For the sake of this section let $\mathbb{N}$ contain 0.

Principle of Mathematical Induction

The set of natural numbers ($\mathbb{N}$) can be constructed in many ways. One of these ways is known as the *Peano axioms*:

i) There is a least element of $\mathbb{N}$ that we denote by 0.

ii) Every natural number a has a successor denoted by $s(a)$.

iii) There is no natural number whose successor is 0. $\nexists x \in \mathbb{N}$ s.t. $s(x) = 0$

iv) Distinct natural numbers have distinct successors.

$a \neq b$ $\quad a, b \in \mathbb{N}$

$s(a) \neq s(b)$

v) If a subset of the natural numbers contains 0 and also has the property that whenever $a \in S$ it follows that $s(a) \in S$, then the subset S is actually equal to $\mathbb{N}$.

S: $\quad 0 \quad s(0) \quad s(s(0)) \quad \ldots$

$s(0) = 1$

$s(s(0)) = s(1) = 2$

$0 \uparrow$ least element

The last axiom enables us to state the Principle of Mathematical Induction (PMI).

PMI is a very strong tool for proving propositions about integers.

Informally, the idea is to first show that the proposition is true for the smallest integer for which the proposition is claimed to be true. Once this is accomplished, we show that if the proposition is true for some admissible integer then it is also true for the next admissible integer. These steps together give us a proof that the proposition is true for any integer (for which it is defined). A more precise description follows.

Let $P(n)$ be a proposition about integers. Let n_0 be the smallest integer for which the proposition is defined.

PMI: If (1) $P(n_0)$ is T (true), and
(2) $P(k) \to P(k+1)$ is T for all $k \geq n_0$,
then $P(n)$ is T for all $n \geq n_0$.

Show $P(n_0)$ is T for the smallest meaningful choice of n_0

and show $P(k)$ is T $\Rightarrow$ $P(k+1)$ is T

$$\underset{\substack{\shortparallel \\ n_0}}{0} \frown \underset{1}{\overset{s(0)}{\shortparallel}} \frown \underset{2}{\overset{s(1)}{\shortparallel}} \frown \underset{3}{\overset{s(2)}{\shortparallel}} \frown \ldots$$

How to do/write a proof by induction:

(i) Clearly state $P(n)$.

(ii) Basis of induction (BI): Choose an appropriate n_0 and prove that $P(n_0)$ is true.

(iii) Induction Step (IS): Prove that $P(k) \to P(k+1)$ is True for all $k \geq n_0$.

- Assume that $P(k)$ is T for some $k \geq n_0$ (this is the **induction hypothesis** (IH)).
- Show that $P(k+1)$ is T follows.

(iv) Conclusion: By PMI, since $P(n_0)$ is T and $P(k) \to P(k+1)$ is T for $k \geq n_0$, it follows that $P(n)$ is T for all $n \geq n_0$.

Now it's time to solve so many examples on mathematical induction that eventually you will see mathematical induction in your dreams.

Example: Use mathematical induction to prove that

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

for all integers $n \geq 1$.

$P(n): \; 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \qquad n \geq 1$

Basis of induction: $n_0 = 1$

We show that $P(n_0) = P(1)$ is true:

$1 = \frac{1 \cdot (1+1)}{2}$ we see that equality holds, so $P(1)$ is true.

Induction step: Suppose $P(k)$ is true $(k \geq 1)$ and show that $P(k+1)$ is true.

Since $P(k)$ is supposed to be true, we have $\underline{1 + 2 + \ldots + k} \overset{*}{=} \frac{k(k+1)}{2}$. We want to show that $P(k+1)$ is true. $P(k+1)$: "$\underline{1 + 2 + \ldots + k} + (k+1) = \frac{(k+1)((k+1)+1)}{2}$"

From $*$, LHS of $P(k+1)$ can be written as $\frac{k(k+1)}{2} + k+1$. Then, $\frac{k(k+1)}{2} + k+1$

$$= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+2)(k+1)}{2} = \frac{(k+1)(k+2)}{2}$$

$$= \frac{(k+1)((k+1)+1)}{2}.$$

So, we showed that $P(k+1)$ holds.

By the Basis of Induction and the Induction step, the proof is now complete

Example: Use mathematical induction to prove that for any real number r except 1, and any integer $n \geq 0$,

$P(n): \sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}, n \geq 0$

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}.$$

BI: Show that $P(n_0) = P(0)$ is true.

LHS: $\sum_{i=0}^{0} r^i = r^0 = 1$ RHS: $\frac{r^{0+1}-1}{r-1} = \frac{r-1}{r-1} = 1$

LHS = RHS, so BI is completed.

IS: Suppose $P(k)$ is true ($k \geq 0$), and show that $P(k+1)$ follows. So we suppose that

$P(k): \sum_{i=0}^{k} r^i \overset{*}{=} \frac{r^{k+1}-1}{r-1}$. Show $P(k+1)$ is true.

$P(k+1): \sum_{i=0}^{k+1} r^i = \boxed{\frac{r^{(k+1)+1}-1}{r-1}}$.

LHS of $P(k+1)$: $\sum_{i=0}^{k+1} r^i = \left(\sum_{i=0}^{k} r^i\right) + r^{k+1} \overset{*}{=} \frac{r^{k+1}-1}{r-1} + r^{k+1}$

$= \frac{r^{k+1}-1}{r-1} + \frac{(r-1)\cdot r^{k+1}}{(r-1)} = \frac{r^{k+1}-1+(r-1)\cdot r^{k+1}}{r-1}$

$= \frac{(r-1+1)r^{k+1}-1}{r-1} = \frac{r\cdot r^{k+1}-1}{r-1} = \boxed{\frac{r^{(k+1)+1}-1}{r-1}}$

This is exactly the RHS of $P(k+1)$.

So, the induction step is complete. By BI and IS, we proved that the given proposition is true for all integers $n \geq 0$

Example: Use mathematical induction to prove that for all integers $n \geq 0$,

$$2^{2n} - 1 \text{ is divisible by 3.}$$

$P(n)$: $2^{2n} - 1$ is divisible by 3, $n \geq 0$

BI: show $P(n_0) = P(0)$ is true. $P(0)$: $2^{2\cdot 0} - 1$ is divisible by 3

$P(0)$: "0 is divisible by 3".

$P(0)$ is true because $0 = \underset{\in \mathbb{Z}}{0} \cdot 3$ (so $3 \mid 0$).

IS: Suppose $P(k)$ is true ($k \geq 0$). So $2^{2k} - 1$ is divisible by 3. * We want to show that $P(k+1)$ is true. So, we want to show that

$2^{2(k+1)} - 1$ is divisible by 3.

Consider $2^{2(k+1)} - 1$. $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^{2k} \cdot 2^2 - 1$

$= 4 \cdot 2^{2k} - 1 = (3+1) \cdot 2^{2k} - 1 = \underbrace{3 \cdot 2^{2k}}_{\text{is divisible by 3 because it is 3 times an integer.}} + \underbrace{2^{2k} - 1}_{\text{By * } 2^{2k}-1 \text{ is divisible by 3.}}$

So, we see that $2^{2(k+1)} - 1$ is divisible by 3, which completes the IS.

By BI and IS, we completed the proof.

$5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$

$3! = 3\cdot 2\cdot 1 = 6$

For a positive integer k, $k!$ (read: "k **factorial**") is defined as

$$k! = k \cdot (k-1) \cdot (k-2) \cdots 3 \cdot 2 \cdot 1$$

Also,

$$0! = 1.$$

Example: Use mathematical induction to prove that for all integers $n \geq 2$

$$2n < (n+1)!$$

$P(n): 2n < (n+1)!, \ n \geq 2$

BI : $P(2)$: $2\cdot 2 < (2+1)!$ So $4 < \overset{3!}{\overset{\shortparallel}{6}}$ is true, so BI is completed.

IS : Suppose $P(k)$ is true $k \geq 2$, So we suppose that $2\cdot k \underset{*}{<} (k+1)!$. We want to show that $P(k+1)$ is true. So we want to show that $2\cdot(k+1) < \underline{((k+1)+1)!}$

Consider LHS of $P(k+1)$: $2(k+1) = 2k+2$

By $*$ $2k+2 < (k+1)! + 2 = \left(1 + \frac{2}{(k+1)!}\right)\cdot(k+1)!$

$\leq (k+2)\cdot(k+1)! = (k+2)! = \underline{((k+1)+1)!}$

So we showed $P(k+1)$ is true, which completes the IS and therefore also the proof.

Example: Prove that for all integers $n \geq 1$

$$1 \cdot 1! + 2 \cdot 2! + \ldots + n \cdot n! = (n+1)! - 1.$$

exercise

Example: Prove that for all integers $n \geq 0$

$$7^n - 2^n \text{ is divisible by } 5.$$

$P(n)$: $7^n - 2^n$ is divisible by 5 $(n \geq 0)$.

BI : $P(0)$: $7^0 - 2^0$ is divisible by 5.

$7^0 - 2^0 = 1 - 1 = 0$ and 0 is indeed divisible by 5 because $0 = \underbrace{0}_{\in \mathbb{Z}} \cdot 5$.

So $P(0)$ is true.

IS : Suppose $P(k)$ is true $(k \geq 0)$. So,

(*) $7^k - 2^k$ is divisible by 5.

We want to show that $P(k+1)$ is true.

$P(k+1)$: $7^{k+1} - 2^{k+1}$ is divisible by 5.

Consider $7^{k+1} - 2^{k+1} = 7 \cdot 7^k - 2 \cdot 2^k$

$$= 7 \cdot 7^k - 2 \cdot 2^k + 7 \cdot 2^k - 7 \cdot 2^k$$

$$= 7(7^k - 2^k) + (7-2) \cdot 2^k = 7 \cdot (7^k - 2^k) + 5 \cdot 2^k.$$

By ~~the~~ (*) $7^k - 2^k$ is divisible by 5, so $7 \cdot (7^k - 2^k)$ is divisible by 5. Also $5 \cdot 2^k$ is divisible by 5 (because it is 5 times an integer). Therefore, $7 \cdot (7^k - 2^k) + 5 \cdot 2^k$ is divisible by 5, showing that $P(k+1)$ is true. This finishes the IS.

By the BI and the IS, we showed that $7^n - 2^n$ is divisible by 5 for $n \geq 0$.

"big product"

Example: Prove that $\forall n \geq 2 \in \mathbb{Z}$

$$\prod_{j=2}^{n}(1 - \frac{1}{j^2}) = \frac{n+1}{2n}.$$

left as an exercise

The Strong Form of Mathematical Induction

The strong form of mathematical induction is so-called because the hypotheses we use are stronger.

Let $P(n)$ be a proposition about integers. Let n_0 be the smallest integer for which the proposition is defined.

Instead of showing that $P_k \to P_{k+1}$ in the inductive step, this time we get to assume that all the statements numbered smaller than P_{k+1} are true.

The statement that needs to be proved in the inductive step is:

$$\forall k(P_{n_0} \wedge P_{n_0+1} \wedge \ldots \wedge P_{k-1} \wedge P_k) \to P_{k+1}.$$

Therefore, a proof by strong induction goes as follows.

(1) Show that $P(n_0)$ is true, and

(2) Show that $\forall k(P_{n_0} \wedge P_{n_0+1} \wedge \ldots \wedge P_{k-1} \wedge P_k) \to P_{k+1}$ is true.

Then $P(n)$ is true for all $n \geq n_0$.

An integer $p > 1$ is called a **prime number** if 1 and p are the only positive divisors of p. An integer $n > 1$ is called a **composite number** if n is not a prime number.

Lemma: Any integer $n > 1$ has a prime factor.

Proof by strong induction: Let $P(n)$ be the proposition that $n > 1$ has a prime factor. $n_0 = 2$

Basis of induction: $P(2)$ is true. 2 is a prime factor of 2. So 2 has a prime factor. So $P(2)$ is true.

Inductive step: Suppose that $P(i)$ is true for $2 < i \leq k$. Show that $P(k+1)$ follows.

Consider $k+1 > 1$. If $k+1$ itself is a prime, then we are done because $k+1$ is a product of one prime. (So $k+1$ is a prime factor of $k+1$.)

Suppose $k+1$ is a composite number. Then $k+1 = ab$ for some positive integers $a \geq 2$ and $b \geq 2$.

⋮

$k+1 = a \cdot b \quad (a, b \geq 2)$

Then $a < k+1$ and $b < k+1$.
Then by the induction hypothesis a has a prime factor, say c.
So $k+1 = a \cdot b$ (where c is a prime factor of a).
Then c is a prime factor of $k+1$, and we are done.

Repeated application of this procedure yields the following result:

Fundamental Theorem of Arithmetic: Any integer greater than 1 can be expressed as a product of one or more prime numbers.