Proofs

- determine if Math statement true or not
- once proven true, will be true forever.

eg: $a^2 + b^2 = c^2$: Pythagoras theorem.

$\sqrt{2}$ is irrational proof.

Proof terminologies

1. Conjecture : statement being proposed to be true (unproven)
2. Theorem : statement proven to be true.
3. Axioms (Postulates) : statements assumed to be true : eg: $6 = 6$
4. Lemma : subsidiary / intermediate theorem (to assist in main theorem)
5. Corollary : theorem established directly from another proven theorem.

Different kinds of Proof

1. Direct Proofs

- using established facts, axioms, existing limits & theorems to prove.

eg 1. if $n \in 2k+1$, $n^2 \in 2k+1$

proof: $(2k+1)^2 = 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$, $2k^2 + 2k$ is integer.

$\equiv 2k + 1$ (proven)

eg 2. if $n \in 2k$, $(-1)^n = 1$

proof: $(-1)^{2k} = ((-1)^2)^k$

$= 1^k \equiv 1$ (proven)

eg 3. if $a \mid b$ & $a \mid c$ then $a \mid (b+c)$

$b = a \cdot r$ $\quad$ $c = a \cdot t$: divisibility rule.

$b + c = (a \cdot r) + (a \cdot t)$

$= a(r + t)$, $r + t$ = Integer.

$\therefore$ $b + c$ must be divisible by a (proven)

2. Proof by Contrapositive

$p \to q$, contrapositive $= \sim q \to \sim p$.

$p \to q \equiv \sim q \to \sim p$. (prove indirectly since logical equivalent).

eg. 1: $n \in \mathbb{Z}$, if n^2 odd, n odd.

proof: $p = n^2$ odd. , $q = n$ odd.

contrapositive : $\sim q = n$ even, $\sim p$ n^2 even.

$n = 2k$, $n^2 = (2k)^2 = 4k^2 = 2\underbrace{(2k^2)}_{\text{integer.}}$

$\therefore n^2 =$ even.

eg. 2:

for all $\to \forall$ +ve real numbers, $n \cdot m > 100$ then $n \vee m > 10$

$p = n \cdot m > 100$, $q = n \vee m \geq 10$

contrapositive : $\sim q = n \wedge m \leq 10$, $\sim p = n \cdot m < 100$

note : $\sim (A \vee B) = \sim A \wedge \sim B$.

$n \leq 10 \to n \cdot m \leq 10 \cdot m$

$m \leq 10 \to n \cdot m \leq 10 \cdot 10$

$n \cdot m \leq 100$ (proved).

3. Proof by Contradiction

- Assume opposite of claim, when lead to contradiction, means claim invalid.

eg 1: There are infinitely many prime. : claim.

opposite: There are finite many primes.

$M = P_1 \times P_2 \times P_3 \times \dots P_n + 1$ is a new prime.

$\therefore$ There is not finite prime, & original claim is true.

eg 2: claim: $\sqrt{2}$ is irrational no.

opposite: $\sqrt{2}$ is rational. (i.e no common factor)

$\sqrt{2} = \frac{m}{n}$, $n \neq 0$ 2 * integer = Even.

$2 = \frac{m^2}{n^2} \rightarrow 2n^2 = m^2$, m^2 is even, then m is even, i.e $m = 2k$

$2n^2 = (2k)^2$ 2 * integer = Even.

$2n^2 = 4k^2 \rightarrow n^2 = 2k^2$

$\therefore$ m & n are both even integers. (common factor)

$\therefore$ claim is true $\because$ $\exists$ contradiction.

4. Proof by Exhaustion / cases

- Divide big statement into smaller cases.
- if can proof all sub case, then main case is proved.

eg 1: $(n+1)^3 \geq 3^n$ for $(n \in \mathbb{N} \wedge n \leq 4)$

cases: $n = 1, 2, 3, 4$

* Must have finite possibilities, else cannot use.

5. Proof by Existence & Uniqueness

Proof by existence: if can show / provide examples, then proven.

eg: $\exists$ prime no. x s.t. $x+2$ & $x+6$ are also primes.

$x = 5$, $x+2 = 7$, $x+6 = 11$: proven.

Aka. constructive proof. ~ Proof with specific example.

Proof by uniqueness: step 1: Proof claim

step 2: Proof uniqueness that only work for value found in step 1.

Proof by Induction

Step 1: Show that $P(a)$ true (Basis step)

step 2: if $P(k)$ true, then $P(k+1)$ true. for $k \geq a$ (induction step)