Lecture Two

Section 2.1 – Sequences and Summations

Sequences

Definition

A sequence is a function from a subset of the set of integers (usually either the set {0, 1, 2, …} or the set {1, 2, 3, …} to a set *S*. We use the notation a_n to denote the image of the integer *n*. We call a_n a term of the sequence.

The sequence $\{a_n\}$, where $a_n = \frac{1}{n}$

The list of the terms of this sequence: $1,\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \ldots$

Definition

A ***geometric progression*** is a sequence of the form $a,\ ar,\ ar^2,\ \ldots,\ ar^n,\ \ldots$ where the *initial* term *a* and the ***common ratio*** *r* are real numbers.

The common ratio for: $6,\ -12,\ 24,\ -48,\ \ldots,\ (-2)^{n-1}(6),\ \ldots$ is $= \frac{-12}{6} = -2$

Definition

An ***arithmetic progression*** is a sequence of the form $a,\ a+d,\ a+2d,\ \ldots,\ a+nd,\ \ldots$ where the *initial* term *a* and the ***common difference*** *d* are real numbers.

Recurrence Relations

Definition

A ***recurrence relation*** for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, $a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ \ldots$, for all integers *n* with $n \ge n_0$, where n_0 is a nonnegative integer. A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation. (A recurrence relation is said to *recursively define* a sequence.)

Example

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

Solution

$$a_1 = a_0 + 3 = 2 + 3 = 5$$
$$a_2 = a_1 + 3 = 5 + 3 = 8$$
$$a_3 = a_2 + 3 = 8 + 3 = 11$$

Example

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

Solution

$$a_2 = a_1 + a_0 = 5 - 3 = 2$$
$$a_3 = a_2 + a_1 = 2 - 5 = -3$$

Definition

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

$$f_n = f_{n-1} + f_{n-2} \quad for \quad n = 2,\ 3,\ 4,\ \ldots$$

Example

Find the Fibonacci number $f_2, f_3, f_4, f_5,\ and\ f_6$

Solution

$$f_2 = f_1 + f_0 = 1 + 0 = 1$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5$$
$$f_6 = f_5 + f_4 5 + 3 = 8$$

Example

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 whenere $a_n = 2^n$ and where $a_n = 5$

Solution

Suppose that $a_n = 3n$. Then, for $n \ge 2$,

$$\begin{aligned} 2a_{n-1} - a_{n-2} &= 2\big(3(n-1)\big) - 3(n-2) \\ &= 6n - 2 - 3n + 6 \\ &= 3n = a_n \end{aligned}$$

Is a solution of the recurrence relation

Suppose that $a_n = 2^n$. Then, for $n \ge 2$,

$$\begin{aligned} 2a_{n-1} - a_{n-2} &= 2\cdot 2^{n-1} - 2^{n-2} \\ &= 2^n\left(2\cdot 2^{-1} - 2^{-2}\right) \\ &= 2^n\left(1 - \frac{1}{4}\right) \\ &= 2^n\left(\frac{3}{4}\right) \\ &= 3\cdot 2^{n-2} \\ &\ne 2^n = a_n \end{aligned}$$

Is ***not*** a solution of the recurrence relation

or $a_0 = 1, \quad a_1 = 2, \quad a_2 = 4$

$2a_1 - a_0 = 2\cdot 2 - 1 = 3 \ne a_2$

Suppose that $a_n = 5$. Then, for $n \ge 2$,

$$2a_{n-1} - a_{n-2} = 2\cdot 5 - 5 = 5 = a_n$$

Is a solution of the recurrence relation

Example

Find the formalc for the sequences with the following first five terms:

a) $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$

b) 1, 3, 5, 7, 9

c) 1, −1, 1, −1, 1

Solution

a) The sequence with $a_n = \frac{1}{2^n}$, *n* = 0, 1, 2, …, This proposed sequence is a geometric progression with $a = 1$ and $r = \frac{1}{2}$.

b) Each term is obtained by adding 2 to the previous term, The sequence with $a_n = 2n+1$, n = 0, 1, 2, …, This proposed sequence is an arithmetic progression with $a=1$ and $d=2$.

c) The terms alternate between 1 and −1, The sequence with $a_n = (-1)^n$, n = 0, 1, 2, …, This proposed sequence is an geometric progression with $a=1$ and $r=-1$.

Example

How can we produce the terms of a sequence if the first 10 terms are 1, 2, 2, 3, 3, 3, 4, 4, 4, 4?

Solution

In this sequence, the integer 1 appears once, the integer 2 appears twice, the integer 3 appears three times, the integer 4 appears four times. A reasonable rule for generating this sequence is that the integer *n* appears exactly *n* times.

The sequence generated this is possible match.

Example

How can we produce the terms of a sequence if the first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

Solution

$d = 11-5 = 6$

The sequence can be obtained by adding 6 to previous term. This produce to $a_n = 5+6(n-1)$.

This sequence is an arithmetic progression with $a=5$ and $d=6$.

Example

How can we produce the terms of a sequence if the first 10 terms are 1, 3, 4, 7, 11, 18, 29, 47, 76, 123?

Solution

4 = 1 + 3

7 = 4 + 3

11 = 4 + 7

And so on. We can see that the third term is the sum of the two previous term.

The sequence is determined by the recurrence relation $L_n = L_{n-1} + L_{n-2}$ with initial conditions $L_1 = 1$ and $L_1 = 2$.

Some Useful Sequences	
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, …
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, …
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, …
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, …
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, …
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, …
f_n	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, …

Summations

To find the sum of many terms of an infinite sequence, it is easy to express using ***summation notation***.

$$\sum_{k=1}^{m} a_k = a_1 + a_2 + a_3 + \ldots + a_m$$

$$\sum\nolimits_{k=m}^{n} a_k \quad or \quad \sum\nolimits_{m \le k \le n} a_k$$

The index of summation runs through all integers starting with its ***lower limit*** and ending with its ***upper limit***.

The large uppercase Greek letter ***sigma***, Σ, is used to denote summation.

Example

Use the summation notation to express the sun of the first 100 terms of the sequence $\left\{a_j\right\}$, where $a_j = \frac{1}{j}$ for j = 1, 2, 3, …

Solution

$$\sum_{j=1}^{100} \frac{1}{j}$$

Example

What is the value of $\sum\limits_{j=1}^{5} j^2$

Solution

$$\begin{aligned}\sum_{j=1}^{5} j^2 &= 1^2+2^2+3^2+4^2+5^2\\ &= 1+4+9+16+25\\ &\underline{=55|}\end{aligned}$$

Example

What is the value of $\sum\limits_{k=4}^{8} (-1)^k$

Solution

$$\begin{aligned}\sum_{k=4}^{8} (-1)^k &= (-1)^4+(-1)^5+(-1)^6+(-1)^7+(-1)^8\\ &= 1+(-1)+1+(-1)+1\\ &\underline{=1|}\end{aligned}$$

Theorem

If *a* and *r* are real numbers and $r \neq 0$, then

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1}-a}{r-1} & if \;\; r \neq 1 \\ (n+1)a & if \;\; r11 \end{cases}$$

Proof

Let $S_n = \sum\limits_{j=0}^{n} ar^j$

$$\begin{aligned} rS_n &= r\sum_{j=0}^{n} ar^j\\ &= \sum_{j=0}^{n} ar^{j+1}\end{aligned}$$

$$= \sum_{k=1}^{n+1} ar^k$$ ***Shifting the index of summation with*** $k = j+1$

$$= \sum_{k=0}^{n} ar^k + \left(ar^{n+1} - a\right)$$

$$= S_n + \left(ar^{n+1} - a\right)$$

$$rS_n = S_n + \left(ar^{n+1} - a\right)$$

$$(r-1)S_n = ar^{n+1} - a$$

$$S_n = \frac{ar^{n+1} - a}{r-1}$$

If $r = 1$, then the $S_n = \sum_{j=0}^{n} a(1)^j = \sum_{j=0}^{n} a = (n+1)a$

Double summations

Double summations arise in many contexts (as in the analysis of nested loops in computer programs). An example of a double summation is

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij$$

To evaluate the double sum, first expand the inner summation and then continue by computing the outer summation

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij = \sum_{i=1}^{4}(i + 2i + 3i)$$

$$= \sum_{i=1}^{4} 6i$$

$$= 6 + 12 + 18 + 24$$

$$= 60$$

Some Useful Summation Formulae	
Sum	Closed Form
$\sum\limits_{k=0}^{n} ar^k \quad (r \neq 0)$	$\frac{ar^{n+1}-a}{r-1}, \quad r \neq 1$
$\sum\limits_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum\limits_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum\limits_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum\limits_{k=0}^{\infty} x^k, \quad \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum\limits_{k=1}^{\infty} kx^{k-1}, \quad \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

Example

What is the value of $\sum_{s\in[0,2,4]} s$

Solution

$$\sum_{s\in[0,2,4]} s \quad = 0+2+4 \quad \underline{=6}$$

Example

What is the value of $\sum\limits_{k=50}^{100} k^2$

Solution

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$= \frac{100\cdot 101\cdot 201}{6} - \frac{49\cdot 50\cdot 99}{6} = 338,350 - 40,425 \quad \underline{= 297,925}$$

Exercises *Section* 2.1 – Sequences and Summations

1. Find these terms of the sequence $\{a_n\}$, where $a_n = 2\cdot(-3)^n + 5^n$

a) a_0 *b)* a_1 *c)* a_4 *d)* a_5

2. What is the term a_8 of the sequence $\{a_n\}$, if a_n equals

a) 2^{n-1} *b)* 7 *c)* $1+(-1)^n$ *d)* $-(2)^n$

3. What are the terms $a_0,\ a_1,\ a_2,\ and\ a_3$ of the sequence $\{a_n\}$, if a_n equals

a) 2^n+1 *b)* $(n+1)^{n+1}$ *c)* $\frac{n}{2}$ *d)* $\frac{n}{2}+\frac{n}{2}$

e) $(-2)^n$ *f)* 3 *g)* $7+4^n$ *h)* $2^n+(-2)^n$

4. Find at least three different sequences beginning with the terms 1, 2, 4 whose terms are generated by a simple formula or rule.

5. Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.

6. Find the first five terms of the sequence defined by each of these recurrence relations and initial conditions.

a) $a_n = 6a_{n-1},\ \ a_0 = 2$

b) $a_n = a_{n-1}^2,\ \ a_1 = 2$

c) $a_n = a_{n-1} + 3a_{n-2},\ \ a_0 = 1,\ a_1 = 2$

d) $a_n = na_{n-1} + n^2a_{n-2},\ \ a_0 = 1,\ a_1 = 1$

e) $a_n = a_{n-1} + a_{n-3},\ \ a_0 = 1,\ a_1 = 2,\ a_2 = 0$

7. Find the first six terms of the sequence defined by each of these recurrence relations and initial conditions.

a) $a_n = -2a_{n-1},\ \ a_0 = -1$

b) $a_n = a_{n-1} - a_{n-2},\ \ a_0 = 2,\ \ a_1 = -1$

c) $a_n = 3a_{n-1}^2,\ \ a_0 = 1$

d) $a_n = na_{n-1} + n^2a_{n-2},\ \ a_0 = -1,\ a_1 = 0$

e) $a_n = a_{n-1} - a_{n-2} + a_{n-3},\ \ \ a_0 = 1,\ a_1 = 2,\ a_2 = 2$

8. Let $a_n = 2^n + 5 \cdot 3^n$ *for* $n = 0, 1, 2, \ldots$

a) Find a_0, a_1, a_2, a_3, *and* a_4

b) Show that $a_2 = 5a_1 - 6a_0$, $a_3 = 5a_2 - 6a_1$, and $a_4 = 5a_3 - 6a_2$

c) Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers *n* with $n \geq 2$

9. Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = 8a_{n-1} - 16a_{n-2}$ if

a) $a_n = 0$?

b) $a_n = 1$?

c) $a_n = 2^n$?

d) $a_n = 4^n$?

e) $a_n = n4^n$?

f) $a_n = 2 \cdot 4^n + 3n4^n$?

g) $a_n = (-4)^n$?

h) $a_n = n^2 4^n$?

10. Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = a_{n-1} + 2a_{n-2} + 2n - 9$ if

i) $a_n = -n + 2$

j) $a_n = 5(-1)^n - n + 2$

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

l) $a_n = 7 \cdot 2^n - n + 2$

11. A person deposits \$1,000.00 in an account that yields 9% interest compounded annually.

a) Set up a recurrence relation for the amount in the account at the end of *n* years.

b) Find an explicit formula for the amount in the account at the end of *n* years.

c) How much money will the account contain after 100 years?

12. Suppose that the number of bacteria in a colony triples every hour.

a) Set up a recurrence relation for the number of bacteria after *n* hours have elapsed.

b) If 100 bacteria are used to begin new colony, how many bacteria will be in the colony in 10 hours?

13. A factory makes custom sports cars at an increasing rate. In the first month only one car is made, in the second month two cars are made, and so on, with n cars made in the *n*th month.

a) Set up a recurrence relation for the number of cars produced in the first n months by this factory.

b) How many cars are produced in the first year?

c) Find an explicit formula for the number of cars produced in the first n months by this factory

14. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list. Assuming that your formula or rule is correct, determine the next three terms of the sequence.

a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, …

b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, …

c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, …

d) 3, 6, 12, 24, 48, 96, 192, …

e) 15, 8, 1, −6, −13, −20, −27, …

f) 3, 5, 8, 12, 17, 23, 30, 38, 47, …

g) 2, 16, 54, 128, 250, 432, 686, …

h) 2, 3, 7, 25, 121, 721, 5041, 40321, …

i) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, …

j) 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, …

k) 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, …

Section 2.2 – Algorithms

Introduction

Definition

An ***algorithm*** is a finite sequence of precise instructions for performing a computation or for solving a problem.

- A program is one type of algorithm
  - All programs are algorithms
  - Not all algorithms are programs!
- Directions to somebody's house is an algorithm
- A recipe for cooking a cake is an algorithm
- The steps to compute the cosine of 90° is an algorithm

Properties of Algorithms

Input: An algorithm has input values from a specified set.

Output: From each set of input values an algorithm produces output values from a specified set. The output values are the solution to the problem.

Definiteness: The steps of an algorithm must be defined precisely.

Correctness: An algorithm should produce the correct output values for each set of input values.

Finiteness: An algorithm should produce the desired output after a finite (but perhaps large) number of steps for any input in the set.

Effectiveness: It must be possible to perform each step of an algorithm exactly and in a finite amount of time.

Generality: The procedure should be applicable for all problems of the desired form, not just for a particular set of input values.

Algorithm 1 – Finding the Maximum Element in a Finite Sequence

Given a list, how do we find the maximum element in the list?

To express the algorithm, we'll use pseudocode

- ✓ Pseudocode is kinda like a programming language, but not really

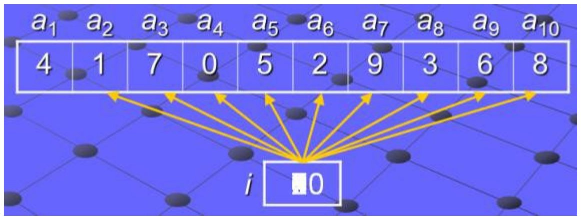
Example

Show that Algorithm 1 for finding the maximum element in a finite sequence of integers has all the properties listed.

Solution

The input to Algorithm 1 is a sequence of integers. The output is the largest integer in the sequence.
Each step of the algorithm is precisely defined, because only assignments, a finite loop, and conditional statements occur.
The values of the variable *max* equals the maximum terms when the algorithm terminates.
The initial value of max is the first term; as successive terms of the sequence are examined. This argument shows that when all the terms have been examined, max equal the value of the largest term and it will take *n* steps.
Algorithm 1 is general, because it can be used to find the maximum of any finite sequence of integers.

```
Procedure max $\{a_1, a_2, \ldots, a_n\}$
max:= $a_1$
for i := 2 to n
        if max $< a_i$ then  max $:= a_i$
return max{max is the largest element}
```



Searching Algorithms

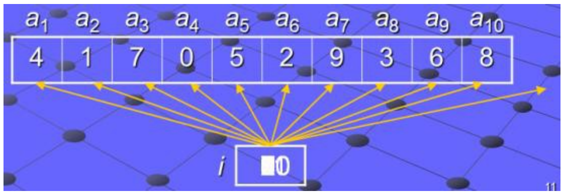
Given a list, find a specific element in the list. There are two types:

1. Linear search
2. Binary search

Algorithm 2 – Linear Search

Given a list which does not have to be sorted, find element in the list

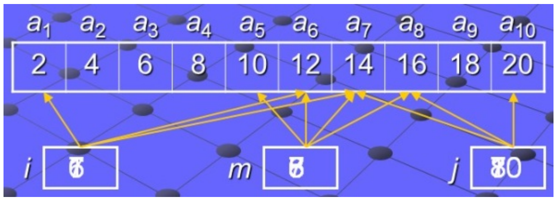
```
procedure linear_search (x: integer; $a_1, a_2, \ldots, a_n$ : integers)
i := 1
while ( $i \le n$ and $\left(i \le n \ \ and \ \ x \ne a_i\right)$
        $i := i + 1$
if $i \le n$ then location := i
else location := 0
{location is the subscript of the term that equals x, or it is 0 if x is not found}
```



Algorithm 3 – Binary Search

Given a list which *must* be sorted, find element in the list

```
***procedure*** linear_search ($x$: integer; $a_1, a_2, \ldots, a_n$ : increasing integers)
$i := 1$        { $i$ is left endpoint of search interval }
$j := n$        { $j$ is right endpoint of search interval }
while $i < j$
begin
    $m := \lfloor (i+j)/2 \rfloor$      {$m$ is the point in the middle }
    if $x > a_m$ then $i := m+1$
    else $j := m$
end
if $x = a_i$ then location := $i$
else location := 0
{location is the subscript of the term that equals $x$, or it is 0 if $x$ is not found}
```



$x = \boxed{14}$ *location* $\boxed{7}$

Sorting

Ordering the elements of a list is a problem that occurs in many contexts. Suppose that we have a list of elements of a set. Suppose that we have a way to order elements of the set. ***Sorting*** is putting these elements into a list in which the elements are in increasing order.

There are two types:

- ✓ ***Bubble sort***
- ✓ ***Insertion sort***

Bubble Sort

The *bubble sort* is one of the simplest sorting algorithms, but not one of the most efficient. It takes successive elements and "***bubbles***" them up the list.

Example

Use the bubble sort to put 3, 2, 4, 1, 5 into increasing order.

Solution

First Pass	3	2	2	2
	2	3	3	3
	4	4	4	1
	1	1	1	4
	5	5	5	5

Second Pass	2	2	2
	3	3	1
	4	1	3
	1	4	4
	$\boxed{5}$	$\boxed{5}$	$\boxed{5}$

Third Pass	2	1
	1	2
	3	3
	$\boxed{4}$	$\boxed{4}$
	$\boxed{5}$	$\boxed{5}$

Fourth Pass	1
	2
	$\boxed{3}$
	$\boxed{4}$
	$\boxed{5}$

Algorithm 4 – **Bubble**

```
procedure bubblesort ($a_1, a_2, \ldots, a_n$ : real numbers with $n \geq 2$)
 for $i := 1$ to $n - 1$
     for $j := 1$ to $n - i$
         if $a_j > a_j + 1$
             then interchange $a_j$ and $a_j + 1$
```

Bubble sort running time

Outer for loop does $n - 1$ iterations

Inner for loop does:

$n - 1$ iterations the first time

$n - 2$ iterations the second time

Total: $(n-1)+(n-2)+\ldots+2+1=\frac{n^2-n}{2}$

The bubble sort will take about n^2 time.

Insertion sort

The *insertion sort* is another simple sorting algorithm, but inefficient. It starts with a list with one element, and inserts new elements into their proper place in the sorted part of the list

Algorithm 5 – Insertion sort

```
procedure insertion_sort $(a_1, a_2, \ldots, a_n)$
        for $j := 2$ to $n$                    take successive elements in the list
    begin
        $i := 1$                               find where that element should be
        while $a_j > a_i$                      in the sorted portion of the list
            $i := i + 1$
        $m := a_i$                             move all elements in the sorted portion of the list
        for $k := 0$ to $j-i-1$                that are greater than the current element up by one
            $a_{j-k} := a_{j-k-1}$
        $a_i := m$                             put the current element into it's proper place
    end {$a_1, a_2, \ldots, a_n$ are sorted}          in the sorted portion of the list
```

The *insertion* sort will take about n^2 time.

Comparison of Running Times

Searches

- *Linear*: n steps
- *Binary*: $\log_2 n$ steps
- *Binary* search is about as fast as you can get

Sorts

- *Bubble:* n^2 steps
- *Insertion:* n^2 steps
- There are other, more efficient, sorting techniques
  - In principle, the fastest are heap sort, quick sort, and merge sort
  - These each take $n \bullet \log_2 n$ steps
  - In practice, quick sort is the fastest, followed by merge sort

Algorithm 6 – Greedy Change-Making Algorithm

```
procedure change ($c_1, c_2, \ldots, c_r$ : values of denominations of coins, where $c_1 > c_2 > \ldots > c_r$ ; n: a
                  positive integer)
 for i := 1 to r
     $d_i := 0$                    $d_i$ counts the coins of denomination $c_i$ used
     While $n \ge c_i$
         $d_i := d_i + 1$          Add a coin of denomination $c_i$
         $n := n - c_i$
{$d_i$ is the number of coins of denomination $c_i$ in the change for i = 1, 2, …, r}
```

Definition

If *n* is a positive integer, then *n* cents in change using quarters, dimes, nickels, and pennies using the fewest coins possible has at most two dimes, at most one nickel, at most four pennies, and cannot have two dimes and a nickel. The amount of change in dimes, nickels, and pennies cannot exceed 24 cents

Theorem

The greedy algorithm (−6) produces change using the fewest coins possible.

Exercises *Section* 2.2 – Algorithms

1. List all the steps used by the Algorithm 1 to find the maximum of the list

1, 8, 12, 9, 11, 2, 14, 5, 10, 4.

2. Devise an algorithm that finds the sum of all the integers in a list.

3. Describe an algorithm that takes as an input a list of n integers and produces as output the largest difference obtained by subtracting an integer in the list from the one following it.

4. Describe an algorithm that takes as an input a list of n integers in non-decreasing order and produces the list of all values that occur more than once.

5. Describe an algorithm that takes as an input a list of n integers and finds the location of the last even integer in the list or returns 0 if there are no even integers in the list.

6. Describe an algorithm that interchanges the values of the variables x and y, using only assignments. What is the minimum number of assignment statements needed to do this?

7. List all the steps used to search for 9 in the sequence 1, 3, 4, 5, 6, 7, 9, 11 using

a) a linear search *b*) a binary earch

8. Describe an algorithm that inserts an integer x in the appropriate position into the list $a_1, a_2, \ldots, a_n$ of integers that are in increasing order.

Section 2.3 – Divisibility and Modular Arithmetics

Division

Definition

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integers. When a divides b we say that a is a factor or divisor of b, and that b is multiple of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Example

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution

We see that $3 \nmid 7$, because 7/3 is not integer.

$3 \mid 12$ because $12/3 = 4$.

Example

Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution

The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < k \leq n/d$. Therefore, there are $\left[n/d \right]$ positive integers not exceeding n that are divisible by d.

Theroem

Let a, b, and c integers, where $a \neq 0$. Then

i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

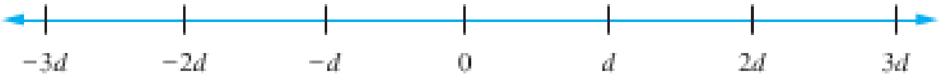
ii) If $a \mid b$, then $a \mid bc$ for all integers c;

iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof (*i*)

Suppose If $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s+t)$$



Therefore, a divides $b + c$.

Corollary

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

The Division Algorithm

Theroem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

Definition

In the equality given in the division algorithm, ***d*** is called the ***divisor***, ***a*** called the ***dividend***, ***q*** is called the ***quotient***, and ***r*** is called the ***remainder***. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \qquad r = a \textbf{ mod } d$$

Example

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

Solution

$101 = 11 \cdot 9 + 2$

Hence, the quotient when 101 is divided by 11 is 9 = 101 ***div*** 11,
and the remainder is 2 = 101 ***mod*** 11.

Example

What are the quotient and remainder when −11 is divided by 3?

Solution

$-11=3(-4)+1$

Hence, the quotient when −11 is divided by 3 is –4 = −11 ***div*** 3,
and the remainder is 1 = −11 ***mod*** 3.

Modular Arithmetic

Definition

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

Theorem

Let *a* and *b* be integers, and let *m* be a positive integer. Then $a \equiv b \pmod{m}$ if and only if
a **mod** *m* = *b* **mod** *m*

Example

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 $17 \equiv 5 \pmod{6}$.

24 – 14 = 10 is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$

Theorem

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

If $a \equiv b \pmod{m}$ that implies by the definition of congruence to $m \mid (a-b)$. Which is that there is an integer *k* such that $a-b=km \quad \Rightarrow \quad a=b+km$.

Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \textit{and} \qquad ac \equiv bd \pmod{m}$$

Proof

Using direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the theorem that are integers s and t with $b = a + sm \quad and \quad d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \qquad \Rightarrow \; a + c \equiv b + d \pmod{m}$$

And

$$bd = (a + sm)(c + tm) = ac + m(at + sc + stm) \qquad \Rightarrow \; ac \equiv bd \pmod{m}$$

Corollary

Let a and b be integers, and let m be a positive integer. Then

$$(a + b) \ \mathbf{mod}\ m \ = \ ((a \ \mathbf{mod}\ m) + (b \ \mathbf{mod}\ m)) \ \mathbf{mod}\ m$$

and

$$ab \ \mathbf{mod}\ m \ = \ ((a \ \mathbf{mod}\ m)(b \ \mathbf{mod}\ m)) \ \mathbf{mod}\ m$$

Arithmetic Modulo m

We define addition by: $a +_m b = (a + b) \ \mathbf{mod}\ m$ and multiplication by $a \cdot_m b = (a \cdot b) \ \mathbf{mod}\ m$

Exercises *Section* 2.3 – Divisibility and Modular Arithmetics

1. Does 17 divide each of these numbers?

a) 68 ***b***) 84 ***c***) 35 ***d***) 1001

2. Prove that if a is an integer other than 0, then

a) $1\ divides\ a$ ***b***) $a\ divides\ 0$

3. Show that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

4. Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$

5. What are the quotient and remainder when

a) 19 is divided by 7?
b) −111 is divided by 11?
c) 789 is divided by 23?
d) 1001 is divided by 13?
e) 0 is divided by 19?
f) 3 is divided by 5?
g) −1 is divided by 3?
h) 4 is divided by 1?

6. What time does a 12-hour clock read

a) 80 hours after it reads 11:00?
b) 40 hours before it reads 12:00?
c) 100 hours after it reads 6:00?

7. What time does a 24-hour clock read

a) 100 hours after it reads 2:00?
b) 45 hours before it reads 12:00?
c) 168 hours after it reads 19:00?

8. Suppose a and b are integers, $a \equiv 4 (\bmod 13)$, and $b \equiv 9 (\bmod 13)$. Find the integer c with $0 \leq c \leq 12$ such that

a) $c \equiv 9a (\bmod 13)$
b) $c \equiv 11b (\bmod 13)$
c) $c \equiv a + b (\bmod 13)$
d) $c \equiv 2a + 3b (\bmod 13)$
e) $c \equiv a^2 + b^2 (\bmod 13)$
f) $c \equiv a^3 - b^3 (\bmod 13)$

9. Suppose a and b are integers, $a \equiv 11 \ (\boldsymbol{mod}\ 19)$, and $b \equiv 3 \ (\boldsymbol{mod}\ 19)$. Find the integer c with $0 \le c \le 10$ such that

a) $c \equiv a - b \ (\boldsymbol{mod}\ 19)$

b) $c \equiv 7a + 3b \ (\boldsymbol{mod}\ 19)$

c) $c \equiv 2a^2 + 3b^2 \ (\boldsymbol{mod}\ 19)$

d) $c \equiv a^3 + 4b^3 \ (\boldsymbol{mod}\ 19)$

10. Let m be a positive integer. Show that $a \equiv b(\text{mod } m)$ if a **mod** $m = b$ **mod** m

11. Show that if n and k are positive integers, then $[n/k] = \left[\frac{n-1}{k}\right] + 1$

12. Evaluate these quantities

a) -17 ***mod*** 2

b) 144 ***mod*** 7

c) -101 ***mod*** 13

d) 199 ***mod*** 19

e) 13 ***mod*** 3

f) -97 ***mod*** 11

13. Find a **div** m and a **mod** m when

a) $a = 228, m = 119$

b) $a = 9009, m = 223$

c) $a = -10101, m = 333$

d) $a = -765432, m = 38271$

14. Find the integer a such that

a) $a \equiv -15(\boldsymbol{mod}\ 27)$ *and* $-26 \le a \le 0$

b) $a \equiv 24(\boldsymbol{mod}\ 31)$ *and* $-15 \le a \le 15$

c) $a \equiv 99(\boldsymbol{mod}\ 41)$ *and* $100 \le a \le 140$

d) $a \equiv 43(\boldsymbol{mod}\ 23)$ *and* $-22 \le a \le 0$

e) $a \equiv 17(\boldsymbol{mod}\ 29)$ *and* $-14 \le a \le 14$

15. Decide whether each of these integers is congruent to 5 modulo 17.

a) 37 *b*) 66 *c*) -17 *d*) -67

16. Find each of these values.

a) $(-133$ **mod** $23 + 261$ **mod** $23)$ **mod** 23 *b)* $\left(457 \textbf{ mod } 23 \cdot 182 \textbf{ mod } 23\right) \textbf{ mod } 23$

c) $\left(177 \textbf{ mod } 31 + 270 \textbf{ mod } 31\right) \textbf{ mod } 31$

d) $\left(19^2 \textbf{\textit{ mod }} 41\right) \textbf{\textit{mod }} 9$

e) $\left(32^3 \textbf{\textit{ mod }} 13\right)^2 \textbf{\textit{ mod }} 11$

f) $\left(99^2 \textbf{\textit{ mod }} 32\right)^3 \textbf{\textit{ mod }} 15$

g) $\left(3^4 \textbf{\textit{ mod }} 17\right)^2 \textbf{\textit{ mod }} 11$

h) $\left(19^3 \textbf{\textit{ mod }} 23\right)^2 \textbf{\textit{ mod }} 31$

i) $\left(89^3 \textbf{\textit{ mod }} 79\right)^4 \textbf{\textit{ mod }} 26$

Section 2.4 – Integer Representations and Algorithms

Representations of integers

Theorem

Let b be an integer greater that 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b_k + a_{k-1} b_{k-1} + \cdots + a_1 b + a_0$$

Where k is a nonnegative integer $a_0,\ a_1,\ \ldots,\ a_k$ are nonnegative integers less than b, and $a_k \neq 0$

Example

What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Solution

$$\begin{aligned}(1\ 0101\ 1111)_2 &= 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \\ &\underline{= 351|}\end{aligned}$$

Octal and Hexadecimal Expansions

Base 8 expansions are called ***octal*** expansions.
Base 16 expansions are called ***hexadecimal*** expansions.

Example

What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution

$$\begin{aligned}(7016)_8 &= 7\cdot 8^3 + 0\cdot 8^2 + 1\cdot 8^1 + 6\cdot 8^0 \\ &\underline{= 3598|}\end{aligned}$$

Example

What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution

$$\begin{aligned}(2AE0B)_{16} &= 2\cdot 16^4 + 10\cdot 16^3 + 14\cdot 16^2 + 0\cdot 16^1 + 11\cdot 16^0 \\ &\underline{= 175627|}\end{aligned}$$

Base Conversion

The algorithm for constructing the base b expansion of an integer n, divide n by b to obtain a quotient and remainder, that is,

$$n = bq_0 + a_0, \qquad 0 \le a_0 \le b$$
$$q_0 = bq_1 + a_1, \qquad 0 \le a_1 \le b$$

Example

Find the octal expansion of $(12345)_{10}$

Solution

$$\begin{aligned}
&12345 = 8 \cdot 1543 + 1 \\
&1543 = 8 \cdot 192 + 7 \\
&192 = 8 \cdot 24 + 0 \\
&24 = 8 \cdot 3 + 0 \\
&3 = 8 \cdot 0 + 3
\end{aligned}$$

$$(12345)_{10} = (30071)_8$$

Example

Find the hexadecimal expansion of $(177130)_{10}$

Solution

$$\begin{aligned}
&177130 = 16 \cdot 11070 + 10 \qquad (10 = A) \\
&11070 = 16 \cdot 691 + 14 \qquad (14 = E) \\
&691 = 16 \cdot 43 + 3 \\
&43 = 16 \cdot 2 + 11 \qquad (11 = B) \\
&2 = 16 \cdot 0 + 2
\end{aligned}$$

$$(177130)_{10} = (2B3EA)_{16}$$

Example

Find the bianry expansion of $(241)_{10}$

Solution

$$\begin{aligned}
&241 = 2 \cdot 120 + 1 \\
&120 = 2 \cdot 60 + 0 \\
&60 = 2 \cdot 30 + 0 \\
&30 = 2 \cdot 15 + 0
\end{aligned}$$

$$15 = 2 \cdot 7 + 1$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

$$(241)_{10} = (11110001)_2$$

***Representation of the Integers* 0 *through* 15.**																
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example

Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$

Solution

Octal: $(11\ 1110\ 1011\ 1100)_2 = (011\ 111\ 010\ 111\ 100)_2$

$$= (37274)_8$$

Hexadecimal: $(11\ 1110\ 1011\ 1100)_2 = (0011\ 1110\ 1011\ 1100)_2$

$$= (3EBC)_{16}$$

Example

Find the binary expansions of $(765)_8$ and $(A8D)_{16}$

Solution

$$(765)_8 = (111\ 110\ 101)_2$$

$$(A8D)_{16} = (1010\ 1000\ 1101)_2$$

Algorithms for Integer Operations

Addition Algorithm

To add *a* and *b*, first add their rightmost bits. This gives

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$$

Example

Add $a = (1110)_2$ *and* $b = (1011)_2$

Solution

$$\begin{array}{lll}
a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1 & \Rightarrow & c_0 = 0, \ s_0 = 1 \\
a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0 & \Rightarrow & c_1 = 1, \ s_1 = 0 \\
a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0 & \Rightarrow & c_2 = 1, \ s_2 = 0 \\
a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1 & \Rightarrow & c_3 = 1, \ s_3 = 1
\end{array}$$

Therefore, $s = a + b = \boxed{(11001)_2}$

$$\begin{array}{lccccc}
(carry) \ c & 1 & 1 & 1 & & \\
 & & 1 & 1 & 1 & 0 \\
 & + & 1 & 0 & 1 & 1 \\
\hline
s & 1 & 1 & 0 & 0 & 1
\end{array}$$

Example

How many additions of bits are required to use Algorithm 2 to add two integers with *n* bits (or less) in their binary representations?

Solution

Two integers are added by successively adding pairs of bits. Adding each pair of bits and the carry requires two additions of bits. Thus, the total number of additions of bits used is less than twice the number of bits in the expansion. Hence, the number of additions of bits used by Algorithm 2 to add two *n*-bit integers is *O*(*n*).

Multiplication Algorithm

$$\begin{aligned} ab &= a\left(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}\right) \\ &= a\left(b_0 2^0\right) + a\left(b_1 2^1\right) + \cdots + a\left(b_{n-1} 2^{n-1}\right) \end{aligned}$$

Algorithm: Multiplication of Integers

```
for $j := 0$ to $n - 1$
        if $b_j = 1$ then $c_j := a$ shifted $j$ places
        else $c_j := 0$
$p := 0$
for $j := 0$ to $n - 1$
        $p := p + c_j$
Return $p$ {$p$ is the value of $ab$}
```

Example

Find the product of $a = (110)_2$ and $b = (101)_2$

Solution

$$\begin{array}{r} 110 \\ \times\, 101 \\ \hline 110 \\ 000 \\ 110 \\ \hline 11110 \end{array}$$

Modular Exponential

It is important to find b^n **mod** m efficiently, where *b, n* and *m* are large integers.

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}}\cdots\cdot b^{a_1\cdot 2}\cdot b^{a_0}$$

Example

Compute 3^{11}

Solution

$$11=(1011)_2 \quad \rightarrow \quad 3^{11}=3^8 3^2 3^1$$

$$3^2=9, \quad 3^4=81, \quad 3^8=(81)^2=6561$$

$$\begin{aligned} 3^{11} &= 3^8 3^2 3^1 \\ &= 6561\cdot 9\cdot 3 \\ &\underline{= 177,147} \end{aligned}$$

Example

Use Algorithm 5 to find 3^{644} **mod** 645

Solution

$i=0$	$a_0=0$	$x=1$	$Power=3^2 \textbf{ mod } 645=9 \textbf{ mod } 645=9$
$i=1$	$a_1=0$	$x=1$	$Power=9^2 \textbf{ mod } 645=81 \textbf{ mod } 645=81$
$i=2$	$a_2=1$	$x=1\cdot 81 \textbf{ mod } 645=81$	$Power=81^2 \textbf{ mod } 645=6561 \textbf{ mod } 645=111$
$i=3$	$a_3=0$	$x=81$	$Power=111^2 \textbf{ mod } 645=12,321 \textbf{ mod } 645=66$
$i=4$	$a_4=0$	$x=81$	$Power=66^2 \textbf{ mod } 645=4356 \textbf{ mod } 645=486$
$i=5$	$a_5=0$	$x=81$	$Power=486^2 \textbf{ mod } 645=236,196 \textbf{ mod } 645=126$
$i=6$	$a_6=0$	$x=81$	$Power=126^2 \textbf{ mod } 645=15,876 \textbf{ mod } 645=396$
$i=7$	$a_7=1$	$x=(81\cdot 396) \textbf{ mod } 645=471$	$Power=396^2 \textbf{ mod } 645=156,816 \textbf{ mod } 645=81$
$i=8$	$a_8=0$	$x=471$	$Power=81^2 \textbf{ mod } 645=6561 \textbf{ mod } 645=111$
$i=9$	$a_9=1$	$x=(471\cdot 111) \textbf{ mod } 645=36$	

This shows that following steps of Algorithm 5 produces the result 3^{644} **mod** $645=36$

Exercises *Section* 2.4 – Integer Representations and Algorithms

1. Convert the decimal expansion of each of these integers to a binary expansion

a) 321 *b)* 1023 *c)* 100632 *d)* 231 *e)* 4532

2. Convert binary the expansion of each of these integers to a decimal expansion

a) $(1\ 1011)_2$ *b)* $(10\ 1011\ 0101)_2$ *c)* $(11\ 1011\ 1110)_2$ *d)*

e) $(111\ 1100\ 0001\ 1111)_2$ *f)* $(1\ 1111)_2$ *g)* $(10\ 0000\ 0001)_2$ *h)*

i) $(10\ 0101\ 0101)_2$ *i)* $(110\ 1001\ 0001\ 0000)_2$ *k)*

3. Convert the binary expansion of each of these integers to an octal expansion

a) $(1111\ 0111)_2$ *b)* $(1010\ 1010\ 1010)_2$

c) $(111\ 0111\ 0111\ 0111)_2$ *d)* $(101\ 0101\ 0101\ 0101)_2$

4. Convert the octal expansion of each of these integers to a binary expansion

a) $(572)_8$ *b)* $(1604)_8$ *c)* $(423)_8$ *d)* $(2417)_8$

5. Convert the hexadecimal expansion of each of these integers to a binary expansion

a) $(80E)_{16}$ *b)* $(135AB)_{16}$ *c)* $(ABBA)_{16}$

d) $(DEFACED)_{16}$ *e)* $(BADFACED)_{16}$ *f)* $(ABCDEF)_{16}$

6. Show that the binary expansion of a positive integer can be obtained from its hexadecimal expansion by translating each hexadecimal digit into a block of four binary digits.

7. Show that the binary expansion of a positive integer can be obtained from its octal expansion by translating each octal digit into a block of three binary digits.

8. Explain how to convert from binary to base 64 expansions and from base 64 expansions to binary expansions and from octal to base 64 expansions and from base 64 expansions to octal expansions

9. Find the sum and product of each of these pairs of numbers. Express your answers as a base 3 expansions

a) $(112)_3$, $(210)_3$ *b)* $(2112)_3$, $(12021)_3$

c) $(20001)_3$, $(1111)_3$ *d)* $(120021)_3$, $(2002)_3$

10. Find the sum and product of each of these pairs of numbers. Express your answers as an octal expansion.

a) $(763)_8$, $(147)_8$ *b)* $(6001)_8$, $(272)_8$

c) $(1111)_8$, $(777)_8$ *d)* $(54321)_8$, $(3456)_8$

11. Find the sum and product of each of these pairs of numbers. Express your answers as an hexadecimal expansion.

a) $(1AE)_{16}$, $(BBC)_{16}$ *b)* $(20CBA)_{16}$, $(A01)_{16}$

c) $(ABCDE)_{16}$, $(1111)_{16}$ *d)* $(E0000E)_{16}$, $(BAAA)_{16}$

Section 2.5 – Primes and Greatest Common Divisors

Primes

Definition

An integer p greater than 1 is called ***prime*** of the only positive factors of p are 1 or p.
A positive integer that is greater than 1 and is not prime is called composite.

Example

The integer 7 is prime because its only positive factors are 1 and 7.
The integer 9 is composite because its is divisible by 3.

Theorem – The Fundamental Theorem of Arithmetic

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

Find the prime factorization of 100, 641, 999, and 1024.

Solution

$$100 = 2\cdot 2\cdot 5\cdot 5 = 2^2\cdot 5^2$$

$$641 = 641$$

$$999 = 3\cdot 3\cdot 3\cdot 37 = 3^3\cdot 37$$

$$1024 = 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2 = 2^{10}$$

Trial Division

Theroem

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

Proof

If n is composite, then it has a factor a (by definition of a composite integer) with $1 < a < n$. Hence, by the definition of a factor, we have $n = ab, \quad b\left(\textit{positive integer}\right) > 1$.

If $a > \sqrt{n} \quad \textit{and} \quad b > \sqrt{n}$, then $ab > \sqrt{n}\cdot\sqrt{n} = n$, which is a contradiction. Consequently, $a \le \sqrt{n}$ *and* $b \le \sqrt{n}$. Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Example

Show that 101 is prime

Solution

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 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

Find the prime factorization of 7007

Solution

None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $\frac{7007}{7}=1001$, and $\frac{1001}{7}=143$, $\frac{143}{11}=13$. Because 13 is prime, the procedure is completed.

It follows that the prime factorization is $7007=7^2\cdot 11\cdot 13$

The Sieve of *Eratosthenes*

The ***Sieve of Eratosthenes*** can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

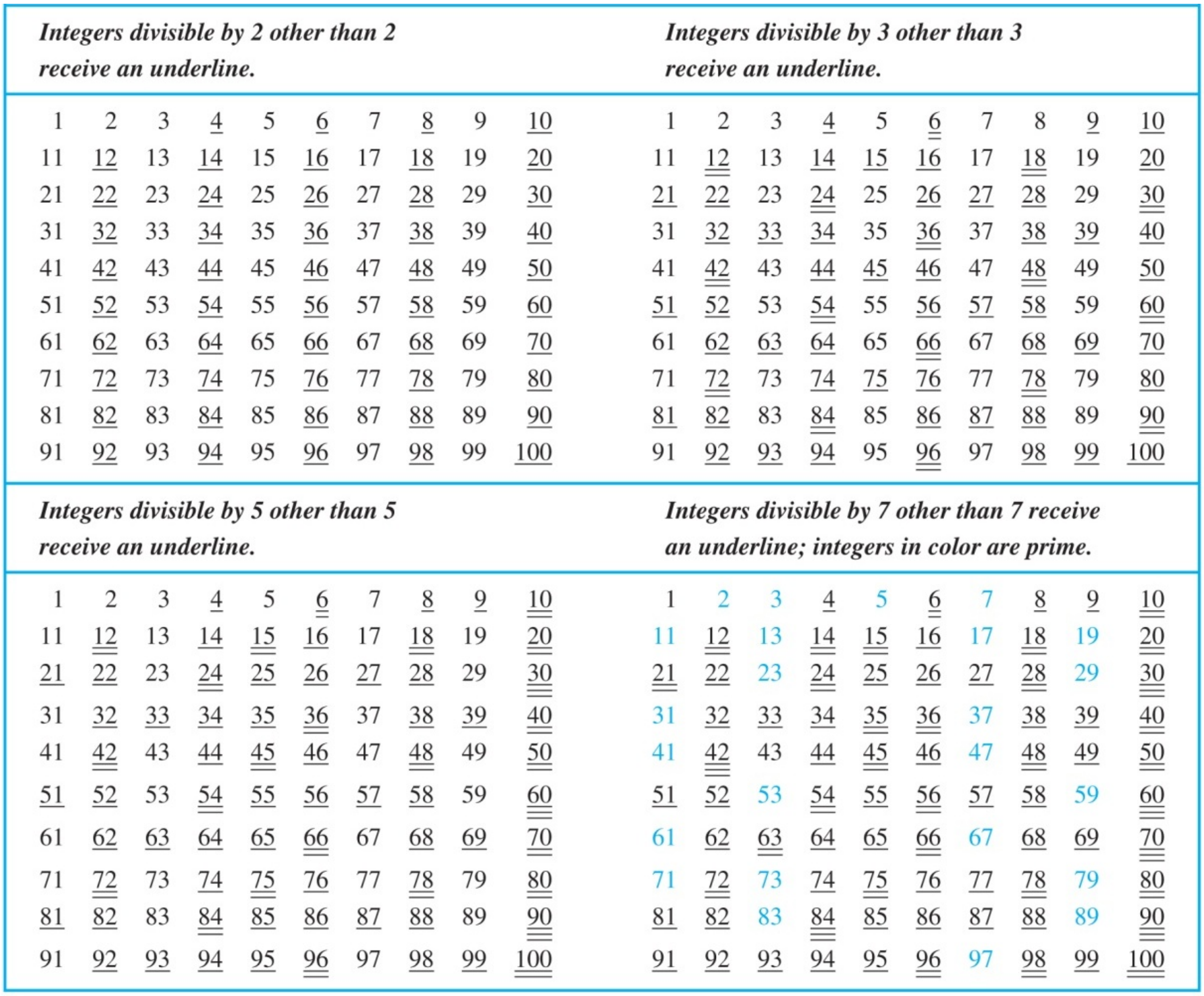
a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are: {2,3,7,11,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

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

To see this, note that if *n* = *ab*, then $a \le \sqrt{n}$ *or* $b \le \sqrt{n}$.

Trial division, a very inefficient method of determining if a number *n* is prime, is to try every integer *i* ≤ $\sqrt{n}$ and see if *n* is divisible by *i*.

The Sieve of Eratosthenes



Integers divisible by 2 other than 2 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	9	$\underline{10}$
11	$\underline{12}$	13	$\underline{14}$	15	$\underline{16}$	17	$\underline{18}$	19	$\underline{20}$
21	$\underline{22}$	23	$\underline{24}$	25	$\underline{26}$	27	$\underline{28}$	29	$\underline{30}$
31	$\underline{32}$	33	$\underline{34}$	35	$\underline{36}$	37	$\underline{38}$	39	$\underline{40}$
41	$\underline{42}$	43	$\underline{44}$	45	$\underline{46}$	47	$\underline{48}$	49	$\underline{50}$
51	$\underline{52}$	53	$\underline{54}$	55	$\underline{56}$	57	$\underline{58}$	59	$\underline{60}$
61	$\underline{62}$	63	$\underline{64}$	65	$\underline{66}$	67	$\underline{68}$	69	$\underline{70}$
71	$\underline{72}$	73	$\underline{74}$	75	$\underline{76}$	77	$\underline{78}$	79	$\underline{80}$
81	$\underline{82}$	83	$\underline{84}$	85	$\underline{86}$	87	$\underline{88}$	89	$\underline{90}$
91	$\underline{92}$	93	$\underline{94}$	95	$\underline{96}$	97	$\underline{98}$	99	$\underline{100}$

Integers divisible by 3 other than 3 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{10}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{20}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	25	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{30}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	35	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{40}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{50}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	55	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{60}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	65	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{70}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{80}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	85	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{90}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	95	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{100}$

Integers divisible by 5 other than 5 receive an underline.

1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{\underline{15}}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{\underline{20}}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{28}$	29	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{35}$	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{42}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	47	$\underline{\underline{48}}$	49	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	$\underline{55}$	$\underline{56}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{63}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{\underline{70}}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	77	$\underline{\underline{78}}$	79	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{84}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{\underline{90}}}$
91	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	97	$\underline{98}$	$\underline{99}$	$\underline{\underline{100}}$

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	**2**	**3**	$\underline{4}$	**5**	$\underline{\underline{6}}$	**7**	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	**13**	$\underline{\underline{14}}$	$\underline{\underline{15}}$	$\underline{16}$	**17**	$\underline{\underline{18}}$	**19**	$\underline{\underline{20}}$
$\underline{\underline{21}}$	$\underline{22}$	**23**	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{\underline{28}}$	**29**	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{\underline{35}}$	$\underline{\underline{36}}$	**37**	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{\underline{42}}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	**47**	$\underline{\underline{48}}$	$\underline{49}$	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	**53**	$\underline{\underline{54}}$	$\underline{55}$	$\underline{\underline{56}}$	$\underline{57}$	$\underline{58}$	**59**	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{\underline{63}}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	**67**	$\underline{68}$	$\underline{69}$	$\underline{\underline{\underline{70}}}$
71	$\underline{\underline{72}}$	**73**	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	$\underline{77}$	$\underline{\underline{78}}$	**79**	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	**83**	$\underline{\underline{\underline{84}}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	**89**	$\underline{\underline{\underline{90}}}$
$\underline{91}$	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	**97**	$\underline{\underline{98}}$	$\underline{99}$	$\underline{\underline{100}}$

The infinitude of Primes

It has long been known that there are infinitely many primes. This means that whenever $p_1, p_2, \dots, p_n$ are the n smallest primes, we know there is a larger.

Theorem

There are infinitely may primes.

Proof: Assume finitely many primes: $p_1, p_2, \dots, p_n$

Let $q = p_1 p_2 \dots p_n + 1$. Either q is prime or by the fundamental theorem of arithmetic it is a product of primes. But none of the primes p_i divides q since if $p_i \mid q$, then p_i divide $q - p_1 p_2 \dots p_n = 1$ .Hence, there is a prime not on the list $p_1, p_2, \dots, p_n$ It is either q, or if q is composite, it is a prime factor of q. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes. Consequently, there are infinitely many primes.

Mersenne Primes

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called ***Mersenne primes***.

Example

$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 37, \quad 2^7 - 1 = 127$ are Mersenne primes.

$2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.

There is an efficient test for determining if $2^p - 1$ is prime. The largest known prime numbers are Mersenne primes. 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.

Distribution of Primes

Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding x.

Theorem – Prime Number

The ratio of the number of primes not exceeding x and $\frac{x}{\ln x}$ approaches 1 as x grows without bound. ($\ln x$ is the natural logarithm of x),

The theorem tells us that the number of primes not exceeding x, can be approximated by $\frac{x}{\ln x}$.

The odds that a randomly selected positive integer less than n is prime are approximately

$(n / \ln n / n) = \frac{1}{\ln n}$

Greatest Common Divisor

Definition

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by gcd(a,b).

One can find greatest common divisors of small numbers by inspection.

Example

What is the greatest common divisor of 24 and 36?

Solution

gcd(24,26) = 12

Example

What is the greatest common divisor of 17 and 22?

Solution

gcd(17,22) = 1

Definition

The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example 17 and 22

Definition

The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd\left(a_i, a_j\right) = 1$ whenever $1 \le i \le j \le n$.

Example

Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution

Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example

Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution

Because gcd(10,24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Least Common Multiple

Definition

The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

The least common multiple can also be computed from the prime factorizations.

$$lcm(a,\ b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$$

This number is divided by both *a* and *b* and no smaller number is divided by *a* and *b*.

Example

$$lcm\left(2^3 3^5 7^2,\ 2^4 3^3\right) = 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)}$$

$$= 2^4 \cdot 3^5 \cdot 7^2$$

Theorem

Let *a* and *b* be positive integers. Then $ab = \gcd(a,b) \cdot lcm(a,b)$

Euclidean Algorithm

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(*a*,*b*) is equal to gcd(*a*,*c*) when *a* > *b* and *c* is the remainder when *a* is divided by *b*.

Lemma 1

Let $a = bq + r$, where *a, b, q*, and *r* are integers. Then $\gcd(a,b) = \gcd(b,r)$

Proof

Suppose that *d* divides both *a* and *b*. Then *d* also divides *a* − *bq* = *r*. Hence, any common divisor of *a* and *b* must also be any common divisor of *b* and *r*. Suppose that *d* divides both *b* and *r*. Then *d* also divides *bq* + *r* = *a*. Hence, any common divisor of *a* and *b* must also be a common divisor of *b* and *r*. Therefore, $\gcd(a,b) = \gcd(b,r)$.

Example

Find $gcd\,(91, 287)$

Solution

$287 = 91 \cdot 3 + 14$ ***Divide 287 by 91***

$91 = 14 \cdot 6 + 7$ ***Divide 91 by 14***

$14 = 7 \cdot 2 + 0$ ***Divide 14 by 7***

$gcd\,(287, 91) = 7$

Example

Find $gcd\,(414, 662)$

Solution

$662 = 414 \cdot 1 + 248$ ***Divide 662 by 414***

$414 = 248 \cdot 1 + 166$ ***Divide 414 by 248***

$248 = 166 \cdot 1 + 82$ ***Divide 248 by 166***

$166 = 82 \cdot 2 + 2$ ***Divide 166 by 82***

$82 = 2 \cdot 41 + 0$ ***Divide 82 by 2***

$gcd(414, 662) = 2$

Euclidean Algorithm

```
procedure gcd(a, b: positive integers)
$x := a$
$x := b$
while $y \neq 0$
    $r := x$ mod $y$
    $x := y$
    $y := r$
return $x$ {gcd($a$,$b$) is $x$}
```

GCDs as Linear Combinations

Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition

If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called ***Bézout coefficients*** of a and b. The equation $\gcd(a,b) = sa + tb$ is called ***Bézout's identity***.

Example

Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution

First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$

ii. $198 = 3 \cdot 54 + 36$

iii. $54 = 1 \cdot 36 + 18$

iv. $36 = 2 \cdot 18$

Now working backwards, from *iii* and *i* above

$18 = 54 - 1 \cdot 36$

$36 = 198 - 3 \cdot 54$

Substituting the 2nd equation into the 1st yields:

$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

Substituting $54 = 252 - 1 \cdot 198$ (from *i*)) yields:

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the ***extended Euclidean algorithm***, is developed in the exercises.

Lemma 2

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof

Assume $\gcd(a, b) = 1$ and $a \mid bc$

Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers s and t such that $sa + tb = 1$.

Multiplying both sides of the equation by c, yields $sac + tbc = c$. $a \mid tbc$ and a divides $sac + tbc$ since $a \mid sac$ and $a|tbc$. We conclude $a \mid c$, since $sac + tbc = c$.

Lemma 3

If p is prime and $p|a_1 a_2 \ldots a_n$, then $p|a_i$ for some i.

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Proof **(*by contradiction*)**

Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$

Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

By Lemma 3, it follows that p_{i_1} divides q_{j_k}, for some *k,* contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Hence, there can be at most one factorization of n into primes in nondecreasing order.

Dividing Congruences by an Integer

Theorem

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof

Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

Exercises *Section* 2.5 – Primes and Greatest Common Divisors

1. Determine whether each of these integers is prime.

a) 21 *b)* 29 *c)* 71 *d)* 97 *e)* 111

f) 143 *g)* 19 *h)* 27 *i)* 93 *j)* 101

k) 107 *l)* 113

2. Find the prime factorization of each these integers.

a) 88 *b)* 126 *c)* 729 *d)* 1001 *e)* 1111

f) 909,090 *g)* 39 *h)* 81 *i)* 101 *j)* 143

k) 289 *l)* 899

3. Find the prime factorization of 10!

4. Show that if $a^m + 1$ is composite if *a* and *m* are integers greater than 1 and *m* is odd. [*Hint*: Show that *x* + 1 is a factor of the polynomial $a^m + 1$ if *m* is odd]

5. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer *n*. [*Hint*: First show the polynomial identity $x^m + 1 = \left(x^k + 1\right)\left(x^{k(t-1)} - x^{k(t-2)} + \cdots - x^k + 1\right)$ holds, where $m = kt$ and *t* is odd]

6. Which positive integers less than 12 are relatively prime to 12?

7. Which positive integers less than 30 are relatively prime to 30?

8. Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55 *b)* 14, 17, 85 *c)* 25, 41, 49, 64 *d)* 17, 18, 19, 23

e) 11, 15, 19 *f)* 14, 15, 21 *g)* 12, 17, 31, 37 *h)* 7, 8, 9, 11

9. We call a positive integer ***perfect*** if it equals the sum of its positive divisors other than itself

a) Show that 6 and 28 are perfect.

b) Show that $2^{p-1}\left(2^p - 1\right)$ is a perfect number when $2^p - 1$ is prime

10. Show that if $2^n - 1$ is prime, then *n* is prime. *Hint*: Use the identity

$$2^{ab} - 1 = \left(2^a - 1\right) \cdot \left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right)$$

11. Determine whether each of these integers is prime, verifying some of Mersenne's claims

a) $2^7 - 1$ *b)* $2^9 - 1$ *c)* $2^{11} - 1$ *d)* $2^{13} - 1$

12. What are the greatest common divisors of these pairs of integers?

a) $2^2 \cdot 3^3 \cdot 5^5,\ \ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ \ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ \ 17^{17}$

d) $2^2 \cdot 7,\ \ 5^3 \cdot 13$

e) $0,\ \ 5$

f) $2 \cdot 3 \cdot 5 \cdot 7,\ \ 2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3,\ \ 2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17,\ \ 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) $23^{31},\ \ 23^{17}$

j) $41 \cdot 43 \cdot 53,\ \ 41 \cdot 43 \cdot 53$

k) $1111,\ \ 0$

13. What is the least common multiple of each pair

a) $2^2 \cdot 3^3 \cdot 5^5,\ \ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ \ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ \ 17^{17}$

d) $2^2 \cdot 7,\ \ 5^3 \cdot 13$

e) $0,\ \ 5$

f) $2 \cdot 3 \cdot 5 \cdot 7,\ \ 2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3,\ \ 2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17,\ \ 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) $23^{31},\ \ 23^{17}$

j) $41 \cdot 43 \cdot 53,\ \ 41 \cdot 43 \cdot 53$

k) $1111,\ \ 0$

14. Find gcd(1000, 625) and lcm(1000, 625) and verify that $\gcd(100,\ 625) \cdot lcm(100,\ 625) = 1000 \cdot 625$

15. Find gcd(92928, 123552) and lcm(92928, 123552) and verify that $\gcd(92928,\ 123552) \cdot lcm(92928,\ 123552) = 92928 \bullet 123552$

16. Use the Euclidean algorithm to find

a) $\gcd(1,\ 5)$ *b)* $\gcd(100,\ 101)$ *c)* $\gcd(123,\ 277)$ *d)* $\gcd(1529,\ 14039)$

e) $\gcd(1529,\ 14038)$ *f)* $\gcd(12,\ 18)$ *g)* $\gcd(111,\ 201)$ *h)* $\gcd(1001,\ 1331)$

i) $\gcd(12345,\ 54321)$ *j)* $\gcd(1000,\ 5040)$ *k)* $\gcd(9888,\ 6060)$

17. Prove that the product of any three consecutive integers is divisible by 6.

18. Show that if *a, b*, and *m* are integers such that $m \geq 2$ and $a \equiv b \left(\mathbf{mod}\ m \right)$, then $\gcd\left(a,\ m\right) = \gcd\left(b,\ m\right)$

19. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever *n* is a positive integer.

Section 2.6 – Applications of Congruences

Hashing Functions

Definition

A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

A common hashing function is $h(k) = k$ **mod** m, where m is the number of memory locations. Because this hashing function is onto, all memory locations are possible.

Example

Find the memory locations assigned by the hashing function $h(k) = k$ **mod** 111 to the records of customers with Social Security numbers 064212848, 037149212, and 107405723.

Solution

This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

$h(064212848) = 064212848$ **mod** $111 = 14$
$h\ (037149212) = 037149212$ **mod** $111 = 65$
$h\ (107405723) = 107405723$ **mod** $111 = 14$,

But since location 14 is already occupied, the record is assigned to the next available position, which is 15.

The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location. For collision resolution, we can use a *linear probing function*:

$$h(k,\ i) = (h(k),\ i)\ \textbf{mod}\ m, \text{ where } i \text{ from 0 to m} - 1.$$

There are many other methods of handling with collisions. You may cover these in a later CS course.

Pseudorandom Numbers

Randomly chosen numbers are needed for many purposes, including computer simulations.
Pseudorandom numbers are not truly random since they are generated by systematic methods.
The ***linear congruential*** *method* is one commonly used procedure for generating pseudorandom numbers.
Four integers are needed: the *modulus m*, the *multiplier a*, the *increment c*, and *seed* x_0, with $2 \le a < m$, 0 $\le c < m$, $0 \le x_0 < m$. We generate a sequence of pseudorandom numbers $\{x_m\}$, with $0 \le x_n < m$ for all *n*, by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

Example

Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus *m* = 9, multiplier *a* = 7, increment *c* = 4, and seed $x_0 = 3$.

Solution

Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \textbf{ mod } 9$, with $x_0 = 3$.

$$x_1 = (7x_0 + 4) \textbf{ mod } 9 = (7 \cdot 3 + 4) \textbf{ mod } 9 = 25 \textbf{ mod } 9 = 7$$

$$x_2 = (7x_1 + 4) \textbf{ mod } 9 = (7 \cdot 7 + 4) \textbf{ mod } 9 = 53 \textbf{ mod } 9 = 8$$

$$x_3 = (7x_2 + 4) \textbf{ mod } 9 = (7 \cdot 8 + 4) \textbf{ mod } 9 = 60 \textbf{ mod } 9 = 6$$

$$x_4 = (7x_3 + 4) \textbf{ mod } 9 = (7 \cdot 6 + 4) \textbf{ mod } 9 = 46 \textbf{ mod } 9 = 1$$

$$x_5 = (7x_4 + 4) \textbf{ mod } 9 = (7 \cdot 1 + 4) \textbf{ mod } 9 = 11 \textbf{ mod } 9 = 2$$

$$x_6 = (7x_5 + 4) \textbf{ mod } 9 = (7 \cdot 2 + 4) \textbf{ mod } 9 = 18 \textbf{ mod } 9 = 0$$

$$x_7 = (7x_6 + 4) \textbf{ mod } 9 = (7 \cdot 0 + 4) \textbf{ mod } 9 = 4 \textbf{ mod } 9 = 4$$

$$x_8 = (7x_7 + 4) \textbf{ mod } 9 = (7 \cdot 4 + 4) \textbf{ mod } 9 = 32 \textbf{ mod } 9 = 5$$

$$x_9 = (7x_8 + 4) \textbf{ mod } 9 = (7 \cdot 5 + 4) \textbf{ mod } 9 = 39 \textbf{ mod } 9 = 3$$

The sequence generated is 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, … It repeats after generating 9 terms.

- Commonly, computers use a linear congruential generator with increment *c* = 0. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Check Digits: UPCs

A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example

Retail products are identified by their *Universal Product Codes* (*UPC*s). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \ (\textbf{mod } 10)$$

a) Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b) Is 041331021641 a valid UPC?

Solution

a) $3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \ (\textbf{mod } 10)$

$98 + x_{12} \equiv 0 \ (\textbf{mod } 10)$

$x_{12} \equiv 0 \ (\textbf{mod } 10)$. So, the check digit is 2.

b) $3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + 1 \equiv 0 \ (\textbf{mod } 10)$

$44 \equiv 4 \not\equiv \ (\textbf{mod } 10)$

Hence, 041331021641 is not a valid UPC.

Exercises *Section* 2.6 – Applications of Congruences

1. Find the memory locations assigned by the hashing function $h(k) = k$ **mod** 97 to the records of customers with Social Security numbers?

a) 034567981 *b)* 183211232 *c)* 220195744 *d)* 987255335
e) 104578690 *f)* 432222187 *g)* 372201919 *h)* 501338753

2. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k$ **mod** 31, where k is the number formed from the first three digits on a visitor's license plate.

a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310

b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

3. Find the sequence of pseudorandom numbers generated by the linear congruential generator

a) $x_{n+1} = \left(3x_n + 2\right)$ **mod** 13 with seed $x_0 = 1$.

b) $x_{n+1} = \left(4x_n + 1\right)$ **mod** 7 with seed $x_0 = 3$.

4. Find the sequence of pseudorandom numbers generated by using the pure multiplicative generator $x_{n+1} = 3x_n$ **mod** 11 with seed $x_0 = 2$.

5. The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are $0-07-119881$. What is the check digit for that book?

6. The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is $0-321-500Q1-8$, where Q is a digit. Find the value of Q.

7. The USPS sells money orders identified by 11-digit number $x_1, x_2, \ldots, x_{11}$. The first ten digits identify the money order: x_{11} is a check digit that satisfies $x_{11} = x_1 + x_2 + \cdots + x_{10}$ **mod** 9. Find the check digit for the USPS money orders that have identification number that start with these ten digits

a) 7555618873 *b)* 6966133421 *c)* 8018927435 *d)* 3289744134
e) 74051489623 *f)* 88382013445 *g)* 56152240784 *h)* 66606631178

8. Determine which single digit errors are detected by the USPS money order code.

9. Determine which transposition errors are detected by the USPS money order code.