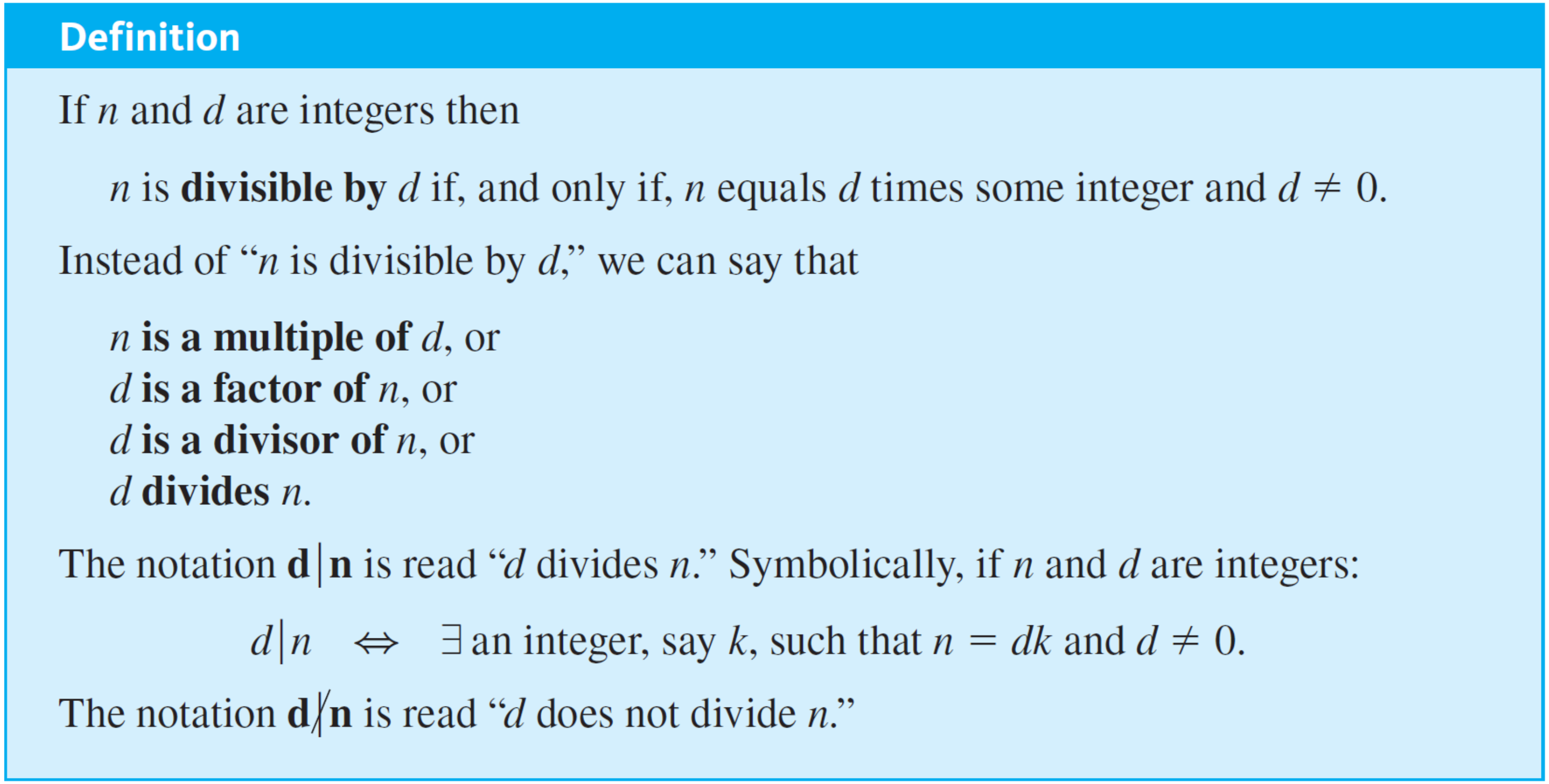
CHAPTER 4

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

4.4 Direct Proof and Counterexample IV: Divisibility

Direct Proof and Counterexample IV: Divisibility

The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory**, the study of properties of integers.



Definition

If n and d are integers then

n is **divisible by** d if, and only if, n equals d times some integer and $d \neq 0$.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer, say } k\text{, such that } n = dk \text{ and } d \neq 0.$$

The notation $\mathbf{d \nmid n}$ is read "d does not divide n."

Example 4.4.1 – *Divisibility*

a. Is 21 divisible by 3?

b. Does 5 divide 40?

c. Does $7 \mid 42$?

d. Is 32 a multiple of −16?

e. Is 6 a factor of 54?

f. Is 7 a factor of −7?

Example 4.4.1 – *Solution*

a. Yes, $21 = 3 \cdot 7$.

b. Yes, $40 = 5 \cdot 8$.

c. Yes, $42 = 7 \cdot 6$.

d. Yes, $32 = (-16) \cdot (-2)$.

e. Yes, $54 = 6 \cdot 9$.

f. Yes, $-7 = 7 \cdot (-1)$.

Example 4.4.2 – *Divisors of Zero*

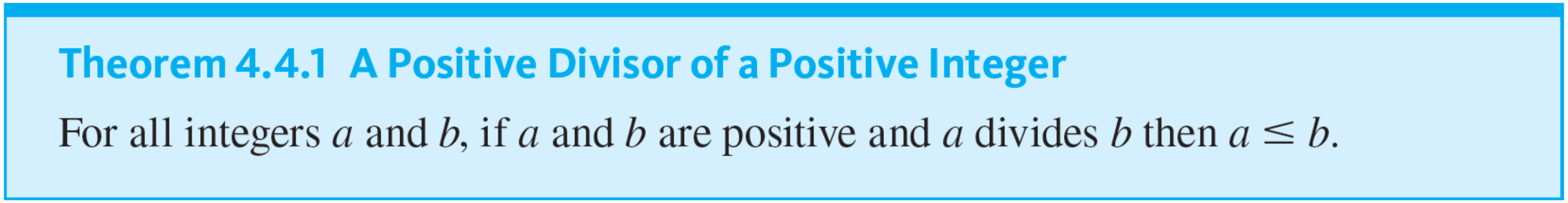
If *k* is any nonzero integer, does *k* divide 0?

Example 4.4.2 – *Solution*

Yes, because $0 = k \cdot 0$.

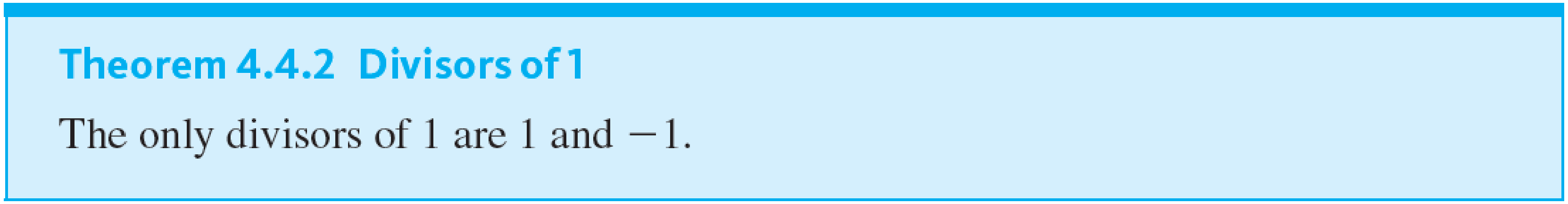
Direct Proof and Counterexample IV: Divisibility

Two useful properties of divisibility are (1) that if one positive integer divides a second positive integer, then the first is less than or equal to the second, and (2) that the only divisors of 1 are 1 and −1.



Theorem 4.4.1 A Positive Divisor of a Positive Integer

For all integers a and b, if a and b are positive and a divides b then $a \leq b$.



Theorem 4.4.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Example 4.4.3 – *Divisibility and Algebraic Expressions*

a. If *a* and *b* are integers, is 3*a* + 3*b* divisible by 3?

b. If *k* and *m* are integers, is 10*km* divisible by 5?

Example 4.4.3 – *Solution*

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers.

Direct Proof and Counterexample IV: Divisibility

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk \text{ and } d \neq 0.$$

Since the negation of an existential statement is universal, it follows that *d* does not divide *n* (denoted $d \nmid n$) if, and only if, ∀ integer *k*, $n \neq dk$ or $d = 0$; in other words, the quotient n/d is not an integer.

$$\text{For all integers } n \text{ and } d, \quad d \nmid n \quad \Leftrightarrow \quad \frac{n}{d} \text{ is not an integer.}$$

Example 4.4.4 – *Checking Nondivisibility*

Does $4 \mid 15$?

Example 4.4.4 – *Solution*

No, $\frac{15}{4} = 3.75,$ which is not an integer.

Example 4.4.5 – *Prime Numbers and Divisibility*

An alternative way to define a prime number is to say that an integer $n > 1$ is prime if, and only if, its only positive integer divisors are 1 and itself.

Proving Properties of Divisibility

Example 4.4.6 – *Transitivity of Divisibility*

Prove that for all integers *a*, *b*, and *c*, if $a|b$ and $b|c$, then $a|c$.

Example 4.4.6 – *Solution*

Since the statement to be proved is already written formally, you can immediately pick out the starting point, or first sentence of the proof, and the conclusion that must be shown.

Starting Point: Suppose *a*, *b*, and *c* are particular but arbitrarily chosen integers such that $a|b$ and $b|c.$

To Show: $a|c.$

You need to show that $a|c,$ or, in other words, that

$$c = a \cdot \text{(some integer)}.$$

Example 4.4.6 – *Solution*

continued

But since $a|b$,

$b = ar$ for some integer r. 4.4.1

And since $b|c$,

$c = bs$ for some integer s. 4.4.2

Equation 4.4.2 expresses *c* in terms of *b*, and equation 4.4.1 expresses *b* in terms of *a*. Thus, if you substitute 4.4.1 into 4.4.2, you will have an equation that expresses *c* in terms of *a*.

Example 4.4.6 – *Solution*

continued

$$c = bs \qquad \text{by equation 4.4.2}$$

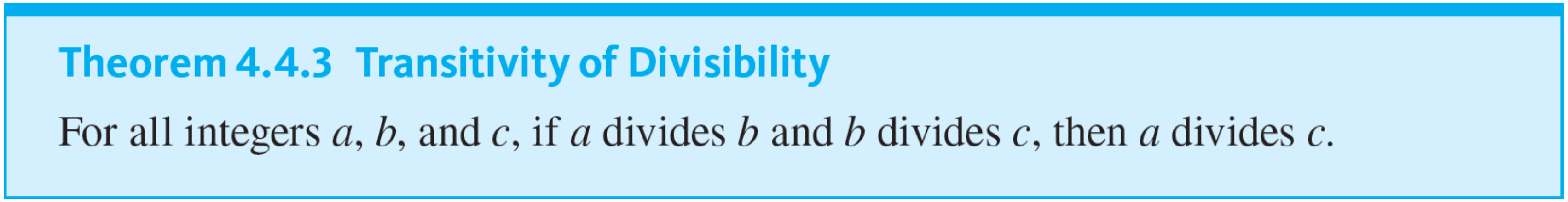
$$= (ar)s \qquad \text{by equation 4.4.1.}$$

But $(ar)s = a(rs)$ by the associative law for multiplication. Hence

$$c = a(rs).$$

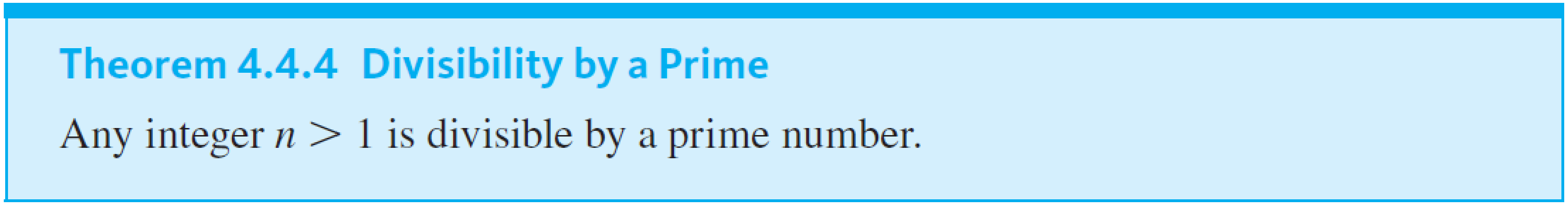
Now you are almost finished. You have expressed c as $a \cdot$ (something). It remains only to verify that that something is an integer. But of course it is, because it is a product of two integers.

Proving Properties of Divisibility



Theorem 4.4.3 Transitivity of Divisibility

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



Theorem 4.4.4 Divisibility by a Prime

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

Counterexamples and Divisibility

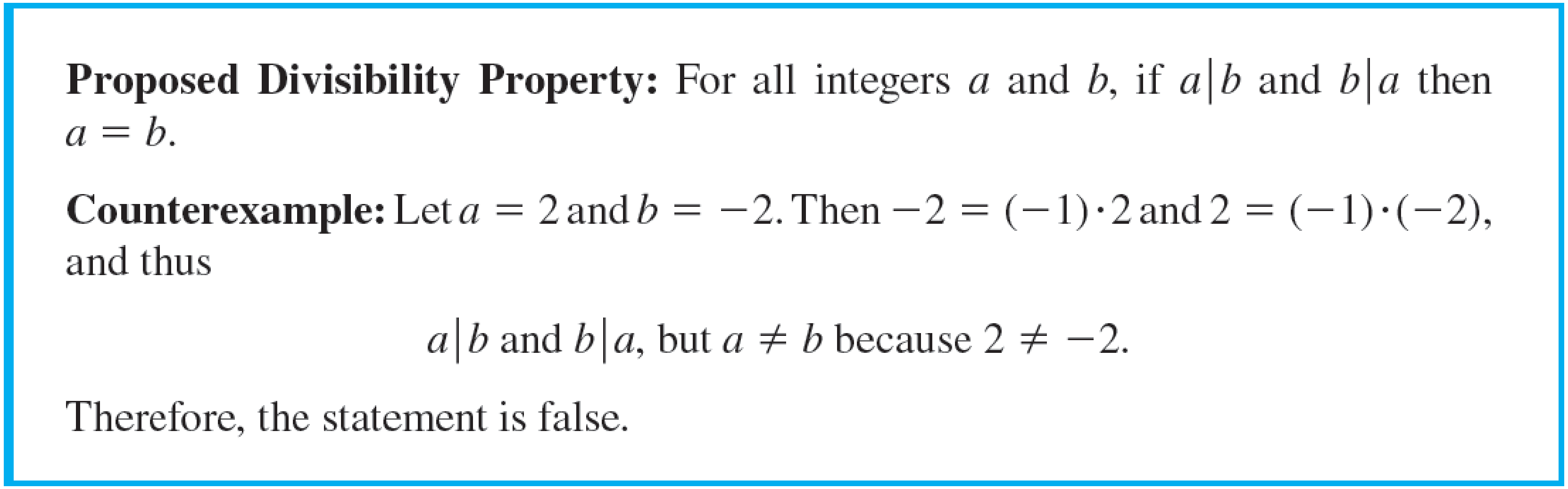
Example 4.4.7 – *Checking a Proposed Divisibility Property*

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

Example 4.4.7 – *Solution*

continued

This statement is false.



Proposed Divisibility Property: For all integers a and b, if $a | b$ and $b | a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then $-2 = (-1) \cdot 2$ and $2 = (-1) \cdot (-2)$, and thus

$$a | b \text{ and } b | a, \text{ but } a \neq b \text{ because } 2 \neq -2.$$

Therefore, the statement is false.

The Unique Factorization of Integers Theorem

The Unique Factorization of Integers Theorem

The most comprehensive statement about divisibility of integers is contained in the *unique factorization of integers theorem*.

Because of its importance, this theorem is also called the *fundamental theorem of arithmetic*.

The unique factorization of integers theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written.

The Unique Factorization of Integers Theorem

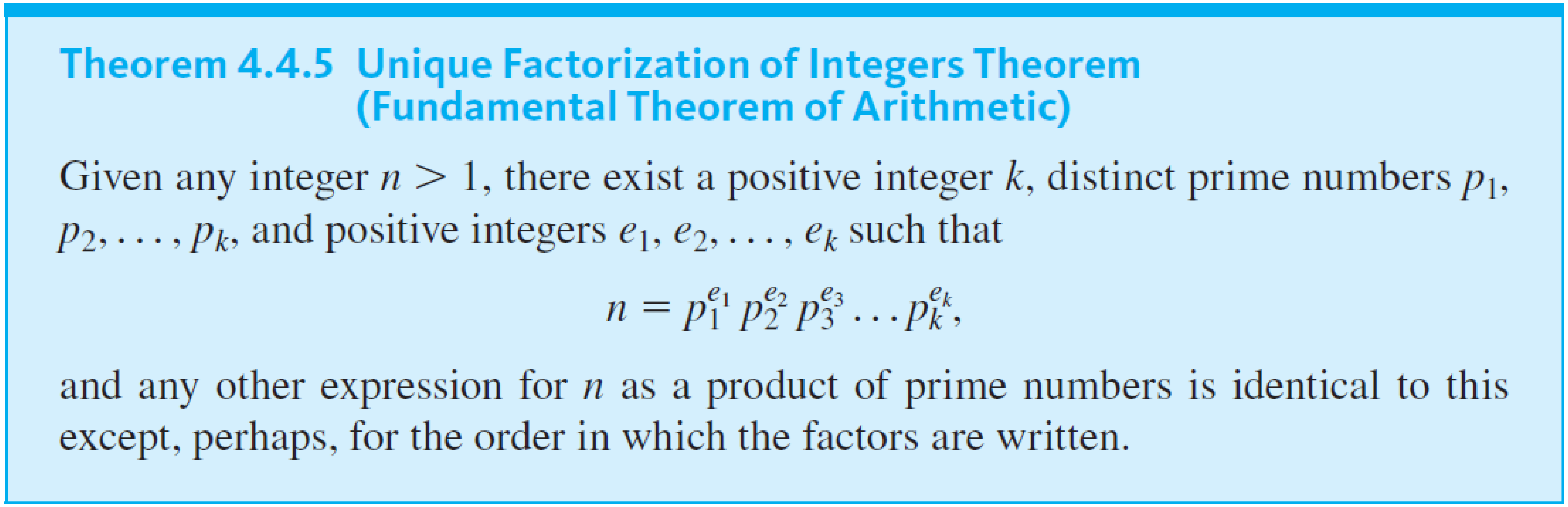
For example,

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2,$$

and so forth.

The three 2’s and two 3’s may be written in any order, but any factorization of 72 as a product of primes must contain exactly three 2’s and two 3’s—no other collection of prime numbers besides three 2’s and two 3’s multiplies out to 72.

The Unique Factorization of Integers Theorem



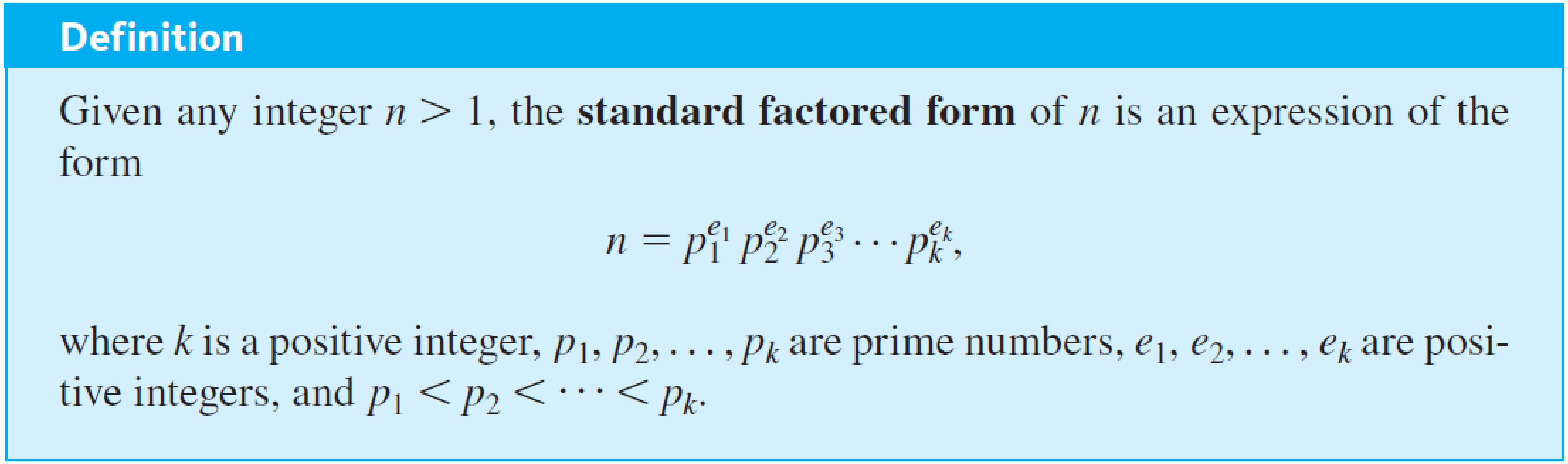
Theorem 4.4.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers p_1, $p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

The Unique Factorization of Integers Theorem



Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer, $p_1, p_2, \ldots, p_k$ are prime numbers, $e_1, e_2, \ldots, e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$.

Example 4.4.8 – *Writing Integers in Standard Factored Form*

Write 3,300 in standard factored form.

Example 4.4.8 – *Solution*

First find all the factors of 3,300. Then write them in ascending order:

$$3{,}300 = 100 \cdot 33 = 4 \cdot 25 \cdot 3 \cdot 11$$

$$= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1.$$

Example 4.4.9 – *Using Unique Factorization to Solve a Problem*

Suppose *m* is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does $17 | m$?

Example 4.4.9 – *Solution*

Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).

But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large).

Hence 17 must occur as one of the prime factors of *m*, and so $17 | m.$