

## Goals

- Describe proof by contrapositive, iff proofs, proof by cases, proof by example.
- Practice writing proofs

\* Doing self-assessment + unsure if correct... contact assigned TA!

## Proof By Contrapositive

- Use: Prove  $P \rightarrow Q$

$$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$$

P	Q	$\neg Q$	$\neg P$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$
T	T	F	F	T	T
T	F	T	F	F	F
F	T	F	T	T	T
F	F	T	T	T	T

### Structure:

We prove the contrapositive. Assume  $\neg Q$ . Explain explain, explain. Therefore,  $\neg P$ .

- Use: Prove  $\forall x \in S, P(x) \rightarrow Q(x)$

### Structure

We prove the contrapositive

Let  $x \in S$  and assume  $\neg Q(x)$

Explain, explain, explain.

Therefore,  $\neg P(x)$ .

Q: What is the first sentence of a contrapositive proof of:

"If  $a^2$  is not divisible by 4, then  $a$  is odd."

- A) We prove the contrapositive. Assume  $a$  is odd.
- B) We prove the contrapositive. Assume  $a$  is even.
- C) We prove the contrapositive. Assume  $\neg 4|a^2$ .
- D) We prove the contrapositive. Assume  $4|a^2$ .

Q: What is the first sentence of a contrapositive proof of:

$$P \quad \rightarrow \quad Q$$

"If [ $a^2$  is not divisible by 4] then [ $a$  is odd]"

A) Assume  $a$  is odd

B) Assume  $a$  is even

C) Assume  $\neg 4|a^2$

D) Assume  $4|a^2$

$$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$$

$$\neg P = "a \text{ is even}"$$

For practice, complete the proof. (Solution on next page.)

Optional



We prove the contrapositive. [Let  $a \in \mathbb{Z}$ .] Suppose  $a$  is even. Then  $\exists k \in \mathbb{Z} : 2k = a$ . This means  $a^2 = 4k^2$ . Since  $k^2$  is an integer,  $4|a^2$ .

# There is an implied "for all" in the proof statement. (Otherwise it is a predicate & we can't prove true or false). Therefore, we need "Let  $a \in \mathbb{Z}$ ."



Iff Proofs


Iff = "if and only if."

Use:  $P \leftrightarrow Q$ 

$$(P \rightarrow Q) \wedge (Q \rightarrow P) \equiv P \leftrightarrow Q \quad (\text{use truth table proof})$$

Structure

- $\mathbb{P}$  For the forward direction, [Proof of  $P \rightarrow Q$ ] 
- $\mathbb{P}$  For the backwards direction, [Proof of  $Q \rightarrow P$ ] 


  
 Could be direct or contrapositive

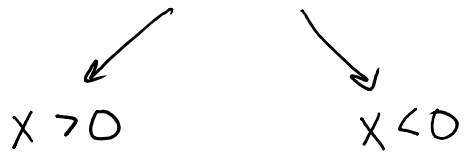
# Proof By Cases

Use:  $\forall x \in A, \dots$

Want to prove for all  $x$  in  $A$ , but sometimes need different techniques for different subsets of  $A$

ex:  $\forall x \in \mathbb{Z} \dots$

where to start?

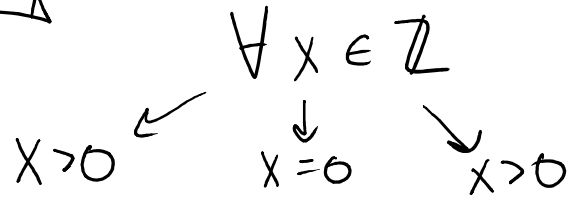


Split into cases.

Now can turn each case into math and move forward.

Better

Missing case  $x=0$   
\*Make sure cases contain all possibilities\*



"Let  $x \in \mathbb{Z}$ . There are three cases:  $x > 0$ ,  $x < 0$ , and  $x = 0$ .

For the first case, assume  $x > 0 \dots$

$\mathbb{P}$  For the second case, assume  $x < 0 \dots$

$\mathbb{P}$  For the third case, assume  $x = 0 \dots$

When proving correctness of algorithm and see

if ..

else ..

}

use proof by cases to show

- cover all situations

- behaves correctly in all situations

Proof by ContradictionUse: any statement  $P$ 

Proof has two parts

→ ①	(Direct)	$\Gamma P \rightarrow Q$	}	Most common
→ ②	(Direct)	$\Gamma P \rightarrow \Gamma Q$		
$\therefore P$				

StructureFor contradiction assume  $\neg P$ Explain explain...  $Q$ Explain explain...  $\neg Q$ , a contradiction.Thus,  $P$  is true

When start, don't know what  $Q$  is... you need to keep your eye out for what might be the contradiction.



Q: Prove  $\sqrt{2}$  is irrational

\* Not of form  $P \rightarrow Q$

A: For contradiction, suppose  $\sqrt{2}$  is rational. Then  
 $\exists a, b \in \mathbb{Z} : \frac{a}{b} = \sqrt{2}$  where the fraction  
 is fully simplified, so  $\nexists c \in \mathbb{Z} : c|a \wedge c|b$ .  
 Squaring both sides, we have

$$a^2 = 2b^2.$$

Thus  $2|a^2$ . But we've previously proved this  
 implies  $2|a$ . This means  $\exists m \in \mathbb{Z} : 2m = a$ . Plugging  
 in, we have

$$4a^2 = 2b^2.$$

Dividing by 2, we get

$$2a^2 = b^2.$$

But this means  $2|b^2$ , and so  $2|b$ . But  
 this means  $2|a$  and  $2|b$ , which contradicts the fact  
 that  $\frac{a}{b}$  is fully simplified.  $\square$

Q: Prove:  $\nexists x, y \in \mathbb{Z} : x^2 = 4y^2 + 2$