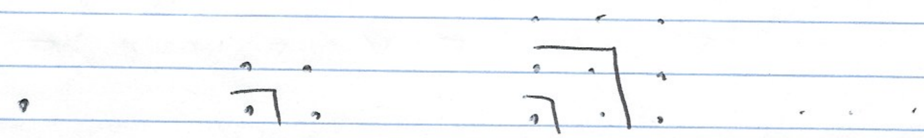
Induction

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

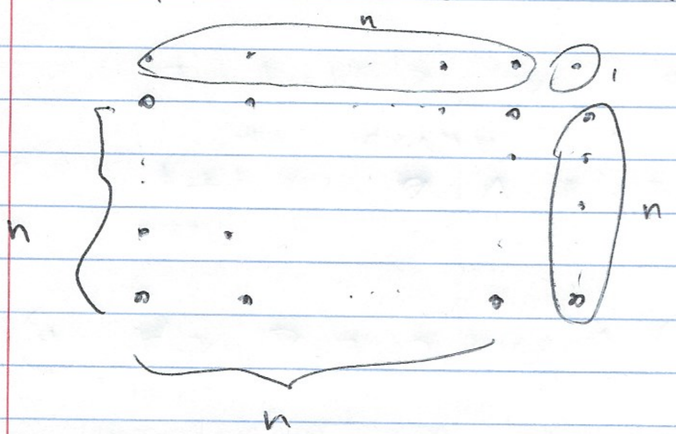
$$1 = 1 = 1^2$$
$$1 + 3 = 4 = 2^2$$
$$1 + 3 + 5 = 9 = 3^2$$
$$1 + 3 + 5 + 7 = 16 = 4^2$$

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

Picture:



1 $\qquad$ 1+3 $\qquad$ 1+3+5



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

How would we prove $(*)$ for every $n \in \mathbb{N}$?

Picture suggests proof for $n+1$ depends on a 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 for $n=1$ since

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

– Sps $n \in \mathbb{N}$ is fixed and we have the identity for n, i.e.

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

– Now consider $n+1$ sum:

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

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

$$= n^2 \quad + 2n+1$$

by our assumption

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

<u>We've shown</u>
(a) identity holds for $n=1$
(b) if it holds for a fixed n
then it holds for $n+1$ too.

But then: since it holds for $n=1$, it holds for $n=2$
and so for $n=3$
and so for $n=4$
⋮
and so <u>for</u> <u>all</u> $n \in \mathbb{N}$! ✓

Validity of this kind of argument is called <u>principle</u> of <u>mathematical induction</u> (PMI)

<u>Theorem</u> Suppose $P(n)$ is a variable prop'n. Suppose further that
① $P(1)$ holds
② $(\forall n \in \mathbb{N})\,(P(n) \Rightarrow P(n+1))$ holds

<u>then</u> $(\forall n \in \mathbb{N})\, P(n)$ holds.

↳ for a "proof" see the back.
→ we'll take PMI as an <u>axiom</u>, and later show it is equiv. to another intuitively obvious principle.

<u>Using</u> <u>PMI</u> to <u>prove</u> <u>$(\forall n \in \mathbb{N})\, P(n)$</u>

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

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

<u>Ex</u> ① What happens if we sum the first n natural numbers?

$$1 + 2 + \cdots + n \overset{??}{=}$$

<u>Thm</u> For every $n \in \mathbb{N}$ we have

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

Before proving, let's check a few n's:

<u>$n=1$</u> $\quad \sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$ ✓

<u>$n=2$</u> $\quad \sum_{k=1}^{2} k = 1+2 = 3 = \frac{2(2+1)}{2}$ ✓

<u>$n=3$</u> $\quad \sum_{k=1}^{3} k = 1+2+3 = 6 = \frac{3(3+1)}{2}$ ✓

Seems plausible...
let's use PMI to prove..

(5)

Pf: Let $P(n)$ be prop'n
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Base case: $P(1)$ is true since
$$\sum_{k=1}^{1} 1 = 1 = \frac{1(1+1)}{2} \checkmark$$

Inductive hypothesis: Fix $n \in \mathbb{N}$ and assume $P(n)$, i.e.
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Inductive step: Now consider
$$\begin{aligned}
\sum_{k=1}^{n+1} k &= 1+2+\cdots+n+n+1 \\
&= \sum_{k=1}^{n} k + (n+1) \\
&\overset{IH}{=} \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1)+2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)((n+1)+1)}{2}
\end{aligned}$$

hence $P(n+1)$ holds $\checkmark$

by PMI we have, $\forall n \in \mathbb{N}$ $P(n)$ holds. $\checkmark$

Note: - Proof doesn't give insight into how we might have guessed formula
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

- But once we can guess the formula, PMI gives us a way of proving it works $\forall n \in \mathbb{N}$.

② (Geometric series) Thm Suppose $x \in \mathbb{R}$ and $x \neq 0, 1$. Then for every $n \in \mathbb{N} \cup \{0\}$ we have
$$1 + x + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1}$$
i.e.
$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1} \quad \leftarrow \text{call this } P(n)$$

Pf. Fix $x \in \mathbb{R}$, $x \neq 0, 1$

(BC). $P(1)$ holds since:
$$\sum_{k=0}^{0} x^k = x^0 = 1 = \frac{x^1 - 1}{x - 1}$$
since $x \neq 0$ since $x \neq 1$

(IH) Fix $n \in \mathbb{N}$ and assume
$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

(IS) Now consider:

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

by IH

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

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

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

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

hence $P(n+1)$ holds

by PMI, $P(n)$ holds for all $n \in \mathbb{N}$ ✓

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

Pf. (BC) if $n=1$, statement holds since $7^1 - 4^1 = 3$ ✓

(IH) Fix $n \in \mathbb{N}$ and assume $\exists K \in \mathbb{N}$ s.t.

$$7^n - 4^n = 3K$$

(IS) Now, observe:

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

$$\Rightarrow 7^{n+1} = (3K + 4^n)7$$

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

hence

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

hence $7^{n+1} - 4^{n+1}$ is a multiple of 3

By PMI, $7^n - 4^n$ is a multiple of 3 for every $n \in N$.

(i)

Variants of Induction

→ nothing special about $n=1$ as a starting point
→ as long as we can prove $P(n_0)$ and $(\forall n \geq n_0)(P(n) \Rightarrow P(n+1))$ we can conclude $(\forall n \geq n_0) P(n)$

Thm (PMI w/ a different base case)

- Sps $P(n)$ is a variable prop'n and $n_0 \in \mathbb{Z}$ is fixed (possibly negative!)
- Let $S = \{n \in \mathbb{Z} \mid n \geq n_0\} = \{n_0, n_0+1, n_0+2, \ldots\}$

If we have
① $P(n_0)$ holds
② $(\forall n \in S)(P(n) \Rightarrow P(n+1))$ holds

then we have that
$(\forall n \in S) P(n)$ holds.

↳ can prove theorem using regular PMI (see book)
↳ template to use theorem nearly the same as w/ regular PMI:

① (BC) Verify $P(n_0)$
② (IH) Fix $n \in \mathbb{Z}$, $n \geq n_0$ arbitrary. Assume $P(n)$
③ (IS) Prove $P(n+1)$

(iii)

Ex: Q: for which $n \in \mathbb{N}$ do we have
$n! > 2^n$?

Lessee...

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

Seems like: if $n \geq 4$ then $n! > 2^n$
Let's prove this.

S here would be $\{4, 5, 6, \dots\}$

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

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

(BC) $P(4)$ holds since $4! = 24 > 16 = 2^4$
(IH) Fix $n \in \mathbb{N}$ with $n \geq 4$.
Assume $P(n)$, i.e. assume
$n! > 2^n$
(IS) Then we have

$$
\begin{aligned}
(n+1)! &= n!\,(n+1) \\
&> 2^n (n+1) && \text{by IH} \\
&> 2^n \cdot 2 && \text{since } n \geq 4 \\
&= 2^{n+1}
\end{aligned}
$$

So $P(n+1)$ holds
by induction we have proved:
$\forall n \in \mathbb{N}$, if $n \geq 4$, then $n! > 2^n$.

(iii)

(11)

Induction w/ 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, etc.
- can still argue inductively!

Theorem Let $P(n)$ be a var. prop'n
Let $n_0 \in \mathbb{Z}$ and $k \in \mathbb{N}$ be fixed, (n_0 = "starting pt", k = "jump")
Let

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

If we have that
① $P(n_0)$
② $(\forall n \in S)\ (P(n) \Rightarrow P(n+k))$ both hold

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

e.g.: if $S = \{2, 4, 6, \ldots\} = E$
and we can show
① $P(2)$
② if $P(n)$ then $P(n+2)$
then we have $P(n)$ for all $n \in E$.

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

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

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

(iv)

Prop'n ① if n is odd, then we have
$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = \sum_{k=1}^{n} k$$

② if n is even, we have:
$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = -\sum_{k=1}^{n} k$$

Pf ① here: $n_0 = 1$
jump $= 2$, so $S = \{1, 3, 5, \ldots\}$

(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) Fix $n \in \{1, 3, 5, \ldots\}$ and assume
$$\sum_{k=1}^{n} (-1)^{k-1} k^2 = \sum_{k=1}^{n} k$$

(IS) Now consider sum up to $n+2$:
$$\sum_{k=1}^{n+2} (-1)^{k-1} k^2 = \sum_{k=1}^{n} (-1)^{k-1} k^2 + (-1)^n (n+1)^2 + (-1)^{n+1} (n+2)^2$$
$$= \sum_{k=1}^{n} (-1)^{k-1} k^2 - (n+1)^2 + (n+2)^2$$

(v)

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

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

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

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

hence the identity holds for $n+2$.
By induction we have, for every $n \in \{1, 3, 5, \ldots\}$

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

We showed
① $P(1)$
② if n odd then $P(n) \Rightarrow P(n+2)$
$\Rightarrow$ hence $P(n)$ is true $\forall n \in \{1, 3, 5, \ldots\}$

where $P(n)$ is "$\sum_{1}^{n} (-1)^{k-1} k^2 = \sum_{1}^{n} k$"

② For <u>n even</u>:

(BC) if $n = 2$

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

(IH) Fix n even. Assume that:

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

(VI)

(IS) Then we have:

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

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

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

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

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

hence, by induction, the identity holds $\forall n \in \{2, 4, 6, \ldots\}$.

The Fibonacci Sequence

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,	..
f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8,	...

(i)

Fib sequence a playground for inductive proofs

<u>Prop'n</u> For every $n \in \mathbb{N}$ we have:

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

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

<u>Pf</u>: (BC) for $n=1$, we have

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

(IH) Fix $n \in \mathbb{N}$, and assume

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

(IS) Now consider:

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

$$\overset{IH}{=} f_{n+2} - 1 + f_{n+1}$$

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

Def'n of Fib seq.

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

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

hence identity holds for $n+1$

By induction identity holds $\forall n \in \mathbb{N}$ ✓

(ii)

16

i.e. if $n \in \{3, 6, 9, \ldots\}$

Prop'n If n is a multiple of 3, then f_n is even.

Pf (BC) if $n = 3$ then $f_3 = 4$, which is even ✓

(IH) Fix $n \in \{3, 6, 9, \ldots\}$ and suppose f_n is even.

(IS) consider f_{n+3}:

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

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

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

By IH f_n is even.
Since $2f_{n+1}$ is even, this gives that $f_n + 2f_{n+1}$ is even,
i.e. f_{n+3} is even.

Hence the statement holds for $n+3$.

By induction, the statement holds $\forall n \in \{3, 6, 9, \ldots\}$ ✓

(iii)

Strong Induction

- In certain proofs, may need to assume more than $P(n)$ to prove $P(n+1)$, e.g. may need $P(n)$ and $P(n-1)$ or even $P(n)$ and $P(n-1)$ and .. and $P(1)$

- these are still legitimate inductive hypotheses!
- this type of induction called strong induction.

Theorem (Principle of Strong mathematical induction) (PSMI)

Sps $P(n)$ is a variable prop'n

If ① $P(1)$ holds
and ② $(\forall n \in \mathbb{N})\left((\forall k \in [n]) P(k) \Rightarrow P(n+1)\right)$ holds

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

Template for a strong induction proof

① Prove $P(1)$
② Fix $n \in \mathbb{N}$. Assume $(\forall k \in [n]) P(k)$
i.e. assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$
③ Deduce $P(n+1)$

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

(iv)

- Despite name, PSMI seems weaker than PMI, since we have to assume more (i.e. all of $P(1) \wedge \cdots \wedge P(n)$ instead of just $P(n)$) to prove $P(n+1)$

- Let's prove PSMI from PMI.

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

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

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

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

(BC) - $Q(1)$ is the statement
$(\forall k \in [1]) P(k)$
i.e.
$(\forall k \in \{1\}) P(k)$
- But this is just 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
$(\forall k \in [n]) P(k)$ holds.

- but 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. that $Q(n+1)$ holds.

<u>we've shown</u>
① $Q(1)$ holds
② $(\forall n \in \mathbb{N})\, (Q(n) \Rightarrow Q(n+1))$ holds

<u>hence</u> by PMI
$(\forall n \in \mathbb{N})\, Q(n)$ holds

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

But then in particular $\forall n \in \mathbb{N}$ we have $P(n)$ holds

which is what we wanted to show ✓

Ex ① Let s_n be the sequence defined by

$$s_0 = 1$$

for $n \geq 1$ $\quad s_n = 1 + \sum_{k=0}^{n-1} s_n$

So e.g. $\quad s_1 = 1 + s_0 = 1 + 1 = 2$

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

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

$= 8$

$\vdots$

looks like (?) $\quad s_n = 2^n$

Let's prove:
will need a strong induction hypothesis

Prop'n $\forall n \in \mathbb{N} \cup \{0\}$ we have $s_n = 2^n$

Pf: (BC) $\quad s_0 = 1 = 2^0$ ✓

(strong IH) Fix $n \in \mathbb{N} \cup \{0\}$ and assume for every $k \in \{0, 1, \ldots, n\}$ we have

$$s_k = 2^k$$

(IS) Then:

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

IH

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

Geo series fmla

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

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

hence the identity holds for $n+1$.

By (strong) induction, $s_n = 2^n$ for all $n \in \mathbb{N} \cup \{0\}$.

② **Def'n**: for $n \in \mathbb{N}$ 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
- $2 \cdot 2 \cdot 3$ is a p.f. of 12.

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

Pf: Let $F(n)$ be proposition "n has a prime factorization"

We prove $(\forall n \in \{2, 3, 4, \ldots\}) F(n)$ by induction

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

(IH) Fix $n \geq 2$ and assume for every $K \in \{2, 3, \dots, n\}$ that K has a prime factorization (i.e. $F(K)$ holds).

(IS) 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 $a \geq 2$ and $b \leq n$.

Hence by the IH a and b have prime factorizations:

$$a = p_1 p_2 \cdots p_n$$
$$b = q_1 q_2 \cdots q_e$$
p_i q_j all prime

but then

$$n+1 = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_e$$

is a prime factorization of $n+1$. ✓

By (strong) induction, $F(n)$ holds for every $n \in \{2, 3, 4, \dots\}$, i.e. every $n \geq 2$ has a prime factorization

(The treachery of ...)
Multiple base cases

↳ sometimes need to check more than one base case in order to make IH/IS valid

↳ often happens when dealing w/ recursively defined sequences.

Ex: Define a sequence x_n by:

$$x_1 = 2$$
$$x_2 = 3$$
and
$$(\forall n \geq 3) \quad x_n = 3x_{n-1} - 2x_{n-2}$$

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

Pf: (BCs)

$n=1$: $x_1 = 2 = 2^{1-1} + 1$ ✓
$n=2$: $x_2 = 3 = 2^{2-1} + 1$ ✓

(IH) Fix $n \geq 2$ and assume $\forall k \in \{1, \ldots, n\}$ we have $x_k = 2^{k-1} + 1$

(observe: IH should always fix $n \geq$ last base case verified!)

<u>Then:</u>

$$x_{n+1} \overset{\text{def'n}}{=} 3x_n - 2x_{n-1} \quad *$$
$$\overset{IH}{=} 3(2^{n-1}+1) - 2(2^{n-2}+1)$$
$$= 3\cdot 2^{n-1} + 3 - 2\cdot^{n-1} - 2$$
$$= 2\cdot 2^{n-1} + 1$$
$$= 2^n + 1$$
$$= 2^{(n+1)-1} + 1 \checkmark$$

Hence by induction identity holds for all $n \in \mathbb{N}$:

$$x_n = 2^{n-1} + 1 \checkmark$$

<u>Notice</u>: - we really needed to check both $n = 1, 2$ as BCs.

- if we only checked $n=1$ and let our IH be:

"Fix $n \geq 1$, Assume $\forall k \leq n$ we have $x_k = 2^{k-1} + 1$"

then step $*$ would have been unjustified for $\underline{n=1}$.

$$x_{n+1} = 3x_n - 2x_{n-1}$$
$$x_{1+1} = 3x_1 - 2x_0$$

undefined!

- Can cook up <u>false</u> induction proofs that play on this issue.

"<u>Prop'n</u>" Let x_n be defined as above. Then $\forall n \in \mathbb{N}$ we have

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

"pf" — we can see identity is <u>False</u> even for $n=2$ since

$$x_2 = 3 \neq 6 = 2^{2+1} - 2$$

But if we ignore this BC we can "prove" this false identity:

(BC) if $n=1$ then

$$x_1 = 2 = 2^{1+1} - 2 \checkmark$$

(IH) Fix $n \geq 1$ and assume $\forall k \in \{1, \dots, n\}$ we have $x_k = 2^{k+1} - 2$

(IS) Then:

$$
\begin{aligned}
x_{n+1} &\overset{\text{def'n}}{=} 3x_n - 2x_{n-1} \\
&\overset{\text{IH}}{=} 3(2^{n+1} - 2) - 2(2^n - 2) \\
&= 3 \cdot 2^{n+1} - 6 - 2^{n+1} + 4 \\
&= 2 \cdot 2^{n+1} - 2 \\
&= 2^{(n+1)+1} - 2 \checkmark
\end{aligned}
$$

implicitly assuming $n \geq 2$! oops!

By induction, identity is "proved"

(i)

The Well-ordering Principle

"Theorem" (WOP) If $X \subseteq \mathbb{N}$ and $X \neq \emptyset$ then X has a least element (i.e. $\exists x \in X$ s.t. $\forall y \in X$ $x \leq y$)

Ex's – if $X = \mathbb{N}$ then its least el't is 1

– if $X = E = \{2, 4, 6, \ldots\}$ then 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 and is often taken as an axiom.

However: we can prove WOP from PSMI.

Proof: want to prove:
$(\forall X \in \mathcal{P}(\mathbb{N}))\,(X \neq \emptyset \Rightarrow X$ has a least el't$)$

– So fix $X \subseteq \mathbb{N}$.
– we argue by contrapositive:
assume X has no least el't
we prove $X = \emptyset$, by induction.

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

– We'll prove $(\forall n \in \mathbb{N})\, P(n)$ using PSMI

(ii)

(BC) $P(1)$ is true (i.e. $1 \notin X$) because if $1 \in X$ then 1 would be least el't of X (it is least el't of $\mathbb{N}$!)

(IH) Fix $n \geq 1$. Assume $\forall k \in [n]$ we have $k \notin X$.

(IS) Consider $n+1$. If $n+1 \in X$ then it must be that $n+1$ is <u>least</u> in X, since by hypothesis $1 \notin X \wedge 2 \notin X \wedge \ldots \wedge n \notin X$.

Hence $n+1 \notin X$, because X has no least el't

That is, $P(n+1)$ holds.

By PSMI $(\forall n \in \mathbb{N})\, P(n)$ holds
i.e. $(\forall n \in \mathbb{N})\, (n \notin X)$
i.e. $X = \emptyset$ ✓

Since X was arbitrary, the theorem is proved.

We just showed:

$$\text{PSMI} \Rightarrow \text{WOP}$$

And previously:

$$\text{PMI} \Rightarrow \text{PSMI}$$

(iii)

In fact, all three statements are <u>equivalent</u>

<u>Thm</u> The following are equivalent (TFAE):

1. PMI
2. PSMI
3. WOP

i.e. PMI $\Leftrightarrow$ PSMI $\Leftrightarrow$ WOP
i.e. from any <u>one</u> of these statements, we can prove the other two.

<u>Pf</u>: We've already shown

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

Hence if we can show

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

$$\begin{tikzcd} & \text{PMI} \arrow[dr, Rightarrow] & \\ \text{WOP} \arrow[ur, Rightarrow] & & \text{PSMI} \arrow[ll, Rightarrow] \end{tikzcd}$$

we will have proved equivalence of the three statements.

- Assume WOP is true.
- Let $P(n)$ be a variable prop'n such that
  1. $P(1)$ holds
  2. $(\forall n \in \mathbb{N})\,(P(n) \Rightarrow P(n+1))$ holds

(iv)

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 element x.

- we know $x \neq 1$, since $P(1)$ holds

- Hence $x = n+1$ for some $n \in \mathbb{N}$.

- by def'n of x, $P(n)$ <u>holds</u>.

- but then by ②, $P(n+1)$ holds as well, 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 of PMI, PSMI, WOP are intuitively obvious and in many contexts are taken as <u>axioms</u>

(v)

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

↳ idea of above proof was: get a contradiction by finding a "minimal counterexample"

↳ useful idea in its own right

Ex Prop'n: every natural number $n > 1$ can be written as a sum of the form

$$n = 2 \cdot a + 3 \cdot b \qquad \text{where } a, b \in \mathbb{N} \cup \{0\}$$

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

Pf. - Suppose not: that is sps there is a natural number ≥ 2 that cannot be so written.

using WOP
- Let N be the least such number
- Then by above $N > 2$.
- hence $N = n + 1$ for some $n \geq 2$.

- but since N was least counterexample we have

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

- at least one of a, b is strictly positive

(vi)

(i) if $a > 0$ then

$$
\begin{aligned}
N = n+1 &= \overbrace{2a + 3b}^{n} + 1 \\
&= 2(a-1) + 2 + 3b + 1 \\
&= 2(a-1) + 3b + 3 \\
&= 2(a-1) + 3(b+1)
\end{aligned}
$$

which, since $a-1, b+1 \in \mathbb{N} \cup \{0\}$, is a 'contradiction' since N has no such representation'

(ii) if $b > 0$ then

$$
\begin{aligned}
N = n+1 &= 2a + 3b + 1 \\
&= 2a + 3(b-1) + 3 + 1 \\
&= 2a + 4 + 3(b-1) \\
&= 2(a+2) + 3(b-1)
\end{aligned}
$$

which, since $a+2, b-1 \in \mathbb{N} \cup \{0\}$ is again a contradiction

hence there is no such n

so that $(\forall n \in \mathbb{N})(n \geq 2 \Rightarrow \exists a, b \in \mathbb{N} \cup \{0\} (n = 2a + 3b))$ ✓