q > p$, finishing the proof.

Twin primes: $p, p+2$ both primes: Is there a biggest pair of twin primes? – Unknown.

2,3 5,7 11,13 17,19 23,29