MATHEMATICAL INDUCTION

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

©P. Rosenthal , MAT246Y1, University of Toronto, Department of Mathematics

The Natural Numbers The set of *natural numbers* is the set $\{1, 2, 3, 4, 5, \ldots\}$, which is denoted by $\mathbb{N}$ (or sometimes $\mathbf{N}$.)

Principle of Mathematical Induction If $S \subset \mathbb{N}$ such that
a) $1 \in S$
b) $(k+1) \in S$ whenever $k \in S$,
then $S = \mathbb{N}$.

Example. Prove: $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
Let $S = \{m : 1^2 + 2^2 + 3^2 + \ldots + m^2 = \frac{m(m+1)(2m+1)}{6}\}$. We need to show that $S = \mathbb{N}$.
By Mathematical Induction, it will suffice to show that
a) $1 \in S$
b) $(k+1) \in S$ whenever $k \in S$

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

Now suppose $k \in S$, that is,

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

Then we must show that

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

First,

$$\begin{aligned}
1^2 + 2^2 + 3^2 + \ldots + k^2 &= \frac{k(k+1)(2k+1)}{6}, \\
\text{and so} \quad 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)}{6}[2k^2 + k + 6k + 6] \\
&= \frac{(k+1)}{6}[2k^2 + 7k + 6] \\
&= \frac{(k+1)}{6}[(2k+3)(k+2)] \\
&= \frac{(k+1)(k+2)(2k+2+1)}{6}
\end{aligned}$$

which is the formula for $n = k + 1$, so $(k + 1) \in S$.
Therefore, S has properties a) and b), so $S = \mathbb{N}$. (And therefore, the formula is true for all natural numbers.)

We can start induction anywhere:

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

Example. Show that $n! > 3^n$ for $n \geq 7$.

Compute the first few values:

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

To prove, use induction starting at 7.
Let $S = \{m \in \mathbb{N} : m! > 3^m\}$.
First, $7 \in S$ (by our calculation above).
Now suppose $k \in S$, i.e. $k! > 3^k$. We must show that $(k + 1)! > 3^{k+1}$.
We have $k! > 3^k$. Multiply both sides by $(k + 1)$ to get $(k + 1)! > 3^k(k + 1)$.
Since $k \geq 7, k + 1 > 3$, so $3^k(k + 1) > 3^k \cdot 3 = 3^{k+1}$,
and therefore $(k + 1)! > 3^{k+1}$.
Therefore, by induction, $S \supset \{m : m \geq 7\}$, and this means that $n! \geq 3^n$ for all $n > 7$.

Well-Ordering Principle Every subset of N other than $\emptyset$ has a smallest element.

The Well-Ordering Principle implies the Principle of Mathematical Induction.

Theorem. 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 $T = \{n \in N : n \notin S\}$. (The “complement” of S).
If $T \neq \emptyset$, then T would have a smallest element, say n_1.
We know that $n_1 \neq 1$, since $1 \in S$, and so $n_1 - 1$ exists.

Since $n_1 - 1 < n_1$ and n_1 is the least element of T, $(n_1 - 1) \notin T$.
Thus $(n_1 - 1) \in S$. By property b), $(n_1 - 1) + 1 \in S$, i.e. $n_1 \in S$.
But this is a contradiction, and so T must be empty.

In $\mathbb{N}$, a divides b (written $a|b$) if $b = ac$ for some $c \in N$.

Definition. A number $p \in \mathbb{N}$ is *prime* if the only divisors of p are p and 1, and $p \neq 1$.

Example. 2, 3, 5, 7, 11, 13 are all prime.

Lemma. If n is a natural number, $n \neq 1$, and n is not a prime number, then n is a product of prime numbers.

Principle of Complete Mathematical Induction. If $S \subset \mathbb{N}$ such that:
a) $1 \in S$
b) $(k + 1) \in S$ whenever $\{1, 2, 3, \ldots, k\} \subset S$
then $S = \mathbb{N}$.

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

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

If $k + 1$ is prime, $k + 1 \in S$.
If $k + 1$ is not prime, then $k + 1 = m \cdot n$ with m, n not 1 or $k + 1$.
Since $m \leq k, n \leq k$, $m, n \in S$ by our hypothesis. Each of m and n is either prime or the product of primes, so $k + 1$ is the product of the primes that multiply to m and the primes that multiply to n. Therefore $k + 1 \in S$.
Therefore, by complete mathematical induction, $S = N$.

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

Theorem. There is no largest prime number.

Proof: Suppose p is the largest prime number.
Multiply all the primes from 2 up to p together and then add 1.
Let $M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p + 1$.

Now $M > p$, so if M is prime, we're done.
On the other hand, suppose M is not prime. Since $M > 1$, by the corollary, $q|M$ (q divides M) for some prime q.

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

Note that $q \neq 2$ since M leaves remainder 1 upon division by 2.
In fact, for any prime $r \leq p$, M leaves remainder 1 upon division by r.
Therefore $q \neq r$ for any $r \leq p$, and so $q > p$, finishing the proof.

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

e.g. 2,3; 5,7; 11,13; 17,19; 23,29