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 $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$. ■

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:

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

For all integers n and d, $d|n \leftrightarrow \frac{n}{d}$ 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

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

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 $a \equiv b(\bmod m)$ to indicate that a is congruent to b modulo m. We say that $a \equiv b(\bmod m)$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b(\bmod m)$.

Although both notations $a \equiv b(\bmod m)$ 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.*

*Then $a \equiv b(\bmod m)$ if and only if a **mod** $m = b$ **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 $a \equiv b(\bmod m)$ 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 $17 \equiv 5(\bmod 6)$. 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

$$m|(a-b)$$

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

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

. 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

$$a_m, a_{m+1}, a_{m+2}, \cdots$$

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 $\frac{i+1}{n+1}$ for each integer i from 0 to n. Hence

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

■

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.

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

$$= 1 - \frac{1}{n+1}$$

■

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,

$$\prod_{k=1}^{5} a_k = a_1 a_2 a_3 a_4 a_5$$

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:

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

3.2 Recurrence Relations

There are many other ways to specify a sequence. For example, another way to specify a sequence is to provide one or more initial terms together with a rule for determining subsequent terms from those that precede them.

Definition 30: Recurrence Relations

A recurrence relation for the sequence $\{a_n\}$ is an equation that expresses an in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, ..., a_{n-1}$, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer. A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation.

Example 3.13. Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1}+3$ for $n = 1, 2, 3, ...,$ and suppose that $a_0 = 2$. What are a_1, a_2, and a_3?

Example 3.14. Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, ...,$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2 and a_3?

Example 3.15. The Fibonacci sequence, $f_0, f_1, f_2, ...,$ is defined by the initial conditions $f_0 = 0$, $f_1 = 1$, and the recurrence relation

$$f_n = f_{n-1} + f_{n-2}$$

for $n = 2, 3, 4, ...$ Find the Fibonacci numbers f_2, f_3, f_4, f_5, and f_6.

Example 3.16. Suppose that $\{an\}$ is the sequence of integers defined by $a_n = n!$, the value of the factorial function at the integer n, where $n = 1, 2, 3, ...$ Because $n! = n((n-1)(n-2)...2 \cdot 1) = n(n-1)! = na_{n-1}$, we see that the sequence of factorials satisfies the recurrence relation $a_n = na_{n-1}$, together with the initial condition $a_1 = 1$.

We say that we have solved the recurrence relation together with the initial conditions when we find an explicit formula, called a **closed formula**, for the terms of the sequence.

Example 3.17. Determine whether the sequence $\{a_n\}$, where $a_n = 3n$ for every nonnegative integer n, is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, ...$. Answer the same question where $a_n = 2n$ and where $a_n = 5$.

Solution. Suppose that $a_n = 3n$ for every nonnegative integer n. Then, for $n \geq 2$, we see that $2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2) = 3n = an$. Therefore, $\{a_n\}$, where $a_n = 3n$, is a solution of the recurrence relation.

Suppose that $a_n = 2n$ for every nonnegative integer n. Note that $a_0 = 1$, $a_1 = 2$, and $a_2 = 4$. Because $2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a2$, we see that $\{a_n\}$, where $a_n = 2n$, is not a solution of the recurrence relation.

Suppose that $a_n = 5$ for every nonnegative integer n. Then for $n \geq 2$, we see that $a_n = 2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n$. Therefore, $\{a_n\}$, where $a_n = 5$, is a solution of the recurrence relation. ■

The Method of Iteration

The most basic method for finding an explicit formula for a recursively defined sequence is iteration. Iteration works as follows: Given a sequence $a_n = a_0, a_1, a_2, ...$ defined by a recurrence relation and initial conditions, you start from the initial conditions and calculate successive terms of the sequence until you see a pattern developing. At that point you guess an explicit formula.

Example 3.18. Solve the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, ...,$ and $a_1 = 2$.

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$
$233 \equiv 23 \pmod{105}$

Solution. We can successively apply the recurrence relation, starting with the initial condition $a_1 = 2$, and working upward until we reach an to deduce a closed formula for the sequence. We see that

$$\begin{aligned} a_2 &= 2+3 \\ a_3 &= (2+3)+3 = 2+3\cdot 2 \\ a_4 &= (2+2\cdot 3)+3 = 2+3\cdot 3 \\ &\vdots \\ a_n &= a_{n-1}+3 = (2+3(n-2))+3 = 2+3(n-1). \end{aligned}$$

At each iteration of the recurrence relation, we obtain the next term in the sequence by adding 3 to the previous term. We obtain the *nth* term after $n-1$ iterations of the recurrence relation. Hence, we have added $3(n-1)$ to the initial term $a_0 = 2$ to obtain an. This gives us the closed formula $a_n = 2+3(n-1)$. ■

Example 3.19. Let $a_0, a_1, a_2, \ldots$ be the sequence defined recursively as follows: For each integer $k \geq 1$,

$$\begin{aligned} a_k &= a_{k-1}+2 \\ a_0 &= 1 \end{aligned}$$

Use iteration to guess an explicit formula for the sequence.

Solution. Here's how the process works for the given sequence:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= a_0+2 = 1+2 = 1+2\cdot 1 \\ a_2 &= a_1+2 = (1+2)+2 = 1+2+2 = 1+2\cdot 2 \\ a_3 &= a_2+2 = (1+2+2)+2 = 1+2+2+2 = 1+2\cdot 3 \\ a_4 &= a_3+2 = (1+2+2+2)+2 = 1+2+2+2+2 = 1+2\cdot 4 \\ &\vdots \\ a_n &= a_{n-1}+2 = (1+2+2\ldots 2)+2 = 1+2+2+2+\ldots+2 = 1+2n \end{aligned}$$

Therefore, $a_n = 1+2n$ for every integer $k \geq 1$. ■

Example 3.20. Let r be a fixed nonzero constant, and suppose a sequence $a_0, a_1, a_2, \ldots$ is defined recursively as follows:

$$\begin{aligned} a_k &= ra_{k-1} \text{ for each integer } k \geq 1, \\ a_0 &= a. \end{aligned}$$

Use iteration to guess an explicit formula for this sequence.

Example 3.21. Solve the recurrence relation $m_k = 2m_{k-1}+1$ for $k \geq 2$ and $m_1 = 1$.

Solution.

$$m_1 = 1$$
$$m_2 = 2m_1 + 1 = 2 \cdot 1 + 1 = 2^1 + 1$$
$$m_3 = 2m_2 + 1 = 2 \cdot (2+1) + 1 = 2^2 + 2 + 1$$
$$m_4 = 2m_3 + 1 = 2 \cdot (2^2 + 2 + 1) + 1 = 2^3 + 2^2 + 2 + 1$$
$$m_5 = 2m_4 + 1 = 2 \cdot (2^3 + 2^2 + 2 + 1) + 1 = 2^4 + 2^3 + 2^2 + 2 + 1$$

Thus it seems that, in general,

$$m_n = 2^{n-1} + 2^{n-2} + \ldots + 2^2 + 2 + 1$$

By the formula for the sum of a geometric sequence

$$m_n = 2^{n-1} + 2^{n-2} + \ldots + 2^2 + 2 + 1 = \frac{2^n - 1}{2 - 1} = 2^n - 1$$

Hence the explicit formula seems to be

$$m_n = 2^n - 1 \text{ for every integer } n \geq 1.$$

■

Example 3.22. Solve the recurrence relation $s_k = s_k + (k-1)$ for each integer $k \geq 2$ and $s_1 = 0$.

Checking the Correctness of a Formula by Mathematical Induction

Example 3.23. Use Mathematical Induction to verify the correctness of a solution to a Recurrence Relation in Example 3.18

Solution. proof of Correctness: Let $a_0, a_1, a_2, a_3, \ldots$ be the sequence defined by specifying that $a_1 = 2$, and $a_n = a_{n-1} + 3$ for each $n = 1, 2, 3, \ldots$, and let the property $P(n)$ be the equation

$$a_n = 2 + 3(n-1)$$

We will use mathematical induction to prove that for every integer $n = 1, 2, 3, \ldots$, $P(n)$ is true.
Show that $P(1)$ is true:
To establish $P(1)$, we must show that

$$a_1 = 2 + 3(1-1) = 2 \text{ and by definition } a_1 = 2$$

Thus the two sides of $P(1)$ equal the same quantity, and hence $P(1)$ is true.
Show that for every integer $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is also true:
Suppose that k is any integer with $k \geq 1$ such that

$$a_k = 2 + 3(k-1) \text{ inductive hypothesis}$$

[We must show that $P(k+1)$ is true. That is:] We must show that

$$a_{k+1} = 2 + 3((k+1) - 1)$$

But the left-hand side of $P(k+1)$ is

$$\begin{aligned} a_{k+1} &= a_{(k+1)-1} + 3 \\ &= a_k + 3 \\ &= 2 + 3(k-1) + 3 \\ &= 2 + 3k - 3 + 3 \\ &= 2 + 3(k-1+1) \\ &= 2 + 3((k+1)-1) \end{aligned}$$

which equals the right-hand side of $P(k+1)$. *[Since the basis and inductive steps have been proved, it follows by mathematical induction that the given formula holds for every integer $n \geq 1$.]* ■

Example 3.24. Use Mathematical Induction to verify the correctness of a solution to a Recurrence Relation in Example 3.19

Example 3.25. Use Mathematical Induction to verify the correctness of a solution to a Recurrence Relation in Example 3.20

Example 3.26. Use Mathematical Induction to verify the correctness of a solution to a Recurrence Relation in Example 3.21

Example 3.27. Use Mathematical Induction to verify the correctness of a solution to a Recurrence Relation in Example 3.22

4. Matrices

Matrices are used throughout discrete mathematics to express relationships between elements in sets. In subsequent chapters we will use matrices in a wide variety of models. For instance, matrices will be used in models of communications networks and transportation systems. Many algorithms will be developed that use these matrix models. This section reviews matrix arithmetic that will be used in these algorithms.

Definition 31: matrix

A matrix is a rectangular array of numbers. A matrix with m rows and n columns is called an $m \times n$ matrix. The plural of matrix is **matrices**. A matrix with the same number of rows as columns is called **square**. Two matrices are **equal** if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.

Example 4.1. The matrix $\begin{bmatrix} 1 & 0 & 1 \\ 3 & 2 & 1 \end{bmatrix}$ is a 2×3 matrix.

Definition 32

Let m and n be positive integers and let

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

The ith row of $\mathbf{A}$ is the $1 \times n$ matrix $[a_{i1}, a_{i2}, \ldots, a_{in}]$. The jth column of $\mathbf{A}$ is the $m \times 1$ matrix

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

The (i, j)th element or entry of $\mathbf{A}$ is the element a_{ij}, that is, the number in the ith row and jth column of $\mathbf{A}$. A convenient shorthand notation for expressing the matrix $\mathbf{A}$ is to write $\mathbf{A} = [a_{ij}]$, which indicates that $\mathbf{A}$ is the matrix with its (i, j)th element equal to a_{ij}.

4.1 Matrix Arithmetic

Definition 33: Matrix Addition

Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be $m \times n$ matrices. The sum of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{A} + \mathbf{B}$, is the $m \times n$ matrix that has $a_{ij} + b_{ij}$ as its (i, j)th element. In other words, $\mathbf{A} + \mathbf{B} = [a_{ij} + b_{ij}]$.

The sum of two matrices of the same size is obtained by adding elements in the corresponding positions. Matrices of different sizes cannot be added, because such matrices will not both have entries in some of their positions.

Example 4.2. Find $\mathbf{A} + \mathbf{B}$ if

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & 3 \\ 3 & 4 & 0 \end{bmatrix} \text{ and } \mathbf{B} = \begin{bmatrix} 4 & 3 & -1 \\ 2 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix}$$

Definition 34: Matrix Product

Let $\mathbf{A}$ be an $m \times k$ matrix and $\mathbf{B}$ be a $k \times n$ matrix. The product of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{AB}$, is the $m \times n$ matrix with its (i,j)th entry equal to the sum of the products of the corresponding elements from the ith row of $\mathbf{A}$ and the jth column of $\mathbf{B}$. In other words, if $\mathbf{AB} = [c_{ij}]$, then

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ddots + a_{ik}b_{kj} = \sum_{r=1}^{k} a_{ir}b_{rj}$$

The product of two matrices is not defined when the number of columns in the first matrix and the number of rows in the second matrix are not the same.

Example 4.3. Let

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \text{ and } \mathbf{B} = \begin{bmatrix} 2 & 4 \\ 2 & 1 \\ 3 & 1 \end{bmatrix}$$

Find $\mathbf{AB}$ if it is defined.

Solution. $\mathbf{AB} = \begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 2 & 1 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} (1\times2+0\times2+4\times3) & (1\times4+0\times1+4\times1) \\ (2\times2+1\times2+1\times3) & (2\times4+1\times1+1\times1) \\ (3\times2+1\times2+0\times3) & (3\times4+1\times1+0\times1) \\ (0\times2+2\times2+2\times3) & (0\times4+2\times1+2\times1) \end{bmatrix} = \begin{bmatrix} 14 & 8 \\ 9 & 10 \\ 8 & 13 \\ 10 & 4 \end{bmatrix}$ ■

Example 4.4. Let

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \text{ and } \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \text{ Does } \mathbf{AB} = \mathbf{BA}?$$

Solution. We find that $\mathbf{AB} = \begin{bmatrix} 3 & 2 \\ 5 & 3 \end{bmatrix}$ and $\mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$ ■

Hence, $\mathbf{AB} \neq \mathbf{BA}$.

4.2 Transposes and Powers of Matrices

Definition 35: Identity Matrix

The identity matrix of order n is the $n \times n$ matrix $\mathbf{I}_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. Hence,

$$\mathbf{I}_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Multiplying a matrix by an appropriately sized identity matrix does not change this matrix. In other words, when $\mathbf{A}$ is an $m \times n$ matrix, we have

$$\mathbf{AI}_n = \mathbf{I}_m\mathbf{A} = \mathbf{A}.$$

Powers of square matrices can be defined because matrix multiplication is associative. When $\mathbf{A}$ is an $n \times n$ matrix, we have

$\mathbf{A}_0 = \mathbf{I}_n$, $\mathbf{A}_r = \mathbf{AAA} \dots \mathbf{A}$

Definition 36: Matrix Transpose

Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix. The transpose of $\mathbf{A}$, denoted by $\mathbf{A}^t$, is the $n \times m$ matrix obtained by interchanging the rows and columns of $\mathbf{A}$. In other words, if $\mathbf{A}^t = [b_{ij}]$, then $b_{ij} = a_{ji}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$.

Example 4.5. Let $\mathbf{A}$ be the matrix $\begin{bmatrix} 1 & 2 & 1 & 1 \\ 3 & 4 & 5 & 6 \\ 9 & 8 & 7 & 0 \end{bmatrix}$. Find $\mathbf{A}^t$

Definition 37: symmetric Matrix

A square matrix $\mathbf{A}$ is called *symmetric* if $\mathbf{A} = \mathbf{A}^t$. Thus, $\mathbf{A} = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for all i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.

Example 4.6. The matrix $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ is symmetric.

4.3 Zero–One Matrices

matrix all of whose entries are either 0 or 1 is called a zero–one matrix. Zero–one matrices are often used to represent discrete structures. Algorithms using these structures are based on Boolean arithmetic with zero–one matrices. This arithmetic is based on the Boolean operations $\wedge$ and $\vee$, which operate on pairs of bits, defined by

$$b_1 \wedge b_2 = \begin{cases} 1, & \text{if } b_1 = b_2 = 1 \\ 0, & \text{otherwise,} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1, & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0, & \text{otherwise,} \end{cases}$$

Definition 38

Let $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ be $m \times n$ zero–one matrices. Then the join of $\mathbf{A}$ and $\mathbf{B}$ is the zero–one matrix with (i, j)th entry $a_{ij} \vee b_{ij}$. The join of $\mathbf{A}$ and $\mathbf{B}$ is denoted by $A \vee B$. The meet of $\mathbf{A}$ and $\mathbf{B}$ is the zero–one matrix with (i, j)th entry $a_{ij} \wedge b_{ij}$. The meet of $\mathbf{A}$ and $\mathbf{B}$ is denoted by $A \wedge B$.

Example 4.7. Find the join and meet of the zero–one matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution. We find that the join of $\mathbf{A}$ and $\mathbf{B}$ is

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

The meet of $\mathbf{A}$ and $\mathbf{B}$ is

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Definition 39: Boolean product of two matrices.

Let $\mathbf{A} = [a_{ij}]$ be an $m \times k$ zero–one matrix and $\mathbf{B} = [b_{ij}]$ be a $k \times n$ zero–one matrix. Then the Boolean product of $\mathbf{A}$ and $\mathbf{B}$, denoted by $\mathbf{A} \odot \mathbf{B}$, is the $m \times n$ matrix with (i, j)th entry c_{ij} where

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{kj}).$$

Note that the Boolean product of A and B is obtained in an analogous way to the ordinary product of these matrices, but with addition replaced with the operation $\vee$ and with multiplication replaced with the operation $\wedge$. We give an example of the Boolean products of matrices.

Example 4.8. Find the Boolean product of $\mathbf{A}$ and $\mathbf{B}$, where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

■

Solution. $A \odot B = \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

Definition 40

Let $\mathbf{A}$ be a square zero–one matrix and let r be a positive integer. The rth Boolean power of $\mathbf{A}$ is the Boolean product of r factors of $\mathbf{A}$. The rth Boolean product of $\mathbf{A}$ is denoted by $\mathbf{A}[r]$. Hence,

$$A^{[r]} = A \odot A \odot A \odot A \odot \cdots \odot A$$

(This is well defined because the Boolean product of matrices is associative.)We also define $A^{[0]}$ to be $\mathbf{I}_n$.

Example 4.9. Let $\mathbf{A} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$. Find ,$A^{[n]}$ for all positive integers n.

Solution. We find that

$$A^{[2]} = A \odot A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

We also find that

$$A^{[3]} = A^{[2]} \odot A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^{[4]} = A^{[3]} \odot A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$A^{[5]} = A^{[4]} \odot A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

■

Therefore, $A^{[n]} = A^{[5]}$ for all positive integers n with $n \geq 5$.