<u>Def'n</u> A <u>prime</u> <u>factorization</u> of a given $n \in \mathbb{N}$ $n>1$ is a way of writing n as a product of primes.

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

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

<u>Pf</u>: 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 that $\forall k \in \{2,3,\dots,n\}$ 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 <u>not</u> 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

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

$$a = p_1 p_2 \cdots p_e$$
$$b = q_1 q_2 \cdots q_m$$
all primes

but then $n+1 = p_1 p_2 \cdots p_e q_1 q_2 \cdots q_m$ is a p.f.
hence $P(n+1)$ holds.

By (strong) induction, $\forall n \in \{2, 3, \ldots\}$ $P(n)$ holds, i.e. every $n \geq 2$ has a p.f.

Multiple Base Cases

- sometimes need to check more than one base case in order to make a valid IH/IS.
- esp often for recursively defined sequences

Ex: define a sequence x_n by:

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

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

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

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

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

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

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

$$\begin{aligned} &\overset{IH}{=} 3(2^{n-1}+1) - 2(2^{n-2}+1) \\ &= 3\cdot 2^{n-1} + 3 - 2^{n-1} - 2 \\ &= 2\cdot 2^{n-1} + 1 \\ &= 2^n + 1 \\ &= 2^{(n+1)-1} + 1 \end{aligned}$$ ✓

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

$\boxed{\text{note}}$ – we really needed to check both $n=1$ and $n=2$ as BCs.

- If we only checked $n=1$ and let our IH be: "Fix $n \geq 1$ and assume $\forall k \in \{1, \dots, n\}$ $\quad x_k = 2^{k-1}+1$"

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

$$x_{1+1} = 3x_1 - 2x_0 \leftarrow \text{undefined!!}$$

- 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 $x_1 = 2 = 2^{1+1} - 2$ ✓

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

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

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

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 allow the possibility $n=1$ since we've only verified $n=1$ in our BC.

PMI, PSMI, WOP

"Theorem" (Well-ordering principle)
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 $\mathbb{N}$.

- eg. if $X = \mathbb{N}$ then least el't is 1
  if $X = \{2, 4, 6, \ldots\}$ then 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 least el't is 36.
- though it's obvious, one can actually prove WOP by strong induction.

PF: We want to prove:
$(\forall X \in P(\mathbb{N}))(X \neq \emptyset \Rightarrow X$ 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:
  $(\forall n \in \mathbb{N})(n \notin X)$

  call this $P(n)$

(BC) $P(1)$ is true (i.e. $1 \notin X$) because

If we had $1 \in X$ it would be the least element of X (1 is least in $\mathbb{N}$!)

(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 in X since by the IH

$$1 \notin X \wedge 2 \notin X \wedge 3 \notin X \wedge \ldots \wedge n \notin X$$

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

by strong induction, $(\forall n \in \mathbb{N})(n \notin X)$ holds

i.e. $X = \emptyset$.

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 <u>more</u>: both are equivalent to PMI.