CSE 16 8-3-21

Principle of Mathematical Induction

follows from : W.O.P. of $\mathbb{Z}^+$

Any non-empty subset of $\mathbb{Z}^+$ contains a least element.

Theorem (PMI):

Given any Prop. fcn. $P(n)$ on the Domain of positive integers $\mathbb{Z}^+$, the statement

$$\left[P(1) \wedge \forall n\,(P(n) \Rightarrow P(n+1))\right] \Rightarrow \forall n\, P(n)$$

is true.

Proof.

Assume both $P(1)$ and $\forall n\,(P(n) \Rightarrow P(n+1))$ are true. We must show

$$\forall n\ P(n)$$

is also true. Let $S \subseteq \mathbb{Z}^+$ be defined as

$$S = \{n \in \mathbb{Z}^+ \mid \sim P(n)\}$$

i.e. S consists of all $n \in \mathbb{Z}^+$ such that $P(n)$ is false. It's sufficient to show that $S = \emptyset$, for then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Assume, to get a $\times$, that $S \neq \emptyset$. Then by the W.O.P., S contains a least element, call it m. Thus $\boxed{m \in S}$ but $m-1 \notin S$.

Now since $P(1)$ is true, $1 \notin S$, so $m \neq 1$, hence $m \geq 2$, so that $m-1 \geq 1$. Thus $m-1 \in \mathbb{Z}^+$.

Recall $m-1 \notin S$, hence

$$P(m-1)$$

is <u>true</u>.

Since $\forall n (P(n) \Rightarrow P(n+1))$ is true, we have for $n = m-1$:

$$P(m-1) \Rightarrow P(m)$$

is also <u>true</u>. (Recall: $(A \wedge (A \Rightarrow B)) \Rightarrow B$ is a tautology.) we conclude that

$$P(m)$$

must be true. Therefore $\boxed{m \notin S}$.

This ※ shows our assumption was false, hence $S = \phi$, as required. $\blacksquare$

<u>Fact</u>: also have PMI $\Rightarrow$ WOP.

<u>Exercise</u> (hint read induction handout from cse 102.)

Variations on PMI.

I. show $P(1)$

IIa. $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

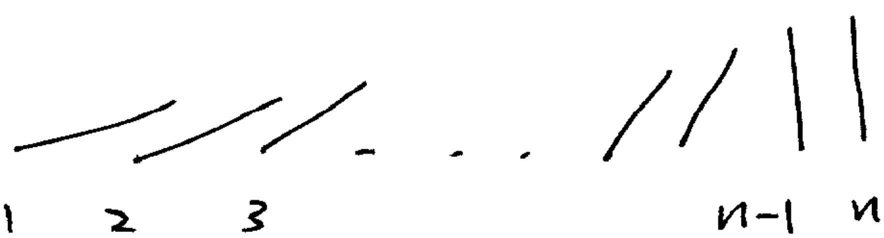
or

IIb. $\forall n > 1 : \underbrace{P(n-1)}_{} \Rightarrow P(n)$ ← induction hypothesis

<u>Rmk.</u>

IIb. is a shift in Ind. Parameter n,

i.e. replace n by $n-1$ in IIa.



<u>Ex.</u> $\forall n \geq 1 : \boxed{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}}$ ← $P(n)$

<u>Proof:</u> I. $P(1)$ is same

II b. $\forall n > 1 : P(n-1) \Rightarrow P(n)$.

Let $n > 1$ be arbitrary. Assume

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

we must show

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

so

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

$$= \left(\frac{n(n-1)}{2}\right) + n \quad \Big\{ \text{by the ind. hyp.}$$

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

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

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

as required. $\blacksquare$

<u>Exercise</u>:
go back and re-do all previous examples using form II b.

Another variation: <u>Strong induction</u> or the <u>2^{nd} P.M.I.</u>

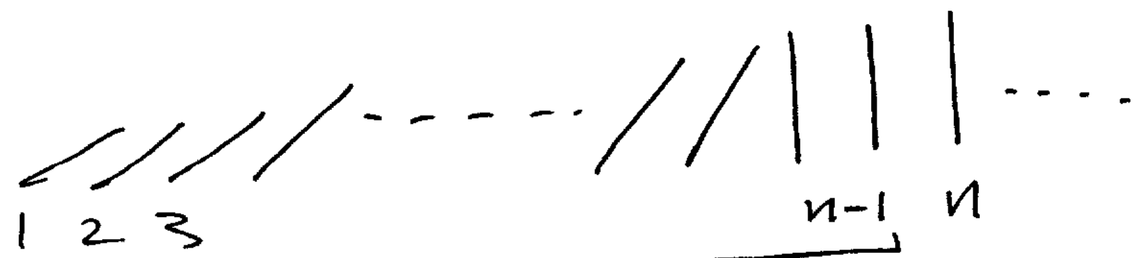
I. show $P(1)$ is true

II c. $\forall n \geq 1: \underbrace{(P(1) \wedge P(2) \wedge \ldots \wedge P(n))}_{\text{induction hypothesis}} \Rightarrow \underbrace{P(n+1)}_{\text{induction conclusion}}$.

<u>or</u>

$$\text{II}d.\ \forall n>1:\ \underbrace{\left(P(1)\wedge P(2)\wedge\dots\wedge P(n-1)\right)}_{\text{ind. hyp.}} \Rightarrow \underbrace{P(n)}_{\substack{\text{ind}\\ \text{concl.}}}$$

Domino analogy (II d.)



assume dominoes 1, 2, ..., n−1 fall

show domino n falls.

<u>Rmk.</u>

most parametrizations of strong induction follow form II d. we do no examples of II c therefore.

Theorem

Every positive integer can be expressed as the product of (zero or more) primes.

Rmk. This is one half of F.T.A.

Proof:

we show

$P(n)$

$$\forall n \geq 1 : \boxed{n \text{ is a product of primes}}$$

I. $P(1)$ is true since 1 is the empty product.

II d. $\forall n>1: (P(1) \wedge \ldots \wedge P(n-1)) \Rightarrow P(n)$

Let $n>1$ be arbitrary. Assume for all k in the range $1 \le k < n$ that k is a product of primes. We must show that n is also a product of primes.

We have 2 cases.

Case 1: n is prime.
In this case n is a product of one prime, itself.

Case 2: n is composite.
In this case $n = ab$ for some $a, b \in \mathbb{Z}$ with $1 < a < n$ and $1 < b < n$.

By the ind. hyp. we have both $P(a)$ and $P(b)$ are true, i.e. both a and b can be written as a product of primes:

$$a = p_1 p_2 \cdots p_k$$

and

$$b = q_1 q_2 \cdots q_l$$

where $k > 1$, $l > 1$ and p_i, q_j are primes for $1 \le i \le k$, $1 \le j \le l$.

Therefore

$$n = ab = (p_1 \cdots p_k)(q_1 \cdots q_l)$$

is also a product of primes.

Result follows for all $n \geq 1$ by 2nd P.M.I. $\blacksquare$

Theorem

The prime factorization of every positive integer n is unique, i.e. if

$$p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_l$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_l$ are prime numbers, then $k = l$ and

$$p_i = q_i \quad (\text{for } 1 \leq i \leq k)$$

Rmk. This is the 2nd half of the F.T.A.

Lemma (Chap. 7 # 30)

Let $a, b, p \in \mathbb{Z}$ and suppose p is prime. If $p \mid a \cdot b$ then either $p \mid a$ or $p \mid b$.

Corollary:

Let $a_1, a_2 \cdots a_k \in \mathbb{Z}$ and suppose $p \mid (a_1 \cdot a_2 \cdots a_k)$, where p is prime. Then $p \mid a_i$ for at least one i in range $1 \leq i \leq k$.

Exercise: Prove this. (ind. on k.)

Proof of Thm (uniqueness in F.T.A.)

Let $P(n)$ be the stmt: $\boxed{\text{the prime factorization of } n \text{ is unique.}}$ We show $\forall n \geq 1: P(n)$.

I. $P(1)$ is true since the empty product is unique.

II d. $\forall n > 1 : (P(1) \wedge \dots \wedge P(n-1)) \Rightarrow P(n)$.

Let $n > 1$ be arbitrary. Assume the prime factorization of any k in the range $1 \leq k < n$ is unique. We must show the prime factorization of n is unique.

Suppose

(*) $\quad p_1 p_2 \cdots p_k = n = q_1 q_2 \cdots q_\ell$

are factorizations of n into primes with $p_1 \leq p_2 \leq \cdots \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_\ell$.

Then $n = (p_1 p_2 \cdots p_{k-1}) \cdot p_k$, so $p_k \mid n$, hence $p_k \mid q_1 q_2 \cdots q_\ell$.

By the corollary, $p_k \mid q_i$ for some $1 \leq i \leq \ell$. By re-indexing if necessary, we have $p_k \mid q_\ell$.

But q_ℓ has only $\{1, q_\ell\}$ as divisors. Since $p_k \neq 1$, we have $p_k = q_\ell$.

cancel p_k from both sides of (*), and define m by

$$p_1 p_2 \cdots p_{k-1} = m = q_1 q_2 \cdots q_{l-1}.$$

Since $p_k > 1$, we have $m < n$. By the induction hypothesis the prime factorization of m is unique, so $k-1 = l-1$ and

$$p_i = q_i \text{ for } 1 \le i \le k-1.$$

Therefore $k = l$ and $p_i = q_i$ for $1 \le i \le k$. $\therefore$ the prime factorization of n is unique.

Result follows for all $n \geq 1$ by 2^{nd} P.M.I. $\blacksquare$