Induction

Motivating example

Q: What happens if we add the first several odd integers together?

$1 = 1 = 1^2$

$1+3 = 4 = 2^2$

$1+3+5 = 9 = 3^2$

$1+3+5+7 = 16 = 4^2$

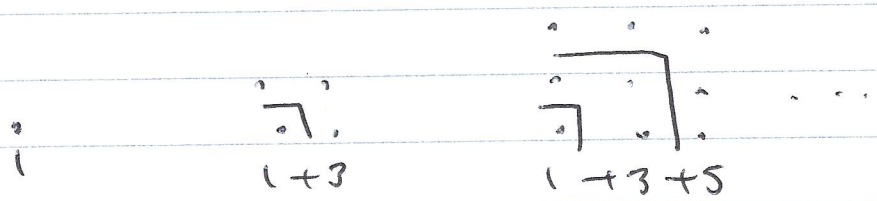
$1+3+5+7+9 = 25 = 5^2$

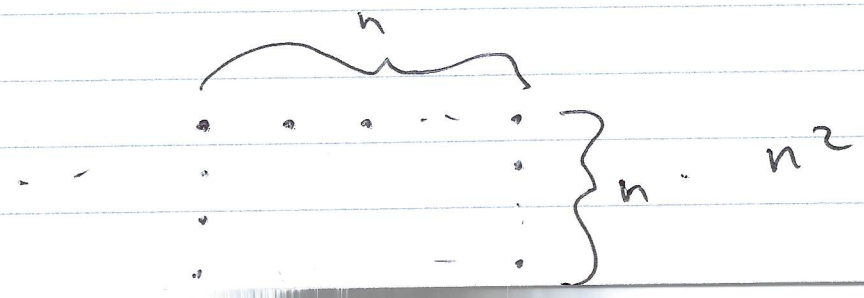
$\vdots$

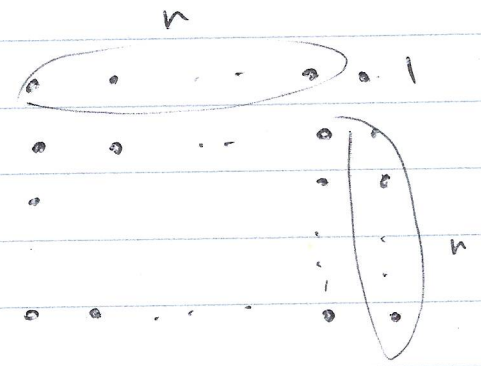
$1+3+5+\cdots+2n-1 \overset{??}{=} n^2$

watch indices

Picture:







$n^2 + 2n - 1 = (n+1)^2$

- How would we prove this identity for every $n \in \mathbb{N}$?
- picture suggests that proof for $n+1$ depends on proof for n.

Theorem For every $n \in \mathbb{N}$ we have

$$1 + 3 + \cdots + (2n-1) = n^2$$

i.e.

$$\sum_{k=1}^{n} 2k-1 = n^2$$

Pf: - Clearly true if $n=1$ since

$$\sum_{k=1}^{1} k = 1 = 1^2$$

- suppose $n \in \mathbb{N}$ is fixed and we have the identity for n

1.1. We know

$$\sum_{k=1}^{n} 2k-1 = n^2$$

Now: Consider the next sum:

$$\sum_{k=1}^{n+1} 2k-1 = 1+3+\cdots+2n-1+2(n+1)-1$$

$$= \left(\sum_{k=1}^{n} 2k-1\right) + 2n+1$$

Then by the identity for n we have

$$= n^2 + 2n + 1$$

$$= (n+1)^2$$

- What have we shown?
  (a) the identity holds for $n=1$
  (b) if the identity holds for n then it holds for $n+1$ as well.

- But then since it holds for $n=1$ it must also hold for $n=2$
  and so for $n=3$
  and so for $n=4$
  ⋮
  and so for <u>every</u> $n \in \mathbb{N}$ ✓

—The validity of this kind of argument is called the principle of mathematical induction (PMI)

Theorem (PMI)

Let $P(n)$ be a variable prop'n. Suppose that

(1) $P(1)$ holds

(2) $(\forall n \in \mathbb{N})\ (P(n) \Rightarrow P(n+1))$ holds

then

$(\forall n \in \mathbb{N})\ P(n)$ holds.

↳ There is a "proof" of PMI in the book, but it's a bit bogus

↳ We'll take PMI as an axiom, and later show it is equiv. to another intuitively clear principle.

How to use PMI to prove $\forall n P(n)$

(1) (Base case) Verify $P(1)$ directly
(2) (Inductive Hypothesis) Let $n \in \mathbb{N}$ be arbitrary but fixed. Assume $P(n)$
(3) Deduce $P(n+1)$, using this hypothesis

PMI tells you: if you can do (1)+(2)+(3) then $(\forall n \in \mathbb{N})\ P(n)$ holds.

Examply

(1) Q: what is the sum of the first n naturals?

i.e. what is

$$1+2+\cdots+n = \sum_{k=1}^{n} k \ ?$$

Theorem For any $n \in \mathbb{N}$ we have

$$\sum_{k=1}^{n} k = \frac{n\cdot(n+1)}{2}$$

↳ before proving, let's verify for the first few possible values of n.

$n=1$ $\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$ ✓

$n=2$ $\sum_{k=1}^{2} k = 1+2 = 3 = \frac{2(2+1)}{2}$ ✓

$n=3$ $\sum_{k=1}^{3} k = 1+2+3 = 6 = \frac{3\cdot 4}{2}$ ✓

↳ formula looks plausible, let's prove it.

Pf: Let $P(n)$ be the prop'n

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

Base Case: $P(1)$ is true since

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

Inductive hypothesis: Fix $n \in \mathbb{N}$. Assume $P(n)$, i.e. assume

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

Now, consider

$$\sum_{k=1}^{n+1} k = \underbrace{1+2+\cdots+n}_{\sum_{k=1}^{n} k} + (n+1)$$

$$= \sum_{k=1}^{n} k + n+1$$

by the IH, we have

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

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

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

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

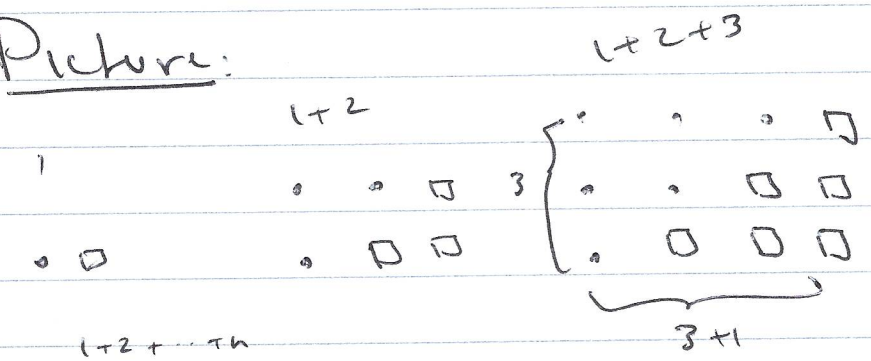
$$= \frac{(n+1)((n+1)+1)}{2}$$

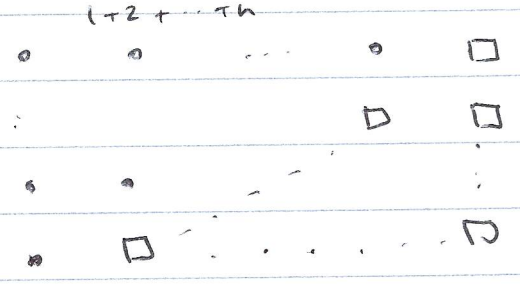
hence $P(n+1)$ holds ✓

By PMI we may conclude $(\forall n \in \mathbb{N})\, P(n)$, i.e. for any $n \in \mathbb{N}$ we have

$$\sum_{k=1}^{n} k = \frac{n \cdot (n+1)}{2}$$ ✓

Picture:





Notice: - the proof above doesn't give much insight into how we might have guessed the formula

$$\sum_{k=1}^{n} k = \frac{n\cdot(n+1)}{2}$$

- but if we can guess such a formula (or it's handed to us) PMI allows us to prove it $\forall n \in \mathbb{N}$.

② **Geometric Series** thm Suppose $x \in \mathbb{R}$ and $x \neq 0, 1$. Then for any $n \in \mathbb{N}$ we have:

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$$

1.1.

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

Pf: - Fix $x \in \mathbb{R}$ with $x \neq 0, 1$

(BC) The identity holds for $n = 1$ since

$$\sum_{k=0}^{1-1} x^k = \sum_{k=0}^{0} x^k = x^0 = 1 = \frac{x^1 - 1}{x - 1}$$

↳ Notice we use $x \neq 0$ and $x \neq 1$ to even verify the BC.

(IH) Fix $n \in \mathbb{N}$. Assume the identity form:

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

Now consider

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

$$\overset{\text{by IH}}{=} \frac{x^n - 1}{x - 1} + x^n$$

$$= \frac{x^n - 1}{(x-1)} + \frac{x^n(x-1)}{(x-1)}$$

$$= \frac{x^n - 1 + x^{n+1} - x^n}{x-1}$$

$$= \frac{x^{n+1} - 1}{x-1}$$

hence the identity holds for $n+1$

By PMI, the identity holds $\forall n \in \mathbb{N}$ ✓

(3) Prop'n For any $n \in \mathbb{N}$, $7^n - 4^n$ is a multiple of 3.

Pf: (BC) if $n=1$ the statement holds since $7^1 - 4^1 = 3$, which is a multiple of 3

(IH) Fix $n \in \mathbb{N}$, and assume $7^n - 4^n$ is a multiple of 3, i.e. $\exists k \in \mathbb{N}$ s.t.

$$7^n - 4^n = 3k.$$

Now, observe:

$$7^n = 3k + 4^n \qquad \text{(by IH)}$$

hence $\quad 7^{n+1} = (3k + 4^n)7$

$$= 21k + 7 \cdot 4^n$$
$$= 21k + (4+3)4^n$$
$$= 21k + 3 \cdot 4^n + 4^{n+1}$$

Hence $7^{n+1} - 4^{n+1} = 21k + 3 \cdot 4^n$
$= 3(7k + 4^n)$
$= 3M$

Hence $7^{n+1} - 4^{n+1}$ is a multiple of 3. ✓

By PMI we may conclude $(\forall n \in \mathbb{N})[(7^{n+1} - 4^n)$ is a multiple of 3$]$

Variants of Induction

↳ nothing special about starting at $n=1$
↳ as long as we have $P(n_0)$ for some (possibly negative) n_0 and $\forall n \geq n_0$ we have $P(n) \Rightarrow P(n+1)$, can conclude $\forall n \geq n_0$ $P(n)$.

Thm (PMI w/ a different base case)

- Suppose $P(n)$ is a var. prop'n and $n_0 \in \mathbb{Z}$ is fixed.
- Let $S = \{n \in \mathbb{Z} \mid n \geq n_0\} = [n_0, n_0+1, n_0+2, \ldots)$

- Suppose we know
  1. $P(n_0)$ holds
  2. $(\forall n \in S)\ (P(n) \Rightarrow P(n+1))$ holds

then

$(\forall n \in S)\ P(n)$ holds.

↳ can prove this using regular PMI, though it is equally obvious (see back if interested)

↳ template nearly the same as w/ regular PMI:

1. Verify $P(n_0)$
2. Fix $n \geq n_0$, assume $P(n)$
3. Deduce $P(n+1)$.

Ex's ① Q: for which $n \in \mathbb{N}$ do we have

$$n! > 2^n ?$$

n	$n!$	2^n
1	1	2
2	2	4
3	6	8
4	24	16
5	120	32

Seems like: $\forall n \geq 4$ we have $n! > 2^n$
Let's prove this.

Theorem For every $n \in \mathbb{N}$ with $n \geq 4$ we have $n! > 2^n$.

Pf: Let $P(n)$ be the prop'n "$n! > 2^n$".

(BC) $P(4)$ holds since $4! = 24 > 16 = 2^4$

(IH) Let $n \geq 4$ be fixed and assume $P(n)$, i.e. assume

$$n! > 2^n$$

Now, consider $(n+1)!$

We have:

$$(n+1)! = (n+1)\,n!$$

$$> (n+1) \cdot 2^n \quad \text{by IH}$$

$$> 2^{n+1} \quad \text{since } n \geq 4 \text{ we knew } n+1 > 2$$

So P(n+1) holds

- by induction we have $\forall n \in \mathbb{N}$ if $n \geq 4$ then $n! > 2^n$. ✓

Induction with jumps

- Sometimes want to prove P(n), not for all n, but when n is even, or when n is odd, or when n is a multiple of 5
- We can also argue inductively in such cases.

Thm - Let P(n) be a var. prop'n and suppose $n_0 \in \mathbb{Z}$ and $k \in \mathbb{N}$ are fixed (n_0 is the "starting point" and k is the "jump")

- Let $S = \{n_0, n_0+k, n_0+2k, \ldots\}$

If:

① P(n_0) holds

② $(\forall n \in S)(P(n) \Rightarrow P(n+k))$ holds

then: $(\forall n \in S)\, P(n)$ holds

e.g. if $E = \{2, 4, 6, \ldots\}$
and we can show $P(2)$
and if $P(n)$ then $P(n+2)$
then we have $P(n)$ for all $n \in E$.

Ex's ① Consider the alternating sum of the first n squares:

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2$$

$$= \sum_{k=1}^{n} (-1)^{k-1} k^2$$

Propln (1) if n is odd we have

$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = + \sum_{k=1}^{n} k$$

(2) if n is even we have

$$\sum_{k=1}^{n} (-1)^{k-1} = - \sum_{k=1}^{n} k$$

PF: (1) (here: $n_0 = 1$ and ~~$k_{inf} = 2$~~)

(BC) if $n = 1$

$$\sum_{k=1}^{1} (-1)^{k-1} k^2 = (-1)^0 1^2 = 1$$

$$= \sum_{k=1}^{1} k \quad \checkmark$$

(IH) Assume $n \geq 1$ is odd and

$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = \sum_{k=1}^{n} k$$

Now consider the sum up to $n+2$:

$$\sum_{k=1}^{n+2} (-1)^{k-1} k^2$$

$$= \sum_{k=1}^{n} (-1)^{k-1} k^2 \quad \textcircled{*} \quad -(n+1)^2 + (n+2)^2$$

IH $\longrightarrow$ $= \sum_{k=1}^{n} k + \left[(n+2)^2 - (n+1)^2\right]$

$$= \sum_{k=1}^{n} k + \left[\cancel{(n+2)} - (n+1)\right]\left[(n+2) + (n+1)\right]$$

$$= \sum_{k=1}^{n} k + n+1 + n+2$$

$$= \sum_{k=1}^{n+2} k$$

hence the identity holds for $n+2$.

By induction we have for every n odd

$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = \sum_{k=1}^{n} k$$

$P(n)$ is "$\sum_{k=1}^{n} (-1)^{k-1} = \sum_{k=1}^{n} k$"

We showed
- $P(1)$
- if n is odd $P(n) \Rightarrow P(n+2)$
- hence $P(n)$ is true $\forall n \in \{1, 3, \dots\}$

For n even:

(BC) if $n=2$ then

$$\sum_{k=1}^{2} (-1)^{k-1} k^2 = 1^2 - 2^2 = -3$$

$$= -(1+2)$$

$$= -\sum_{k=1}^{2} k$$

(IH) Assume n is even and

$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = -\sum_{k=1}^{n} k$$

Now consider:

$$\sum_{k=1}^{n+2} (-1)^{k-1} k^2 = -\sum_{k=1}^{n} (-1)^{k-1} k + (n+1)^2 - (n+2)^2$$

$$\overset{IH}{=} -\sum_{k=1}^{n} k + (n+1)^2 - (n+2)^2$$

$$= -\sum_{k=1}^{n} k + [(n+1) - (n+2)]$$

$$[(n+1) + (n+2)]$$

$$= -\sum_{k=1}^{n} k - (n+1) - (n+2)$$

$$= -\sum_{k=1}^{n+2} k$$

hence, by induction, the identity holds $\forall n \in \{2, 4, \ldots\}$

② The Fibonacci Sequence:

Recall: the Fibonacci Sequence is defined recursively by:

$f_0 = 0 \quad f_1 = 1$ and $\forall n \in \mathbb{N}, n \geq 2$

$f_n = f_{n-1} + f_{n-2}$

$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$
$f_0 \; f_1 \; f_2 \; f_3 \; f_4 \ldots$

Thm: (i) for every $n \in \mathbb{N}$ we have:

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1$$

(i.e. $f_1 + f_2 + \ldots + f_n = f_{n+2} - 1$)

Pf (BC) for $n=1$ we have

$$\sum_{k=1}^{1} f_k = f_1 = 1 = 2-1 = f_3 - 1 \quad \checkmark$$

(IH) Fix $n \in \mathbb{N}$, and assume the identity for n, that is,

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1$$

Consider the sum for $n+1$:

$$\sum_{k=1}^{n+1} f_k = \sum_{k=1}^{n} f_k + f_{n+1}$$

$$= f_{n+2} - 1 + f_{n+1}$$

$$= f_{(n+1)+2} - 1$$

hence the identity holds for $n+1$.
hence, by induction, the identity holds for all $n \in \mathbb{N}$.

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1 \quad \checkmark$$

(ii) if n is a multiple of 3, then f_n is even

Pf (BC) if $n=3$ then $f_3 = 4$ and the statement holds

(IH) Suppose n is a multiple of 3 and f_n is even.

Consider f_{n+3}

$$f_{n+3} = f_{n+2} + f_{n+1}$$

$$= f_n + f_{n+1} + f_{n+1}$$

$$= f_n + 2f_{n+1}$$

by IH, f_n is even; hence $f_n + 2f_{n+1}$ is even

that is, f_{n+3} is even

- hence the statement holds for $n+3$.

By induction, f_n is even for every $n \in \{3, 6, 9, \ldots\}$

Strong Induction

- In certain proofs, to show $P(n+1)$ holds we may need to assume more than just $P(n)$
- e.g. may need to assume $P(n)$ and $P(n-1)$
  or $P(n), P(n-1), P(n-2), \ldots, P(1)$

- this is still a legitimate inductive hypothesis to make!
- this type of argument is called strong induction.

Theorem (PSMI) (Principle of Strong Mathematical Induction)

Suppose $P(n)$ is a var prop'n and suppose

(1) $P(1)$ holds

(2) $(\forall n \in \mathbb{N})\ ((\forall k \in \{1, \ldots, n\}\ P(k)) \Rightarrow P(k+1))$ holds

Then:

$(\forall n \in \mathbb{N})\ P(n)$ holds.

Template for Strong Induction

① Show $P(1)$ directly
② Fix $n \geq 1$. Assume $\forall k \in \{1, \ldots, n\}\ P(k)$
(that is, $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$)
③ From this, deduce $P(n+1)$

then PSMI gives: $(\forall n \in \mathbb{N}) P(n)$

↳ SPMI seems harder to apply than PMI
(we have to assume more:
all of $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$, not just
$P(n)$, to get $P(n+1)$)

↳ but can actually prove SPMI
from PMI.

Pf: - Let $P(n)$ be a variable
prop'n s.t.

[redacted]

① $P(1)$ holds
② $((\forall k \in [n])\ P(k)) \Rightarrow P(n+1)$ holds

- Let $Q(n)$ be the prop'n $(\forall k \in [n])\ P(k)$

- We proceed by induction on $Q(n)$

- (BC) $Q(1)$ is the statement $(\forall k \in \{1\})\ P(k)$
- this is equivalent to $P(1)$ which holds by ①. Hence $Q(1)$ holds ✓

(IH) Fix $n \in \mathbb{N}$ and assume $Q(n)$ holds, i.e. assume $(\forall k \in [n])\ P(k)$

- then by ② we have that $P(n+1)$ holds
- hence the conjunction $(\forall k \in [n])\ P(k) \wedge P(n+1)$ holds
- this is equivalent to saying $(\forall k \in [n+1])\ P(k)$ holds

- i.e. $Q(n+1)$ holds.

- we have shown
  ① $Q(1)$ holds
  ② $(\forall n \in \mathbb{N})(Q(n) \Rightarrow Q(n+1))$ holds

- hence by PMI we know
  $(\forall n \in \mathbb{N})\, Q(n)$ holds

- i.e. $\forall n \in \mathbb{N}$ we have
  $(\forall k \in [n])\, P(k)$ holds "$P(1) \wedge P(2) \wedge \cdots \wedge P(n)$"

- but this implies that $\forall n \in \mathbb{N}$
  $P(n)$ holds.

- this is what we wanted to show. ✓

Example
↳ PMI often used when dealing with recursively defined sequences

① Let s_n be the sequence defined by

$$s_0 = 1 \quad \text{and for } n > 1 \quad s_n = 1 + \sum_{k=0}^{n-1} s_k$$

So that: $s_1 = 1 + s_0 = 1 + 1 = 2$

$s_2 = 1 + s_0 + s_1 = 1 + 1 + 2 = 4$

$s_3 = 1 + s_0 + s_1 + s_2 = 1 + 1 + 2 + 4 = 8$

Seems like $S_n = 2^n$

Let's prove this.

Claim: $\forall n \in \mathbb{N} \cup \{0\}$ we have $S_n = 2^n$

Pf: (SC) If $n=0$, $S_0 = 1 = 2^0$ and the identity holds.

(IH) Fix $n \geq 0$ and assume that for every $k \in \{0, 1, \ldots, n\}$ we have $S_k = 2^k$

Then

$$S_{n+1} = 1 + \sum_{k=0}^{n} S_k$$

Strong IH $\rightarrow$

$$= 1 + \sum_{k=0}^{n} 2^k$$

Geometric series fmla $\rightarrow$

$$= 1 + \frac{2^{n+1} - 1}{2 - 1}$$

$$= 1 + 2^{n+1} - 1 = 2^{n+1}$$

Hence the identity holds for $n+1$.

by the SPMI we have, $\forall n \in \mathbb{N} \cup \{0\}$

$S_n = 2^n$ ✓.

Def'n For an $n \in \mathbb{N}$ with $n > 1$, a prime factorization for n is a way of writing n as a product of primes (w/ possible repeats)

e.g. -2 is a prime factorization of 2

$-2 \cdot 3$ is a prime factorization of 6

$-2 \cdot 3 \cdot 3$ is a prime factorization of 18.

Theorem For every $n \in \mathbb{N}$ with $n > 1$, n has a prime factorization.

Pf. - Let $F(n)$ be the statement "n has a prime factorization"

- We prove $(\forall n \geq 2)\ F(n)$ by strong induction.

(BC) $F(2)$ holds because 2 has a prime factorization.

(IH) Fix $n \geq 2$ and assume for every k with $2 \leq k \leq n$ that k has a prime factorization (i.e. $F(k)$ holds)

- Now, Consider $n+1$. If $n+1$ is prime then $n+1 = n+1$ is a prime factorization.
- If $n+1$ is not prime then $n+1$ can be factored as
$$n+1 = a \cdot b$$
where $a, b \in \mathbb{N}$ and $2 \leq a, b \leq n$.

- Hence by the IH, a, b have prime factorizations, say
$$a = p_1 p_2 \cdots p_e$$
$$b = q_1 q_2 \cdots q_m$$
where p_i, q_i are all prime

- but then
$n+1 = p_1 \cdots p_e q_1 \cdots q_m$ is a prime factorization of $n+1$
- by SPMI, every $n \geq 2$ has a prime factorization

An example with multiple base cases

Theorem: Every amount of postage that is at least 12 cents can be made from 4 and 5 cent stamps.
i.e. $(\forall n \geq 12)(\exists a,b \in \mathbb{N} \cup \{0\})(n = 4a+5b)$

Pf (BCs)

$n = 12$ $\quad n = 4\cdot 3 + 5\cdot 0$
$n = 13$ $\quad n = 4\cdot 2 + 5\cdot 1$
$n = 14$ $\quad n = 4\cdot 1 + 5\cdot 2$
$n = 15$ $\quad n = 4\cdot 0 + 5\cdot 3$

(IH) Suppose $n \geq 15$, and $\forall k \in \{12, \ldots, n\}$ we have the claim.

Then: $n+1 \geq 16$
hence $n+1-4 \geq 12$

by the IH, $\exists a,b \in \mathbb{N} \cup \{0\}$ s.t.
$n+1-4 = 4\cdot a + 5b$
hence $n+1 = 4a+4+5b$
$= 4(a+1)+5b$

so the claim holds for $n+1$
By SPMI, the claim holds for all $n \geq 12$ ✓

— Multiple base case considerations often pop up when dealing with recursively defined sequences.

(4) Define a sequence x_n recursively by

$x_1 = 2$ $\quad x_2 = 3$ and

$\forall n \in \mathbb{N} - \{1,2\}$ let $x_n = 3x_{n-1} - 2x_{n-2}$

Claim $(\forall n \in \mathbb{N})\ (x_n = 2^{n-1} + 1)$

Pf. (BC's)

$n=1$ $\quad x_1 = 2 = 2^{1-1} + 1$ ✓

$n=2$ $\quad x_2 = 3 = 2^{2-1} + 1$ ✓

(IH) Fix $n \geq 2$ and assume $\forall k \leq n$ we have $x_n = 2^{n-1} + 1$

Then
$$\begin{aligned} x_{n+1} &\overset{\text{defn}}{=} 3x_n - 2x_{n-1} \quad \text{⋆} \\ &\overset{\text{IH}}{=} 3(2^{n-1}+1) - 2(2^{n-2}+1) \\ &= 3\cdot 2^{n-1} + 3 - 2\cdot 2^{n-2} - 2 \\ &= 3\cdot 2^{n-1} - 2^{n-1} + 1 \\ &= 2\cdot 2^{n-1} + 1 \\ &= 2^n + 1 \\ &= 2^{(n+1)-1} + 1 \end{aligned}$$

by SPMI we have, $\forall n \in \mathbb{N}$,
$x_n = 2^{n-1} + 1$ ✓

Notice: - we really needed to check both base cases $n=1$ and $n=2$.
- if we had only checked $n=1$ and used "Let $n \geq 1$. Assume $\forall k \leq n$ $x_k = 2^{k-1} + 1$" as our IH, Step ★ would have been unjustified for $n=1$.

$$x_{n+1} = 3x_n - 2x_{n-1}$$
i.e. $x_{1+1} = 3x_1 - 2x_0$ ← undefined!

- you can actually cook up false induction proofs that play on this issue.

- e.g. Let $P(n)$ be the prop'n "In any group of n cats, if one is black, all are black"

Pf:- $P(1)$ is clearly true.
- Suppose $P(n)$ is true.

- now suppose we have a group of n+1 cats, at least one of which is black.
- call the black cat <u>midnight</u>
- Fix another cat, call it <u>Snow</u>. Remove this cat from the group.
- the remaining group of n cats contains a black cat (Midnight) hence by our IH all cats in this group are black.
- Now remove Midnight and put Snow in his place
- in this group of n cats, <u>all</u> are black (except possibly Snow)
- hence again by our IH all cats in this group must be black, including Snow
- hence all n+1 cats are black and P(n+1) holds. ✓
- by induction, P(n) holds for all n

- It follows that since there is a black cat, all cats are black.

The Well-ordering Principle

"Theorem" (WOP) If $X \subseteq \mathbb{N}$ and $X \neq \emptyset$ then X has a least element.

- e.g. if $X = \mathbb{N}$ then its least el't is 1
- if $X = E = \{2, 4, 6, \ldots\}$ its least el't is 2
- if $X = \{n \in \mathbb{N} \mid (\exists k \in \mathbb{N})(k > 5 \wedge n = k^2)\}$
  $= \{36, 49, 64, \ldots\}$
  then its least el't is 36.

↳ This "theorem" is intuitively obvious
↳ we can prove it using SPMI

Pf:- Suppose $X \subseteq \mathbb{N}$ and X has no least el't.
- we'll prove $X = \emptyset$.

- Let $P(n)$ be the var prop'n "$n \notin X$"

- We prove $(\forall n \in \mathbb{N})\, P(n)$ by SPMI

(SC)

Clearly, P(1) is true, that is $1 \notin X$. Because, if $1 \in X$ then 1 would be the 'least el't of X (it is the least el't of N!)

(IH) Fix $n \geq 1$. Suppose $\forall k \leq n$ P(k) holds, i.e. $(\forall k \leq n)(k \notin X)$

Consider n+1. If $n+1 \in X$ then n+1 is the least el't of X. This follows from our induction hypothesis: since we know $1 \notin X$ $1 \notin X$ $1 \cdots 1 n \notin X$.

- Hence $n+1 \notin X$. That is P(n+1) holds
- by SPMI $(\forall n \in N)$ P(n) holds
- hence $X = \emptyset$. ✓

We have just showed

SPMI $\Rightarrow$ WOP

We previously proved SPMI from PMI, i.e. we showed

PMI $\Rightarrow$ SPMI

In fact, all of these statements are <u>equivalent</u>.

Theorem: The following are equivalent:

1. PMI
2. SPMI
3. WOP

that is

$$\text{PMI} \Leftrightarrow \text{SPMI} \Leftrightarrow \text{WOP}$$

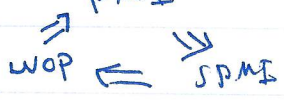
i.e. <u>from</u> any of these statements we can <u>prove</u> the other two.

Pf: We have already shown

$$\text{PMI} \Rightarrow \text{SPMI} \Rightarrow \text{WOP}$$

Hence if we can show

$$\text{WOP} \Rightarrow \text{PMI}$$



we will have proved equivalence

- So assume WOP
- Let $P(n)$ be a var prop'n such that

(1) $P(1)$ holds
(2) $(\forall n \in \mathbb{N})\ (P(n) \Rightarrow P(n+1))$ holds

We want to show $(\forall n \in \mathbb{N})\ P(n)$ holds.

Let $S = \{n \in \mathbb{N} \mid P(n) \text{ fails}\}$

We will use WOP to prove $S = \emptyset$.

- if $S \neq \emptyset$, then by WOP, S has a least el't. Call this el't x.
- We know that $x \neq 1$, since $P(1)$ holds
- hence $x = n+1$ for some $n \in \mathbb{N}$.
- by defn of x, $P(n)$ holds
- but then by (2), $P(n+1)$ holds, i.e. $P(x)$ holds, a contradiction
- hence no such x exists, i.e. $S = \emptyset$.
- hence $(\forall n \in \mathbb{N})\ P(n)$ holds. ✓

↳ All three principles WOP, PMI, and sPMI are so basic

that in many contexts they are taken as axiom

↳ content of theorem is: if you assume any one of them, the other two are entailed.

↳ the central idea in the above proof "finding a minimal counterexample" is useful in its own right.

Example Prop'n every natural number $n > 1$ can be written $n = 2 \cdot a + 3 \cdot b$ for some $a, b \in \mathbb{N} \cup \{0\}$

e.g. $2 = 2 \cdot 1 + 3 \cdot 0$
$7 = 2 \cdot 2 + 3 \cdot 1$, etc.

Pf: - Suppose not. That is, suppose there is a number ≥ 2 that cannot be so written.
- let N be the least such number.
- by above, $N > 2$

- hence $N = n+1$ for some $n \geq 2$.
- since N was the least counterexample we have

$$n = 2 \cdot a + 3 \cdot b \quad \text{for some } a, b \in \mathbb{N} \cup \{0\}$$

- observe: at least one of a, b is positive
- if $a > 0$ then

$$N = n+1 = 2a + 3b + 1$$
$$= 2(a-1) + 2 + 3b + 1$$
$$= 2(a-1) + 3(b+1)$$

- if $b > 0$ then

$$N = n+1 = 2a + 3(b-1) + 3 + 1$$
$$= 2(a+2) + 3(b-1)$$

- hence in either case, N does have a representation of the form

$$N = 2x + 3y \qquad x, y \in \mathbb{N} \cup \{0\}$$

- this contradicts the def^n of N.

- hence in fact $\forall n \geq 2$ we have $a, b \in \mathbb{N} \cup \{0\}$ s.t.

$$n = 2a + 3b \checkmark$$