e.g. $6 = 2 \cdot 3$ is a p.f. of 6

$2 = 2$ is a p.f. of 2

$100 = 2 \cdot 2 \cdot 5 \cdot 5$ is a p.f. of 100

Thm For every $n \in \mathbb{N}$, $n > 1$, (i.e. $\forall n \in \{2,3,4,\dots\}$)
n has a prime factorization.

Pf: Let $P(n)$ be the prop'n
"n has a prime factorization"

(BC) $P(2)$ holds since 2 has a p.f.

(IH) Fix $n \in \{2,3,4,\dots\}$ and assume for all $k \in \{2,3,4,\dots,n\}$, k has a p.f. (i.e. $P(k)$ holds).

(IS) Consider $n+1$. If $n+1$ is prime, then $n+1 = n+1$ is a p.f. of $n+1$.

If $n+1$ is not prime, then it can be factored:

$n+1 = a \cdot b$ where $a, b \in \{2,3,\dots,n\}$

neither are 1, hence neither are $n+1$

by the IH, a and b have p.f.'s:

$a = p_1 p_2 \cdots p_k$

$b = q_1 q_2 \cdots q_l$

but then $n+1 = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$ is a p.f.

hence $P(n+1)$ holds

By (strong) induction $\forall n \in \{2,3,4\ldots\}$ $P(n)$ holds

i.e. every $n \geq 2$ has a p.f.

(The treachery of...) Multiple Base Cases.

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

— esp for recursively defined sequences.

Ex: define a sequence x_n by:

$$x_1 = 2$$
$$x_2 = 3$$
$$x_n = 3x_{n-1} - 2x_{n-2} \quad \text{if } n \geq 3.$$

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

Pf. (BCs) if $n=1$: $x_1 = 2 = 2^{1-1} + 1$

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

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

(notice: IH fixes $n \geq$ last verified base case — that's our "spring off" point)

(IS) Then: $x_{n+1} \overset{\text{defn of sequence}}{=} 3x_n - 2x_{n-1}$ (*)

$\overset{IH}{=} 3(2^{n-1}+1) - 2(2^{n-2}+1)$

$= 3\cdot 2^{n-1} + 3 - 2^{n-1} - 2$

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

$= 2^n + 1$

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

by induction, the identity $x_n = 2^{n-1}+1$ holds for all $n \in \mathbb{N}$.

---

note: - we really needed to check both $n=1$ and 2 as BC's.

- if we only checked $n=1$ and let our IH be: " fix $n \geq 1$ and assume $\forall k \in \{1,2,\ldots,n\}$ we have $x_k = 2^{k-1}+1$."

then step (*) would have been unjustified for $n=1$. In this case, (*) would be:

$x_{1+1} = 3x_1 - 2x_0$ ← undefined!!

↳ can cook up false induction proofs that play on this issue.

e.g. "**Prop'n**" Let the sequence x_n be defined as above. Then $\forall n \in \mathbb{N}$ we have:

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

"**Pf**" (BC) if $n=1$, then

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

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

(IS) then: $x_{n+1} = 3x_n - 2x_{n-1}$ $(*)$

$$= 3(2^{n+1} - 2) - 2(2^n - 2)$$

$$= 3 \cdot 2^{n+1} - 6 - 2^{n+1} + 4$$

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

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

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

By induction, the identity is "proved" $\forall n \in \mathbb{N}$.

— of course, we can verify the identity is wrong even for $n=2$:

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

— the issue is exactly that $(*)$ is not justified when $n=1$, but in our

IH we're allowing the possibility of $n=1$, since we've only verified $n=1$ in our BC.

PMI, PSMI, and WOP

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

- this "theorem" is intuitively obvious and is often taken as an axiom for $\mathbb{N}$.
- e.g. if $X = \mathbb{N}$, then X's least el't is 1

  if $X = \{2, 4, 6, \ldots\}$ " " " 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 " " " is 36.
- though it's obvious, one can actually prove WOP by strong induction

Pf: We want to prove:

$$(\forall X \in P(\mathbb{N}))(X \neq \emptyset \Rightarrow X \text{ has a least el't})$$

- So fix $X \in P(\mathbb{N})$
- we argue by contrapositive:
  - assume X has no least el't
  - we prove $X = \emptyset$ by strong induction
- specifically, we prove:

$$\underbrace{(\forall n \in \mathbb{N})\ (n \notin X)}_{\text{call this } P(n)} \quad \text{by induction}$$

- (BC) $P(1)$ is true (i.e. $1 \notin X$) because if we had $1 \in X$ it would be least el't of X (1 is least el't of $\mathbb{N}$!)
- (IH) Fix $n \in \mathbb{N}$. Assume $\forall k \in \{1, 2, \ldots, n\}$ we have $k \notin X$ (i.e. $P(k)$ holds)
- (IS) Consider $n+1$. If $n+1 \in X$ it would be least int, since by IH

$$1 \notin X \wedge 2 \notin X \wedge \ldots \wedge n \notin X.$$

by strong induction $(\forall n \in \mathbb{N})\ P(n)$ holds
i.e. $(\forall n \in \mathbb{N})\ (n \notin X)$ holds

hence $X = \emptyset$.

We've proved WOP ✓

We just showed

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

In fact, PSMI and WOP are equivalent (i.e. can also prove WOP $\Rightarrow$ PSMI)

and more: both are equivalent to PMI.

<u>Thm</u> The following are equivalent:

1. PMI
2. PSMI
3. WOP

i.e. $\text{PMI} \Leftrightarrow \text{PSMI} \Leftrightarrow \text{WOP}$

i.e. from any one of these statements, can prove the other two.

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

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

Hence if we can show

<u>Claim 1</u>: $\text{PMI} \Rightarrow \text{PSMI}$

<u>Claim 2</u>: $\text{WOP} \Rightarrow \text{PMI}$

$$\begin{tikzcd} & \text{PMI} \arrow[dr, Rightarrow, "\text{Claim 1}"] & \\ \text{WOP} \arrow[ur, Rightarrow, "\text{Claim 2}"] & & \text{PSMI} \arrow[ll, Rightarrow, "\text{know}"] \end{tikzcd}$$

we will have established the equivalence of all three statements

Before proving PMI $\Rightarrow$ PSMI, let's illustrate idea of proof w/ an example.

Recall our first strong induction pf:

Define $S_0 = 1$

$$S_n = 1 + \sum_{k=0}^{n-1} S_k \quad \text{for } n \geq 1.$$

<u>Claim</u> $\forall n \in \mathbb{N} \cup \{0\}$ we have $\underbrace{S_n = 2^n}_{\text{call this } P(n)}$

<u>Pf</u>: We proved this w/ PSMI.

- To prove using just PMI we can "hack" a strong inductive hypothesis into statement we induct on.

- Let $Q(n)$ be "$(\forall k \in \{0, 1, \ldots, n\})\ S_k = 2^k$"

- if we can prove $Q(n)$ holds for all n, then in particular we've proved $S_n = 2^n$ holds for all n, i.e. $P(n)$ holds for all n.

~~BS~~ (BC) $Q(0)$ holds since this is just "$\forall k \in \{0\} (S_k = 2^k)$" which is true since $S_0 = 1 = 2^0$.

(IH) Fix $n \in \mathbb{N} \cup \{0\}$ and assume $Q(n)$
i.e. assume $(\forall k \in \{0, 1, \ldots, n\})(s_k = 2^k)$

(IS) To prove $Q(n+1)$, i.e.
$(\forall k \in \{0, 1, \ldots, n+1\})(s_k = 2^k)$

It is sufficient to prove $s_{n+1} = 2^{n+1}$
since our IH already gives $\forall k \in \{0, 1, \ldots, n\}\ s_k = 2^k$

observe:

$$s_{n+1} = 1 + \sum_{k=0}^{n} s_k \quad \text{def'n of sequence}$$
$$= 1 + \sum_{k=0}^{n} 2^k \quad \text{IH}$$
$$= \frac{2^{n+1} - 1}{2 - 1} + 1 \quad \text{(geo series fmla)}$$
$$= 2^{n+1}$$

So by regular induction we've proved ~~(∀n∈{0,1,…})~~ $(\forall n \in \mathbb{N} \cup \{0\})\ Q(n)$
which as noted above gives
$(\forall n \in \mathbb{N} \cup \{0\})\ P(n)$
i.e. $(\forall n \in \mathbb{N} \cup \{0\})\ s_n = 2^n$