Solution. We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.
Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.
Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n.n \geq n.1$. This implies that $n^2 \geq n$ for $n \geq 1$.
Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$. ∎

Example 2.18. Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution. Exercise ∎

Example 2.19. Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.

Solution. Exercise ∎

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a **uniqueness proof** are:

Existence: We show that an element x with the desired property exists.
Uniqueness: We show that if x and y both have the desired property, then $x = y$.

Example 2.20. Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution. First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because

$$a(-b/a) + b = -b + b = 0$$

Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides, we find that $ar = as$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$. This establishes the uniqueness part of the proof. ∎

2.1 Prime and Composite Numbers

Definition 20: Prime and Composite Numbers

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: For each integer n with $n > 1$,

$$\begin{aligned} n \text{ is prime } &\leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \\ &\quad \text{then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1. \\ n \text{ is composite } &\leftrightarrow \exists \text{ positive integers } r \text{ and } s, \text{ such that } n = rs \\ &\quad \text{and } 1 < r < n \text{ and } 1 < s < n. \end{aligned}$$

Example 2.21. 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.

Proving Existential Statements

Example 2.22. Prove that there exists an even integer n that can be written in two ways as a sum of two prime numbers

Example 2.23. Suppose that r and s are integers. Prove that there exists an integer k such that $22r+18s = 2k$.

Example 2.24. Show that the following statement is false:

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

Solution. Exercise! ∎

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Theorem 2.3. *Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.*

Example 2.25. Obtain the prime factorizations of 100, 641, 999, and 1024

Solution. The prime factorizations of 100, 641, 999, and 1024 are given by
$100 = 2.2.5.5 = 2^2.5^2$,
$641 = 641$,
$999 = 3.3.3.37 = 3^3.37$,
$1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$. ∎

Theorem 2.4. *If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.*

Example 2.26. Show that 101 is prime.

Solution. The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime. ∎

Example 2.27. Find the prime factorization of 7007.

Solution. To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7. It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ∎

2.2 Divisibility

When one integer is divided by a second nonzero integer, the quotient may or may not be an integer. For example, $12/3 = 4$ is an integer, whereas $11/4 = 2.75$ is not.

Definition 21: Divisibility

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 $d|n$ is read "d divides n." Symbolically, if n and d are integers:

$$d|n \leftrightarrow \exists \text{ an integer, say } k, \text{ such that } n = dk \text{ and } d \neq 0.$$
$$\text{For all integers } n \text{ and } d,\ d|n \leftrightarrow \tfrac{n}{d} \text{ is not an integer.}$$

Example 2.28. Determine whether $3|7$ and whether $3|12$.

Solution. Exercise

Theorem 2.5. *For all integers a and b, if a and b are positive and a divides b then $a \leq b$.*

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.

Theorem 2.6. *Let a, b, and c be integers, where $a \neq 0$. Then*

i if $a|b$ and $a|c$, then $a|(b+c)$;

ii if $a|b$, then $a|bc$ for all integers c;

iii if $a|b$ and $b|c$ then $a|c$;

Example 2.29. Is the following statement true or false? For all integers a and b, if $a|b$ and $b|a$ then $a = b$.

Corollary

If a, b, and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers.

The Division Algorithm

Theorem 2.7. *Given any integer n and positive integer d, there exist unique integers q and r such that*

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

Definition 22

In the equality given in the division algorithm, d is called the ***divisor***, a is called the ***dividend***, q is called the ***quotient***, and r is called the ***remainder***.

Example 2.30. For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$

a $n = 54, d = 4$

b $n = -54, d = 4$

c $n = 54, d = 70$

Example 2.31. What are the quotient and remainder when 101 is divided by 11?

Solution. Exercise

2.3 Modular Arithmetic

Definition 23

Given an integer n and a positive integer d, if n and d are integers and $d > 0$, then

$$n \text{ div } d = q \text{ and } n \text{ mod } d = r \leftrightarrow n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

Example 2.32. Compute 32 div 9 and 32 mod 9 by hand or with a four-function calculator.

Because we are often interested only in remainders, we have special notations for them. We have already introduced the notation a **mod** m to represent the remainder when an integer a is divided by the positive integer m. We now introduce a different, but related, notation that indicates that two integers have the same remainder when they are divided by the positive integer m.

Definition 24

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation $a \equiv b(\text{ mod } m)$ to indicate that a is congruent to b modulo m. We say that $a \equiv b(\text{mod} m)$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b(\text{mod} m)$.

Although both notations $a \equiv b(\text{mod} m)$ and a **mod** $m = b$ include "mod," they represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function.

Theorem 2.8. *Let a and b be integers, and let m be a positive integer.*

$$\text{Then } a \equiv b(\text{ mod } m) \text{ if and only if } a \text{ mod } m = b \text{ mod } m.$$

Recall that a **mod** m and b **mod** m are the remainders when a and b are divided by m, respectively. Consequently, *Theorem 2.8* also says that $a \equiv b(\text{ mod } m)$ if and only if a and b have the same remainder when divided by m.

Example 2.33. Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution. Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5(\text{ mod } 6)$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14(textmod6)$.

Theorem 2.9. *Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.*

Proof: Suppose $a \equiv b(\bmod m)$, then by the definition of congruence

$$m|(a-b)$$

$$\implies a-b = km \text{ for some integer } k$$

$$\text{so that } a = b + km$$

Conversely, suppose there is an integer k such that

$$a = b + km$$

$$\text{then } km = a - b$$

Hence, m divides $a-b$, so that $a \equiv b(\bmod m)$. □

Theorem 2.10. *Let m be a positive integer. If $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then*

$$a + c \equiv b + d(\bmod m) \text{ and } ac \equiv bd(\bmod m).$$

Proof: We use a direct proof. Because $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$,

$$b = a + sm \text{ and } d = c + tm \text{ for integers } s \text{ and } t$$

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$$

Hence,

$$a + c \equiv b + d(\bmod m) \text{ and } ac \equiv bd(\bmod m)$$

□

Example 2.34. Because $7 \equiv 2(\bmod 5)$ and $11 \equiv 1(\bmod 5)$, it follows from *Theorem 2.9* that

$$18 = 7 + 11 \equiv 2 + 1 = 3(\bmod 5)$$

and that

$$77 = 7.11 \equiv 2.1 = 2(\bmod 5).$$

Corollary 2.11. *Let m be a positive integer and let a and b be integers. Then*

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Example 2.35. Find the value of $(19^3 \bmod 31)^4 \bmod 23$.

Solution. To compute $(19^3 \bmod 31)^4 \bmod 23$, we will first evaluate $19^3 \bmod 31$.

$$19^3 \bmod 31 = 6859 \bmod 31 = 8$$

Therefore,

$$(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$$

Next, note that $8^4 = 4096$. Because $4096 = 178 \times 23 + 2$, we have $4096 \bmod 23 = 2$.
Hence,

$$(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23 = 4096 \bmod 23 = 2$$

□

3

3. Sequences, Mathematical induction and recursion

3.1 Sequences

Definition 25: Sequence

sequence is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

We typically represent a sequence as a set of elements written in a row. In the sequence denoted

$$a_m, a_{m+1}, a_{m+2}, ..., a_n$$

each individual element a_k (read "a sub k") is called a term. The k in a_k is called a subscript or index; m (which may be any integer) is the subscript of the initial term, and n (which must be an integer that is greater than or equal to m) is the subscript of the final term. The notation

$$a_m, a_{m+1}, a_{m+2}, ...$$

denotes an infinite sequence. An explicit formula or general formula for a sequence is a rule that shows how the values of a_k depend on k.

The following example shows that it is possible for two different formulas to give sequences with the same terms.

Example 3.1. Define sequences $a_1, a_2, a_3, ...$ and $b_2, b_3, b_4, ..$ by the following explicit formulas:

$$a_k = \frac{k}{k+1} \text{ for every integer } k \geq 1$$

$$b_i = \frac{i-1}{i} \text{ for every integer } i \geq 2$$

Compute the first five terms of both sequences.

Example 3.2. Compute the first six terms of the sequence $c_0, c_1, c_2, ...$ defined as follows:

Finding an Explicit Formula to Fit Given Initial Terms

The next example treats the question of how to find an explicit formula for a sequence with given initial terms. Any such formula is a guess, but it is useful to be able to make such guesses.

Example 3.3. Find an explicit formula for a sequence with the following initial terms:

$$1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, -\frac{1}{36}, ...$$

Summation Notation

If m and n are integers and $m \leq n$, the symbol $\sum_{k=m}^{n} a^k$, read the summation from k equals m to n of a-sub-k, is the sum of all the terms $a_m, a_{m+1}, a_{m+2}, ..., a_n$. We say that $a_m + a_{m+1} + a_{m+2} + ... + a_n$ is the expanded form of the sum, and we write

$$\sum_{k=m}^{n} a^k = a_m + a_{m+1} + a_{m+2} + ... + a_n$$

We call k the index of the summation, m the lower limit of the summation, and n the upper limit of the summation.

Example 3.4. Compute $\sum_{k=1}^{5} k^2$

Example 3.5. Write $\sum_{i=0}^{n} \frac{(-1)^i}{i+1}$ in expanded form

Example 3.6. Express the following using summation notation:

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \ldots + \frac{n+1}{2n}$$

Solution. The general term of this summation can be expressed as $\frac{i+1}{n+i}$ for each integer i from 0 to n. Hence

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \ldots + \frac{n+1}{2n} = \sum_{i=0}^{n} \frac{i+1}{n+i}$$

Example 3.7. Write $\sum_{i=0}^{n} 2^i + 2^{n+1}$ as a single summation

Example 3.8. Rewrite $\sum_{i=1}^{n+1} \frac{1}{i^2}$ by separating off the final term.

A Telescoping Sum

Some sums can be transformed so that successive cancellation of terms collapses the final result like a telescope. For instance, observe that for every integer $k \geq 1$,

$$\frac{1}{k} - \frac{1}{k+1} = \frac{(k+1)-k}{k(k+1)} = \frac{1}{k(k+1)}$$

Example 3.9. Use this identity to find a simple expression for $\sum_{k=1}^{n} \frac{1}{k(k+1)}$

Solution.

$$\begin{aligned}\sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{k+1} \\ &= 1 - \frac{1}{n+1}\end{aligned}$$

Product Notation

The notation for the product of a sequence of numbers is analogous to the notation for their sum. The Greek capital letter pi, $\prod$, denotes a product. For example,

$$\prod_{k=1}^{5} a_k = a_1a_2a_3a_4a_5.$$

A recursive definition for the product notation is the following: If m is any integer, then

$$\prod_{k=m}^{m} a_k = a_m \text{ and } \prod_{k=m}^{n} a_k = (\prod_{k=m}^{n-1} a_k).a_n \text{ for every integer } n > m$$

Example 3.10. Compute the following products:

(a) $\prod_{k=1}^{5} k$ (b) $\prod_{k=1}^{1} \frac{k}{k+1}$

Properties of Summations and Products

Theorem 3.1. *If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$:*

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$

2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$

3. $(\prod_{k=m}^{n} a_k)(\prod_{k=m}^{n} b_k) = \prod_{k=m}^{n} (a_k \cdot b_k)$

Example 3.11. Let $a_k = k + 1$ and $b_k = k - 1$ for every integer k. Write each of the following expressions as a single summation or product:

(a) $\sum_{k=m}^{n} a_k + 2 \sum_{k=m}^{n} b_k$ (b) $(\prod_{k=m}^{n} a_k)(\prod_{k=m}^{n} b_k))$

Example 3.12. Transform the following summation by making the specified change of variable:

$$\text{summation } \sum_{k=0}^{6} \frac{1}{k+1} \text{ change of variable: } j = k + 1$$