# **(Direct Proof, Proof** by contrapositive





DISCRETE STRUCTURES

Lecture 06

**Arfan Shahzad** 

{ <u>arfanskp@gmail.com</u> }

# Definitions



- A **theorem** is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important.
- Less important theorems sometimes are called propositions. (Theorems can also be referred to as facts or results.) A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion.
- However, it may be some other type of logical statement, as the examples later in this chapter will show. We demonstrate that a theorem is true with a **proof**.





#### Methods of Proving Theorems

- Direct Proof
- Proof by Contraposition (Contrapositive)



## Methods of Proving Theorems cont... Direct Proof

- The simplest (from a logic perspective) style of proof is a *direct proof*.
- Often all that is required to prove something is a systematic explanation of what everything means.
- Direct proofs are especially useful when proving implications.
- The general format to prove  $p \rightarrow q$  is this:
- Assume p. Explain, explain, ..., explain. Therefore q.



## Methods of Proving Theorems cont... Direct Proof

- Often we want to prove universal statements, perhaps of the form  $\forall x(p(x) \rightarrow q(x))$ .
- Again, we will want to assume p(x) is true and deduce q(x).
- But what about the x? We want this to work for all x.
- We accomplish this by fixing x to be an arbitrary element (of the sort we are interested in).



- **Prove:** For all integers n, if n is even, then n<sup>2</sup> is even.
- The format of the proof with be this: Let n be an arbitrary integer. Assume that n is even. Therefore  $n^2$  is even.
- To fill in the details, we will basically just explain what it means for n to be even, and then see what that means for n<sup>2</sup>. Here is a complete proof.



- The integer n is even if there exists an integer k such that n = 2k, and n is odd if there exists an integer k such that n = 2k + 1. (every integer is either even or odd, and no integer is both even and odd.)
- Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.



- **Proof** Let n be an arbitrary integer.
- Suppose n is even.
- Then n=2k for some integer k.
- Now  $n^2=(2k)^2=4k^2=2(2k^2)$ . Since  $2k^2$  is an integer,  $n^2$  is even.
- Hence proved (For all integers n, if n is even, then n<sup>2</sup> is even.)



Give a direct proof that if **m** and **n** are both perfect squares, then **nm** is also a perfect square.

• (An integer **a** is a perfect square if there is an integer **b** such that  $a=b^2$ .)



- Solution: To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, i.e. m and n are both perfect squares.
- By the definition of a perfect square, it follows that there are integers **s** and **t** such that  $\mathbf{m} = \mathbf{s}^2$  and  $\mathbf{n} = \mathbf{t}^2$ .



- The goal of the proof is to show that mn must also be a perfect square when m and n are; looking ahead we see how we can show this by substituting s<sup>2</sup> for m and t<sup>2</sup> for n into mn.
- This tells us that **mn = s<sup>2</sup>t<sup>2</sup>**.
- Hence,  $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$ , using commutativity and

associativity of multiplication.



- By the definition of perfect square, it follows that **mn** is also a perfect square, because it is the square of **st**, which is an integer.
- We have proved that if m and n are both perfect squares, then mn is also a perfect square.





- Recall that an implication  $p \rightarrow q$  is logically equivalent to its contrapositive  $\neg q \rightarrow \neg p$ .
- There are plenty of examples of statements which are hard to prove directly, but whose contrapositive can easily be proved directly.
- This is all that proof by contrapositive does.
- It gives a direct proof of the contrapositive of the implication.

ArfanShahzadTech







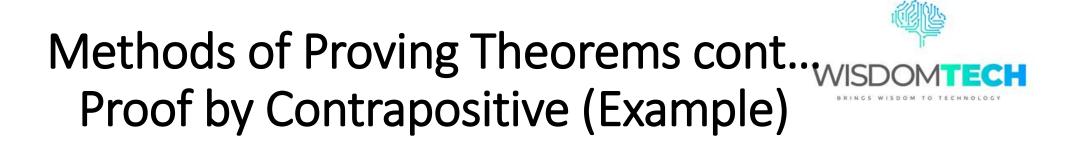
- This is enough because the contrapositive is logically equivalent to the original implication.
- The skeleton of the proof of  $p \rightarrow q$  by contrapositive will always look roughly like this: Assume  $\neg q$ . Explain, explain, ... explain. Therefore  $\neg p$ .
- As before, if there are variables and quantifiers, we set them to be arbitrary elements of our domain. Here are a couple examples:



# 

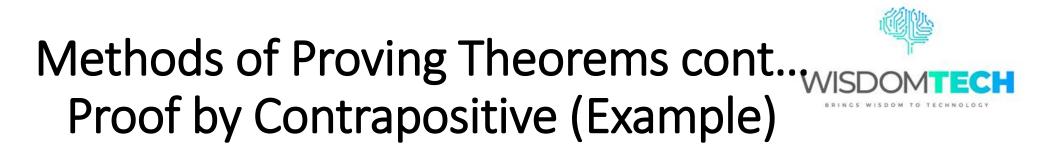
- Prove the statement "for all integers n, if n<sup>2</sup> is even, then n is even" true?
- **Solution:** This is the converse of the statement we proved above using a direct proof.
- A direct proof of this statement would require fixing an arbitrary n and assuming that n<sup>2</sup> is even. But it is not at all clear how this would allow us to conclude anything about n. Just because n<sup>2</sup>=2k does not in itself suggest how we could write n as a multiple of 2.





- Try something else: write the contrapositive of the statement. We get, for all integers n, if n is odd then n<sup>2</sup> is odd. Our proof will look something like this:
- Let n be an arbitrary integer. Suppose that n is not even. .... Therefore n<sup>2</sup> is not even.





- Now we fill in the details:
- **<u>Proof</u>**: We will prove the contrapositive. Let n be an arbitrary integer. Suppose that n is not even, and thus odd. Then n=2k+1 for some integer k.
- Now  $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ .
- Since 2k<sup>2</sup>+2k is an integer, we see that n<sup>2</sup> is odd and therefore not even.

