SOLUTIONS TO QUESTIONS IN CHAPTER 4

SECTION 1

1.1 $\frac{3}{12} = \frac{1}{4}$, $\frac{13}{121}$ is simplified, $\frac{65}{130} = \frac{1}{2}$, and $\frac{34,567}{891,011}$ is simplified. $\frac{1}{3} + \frac{1}{2} = \frac{5}{6}$, $\frac{1}{4} + \frac{1}{3} = \frac{7}{12}$, and $\frac{1}{15} + \frac{1}{65} = \frac{16}{195}$.

1.2 *(a)* 65, ***(b)*** 8, and (c) 1.

1.3 (a) gcd(5, 7) = 1, ***(b)*** gcd(4, 6) = 2, and (c) gcd (5, 10)=5. Since gcd(*b*, c) must divide both *b* and c, it cannot be larger than either.

1.4 Algorithm GCD1 run on the pair (3,4):

Step No.	*b*	*c*	*Are both b/g and c/g integers?*	*g*	gcd
1	3	4		3	
3,4	3	4	no	2	
3,4	3	4	no	1	
5 STOP	3	4			1

Algorithm GCD1 run on the pair (3, 12):

Step No.		b	c	Are both b/g and c/g integers?	g	gcd
1		3	12		3	
3	STOP	3	12	yes	3	3

Algorithm GCD1 run on the pair (6, 20):

Step No.		b	c	Are both b/g and c/g integers?	g	gcd
1		6	20		6	
3,4		6	20	no	5	
3,4		6	20	no	4	
3,4		6	20	no	3	
3,4		6	20	no	2	
3	STOP	6	20	yes		2

1.5 (a) (5, 7) or any pair for which gcd = 1, (b) (4,6) or any pair with 1< gcd, and (c) (4, 12) or any pair where gcd = b.

1.6 *Algorithm ADDFRACT1*

STEP 1. Input a, b, c, d {The sum a/b + c/d is to be calculated and output as a simplified fraction. }

STEP 2. Set numer $:= a * d + b * c$; set denom $:= b * d$

STEP 3. Use SIMPLIFY on the pair (numer, denom)

STEP 4. Output the result of step 3 and stop.

1.7 Let m = minimum $\{a, b\}$. Then upon input of a and h, the algorithm SIMPLIFY performs (at most) $2(m-1)$ divisions (in GCD1) plus two divisions (in step 3). Let m' = minimum $\{(ad - be), bd\}$. AD DFRACT1 performs three multiplications .in step 2 for a total of $2m' + 3$ multiplications and divisions.

SECTION 2

2.1 Using $\log(n) < B$, (a) $(\log(n))^2 < B^2$, (b) $\log(n^2) = 2\log(n) < 2B$, and (c) $\log(\log(n)) < \log(B)$.

2.2 Since by (1), $\log(n) \geq B/2$, $n = 2^{\log(n)} \geq 2^{B/2} = \sqrt{2}^B$.

SECTION 3

3.1 gcd (18, 30)= gcd (12, 18) = gcd (6, 12)= gcd (0, 6) = 6; gcd (18, 48) = gcd (18, 30)= 6; and gcd (18, 66) = gcd (18, 48) = 6.

3.2 (a) 1, (b) 3, and (c) 5.

3.3 (a) $q_1 = 4$, $r_1 = 0$, and gcd (3, 12) = gcd (0, 3) = 3. (b) $q_1 = 9$, $r_1 = 4$, and gcd (13, 121)= gcd (4, 13) = 1. (c) $q_1 = 1$, $r_1 = 144$, and gcd (233, 377) = gcd (144,233) = 1. (d) $q_1 = 25$, $r_1 = 26{,}836$, and gcd (34,567; 891,011)= gcd (26,836; 34,567)= 1. (See solution to Question 3.4(d).)

3.4 (a) (12, 20): $20 = 1 \cdot 12 + 8$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4 + 0 \qquad \text{so } \gcd(12, 20) = 4.$$

It took three divisions to find that gcd (12, 20) = 4.

(b) (5,15): $15 = 3 \cdot 5 + 0$ so gcd (5, 15) = 5.

It took one division to find that gcd (5, 15) = 5.

(c) (377,610) $610 = 1 \cdot 377 + 233$

$$377 = 1 \cdot 233 + 144$$

The remaining equations are identical to those in the second part of Example 3.1, so gcd (377, 610) = 1. It took 13 divisions to find that gcd (377, 610) = 1.

(d) (34,567; 891,01 1): 891,011 =25 34,567 + 26,836

$$\begin{aligned}
34{,}567 &= 1 \cdot 26{,}836 + 7731\\
26{,}836 &= 3 \cdot 7731 + 3643\\
7731 &= 2 \cdot 3643 + 445\\
3643 &= 8 \cdot 445 + 83\\
445 &= 5 \cdot 83 + 30\\
83 &= 2 \cdot 30 + 23\\
30 &= 1 \cdot 23 + 7\\
23 &= 3 \cdot 7 + 2\\
7 &= 3 \cdot 2 + 1\\
2 &= 2 \cdot 1 + 0 \qquad \text{so } \gcd(34{,}567;\ 891{,}011) = 1.
\end{aligned}$$

It took 11 divisions to find that gcd (34,567; 891,011) = 1.

3.5 ***(a)*** Algorithm EUCLID run on the pair (6, 20)

Step No.	*b*	*c*	*q*	*r*	gcd
1	6	20		6	
3,4			3	2	
5	2	6			
3,4			3	0	
5					2
6 STOP					

The Euclidean equations are 20 = 3.6 + 2 and 6 = 3 2 + O. Using the first equation, we obtain $2 = -3 \cdot 6 + 1 \cdot 20$.

(b) Algorithm EUCLID run on the pair (3,4):

Step No.	*b*	*c*	*q*	*r*	gcd
1	3	4		3	
3,4			1	1	
5	1	3			
3,4			3	0	
5					1
6 STOP					

The Euclidean equations are $4 = 1 \cdot 3 + 1$ and $3 = 3\ 1 + O$. Using the first equation, we obtain $1 = -1 \cdot 3 + 1 \cdot 4$.

(c) Algorithm EUCLID run on the pair (55, 89):

Step No.	b	c	q	r	gcd
1	55	89		55	
3,4			1	34	
5	34	55			
3,4			1	21	
5	21	34			
3,4			1	13	
5	13	21			
3,4			1	8	
5	8	13			
3,4			1	5	
5	5	8			
3,4			1	3	
5	3	5			
3,4			1	2	
5	2	3			
3,4			1	1	
5	1	2			
3,4			2	0	
5					1
6 STOP					

The Euclidean equations are

1. $89 = 1 \cdot 55 + 34$
2. $55 = 1 \cdot 34 + 21$
3. $34 = 1" 21 + 13$
4. $21 = 1 \cdot 13 + 8$
5. $13 = 1 \cdot 8 + 5$
6. $8 = 1 \cdot 5 + 3$
7. $5 = 1 \cdot 3 + 2$
8. $3 = 1 \cdot 2 + 1$
9. $2 = 2 \cdot 1 + 0.$

We must start with equation 8 and work our way backward to express the gcd as a linear combination of 55 and 89:

$1 = -1 \cdot 2 + 1 \cdot 3 = -1 \cdot (-1 \cdot 3 + 1 \cdot 5) + 1 \cdot 3$	using equation 7
$= 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (-1 \cdot 5 + 1 \cdot 8) - 1 \cdot 5$	using equation 6
$= -3 \cdot 5 + 2 \cdot 8 = -3 \cdot (-1 \cdot 8 + 1 \cdot 13) + 2 \cdot 8$	using equation 5
$= 5 \cdot 8 - 3 \cdot 13 = 5 \cdot (-1 \cdot 13 + 1 \cdot 21) - 3 \cdot 13$	using equation 4
$= -8 \cdot 13 + 5 \cdot 21 = -8 \cdot (-1 \cdot 21 + 1 \cdot 34) + 5 \cdot 21$	using equation 3
$= 13 \cdot 21 - 8 \cdot 34 = 13 \cdot (-1 \cdot 34 + 1 \cdot 55) - 8.34$	using equation 2
$= -21 \cdot 34 + 13 \cdot 55 = -21 \cdot (-1 \cdot 55 + 1 \cdot 89) + 13 \cdot 55$	using equation 1
$= 34.55 - 21.89.$	

SECTION 4

4.1

n	2	3	4	5	6	11	13
F_{n-2}	O	1	1	2	3	34	89
F_{n-1}	1	1	2	3	5	55	144
sum	1	2	3	5	8	89	233

4.2

n	16	17	18	19	20
F_{n-2}	377	610	987	1,597	2,584
F_{n-1}	610	987	1,597	2,584	4,181
sum = F_n	987	1,597	2,584	4,181	6,765
2^n	65,536	131,072	262,144	524,288	1,048,576

In each case listed above, $F_n < 2^n$.

4.3 We claim that the Principle of Complete Induction is valid, by which we mean that if assertions (i) and (ii) are both verified, then the proposition P_n *is* proved for all $n \geq N$: Suppose that we verify (by hand) that $P_N, P_{N+1}, \ldots,$ and P_{N+i} are all true. Then setting $k = N + i$ in (ii) shows that $P_{k+1} = P_{N+i+1}$ *is* true. Then we can repeat (ii) with $k = N + i + 1$. Since we've just demonstrated that $P_N, \ldots, P_{N+i+1}$ are all true, we get that P_{N+i+2} is true, and so on. In general, we can work our way up to the truth of P_n for any integer $n \geq N$.

4.4 Using a calculator, one can check that

$$F_{10} = 55 < (\tfrac{3}{2})^{10} < (\tfrac{3}{2})^{11} < F_{11} = 89.$$

We must prove for $n \geq 11$ that $F_n \geq (\tfrac{3}{2})^n$: For the base cases we notice that

$$F_{11} = 89 > (\tfrac{3}{2})^{11} = 86.4 \ldots$$

and

$$F_{12} = 144 > (\tfrac{3}{2})^{12} = 129.7 \ldots .$$

As in Example 4.2 we require base cases with two consecutive integers (or $j = 1$) because the proof uses the fact that $F_{k+1} = F_k + F_{k-1}$. We use complete induction and so assume that $P_{11}, P_{12}, \ldots P_k$ are all true for some arbitrary value of k. That is, $F_i > (\tfrac{3}{2})^i$ for all $11 \le i \le k$. Notice that $i \ge 11$, since otherwise the claim that $F_i > (\tfrac{3}{2})^i$ *is* not true. We must prove that $F_{k+1} > (\tfrac{3}{2})^{k+1}$.

$$\begin{aligned} F_{k+1} = F_k + F_{k-1} &> (\tfrac{3}{2})^k + (\tfrac{3}{2})^{k-1} \qquad \text{by inductive hypothesis} \\ &= (\tfrac{3}{2})^{k-1}(\tfrac{3}{2} + 1) > (\tfrac{3}{2})^{k-1} \text{“} (\tfrac{9}{4}) = (\tfrac{3}{2})^{k+1}. \end{aligned}$$

Thus $F_n > (\tfrac{3}{2})^n$ for all $n \ge 11$.

4.5 We begin with the equation x – 1 = l/x and multiply both sides by x to obtain $X^2 - x = 1$ or $X^2 - x - 1 = O$. Using the quadratic formula, we find the roots to be $(1 + \sqrt{5})/2 = \phi$ and $(1 - \sqrt{5})/2 = \phi'$. Since these are not zero, they are also solutions to the original equation. Alternatively,

$$\begin{aligned} \frac{1}{\phi} &= \frac{2}{1+\sqrt{5}} = \frac{2(1 \ -\&)}{(1+\sqrt{5})(1-\sqrt{5})} \\ &= \frac{2(1-\sqrt{5})}{1-5} = \frac{1-\sqrt{5}}{-2} \cdot \frac{-1+\sqrt{5}}{2} \\ &- \frac{1+\sqrt{5}}{2} - 1 = \phi - 1. \end{aligned}$$

4.6 $$\begin{aligned} \frac{\phi^2 - \phi'^2}{\sqrt{5}} &= \frac{((1+\sqrt{5})/2)^2 - ((1-\sqrt{5})/2)^2}{\sqrt{5}} \\ &- \frac{(1+2\sqrt{5}+5)/4 - (1-2\sqrt{5}+5)/4}{\sqrt{5}} \\ &\cdot \frac{4\sqrt{5}/4}{\sqrt{5}} = 1 = F_2. \end{aligned}$$

4.7 The algorithm segment

Set $C := A + B$

Set $B := A$

Set $A := C$

placed inside the appropriate loop will calculate Fibonacci numbers if A and B are initially assigned the values F_1 and F_0, respectively. This uses three memory locations. It is possible to use only two memory locations with the segment

Set $B := A + B$

Set $A := A + B$

placed inside the appropriate loop.

SECTION 5

5.1 **(i)** $c = F_8 = 21$ and $b = F_7 = 13$

$$
\begin{aligned}
21 &= 1 \cdot 13 + 8, && q_1 = 1, r_1 = 8\\
13 &= 1 \cdot 8 + 5, && q_2 = 1, r_2 = 5\\
8 &= 1 \cdot 5 + 3, && q_3 = 1, r_3 = 3\\
5 &= 1 \cdot 3 + 2, && q_4 = 1, r_4 = 2\\
3 &= 1 \cdot 2 + 1, && q_5 = 1, r_5 = 1\\
2 &= 2 \cdot 1 + 0, && q_6 = 2, r_6 = 0
\end{aligned}
$$

(ii) $c = F_{10} = 55$ and $b = F_9 = 34$

$$
\begin{aligned}
55 &= 1 \cdot 34 + 21, && q_1 = 1, r_1 = 21\\
34 &= 1 \cdot 21 + 13, && q_2 = 1, r_2 = 13\\
21 &= 1 \cdot 13 + 8, && q_3 = 1, r_3 = 8
\end{aligned}
$$

... as in the preceding part.

5.2 The maximum number of Euclidean equations occurs when $b = 3$ and $c = 5$, and this number is three.

5.3 If $b = 77$ and $c = 185$, the first two Euclidean equations are
1. $185 = 2 \cdot 77 + 31, \quad q_1 = 2, r_1 = 31$
2. $77 = 2 \cdot 31 + 15, \quad q_2 = 2, r_2 = 15$

5.4 (When $b = 26$ and $c = 32$. there is no value of t such that r_{2t+2} and r_{2t} are defined.) When $b = 233$ and $c = 377$, the largest integer t for which r_{2t+2} is defined is $t = 5$. Thus we compute the quantity r_{2t+2}/r_{2t} for $t = 1, 2, 3, 4, 5$: $r_4/r_2 = \frac{34}{89}$, $r_6/r_4 = \frac{13}{34}$, $r_8/r_6 = \frac{5}{13}$, $r_{10}/r_8 = \frac{2}{5}$, and $r_{12}/r_{10} = 0$. These fractions are all less than $\frac{1}{2}$.

SECTION 6

6.1 *(a)* False, (b) False, (c) False, *(d)* True, (e) True, and *(f)* True. An integer is congruent to O modulo 2 if and only if it is even. [1] = {1,4, –2, 7, –5, 10,...} = {1 + *3k: k is* an integer}.

6.2 *(a)* $n+ i$, *(b)* $-n+$ i.

6.3 (i) $a \equiv a$ (mod n):

Proof. $a - a = O = O" n$. Since a – a is divisible by n, we have a $\equiv a$ (mod n). ☐

(ii) If $a \equiv b$ (mod n), then $b \equiv a$ (mod n)

Proof. If $a \equiv b$ (mod n), then there is an integer i such that $(a - b) = in$. But then $(b - a) = - in$, which implies that $b - a$ *is* divisible by n. Thus $b \equiv a$ (mod n). ❑

6.4 Both $\leq$ and $\subseteq$ are relations on Z and on all subsets of Z, respectively. If two numbers are called related when their difference is even, then this gives a relation on Z, but not on *R*, since we do not know what it means for an arbitrary real number to be even.

6.5 **(i)** Given that $a \equiv$ c (mod n) and $b \equiv d$ (mod n), *we* know that there exist integers i and j such that $a = c + in$ and $b = d + jn$. Thus

$$a + b = c + d + in + jn = c + d + (i + j)n.$$

Thus $a + b - (c + d)$ is divisible by n and so a + $b \equiv c + d$ (mod n). ☐
(ii) Proceedings in(i) we have $a - b = c - d + in - jn$. Thus $a - c - (b - d)$ is divisible by n and so $a - c \equiv b - d$ (mod n). ☐

6.6 If x is in [a] and y is in *[b]*, then

$$a \equiv x \pmod{n} \quad \text{and} \quad b \equiv y \pmod{n}.$$

By Lemma 6.3, part (iii)

$$ab \equiv xy \pmod{n} \quad \text{and} \quad [ah] = [xy].$$

Thus multiplication is well defined.

6.7 **(i)** $a = 3, b = 4, c = 8, d = 9$, and $n = 5$. Note that $a \cdot b = 3 \cdot 4 = 12 \equiv$ 2 (mod 5) and that c. $d = 8 \cdot 9 = 72$-2 (mod 5). Further, 3 $\equiv$ 8 (mod 5) and gcd (3,5) = 1. Finally, 4-9 (mod 5).
(ii) $a = 3, b = 4, c = 15, d = 8$, and $n = 12$. Note that $ab = 3 . 4$- *0* (mod 12) and that $c \cdot$ d = 15.8 = 120= O (mod 12). Further, gcd (3, 12) = 3. and 4 $\not\equiv$ 8 (mod 12).

6.8 (a) All nonzero elements of Z_5 have multiplicative inverses: [1][1] = [I], [2][3] = [3][2] = [6] = [1], and [4][4] = [16] = [I]. (b) Since 10 is not a prime number, only numbers relatively prime to 10 have multiplicative inverses, namely 1,3,7,9: [1][1] = [1], [3][7] = [7][3] = [21] = [1], and [9][9] = [81] = [I]. (c) The elements of Z_{18} that have inverses are the numbers relatively prime to 18: [1], [5], [7], [11], [13], [17].

6.9 If p = 11 and b =4, the equivalence classes (mod 11) are [4], [2 .4] = [8], [3 · 4] = [12] = [1], [4 · 4] = [16] = [5], [5 · 4] = [20] = [9], [6 · 4] = [24] = [2], [7 · 4] = [28] = [6], [8 · 4] = [32] = [10], [9 · 4] = [36] = [3], [10 · 4] = [40]= [7]. We also note that

$$4^{11-1} = 4^{10} = 1{,}048{,}576 = 1 + 95{,}325.11 \equiv 1 \pmod{11}.$$

Finally, if c = 11, $11^{10} \equiv$ O (mod 11).

SECTION 7

7.1 In ASCII "HOWDY" = 7279876889. The message 83858270327383328580 represents "SURF IS UP."

7.2 ZZ produces 9090. With B = 4 the smallest number is 3232.

7.3 *(a)* 323 = 17 · 19, **(*b*)** 4087=61 · 67, and (c) 8633=89 · 97.

7.4 Here are all numbers between 2 and 76 that are relatively prime to 607,11, 13,17,19,23,29,31,37,41,43,47,49, 53,59,61,67,71,73.

7.5 We know that 9991 = 97 · 103. To show that gcd (7676, 9991) = 1 and that gcd (7932, 9991) = 1 we check that neither 97 nor 103 divides 7676 or 7932. Next we calculate R_2 and R_3:

$$R_2 \equiv M_2^{11} \equiv M_2 M_2^2 M_2^8 \pmod{9991}.$$
$$M_2^2 \equiv 7676^2 \equiv 58920976 \equiv 4049 \pmod{9991}.$$
$$M_2^4 \equiv 4049^2\text{-}16394401\text{-}9161 \pmod{9991}.$$
$$M_2^8 \equiv 9161^2 \equiv 83923921 \equiv 9512 \pmod{9991}.$$

Thus $R_2 \equiv$ 7676 · 4049-9512 ≡ 9884 (mod 9991).

$$R_3 \equiv M_3^{11} \equiv M_3 M_3^2 M_3^8 \pmod{9991}.$$
$$M_3^2 \equiv 7932^2 \equiv 62916624 \equiv 3297 \pmod{9991}.$$
$$M_3^4 \equiv 3297^2 \equiv 10870209 \equiv 1 \pmod{9991}.$$
$$M_3^8 \equiv 1^2 \equiv 1 \pmod{9991}.$$

Thus $R_3 \equiv$ 7932 · 3297 · 1-5357 (mod 9991).

7.6 Assume that there are 30 days = 30.24.60 = 43,200 minutes in a month. Then to check all N B digit numbers from O to N with e = 11 requires roughly

N15B2 = $10^{B+1}15B^2$ single-digit operations. The problem can be restated as follows: For what value of B is $10^{B+1}15B^2/17{,}800 \geq 43{,}200$? The answer is $B \geq 6$. Thus in order to keep Eve calculating for a month, the value of N must be at least 10^7.

7.7 The multiplicative inverse (mod 8) of e = 7 is d = 7. The encryption of 2: $2^7 = 128 \equiv 8$ (mod 15). The decryption of 8:87 = 2097152-2 (mod 15). The encryption of 7: $7^7 = 823543 \equiv 13$ (mod 15). The decryption of 13: 137 = $62748517 \equiv 7$ (mod 15).

7.8 First we show that $R_2^{4451} \equiv M_2$:

$R_2^{4451} \equiv (9884^{4096})$ (9884256)(988464)(988432)(98842)(9884)

With a total of 12 multiplications we find

$$9884^2 \equiv 97693456\text{-}1458 \pmod{9991}$$
$$9884^4 \equiv 1458^2 \pmod{9991}$$
$$\text{-}2125764 \pmod{9991} \equiv 7672 \pmod{9991}$$
$$9884^8 \equiv 7672^2 \pmod{9991}$$
$$\equiv 58859584 \pmod{9991} \equiv 2603 \pmod{9991}$$
$$9884^{16}\text{-}26032 \pmod{9991}$$
$$\equiv 6775609 \pmod{9991} \equiv 1711 \pmod{9991}$$
$$9884^{32} \equiv 1711^2 \pmod{9991}$$
$$\equiv 2927521 \pmod{9991} \equiv 158 \pmod{9991}$$
$$9884^{64} \equiv 158^2 \pmod{9991}$$
$$\equiv 24964 \pmod{9991} \equiv 4982 \pmod{9991}$$
$$9884^{128} \equiv 4982^2 \pmod{9991}$$
$$\equiv 24820324 \pmod{9991} \equiv 2680 \pmod{9991}$$
$$9884^{256}\text{-}268^0{}_2 \pmod{9991}$$
$$\equiv 7182400 \pmod{9991} \equiv 8862 \pmod{9991}$$
$$9884^5 12\text{-}8862^2 \pmod{9991}$$
$$\equiv 78535044 \pmod{9991} \equiv 5784 \pmod{9991}$$
$$9884^{1024} \equiv 5784^2 \pmod{9991}$$
$$\equiv 33454656 \pmod{9991} = 4788 \pmod{9991}$$
$$9884^{2048} \equiv 4788^2 \pmod{9991}$$
$$\equiv 22924944 \pmod{9991} \equiv 5590 \pmod{9991}$$
$$9884^{4096}\text{-}55^9{}_0 2 \pmod{9991}$$
$$\equiv 31248100 \pmod{9991} = 6243 \pmod{9991}$$

With five more multiplications we find

$$
\begin{aligned}
9884^{4451} &\equiv 6243 \cdot 8862 \cdot 4982 \cdot 158 \cdot 1458 \cdot 9884 \pmod{9991} \\
&\equiv (6243 \cdot 8862) \cdot (4982 \cdot 158) \cdot (1458 \cdot 9884) \pmod{9991} \\
&\equiv 5299 \cdot 7858 \cdot 3850 \pmod{9991} \\
&\equiv (5299 \cdot 7858) \cdot 3850 \pmod{9991} \\
&\equiv 7045 \cdot 3850 \pmod{9991} \\
&\equiv 27123250 \pmod{9991} \\
&\equiv 7676 \pmod{9991} \\
&= M_2.
\end{aligned}
$$

Next we show that $R_3^{4451} \equiv M_3$:

$$
R_3^{4451} \equiv (5357^{4096})(5357^{256})(5357^{64})(5357^{32})(5357^{2})(5357)
$$

With a total of two multiplications we find that

$$
\begin{aligned}
5357^2 &\equiv 28697449 \equiv 3297 \pmod{9991} \\
5357^4 &\equiv 3297^2 \pmod{9991} \\
&\equiv 10870209 \pmod{9991} = 1 \pmod{9991}
\end{aligned}
$$

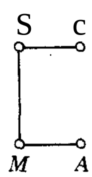
All of the remaining powers of 5357 will equal 1 modulo 9991. Then with one more multiplication we find that

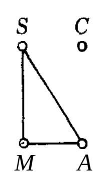
$$
\begin{aligned}
R_3^{4451} &\equiv 5357^{4451} \pmod{9991} \\
&\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 3297 \cdot 5357 \pmod{9991} \\
&\equiv 17662029 \pmod{9991} \\
&\equiv 7932 \pmod{9991} \\
&= M_3.
\end{aligned}
$$

SOLUTIONS TO QUESTIONS IN CHAPTER 5

SECTION 1

1.1 There are $\binom{4}{2} = 6$ pairs of possible direct connections among the four buildings A, C, M, and S. At least three direct connections are needed so that communication is possible between every pair of buildings. Not every set of three direct connections will ensure that each pair of buildings can communicate. See the following illustrations.



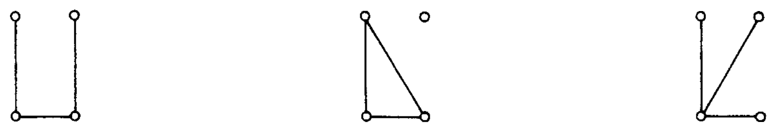


There are $\binom{5}{2} = 10$ pairs of possible direct connections among five buildings. At least four direct connections are required to ensure communications among every pair of buildings. Not every set of four direct connections will guarantee communications between each pair of buildings. See the following illustrations.

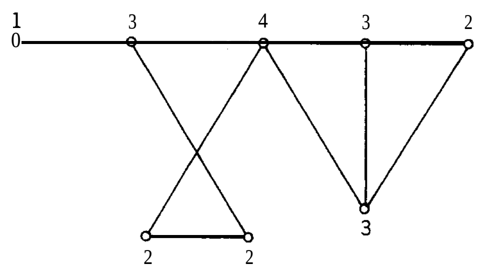
1.2 There are 16 possible LAN configurations. Four of these have one building directly linked to each of the other three buildings. In the remaining 12 the buildings are linked in a path of three cables. By checking all possibilities, one can determine that joining Stoddard with each of the other three buildings has a minimum total cost of $148,000. Note that the total cost with Stoddard is less than the cost without it.

SECTION 2

2.1 Here are three graphs with $V = 4$ and $E = 3$.

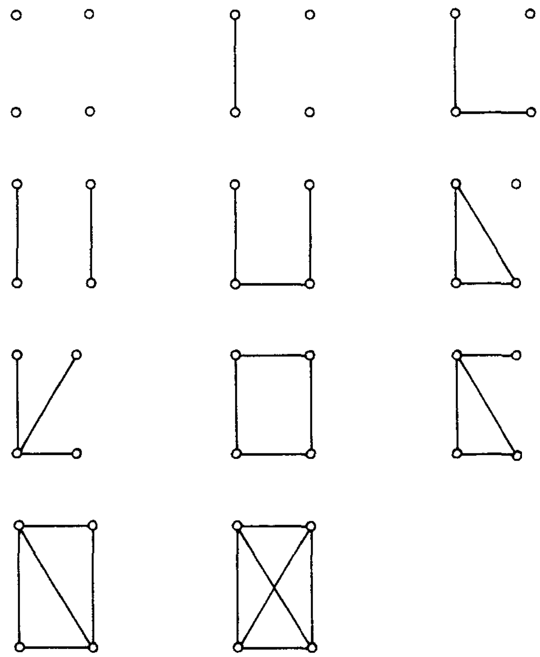


2.2 We display the graph in Figure 5.4 with each vertex labeled with its degree: $V = 8$, $E = 10$, and the sum of the degrees of all the vertices is 20.

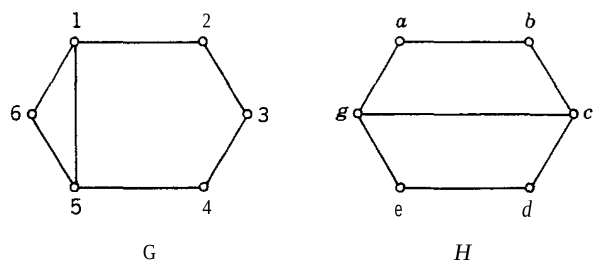


2.3 From Theorem 2.1 the sum of all of the degrees is an even number. The contribution to this sum made by the vertices of even degree is even. Therefore the contribution to this sum made by the vertices of odd degree also must be even. The only way this can occur is if the number of odd vertices is even.

2.4 The 11 different graphs on 4 vertices are as follows. (Note that in the solution to Question 2.1 we listed all different graphs with $V = 4$ and $E = 3$.)



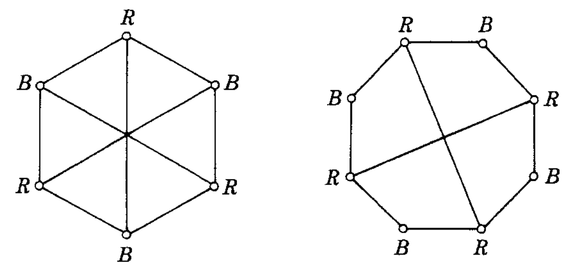
2.5 We show the graphs, G and H, from Figure 5.7 with each vertex labeled, and then proceed with an adjacency argument.



If f were an isomorphism from G to H, it would satisfy the relation deg (x, G) = deg $(f(x), H)$ for each vertex x of G. Thus we must have that $f(1)$ = g or c and $f(5) = c$ or g. Without loss of generality, we choose $f(1) = g$ and $f(5)$ = c. The question is, what is $f(6)$? (This is where we get stuck and can conclude that G and H are not isomorphic.) In order to preserve adjacency, f must map the vertex 6 to a vertex in H that is adjacent to both *f*(1) = g and ~(5)= c. But there is no vertex in *H* that is adjacent to both g and c. Thus we cannot find $f:$ V(G) $\rightarrow V(H)$ that satisfies property (ii) of the definition of isomorphic. Therefore, G is not isomorphic to *H*.

2.6 From Theorem 2.2, *K,* contains 7(7 – 1)/2 = 21 edges.

2.7 The graph shown in (a) is bipartite. The vertices are labeled with *R* and *B*. To see why the graph in (b) is not bipartite, attempt to label the vertices with *R* and *B*. There is essentially only one way of doing this, by alternating *R* with *B* around the outside cycle. When we do this, we see that some *Rs* are adjacent to other *Rs.*

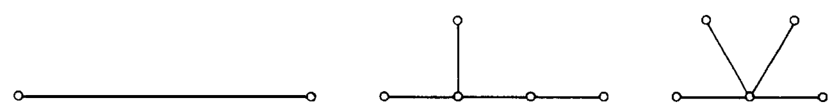


(a) Bipartite (b) Not bipartite

SECTION 3

3.1 A path of length 5 from *a* to *b* is given by <a, *x*, *r*, *e*, *w*, *b*). A path of length 3 from *z* to *r* is given by (z, *a*, *x*, *r*). A 4-cycle ‘through *b is* given by *(b*, *w*, *c*, *z*, *b*).

3.2 The three different trees on five vertices are



3.3 A tree on six vertices must contain five edges, regardless of the particular tree. (Move on to Theorem 3.1 for a proof of this fact.)

3.4 A set of 40 buildings with every pair connected by coaxial cable can be thought of as a 40-clique. From Theorem 2.2, a 40-clique contains 40(40 – 1)/2 = 780 edges, or in this case, cables. A good guess as to the minimum number of cables needed to connect 40 buildings is 39. The reasoning behind this guess is as follows: A graph that models the LAN (i) should be connected (since every pair of buildings must be able to communicate), and (ii) should not contain any cycles (since these introduce unnecessary connections). Thus the model for the LAN that uses the fewest number of edges is a tree with 40 vertices, which necessarily has 39 edges.

3.5 **(a)** The forest in Figure 5.15 contains 5 components, 14 vertices and 9 edges. Thus $E = V - C$. **(b)** Let the component trees be labeled $T_1, T_2, \ldots, T_C$ with the number of vertices and edges of each component given by $V_1, V_2, \ldots, V_C$ and $E_1, E_2, \ldots, E_C$, respectively. Then, in total, $E = E_1 + E_2 + \cdots + E_C$ and $V = V_1 + V_2 + \cdots + V_C$. Since each component is a tree, we know that $E_i = V_i - 1$ for $i = 1,2,. ... C$. Our goal is to compute E, the total number of edges in the forest F, and we hope the result will be that $E = V - C$:

$$E = E_1 + E_2 + \cdots + E_C = (V_1 - 1) + (V_2 - 1) + \cdots + (V_C - 1)$$
$$= V_1 + V_2 + \cdots + V_C - (1 + 1 + \cdots + 1) = V - C.$$

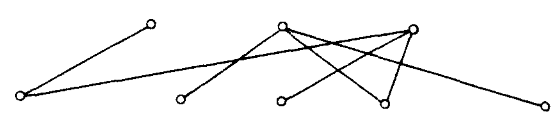
3.6 We shall show that after the removal of edge e, every pair of vertices in the graph G – e is still connected by some path, and thus the graph G – e is connected.

Proof. Suppose that e is an edge of the cycle C. Pick two vertices, say z and w in $V(G)$. Since G is connected, there is a path $P = P(z, w)$ from z to w. If P does not include e, then there is a path from z to w in G — e. Otherwise, P uses e and thus intersects with C. Suppose that u is the first vertex of P that is a vertex of C and u is the last vertex of P that is a vertex of C. Thus P consists of three segments, $P(z, u)$ from z to u, $P(u, v)$ from u to U, and $P(v, w)$ from v to w. If u = v, then we can construct a new path P' consisting of $P(z, u)$ followed by $P(v, w)$. P' is a path from z to w in G – e. If $u \# v$, then within C there is a path $P^{\#}$ that joins u with v but does not contain the edge e. Let P' consist of $P(z, u)$ followed by $P^{\#}$ followed by $P(v, w)$. P' *is* a path from z to w in G – e. Thus G – e is connected. ❑

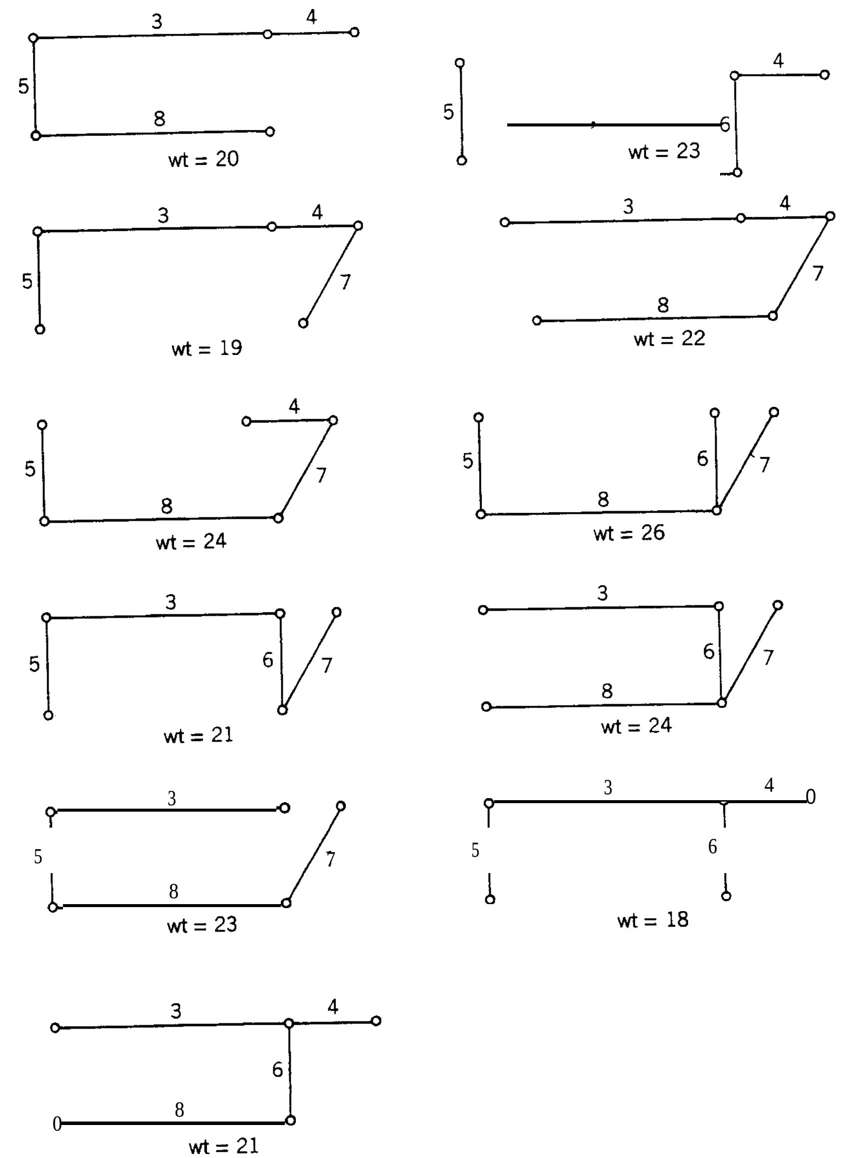
3.7 A connected graph with V vertices and $V - 1$ edges is a tree.

Proof. If G is acyclic, then by definition, G is a tree. If G contains a cycle, by the preceding question it is possible to remove an edge from G, leaving a connected graph. Continue removing edges from cycles until you are left with a connected, acyclic graph. Such a graph has $V — 1$ edges, the original number of edges. Thus no edges were removed, there can be no cycle in G, and G is a tree. ❑

3.8 One possible spanning tree of the graph in Figure 5.19 is as follows.

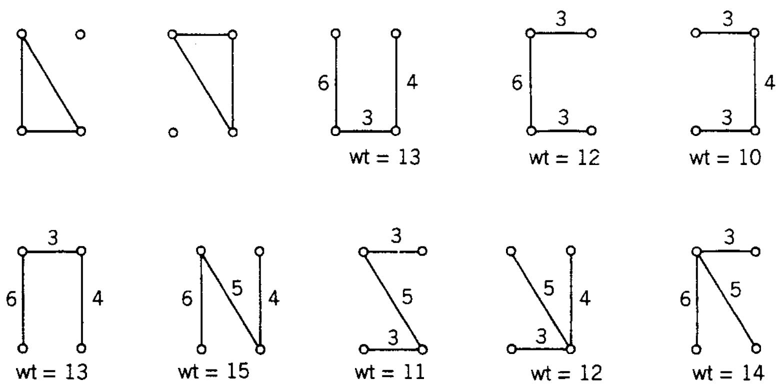


3.9 All spanning trees of the graph shown in Figure 5.21, along with the weight of each, are as follows.



3.10 Algorithm BADMINTREE run on the graph in Figure 5.22:
Steps 2 and 3. A list of all subsets of the edges of the graph in Figure 5.22

with exactly three edges follows. For those graphs that are trees, we give the total weight:



Step *4*. The spanning tree of minimum weight is the tree shown above whose weight is 10.

3.11 $V = 3$: $\binom{3(3-1)/2}{3-1} = \binom{3}{2} = 3$

$V=4$: $\binom{4(4-1)/2}{4-1} = \binom{6}{3} = 20$

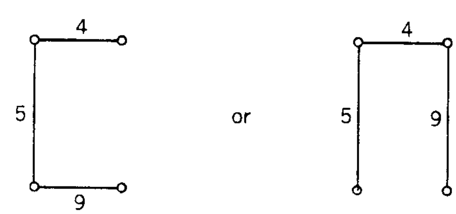
$V=5$: $\binom{5(5-1)/2}{5-1} = \binom{10}{4} = 210$

$V = 6$: $\binom{6(6-1)/2}{6-1} = \binom{15}{5} = 3003$

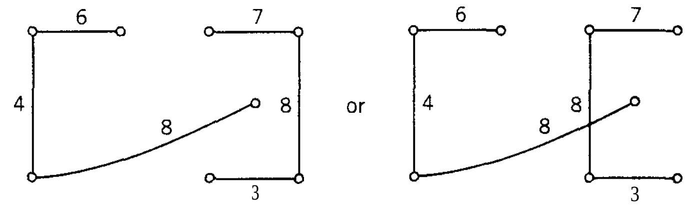
$V = 7$: $\binom{7(7-1)/2}{7-1} = \binom{21}{6} = 54264$

SECTION 4

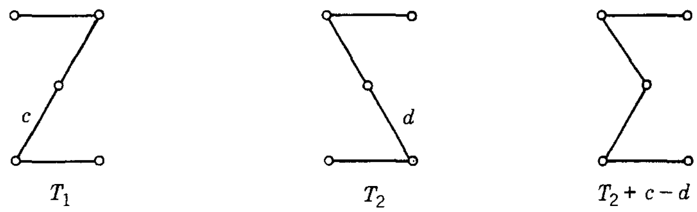
4.1 (a) The result of running KRUSKAL on the first graph in Figure 5.24.



(b) The result of running KRUSKAL on the second graph in Figure 5.24 is a spanning forest. KRUSKAL reports failure, since the graph is not connected.



4.2 We show T_1 and T_2 labeled with c and d, respectively, and then we exhibit the graph $T_2 + c - d$. (Note that this is only one of several ways of choosing c and d.)



4.3 Since $E = O(V^2)$, $O(E^2) + O(EV) = O((V^2)^2) + O(V^2V) = O(V^4) + O(V^3) = O(V^4)$. Similarly, $O(E\log(E)) = O(V^2\log(V^2)) = O(V^2\log(V))$.

4.4 (a) $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ (b) $\begin{vmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{vmatrix}$

4.5

(a) (b)

4.6 If $f(n) = O(n^k)$, there are constants C and N such that

$$\begin{aligned} f(n) &\leq Cn^k && \text{for all } n \geq N \\ &= C(B^{1/2})^k && \text{since } B = n^2 \\ &= C(B^{k/2}) \\ &. \ O(B^{k/2}). \end{aligned}$$

SECTION 5

5.1 *Algorithm GREED YMAX*

STEP 1. Order the objects of E in order of decreasing weight; assume E contains m objects $e_1, \ldots, e_m$

STEP 2. Set j:= 1 {j will index the objects.}

STEP 3. Set T to be empty {T will contain the desirable subset being created.}

STEP 4. Repeat
Begin
STEP 5. If $T + e_j$ is desirable, set $T := T + e_j$
STEP 6. $j := j + 1$
End
Until j > m

STEP 7. Output T and stop.

If E is the set of weighted edges in a graph and desirability is defined as being acyclic, then the algorithm GREEDYMAX adds the heaviest weight edges to T unless a cycle is formed. Thus at the end T contains a maximum weight spanning forest.

5.2 *Algorithm GREED YCYCLE*

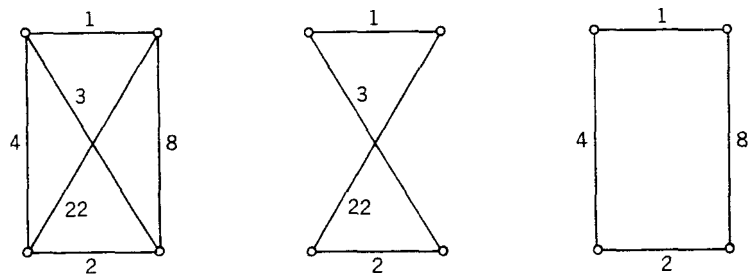
STEP 1. Set C to be empty; set j: = O

STEP 2. Repeat
Begin
STEP 3. Find the lightest edge e such that C + e is a path; set $C := C + e$
STEP 4. Set $j := j + 1$
End
Until $j = V - 1$

STEP 5. Set C : = C + (x, y), where x and y are the end vertices of the path of C

STEP 6. Output C and stop.

An example of a weighted K_4 followed by the result of running GREEDYCYCLE on this K_4 with $V = 4$ is shown in the following figure. The final graph shown is the true minimum weight 4-cycle.



K_4 Result of GREEDYCYCLE True minimum-weight 4-cycle

SOLUTIONS TO QUESTIONS IN CHAPTER 6

SECTION 1

1.1 (a) 1, the social security number might be first in the card file. (b) 20, the social security number might be last in the card file. (c) On average you might expect the director to check about one-half or (1 + 20)/2 = 10.5 cards.

1.2 (a) To find the card with the social security number that is alphabetically *first* in the card file, the director must make one comparison. To find the card with the social security number that is alphabetically second in the card file, the director must make two comparisons. In general, to find the card that is alphabetically in the ith position in the card file, the director must make i comparisons. In total, the director must make

$$1 + 2 + 3 + \cdots + 19 + 20 = \frac{20(20 + 1)}{2} = 210 \text{ comparisons.}$$

(b) It takes 420 seconds = 7 minutes to make all the comparisons. It takes 20 minutes to record all the information. Thus the director spends more time recording than comparing.

1.3 The director will have to examine all cards to be certain of finding the one with the smallest social security number. Thus it will require 19 comparisons if she compares the first card with the second, the smaller with the third, the smallest with the fourth, and so on.

1.4 Trace of Algorithm SELECTSORT run on {6,4,2, 3}:

Step No.	*i*	*j*	a_1	a_2	a_3	a_4	*TN*
4	1	2	6	4	2	3	6
5	1	2	6	6	2	3	4
4	1	3	6	6	2	3	4
5	1	3	6	6	4	3	2
4	1	4	6	6	4	3	2
5	1	4	6	6	4	3	2
6	1	4	2	6	4	3	2
2, 3, 4	2	3	2	6	4	3	6
5	2	3	2	6	6	3	4
4	2	4	2	6	6	3	4
5	2	4	2	6	6	4	3
6	2	4	2	3	6	4	3
2, 3, 4	3	4	2	3	6	4	6
5	3	4	2	3	6	6	4
6	3	4	2	3	4	6	4
7 STOP							

SECTION 2

2.1

$n =$	136	68	34	17	9	5	3
$\lfloor (n+1)/2 \rfloor =$	68	34	17	9	5	3	2

2.2 If n is odd, then there are exactly (n – 1)/2 records before and after the mth record. Otherwise, if n is even, there are $n/2-1$ records before the mth record and $n/2$ after it. The largest number of records that still must be searched is no more than $n/2$.

2.3

pair =	(6,8)	(lo, 17)	(18,33)	(35,67)	(69, 136)
mid =	7	13	25	51	102

2.4 A = (2,3,5,7,11,13, 17,19)

(a) Trace of algorithm BINARYSEARCH run with S = 5:

Step No.	*first*	*last*	*mid*	a_{mid}
4	1	8	4	7
5	1	8	4	7
6	1	3	4	7
4,5	1	3	2	3
6	3	3	2	3
4	3	3	3	5
5 Found S at location 3 and STOP.				

We examined and compared S with three entries of *A*.

(b) With S = 10:

Step No.	*first*	*last*	*mid*	a_{mid}
4, 5	1	8	4	7
6	5	8	4	7
4,5	5	8	6	13
6	5	5	6	13
4, 5	5	5	5	11
6	5	4	5	11
7 S is not in *A* and STOP.				

We examined three elements in *A*.

(c) With S = 17:

Step No.	*first*	*last*	*mid*	a_{mid}
4,5	1	8	4	7
6	5	8	4	7
4,5	5	8	6	13
6	7	8	6	13
4	7	8	7	17
5 Found S at location 7 and STOP.				

We compared S with three entries of *A*.

2.5

n	S	$3\lfloor \log(n) \rfloor + 4$	*Array*	*No. of Comparisons Required*
2	3	7	<1,2)	7
2	1	7	(1,2)	2
3	4	7	(1,2,3)	7
3	2	7	(1,2,3)	2
4	5	10	(1,2,3,4)	10
4	2	10	(1,2,3,4)	2

2.6 (a) Because SEQSEARCH sequentially searches the card file, 1000 comparisons are required in the worst case, the case where the card being searched for is last in the file. (b) From Theorem 2.1, BINARYSEARCH requires at most $3\lfloor \log(1000) \rfloor + 4 = 31$ comparisons.

SECTION 3

3.1 Trace of algorithm BININSERT run on A = (2,5,7,9, 13,15, 19)

(a) With $D = 1$

Step No.	*first*	*last*	*mid*	a_{mid}	*A*
1	1	7	?	?	(2,5,7,9,13,15,19,1)
3	1	7	4	9	
4	1	3	4	9	
3	1	3	2	5	
4	1	1	2	5	
3	1	1	1	2	
4	1	0	1	2	
8	1				(2,2,5,7,9, 13,15, 19⟩
9	1				(1,2,5,7,9, 13, 15,19)

(*b*) With $D = 4$

Step No.	*first*	*last*	*mid*	a_{mid}	*A*
1	1	7	?	?	⟨2, 5, 7, 9, 13,15, 19, 4⟩
3	1	7	4	9	
4	1	3	4	9	
3	1	3	2	5	
4	1	1	2	5	
3	1	1	1	2	
4	2	1	1	2	
8	2				(2, 5,5.7,9,13,15. 19)
9	2				<2,4,5,7,9,13,15, 19)

(c) With $D = 14$

Step No.	*first*	*last*	*mid*	a_{mid}	*A*
1	1	7	?	?	(2, 5,7,9,13,15,19, 14)
3	1	7	4	9	
4	5	7	4	9	
3	5	7	6	15	
4	5	5	6	15	
3	5	5	5	13	
4	6	5	5	13	
8	6				(2,5,7,9, 13,15,15, 19)
9	6				(2,5,7,9, 13,14,15, 19)

(d) With $D = 23$

Step No.	*first*	last	*mid*	a_{mid}	*A*
1	1	7	?	?	(2, 5,7,9,13,15, 19,23)
3	1	7	4	9	
4	5	7	4	9	
3	5	7	6	15	
4	7	7	6	15	
3	7	7	7	19	
4	8	7	7	19	
5	8				(2,5,7,9, 13,15,19,23>

3.2 Trace of BININSERT with A = (2,5,9, 13,15,19, 16):

Step No.	*first*	*last*	*mid*	a_{mid}	*A*
1	1	7	?	?	(2,5,7,9, 13,15,19, 16)
3	1	7	4	9	
4	5	7	4	9	
3	5	7	6	15	
4	7	'7	6	15	
3	7	7	7	19	
4	7	6	7	19	
8	7				(2,5,7,9, 13,15,19, 19)
9	7				(2,5,7,9,13,15,16,19)

Trace of BINARYSEARCH with $A = (2,5,7,9, 13,15, 19)$ and $S = 16$:

Step No.	*first*	*last*	*mid*	a_{mid}
4,5	1	7	4	9
6	5	7	4	9
4,5	5	7	6	15
6	7	7	6	13
4,5	7	7	7	19
6	7	6	7	19
7 S is not in A				

The algorithm BININSERT is an extended version of BINARYSEARCH. The variables in the algorithm take on exactly the same values and similar comparisons of elements are made. However, instead of just announcing that "S is not in A," BININSERT continues by shifting part of A and inserting S into the array A.

3.3 Trace of BINARYSORT with $A = (13, 23,17,19,18, 28)$:

Step No.	*m*	*n*	*A*
1	?	6	<13,23,17,19, 18,28)
2	2		
3			(13,23, 17,19, 18,28)
2	3		
3			(13,17,23,19,18,28)
2	4		
3			(13, 17,19,23, 18,28)
2	5		
3			(13, 17,18, 19,23,28)
2	6		
3			(13, 17,18, 19,23,28)

3.4 In BININSERT every execution of step 2, except for the final one, forces an execution of step 4. Steps 2 and 4 each require one comparison. The final execution of step 2 requires one additional comparison and step 5 requires one additional comparison. In total then, BININSERT requires 2(the number of executions of step 4) + 2. In each part of Question 3.1, step 4 is executed three times. Thus the total number of comparisons is $2 \cdot 3 + 2 = 8$. Further,

$$8 \leq 2\lfloor \log(7) \rfloor + 4 = 2 \cdot 2 + 4 = 8.$$

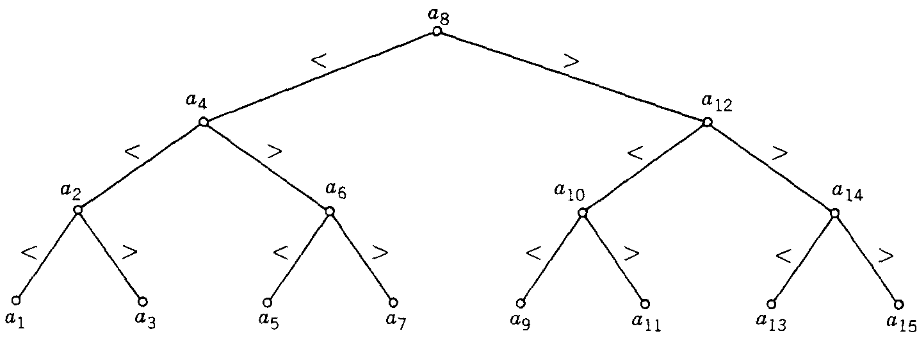
3.5 In Question 3.3, BINARYSORT is performed on an array of size 6. Within BINARYSORT, the procedure BININSERT is called five times on arrays of sizes 2,3,4,5 and 6, respectively. From Theorem 3.1 we have that BININSERT requires at most $2\lfloor \log(r) \rfloor + 4$ comparisons to insert the $(r+1)$st item into a sorted array of r items. Thus the total number of comparisons in Question 3.3 is given by

$$(2\lfloor \log(1) \rfloor + 4) + (2\lfloor \log(2) \rfloor + 4) + (2\lfloor \log(3) \rfloor + 4) + (2\lfloor \log(4) \rfloor + 4) + (2\lfloor \log(5) \rfloor + 4) = 4 + 6 + 6 + 8 + 8 = 32.$$

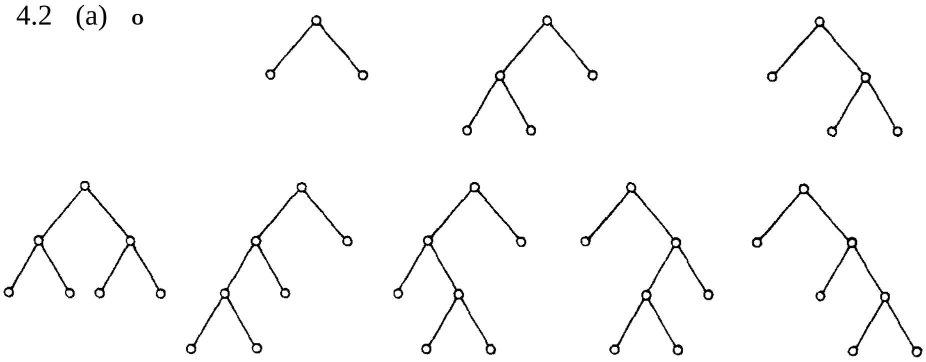
Note that when $n = 6$, $(n-1)(2\lfloor \log(n-1) \rfloor + 4) = 5(2\lfloor \log(5) \rfloor + 4) = 40$.

SECTION 4

4.1 A search tree illustrating a binary search of an array of 15 elements follows.



4.2 (a) o



(b) There is one binary tree with two leaves: the one above with three vertices. There are two binary trees with three leaves: These are the binary trees with