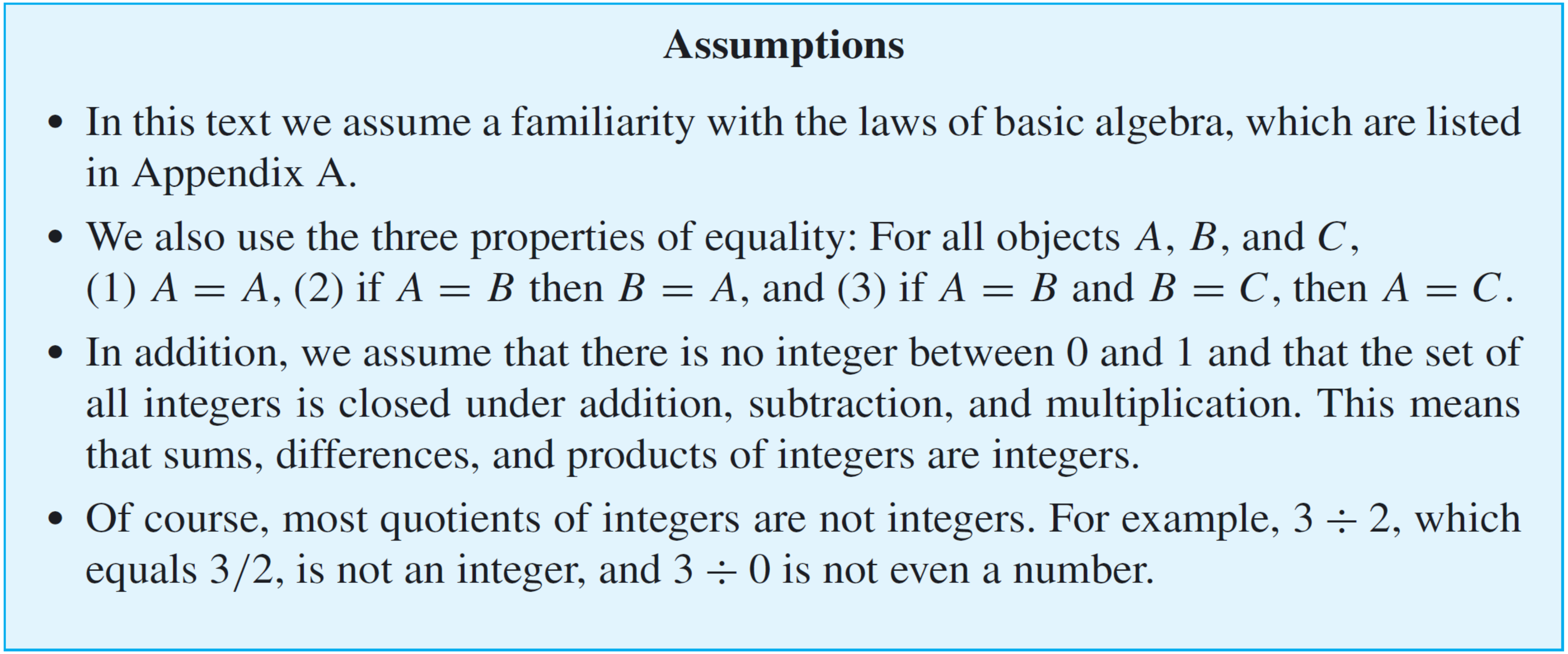
CMSC 207- Lecture 10
CHAPTER 4: Elementary Number Theory and Methods of Proof (4.1-4.4)

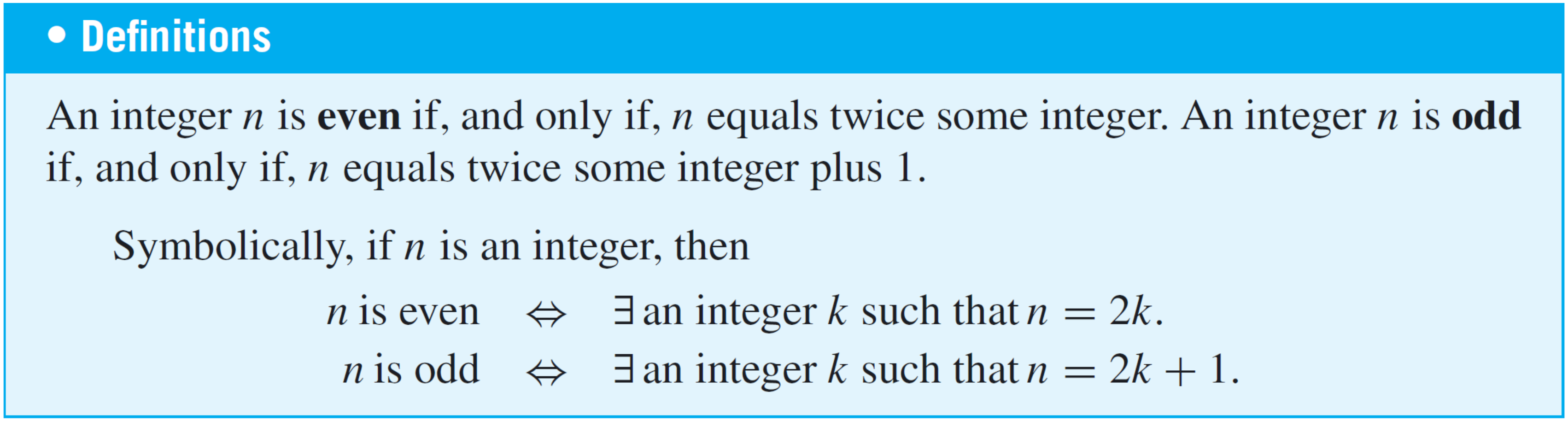
Dr. Ahmed Tarek

Direct Proof and Counterexample:



Assumptions

- In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A.
- We also use the three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$.
- In addition, we assume that there is no integer between 0 and 1 and that the set of all integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers.
- Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.



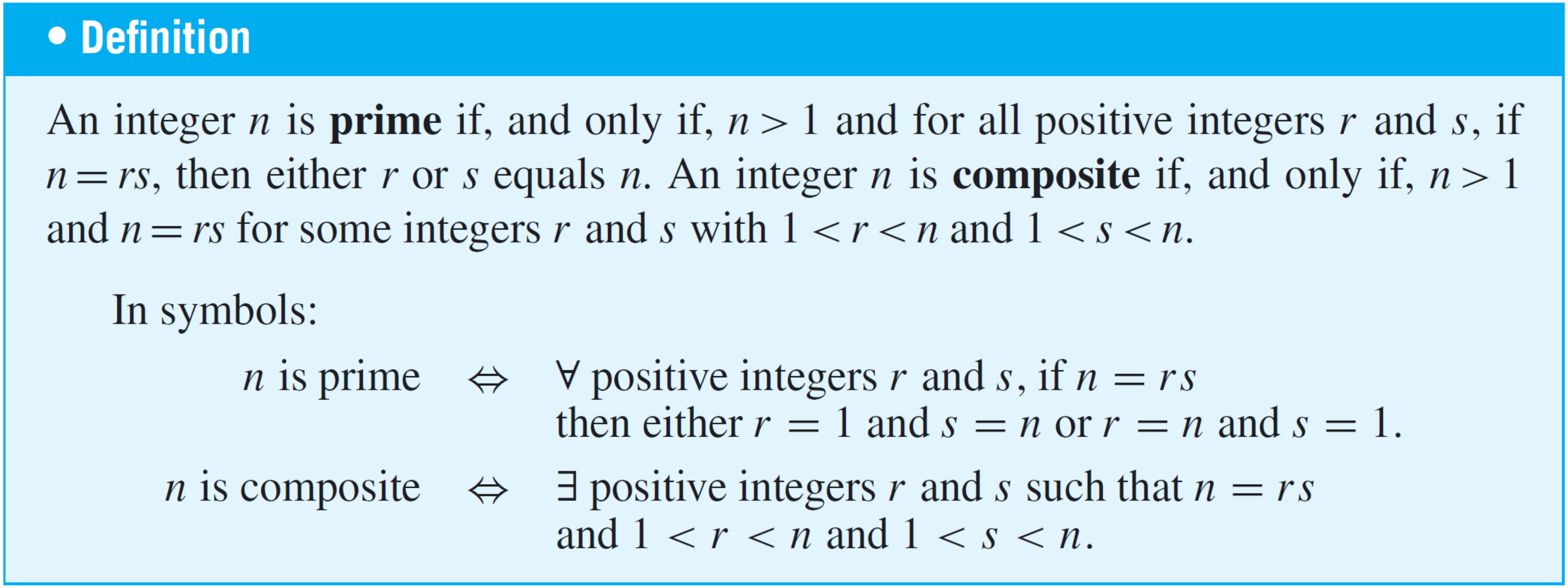
- **Definitions**

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$
\begin{aligned}
n \text{ is even} \quad &\Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k. \\
n \text{ is odd} \quad &\Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k + 1.
\end{aligned}
$$

Prime and Composite Integers



- **Definition**

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Example 2 – *Prime and Composite Numbers*

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

- Solution:

a. No. A prime number is required to be greater than 1.

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely $r = n$ and $s = 1$ and $r = 1$ and $s = n$.

Example 2 – *Solution*

- Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \leq r \leq n$ and $1 \leq s \leq n$. If n is prime, then the two displayed pairs are the only ways to write n as rs.

- Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

- **c**. 2, 3, 5, 7, 11, 13

- **d**. 4, 6, 8, 9, 10, 12

- **In-class Assignment 1**

Proving Existential Statements

- We have known that a statement in the form: $\exists x \in D$ such that $Q(x)$ is true if, and only if, $Q(x)$ is true for at least one x in D.
- One way to prove this is to find an x in D that makes $Q(x)$ true.
- Another way is to give a set of directions for finding such an x. Both of these methods are called **constructive proofs of existence**.

Example 3 – *Constructive Proofs of Existence*

- **a**. Prove the following: ∃ an even integer n that can be written in two ways as a sum of two prime numbers.
- **b**. Suppose that r and s are integers. Prove the following: ∃ an integer k such that $22r + 18s = 2k$.

- **Solution:**

- **a**. Let $n = 16$. Then $16 = 13 + 3 = 11 + 5$ and 3, 5, 11, and 13 are all prime numbers.

- **b**. Let $k = 11r + 9s$.

Example 3 – *Solution*

- Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.

Disproving Universal Statements by Counterexample

- To disprove a statement means to show that it is false. Consider the question of disproving a statement of the form

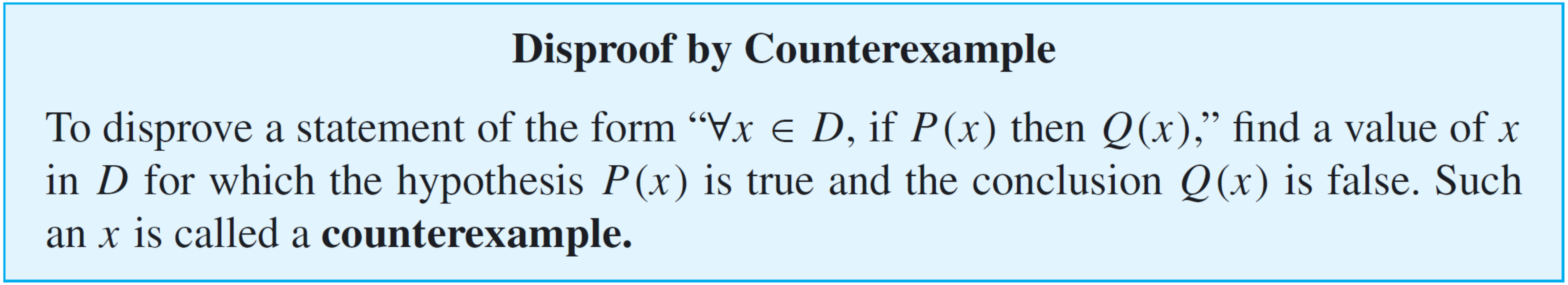
$\forall x$ in D, if $P(x)$ then $Q(x)$.

- Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$\exists x$ in D such that $P(x)$ and not $Q(x)$.

Disproving Universal Statements by Counterexample

- Now, to show that an existential statement is true, we generally give an example, and because the example is used to show that the original statement is false, we call it a ***counterexample***. Thus the method of disproof by *counterexample* can be written as follows:



Disproof by Counterexample

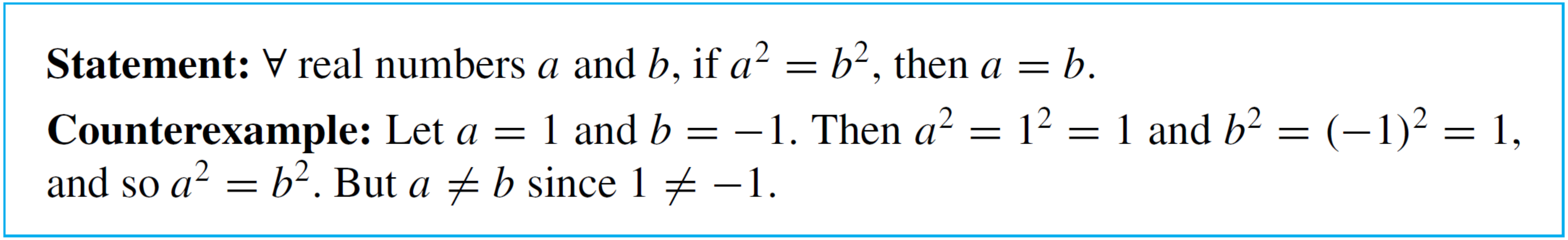
To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**

Example 4 – *Disproof by Counterexample*

- Disprove the following statement by finding a counterexample:
- ∀ real numbers a and b, if $a^2 = b^2$ then $a = b$.
- Solution:
- To disprove this statement, you need to find real numbers a and b such that the hypothesis $a^2 = b^2$ is true and the conclusion $a = b$ is false.
- The fact that both positive and negative integers have positive squares helps.

Example 4 – *Solution*

- If you flip through some possibilities in your mind, you will quickly see that 1 and –1 will work (or 2 and –2, or 0.5 and –0.5, and so forth).



Statement: $\forall$ real numbers a and b, if $a^2 = b^2$, then $a = b$.

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.

Proving Universal Statements

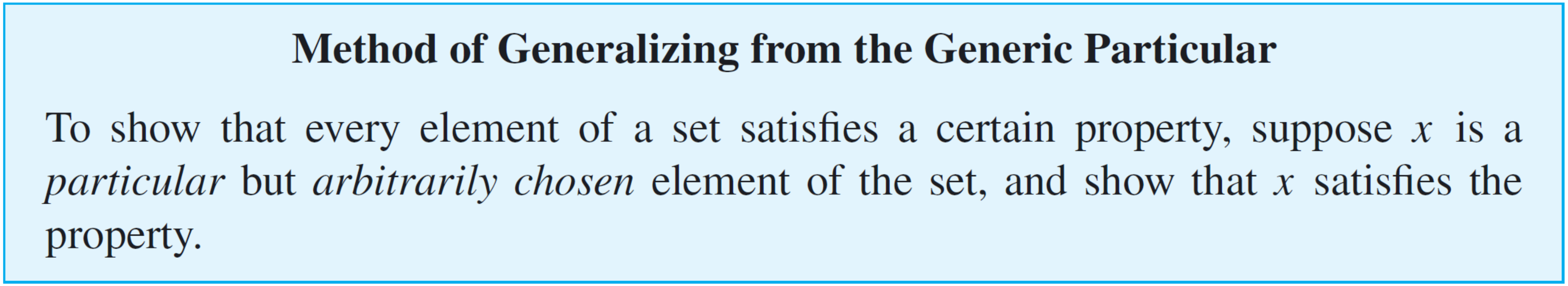
- The vast majority of mathematical statements to be proved are universal. In general, the standard form for such statements is: **$\forall x \in D$, if $P(x)$ then $Q(x)$.**
- When the domain *D* is finite or when only a finite number of elements need to be checked to satisfy *P*(*x*), such a statement can be proved by the method of exhaustion.

Practice Exercise – *The Method of Exhaustion*

- Use the method of exhaustion to prove the following statement:
- Every positive even integer less than 26 can be expressed as a sum of three or fewer perfect squares (for instance: $14 = 1 + 4 + 9 = 1^2 + 2^2 + 3^2$)

Proving Universal Statements

- The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified.
- It is called the *method of generalizing from the generic particular*. Here is the idea underlying the method:



Method of Generalizing from the Generic Particular

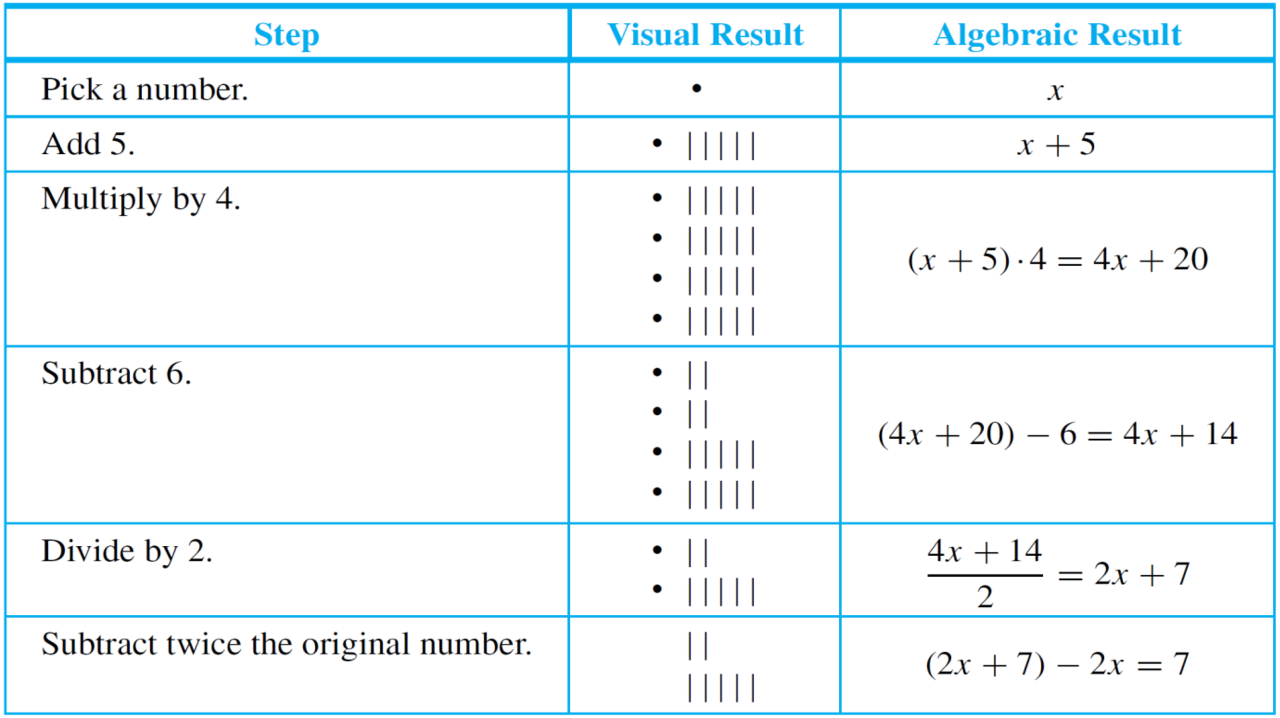
To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Example 6 – *Method of Generalizing from the Generic Particular*

- At some time you may have been shown a “mathematical trick” like the following.
- You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number.
- Then you surprise the person by announcing that the final result was 7. How does this “trick” work?

Example 6 – *Method of Generalizing from the Generic Particular*

- Let an empty box • or the symbol *x* stand for the number the person picks.
- Here is what happens when the person follows your directions:



Step	Visual Result	Algebraic Result
Pick a number.	•	x
Add 5.	• |||||	$x + 5$
Multiply by 4.	• ||||| • ||||| • ||||| • |||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	• || • || • ||||| • |||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	• || • |||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	|| |||||	$(2x + 7) - 2x = 7$

Example 6 – *Method of Generalizing from the Generic Particular*

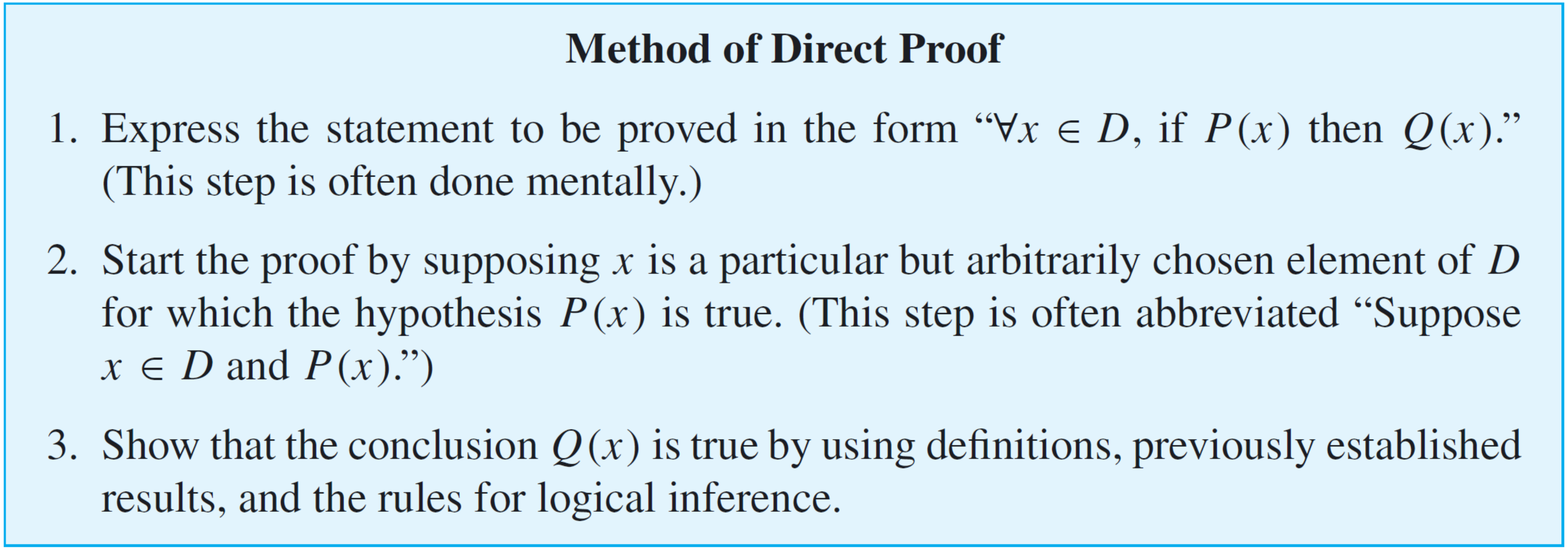
- Thus no matter what number the person starts with, the result will always be 7.
- The *x* in the analysis above is *particular* (because it represents a single quantity), but it is also *arbitrarily chosen* or *generic* (because any number whatsoever can be put in its place).
- This illustrates the process of drawing a general conclusion from a particular but generic object.

Proving Universal Statements

- When the method of generalizing from the generic particular is applied to a property of the form "**If *P*(*x*) then *Q*(*x*)**," the result is the method of *direct proof*.
- We have known that the only way an if-then statement can be false is for the hypothesis to be true and the conclusion to be false.
- Thus, given the statement "If *P*(*x*) then *Q*(*x*)," if one can show that the truth of *P*(*x*) compels the truth of *Q*(*x*), then the statement will be proved.

Proving Universal Statements

- To show that "**∀*x*, if *P*(*x*) then *Q*(*x*)**," is true for *all* elements *x* in a set *D*, you suppose *x* is a particular but arbitrarily chosen element of *D* that makes *P*(*x*) true, and then you show that *x* makes *Q*(*x*) true.



Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Showing That an Existential Statement Is False

- We have known that the negation of an existential statement is universal.
- It follows that to prove an existential statement is false, you must prove a universal statement (its negation) is true.

Example 9 – *Disproving an Existential Statement*

- Show that the following statement is false:

There is a positive integer *n* such that $n^2 + 3n + 2$ is prime.

- **Solution:**

- Proving that the given statement is false is equivalent to proving its negation is true.

- **The negation is:** For all positive integers *n*, $\boldsymbol{n^2 + 3n + 2}$ is not prime.

- Because the negation is universal, it is proved by the method of generalizing from the generic particular.

Example 9 – *Solution*

- **Claim:** The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

- **Proof:**

- Suppose n is any *particular but arbitrarily chosen* positive integer. *It is required to show that* $n^2 + 3n + 2$ *is not prime*.

We can factor $n^2 + 3n + 2$ to obtain $n^2 + 3n + 2$

$= (n + 1)(n + 2)$. Also, $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$).Thus $n^2 + 3n + 2$ is a product of two positive integers each greater than 1, and smaller than $n^2 + 3n + 2$. So, according to the definition of composite integers, $n^2 + 3n + 2$ is not prime, and is composite.

Example – *Deriving Results about Even and Odd Integers*

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.

2. The sum and difference of any two odd integers are even.

3. The product of any two odd integers is odd.

4. The product of any even integer and any odd integer is even.

Example – *Deriving Results about Even and Odd Integers*

5. The sum of any odd integer and any even integer is odd.

6. The difference of any odd integer minus any even integer is odd.

7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if *a* is any even integer and *b* is any odd integer, then $\frac{a^2+b^2+1}{2}$ is an integer.

Example – *Solution*

Suppose *a* is any even integer and *b* is any odd integer. So, b^2 is odd, and a^2 is even.

Then $a^2 + b^2$ is odd, and because 1 is also odd, the sum is even. $(a^2 + b^2) + 1 = a^2 + b^2 + 1$

Hence, by definition of even, there exists an integer *k* such that $a^2 + b^2 + 1 = 2k.$

Dividing both sides by 2 gives $\frac{a^2+b^2+1}{2} = k$, which is an integer.

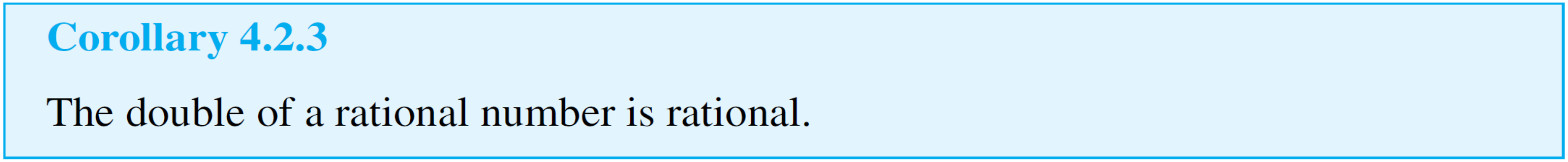
Thus $\frac{a^2+b^2+1}{2}$ is an integer.

Proof Structure in Computer Science

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example – *The Double of a Rational Number*

Derive the following as a corollary of Theorem: **the sum of any two rational numbers is rational**



Corollary 4.2.3

The double of a rational number is rational.

Proof:

Suppose *r* is any rational number. Then 2*r* = *r* + *r* is a sum of two rational numbers.

So, by the Theorem discussed, 2*r* is rational. **Q.E.D.**

Proving Properties of Divisibility

One of the most useful properties of divisibility is that it is transitive. If one number divides a second, and the second number divides a third, then the first number divides the third.

Example – *Solution*

Prove that for all **integers** a, b, and c, if $\boldsymbol{a \mid b}$ and $\boldsymbol{b \mid c}$, then $\boldsymbol{a \mid c}$.

Solution:

Suppose a, b, and c are particular but arbitrarily chosen integers such that $a \mid b$ and $b \mid c$.

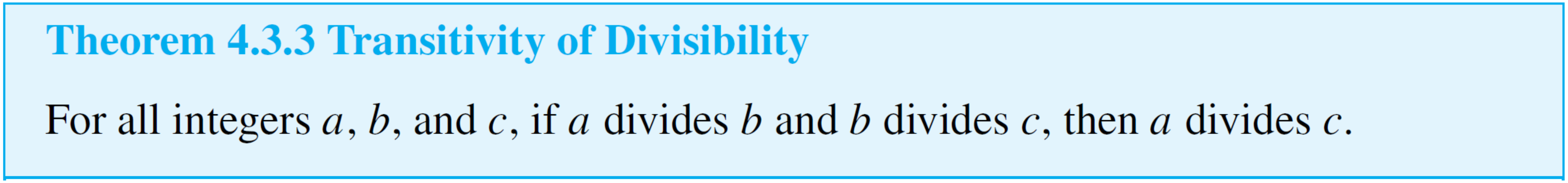
To Show: $a \mid c$. Show $c = a \cdot (\text{some integer})$.

But since $a \mid b$, $b = ar$ for some integer r. 4.3.1

And since $b \mid c$, $c = bs$ for some integer s. 4.3.2

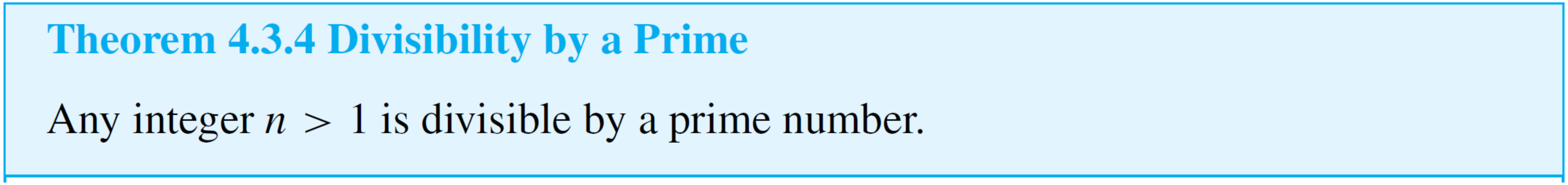
Now, $c = bs = (ar)s = a \times rs = a(rs)$. Now, $a \times rs$ is a product of two integers, and is an integer. Also, **rs** is an integer. So, $a \mid c$. **Q.E.D.**

Proving Properties of Divisibility



Theorem 4.3.3 Transitivity of Divisibility

For all integers a, b, and c, if a divides b and b divides c, then a divides c.



Theorem 4.3.4 Divisibility by a Prime

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

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

Example – *Checking a Proposed Divisibility Property*

Is the following statement true or false? For all integers *a* and *b*, if ***a* | *b*** and ***b* | *a*** then ***a* = *b***.

Solution:

This statement is false. Counterexample: **2 | -2 and -2 | 2, but 2 ≠ -2.** By definition of divisibility, the conditions *a* | *b* and *b* | *a* mean that $b = ka$ and $a = lb$ for some integers k and l.

The equations imply that: $b = ka = k(lb) = (kl)b.$

Since ***b* | *a***, ***b* ≠ 0**, and so one can cancel ***b*** from the extreme left and right sides to obtain: $1 = kl.$

So, either k = l = 1 or, k = l = -1. If k = l = 1, then a = b.

If k = l = -1, b = -a, and **a ≠ b**. **Q.E.D.**

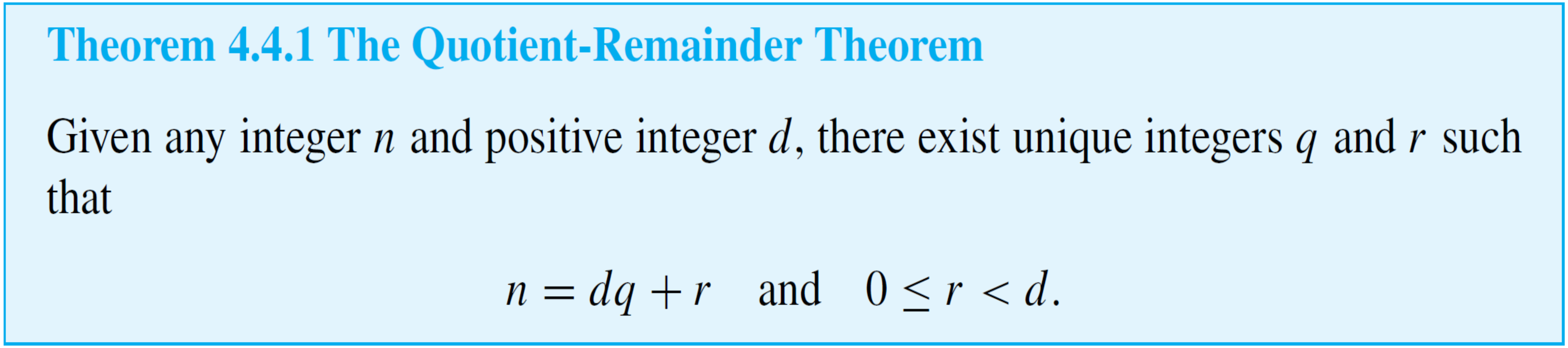
In-class Assignment #4:

Practice Exercise

Prove that the product of any two odd integers is odd.

The Quotient-Remainder Theorem

- The quotient-remainder theorem says that when any integer *n* is divided by any positive integer *d*, the result is a quotient *q*, and a nonnegative remainder *r* that is smaller than *d*.



Theorem 4.4.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Example – *The Quotient-Remainder Theorem*

- For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \le r < d$.

a. *n* = 54, *d* = 4 **b.** *n* = –54, *d* = 4 **c.** *n* = 54, *d* = 70

- **Solution:**

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$.

Representations of Integers

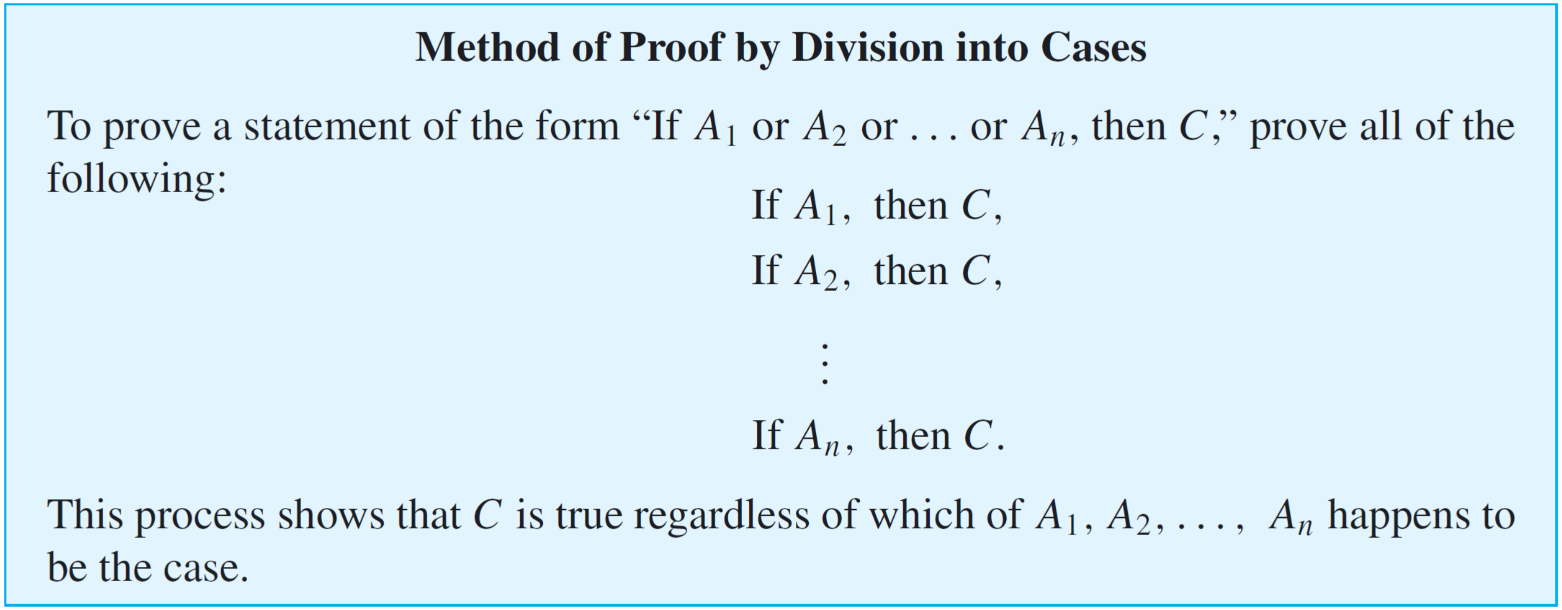
- There are times when division into more than two cases is called for. Suppose that at some stage of developing a proof, you know that a statement of the form $A_1 \text{ or } A_2 \text{ or } A_3 \text{ or} \ldots \text{or } A_n$

is true, and suppose you want to deduce a conclusion *C*.
By definition of *or*, you know that at least one of the statements A_i is true (although you may not know which).

- In this situation, you should use the method of division into cases.

Representations of Integers

- First assume A_1 is true and deduce C; next assume A_2 is true and deduce C; and so forth until you have assumed A_n is true and deduced C.
- At that point, you can conclude that regardless of which statement A_i happens to be true, the truth of C follows.



Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or . . . or A_n, then C," prove all of the following:

$$\begin{gathered}\text{If } A_1, \text{ then } C,\\ \text{If } A_2, \text{ then } C,\\ \vdots\\ \text{If } A_n, \text{ then } C.\end{gathered}$$

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Example – *Representations of Integers Modulo 4*

- Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer *q*.

- Solution:

Given any integer *n*, apply the quotient-remainder theorem to *n* with *d* = 4.

- This implies that there exist an integer quotient *q* and a remainder *r* such that

$$n = 4q + r \quad \text{and} \quad 0 \le r < 4.$$

Example – *Solution*

- But the only nonnegative remainders *r* that are less than 4 are 0, 1, 2, and 3.

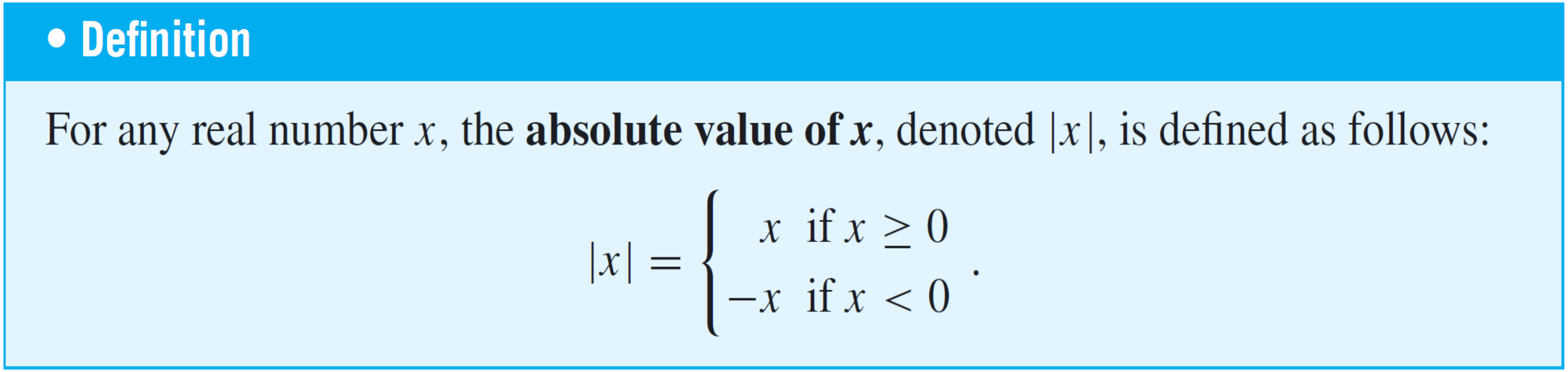
- Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer *q*.

Absolute Value and the Triangle Inequality

- The triangle inequality is one of the most important results involving absolute value. It has applications in many areas of mathematics.



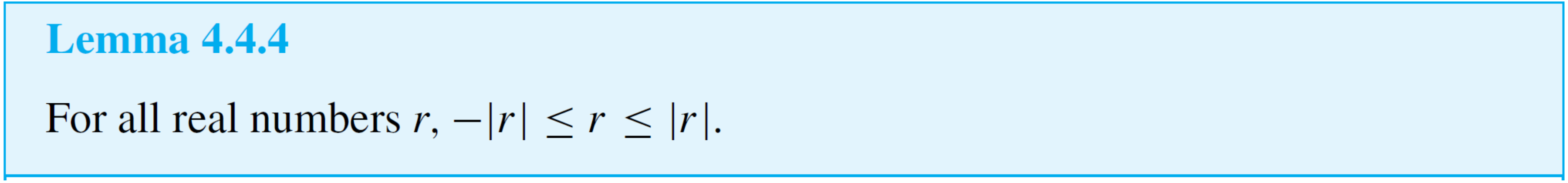
• **Definition**

For any real number x, the **absolute value of *x***, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

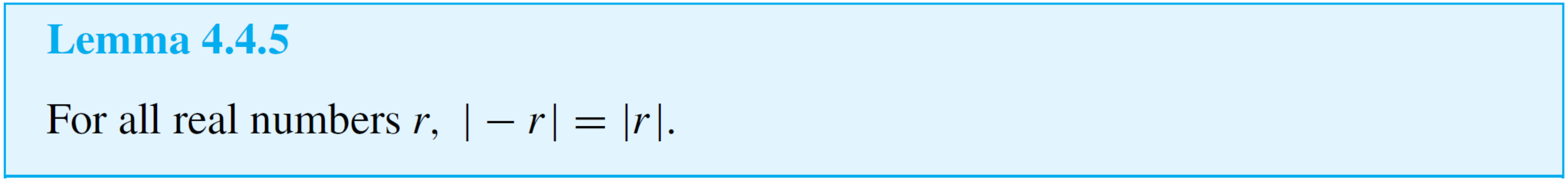
Absolute Value and the Triangle Inequality

- A **lemma** is a statement with preliminary result that is useful in deriving more important results such as a theorem or a proposition.



Lemma 4.4.4

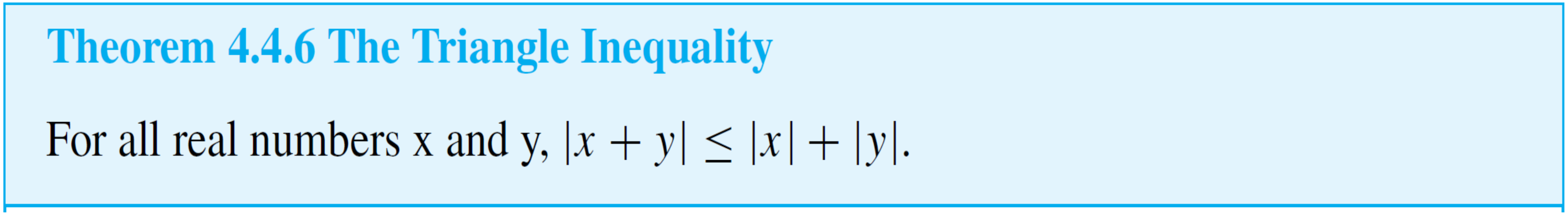
For all real numbers r, $-|r| \leq r \leq |r|$.



Lemma 4.4.5

For all real numbers r, $|-r| = |r|$.

- Lemmas 4.4.4 and 4.4.5 now provide a basis for proving the triangle inequality.



Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x+y| \leq |x| + |y|$.

The Final Picture

- Lemma/Lemmas help you in deriving a Theorem (**Slide 41**)
- From a Theorem, you can derive Corollaries and prove Corollaries using the parent Theorem (**Slide 28**)