

# Indirect Proof

$$\begin{array}{l} P \rightarrow q \\ \sim q \\ \hline \therefore \sim P \end{array}$$

$$\begin{array}{l} P \rightarrow q \\ P \wedge \sim q \\ \hline \therefore \text{E} \end{array}$$

proof by contradiction

(reductio ad absurdum)

1. Suppose the statement is false  
(Suppose negation is true)
2. Supposition leads to a contradiction
3. Conclude the orig. statement is true.

There is no greatest integer.

proof: (by contradiction)

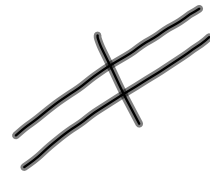
Suppose there is a greatest integer,  $N$ .

$$\textcircled{1} \quad \forall n \in \mathbb{Z}, n \leq N$$

Let  $M = N + 1$ . so  $m \in \mathbb{Z}$

and  $M > N$ .

which contradicts  $\textcircled{1}$



The sum of any rational number  
and any irrational number  
is irrational.

$$\forall r \in \mathbb{Q}, s \notin \mathbb{Q}, r+s \notin \mathbb{Q}$$

suppose (not)

$$\exists r \in \mathbb{Q}, s \notin \mathbb{Q} \text{ s.t. } r+s \in \mathbb{Q}$$

$$r = \frac{a}{b} \quad a, b \in \mathbb{Z} \quad b \neq 0$$

$$r+s = \frac{c}{d} \quad c, d \in \mathbb{Z} \quad d \neq 0$$

$$\frac{a}{b} + s = \frac{c}{d}$$

$$s = \frac{c}{d} - \frac{a}{b}$$

$$= \frac{cb - ad}{db} \quad \begin{matrix} d \neq 0 \\ b \neq 0 \end{matrix}$$

so  $db \neq 0$

$$\text{Let } p = cb - ad$$

$$q = db \quad (q \neq 0)$$

$$\text{so } s = \frac{p}{q} \quad \begin{matrix} p \in \mathbb{Z} \\ q \in \mathbb{Z} \end{matrix}$$

so  $s$  is rational  
but  $s$  was not rational  
which is a contradiction.

~~///~~

## Contraposition

1. Express statement as

$$\forall x \in D, P(x) \rightarrow Q(x)$$

2. Rewrite as contrapositive

$$\forall x \in D, \neg Q(x) \rightarrow \neg P(x)$$

3. Prove contrapositive as in a direct proof:

Suppose:  $\neg Q(x)$

Show:  $\neg P(x)$

For all  $n \in \mathbb{Z}$ , if  $n^2$  is even  
then  $n$  is even.

contrapositive:

if  $n$  is odd then  $n^2$  is odd.

suppose  $n$  is an odd integer.

$$n = 2k + 1 \quad k \in \mathbb{Z}$$

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

$$= 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1$$

⋮

for all  $a, b, c \in \mathbb{Z}$ ,

$$a \nmid bc \rightarrow a \nmid b$$

$p \rightarrow q$

Proof by contradiction.

$p \rightarrow q$

Suppose:  $\exists a, b, c \in \mathbb{Z}$  s.t.  
 $a \nmid bc$  and  $a \mid b$

since  $a \mid b$ ,  $b = a \cdot k$   $k \in \mathbb{Z}$

$$\begin{aligned} \text{so } bc &= (ak)c \\ &= (ck)a \end{aligned}$$

$$\text{Let } l = ck \quad l \in \mathbb{Z}$$

$$\text{so } bc = l \cdot a$$

$$\therefore a \mid bc$$

which is a contradiction.

Therefore

$$\forall a, b, c \in \mathbb{Z}, a \nmid bc \rightarrow a \nmid b$$

for all  $a, b, c \in \mathbb{Z}$ ,

$$a \mid bc \rightarrow a \mid b$$

proof by contraposition

$$\forall a, b, c \in \mathbb{Z}, a \mid b \rightarrow a \mid bc$$

suppose  $a \mid b$   $a, b \in \mathbb{Z}$

show  $a \mid bc$

since  $a \mid b$  we have  $b = a \cdot k$ ,  
 $k \in \mathbb{Z}$

consider  $b \cdot c = (a \cdot k) \cdot c$  subst  
 $= (c \cdot k) a$

Let  $l = c \cdot k$   
so  $bc = l \cdot a$   $l \in \mathbb{Z}$

which by def. of  $\mid$   
 $a \mid bc$ .



