CMSC 207- Lecture 11
CHAPTER 4: Elementary Number Theory and Methods of Proof (4.5-4.8)

Dr. Ahmed Tarek

Direct Proof and Counterexample: Floor and Ceiling

- The *floor* and *ceiling* of the number are the integers to the immediate left and to the immediate right of the number (unless the number is an integer, in which case its floor and ceiling both equal the number itself).

- Many computer languages have built-in functions that compute floor and ceiling automatically. These functions are very convenient to use when writing certain kinds of computer programs.

- In addition, the concepts of floor and ceiling are important in analyzing the efficiency of many computer algorithms.

Direct Proof and Counterexample: Floor and Ceiling

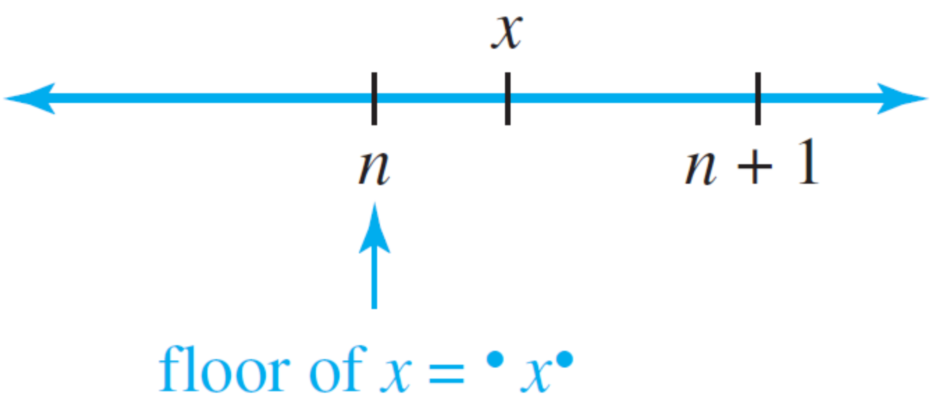
- **Definition**

Given any real number x, the **floor of x**, denoted $\lfloor x \rfloor$, is defined as follows:

$$\lfloor x \rfloor = \text{that unique integer } n \text{ such that } n \leq x < n + 1.$$

Symbolically, if x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$



Direct Proof and Counterexample: Floor and Ceiling

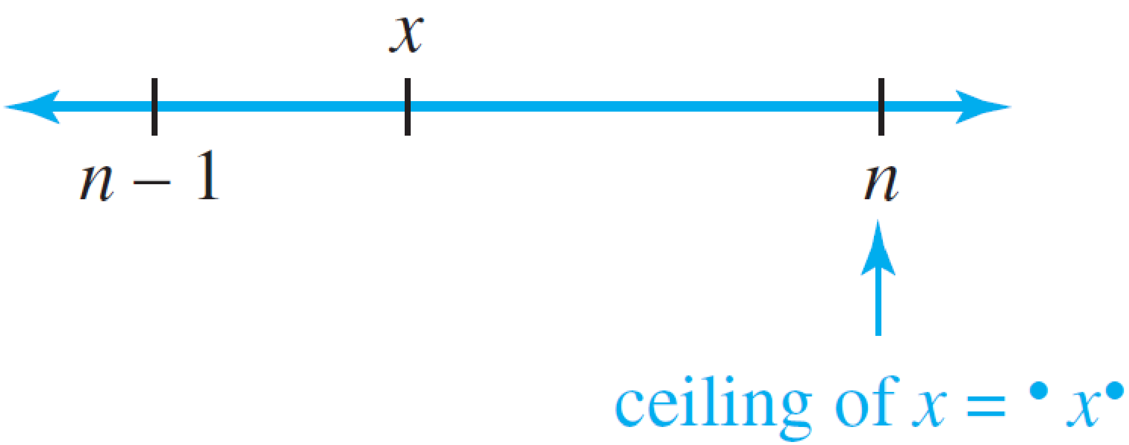
• Definition

Given any real number x, the **ceiling of x**, denoted $\lceil x \rceil$, is defined as follows:

$$\lceil x \rceil = \text{that unique integer } n \text{ such that } n - 1 < x \leq n.$$

Symbolically, if x is a real number and n is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$



Example 1 – *Computing Floors and Ceilings*

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the following values of *x*:

a. 25/4 **b.** 0.999 **c.** –2.01

Solution:

a. $25/4 = 6.25$ and $6 < 6.25 < 7$; hence $\lfloor 25/4 \rfloor = 6$ and $\lceil 25/4 \rceil = 7$.

b. $0 < 0.999 < 1$; hence $\lfloor 0.999 \rfloor = 0$ and $\lceil 0.999 \rceil = 1$.

c. $-3 < -2.01 < -2$; hence $\lfloor -2.01 \rfloor = -3$ and $\lceil -2.01 \rceil = -2$.

Note that on some calculators $\lfloor x \rfloor$ is denoted INT (*x*).

Example – *Disproving an Alleged Property of Floor*

Is the following statement true or false?

For all real numbers *x* and *y*, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.

Solution:

The statement is false. As a counterexample, take

$x = y = \frac{1}{2}$.

Then

$$\lfloor x \rfloor + \lfloor y \rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = 0 + 0 = 0,$$

whereas $\lfloor x + y \rfloor = \left\lfloor \frac{1}{2} + \frac{1}{2} \right\rfloor = \lfloor 1 \rfloor = 1.$

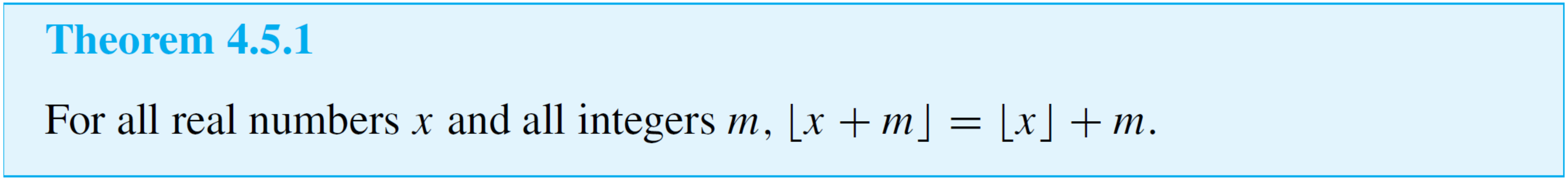
Example – *Solution*

$$\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor.$$

Theorem

This discussion is summarized as follows:

Theorem 1



Theorem 4.5.1

For all real numbers x and all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof:

Suppose a real number *x* and an integer *m* are given. *[We must show that* $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. *]*

Let *n* = $\lfloor x \rfloor$. By definition of floor, *n* is an integer and

$$n \leq x < n + 1.$$

Theorem

Add *m* to all three parts to obtain

$$n + m \leq x + m < n + m + 1$$

[since adding a number to both sides of an inequality does not change the direction of the inequality].

Now *n* + *m* is an integer *[since n and m are integers and a sum of integers is an integer]*, and so, by definition of floor, the left-hand side of the equation to be shown is $\lfloor x + m \rfloor = n + m.$

Theorem

But *n* = $\lfloor x \rfloor$. Hence, by substitution,

$$n + m = \lfloor x \rfloor + m,$$

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

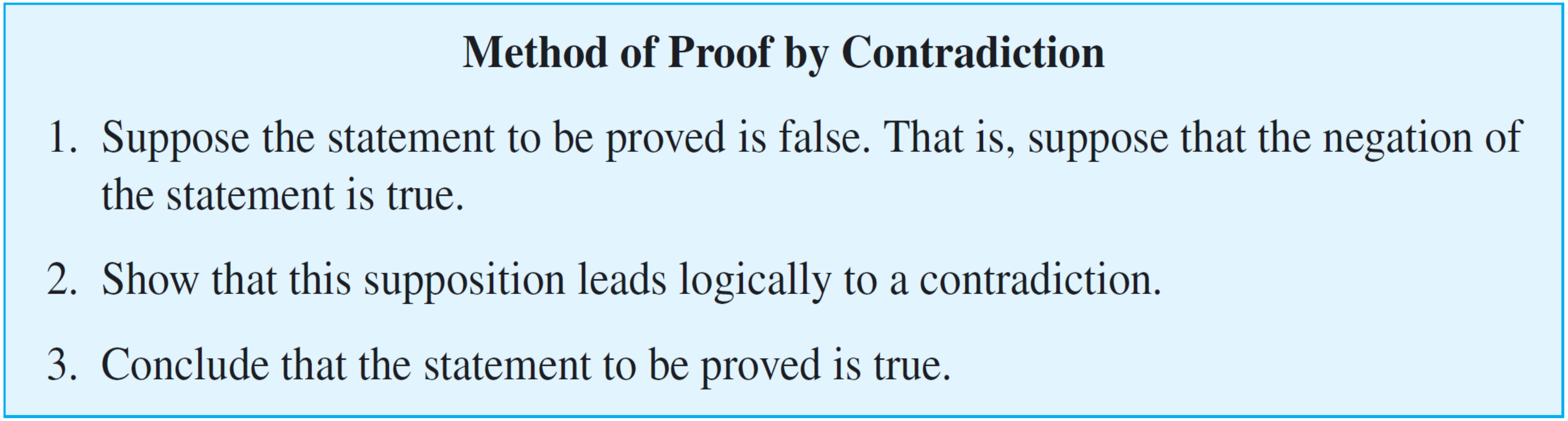
which is the right-hand side of the equation to be shown.

Indirect Argument: Contradiction and Contraposition

- In a direct proof you **start with the hypothesis of a statement** and make one deduction after another until you **reach the conclusion**.
- One kind of indirect proof, *argument by contradiction*, is based on the fact that either a statement is true or it is false but not both.
- So if you can show that the assumption that a given statement is not true leads logically to a contradiction, impossibility, or absurdity, then that assumption must be false: and, hence, the given statement must be true.

Indirect Argument: Contradiction and Contraposition

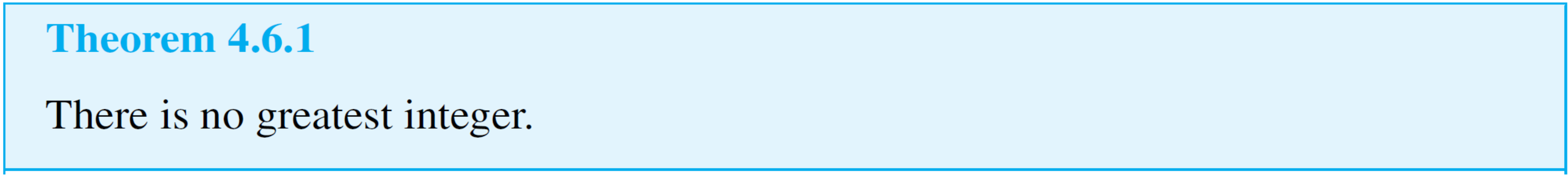
- The point of departure for **a proof by contradiction** is the supposition that the **statement to be proved is false**. The goal is to reason to a contradiction. Thus proof by contradiction has the following outline:



Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

In-class Assignment #2: – *Prove that there Is No Greatest Integer*



Theorem 4.6.1

There is no greatest integer.

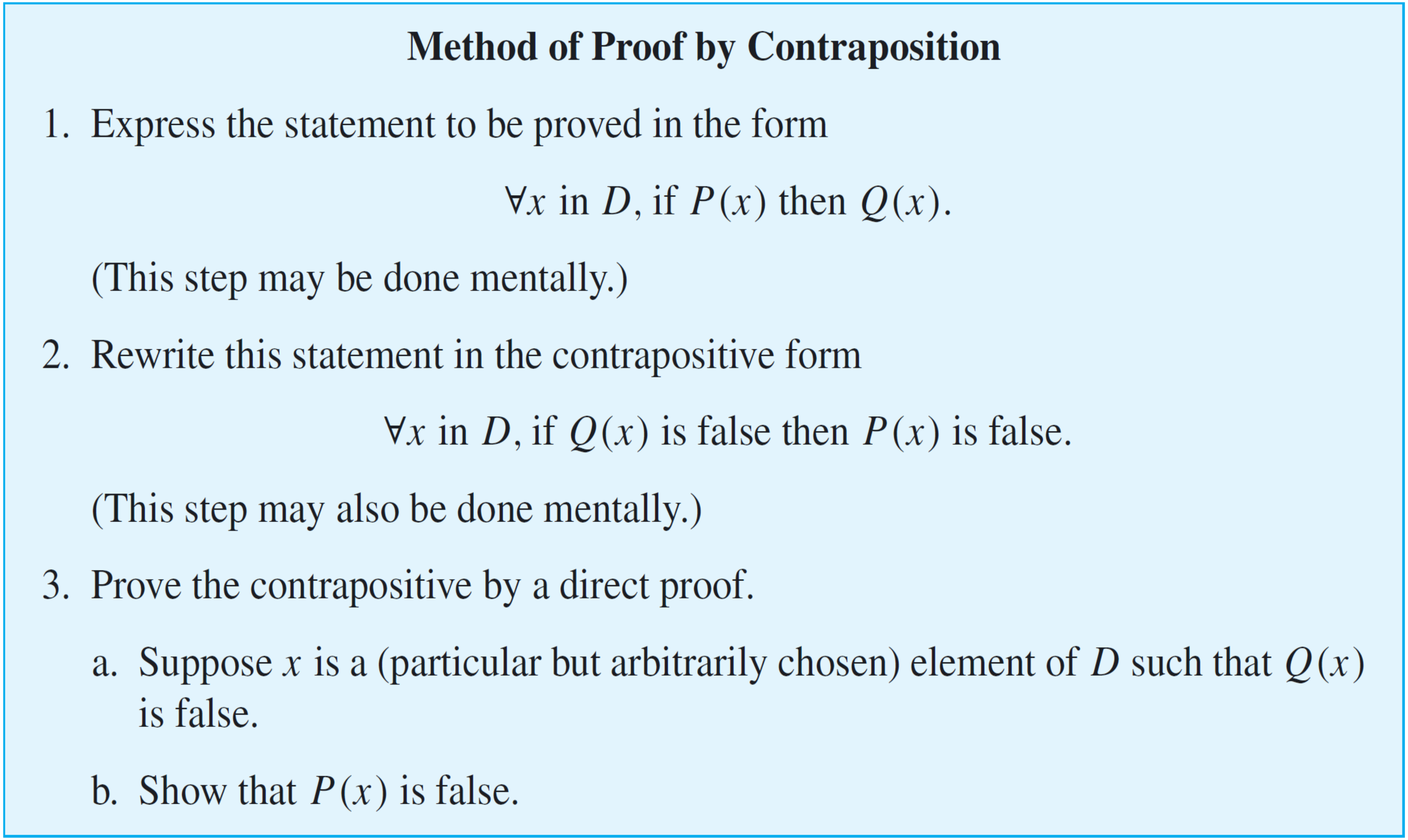
•Proof:

[*Hints: Take the negation of the theorem and suppose it to be true.*] Suppose not. That is, suppose there is a greatest integer *N*. [*Next deduce a contradiction.*]

Argument by Contraposition

- A second form of indirect argument, *argument by contraposition*, is based on the logical equivalence between a statement and its contrapositive.
- To prove a statement by contraposition, you take the contrapositive of the statement, prove the contrapositive by a direct proof, and conclude that the original statement is true.
- The underlying reasoning is that since a conditional statement is logically equivalent to its contrapositive, if the contrapositive is true then the statement must also be true.

Argument by Contraposition



Method of Proof by Contraposition

1. Express the statement to be proved in the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

(This step may be done mentally.)

2. Rewrite this statement in the contrapositive form

$$\forall x \text{ in } D, \text{ if } Q(x) \text{ is false then } P(x) \text{ is false.}$$

(This step may also be done mentally.)

3. Prove the contrapositive by a direct proof.

   a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.

   b. Show that $P(x)$ is false.

In-class Assignment #3: – *If the Square of an Integer Is Even, Then the Integer Is Even*

- Prove that for all integers *n*, if n^2 is even then n is even.

- Solution Hints:

First form the contrapositive of the statement to be proved.

- *Contrapositive*: For all integers *n*, if *n* is not even then n^2 is not even.

- By the quotient-remainder theorem, any integer is either even or odd. So any integer that is not even is odd. Also, no integer can be both even and odd. So if an integer is odd, then it is not even. **NOW PROVE.**

Relation between Proof by Contradiction and Proof by Contraposition

- Observe that any proof by contraposition can be recast in the language of proof by contradiction. In a proof by contraposition, the statement

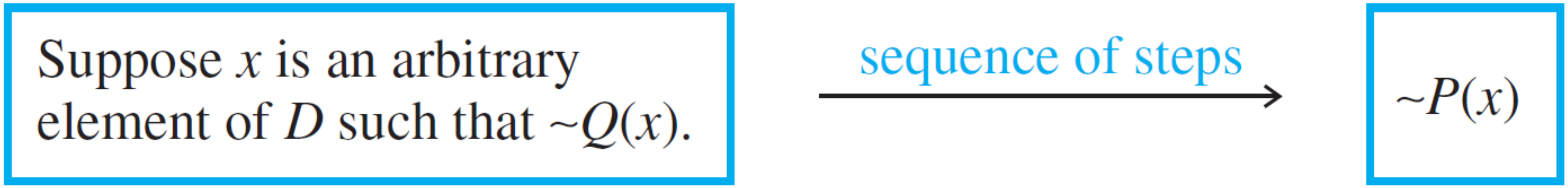
$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$$

- is proved by giving a direct proof of the equivalent statement

$$\forall x \text{ in } D, \text{ if } \sim Q(x) \text{ then } \sim P(x).$$

Relation between Proof by Contradiction and Proof by Contraposition

- To do this, you suppose you are given an arbitrary element *x* of *D* such that ~*Q*(*x*). You then show that ~*P*(*x*). This is illustrated in Figure below.



Suppose x is an arbitrary element of D such that $\sim Q(x)$.

sequence of steps

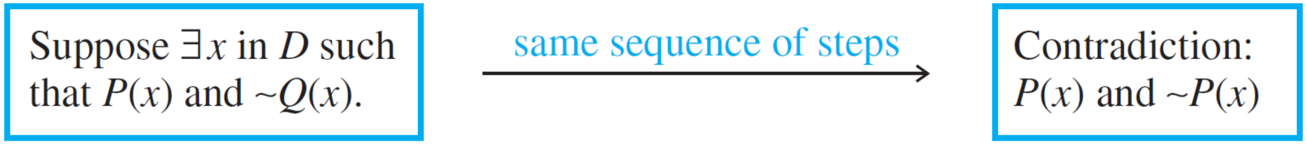
$\sim P(x)$

Proof by Contraposition

- Exactly the same sequence of steps can be used as the heart of a proof by contradiction for the given statement. The only thing that changes is the context in which the steps are written down.

Relation between Proof by Contradiction and Proof by Contraposition

- To rewrite the proof as a proof by contradiction, you suppose there is an *x* in *D* such that *P* (*x*) and ~*Q* (*x*).
- You then follow the steps of the proof by contraposition to deduce the statement ~*P* (*x*). But ~*P* (*x*) is a contradiction to the supposition that *P* (*x*) and ~*Q* (*x*). (Because to contradict a conjunction of two statements, it is only necessary to contradict one of them.) This process is illustrated in Figure below.



Suppose $\exists x$ in D such that $P(x)$ and $\sim Q(x)$.

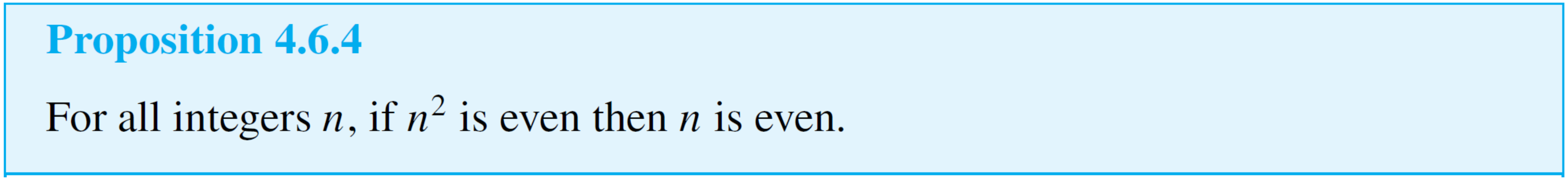
same sequence of steps

Contradiction: $P(x)$ and $\sim P(x)$

Proof by Contradiction

Relation between Proof by Contradiction and Proof by Contraposition

- As an example, here is a proof by contradiction of Proposition 4.6.4, namely that for any integer n, if n^2 is even then n is even.



Proposition 4.6.4

For all integers n, if n^2 is even then n is even.

- **Proof (by contradiction):**

[We take the negation of the theorem and suppose it to be true.] Suppose not. That is, suppose there is an integer n such that n^2 is even and n is not even. *[We must deduce a contradiction.]*

Relation between Proof by Contradiction and Proof by Contraposition

- By the quotient-remainder theorem with $d = 2$, any integer is even or odd (remainder or no remainder). Hence, since n is not even, so it is odd, and thus, by definition of odd, $n = 2k + 1$ for some integer k. By substitution and algebra:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

- But $2k^2 + 2k$ is an integer because products and sums of integers are integers.
- So $n^2 = 2 \cdot (\text{an integer}) + 1$, and thus, by definition of odd, n^2 is odd. Therefore, n^2 is both even and odd.

Relation between Proof by Contradiction and Proof by Contraposition

- This contradicts Theorem 4.6.2, which states that no integer can be both even and odd.

- *[This contradiction shows that the* ***supposition is false*** *and, hence, that the* ***proposition is true****.]*

- When you use proof by contraposition, you know exactly what conclusion you need to show, namely the negation of the hypothesis; whereas in proof by contradiction, it may be difficult to know what contradiction to head for.
- On the other hand, when you use proof by contradiction, once you have deduced any contradiction whatsoever, you are done.
- The main advantage of contraposition over contradiction is that you avoid having to take the negation of a complicated statement.

Relation between Proof by Contradiction and Proof by Contraposition

- The disadvantage of contraposition as compared with contradiction is that you can use contraposition only for a specific class of statements—those that are universal and conditional.
- The previous discussion shows that any statement that can be proved by contraposition can be proved by contradiction. But the converse is not true.

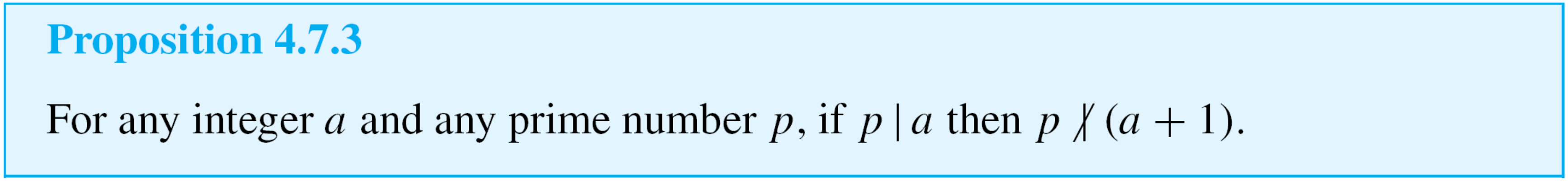
Are There Infinitely Many Prime Numbers?

You know that a prime number is a positive integer that cannot be factored as a product of two smaller positive integers.

Is the set of all such numbers infinite, or is there a largest prime number?

Are There Infinitely Many Prime Numbers?

Euclid’s proof requires one additional fact we have not yet established: If a prime number divides an integer, then it does not divide the next successive integer.



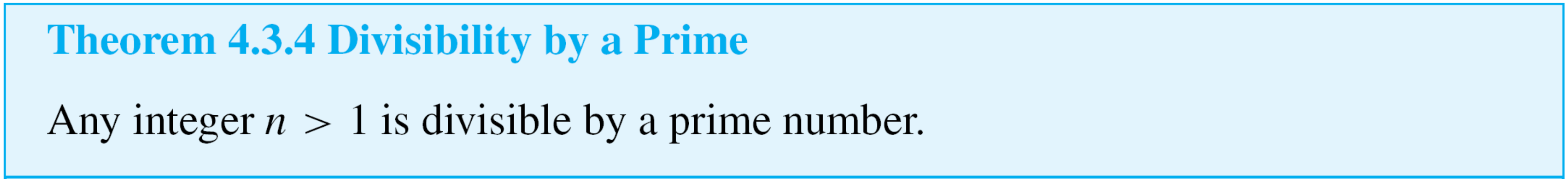
Proposition 4.7.3

For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a+1)$.

The idea of Euclid’s proof is this: Suppose the set of prime numbers were finite. Then you could take the product of all the prime numbers and add one.

Are There Infinitely Many Prime Numbers?

By Theorem 4.3.4 this number must be divisible by some prime number.



Theorem 4.3.4 Divisibility by a Prime

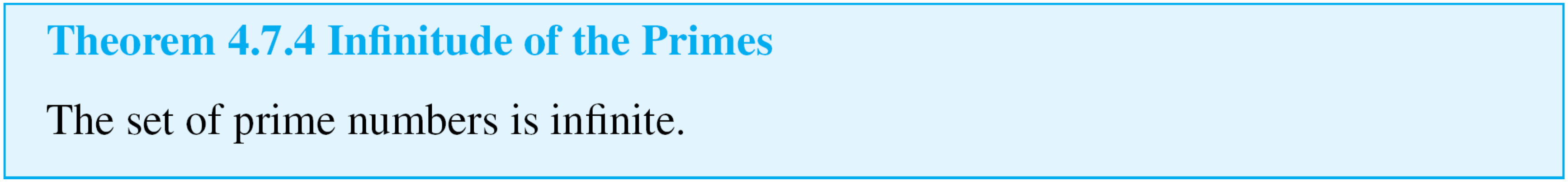
Any integer $n > 1$ is divisible by a prime number.

But by Proposition 4.7.3, this number is not divisible by any of the prime numbers in the set.

Are There Infinitely Many Prime Numbers?

Hence there must be a prime number that is not in the set of all prime numbers, which is impossible.

The following formal proof fills in the details of this outline.



Theorem 4.7.4 Infinitude of the Primes

The set of prime numbers is infinite.

Proof (by contradiction):

Suppose not. That is, suppose the set of prime numbers is finite. *[We must deduce a contradiction.]*

Are There Infinitely Many Prime Numbers?

Then some prime number *p* is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2,\ 3,\ 5,\ 7, 11, \ldots, p.$$

Let *N* be the product of all the prime numbers plus 1: $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$

Then *N* > 1, and so, by Theorem 4.3.4, *N* is divisible by some prime number *q*. Because *q* is prime, *q* must equal one of the prime numbers

$$2,\ 3,\ 5,\ 7, 11, \ldots, p.$$

Are There Infinitely Many Prime Numbers?

Thus, by definition of divisibility, *q* divides

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p,$$

and so, by Proposition 4.7.3, *q* does not divide

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1, \text{ which equals } N.$$

Hence, *N* is divisible by *q* and *N* is not divisible by *q*, and we have reached a contradiction. *[Therefore, the **supposition** is false and the **theorem** is true.]*

When to Use Indirect Proof

Many theorems can be proved either way. Usually, however, when both types of proof are possible, indirect proof is clumsier than direct proof.

In the absence of obvious clues suggesting indirect argument, try first to prove a statement directly. Then, if that does not succeed, look for a counterexample.

If the search for a counterexample is unsuccessful, look for a proof by contradiction or contraposition.