

# CHAPTER 6 - PROOF BY CONTRADICTION

STATEMENT P

PROOF OUTLINE:

SUPPOSE FOR CONTRADICTION  $\neg P$ .

..... BULLSHIT  $\square$

SOMETHING LIKE  $1=0$  ? ← CLEARLY  
FALSE STATEMENT.

EXAMPLE (logic)

PREMISES {  $(\neg B \vee C) \rightarrow A$   
 $B \rightarrow D$   
 $C \vee \neg D$

PROVE A

PROOF

1)  $\neg A$  ... FOR CONTRADICTION

2)  $(\neg B \vee C) \rightarrow A$  PREMISE

3)  $\neg(\neg B \vee C)$  MODUS TOLLENSE 1+2

4)  $B \& \neg C$  DE MORGAN 3

5)  $\neg C$  DECOMP. OF WPS. 4

6, D

DECOMP. CONS. 4

7, C V  $\neg$  D

Premise

8, C

DISJUNCTIVE SYLLOGISM(6,7)

9, C  $\&$   $\neg$  C

CONSTRUCTING A CONS. (5,8)

THIS IS FALSE! NOT POSSIBLE IF  
ALL LINES WERE TRUE. HENCE  $\neg$ A  
MUST BE FALSE. THEREFORE A  
IS TRUE.

P

WE SHOWED  $\neg$ A  $\Rightarrow$  (C  $\&$   $\neg$ C)

WHEN IS  $\neg$ A  $\Rightarrow$  (C  $\&$   $\neg$ C) TRUE ??

A	C	$\neg$ A	C $\&$ $\neg$ C	$\neg$ A $\Rightarrow$ (C $\&$ $\neg$ C)
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

↗

TRUE ONLY IFF A IS TRUE

(C  $\&$   $\neg$ C) IS CALLED CONTRADICTION

# THEOREM (EUCLID)

THERE ARE INFINITELY MANY PRIME NUMBERS

PROOF (HARD FOR DIRECT - WHERE TO START?)

SUPPOSE FOR THE SAKE OF CONTRADICTION

THAT THERE ARE FINITELY MANY PRIME NUMBERS.

$P = \{p_1, p_2, \dots, p_n\}$  BE ALL PRIMES FOR SOME  $n \in \mathbb{N}$ . LET  $x = 1 + p_1 p_2 \dots p_n$ . SINCE  $x \notin P$  THEN  $x = c \cdot p_k$  FOR SOME  $c \in \mathbb{Z}$  AND  $k \in \{1, \dots, n\}$ .

THEN

$$1 + p_1 p_2 \dots p_n = c \cdot p_k$$

$$\underbrace{\frac{1}{p_k}}_{\notin \mathbb{Z}} + \underbrace{(p_1 \dots p_n)/p_k}_{c \in \mathbb{Z}} = \underbrace{c}_{\in \mathbb{Z}}$$

CONTRADICTION!

□

# THEOREM

THE NUMBER  $\sqrt{2}$  IS NOT RATIONAL

## PROOF

SUPPOSE FOR THE SAKE OF CONTRADICTION THAT  $\sqrt{2}$  IS RATIONAL. HENCE

$\sqrt{2} = \frac{p}{q}$  FOR  $p, q \in \mathbb{Z}$ . PICK  $p, q$  ST.

AT MOST ONE IS EVEN,

$$\sqrt{2} = \frac{p}{q}$$

$$2 = \frac{p^2}{q^2}$$

$$2q^2 = p^2$$

HENCE  $p^2$  IS EVEN. SINCE ODD  $\times$  ODD = ODD,

ALSO  $p$  IS EVEN AND  $p = 2a$  FOR SOME  
 $a \in \mathbb{Z}$ .

$$2q^2 = p^2 = (2a)^2 = 4a^2$$

$$q^2 = 2a^2$$

HENCE  $q^2$  IS EVEN. THEREFORE,  $q$  IS EVEN.

THEN  $p, q$  BOTH EVEN, CONTRADICTION  
WITH CHOICE OF  $p, q$  (AT MOST  
ONE EVEN)

3

## NOTICE

- PROOF BY CONTRADICTION GIVES YOU SOMETHING TO START WITH
- NOT CLEAR WHAT WILL BE THE CONTRADICTION
- ALWAYS START WRITING PROOF BY CONTRADICTION AS:

SUPPOSE FOR CONTRADICTION...  
OPTIONAL THE SAKE OF

## 6.2 PROVING CONDITIONAL STATEMENTS BY CONTRADICTION

THEOREM  $P \Rightarrow Q$

$$\neg(P \Rightarrow Q)$$

↓

PROOF: FOR CONTRADICTION  $P \wedge \neg Q$

$$\therefore C \wedge \neg C - D$$

YOU GET 2 STATEMENTS TO START

(Ex) PROPOSITION: LET  $a \in \mathbb{Z}$ .

IF  $a^2$  IS EVEN THEN  $a$  IS EVEN.

PROOF

SUPPOSE FOR CONTRADICTION

THAT  $\exists a \in \mathbb{Z}$ :  $a^2$  EVEN AND  $a$  ODD.

IF  $a$  ODD THEN  $a = 2k+1$  FOR  
SOME  $k \in \mathbb{Z}$ . THEN

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

WHICH IS ODD. THIS CONTRADICTS  
THAT  $a^2$  IS EVEN.  $\square$

PROPOSITION EVERY NON-ZERO RATIONAL NUMBER IS A PRODUCT OF TWO IRRATIONAL NUMBERS.

PROOF

LET  $a \in \mathbb{Q}$ . THEN  $a = \frac{p}{q}$  FOR SOME  $p, q \in \mathbb{Z}$ . ALSO  $a = \sqrt{2} \cdot \frac{a}{\sqrt{2}}$ .  $\sqrt{2}$  IS IRRATIONAL. WHAT  $\frac{a}{\sqrt{2}}$ ?

SUPPOSE FOR CONTRADICTION  $a/\sqrt{2}$  IS RATIONAL. THEN FOR SOME  $c, d \in \mathbb{Z}$

$$\frac{a}{\sqrt{2}} = \frac{c}{d}, \quad a \cdot d = \sqrt{2} \cdot c$$

$$\frac{p}{q}, \frac{d}{c} = \sqrt{2}$$

$$\left[ \frac{p \cdot d}{q \cdot c} \right] = (\sqrt{2})$$

RATIONAL      IRRATIONAL

$\Rightarrow$  CONTRADICTION.

HENCE  $\frac{a}{\sqrt{2}}$  IS IRRATIONAL. SO  $a$  IS A PRODUCT OF  $\sqrt{2}, \frac{a}{\sqrt{2}}$ .

□