<u>Proof of</u> : $\exists$ x, y irrational s.t. x^y is rational

<u>Proof</u>

let $x = \sqrt{2}$, $y = \log_2(9)$ both proven to be irrational. Then

$$x^y = \sqrt{2}^{\log_2(9)} = \sqrt{2}^{\log_2(3^2)}$$

$$= \sqrt{2}^{2 \cdot \log_2(3)}$$

$$= (\sqrt{2}^2)^{\log_2(3)}$$

$$= 2^{\log_2(3)}$$

$$= 3 \in \mathbb{Q}.$$

$\blacksquare$

Exercise

- Try $x = \sqrt{3}$, $y = \log_3(25)$

- Try $x = \sqrt[3]{2}$, $y = \log_2(27)$

- make up more examples

Theorem

let $a, b \in \mathbb{Z}$. Then there exists $n, m \in \mathbb{Z}$ such that

$$\gcd(a,b) = an + bm$$

Proof.

Let

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

note S contains some positive integers. However $S \cap \mathbb{N}$ contains only positive ints.

Let d be the least positive integer in S. (which exists by the W.O.P of $\mathbb{N}$.)

we will show that $d = \gcd(a,b)$.

By the defn of S, there exist $n, m \in \mathbb{Z}$ s.t.

$$d = an + bm$$

we must show that both

(i) $d \mid a$ and $d \mid b$

and (ii) if $e \mid a$ and $e \mid b$, then $e \leq d$.

<u>Proof of (i)</u>

To prove $d \mid a$, use div. alg.

$$a = qd + r \quad (0 \leq r < d)$$

$$\therefore \quad r = a - qd$$
$$= a - q(an + bm)$$
$$= a(1 - qn) + b(-qm)$$

so r has the form $ax + by$, so $r \in S$. But $0 \leq r < d$. Since d is the least positive element in S, we have $r = 0$.

$$\therefore \quad a = qd$$

$$\therefore \quad d \mid a.$$

$d \mid b$ is proved similarly.

<u>Proof of (ii)</u>

Suppose $e \mid a$ and $e \mid b$. By a prev. lemma, e must divide any integer comb. of a and b, so

$$e \mid (an + bm) = d.$$

$$\therefore e \leq d.$$

Proving (ii). Thus

$$d = (an + bm) = \gcd(a, b).$$

$\blacksquare$

Chapter 10 :

Mathematical Induction

Ex observe

$$1 = 1^2$$

$$1+3 = 2^2$$

$$1+3+5 = 3^2$$

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

$$\vdots$$

we might guess

$$1+3+5+\cdots+(2n-1) = n^2$$

for any $n \in \mathbb{N}$. other notation

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

<u>Lemma</u>: $\forall n \in \mathbb{N} : \sum_{k=1}^{n} (2k-1) = n^2$

Let $P(n)$ be a prop. fcn. with universe of discourse $\mathbb{N}$.

Goal: Prove $\boxed{\forall n \in \mathbb{N} : P(n)}$ (*)

A proof by Math. Ind. has 2 steps.

I. Base

Prove that $P(1)$ is true.

II. Induction.

Prove that $\forall n \geq 1 : P(n) \Rightarrow P(n+1)$

i.e. let $n \geq 1$ be an arbitrary pos. int., assume $P(n)$ is true, show as a conseq. that $P(n+1)$ is true.

once parts I & II are complete, we conclude: $\forall n \in \mathbb{N} : P(n)$.

<u>note</u>: $P(n)$ is called the <u>induction hypothesis</u>.

why is this valid?

<u>Inference rule</u>: (modus ponens)

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore\ q \end{array}$$

<u>Tautology</u>: $[p \wedge (p \to q)] \to q$

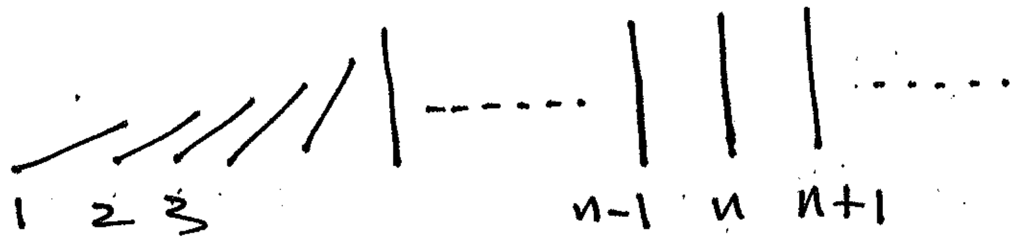
Consider the following "proof".

$P(1)$	by I.
$P(1) \Rightarrow P(2)$	by II with $n=1$
$\therefore P(2)$	by modus Ponens
$P(2) \Rightarrow P(3)$	by II, $n=2$
$\therefore P(3)$	by modus Ponens

$\vdots$

But a proof is supposed to be a finite seq. of statements.

The Domino Analogy



$P(n) =$ "the n^{th} domino falls".

we wish to prove

$$\forall n \geq 1 : P(n)$$

which says "all dominos fall".

I. $P(1) =$ "1^{st} domino falls".

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

"if any domino falls, so does the next"

Conclude from I & II : all dominos fall.

The validity of induction is based on

<u>Thm</u> (Principle of Matheniatical Induction (PMI))

For any prop. fcn $P(n)$ on $\mathbb{N}$, the following is true:

$$[P(1) \wedge \forall n\,(P(n) \rightarrow P(n+1))] \rightarrow \forall n\, P(n).$$

<u>Ex</u> $\forall n \geq 1 : \boxed{\sum_{k=1}^{n} (2k-1) = n^2} \leftarrow P(n)$

<u>Proof.</u>

I. $P(1)$ says $\sum_{k=1}^{1} (2k-1) = 1^2$, i.e.

$2 \cdot 1 - 1 = 1^2$, i.e. $1 = 1$ which is true.

II. $\forall n \geq 1 : P(n) \longrightarrow P(n+1)$.

Let $n \geq 1$ be chosen arbitrarily.
Assume (for this n) that

$$\sum_{k=1}^{n} (2k-1) = n^2 \qquad \text{(ind. hypothesis)}$$

we must show that

$$\sum_{k=1}^{n+1} (2k-1) = (n+1)^2 \qquad \text{(ind. conclusion)}$$

so

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

$$= n^2 + 2(n+1) - 1 \qquad \left\{ \begin{array}{l} \text{by the} \\ \text{ind. hyp.} \end{array} \right.$$

$$= n^2 + 2n + 1$$

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

By the P.M.I., we conclude

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

■

Ex. let $x \in \mathbb{R}, x \neq 1$. show

$$\forall n \geq 1: \boxed{\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}}$$ $P(n)$

Proof

I. $P(1)$ is $\displaystyle\sum_{k=0}^{0} x^k = \frac{x^1 - 1}{x - 1}$,

i.e. $x^0 = \dfrac{x-1}{x-1}$, i.e. $1 = 1$

which is true.

II. $\forall n \geq 1 : P(n) \rightarrow P(n+1)$

let $n \geq 1$ be arbitrary. Assume

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x-1} \qquad \text{(ind. hyp.)}$$

we must show

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1} - 1}{x-1} \qquad \text{(ind. conc.)}$$

observe

$$\sum_{k=0}^{n} x^k = \left(\sum_{k=0}^{n-1} x^k\right) + x^n$$

$$= \left(\frac{x^n - 1}{x-1}\right) + x^n \quad \left\{\begin{array}{l}\text{by the} \\ \text{ind. hyp.}\end{array}\right.$$

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

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

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

The result follows by P.M.I. ∎

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

I. $P(1)$ says $\sum_{k=1}^{1} k = \frac{1(1+1)}{2}$,

i.e. $1 = \frac{1 \cdot 2}{2}$, i.e. $1 = 1$.

II. $\forall n \geq 1: P(n) \rightarrow P(n+1)$.

Let $n \geq 1$. Assume

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

We must show

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

So

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

$$= \frac{n(n+1)}{2} + (n+1) \quad \text{\{ by ind. hyp.}$$

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

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

Result follows by P.M.I. ∎

Exercises

- $\forall n \geq 1: \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ (hw)

- $\forall n \geq 1: \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$

Sometimes $P(n)$ is false for some finite # of initial terms, say

$P(1), P(2), \ldots, P(n_0 - 1)$

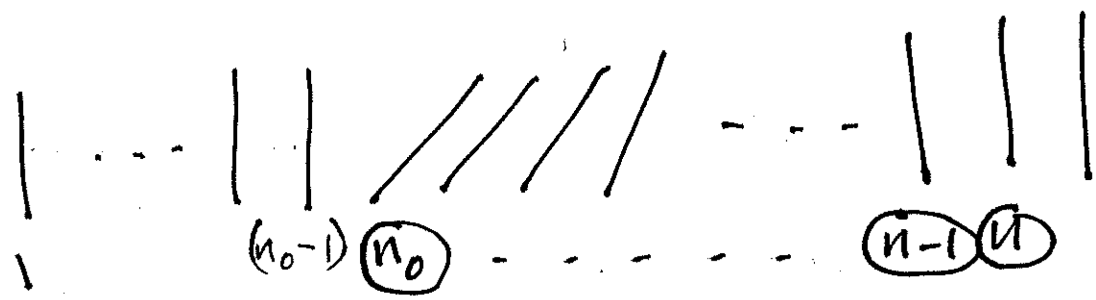
are false.

To Prove

$$\forall n \geq n_0 : P(n)$$

I. $P(n_0)$ is true

II. $\forall n \geq n_0 : P(n) \rightarrow P(n+1)$



EX. $\forall n \geq 4 : \boxed{5n+8 < n^2+4n+1}$ ← $P(n)$

check: $P(1)$, $P(2)$, $P(3)$ are false.

I. $P(4)$: $5 \cdot 4 + 8 < 4^2 + 4 \cdot 4 + 1$

i.e. $28 < 33$ ✓

II. $\forall n \geq 4 : P(n) \rightarrow P(n+1)$

let $n \geq 4$. Assume

$$5n+8 < n^2+4n+1.$$

must show

$$5(n+1)+8 < (n+1)^2+4(n+1)+1.$$

so

$$5(n+1)+8 = (5n+8)+5$$

$$< (n^2+4n+1)+5 \quad \left\{ \begin{array}{l} \text{by ind.} \\ \text{hyp.} \end{array} \right.$$

$$= n^2+4n+6$$

$$< (n^2+4n+6)+2n \quad \left\{ \begin{array}{l} \text{since} \\ n \geq 4 \rightarrow 2n > 0. \end{array} \right.$$

$\vdots$

later