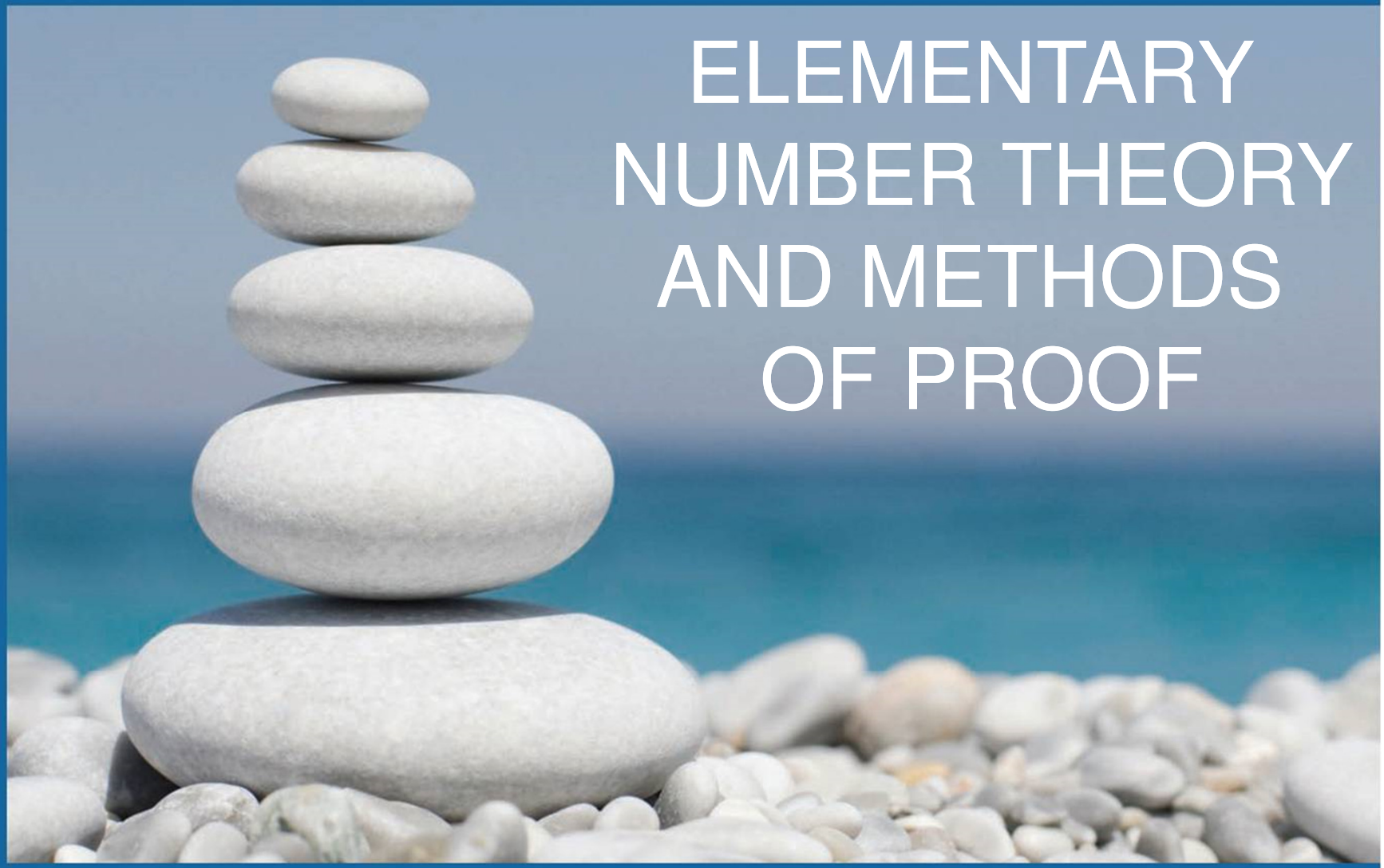
CHAPTER 4



ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

SECTION 4.3

Direct Proof and Counterexample III: Divisibility

Direct Proof and Counterexample III: 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 and $d \neq 0$ then

n is **divisible by** d if, and only if, n equals d times some integer.

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 and $d \neq 0$:

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

Example 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 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, $-7 = 7 \cdot (-1)$.

Direct Proof and Counterexample III: 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 4.3.1 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 4.3.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Example 1 – *Divisibility of Algebraic Expressions*

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

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

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 III: Divisibility

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

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

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, ∀ integers *k*, $n \neq dk$, or, in other words, the quotient *n*/*d* is not an integer.

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

Example 4 – *Checking Nondivisibility*

Does 4 | 15?

Solution:

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

Proving Properties of Divisibility

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 6 – *Transitivity of Divisibility*

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

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 $a \mid b$ and $b \mid c$.

Example 6 – *Solution*

cont'd

To Show: $a \mid c$.

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

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

But since $a \mid b$,

$$b = ar \quad \text{for some integer } r. \tag{4.3.1}$$

And since $b \mid c$,

$$c = bs \quad \text{for some integer } s. \tag{4.3.2}$$

Equation 4.3.2 expresses c in terms of b, and equation 4.3.1 expresses b in terms of a.

Example 6 – *Solution*

cont'd

Thus if you substitute 4.3.1 into 4.3.2, you will have an equation that expresses *c* in terms of *a*.

$$c = bs \qquad \text{by equation 4.3.2}$$

$$= (ar)s \qquad \text{by equation 4.3.1.}$$

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

$$c = a(rs).$$

Now you are almost finished.

Example 6 – *Solution*

cont'd

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.

This discussion is summarized as follows:

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.

Example 6 – *Solution*

cont'd

Proof:

Suppose *a*, *b*, and *c* are *[particular but arbitrarily chosen]* integers such that *a* divides *b* and *b* divides *c*. *[We must show that a divides c.]* By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \qquad \text{by basic algebra.} \end{aligned}$$

Example 6 – *Solution*

cont'd

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus a divides c by definition of divisibility. *[This is what was to be shown.]*

Proving Properties of Divisibility

Theorem 4.3.4 Divisibility by a Prime

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

Counterexamples and Divisibility

Counterexamples and Divisibility

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 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 $a = b$.

Solution:

This statement is false. Can you think of a counterexample just by concentrating for a minute or so?

The following discussion describes a mental process that may take just a few seconds. It is helpful to be able to use it consciously, however, to solve more difficult problems.

Example 7 – *Solution*

cont'd

To discover the truth or falsity of the given statement, start off much as you would if you were trying to prove it.

Starting Point: Suppose a and b are integers such that $a \mid b$ and $b \mid a$.

Ask yourself, "Must it follow that $a = b$, or could it happen that $a \neq b$ for some a and b?" Focus on the supposition. What does it mean? By definition of divisibility, the conditions $a \mid b$ and $b \mid a$ mean that

$$b = ka \quad \text{and} \quad a = lb \quad \text{for some integers } k \text{ and } l.$$

Example 7 – *Solution*

cont'd

Must it follow that $a = b$, or can you find integers a and b that satisfy these equations for which $a \neq b$? The equations imply that

$$b = ka = k(lb) = (kl)b.$$

Since $b \mid a$, $b \neq 0$, and so you can cancel b from the extreme left and right sides to obtain

$$1 = kl.$$

In other words, k and l are divisors of 1. But, by Theorem 4.3.2, the only divisors of 1 are 1 and –1. Thus k and l are both 1 or are both –1. If $k = l = 1$, then $b = a$.

Example 7 – *Solution*

cont'd

But if $k = l = -1$, then $b = -a$ and so $a \neq b$.

This analysis suggests that you can find a counterexample by taking $b = -a$.

Here is a formal answer:

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

Counterexample: Let $a = 2$ and $b = -2$. Then

$$a \mid b \text{ since } 2 \mid (-2) \text{ and } b \mid a \text{ since } (-2) \mid 2, \text{ but } a \neq b \text{ since } 2 \neq -2.$$

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

Theorem 4.3.5 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

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

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

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

• 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 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 $17 \mid m$?

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 $17 \mid m$.