PROOF TECHNIQUES

① Direct Proof + Indirect Proof :

$p \to q \equiv \neg p \vee q$ (if ... then)

$\equiv \neg(\neg q) \vee \neg p$

$\equiv \neg q \to \neg p$

(Contrapositive)

#Ex: for all $n \in \mathbb{Z}$

$\underset{p}{n \text{ is odd}} \underset{\text{if \& only if}}{\iff} \underset{q}{(3n+5) \text{ is even}}$

'$\Rightarrow$' $n = 2k+1$ $\quad \therefore (3n+5) = 3(2k+1)+5 = 6k+8 = 2(3k+4)$ even

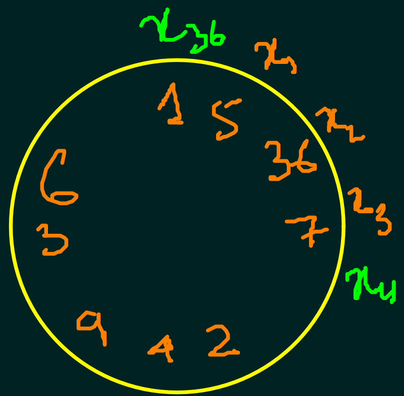
(direct)

'$\Leftarrow$' $q \to p \equiv \neg p \to \neg q$

n is even $= 2k$

$\therefore (3n+5) = 3 \times 2k + 5 = 2(3k+2) + 1$ odd

② Proof by Contradiction :



$1, 2, \ldots, 36$

$x_i + x_{i+1} + x_{i+2} \geq 55$

$\exists\, x_i, x_{i+1}, x_{i+2}$

$x_1 + x_2 + x_3 < 55$

$x_2 + x_3 + x_4 < 55$

$\vdots$

$x_{36} + x_1 + x_2 < 55$

$3 \times \sum_{i=1}^{36} i < 55 \times 36$

$111 \leq 110 \Leftarrow$

Ex: $\sqrt{2}$ is irrational ✓ (assume rational) $\sqrt{2} = \frac{a}{b}$

$a, b \in \mathbb{Z}^+$

$2b^2 = a^2$ ✗

contradiction

$a^2 = p_1^{2e_1} p_2^{2e_2} p_3^{2e_3} \cdots$

$b^2 = q_1^{2f_1} q_2^{2f_2} q_3^{2f_3} \cdots$

$2^1 \times \frac{}{2}$

$60 = 2^2 \times 3 \times 5$

$2 \times 9 = 3^2 \times 2^1$

③ Existance Proofs : $\exists x\, P(x)$ $\quad \forall y\, \exists x\, P(x, y)$ → Non Constr → Constructive

Ex: $\exists$ irrational num x, y, s.t. x^y is rational.

NC

$z = \sqrt{2}^{\sqrt{2}}$ → if z is rational ✓

→ if z is irrational $z^{\sqrt{2}} = (\sqrt{2})^2 = 2$ ← rational

Ex: $\forall$ +ve int n s.t. $\exists$ prime $> n$.

NC

$\boxed{(n! + 1)} > n$ → if prime

→ not a prime → there exist some prime div more than n

Ex: $\forall$ +ve int n, $\exists$ +ve int x, s.t.

$x, x+1, \ldots, x+(n-1)$ are all composite. ✓

CP

$x = (n+1)! + 2 \leftarrow$ 2 divides x

$x+1 = (n+1)! + 3 \leftarrow$ 3 divides x

$x+2 = (n+1)! + 4 \leftarrow$ 4 divides x

$\vdots$

$x+n-1 = (n+1)! + (n+1) \leftarrow$ $(n+1)$ divides $x+n-1$.

Ⓐ Proof by cases:

$$\boxed{p_1} \vee \boxed{p_2} \rightarrow q \equiv (\neg p_1 \wedge \neg p_2) \vee q$$

$$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$$

Ex: $\forall$ +ve int $n > 1$.

$(4^n + n^4)$ is composite

Case-1: $n =$ odd

$$\therefore (4^n + n^4) = (2^n + n^2)^2 - 2^{n+1} \cdot n^2$$

$$= \underbrace{\left(2^n + n^2 + 2^{\frac{n+1}{2}} \cdot n\right)}_{p} \times \underbrace{\left(2^n + n^2 - 2^{\frac{n+1}{2}} \cdot n\right)}_{q}$$

Case-2: $n =$ even $= 2k$

$4^n + n^4 > 2$

$4^n + n^4 = 4^{2k} + (2k)^4 \leftarrow$ multiple of 2

5. Proof by Disjunctions:

$p \to q \vee r$ $\to$ $p \wedge \neg q \to r$ OR $p \wedge \neg r \to q$

$\neg p \vee q \vee r \equiv \neg(p \wedge \neg q) \vee r$

Ex: Let p be prime. a, b are int. If p divides ab then $p \mid a$ or $p \mid b$.

$\neg p \mid a$

$\gcd(p, a) = 1 \Rightarrow 1 = up + va$ where $u, v \in \mathbb{Z}$ (?)

$b = \underbrace{upb}_{\text{div by } p} + \underbrace{vab}_{p \mid ab}$

$p \mid b$

6. Cycle of Implications:

$1 \to 2 \to 3 \to 1$

$1 \to 2 \to 4 \to 1$ & $1 \to 3 \to 1$

Ex: (1) a divides b.

(2) $\gcd(a, b) = a$

(3) $\lfloor b/a \rfloor = b/a$

equivalent.

$1 \to 2 \to$ $b = ak$, $\gcd(a,b) = a$

$2 \to 3 \Rightarrow \gcd(a,b) = a$ $ak = b$

$\lfloor b/a \rfloor = \frac{b}{a} = k = \text{int}$

$3 \to 1 \Rightarrow \lfloor b/a \rfloor = b/a = k$ int

$b = ak$

7 Proof by Induction: → Strong, → Weak

$\underbrace{P_1 \quad P_2 \, \cdots \, P_k}_{} \Rightarrow P_{k+1}$

$P_i \rightarrow P_{i+1}$

Ex: $F_0 = 0$ $\quad F_n = F_{n-1} + F_{n-2}, \; \forall n \geq 2$

$F_1 = 1$

P.T. $F_0^2 + F_1^2 + F_2^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$

Base: $0^2 = F_0^2 = F_0 \times F_1 = 0 \times 1 = 0$

Induction Hyp: $F_0^2 + F_1^2 + \cdots + F_n^2 = F_n F_{n+1}$ holds

Proof: $(F_0^2 + \cdots + F_n^2) + F_{n+1}^2 = F_n F_{n+1} + F_{n+1}^2$

$= F_{n+1}(F_n + F_{n+1})$

$= F_{n+1} F_{n+2}$

Disprove: Only one counter example

$\exists x \, \neg P(x)$ holds

$\boxed{\text{P.T. } \forall x \, P(x) \text{ holds}}$

Ex: $\forall a, b \in \mathbb{R}$ $\quad a^2 > b^2 \Rightarrow a > b$? → No. $\left.\begin{matrix} a = -3 \\ b = +2 \end{matrix}\right\}$ ✓

Excersise : $L_1 \; L_2 \; \cdots \; L_n$ (lamps) → ON (1), → OFF (0)

initially all $L_i \leftarrow 0$

```
for (i=1 ; i<=n ; i++)
    for (j=i ; j<=n ; j+=i)
        L_j = 1 - L_j ; // flipping lamp ON/OFF
```

Question: Which lamp is/are ON ?? Why!!

Introduction

Proof Tech.