e.g. \( G = 2 \cdot 3 \) is a p.f. of \( G \)
\( 2 = 2 \) is a p.f. of \( 2 \)
\( 100 = 2 \cdot 2 \cdot 5 \cdot 5 \) is a p.f. of \( 100 \)

Thus, for every \( n \in \mathbb{N} \), \( n > 1 \), (i.e. the \( \{2,3,4,\ldots\} \)
\( n \) has a prime factorization.

**PF.** Let \( P(n) \) be the proposi
**n has a prime factorization**

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

(IIH) Fix \( n \in \{2,3,4,\ldots\} \) and assume for all
\( k \in \{2,3,4,\ldots,n\}, \) \( k \) 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 \( a, b \in \{2,3,\ldots,n\} \)

neither one,
hence neither or \( n+1 \).

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 \( n = 2, 3, 4 \ldots \), \( P(n) \) holds i.e. every \( n \geq 2 \) has a p.f.

(The treachery of ...) Multiple Base Cases

So 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:

\[
\begin{align*}
x_1 &= 2 \\
x_2 &= 3 \\
x_n &= 3x_{n-1} - 2x_{n-2} & \text{if } n \geq 3.
\end{align*}
\]

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

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 is our "spring off" point)
Then \( x_{n+1} = 3x_n - 2x_{n-1} \) \((*)\)

\[
\begin{align*}
&= 3(2^{n-1} + 1) - 2(2^{n-2} + 1) \\
&= 3 \cdot 2^{n-1} + 3 - 2^{n-1} - 2 \\
&= 2 \cdot 2^{n-1} + 1 \\
&= 2^n + 1 \\
&= 2^{n+1} - 1 + 1
\end{align*}
\]

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 \( x_k \in (1,3...14) \) we have \( x_k = 2^{k-1} + 1 \)."

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

\[
x_{1+1} = 3x_1 - 2x_0 \quad \text{undefined}!!
\]

We can cook up false induction proofs that play on this issue.
e.g. "Prop'h" let the sequence $x_n$ be defined as above. Then we have:

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

"PF" (BC) if $n=1$, then

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

(TH) Fix $n \geq 1$ and assume $x_k \in \{2^{1/2}, \ldots\}$

then $x_k = 2^{k+1} - 2$

(TS) Then:

$$x_{n+1} = 3x_n - 2x_{n-1} \quad (*)$$

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

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

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

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

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

By induction, the identity is "proved".

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 cur
IT we're allowing the possibility of n=1, since we've only verified n=1 in our PC.

PMI, PSMI, and WOP

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

This "theorem" is intuitively obvious and is often taken as an axiom for N.

E.g. if x = N, then x's least element

If x = \{2, 4, 6, \ldots\} " " " U 2
If x = \{n \in N | (\exists k \in N)(k > s \land 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 PCN) (x \neq \emptyset \rightarrow x \text{ has a least element})
So fix \( x \in P(N) \)
we argue by contrapositive:
(1) Assume \( x \) has no least elt.
(2) we prove \( x = \emptyset \) by strong induction.

- specifically, we prove:
  \((\forall n \in N) (x \not\in X)\) by induction.
  \(\Rightarrow\)
  call this \( P(n) \)

- \( P(1) \) is true (i.e. \( 1 \not\in X \)) because
  if we had \( 1 \in X \) it would be least elt of \( X \) (it is least elt of \( N \) !)

- \( P(n) \) Fix \( n \in N \). Assume \( \forall k \in \{1, 2, \ldots, n\} \)
  \( k \not\in X \) (i.e. \( P(k) \) holds)

- \( P(n+1) \) Consider \( n+1 \). If \( n+1 \in X \) it would be least elt, since by \( P(n) \),
  \( 1 \not\in X \) \( \& \) \( 2 \not\in X \) \( \& \) \( n \not\in X \).
  by strong induction \( (\forall n \in N) P(n) \) holds
  \( \Rightarrow \)
  \( \forall n \in N ) (x \not\in X) \) holds
  hence \( x = \emptyset \).
  We've proved wep \( \checkmark \)
We just showed
PSMI \implies \text{wop}

In fact, PSMI and wop are equivalent (i.e., can also prove \text{wop} \implies \text{PSMI})

and more: both are equivalent to PMI.

Thus, the following are equivalent:

\begin{enumerate}
  \item PMI
  \item PSMI
  \item wop
\end{enumerate}

i.e., \text{PMI} \iff \text{PSMI} \iff \text{wop}

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

PF: we've already shown:

PSMI \implies \text{wop}

Hence if we can show

\begin{enumerate}
  \item PMI \implies \text{PSMI}
  \item \text{wop} \implies \text{PMI}
\end{enumerate}

we will have established the equivalence of all three statements.
Before proving \( \text{PMI} \Rightarrow \text{PSMI} \), let's illustrate idea of proof w/ an example.

Recall our first strong induction PF:

Define \( S_0 = 1 \)

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

Claim \( \forall n \in \mathbb{N} \) we have \( S_n = 2^n \) (call this \( P(n) \))

PF: We proved this w/ \( \text{PSMI} \).

To prove using just \( \text{PMI} \) 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 \( n \).

\[ (BC) \] \( Q(0) \) holds since this is just "\( \forall k \in \{0\} (S_k = 2^k) \)" which is true since \( S_0 = 1 = 2^0 \).
**(I.H.)** Fix \( n \in \mathbb{N} \) and assume \( P(n) \)

i.e. assume \(( \forall k \in \{0, 1, \ldots, n\}) (S_k = 2^k)\)

**(I.S.)** To prove \( P(n+1) \), 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 I.H. already gives \(( \forall k \in \{0, 1, \ldots, n\}) S_k = 2^k\)

Observe:

\[
S_{n+1} = 1 + \sum_{k=0}^{n} 2^k \quad \text{defn of sequence} \\
= 1 + \sum_{k=0}^{n} 2^k \quad \text{I.H.} \\
= 1 + \left[ \frac{2^{n+1} - 1}{2-1} \right] + 1 \quad \text{(geo series formula)} \\
= 2^{n+1} \\
\]

So by **regular induction** we've proved \(( \forall n \in \mathbb{N} ) P(n) \)

which as noted above gives

\(( \forall n \in \mathbb{N} ) S_n = 2^n \quad \checkmark \)