PART 3

GRAPH THEORY

AND

APPLICATIONS

CHAPTER 11
AN INTRODUCTION TO GRAPH THEORY

Section 11.1

1. (a) To represent the air routes traveled among a certain set of cities by a particular airline.
(b) To represent an electrical network. Here the vertices can represent switches, transistors, etc., and an edge (x, y) indicates the existence of a wire connecting x to y.
(c) Let the vertices represent a set of job applicants and a set of open positions in a corporation. Draw an edge (A,b) to denote that applicant A is qualified for position b. Then all open positions can be filled if the resulting graph provides a matching between the applicants and open positions.

2. (a) $\{b, e\}, \{e, f\}, \{f, g\}, \{g, e\}, \{e, b\}, \{b, c\}, \{c, d\}$
(b) $\{b, e\}, \{e, f\}, \{f, g\}, \{g, e\}, \{e, d\}$
(c) $\{b, e\}, \{e, d\}$
(d) $\{b, e\}, \{e, f\}, \{f, g\}, \{g, e\}, \{e, b\}$
(e) $\{b, e\}, \{e, f\}, \{f, g\}, \{g, e\}, \{e, d\}, \{d, c\}, \{c, b\}$
(f) $\{b, a\}, \{a, c\}, \{c, b\}$

3. 6

4. We claim that $\kappa(G) = 2$. To verify this consider the following:
(1) Let C_1 be the set of all vertices $v \in V$ where the binary label of v has an even number of 1s. This includes the vertex z whose binary label is the n-tuple of all 0s. For any $v_0 \in C_1$, where $v_0 \neq z$, we can find a path from v_0 to z as follows. Suppose that the binary label for v_0 has $2m$ 1s, where $2 \leq 2m \leq n$. Change the first two 1s in the binary label for v_0 to 0s and call the resulting vertex v_1. Then $v_1 \in C_1$ and $\{v_0, v_1\} \in E$. Now change the first two 1s in the binary label for v_1 to 0s and call the resulting vertex v_2. Once again $v_2 \in C_1$ and $\{v_0, v_1\} \in E$. Continuing this process we reach the vertex $v_m = z$ and find that $\{v_{m-1}, v_m\} \in E$, with $v_{m-1} \in C_1$. Hence each of the vertices in $C_1 - \{z\}$ is connected to z.

(2) Now let C_2 be the set of all vertices $w \in V$ where the binary label for w has an odd number of 1s. Let $z^* \in C_2$ where the binary label for z^* consists of a 1 followed by $n-1$ 0s. For each $w_0 \in C_2$, $w_0 \neq z^*$, one of two possibilities can occur:

(i) There are $2m+1$ 1s in the binary label for w_0, with $3 \leq 2m+1 \leq n$, and the first entry in the label for w_0 is 1. Here we change the next two 1s in the binary label for w_0 to 0s and obtain the vertex $w_1 \in C_2$ with $\{w_0, w_1\} \in E$. Now the first entry in the binary label

for w_1 is a 1 and upon changing the second and third 1s in this label to 0s we obtain the vertex $w_2 \in C_2$ with $\{w_1, w_2\} \in E$. Continuing this process we reach the vertex $w_m = z^*$ with $w_{m-1} \in C_2$ and $\{w_{m-1}, w_m\} \in E$. Consequently each vertex in $C_2 - \{z^*\}$ whose binary label starts with 1 is connected to z^*.
(ii) There are $2m+1$ 1s in the binary label for w_0, with $3 \leq 2m+1 \leq n$, and the first entry in the label for w_0 is 0. Change the first entry in the binary label for w_0 to 1 and the first 1 in the binary label for w_0 to 0. This results in the vertex $w_1 \in C_2$ with $\{w_0, w_1\} \in E$. Upon changing the second and third 1s in the binary label for w_1 to 0s we obtain the vertex $w_2 \in C_2$ with $\{w_1, w_2\} \in E$. Continuing this process we reach the vertex $w_{m+1} = z^*$ with $\{w_m, w_{m+1}\} \in E$. This shows that each vertex in C_2 whose binary label starts with 0 is also connected to z^*.

(3) We claim that the components of G are the graphs determined by C_1 and C_2. Can there exist an edge $\{x, y\} \in E$ where $x \in C_1$, $y \in C_2$? Here the binary label for x has an even number of 1s while the label for y has an odd number of 1s. This contradicts the definition of E – for if $\{a, b\} \in E$ then the total number of 1s in the binary labels for a, b is even.

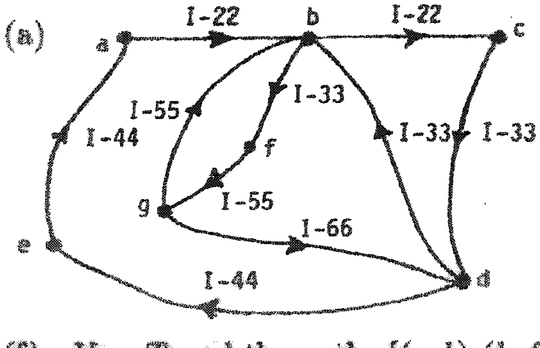
5. Each path from a to h must include the edge $\{b, g\}$. There are three paths (in G) from a to b and three paths (in G) from g to h. Consequently, there are nine paths from a to h in G.

There is only one path of length 3, two of length 4, three of length 5, two of length 6, and one of length 7.

6.

c: 1	e: 1	f: 1	g: 2	h: 3
i: 4	j: 3	k: 2	l: 3	m: 3

7. (a)



(b) $\{(g, d), (d, e), (e, a)\}$;
$\{(g, b), (b, c), (c, d), (d, e), (e, a)\}$.
(c) Two: One of $\{(b, c), (c, d)\}$ and one of $\{(b, f), (f, g), (g, d)\}$.
(d) No
(e) Yes: Travel the path $\{(c, d), (d, e), (e, a), (a, b), (b, f), (f, g)\}$.
(f) Yes: Travel the path $\{(g, b), (b, f), (f, g), (g, d), (d, b), (b, c), (c, d), (d, e), (e, a), (a, b)\}$.

8. The smallest number of guards needed is 3 - e.g., at vertices a, g, i.

9. If $\{a, b\}$ is not part of a cycle, then its removal disconnects a and b (and G). If not, there is a path P from a to b and P, together with $\{a, b\}$, provides a cycle containing $\{a, b\}$.
Conversely, if the removal of $\{a, b\}$ from G disconnects G then there exist $x, y \in V$ such that the only path P from x to y contains $e = \{a, b\}$. If e were part of a cycle

C, then the edges in $(P - \{e\}) \cup (C - \{e\})$ would provide a second path connecting x to y.

10. Any path. **11.** (a) Yes (b) No (c) $n-1$

12. (a) In a loop-free undirected graph (that is not a multigraph) the maximum number of edges is $\binom{v}{2}$. Hence $e \leq \binom{v}{2} = v(v-1)/2$, so $2e \leq v^2 - v$.

(b) In a loop-free directed graph (that is not a multigraph), $e \leq v^2 - v$.

13. This relation is reflexive, symmetric and transitive, so it is an equivalence relation. The partition of V induced by $\mathcal{R}$ yields the (connected) components of G.

14. (a) There are three cycles of length 4 in W_3, five cycles of length 4 in W_4, and five such cycles in W_5.
(b) Denote the consecutive cycle (rim) vertices of W_n by $v_1, v_2, \ldots, v_n$ and the additional (central) vertex by v_{n+1}.

(i) For $n \neq 4$, there are n cycles of length 4:
(1) $v_1 \to v_2 \to v_3 \to v_{n+1} \to v_1$;
(2) $v_2 \to v_3 \to v_4 \to v_{n+1} \to v_2$;
$\ldots$;
$(n-1)$ $v_{n-1} \to v_n \to v_1 \to v_{n+1} \to v_{n-1}$; and
(n) $v_n \to v_1 \to v_2 \to v_{n+1} \to v_n$.

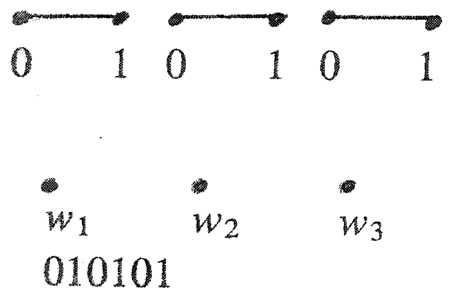
When $n = 4$ the vertices v_1, v_2, v_3, v_4 provide a cycle. The other four cycles of length 4 consist of vertex v_5 and three of the four vertices v_1, v_2, v_3, v_4.

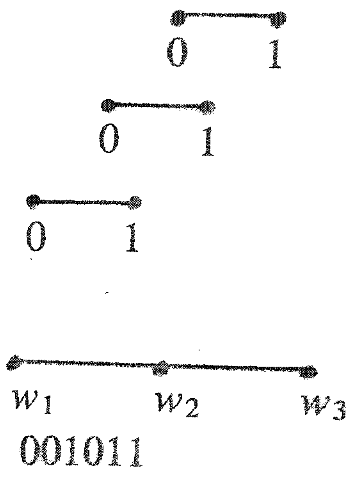
(ii) There are $n+1$ cycles of length n in W_n:
(1) $v_1 \to v_2 \to v_3 \to \ldots \to v_{n-1} \to v_n \to v_1$;
(2) $v_1 \to v_{n+1} \to v_3 \to v_4 \to \ldots \to v_{n-1} \to v_n \to v_1$;
(3) $v_2 \to v_{n+1} \to v_4 \to v_5 \to \ldots \to v_{n-1} \to v_n \to v_1 \to v_2$;
$\ldots$;
(n) $v_{n-1} \to v_{n+1} \to v_1 \to v_2 \to \ldots \to v_{n-3} \to v_{n-2} \to v_{n-1}$; and
$(n+1)$ $v_n \to v_{n+1} \to v_2 \to v_3 \to \ldots \to v_{n-3} \to v_{n-1} \to v_n$.

15. For $n \geq 1$, let a_n count the number of closed $v-v$ walks of length n (where, in this case, we allow such a walk to contain or consist of one or more loops). Here $a_1 = 1$ and $a_2 = 2$. For $n \geq 3$ there are a_{n-1} $v-v$ walks where the last edge is the loop $\{v, v\}$ and a_{n-2} $v-v$ walks where the last two edges are both $\{v, w\}$. Since these two cases are exhaustive and have nothing in common we have $a_n = a_{n-1} + a_{n-2}$, $n \geq 3$, $a_1 = 1$, $a_2 = 2$.

We find that $a_n = F_{n+1}$, the $(n+1)$st Fibonacci number.

16. a) There are two other unit-interval graphs for three unit intervals.





b) For four unit intervals there are 14 unit-inteval graphs.

c) For $n \geq 1$, there are $b_n = \frac{1}{n+1}\binom{2n}{n}$ unit-interval graphs for n unit intervals. Here b_n is the nth Catalan number. The binary representations set up a one-to-one correspondence with the situations in Example 1.40 – in particular, change 0 to 1 and 1 to 0 in part (b) of Example 1.40 to obtain the binary representations of the 14 unit-interval graphs on four unit intervals.

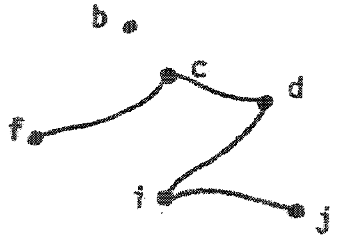
Section 11.2

1. (a) Three: (1) $\{b,a\},\{a,c\},\{c,d\},\{d,a\}$
(2) $\{f,c\},\{c,a\},\{a,d\},\{d,c\}$
(3) $\{i,d\},\{d,c\},\{c,a\},\{a,d\}$

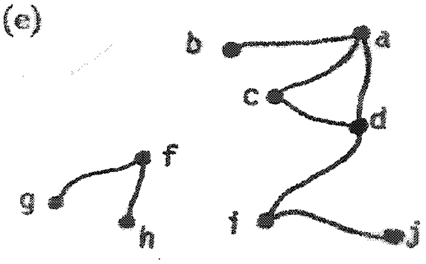
(b) G_1 is the subgraph induced by $U = \{a,b,d,f,g,h,i,j\}$
$G_1 = G - \{c\}$

(c) G_2 is the subgraph induced by $W = \{b,c,d,f,g,i,j\}$
$G_2 = G - \{a,h\}$

(d)



(e)



2. (a) G_1 is *not* an induced subgraph of G if there exists an edge $\{a,b\}$ in E such that

$a, b \in V$, but $\{a, b\} \notin E_1$.

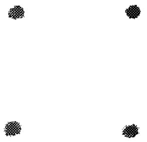
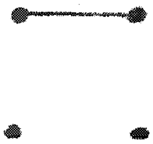
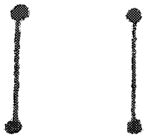
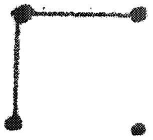
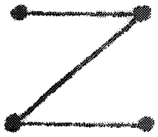
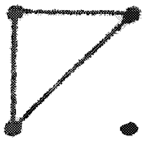
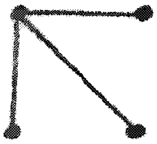
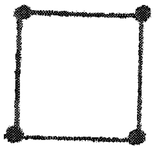
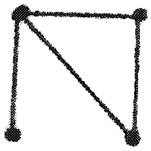
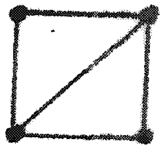
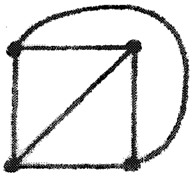
(b) Let $e = \{a, d\}$. Then $G - e$ is a subgraph of G but it is not an induced subgraph.

3. (a) There are $2^9 = 512$ spanning subgraphs.
(b) Four of the spanning subgraphs in part (a) are connected.
(c) 2^6

4. There is only one – the graph G itself.

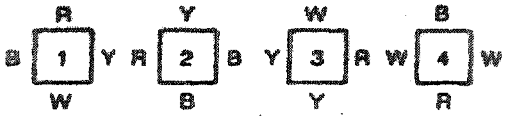
5. G is (or is isomorphic to) the complete graph K_n, where $n = |V|$.

6. There are 11 loop-free nonisomorphic undirected graphs with four vertices.

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

(10)

(11)


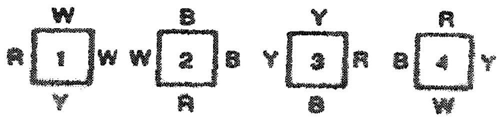
Six of these graphs are connected.

7. (a)



(b) No solution.

(c)



8. (a) There are $(1/2)(7)(6)(5)(4)(3) = 1260$ paths of length 4 in K_7.
(b) The number of paths of length m in K_n, for $0 < m < n$, is $(1/2)(n)(n-1)(n-2)\cdots(n-m)$.

9. (a) Each graph has four vertices that are incident with three edges. In the second graph

these vertices (w,x,y,z) form a cycle. This is not so for the corresponding vertices (a,b,g,h) in the first graph. Hence the graphs are *not* isomorphic.

(b) In the first graph the vertex d is incident with four edges. No vertex in the second graph has this property, so the graphs are *not* isomorphic.

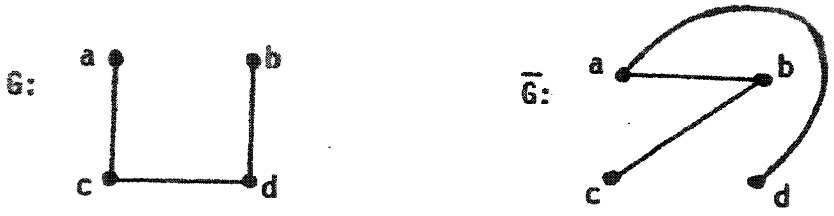
10. If G has v vertices and e edges, then by the definition of $\overline{G}$, there are $\binom{v}{2} - e$ edges in $\overline{G}$ since there are $\binom{v}{2}$ edges in K_v.

11. (a) If $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic, then there is a function $f : V_1 \longrightarrow V_2$ that is one-to-one and onto and preserves adjacencies. If $x, y \in V_1$ and $\{x, y\} \notin E_1$, then $\{f(x), f(y)\} \notin E_2$. Hence the same function f preserves adjacencies for $\overline{G}_1, \overline{G}_2$ and can be used to define an isomorphism for $\overline{G}_1, \overline{G}_2$. The converse follows in a similar way.

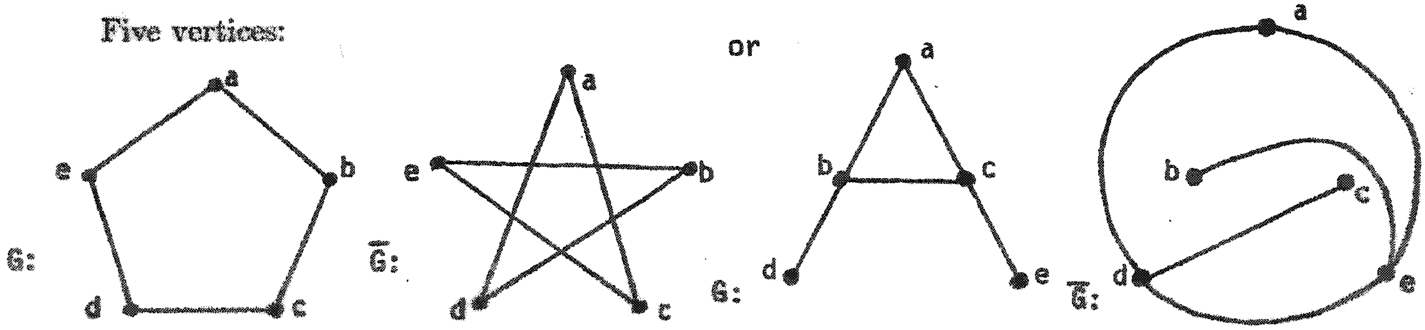
(b) They are not isomorphic. The complement of the graph containing vertex a is a cycle of length 8. The complement of the other graph is the disjoint union of two cycles of length 4.

12. (a) Let e_1 be the number of edges in G and e_2 the number in $\overline{G}$. For any (loop-free) undirected graph G, $e_1 + e_2 = \binom{n}{2}$, the number of edges in K_n. Since G is self-complementary, $e_1 = e_2$, so $e_1 = (1/2)\binom{n}{2} = n(n-1)/4$.

(b) Four vertices:

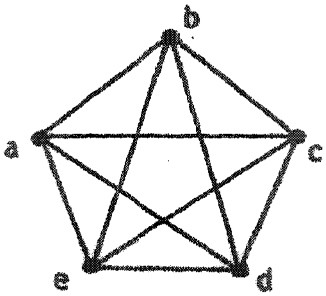


Five vertices:



(c) From part (a), $4|n(n-1)$. One of n and $n-1$ is even and the other factor odd. If n is even, then $4|n$ and $n = 4k$, for some $k \in \mathbf{Z}^+$. If $n-1$ is even, then $4|(n-1)$ and $n - 1 = 4k$, or $n = 4k + 1$, for some $k \in \mathbf{Z}^+$.

13. If G is the cycle with edges $\{a,b\},\{b,c\},\{c,d\},\{d,e\}$ and $\{e,a\}$, then $\overline{G}$ is the cycle with edges $\{a,c\}$, $\{c,e\}$, $\{e,b\}$, $\{b,d\}$, $\{d,a\}$. Hence, G and $\overline{G}$ are isomorphic. Conversely, if G is a cycle on n vertices and $G,\overline{G}$ are isomorphic, then $n=(1/2)\binom{n}{2}$, or $n=(1/4)(n)(n-1)$, and $n=5$.



14. (a) All of the examples in Exercise 12 above satisfy these conditions.
(b) Since G is not connected, there exist vertices x,y and no path in G connecting these vertices. Hence $\{x,y\}$ is an edge in $\overline{G}$. For each vertex a in G, $a\neq x,y$, either $\{a,x\}$ or $\{a,y\}$ is in $\overline{G}$. If not, both $\{a,x\},\{a,y\}$ are in G and $\{x,a\},\{a,y\}$ provide a path in G connecting x and y. Let $b,c\in V$. If $\{b,x\},\{c,x\}$ are both in $\overline{G}$, there is a path connecting b,c: namely, $\{b,x\},\{x,c\}$. The same is true if $\{b,y\},\{c,y\}$ both occur in $\overline{G}$. If neither of these situations occurs we have $\{b,x\},\{c,y\}$ in $\overline{G}$ (or $\{b,y\},\{c,x\}$) and then the edges $\{b,x\},\{x,y\},\{y,c\}$ provide a path connecting b and c.

15. (a) Here f must also maintain directions. So if $(a,b)\in E_1$, then $(f(a),f(b))\in E_2$.

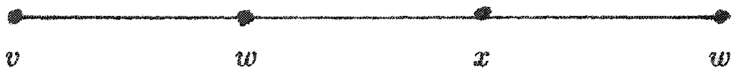
(b) They are not isomorphic. Consider vertex a in the first graph. It is incident to one vertex and incident from two other vertices. No vertex in the other graph has this property.

16. (a) $\binom{6}{3}(2^3)=\binom{6}{3}(2^{\binom{3}{2}})$ (b) $\binom{6}{4}(2^{\binom{4}{2}})$

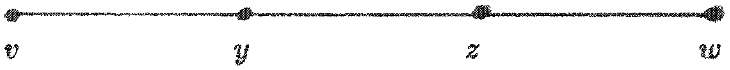
(c) $\sum_{k=1}^{6}\binom{6}{k}(2^{\binom{k}{2}})$ (d) $\sum_{k=1}^{n}\binom{n}{k}(2^{\binom{k}{2}})$

17. There are two cases to consider:

Case 1:



Case 2:



Here there are $n-2$ choices for y – namely, any vertex other than v,w – and there are $n-2$ choices for z – namely, any vertex other than w or the vertex selected for z.

Consequently, there are $(n-1)+(n-2)^2=n^2-3n+3$ walks of length 3 from v to w.

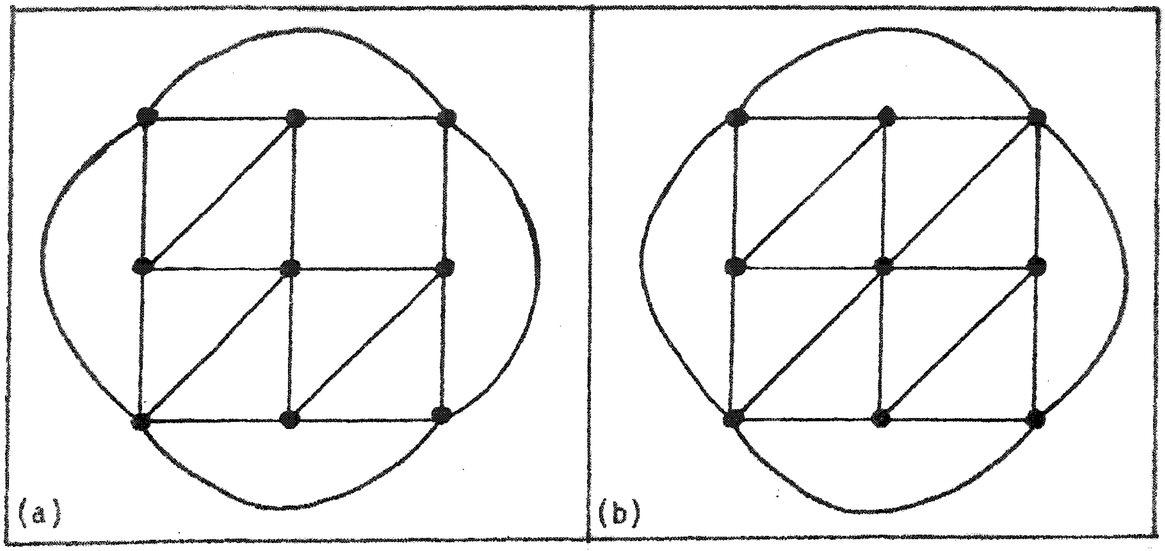
Section 11.3

1. (a) $|V|=6$
(b) $|V|=1$ or 2 or 3 or 5 or 6 or 10 or 15 or 30. [In the first four cases G must be a multigraph; when $|V|=30$, G is disconnected.]

(c) $|V| = 6$

2. $2|E| = 2(17) = 34 = \sum_{v \in V} \deg(v) \geq 3|V|$, so the maximum value of $|V|$ is 11.

3. Since $38 = 2|E| = \sum_{v \in V} \deg(v) \geq 4|V|$, the largest possible value for $|V|$ is 9. We can have (i) seven vertices of degree 4 and two of degree 5; or (ii) eight vertices of degree 4 and one of degree 6. The graph in part (a) of the figure is an example for case (i); an example for case (ii) is provided in part (b) of the figure.



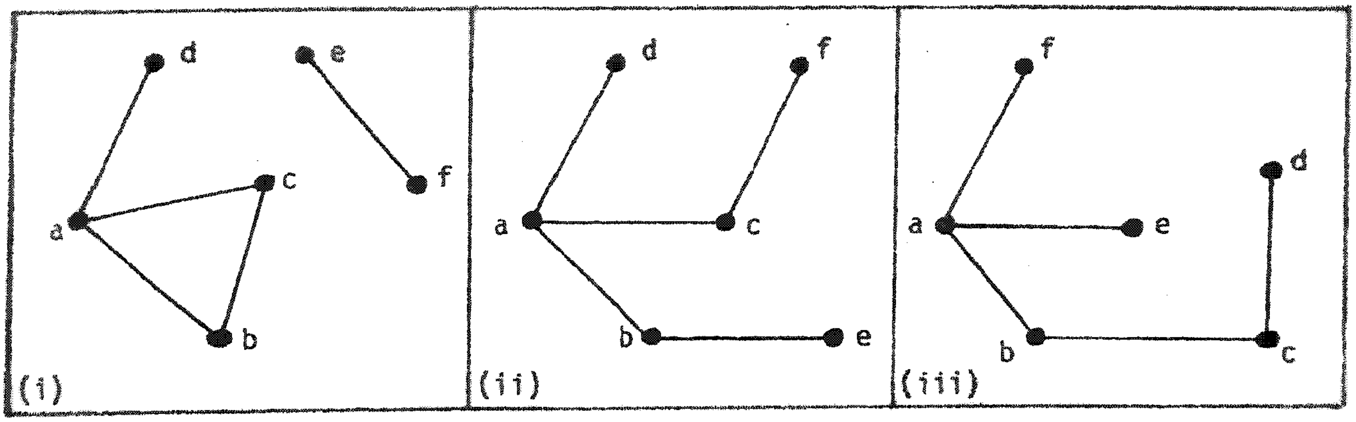
4. a) We must note here that G need *not* be connected. Up to isomorphism G is either a cycle on six vertices or (a disjoint union of) two cycles, each on three vertices.
b) Here G is either a cycle on seven vertices or (a disjoint union of) two cycles — one on three vertices and the other on four.
c) For such a graph G_1, $\overline{G_1}$ is one of the graphs in part (a). Hence there are two such graphs G_1.
d) Here $\overline{G_1}$ is one of the graphs in part (b). There are two such graphs G_1 (up to isomorphism).
e) Let $G_1 = (V_1, E_1)$ be a loop-free undirected $(n-3)$-regular graph with $|V| = n$. Up to isomorphism the number of such graphs G_1 is the number of partitions of n into summands that exceed 2.

5. (a) $|V_1| = 8 = |V_2|$; $|E_1| = 14 = |E_2|$.
(b) For V_1 we find that $\deg(a) = 3$, $\deg(b) = 4$, $\deg(c) = 4$, $\deg(d) = 3$, $\deg(e) = 3$, $\deg(f) = 4$, $\deg(g) = 4$, and $\deg(h) = 3$. For V_2 we have $\deg(s) = 3$, $\deg(t) = 4$, $\deg(u) = 4$, $\deg(v) = 3$, $\deg(w) = 4$, $\deg(x) = 3$, $\deg(y) = 3$, and $\deg(z) = 4$. Hence each of the two graphs has four vertices of degree 3 and four of degree 4.
(c) Despite the results in parts (a) and (b) the graphs G_1 and G_2 are *not* isomorphic.

In the graph G_2 the four vertices of degree 4 — namely, t, u, w, and z — are on a cycle of length 4. For the graph G_1 the vertices b, c, f, and g — each of degree 4 — do not lie on a cycle of length 4.

A second way to observe that G_1 and G_2 are not isomorphic is to consider once again the vertices of degree 4 in each graph. In G_1 these vertices induce a disconnected subgraph consisting of the two edges $\{b, c\}$ and $\{f, g\}$. The four vertices of degree 4 in graph G_2 induce a connected subgraph that has five edges — every possible edge except $\{u, z\}$.

6.



7. a) 19 b) $\sum_{i=1}^{n}\binom{d_i}{2}$ [Note: No assumption about connectedness is made here.]

8. a) There are $8 \cdot 2^7 = 1024$ edges in Q_8.
b) The maximum distance between pairs of vertices is 8. For example, the distance between 00000000 and 11111111 is 8.
c) A longest path in Q_8 contains all of the vertices in Q_8. Such a path has length $2^8 - 1 = 255$.

9. a) $n \cdot 2^{n-1} = 524,288 \Rightarrow n = 16$
b) $n \cdot 2^{n-1} = 4,980,736 \Rightarrow n = 19$, so there are $2^{19} = 524,288$ vertices in this hypercube.

10. The typical path of length 2 uses two edges of the form $\{a, b\}$, $\{b, c\}$. We can select the vertex b as any vertex of Q_n, so there are 2^n choices for b. The vertex b (labeled by a binary n-tuple) is adjacent to n other vertices in Q_n and we can choose two of these in $\binom{n}{2}$ ways. Consequently, there are $\binom{n}{2}2^n$ paths of length 2 in Q_n.

11. The number of edges in K_n is $\binom{n}{2} = n(n-1)/2$. If the edges of K_n can be partitioned into such cycles of length 4, then 4 divides $\binom{n}{2}$ and $\binom{n}{2} = 4t$ for some $t \in \mathbf{Z}^+$. For each vertex v that appears in a cycle, there are two edges (of K_n) incident to v. Consequently, each vertex v of K_n has even degree, so n is odd. Therefore, $n-1$ is even and as $4t = \binom{n}{2} = n(n-1)/2$, it follows that $8t = n(n-1)$. So 8 divides $n(n-1)$, and since n is odd, it follows (from the Fundamental Theorem of Arithmetic) that 8 divides $n-1$. Hence $n - 1 = 8k$, or $n = 8k + 1$, for some $k \in \mathbf{Z}^+$.

12. a) Let $v \in V$. Then $v\mathcal{R}v$ since v and itself have the same bit in position k and the same bit in position ℓ — hence, $\mathcal{R}$ is reflexive. If $v, w \in V$ and $v\mathcal{R}w$ then v, w have the same bit in position k and the same bit in position ℓ. Hence w, v have the same bit in position k and the same bit in position ℓ. So $w\mathcal{R}v$ and $\mathcal{R}$ is symmetric. Finally, suppose that $v, w, x \in V$ with $v\mathcal{R}w$ and $w\mathcal{R}x$. Then v, w have the same bit in position k and the same bit in position ℓ, and w, x have the same bit in position k and the same bit in position ℓ. Consequently, v, x have the same bit in position k and the same bit in position ℓ, so $v\mathcal{R}x$ — and $\mathcal{R}$ is transitive. In so much as $\mathcal{R}$ is reflexive, symmetric and transitive, it follows that $\mathcal{R}$ is an equivalence relation.

There are four blocks for (the partition induced by) this equivalence relation. Each block contains 2^{n-2} vertices; the vertices in each such block induce a subgraph isomorphic to Q_{n-2}.

(b) For $n \geq 1$ let V denote the vertices in Q_n. For $1 \leq k_1 < k_2 < \ldots < k_t \leq n$ and $w, x \in V$ define the relation $\mathcal{R}$ on V by $w\mathcal{R}x$ if w, x have the same bit in position k_1, the same bit in position $k_2, \ldots,$ and the same bit in position k_t. Then $\mathcal{R}$ is an equivalence relation for V and it partitions V into 2^t blocks. Each block contains 2^{n-t} vertices and the vertices in each such block induce a subgraph of Q_n isomorphic to Q_{n-t}.

13. $\delta|V| \leq \sum_{v \in V} \deg(v) \leq \Delta|V|$. Since $2|E| = \sum_{v \in V} \deg(v)$, it follows that
$\delta|V| \leq 2|E| \leq \Delta|V|$ so $\delta \leq 2(e/n) \leq \Delta$.

14. (a) f^{-1} is one-to-one and onto. Let $x, y \in V'$ and $\{x, y\} \in E'$. Then f one-to-one and onto $\Longrightarrow$ there exist unique $a, b \in V$ with $f(a) = x$, $f(b) = y$. If $\{a, b\} \notin E$, then $\{f(a), f(b)\} \notin E'$.

(b) If $\deg(a) = n$, then there exist $x_1, x_2, \ldots, x_n \in V$ and $\{a, x_i\} \in E, 1 \leq i \leq n$. Hence, the edge $\{f(a), f(x_i)\} \in E'$ for all $1 \leq i \leq n$, so $\deg(f(a)) \geq n$. If $\deg(f(a)) > n$, let $y \in V'$ such that $y \neq f(x_i)$ for all $1 \leq i \leq n$, and $y = f(x)$. Since f^{-1} is an isomorphism by part (a), $\{a, x\} \in E$ and $\deg(a) > n$. Hence $\deg f(a) = n$.

15. Proof: Start with a cycle $v_1 \to v_2 \to v_3 \to \ldots \to v_{2k-1} \to v_{2k} \to v_1$. Then draw the k edges $\{v_1, v_{k+1}\}, \{v_2, v_{k+2}\}, \ldots, \{v_i, v_{i+k}\}, \ldots, \{v_k, v_{2k}\}$. The resulting graph has $2k$ vertices each of degree 3.

16. Proof: (By the Alternative Form of the Principle of Mathematical Induction)
The result is true for $n = 1$ (for the complete graph K_2) and for $n = 2$ (for the path on four vertices). So let us assume the result for all $1 \leq n \leq k$, and consider the case for $n = k+1$. Let G' be a graph for $n = k-1$, and add to this graph two isolated vertices x and y. Now introduce two other vertices a and b and the edge $\{a, b\}$. Draw an edge between a and x, and between a and $k-1$ of the vertices (one of each of the degrees $1, 2, \ldots, k-1$) in G'. Now draw an edge between b and y, and between b and the other $k-1$ vertices in G' (the vertices not adjacent to vertex a). The resulting graph has $2(k+1)$ vertices where exactly two vertices have degree i for all $1 \leq i \leq k+1$.
Consequently, the result follows for all $n \in \mathbf{Z}^+$ by the Alternative Form of the Principle of

Mathematical Induction.

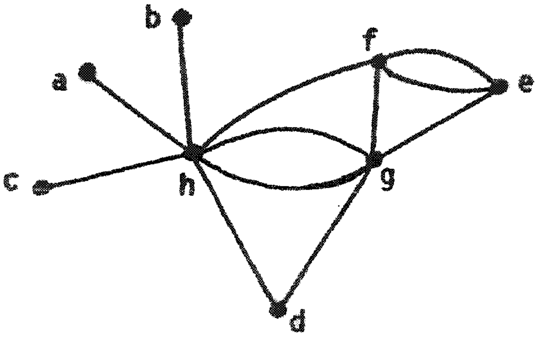
17. (Corollary 11.1) Let $V = V_1 \cup V_2$ where V_1 (V_2) contains all vertices of odd (even) degree. Then $2|E| - \sum_{v \in V_2} \deg(v) = \sum_{v \in V_1} \deg(v)$ is an even integer. For $|V_1|$ odd, $\sum_{v \in V_1} \deg(v)$ is odd.

(Corollary 11.2) For the converse let $G = (V, E)$ have an Euler trail with a, b as the starting and terminating vertices, respectively. Add the edge $\{a, b\}$ to G to form the graph $G' = (V, E')$, where G' has an Euler circuit. Hence G' is connected and each vertex has even degree. Removing edge $\{a, b\}$ the vertices in G will have the same even degree except for a, b. $\deg_G(a) = \deg_{G'}(a) - 1, \deg_G(b) = \deg_{G'}(b) - 1$, so the vertices a, b have odd degree in G. Also, since the edges in G form an Euler trail, G is connected.

18. Select $v_1, v_2 \in V$ where $\{v_1, v_2\} \in E$. Such an edge must exist since $V \neq \emptyset$ and $\deg(v) \geq k \geq 1$ for all $v \in V$. If $k = 1$ the result follows. If $k > 1$, suppose that we have selected $v_1, v_2, \ldots, v_k \in V$ with $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{k-1}, v_k\} \in E$. Since $\deg(v_k) \geq k$, there exists $v_{k+1} \in V_1$ where $v_{k+1} \neq v_i$ for $1 \leq i \leq k-1$, and $\{v_k, v_{k+1}\} \in E$. Then $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{k-1}, v_k\}, \{v_k, v_{k+1}\}$ provides a path of length k.

19. (a) Let $a, b, c, x, y \in V$ with $\deg(a) = \deg(b) = \deg(c) = 1$, $\deg(x) = 5$, and $\deg(y) = 7$. Since $\deg(y) = 7$, y is adjacent to all of the other (seven) vertices in V. Therefore vertex x is not adjacent to any of the vertices a, b, and c. Since x cannot be adjacent to itself, unless we have loops, it follows that $\deg(x) \leq 4$, and we cannot draw a graph for the given conditions.

(b)



20. (a) $a \rightarrow b \rightarrow c \rightarrow g \rightarrow k \rightarrow j \rightarrow g \rightarrow b \rightarrow f \rightarrow j \rightarrow i \rightarrow f \rightarrow e \rightarrow i \rightarrow h \rightarrow d \rightarrow e \rightarrow b \rightarrow d \rightarrow a$

(b) $d \rightarrow a \rightarrow b \rightarrow d \rightarrow h \rightarrow i \rightarrow e \rightarrow f \rightarrow i \rightarrow j \rightarrow f \rightarrow b \rightarrow c \rightarrow g \rightarrow k \rightarrow j \rightarrow g \rightarrow b \rightarrow e$

21. n odd: $n = 2$

22. 1; Any single bridge.

23. Yes. Model the situation with a graph where there is a vertex for each room and the surrounding corridor. Draw an edge between two vertices if there is a door common to both rooms, or a room and the surrounding corridor. The resulting multigraph is connected with every vertex of even degree.

24. We find that $\sum_{v \in V} \text{id}(v) = e = \sum_{v \in V} \text{od}(v)$.

25. (a) (i) Let the vertices of K_6 be $v_1, v_2, v_3, v_4, v_5, v_6$, where $\deg(v_i) = 5$ for all $1 \leq i \leq 6$. Consider the subgraph S of K_6 obtained (from K_6) by deleting the edges $\{v_2, v_5\}$ and $\{v_3, v_6\}$. Then S is connected with $\deg(v_1) = \deg(v_4) = 5$, and $\deg(v_i) = 4$ for $i \in \{2, 3, 5, 6\}$. Hence S has an Euler trail that starts at v_1 (or v_4) and terminates at v_4 (or v_1). This Euler trail in S is then a trail of maximum length in K_6, and its length is $\binom{6}{2} - (1/2)[6-2] = 15 - 2 = 13$.

(ii) $\binom{8}{2} - (1/2)[8-2] = 28 - 3 = 25$

(iii) $\binom{10}{2} - (1/2)[10-2] = 45 - 4 = 41$

(iv) $\binom{2n}{2} - (1/2)[2n-2] = n(2n-1) - (n-1) = 2n^2 - 2n + 1$.

(b) (i) Label the vertices of K_6 as in section (i) of part (a) above. Now consider the subgraph T of K_6 obtained (from K_6) by deleting the edges $\{v_1, v_4\}$, $\{v_2, v_5\}$, and $\{v_3, v_6\}$. Then T is connected with $\deg(v_i) = 4$ for all $1 \leq i \leq n$. Hence T has an Euler circuit and this Euler circuit for T is then a circuit of maximum length in K_6. The length of the circuit is $\binom{6}{2} - (1/2)(6) = 15 - 3 = 12$.

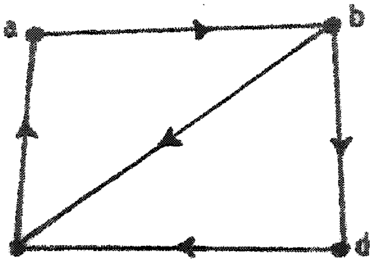
(ii) $\binom{8}{2} - (1/2)(8) = 28 - 4 = 24$

(iii) $\binom{10}{2} - (1/2)(10) = 45 - 5 = 40$

(iv) $\binom{2n}{2} - (1/2)(2n) = n(2n-1) - n = 2n^2 - 2n = 2n(n-1)$.

26. (a) If $G = (V, E)$ has a directed Euler circuit, then for all $x, y \in V$ there is a directed trail from x to y (that part of the directed Euler circuit from x to y). This results in a directed path from x to y , as well as one from y to x . Hence G is connected (in fact, G is strongly connected as defined in part (b) of this exercise). Let s be the starting vertex (and terminal vertex) of the directed Euler circuit. For every $v \in V, v \neq s$, each time the circuit comes upon vertex v it must also leave the vertex, so $\text{od}(v) = \text{id}(v)$. In the case of s the last edge of the circuit is different from the first edge and $\text{od}(s) = \text{id}(s)$.

Conversely, if G satisifies the stated conditons, we shall prove by induction on $|E|$ that G has a directed Euler circuit. For $|E| = 1$ the result is true (and the graph consists of a (directed) loop on one vertex). We assume the result for all such graphs with $|E|$ edges where $1 \leq |E| < n$. Now consider a directed graph $G = (V, E)$ where G satisfies the given conditions and $|E| = n$. Let $a \in V$. There exists a circuit in G that contains a. If the loop $(a, a) \notin E$, then there is an edge $(a, b) \in E$ for $b \neq a$. If not, a is isolated and this contradicts G being connected. If $(b, a) \in E$ we have the circuit $\{(a, b), (b, a)\}$ containing a. If $(b, a) \notin E$, then there is an edge of the form (b, c), $c \neq b$, $c \neq a$, because $\text{od}(b) = \text{id}(b)$. Continuing this process, since $\text{od}(a) = \text{id}(a)$ and G is finite, we obtain a directed circuit C containing a. If $C = G$ we are finished. If not, remove the edges of C from G, along with any vertex that becomes isolated. The resulting subgraph $H = (V_1, E_1)$ is such that (in H) $\text{od}(v) = \text{id}(v)$ for all $v \in V_1$. However, H is not necessarily connected. But each component of H is connected with $\text{od}(v) = \text{id}(v)$ for each vertex in a component. Consequently, by the induction hypothesis, each component of H has a directed Euler circuit, and each component has a vertex on the circuit C (from above). Hence, starting at vertex a we travel on C until we encounter a vertex v_1 on the directed Euler circuit of the component C_1 of H. Traversing C_1 we return to v_1 and continue on C to vertex v_2 on component C_2 of H. Continuing the process, with G finite we obtain a directed Euler circuit for G.

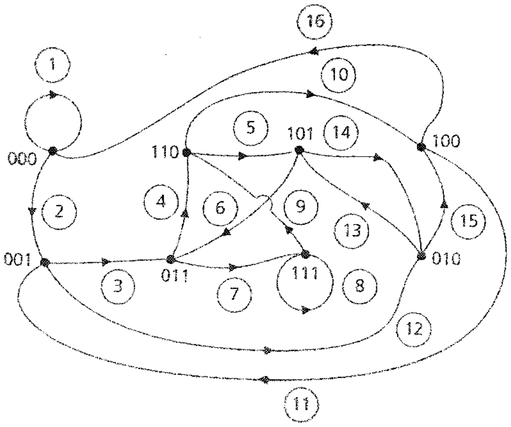


(b) If $G = (V, E)$ is a directed graph with a directed Euler circuit then for all $x, y \in V$, $x \neq y$, there is a directed path from x to y, and one from y to x, so the graph is strongly connected. The converse, however, is false. The directed graph shown here is strongly connected. However, since $\text{od}(b) \neq \text{id}(b)$ the graph does not have a directed Euler circuit.

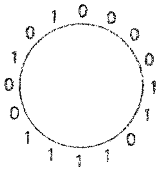
27. From Exercise 24 we see that $\sum_{v \in V}[\text{od}(v) - \text{id}(v)] = 0$. For each $v \in V$, $\text{od}(v) + \text{id}(v) = n - 1$, so $0 = (n-1) \cdot 0 = \sum_{v \in V}(n-1)[\text{od}(v) - \text{id}(v)] = \sum_{v \in V}[\text{od}(v) + \text{id}(v)][\text{od}(v) - \text{id}(v)] = \sum_{v \in V}[(\text{od}(v))^2 - (\text{id}(v))^2]$, and the result follows.

28. Let G be a directed graph satisfying the three conditions. Add the edge (x, y). Then by part (a) of Exercise 26 the resulting graph has a directed Euler circuit C. Removing (x, y) from C yields a directed Euler trail for the given graph G. (This trail starts at y and terminates at x.) In a similar manner we find that if a directed graph G has a directed Euler trail then it satisfies the three conditions.

29. (a) and (b)



(c)



30. 3; 3

31. Let $|V| = n \geq 2$. Since G is loop-free and connected, for all $x \in V$ we have $1 \leq \deg(x) \leq n - 1$. Apply the pigeonhole principle with the n vertices as the pigeons and the $n - 1$ possible degrees as the pigeonholes.

32. (a)

$$A = \begin{array}{c|ccccc|} & v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 1 & 0 & 1 \\ v_2 & 1 & 0 & 1 & 1 & 1 \\ v_3 & 1 & 1 & 1 & 1 & 1 \\ v_4 & 0 & 1 & 1 & 0 & 1 \\ v_5 & 1 & 1 & 1 & 1 & 1 \end{array}$$

$$I = \begin{array}{c|ccccccccccc|} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} & e_{11} \\ v_1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ v_2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ v_3 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ v_4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ v_5 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

(b) If there is a walk of length two between v_i and v_j, denote this by $\{v_i, v_k\}, \{v_k, v_j\}$. Then $a_{ik} = a_{kj} = 1$ in A and the (i,j)-entry in A^2 is 1. Conversely, if the (i,j)-entry of A^2 is 1 then there is at least one value of k, $1 \leq k \leq n$, such that $a_{ik} = a_{kj} = 1$, and this indicates the existence of a walk $\{v_i, v_k\}, \{v_k, v_j\}$ between the ith and jth vertices of V.

(c) For all $1 \leq i, j \leq n$, the (i,j)-entry of A^2 counts the number of distinct walks of length two between the ith and jth vertices of V.

(d) For v at the top of the column, the column sum is the degree of v, if there is no loop at v. Otherwise, $\deg(v) =$ [(column sum for v) $- 1] + 2$ (number of loops at v).

(e) For each column of I the column sum is 1 for a loop and 2 for an edge that is not a loop.

33. (a) Label the rows and columns of the first matrix with a, b, c. Then the graph for this adjacency matrix is a path of two edges where $\deg(a) = \deg(b) = 1$ and $\deg(c) = 2$.

Now label the rows and columns of the second matrix with x, y, z. The graph for this adjacency matrix is a path of two edges where $\deg(y) = \deg(z) = 1$ and $\deg(x) = 2$.

Define $f : \{a, b, c\} \rightarrow \{x, y, z\}$ by $f(a) = y$, $f(b) = z$, $f(c) = x$. This function provides an isomorphism for these two graphs.

Alternatively, if we start with the first matrix and interchange rows 1 and 3 and then interchange columns 1 and 3 (on the resulting matrix), we obtain the second matrix. This also shows us that the graphs (corresponding to these adjacency matrices) are isomorphic.

(b) Yes
(c) No

34. (a) Here each graph is a cycle on three vertices – so they are isomorphic.

(b) The graphs here are not isomorphic. The graph for the first incidence matrix is a cycle of length 3 with the fourth (remaining) edge incident with one of the cycle vertices. The second graph is a cycle on four vertices.
(c) Yes

35. No. Let each person represent a vertex for a graph. If v, w represent two of these people, draw the edge $\{v, w\}$ if the two shake hands. If the situation were possible, then we would have a graph with 15 vertices, each of degree 3. So the sum of the degrees of the vertices would be 45, an odd integer. This contradicts Theorem 11.2.

36. Define the function f from the domain $A \times B$ (or the set of processors of the grid) to the codomain of corresponding vertices of Q_5 as follows:

$$f((ab, cde)) = abcde, \text{ where } ab \in A,\ cde \in B, \text{ and } a, b, c, d, e \in \{0, 1\}.$$

If $f((ab, cde)) = f(a_1b_1, c_1d_1e_1))$, then $abcde = a_1b_1c_1d_1e_1$, so $a = a_1$, $b = b_1$, $c = c_1$, $d = d_1$, $e = e_1$, and $(ab, cde) = (a_1b_1, c_1d_1e_1)$, making f one-to-one. Since $|A \times B| = 15 =$ the number of vertices (of Q_5) in the codomain of f, it follows from Theorem 5.11 that f is also onto.

Now let $\{(ab, cde), (vw, xyz)\}$ be an edge in the 3×5 grid. Then either $ab = vw$ and cde, xyz differ in (exactly) one component or $cde = xyz$ and ab, vw differ in (exactly) one component. Suppose that $ab = vw$ (so $a = v, b = w$) and $c = x$, $d = y$, but $e \neq z$. Then $\{abcde, vwxyz\}$ is an edge in Q_5. [The other four cases follow in a similar way.] Conversely, suppose that $\{f(a_1b_1, c_1d_1e_1), f(v_1w_1, x_1y_1z_1)\}$ is an edge in the subgraph of Q_5 induced by the codomain of f. Then $a_1b_1c_1d_1e_1$ and $v_1w_1x_1y_1z_1$ differ in (exactly) one component – say the last. Then in the 3×5 grid, there is an edge for the vertices (a_1b_1, c_1d_10), $(a_1b_1c_1d_11)$. [Similar arguments can be given for any of the other first four components.] Consequently, f provides an isomorphism between the 3×5 grid and a subgraph of Q_5.

[Note that the 3×5 grid has 22 edges while Q_5 has $5 \cdot 2^4 = 80$ edges.]

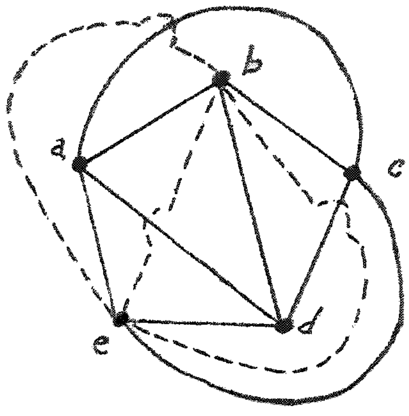
37. Assign the Gray code $\{00, 01, 11, 10\}$ to the four horizontal levels: top – 00; second (from the top) – 01; second from the bottom – 11; bottom – 10. Likewise, assign the same code to the four vertical levels: left (or, first) – 00; second – 01; third – 11; right (or, fourth) – 10. This provides the labels for $p_1, p_2, \ldots, p_{16}$, where, for instance, p_1 has the label $(00, 00)$, p_2 has the label $(01, 00), \ldots, p_7$ has the label $(11, 01), \ldots, p_{11}$ has the label $(11, 10)$, and p_{16} has the label $(10, 10)$.

Define the function f from the set of 16 vertices of this grid to the vertices of Q_4 by $f((ab, cd)) = abcd$. Here $f((ab, cd)) = f((a_1b_1, c_1d_1)) \Rightarrow abcd = a_1b_1c_1d_1 \Rightarrow a = a_1, b = b_1, c = c_1, d = d_1 \Rightarrow (ab, cd) = (a_1b_1, c_1d_1) \Rightarrow f$ is one-to-one. Since the domain and codomain of f both contain 16 vertices, it follows from Theorem 5.11 that f is also onto. Finally, let $\{(ab, cd), (wx, yz)\}$ be an edge in the grid. Then either $ab = wx$ and cd, yz differ in one component or $cd = yz$ and ab, wx differ in one component. Suppose that $ab = wx$ and $c = y$, but $d \neq z$. Then $\{abcd, wxyz\}$ is an edge in Q_4. The other cases follow in a similar way. Conversely, suppose that $\{f((a_1b_1, c_1d_1)), f((w_1x_1, y_1z_1))\}$ is an edge in Q_4. Then $a_1b_1c_1d_1, w_1x_1y_1z_1$ differ in exactly one component – say the first. Then in the grid, there is an edge for the vertices $(0b_1, c_1d_1)$, $(1b_1, c_1d_1)$. The arguments are similar for the other three components. Consequently, f establishes an isomorphism between the three-by-three grid and a subgraph of Q_4.

[Note: The three-by-three grid has 24 edges while Q_4 has 32 edges.]

Section 11.4

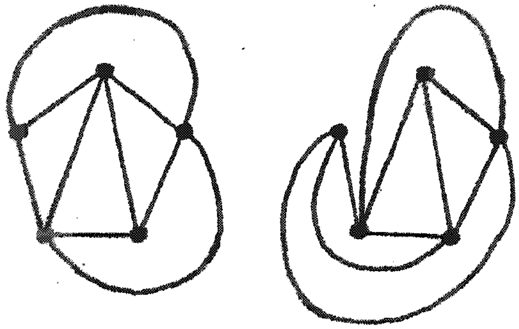
1.



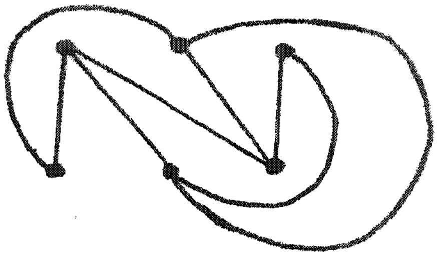
In this situation vertex b is in the region formed by the edges {a,d}, {d,c}, {c,a} and vertex e is outside of this region. Consequently the edge {b,e} will cross one of the edges {a,d}, {d,c}, {a,c} (as shown).

2. From the symmetry in these graphs the following demonstrate the situations we must consider

K_5 :



$K_{3,3}$:



3. (a)

Graph	Number of vertices	Number of edges
$K_{4,7}$	11	28
$K_{7,11}$	18	77
$K_{m,n}$	$m+n$	mn

(b) $m = 6$

4. Let $G = (V, E)$ be bipartite with V partitioned as $V_1 \cup V_2$, so that each edge in E is of the form $\{a, b\}$ where $a \in V_1$, $b \in V_2$. If H is a subgraph of G let W denote the set of vertices for H. Then $W = W \cap V = W \cap (V_1 \cup V_2) = (W \cap V_1) \cup (W \cap V_2)$, where $(W \cap V_1) \cap (W \cap V_2) = \emptyset$. If $\{x, y\}$ is an edge in H then $\{x, y\}$ is an edge in G — where, say, $x \in V_1$ and $y \in V_2$. Hence $x \in W_1$, $y \in W_2$ and H is a bipartite graph.

5. (a) Let $V_1 = \{a, d, e, h\}$ and $V_2 = \{b, c, f, g\}$. Then every vertex of G is in $V_1 \cup V_2$ and $V_1 \cap V_2 = \emptyset$. Also every edge in G may be written as $\{x, y\}$ where $x \in V_1$ and $y \in V_2$. Consequently, the graph G in part (a) of the figure is bipartite.

(b) Let $V_1' = \{a, b, g, h\}$ and $V_2' = \{c, d, e, f\}$. Then every vertex of G' is in $V_1' \cup V_2'$ and $V_1' \cap V_2' = \emptyset$. Since every edge of G' may be written as $\{x, y\}$, with $x \in V_1'$ and $y \in V_2'$, it follows that this graph is bipartite. In fact G' is (isomorphic to) the complete bipartite graph $K_{4,4}$.

(c) This graph is *not* bipartite. If $G'' = (V'', E'')$ were bipartite, let the vertices of G'' be partitioned as $V_1'' \cup V_2''$, where each edge in G'' is of the form $\{x, y\}$ with $x \in V_1''$ and $y \in V_2''$. We assume vertex a is in V_1''. Now consider the vertices b, c, d, and e. Since $\{a, b\}$ and $\{a, c\}$ are edges of G'' we must have b, c in V_2''. Also, $\{b, d\}$ is an edge in the graph, so d is in V_1''. But then $\{d, e\} \in E'' \Rightarrow e \in V_2''$, while $\{c, e\} \in E'' \Rightarrow e \in V_1''$.

6. There are four vertices in $K_{1,3}$ and we can select four vertices from those of K_n in $\binom{n}{4}$ ways. Since each of the four vertices (in each of the $\binom{n}{4}$ selections) can be the unique vertex of degree 3 in $K_{1,3}$, there are $4\binom{n}{4}$ subgraphs of K_n that are isomorphic to $K_{1,3}$.

Alternately, select the vertex of degree 3 in $K_{1,3}$ — this can be done in n ways. Then select the remaining pendant vertices — this can be done in $\binom{n-1}{3}$ ways. Hence the number of subgraphs of K_n that are isomorphic to $K_{1,3}$ is

$$n\binom{n-1}{3} = (n)(n-1)(n-2)(n-3)/6 = (4)[(n)(n-1)(n-2)(n-3)/24] = 4\binom{n}{4}.$$

7. The vertices in $K_{m,n}$ may be partitioned as $V_1 \cup V_2$ where $|V_1| = m$, $|V_2| = n$, and each edge of the graph has the form $\{x, y\}$ where $x \in V_1$ and $y \in V_2$.

(a) In order to obtain a cycle of length four we need to select two vertices from each of V_1 and V_2. This can be done in $\binom{m}{2}\binom{n}{2}$ ways — each resulting in a distinct cycle of length four.
[Note: Say we select vertices a, b from V_1 and vertices c, d from V_2. We do *not* distinguish the cycles $a \rightarrow c \rightarrow b \rightarrow d \rightarrow a$ and $a \rightarrow d \rightarrow b \rightarrow c \rightarrow a$.]
(b) For a path of length two there is one vertex of (path) degree 2 and two vertices of (path) degree 1. If the vertex of (path) degree 2 is in V_1 then there are $m\binom{n}{2}$ such paths. There are $n\binom{m}{2}$ such paths when the vertex of (path) degree 2 is in V_2. Hence there are $m\binom{n}{2} + n\binom{m}{2} = (1/2)(mn)[m + n - 2]$ paths of length 2 in $K_{m,n}$.
(c) Here a path of length 3 has the form $a \rightarrow b \rightarrow c \rightarrow d$ where $a, c \in V_1$ and $b, d \in V_2$. By the rule of product there are $(m)(n)(m-1)(n-1) = 4\binom{m}{2}\binom{n}{2}$ such paths in $K_{m,n}$.

8. (a) 2 (b) 6 $(= 2(3))$ (c) 14 $(= 2(7))$ (d) $2m$

9. (a) 6 (b) $(1/2)(7)(3)(6)(2)(5)(1)(4) = 2520$ (c) 50,295,168,000
(d) $(1/2)(n)(m)(n-1)(m-1)(n-2)\cdots(2)(n-(m+1))(1)(n-m)$

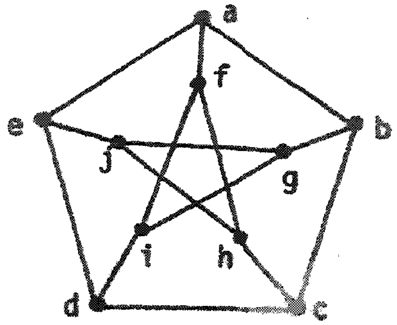
10. Let $G = (V, E)$ be bipartite with $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$. If G has a cycle of odd length then there is an edge in the cycle of the form $\{x, y\}$ with $x, y \in V_1$ (or $x, y \in V_2$). This contradicts the definition of a bipartite graph.

11. Partition V as $V_1 \cup V_2$ with $|V_1| = m$, $|V_2| = v - m$. If G is bipartite, then the maximum number of edges that G can have is $m(v-m) = -[m-(v/2)]^2 + (v/2)^2$, a function of m. For a given value of v, when v is even, $m = v/2$ maximizes $m(v-m) = (v/2)[v-(v/2)] = (v/2)^2$. For v odd, $m = (v-1)/2$ or $m = (v+1)/2$ maximizes $m(v-m) = [(v-1)/2][v-((v-1)/2)] = [(v-1)/2][(v+1)/2] = [(v+1)/2][v-((v+1)/2)] = (v^2-1)/4 = \lfloor (v/2)^2 \rfloor < (v/2)^2$. Hence if $|E| > (v/2)^2$, G cannot be bipartite.

12. (a) There are 3: (i) $K_{1,5}$; (ii) $K_{2,4}$; and (iii) $K_{3,3}$.
(b) $\lfloor n/2 \rfloor$ for $n \in \mathbf{Z}^+$, $n \geq 2$.

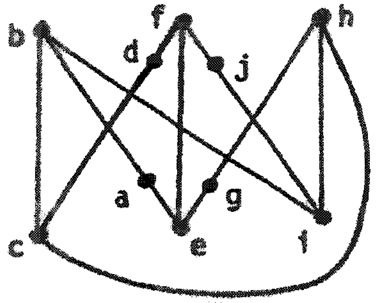
13. (a)

a: {1,2}	f: {4,5}
b: {3,4}	g: {2,5}
c: {1,5}	h: {2,3}
d: {2,4}	i: {1,3}
e: {3,5}	j: {1,4}

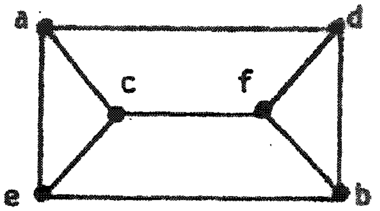


(b) G is (isomorphic to) the Petersen graph. (See Fig. 11.52(a)).

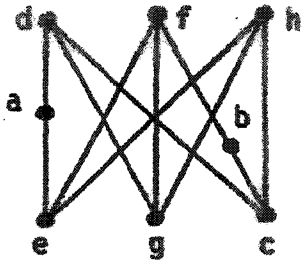
14. (1)



(2)

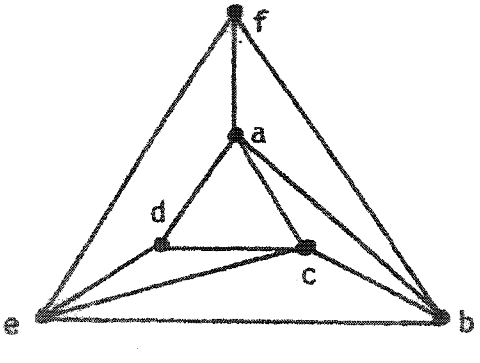


(3)

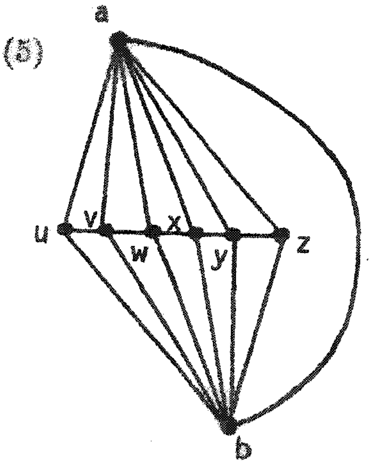


Graph (1) shows that the first graph contains a subgraph homeomorphic to $K_{3,3}$, so it is not planar. The second graph is planar and isomorphic to the second graph of the exercise. The third graph provides a subgraph homeomorphic to $K_{3,3}$ so the third graph given here is not planar. Graph (6) is not planar because it contains a subgraph homeomorphic to K_5.

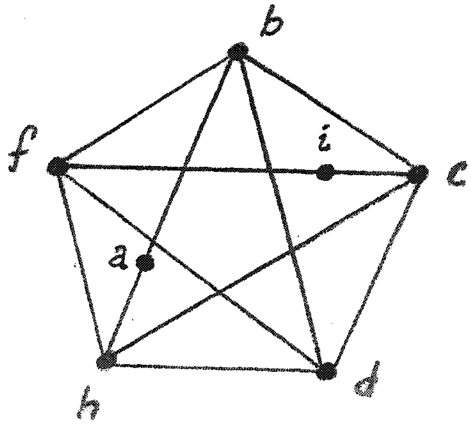
(4)



(5)



(6)



15. The result follows if and only if mn is even (that is, at least one of m, n is even).

Suppose, without loss of generality, that m is even — say, $m = 2t$. Let V denote the vertex set of $K_{m,n}$ where $V = V_1 \cup V_2$ and $V_1 = \{v_1, v_2, \ldots, v_t, v_{t+1}, \ldots, v_m\}$, $V_2 = \{w_1, w_1, \ldots, w_n\}$. The mn edges in $K_{m,n}$ are of the form $\{v_i, w_j\}$ where $1 \leq i \leq m$, $1 \leq j \leq n$. Now consider the subgraphs G_1, G_2 of $K_{m,n}$ where G_1 is induced by $\{v_1, v_2, \ldots, v_t\} \cup V_2$ and G_2 is induced by $\{v_{t+1}, v_{t+2}, \ldots, v_m\} \cup V_2$. Each of G_1, G_2 is isomorphic to $K_{t,n}$, and every edge in $K_{m,n}$ is in exactly one of G_1, G_2.

If both m, n are odd, then $K_{m,n}$ has an odd number of edges and cannot be decomposed into two isomorphic subgraphs — since each such subgraph has the same number of edges as the other.

16. Consider how the vertices of the Petersen graph are labeled in Fig. 11.52(a). The following correspondence of vertices provides an isomorphism for the two graphs:

$$\begin{array}{ccccc} a \to s & b \to v & c \to z & d \to y & e \to t \\ f \to u & g \to r & h \to w & i \to x & j \to q \end{array}$$

17. (a) There are 17 vertices, 34 edges and 19 regions and $v - e + r = 17 - 34 + 19 = 2$.
(b) Here we find 10 vertices, 24 edges and 16 regions and $v - e + r = 10 - 24 + 16 = 2$.

18. Proof: Since each region has at least five edges in its boundary, $2|E| > 5(53)$, or $|E| \geq (1/2)(5)(53)$. And from Theorem 11.6 we have $|V| = |E| - 53 + 2 = |E| - 51 \geq (1/2)(5)(53) - 51 = (265/2) - 51 = 81\frac{1}{2}$. Hence $|V| \geq 82$.

19. 10

20. (a) For each component $C_i = (V_i, E_i)$, $1 \leq i \leq n$, of G, if $e_i = |E_i|$ and $v_i = |V_i|$ then $e_i - v_i + 2 = r_i$. Summing as i goes from 1 to n we have $e - v + 2n = r + (n-1)$ because the infinite region is counted $n = \kappa(G)$ times. Hence $e - v + n + 1 = r = e - v + [\kappa(G) + 1]$.

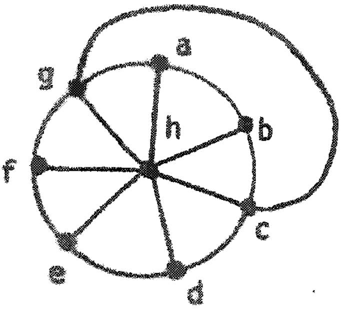
(b) Using the same notation as in part (a) we have $3r_i \leq 2e_i$, $1 \leq i \leq n$, so $3r \leq \sum_{i=1}^{n}(3r_i) \leq \sum_{i=1}^{n} 2e_i = 2e$. Also, $e_i \leq 3v_i - 6$, $1 \leq i \leq n$, so $e = \sum_{i=1}^{n} e_i \leq \sum_{i=1}^{n}(3v_i - 6) = 3v - 6n \leq 3v - 6$.

21. If not, $\deg(v) \geq 6$ for all $v \in V$. Then $2e = \sum_{v \in V} \deg(v) \geq 6|V|$, so $e \geq 3|V|$, contradicting $e \leq 3|V| - 6$ (Corollary 11.3.)

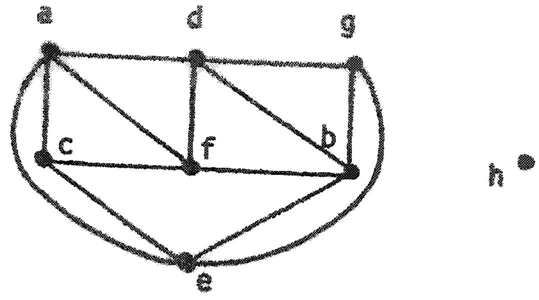
22. (a) Suppose that $G = (V, E)$ with $|V| = 11$. Then $\overline{G} = (V, E_1)$ where $\{a, b\} \in E_1$ iff $\{a, b\} \notin E$. Let $e = |E|$, $e_1 = |E_1|$. If both G and $\overline{G}$ are planar, then by Corollary 11.3 (and part (b) of Exercise 20, if necessary), $e \leq 3|V| - 6 = 33 - 6 = 27$ and $e_1 \leq 3|V| - 6 = 27$. But with $|V| = 11$, there are $\binom{11}{2} = 55$ edges in K_{11}, so $|E| + |E_1| = 55$ and either $e \geq 28$ or $e_1 \geq 28$. Hence, one of G, $\overline{G}$ must be planar.

If $G = (V, E)$ and $|V| > 11$, consider an induced subgraph of G on $V' \subset V$ where $|V'| = 11$.

(b) G:



$\overline{G}$:



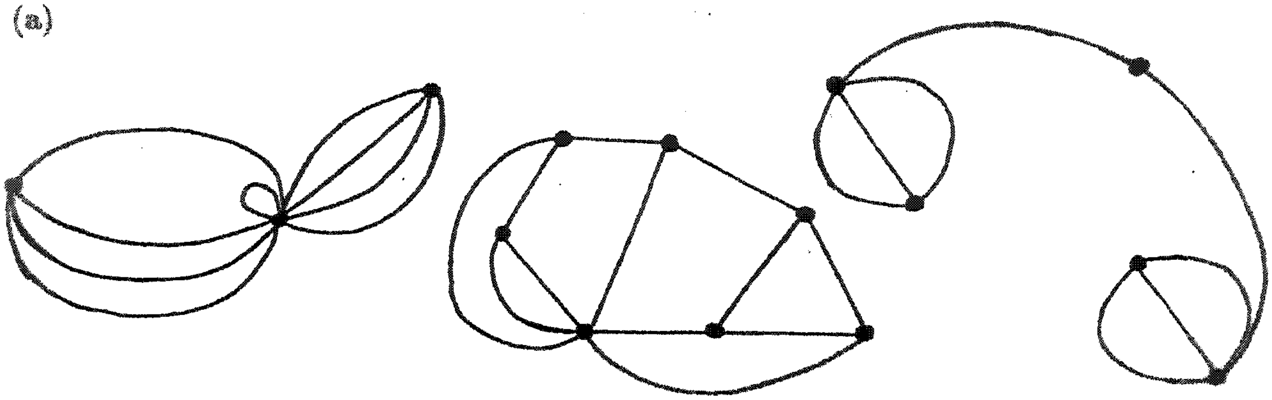
23. (a) $2e \geq kr = k(2 + e - v) \Longrightarrow (2 - k)e \geq k(2 - v) \Longrightarrow e \leq [k/(k-2)](v-2)$.

(b) 4

(c) In $K_{3,3}$, $e = 9$, $v = 6$. $[k/(k-2)](v-2) = (4/2)(4) = 8 < 9 = e$. Since $K_{3,3}$ is connected, it must be nonplanar.

(d) Here $k = 5$, $v = 10$, $e = 15$ and $[k/(k-2)](v-2) = (5/3)(8) = (40/3) < 15 = e$. Since the Petersen graph is connected, it must be nonplanar.

24. (a)



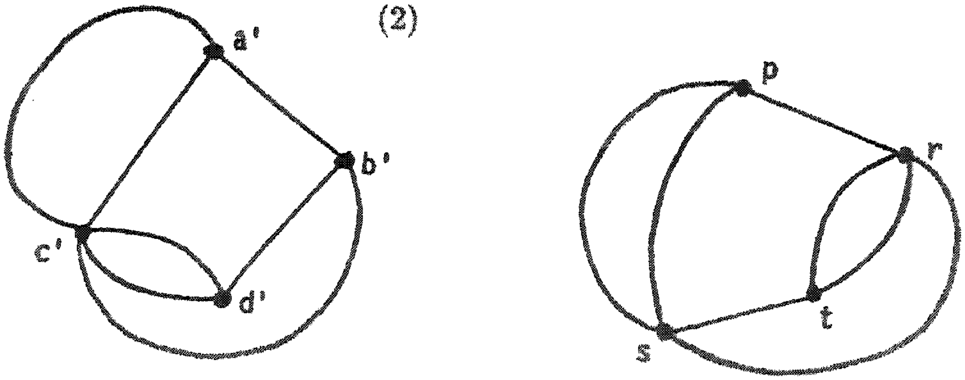
(b) There are no pendant vertices. But this does not contradict the condition mentioned because the loops contain other vertices and edges of the graph.

25. (a) The dual for the tetrahedron (Fig. 11.59(b)) is the graph itself. For the graph (cube) in Fig. 11.59(d) the dual is the octahedron, and vice versa. Likewise, the dual of the dodecahedron is the icosahedron, and vice versa.

(b) For $n \in \mathbf{Z}^+$, $n \geq 3$, the dual of the wheel graph W_n is W_n itself.

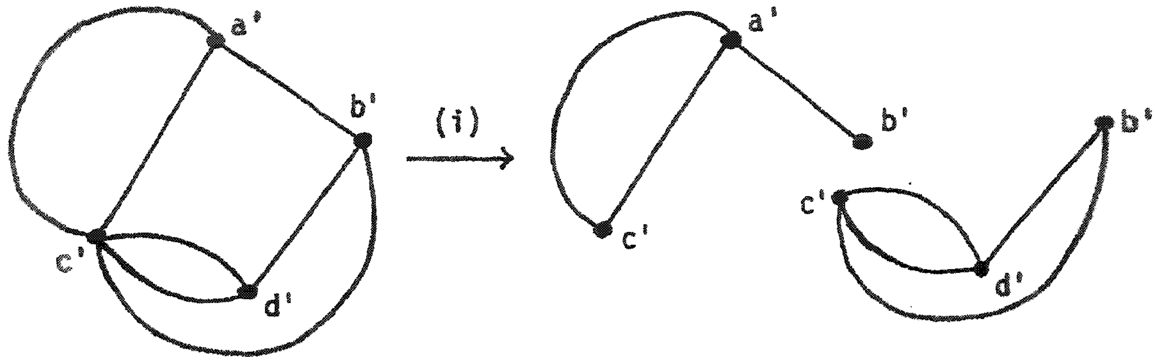
26. (a) The correspondence $a \rightarrow v$, $b \rightarrow w$, $c \rightarrow y$, $d \rightarrow z$, $e \rightarrow x$ provides an isomorphism.

(b) (1) (2)



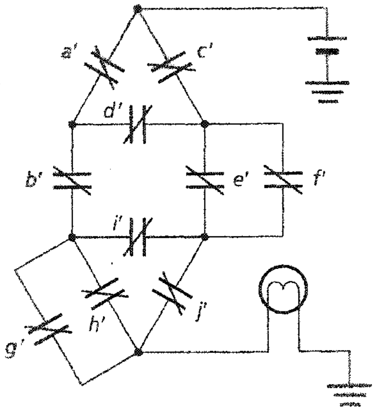
(c) In the first graph in part (b) vertex c' has degree 5. Since no vertex has degree 5 in the second graph, the two graphs cannot be isomorphic.

(d)



(e) $\{\{a', c'\}, \{c', b'\}, \{b', a'\}\}$; $\{\{p, r\}, \{r, t\}, \{r, t\}, \{r, s\}\}$.

27.



28. The number of vertices in G^d, the dual of G, is r, the number of regions in a planar depiction of G. Since G is isomorphic to G^d it follows that $r = n$. Consequently, $|V| - |E| + r = 2 \Rightarrow n - |E| + n = 2 \Rightarrow |E| = 2n - 2$.

29. Proof:

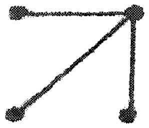
a) As we mentioned in the remark following Example 11.18, when G_1, G_2 are homeomorphic graphs then they may be regarded as isomorphic except, possibly, for vertices of degree 2. Consequently, two such graphs will have the same number of vertices of odd degree.

b) Now if G_1 has an Euler trail, then G_1 (is connected and) has all vertices of even degree – except two, those being the vertices at the beginning and end of the Euler trail. From part (a) G_2 is likewise connected with all vertices of even degree, except for two of odd degree. Consequently, G_2 has an Euler trail. [The converse follows in a similar way.]

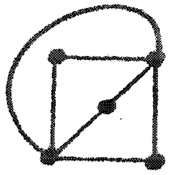
c) If G_1 has an Euler circuit, then G_1 (is connected and) has all vertices of even degree. From part (a) G_2 is likewise connected with all vertices of even degree, so G_2 has an Euler circuit. [The converse follows in a similar manner.]

Section 11.5

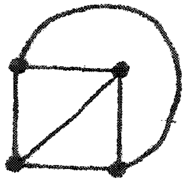
1.



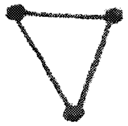
(a)



(b)



(c)



(d)

2. The graph is a path (cycle).

3. (a) Hamilton cycle: $a \to g \to k \to i \to h \to b \to c \to d \to j \to f \to e \to a$
(b) Hamilton cycle: $a \to d \to b \to e \to g \to j \to i \to f \to h \to c \to a$
(c) Hamilton cycle: $a \to h \to e \to f \to g \to i \to d \to c \to b \to a$
(d) The edges $\{a, c\}$, $\{c, d\}$, $\{d, b\}$, $\{b, e\}$, $\{e, f\}$, $\{f, g\}$ provide a Hamilton path for the given graph. However, there is no Hamilton cycle, for such a cycle would have to include the edges $\{b, d\}$, $\{b, e\}$, $\{a, c\}$, $\{a, e\}$, $\{g, f\}$, and $\{g, e\}$ – and, consequently, the vertex e will have degree greater than 2.
(e) The path $a \to b \to c \to d \to e \to j \to i \to h \to g \to f \to k \to l \to m \to n \to o$ is one possible Hamilton path for this graph. Another possibility is the path $a \to b \to c \to d \to i \to h \to g \to f \to k \to l \to m \to n \to o \to j \to e$. However, there is no Hamilton cycle. For if we try to construct a Hamilton cycle we must include the edges $\{a, b\}$, $\{a, f\}$, $\{f, k\}$, $\{k, l\}$, $\{d, e\}$, $\{e, j\}$, $\{j, o\}$ and $\{n, o\}$. This then forces us to eliminate the edges $\{f, g\}$ and $\{i, j\}$ from further consideration. Now consider the vertex i. If we use edges $\{d, i\}$ and $\{i, n\}$, then we have a cycle on the vertices d, e, j, o, n and i – and we cannot get a Hamilton cycle for the given graph. Hence we must use only one of the edges $\{d, i\}$ and $\{i, n\}$. Because of the symmetry in this graph let us select edge $\{d, i\}$ – and then edge $\{h, i\}$ so that vertex i will have degree 2 in the Hamilton cycle we are trying to construct. Since edges $\{d, i\}$ and $\{d, e\}$ are now being used, we eliminate edge $\{c, d\}$ and this then forces us to include edges $\{b, c\}$ and $\{c, h\}$ in our construction. Also we must include the edge $\{m, n\}$ since we eliminated edge $\{i, n\}$ from consideration. Next we eliminate edges $\{h, m\}$, $\{h, g\}$ and $\{b, g\}$. Finally we must include edge $\{m, l\}$ and then eliminate edge $\{l, g\}$. But now we have eliminated the four edges $\{b, g\}$, $\{f, g\}$, $\{h, g\}$ and $\{l, g\}$ and g is consequently isolated.
(f) For this graph we find the Hamilton cycle $a \to b \to c \to d \to e \to j \to i \to h \to g \to l \to m \to n \to o \to t \to s \to r \to q \to p \to k \to f \to a$.

4. (a) Consider the graph as shown in Fig. 11.52(a). We demonstrate one case. Start at vertex a and consider the partial path $a \to f \to i \to d$. These choices require the removal of edges $\{f, h\}$ and $\{g, i\}$ from further consideration since each vertex of the graph will be incident with exactly two edges in the Hamilton cycle. At vertex d we can

go to either vertex c or vertex e. (i) If we go to vertex c we eliminate edge $\{e,d\}$ from consideration, but we must now include edges $\{e,j\}$ and $\{e,a\}$, and this forces the elimination of edge $\{a,b\}$. Now we must consider vertex b, for by eliminating edge $\{a,b\}$ we are now required to include edges $\{b,g\}$ and $\{b,c\}$ in the cycle. This forces us to remove edge $\{c,h\}$ from further consideration. But we have now removed edges $\{f,h\}$ and $\{c,h\}$ and there is only one other edge that is incident with h, so no Hamilton cycle can be obtained. (ii) Selecting vertex e after d, we remove edge $\{d,c\}$ and include $\{c,h\}$ and $\{b,c\}$. Having removed $\{g,i\}$ we must include $\{g,b\}$ and $\{g,j\}$. This forces the elimination of $\{a,b\}$, the inclusion of $\{a,e\}$ (and the elimination of $\{e,j\}$). We now have a cycle containing a,f,i,d,e, hence this method has also failed.

However, this graph does have a Hamilton path: $a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow j \rightarrow h \rightarrow f \rightarrow i \rightarrow g$.

(b) For example, remove vertex j and the edges $\{e,j\},\{g,j\},\{h,j\}$. Then $e \rightarrow a \rightarrow f \rightarrow h \rightarrow c \rightarrow b \rightarrow g \rightarrow i \rightarrow d \rightarrow e$ provides a Hamilton cycle for this subgraph.

5. (a) If we remove any one of the vertices a, b or g, the resulting subgraph has a Hamilton cycle. For example, upon removing vertex a, we find the Hamilton cycle $b \rightarrow d \rightarrow c \rightarrow f \rightarrow g \rightarrow e \rightarrow b$.
(b) The following Hamilton cycle exists if we remove vertex g : $a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow j \rightarrow o \rightarrow n \rightarrow i \rightarrow h \rightarrow m \rightarrow l \rightarrow k \rightarrow f \rightarrow a$. A symmetric situation results upon removing vertex i.

6. Let the vertices on the cycle (rim) of W_n be consecutively denoted by $v_1, v_2, \ldots, v_n$, and let v_{n+1} denote the additional (central) vertex of W_n. Then the following cycles provide n Hamilton cycles for the wheel graph W_n.
(1) $v_1 \rightarrow v_{n+1} \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow v_n \rightarrow v_1$;
(2) $v_1 \rightarrow v_2 \rightarrow v_{n+1} \rightarrow v_3 \rightarrow v_4 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow v_n \rightarrow v_1$;
(3) $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_{n+1} \rightarrow v_4 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow v_n \rightarrow v_1$;
$\vdots$
$(n-1)$ $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow v_{n+1} \rightarrow v_n \rightarrow v_1$; and
(n) $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow v_n \rightarrow v_{n+1} \rightarrow v_1$.

7. (a) $(1/2)(n-1)!$ (b) 10 (c) 9

8. (a) Partition the vertices of $K_{n,n}$ as $X \cup Y$ where $|X| = |Y| = n$. Write $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$; each edge of $K_{n,n}$ is of the form $\{x_i, y_i\}$ where $1 \leq i,j \leq n$. Since x_1 is on every Hamilton cycle of $K_{n,n}$, start with x_1. There are then n choices for y_j where $\{x_1, y_j\}$ is on the cycle. From y_j we can return to X in $n-1$ ways (we cannot use x_1 again), forming the second edge $\{y_j, x_i\}$, where $2 \leq i \leq n$. Continuing in this manner there are $(n-1)!n!$ results. Since directions are not assigned to any of the edges we get a total of $(1/2)(n-1)!n!$ Hamilton cycles for $K_{n,n}$.

(b) In this case the "starting" vertex of a Hamilton path is in one of X or Y (as described in part (a)) and the "terminating" vertex is then in the other set. The number of such paths is $(n!)^2$. (Note: $n = 1$ makes sense in this part but not for the formula in part (a).)

9. Let $G = (V, E)$ be a loop-free undirected graph with no odd cycles. We assume that G is connected – otherwise, we work with the components of G. Select any vertex x in V and let $V_1 = \{v \in V | d(x, v)$, the length of a shortest path between x and v, is odd$\}$ and $V_2 = \{w \in V | d(x, w)$, the length of a shortest path between x and w, is even$\}$. Note that (i) $x \in V_2$; (ii) $V = V_1 \cup V_2$; and (iii) $V_1 \cap V_2 = \emptyset$. We claim that each edge $\{a, b\}$ in E has one vertex in V_1 and the other vertex in V_2.

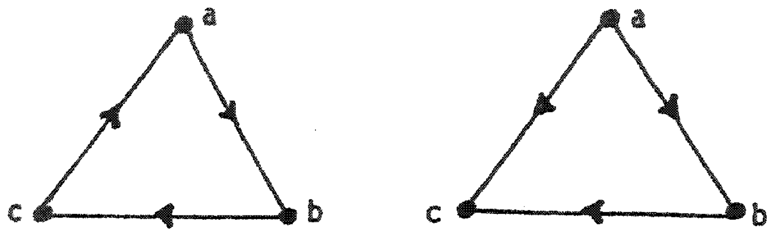
For suppose that $e = \{a, b\} \in E$ with $a, b \in V_1$. (The proof for $a, b \in V_2$ is similar.) Let $E_a = \{\{a, v_1\}, \{v_1, v_2\}, \ldots, \{v_{m-1}, x\}\}$ be the m edges in a shortest path from a to x, and let $E_b = \{\{b, v_1'\}, \{v_1', v_2'\}, \ldots, \{v_{n-1}', x\}\}$ be the n edges in a shortest path from b to x. Note that m, n are both odd. If $\{v_1, v_2, \ldots, v_{m-1}\} \cap \{v_1', v_2', \ldots, v_{n-1}'\} = \emptyset$, then the set of edges $E' = \{\{a, b\}\} \cup E_a \cup E_b$ provides an odd cycle in G. Otherwise, let $w (\neq x)$ be the first vertex where the paths come together, and let $E'' = \{\{a, b\}\} \cup \{\{a, v_1\}, \{v_1, v_2\}, \ldots, \{v_i, w\}\} \cup \{\{b, v_1'\}, \{v_1', v_2'\}, \ldots, \{v_j', w\}\}$, for some $1 \leq i \leq m-1$ and $1 \leq j \leq n-1$. Then either E'' provides an odd cycle for G or $E' - E''$ contains an odd cycle for G.

10. (a) Suppose that G has a Hamilton cycle C. Then C contains $|V|$ edges and the vertices on C must alternate between vertices in V_1 and those in V_2 because G is bipartite. This forces $|V|$ to be even and $|V_1| = |V_2|$.

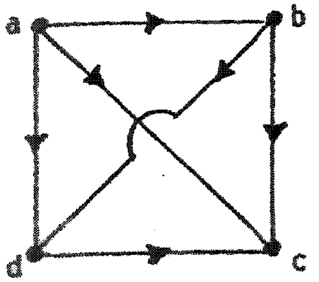
(b) In a similar way, if G has a Hamilton path P, then P has $|V| - 1$ edges and the vertices on P must alternate between the vertices in V_1 and those in V_2. Since $|V_1| \neq |V_2|$, it follows that $|V_1| - |V_2| = \pm 1$.

(c) Let $V = \{a, b, c, d, e\}$ with $V_1 = \{a, b\}$, $V_2 = \{c, d, e\}$ and $E = \{\{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}\}$.

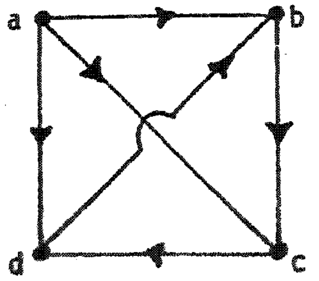
11. (a)



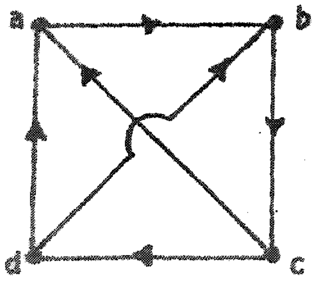
(b)



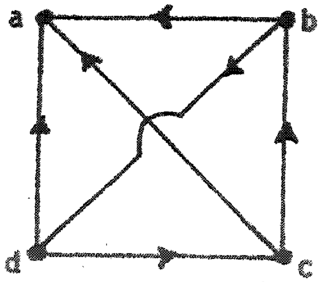
$\text{od}(a) = 3$ $\text{id}(a) = 0$
$\text{od}(b) = 2$ $\text{id}(b) = 1$
$\text{od}(c) = 0$ $\text{id}(c) = 3$
$\text{od}(d) = 1$ $\text{id}(d) = 2$



$\text{od}(a) = 3$ $\text{id}(a) = 0$
$\text{od}(b) = 1$ $\text{id}(b) = 2$
$\text{od}(c) = 1$ $\text{id}(c) = 2$
$\text{od}(d) = 1$ $\text{id}(d) = 2$



$\text{od}(a) = 1$ $\text{id}(a) = 2$
$\text{od}(b) = 1$ $\text{id}(b) = 2$
$\text{od}(c) = 2$ $\text{id}(c) = 1$
$\text{od}(d) = 2$ $\text{id}(d) = 1$



$\text{od}(a) = 0$ $\text{id}(a) = 3$
$\text{od}(b) = 2$ $\text{id}(b) = 1$
$\text{od}(c) = 2$ $\text{id}(c) = 1$
$\text{od}(d) = 2$ $\text{id}(d) = 1$

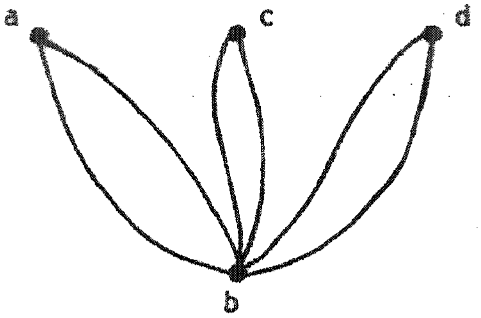
12. Proof: From Example 11.26 we know the result is true for $n = 2$. Assume that Q_n has a Hamilton cycle for some arbitrary (but fixed) $n \geq 2$. Now consider Q_{n+1}. From Example 11.12 we know that Q_{n+1} can be constructed from two copies of Q_n – one copy, $Q_{n,0}$, induced by the vertices of Q_{n+1} that start with 0, the other copy, $Q_{n,1}$, induced by the vertices of Q_{n+1} that start with 1. Each of $Q_{n,0}$, $Q_{n,1}$ has a Hamilton cycle – each may have more than one but we agree to pick the same cycle in each. [The only difference in the cycles is the first bit in the vertices of an edge – that is, if $\{0x, 0y\}$ is an edge in the Hamilton cycle for $Q_{n,0}$ (where x, y are binary strings of length n that differ in only one position), then $\{1x, 1y\}$ is the corresponding edge in the Hamilton cycle for $Q_{n,1}$.] Select edges $\{0v, 0w\}$ and $\{1v, 1w\}$ from the Hamilton cycles for $Q_{n,0}$ and $Q_{n,1}$, respectively. Remove these edges and replace them with the edges $\{0v, 1v\}$, $\{0w, 1w\}$ (in Q_{n+1}). The result is a Hamilton cycle for Q_{n+1}.

It now follows from the Principle of Mathematical Induction that Q_n has a Hamilton cycle for all $n \geq 2$.

13. Proof: If not, there exists a vertex x such that $(v, x) \notin E$ and, for all $y \in V$, $y \neq v, x$, if $(v, y) \in E$ then $(y, x) \notin E$. Since $(v, x) \notin E$, we have $(x, v) \in E$, as T is a tournament. Also, for each y mentioned earlier, we also have $(x, y) \in E$. Consequently, $od(x) \geq od(v)+1$ – contradicting $od(v)$ being a maximum!

14. Let G be any path with more than three vertices.

15.



For the multigraph in the given figure, $|V| = 4$ and $\deg(a) = \deg(c) = \deg(d) = 2$ and $\deg(b) = 6$. Hence $\deg(x) + \deg(y) \geq 4 > 3 = 4 - 1$ for all nonadjacent $x, y \in V$, but the multigraph has no Hamilton path.

16. Corollary 11.4: Proof: For all $x, y \in V$, $\deg(x) + \deg(y) \geq 2[(n-1)/2] = n - 1$, so the result follows from Theorem 11.8.

Corollary 11.5: Proof: Let $a, b \in V$ where $\{a, b\} \notin E$. Then $\deg(a) + \deg(b) \geq (n/2) + (n/2) = n$, so the result follows from Theorem 11.9.

17. For $n \geq 5$ let $C_n = (V, E)$ denote the cycle on n vertices. Then C_n has (actually is) a Hamilton cycle, but for all $v \in V$, $\deg(v) = 2 < n/2$.

18. Construct a graph with 12 vertices, one for each person. If two people know each other, draw an edge connecting their corresponding vertices. By Theorem 11.9 this graph has a Hamilton cycle and this cycle provides such a seating arrangement.

19. This follows from Theorem 11.9, since for all (nonadjacent) $x, y \in V$, $\deg(x) + \deg(y) = 12 > 11 = |V|$.

20. Proof: Let $x, y \in V$ with $\{x, y\} \in E$. Consequently, x, y are nonadjacent in $\overline{G}$. In $\overline{G}$ we find that $\deg_{\overline{G}}(x) = \deg_{\overline{G}}(y) \geq 2n+2-n = n+2$, so $\deg_{\overline{G}}(x) + \deg_{\overline{G}}(y) = 2n+4 > 2n+2 = |V|$. Therefore, by virtue of Theorem 11.9, the graph $\overline{G}$ has a Hamilton cycle.

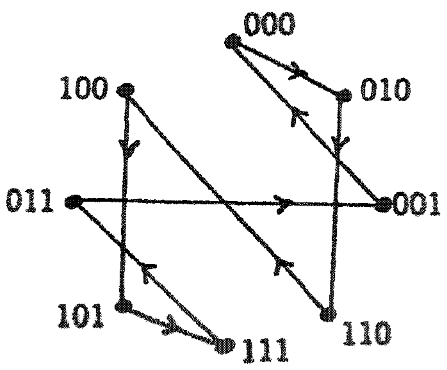
21. When $n = 5$ the graphs C_5 and $\overline{C}_5$ are isomorphic, and both are Hamilton cycles on five vertices.

For $n \geq 6$, let u, v denote nonadjacent vertices in $\overline{C}_n$. Since $\deg(u) = \deg(v) = n - 3$ we find that $\deg(u) + \deg(v) = 2n - 6$. Also, $2n - 6 \geq n \iff n \geq 6$, so it follows from Theorem 11.9 that the cocycle $\overline{C}_n$ contains a Hamilton cycle when $n \geq 6$.

22. (a) If $x \neq v$ and $y \neq v$, then $\deg(x) = \deg(y) = n - 2$, and $\deg(x) + \deg(y) = 2n - 4 \geq n$, for $n \geq 4$.
If one of x, y is v, say x, then $\deg(x) = 2$ and $\deg(y) = n - 2$, and $\deg(x) + \deg(y) = n$.
(b) From part (a) it follows that $\deg(x) + \deg(y) \geq n$ for all nonadjacent x, y in V. Therefore G_n has a Hamilton cycle — by virtue of Theorem 11.9.
(c) Here $|E| = \binom{n-1}{2} - 1 + 2$, where we subtract 1 for the edge $\{v_1, v_2\}$, and add 2 for the pair of edges $\{v_1, v\}$ and $\{v, v_2\}$. Consequently, $|E| = \binom{n-1}{2} + 1$.
(d) The results in parts (b) and (c) do not contradict Corollary 11.6. They show that the converse of this corollary is false — as is its inverse.

23. (a) The path $v \rightarrow v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow \ldots \rightarrow v_{n-1}$ provides a Hamilton path for H_n. Since $\deg(v) = 1$ the graph cannot have a Hamilton cycle.
(b) Here $|E| = \binom{n-1}{2} + 1$. (So the number of edges required in Corollary 11.6 cannot be decreased.)

24. (a)



Since the given graph has a Hamilton path we use this path to provide the following Gray code for $1, 2, 3, \ldots, 8$.

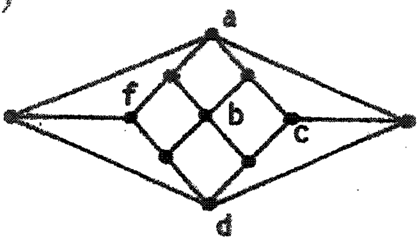
1: 000	2: 010	3: 110	4: 100
5: 101	6: 111	7: 011	8: 001

(b)

1: 0000	2: 0001	3: 0011	4: 0111
5: 1111	6: 1110	7: 1100	8: 1000
9: 1010	10: 1011	11: 1001	12: 1101
13: 0101	14: 0100	15: 0110	16: 0010

25. (a) (i) $\{a,c,f,h\},\{a,g\}$; (ii) $\{z\},\{u,w,y\}$
(b) (i) $\beta(G)=4$; (ii) $\beta(G)=3$
(c) (i) 3 (ii) 3 (iii) 3 (iv) 4 (v) 6
(vi) The maximum of m and n.
(d) The complete graph on $|I|$ vertices.

26. (a) If not, there is an edge $\{a,b\}$ in E where $a,b\in I$. This contradicts the independence of I.
(b) A Hamilton cycle on v vertices must have v edges.
(c)



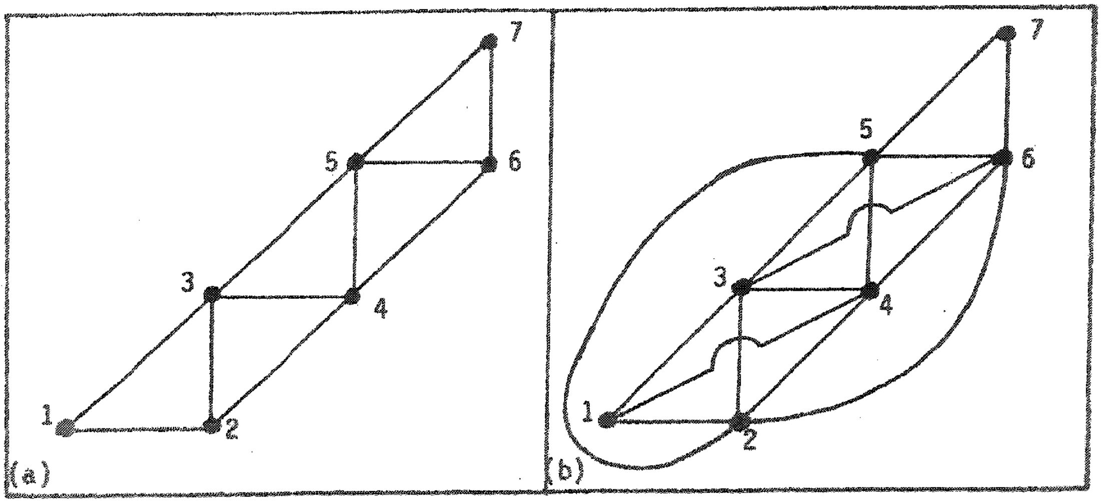
Let $I=\{a,b,c,d,f\}$, as shown in the figure. Here $v=11, e=18$, and $e-\sum_{v\in I}\deg(v)+2|I|=18-(4+4+3+4+3)+2(5)=10<11$, so by part (b), the Herschel graph has no Hamilton cycle.

Section 11.6

1. Draw a vertex for each species of fish. If two species x,y must be kept in separate aquaria, draw the edge $\{x,y\}$. The smallest number of aquaria needed is then the chromatic number of the resulting graph.

2. Draw a vertex for each committee. If someone serves on two committees c_i,c_j draw the edge joining the vertices for c_i and c_j. Then the least number of meeting times is the chromatic number of the graph.

3. We can model this problem with graphs. For either part of the problem draw the undirected graph $G=(V,E)$ where $V=\{1,2,3,4,5,6,7\}$ and $\{i,j\}\in E$ when chemicals i and j require separate storage compartments. For part (a), the graph (in part (a) of the figure) has chromatic number 3, so here Jeannette will need three separate storage compartments to safely store these seven chemicals.



Now consider the graph in part (b) of the figure. Note here that the subgraph induced by the vertices 2,3,4,5,6 is (isomorphic to) K_5. Consequently, with these additional conditions Jeannette will need five separate storage compartments to store these seven chemicals safely.

4. Let G be a cycle on n vertices where n is odd and $n \geq 5$.

5. (a) $P(G, \lambda) = \lambda(\lambda - 1)^3$
(b) For $G = K_{1,n}$ we find that $P(G, \lambda) = \lambda(\lambda - 1)^n$.
$\chi(K_{1,n}) = 2$.

6. (a) (i) Here we have λ choices for vertex a, 1 choice for vertex b (the same choice as that for vertex a), and $\lambda - 1$ choices for each of vertices x, y, z. Consequently, there are $\lambda(\lambda - 1)^3$ proper colorings of $K_{2,3}$ where vertices a and b are colored the same.
(ii) Now we have λ choices for vertex a, $\lambda - 1$ choices for vertex b, and $\lambda - 2$ choices for each of the vertices x, y, and z. And here there are $\lambda(\lambda - 1)(\lambda - 2)^3$ proper colorings.

(b) Since the two cases in part (a) are exhaustive and mutually exclusive, the chromatic polynomial for $K_{2,3}$ is

$$\lambda(\lambda - 1)^3 + \lambda(\lambda - 1)(\lambda - 2)^3 = \lambda(\lambda - 1)(\lambda^3 - 5\lambda^2 + 10\lambda - 7).$$

$\chi(K_{2,3}) = 2$.

(c) $P(K_{2,n}, \lambda) = \lambda(\lambda - 1)^n + \lambda(\lambda - 1)(\lambda - 2)^n$

$\chi(K_{2,n}) = 2$.

7. (a) 2 (b) 2 (n even); 3 (n odd)

(c) Figure 11.59(d): 2; Fig. 11.62(a): 3; Fig. 11.85(i); 2; Fig. 11.85(ii): 3 (d) 2

8. If $G = (V, E)$ is bipartite, then $V = V_1 \cup V_2$ where $V_1 \cap V_2 = \emptyset$ and each edge is of the form $\{x, y\}$ where $x \in V_1, y \in V_2$. Color all the vertices in V_1 with one color and those in V_2 with a second color. Then $\chi(G) = 2$.
Conversely, if $\chi(G) = 2$, let V_1 be the set of all vertices with one color and V_2 the set of vertices with the second color. Then $V = V_1 \cup V_2$ with $V_1 \cap V_2 = \emptyset$ and each edge of G has one vertex in V_1 and the other in V_2, so G is bipartite.

9. (a) (1) $\lambda(\lambda - 1)^2(\lambda - 2)^2$; (2) $\lambda(\lambda - 1)(\lambda - 2)(\lambda^2 - 2\lambda + 2)$;
(3) $\lambda(\lambda - 1)(\lambda - 2)(\lambda^2 - 5\lambda + 7)$

(b) (1) 3: (2) 3; (3) 3

(c) (1) 720; (2) 1020; (3) 420

10. (a) These graphs are not isomorphic. The first graph has two vertices of degree 4 – namely, f and k. The second graph has three vertices of degree 4 – namely u,w,z.

(b) For the first graph there are two cases to consider.

Case (i): Vertices f and k have the same color: Here there are $\lambda(\lambda-1)^2(\lambda-2)^2$ ways to properly color the vertices.

Case (ii): Vertices f and k are colored with different colors: Here the vertices can be properly colored in $\lambda(\lambda-1)(\lambda-2)^2(\lambda-3)^2$ ways.

By the rule of sum, $P(G,\lambda) = \lambda(\lambda-1)^2(\lambda-2)^2 + \lambda(\lambda-1)(\lambda-2)^2(\lambda-3)^2 =$
$\lambda(\lambda-1)^2(\lambda-2)^2(\lambda^2-5\lambda+8)$.

Using the same type of argument, with the two cases for vertices u and z, the chromatic polynomial for the second graph is also found to be $\lambda(\lambda-1)^2(\lambda-2)^2(\lambda^2-5\lambda+8)$.

(c) If G_1, G_2 are two graphs with $P(G_1,\lambda) = P(G_2,\lambda)$, it need not be the case that G_1 and G_2 are isomorphic.

11. Let $e = \{v, w\}$ be the deleted edge. There are $\lambda(1)(\lambda-1)(\lambda-2)\cdots(\lambda-(n-2))$ proper colorings of G_n where v, w share the same color and $\lambda(\lambda-1)(\lambda-2)\cdots(\lambda-(n-1))$ proper colorings where v, w are colored with different colors. In total there are $P(G_n,\lambda) = \lambda(\lambda-1)\cdots(\lambda-n+2) + \lambda(\lambda-1)\cdots(\lambda-n+1) = \lambda(\lambda-1)\cdots(\lambda-n+3)(\lambda-n+2)^2$ proper colorings for G_n.

Here $\chi(G_n) = n-1$.

12. a) Here $\binom{r}{2} + \binom{g}{2} = \binom{6}{2} + \binom{3}{2} = 15 + 3 = 18$, and $\binom{r+g}{2} = \binom{9}{2} = 36$. So there are 18 edges that are red or green, and 18 blue edges.

b) $\binom{r}{2} + \binom{g}{2} = (1/2)\binom{r+g}{2} \Leftrightarrow (1/2)r(r-1) + (1/2)g(g-1) = (1/4)(r+g)(r+g-1) \Leftrightarrow$ $2r(r-1) + 2g(g-1) = (r+g)(r+g-1) \Leftrightarrow r^2 - r + g^2 - g = 2rg \Leftrightarrow (r-g)^2 = r+g$. Let $r = g+k$, $k \geq 0$. Then $[(r-g)^2 = k^2 = r+g = 2g+k] \Leftrightarrow [g = (1/2)(k^2-k) = (1/2)k(k-1) = t_{k-1}$ and $r = g+k = (1/2)k(k-1)+k = (1/2)k[(k-1)+2k] = (1/2)k(k+1) = t_k] \Leftrightarrow r, g$ are two consecutive triangular numbers.

13. (a) $|V| = 2n$; $|E| = (1/2)\sum_{v\in V}\deg(v) = (1/2)[4(2) + (2n-4)(3)] = (1/2)[8 + 6n - 12] =$ $3n-2$, $n \geq 1$.

(b) For $n = 1$, we find that $G = K_2$ and $P(G,\lambda) = \lambda(\lambda-1) = \lambda(\lambda-1)(\lambda^2-3\lambda+3)^{1-1}$ so the result is true in this first case. For $n = 2$, we have $G = C_4$, the cycle of length 4, and here $P(G,\lambda) = \lambda(\lambda-1)^3 - \lambda(\lambda-1)(\lambda-2) = \lambda(\lambda-1)(\lambda^2-3\lambda+3)^{2-1}$. So the result follows for $n = 2$. Assuming the result true for an arbitrary (but fixed) $n \geq 1$, consider the situation for $n+1$. Write $G = G_1 \cup G_2$, where G_1 is C_4 and G_2 is the ladder graph for n rungs. Then $G_1 \cap G_2 = K_2$, so from Theorem 11.14 we have $P(G,\lambda) = P(G_1,\lambda)\cdot P(G_2,\lambda)/P(K_2,\lambda) =$ $[(\lambda)(\lambda-1)(\lambda^2-3\lambda+3)][(\lambda)(\lambda-1)(\lambda^2-3\lambda+3)^{n-1}]/(\lambda)(\lambda-1) = (\lambda)(\lambda-1)(\lambda^2-3\lambda+3)^n$. Consequently, the result is true for all $n \geq 1$, by the Principle of Mathematical Induction.

14. (a) Select a vertex $v \in V$ and color it with one of the $\Delta+1$ available colors. If $w \in V$ and w has not been colored, since $\deg(w) \leq \Delta$ we can color w, *not* using any of the colors used on the vertices adjacent to w. This procedure is repeated until all of the vertices in V have been (properly) colored.

(b) For $n \in \mathbf{Z}^+$, $n \geq 3$, $\chi(K_n) = n = \Delta + 1$.

15. (a) $\lambda(\lambda-1)(\lambda-2)$ (b) Follows from Theorem 11.10

(c) Follows by the rule of product.

(d)

$$\begin{aligned} P(C_n, \lambda) &= P(P_{n-1}, \lambda) - P(C_{n-1}, \lambda) = \lambda(\lambda-1)^{n-1} - P(C_{n-1}, \lambda) \\ &= [(\lambda-1)+1](\lambda-1)^{n-1} - P(C_{n-1}, \lambda) \\ &= (\lambda-1)^n + (\lambda-1)^{n-1} - P(C_{n-1}, \lambda) \Longrightarrow \\ & \quad\; P(C_n, \lambda) - (\lambda-1)^n = (\lambda-1)^{n-1} - P(C_{n-1}, \lambda). \end{aligned}$$

Replacing n by $n-1$ yields

$$P(C_{n-1}, \lambda) - (\lambda-1)^{n-1} = (\lambda-1)^{n-2} - P(C_{n-2}, \lambda) = (-1)[P(C_{n-2}, \lambda) - (\lambda-1)^{n-2}].$$

Hence

$$P(C_n, \lambda) - (\lambda-1)^n = P(C_{n-2}, \lambda) - (\lambda-1)^{n-2} = (-1)^2[P(C_{n-2}, \lambda) - (\lambda-1)^{n-2}].$$

(e) Continuing from part (d),

$$\begin{aligned} P(C_n, \lambda) &= (\lambda-1)^n + (-1)^{n-3}[P(C_3, \lambda) - (\lambda-1)^3] \\ &= (\lambda-1)^n + (-1)^{n-1}[\lambda(\lambda-1)(\lambda-2) - (\lambda-1)^3] \\ &= (\lambda-1)^n + (-1)^n(\lambda-1). \end{aligned}$$

16. (a) $\chi(W_n) = \chi(C_n) + 1$. [$C_n$ has n vertices; W_n has $n+1$ vertices.]

(b) $P(W_n, \lambda) = \lambda P(C_n, \lambda - 1) = \lambda[(\lambda-2)^n + (-1)^n(\lambda-2)]$.

(c) (i) and (ii) $P(W_5, \lambda) = \lambda(\lambda-2)^5 + (-1)^5\lambda(\lambda-2)$ - For k colors we have $P(W_5, k) = k(k-2)^5 + (-1)^5 k(k-2) = k(k-2)[(k-2)^4 - 1]$ proper colorings, whenever $k \geq 4$.

17. From Theorem 11.13, the expansion for $P(G, \lambda)$ will contain exactly one occurrence of the chromatic polynomial of K_n. Since no larger graph occurs this term determines the degree as n and the leading coefficient as 1.

18. (a)

$$\begin{array}{lll} |V| = 1: & P(G,\lambda) = \lambda & \\ |V| = 2: & |E| = 0: & P(G,\lambda) = \lambda^2 \\ & |E| = 1: & P(G,\lambda) = \lambda(\lambda-1) = \lambda^2 - \lambda \\ |V| = 3: & |E| = 0: & P(G,\lambda) = \lambda^3 \\ & |E| = 1: & P(G,\lambda) = \lambda^2(\lambda-1) = \lambda^3 - \lambda^2 \\ & |E| = 2: & P(G,\lambda) = \lambda(\lambda-1)^2 = \lambda^3 - 2\lambda^2 + \lambda \\ & |E| = 3: & P(G,\lambda) = \lambda(\lambda-1)(\lambda-2) = \lambda^3 - 3\lambda^2 + 2\lambda \end{array}$$

(b) Let $G = (V, E)$ be a loop-free undirected graph where $|V| = n \geq 4$ and $|E| = k \geq 1$. (If $k = 0$, $P(G, \lambda = \lambda^n$ and the result is true.) From Theorem 11.10, $P(G, \lambda) = P(G_e, \lambda) - P(G'_e, \lambda)$ where $e = \{a, b\}$ is an edge in G. Since G_e has n vertices but $k-1$ edges, by the induction hypothesis,

$$P(G_e, \lambda) = \lambda^n - (k-1)\lambda^{n-1} + c_{n-2}\lambda^{n-2} - c_{n-3}\lambda^{n-3} + \ldots + (-1)^{n-1}c_1\lambda,$$

where $k-1, c_{n-2}, c_{n-3}, \ldots, c_1 \geq 0$. (When a coefficient in this list is zero, all successive coefficients are zero.) Likewise, since G'_e has $n-1$ vertices, by the induction hypothesis,

$$P(G'_e, \lambda) = \lambda^{n-1} - b_{n-2}\lambda^{n-2} + b_{n-3}\lambda^{n-3} - \ldots + (-1)^{n-2}b_1\lambda,$$

where $b_{n-2}, b_{n-3}, \ldots, b_1 \geq 0$.

Then $P(G, \lambda) = P(G_e, \lambda) - P(G'_e, \lambda) =$

$$\lambda^n - (k)\lambda^{n-1} + (c_{n-2} + b_{n-2})\lambda^{n-2} + \ldots + (-1)^{n-1}(c_1 + b_1)\lambda.$$

(c) This was shown in part (b).

19. (a) For $n \in \mathbf{Z}^+$, $n \geq 3$, let C_n denote the cycle on n vertices.

If n is odd then $\chi(C_n) = 3$. But for each v in C_n, the subgraph $C_n - v$ is a path with $n-1$ vertices and $\chi(C_n - v) = 2$. So for n odd C_n is color-critical.

However, when n is even we have $\chi(C_n) = 2$, and for each v in C_n, the subgraph $C_n - v$ is still a path with $n-1$ vertices and $\chi(C_n - v) = 2$. Consequently, cycles with an even number of vertices are not color-critical.

(b) For every complete graph K_n, where $n \geq 2$, we have $\chi(K_n) = n$, and for each vertex v in K_n, $K_n - v$ is (isomorphic to) K_{n-1}, so $\chi(K_n - v) = n - 1$. Consequently, every complete graph with at least one edge is color-critical.

(c) Suppose that G is not connected. Let G_1 be a component of G where $\chi(G_1) = \chi(G)$, and let G_2 be any other component of G. Then $\chi(G_1) \geq \chi(G_2)$ and for all v in G_2 we find that $\chi(G - v) = \chi(G_1) = \chi(G)$, so G is not color-critical.

(d) If not, let $v \in V$ with $\deg(v) \leq k-2$. Since G is color-critical we have $\chi(G - v) \leq k-1$, and so we can properly color the vertices in the subgraph $G - v$ with at most $k-1$ colors. Since $\deg(v) \leq k-2$, we have used at most $k-2$ colors to color all vertices in G adjacent to v. Therefore we do not need a new color (beyond those needed to color the subgraph $G - v$) in order to color v and can color all vertices in G with at most $k-1$ colors. But this contradicts $\chi(G) = k$.

Supplementary Exercises

1. $\binom{n}{2} = 56 + 80 = 136 \Longrightarrow n(n-1) = 272 \Longrightarrow n = 17.$

2. For $n \geq 1$, let c_n count the number of cycles of length four in Q_n. Then $c_1 = 0$ and $c_2 = 1$. Recall the recursive construction of Q_{n+1} from Q_n — given in Section 11.3. Let $V_{n+1}^{(0)}$ denote all the vertices in Q_{n+1} that start with 0, and $V_{n+1}^{(1)}$ those vertices in Q_{n+1} that start with 1. [Each of the subgraphs of Q_{n+1} induced by $V_{n+1}^{(0)}$ and $V_{n+1}^{(1)}$ is isomorphic to Q_n.] Let $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$ denote a cycle of length four in Q_{n+1}. There are three cases to consider:

(1) $v_1, v_2, v_3, v_4 \in V_{n+1}^{(0)}$: Here there are c_n such cycles;
(2) $v_1, v_2, v_3, v_4 \in V_{n+1}^{(1)}$: Here there are also c_n such cycles; and,
(3) one edge of the cycle (call it the first) is in $\langle V_{n+1}^{(0)} \rangle$ and another edge (namely, the third) is in $\langle V_{n+1}^{(1)} \rangle$: Here the other two edges are each adjacent to a vertex in $V_{n+1}^{(0)}$ and one in $V_{n+1}^{(1)}$. [Let $\{v_1, v_2\} \in \langle V_{n+1}^{(0)} \rangle$, then $\{v_3, v_4\} \in \langle V_{n+1}^{(1)} \rangle$ and the binary labels on v_1 and v_4 differ only in the first (left-most) position, while the binary labels on v_2 and v_3 also differ only in the first (left-most) position.] Since there are $n2^{n-1}$ possible choices (the number of edges in Q_n) for the so called "first" edge, here we find $n2^{n-1}$ new cycles of length four.

The preceding discussion gives us
$c_{n+1} = 2c_n + n2^{n-1} = 2c_n + (1/2)n2^n \quad n \geq 1,\ c_1 = 0,\ c_2 = 1.$
$c_n^{(h)} = A2^n, \quad c_n^{(p)} = n(B + Cn)2^n$
$(n+1)(B + C(n+1))2^{n+1} = 2n(B + Cn)2^n + n2^{n-1}$
$\Rightarrow [B(n+1) + C(n+1)^2]2^{n+1} = [Bn + Cn^2]2^{n+1} + (n/4)2^{n+1}$
$\Rightarrow 2C = 1/4,\ B + C = 0 \Rightarrow C = 1/8,\ B = -1/8.$
So $c_n^{(p)} = (1/8)(n^2 - n)2^n$.
$0 = c_1 = c_1^{(h)} + c_1^{(p)} = 2A + 0 \Rightarrow A = 0$, so
$c_n = (1/8)(n^2 - n)2^n = \binom{n}{2}2^{n-2}, \quad n \geq 1.$

Alternate Solution: Let $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$ be a cycle of length four in Q_n. Say v_1, v_2 differ in position i and v_2, v_4 differ in position j, where $1 \leq i \leq n$, $1 \leq j \leq n$, and $i \neq j$. Then v_3 is determined: it differs from v_1 in positions i and j. Starting with v_1 there are 2^n choices. Then for a specific v_1 there are $\binom{n}{2}$ ways to select positions i, j. [Remember that $v_1 \rightarrow v_4 \rightarrow v_3 \rightarrow v_2 \rightarrow v_1$ is the same cycle as $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$.] So at this point we have $\binom{n}{2}2^n$ cycles. But since each of $v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1 \rightarrow v_2$, $v_3 \rightarrow v_4 \rightarrow v_1 \rightarrow v_2 \rightarrow v_3$, and $v_4 \rightarrow v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4$ is the same cycle as $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$, the total number of *distinct* cycles of length four in Q_n is $(1/4)\binom{n}{2}2^n = \binom{n}{2}2^{n-2}, \quad n \geq 1$.

3. (a) Label the vertices of K_6 with $a, b, \ldots, f$. Of the five edges on a at least three have the same color, say red, and let these edges be $\{a,b\}, \{a,c\}, \{a,d\}$. If the edges $\{b,c\}, \{c,d\}, \{b,c\}$ are all blue, the result follows. If not, one of these edges, say $\{c,d\}$, is red and then $\{a,c\}, \{a,d\}, \{c,d\}$ yield a red triangle.

(b) Consider the six people as vertices. If two people are friends (strangers) draw a red (blue) edge connecting their respective vertices. The result then follows from part (a).

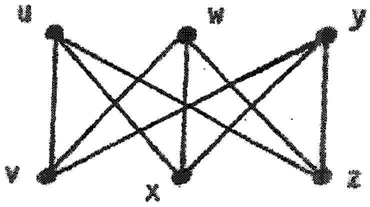
4. (a) (i) $|E| = (1/2)\binom{n}{2}$

(ii) For any undirected graph G , if G is not connected then $\overline{G}$ is connected. In this situation $G \cong \overline{G}$, so G is connected.

(b) Proof: When $n = 1$ we have K_1. For $n = 4$ the path on four vertices is an example of a self-complementary graph. The cycle on five vertices provides an example for $n = 5$.

Now suppose we have a self-complementary graph $G = (V, E)$. Construct the graph $G_1 = (V_1, E_1)$ where $V_1 = V \cup \{a, b, c, d\}$ (so none of a, b, c, d is in V) and $E_1 = E \cup \{\{a, b\}, \{b, c\}, \{c, d\}\} \cup \{\{v, a\} | v \in V\} \cup \{\{v, d\} | v \in V\}$. Then G_1 is self-complementary and $|V_1| = |V| + 4$.

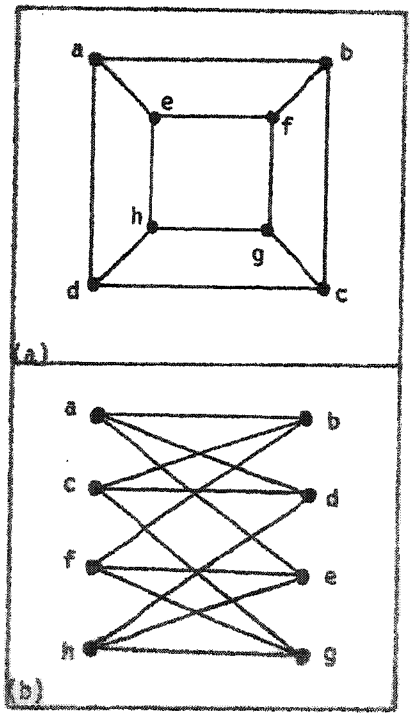
5. (a) We can redraw G_2 as



(b) 72

6.

Only the graph for the cube is bipartite as seen in part (b) of the given figure. In any of the other four graphs (See Fig. 11.59(b) and Fig. 11.60) there are cycles of odd length, so these graphs cannot be bipartite.



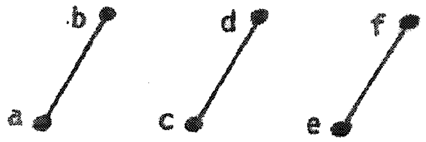
7. (a) Let the vertices of $K_{3,7}$ be partitioned as $V_1 \cup V_2$ where $|V_1| = 3$ and $|V_2| = 7$. Then there are (3)(7)(2)(6)(1)(5) = 1260 paths of length 5 where each such path contains all three vertices in V_1.

(b) With V_1, V_2 as in part (a) we find that there are $(1/2)(3)(7)(2)(6)(1)$ paths of length 4 that start and end with a vertex in V_1, and there are also $(1/2)(7)(3)(6)(2)(5)$ paths of length 4 that start and end with a vertex in V_2. Consequently, there are $126 + 630 = 756$ paths of length 4 in $K_{3,7}$.

(c) (Case 1: p is odd, $p = 2k+1$ for $k \in \mathbf{N}$). Here there are mn paths of length $p = 1$ (when $k = 0$) and $(m)(n)(m-1)(n-1)\cdots(m-k)(n-k)$ paths of length $p = 2k+1 \geq 3$. (Case 2: p is even, $p = 2k$ for $k \in \mathbf{Z}^+$). When $p < 2m$ (i.e., $k < m$) the number of paths of length p is $(1/2)(m)(n)(m-1)(n-1)\cdots(n-(k-1))(m-k)+(1/2)(n)(m)(n-1)(m-1)\cdots(m-(k-1))(n-k)$. For $p = 2m$ we find $(1/2)(n)(m)(n-1)(m-1)\cdots(m-(m-1))(n-m)$ paths of (longest) length $2m$.

8. (a) $(n=2): X = \{1,2\}$ and G consists of the single vertex v that corresponds to X.
$(n=3): X = \{1,2,3\}$. Here G is made up of three isolated vertices.
$(n=4): X = \{1,2,3,4\}$. Now G has six vertices and is drawn as follows:

a: {1,2}	d: {2,4}
b: {3,4}	e: {1,4}
c: {1,3}	f: {2,3}



(b) Let $v(\{a,b\})$ and $w(\{x,y\})$ be two vertices of G. If $\{a,b\} \cap \{x,y\} = \emptyset$, the edge $\{v,w\}$ is in G. If $\{a,b\} \cap \{x,y\} \neq \emptyset$, assume without loss of generality that $a = x$ but $b \neq y$. Hence a, b, y are three distinct elements of X and since $|X| \geq 5$, let $c, d \in X$ with $c \neq d$ and $c, d \notin \{a, b, y\}$. Then there exist edges from $\{a,b\}$ to $\{c,d\}$ and from $\{c,d\}$ to $\{x(=a), y\}$, since $\{a,b\} \cap \{c,d\} = \emptyset = \{c,d\} \cap \{x,y\}$. Hence G is connected.

(c) For $n = 5$ G is (isomorphic to) the Petersen graph, which is nonplanar. For $n \geq 6$ G contains a subgraph isomorphic to the Petersen graph and consequently G is nonplanar.

9. (a) Let I be independent and $\{a,b\} \in E$. If neither a nor b is in $V - I$, then $a, b \in I$, and since they are adjacent, I is not independent. Conversely, if $I \subseteq V$ with $V - I$ a covering of G, then if I is not independent there are vertices $x, y \in I$ with $\{x,y\} \in E$. But $\{x,y\} \in E \Longrightarrow$ either x or y is in $V - I$.

(b) Let I be a largest maximal independent set in G and K a minimal covering. From part (a), $|K| \leq |V - I| = |V| - |I|$ and $|I| \geq |V - K| = |V| - |K|$, or $|K| + |I| \geq |V| \geq |K| + |I|$.

10. (a) Let D be a minimal dominating set for G. If $V - D$ is not dominating, then there is a vertex $x \in D$ such that x is not adjacent to any vertex in $V - D$. Since G has no isolated vertices, x is adjacent to at least one vertex in $D - \{x\}$ and $D - \{x\}$ is a dominating set, contradicting the minimality of D.

(b) Suppose that I is a dominating set. If I is independent but not maximal independent, then there is a vertex $v \in V$ such that v is not in I and is not adjacent to any vertex in I. But this contradicts I being a dominating set. Conversely, if I is maximal independent then every vertex in V is in I or is adjacent to a vertex in I. Hence I is dominating.

(c) $\gamma(G) \leq \beta(G)$ follows from part (b). For the other condition, let $\chi(G) = m$. We can partition the vertices of G into m cells V_i, $1 \leq i \leq m$, where two vertices are in the same cell if they have the same color in G. Each of these cells is an independent set so $|V_i| \leq \beta(G)$, for all $1 \leq i \leq m$. Since $|V| = \sum_{i=1}^{m} |V_i|$, $|V| \leq \sum_{i=1}^{m} \beta(G) = m\beta(G) = \beta(G)\chi(G)$.

11. Since we are selecting n edges and no two have a common vertex, the selection of n edges will include exactly one occurrence of every vertex. We consider two mutually disjoint and exhaustive cases:

(1) The edge $\{x_n, y_n\}$ is in the selection: Then $\{x_{n-1}, x_n\}$ and $\{y_{n-1}, y_n\}$ are not in the selection and we must select the remaining $n-1$ edges from the resulting subgraph (a ladder graph with $n-1$ rungs) in a_{n-1} ways.

(2) The edge $\{x_n, y_n\}$ is not in the selection: Then in order to have x_n and y_n appear in the selection we must include edges $\{x_{n-1}, x_n\}$ and $\{y_{n-1}, y_n\}$. Consequently, we must now select the other $n-2$ edges from the resulting subgraph (a ladder graph with $n-2$ rungs) in a_{n-2} ways.

Hence $a_n = a_{n-1} + a_{n-2}$, $a_0 = 1$, $a_1 = 1$, and $a_n = F_{n+1}$, the $(n+1)$st Fibonacci number.

12. There are two cases to consider:
(1) The vertex y_n is not used. Then there are a_{n-1} independent subsets that contain x_n, and another a_{n-1} such subsets that do not contain x_n.
(2) The vertex y_n is included in the independent subset. Now we cannot use either of the vertices x_n or y_{n-1}. Consequently, there are a_{n-2} such subsets for each of the following situations: (i) x_{n-1} is in the subset; and (ii) x_{n-1} is not in the subset.
These considerations give rise to the recurrence relation

$$a_n = 2a_{n-1} + 2a_{n-2},$$

with initial conditions $a_0 = 1$, $a_1 = 3$. (We used $a_2 = 8$ to determine $a_0 = 1$.)
To solve this recurrence relation let $a_n = Ar^n$, where $A \neq 0$, $r \neq 0$. This leads to the characteristic equation

$$r^2 - 2r - 2 = 0,$$

and the characteristic roots $1 \pm \sqrt{3}$. Consequently, $a_n = A_1(1+\sqrt{3})^n + A_2(1-\sqrt{3})^n$, where A_1, A_2 are constants.

$1 = a_0 = A_1 + A_2$
$3 = a_1 = A_1(1+\sqrt{3}) + A_2(1-\sqrt{3}) = (A_1 + A_2) + \sqrt{3}(A_1 - A_2)$

$= 1 + \sqrt{3}(A_1 - A_2)$, so $2/\sqrt{3} = (A_1 - A_2)$.
Therefore, $A_1 = (\sqrt{3}+2)/2\sqrt{3}$, $A_2 = (\sqrt{3}-2)/2\sqrt{3}$, and
$a_n = [(\sqrt{3}+2)/2\sqrt{3}](1+\sqrt{3})^n + [(\sqrt{3}-2)/2\sqrt{3}](1-\sqrt{3})^n$, $n \geq 0$ (or $n \geq 1$).

13. If the vertex y_n is included in the independent subset then we cannot use any of the vertices y_{n-1}, x_{n-1}, or x_n. There are a_{n-2} such subsets — and another a_{n-2} independent subsets where x_n is included. In addition, there are a_{n-1} independent subsets when both x_n and y_n are excluded. This leads us to the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2},$$

with initial conditions $a_1 = 3$, $a_2 = 5$.

To solve this recurrence relation let $a_n = Ar^n$, where $A \neq 0$, $r \neq 0$. This leads to the characteristic equation

$$r^2 - r - 2 = 0,$$

and the characteristic roots -1 and 2. Therefore, $a_n = A_1(-1)^n + A_2(2^n)$, where A_1, A_2 are constants.

$a_1 = 3, a_2 = 5 \Rightarrow 2a_0 = 5 - 3 \Rightarrow a_0 = 1$.
$1 = a_0 = A_1 + A_2$.
$3 = a_1 = -A_1 + 2A_2 = -(1 - A_2) + 2A_2 = -1 + 3A_2$, so $A_2 = 4/3$, and $A_1 = 1 - A_2 = -1/3$.
Consequently, $a_n = (-1/3)(-1)^n + (4/3)(2^n)$, $n \geq 0$ (or $n \geq 1$).

14. $a_0 = a_1 = 0$
For $n \geq 2$, $a_n = \binom{n}{2} = (1/2)n(n-1) > 0$.
$1/(1-x) = 1 + x + x^2 + x^3 + \ldots$
$(d/dx)[1/(1-x)] = 1 + 2x + 3x^2 + 4x^3 + \ldots$
$(d/dx)[1/(1-x)] = (d/dx)[(1-x)^{-1}] = (-1)(1-x)^{-2}(-1) = (1-x)^{-2}$
$(1-x)^{-2} = 1 + 2x + 3x^2 + 4x^3 + \ldots$
$(d/dx)[(1-x)^{-2}] = (-2)(1-x)^{-3}(-1) = 2(1-x)^{-3}$, so $2(1-x)^{-3} = 2 + 3 \cdot 2x + 4 \cdot 3x^2 + 5 \cdot 4x^3 + \ldots$

$$2x^2/(1-x)^3 = 2 \cdot 1x^2 + 3 \cdot 2x^3 + 4 \cdot 3x^4 + 5 \cdot 4x^5 + \ldots = \sum_{n=2}^{\infty} n(n-1)x^n = \sum_{n=0}^{\infty} n(n-1)x^n.$$

Hence $f(x) = x^2/(1-x)^3 = \sum_{n=0}^{\infty}[n(n-1)/2]x^n$ is the generating function for the sequence $a_n = \binom{n}{2}$, $n \geq 0$.

15. (a) $\gamma(G) = 2$; $\beta(G) = 3$; $\chi(G) = 4$.

(b) G has neither an Euler trail nor an Euler circuit; G does have a Hamilton cycle.

(c) G is not bipartite but it is planar.

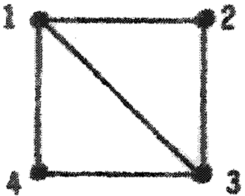
16. (a) (i) $m = 2$, $n = 8$ (ii) $m = n = 4$

(b) (i) $K_{m,n}$, for $m \leq n$, has an Euler circuit but not a Hamilton cycle if m and n are both even and $m \neq n$.

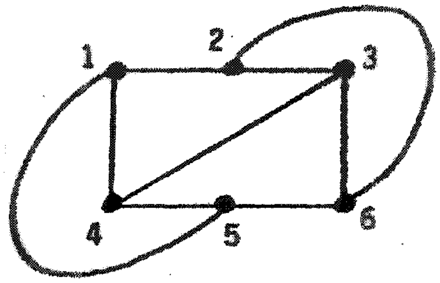
(ii) When m, n are both even and $m = n$, then $K_{m,n}$ has both an Euler circuit and a Hamilton cycle.

17. (a) $\chi(G) \geq \omega(G)$ (b) They are equal.

18. (a) (i) Here vertex 1 is for edge $\{a, c\}$, 2 for $\{a, b\}$, 3 for $\{b, c\}$, and 4 for $\{c, d\}$.

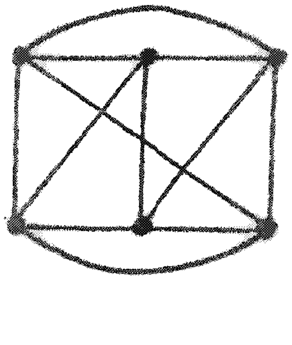


(ii) Here the correspondence between vertices in $L(G)$ and edges in G is given by
$1: \{y, z\}$; $2: \{x, z\}$; $3: \{w, x\}$;
$4: \{w, y\}$; $5: \{u, y\}$; $6: \{u, x\}$



(b) Let $v \in V$ with $\deg(v) = k$. Then there are k edges in G of the form $\{v_i, v\}$, $1 \leq i \leq k$. Any two of these edges are adjacent at v and give rise to an edge in $L(G)$. Hence v brings about $\binom{\deg(v)}{2}$ edges in $L(G)$. In total, $L(G)$ has $\sum_{v \in V} \binom{\deg(v)}{2} = (1/2) \sum_{v \in V} \deg(v)[\deg(v) - 1] = (1/2) \sum_{v \in V} \deg(v)^2 - (1/2) \sum_{v \in V} \deg(v) = (1/2) \sum_{v \in V} \deg(v)^2 - e$ edges.

(c) First we shall prove that $L(G)$ is connected. Let e_1, e_2 be two vertices in $L(G)$ where e_1 arises from edge $\{a, b\}$ and e_2 from edge $\{x, y\}$ in G. Since G is connected there is a path in G from b to x : $b \rightarrow v_1 \rightarrow v_2 \rightarrow \ldots \rightarrow v_k \rightarrow x$ and a path from a to y : $a \rightarrow b \rightarrow v_1 \rightarrow \ldots \rightarrow v_k \rightarrow x \rightarrow y$. These vertices and edges then determine a path in $L(G)$ from e_1 to e_2, so $L(G)$ is connected. Now for any vertex e in $L(G)$, let $\{a, b\}$ be the edge in G that determines e. Then $\deg(e)$ (in $L(G)$) $= (\deg(a)-1)+(\deg(b)-1)$, an even integer, since $\deg(a)$, $\deg(b)$ are both even. Hence by Theorem 11.3, $L(G)$ has an Euler circuit. Furthermore, the ordered list of edges in an Euler circuit for G determine a corresponding Hamilton cycle for the vertices of $L(G)$.



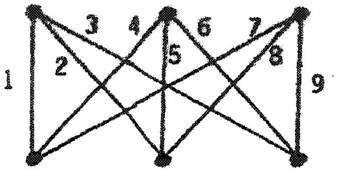
(d) For $G = K_4$, $L(K_4)$ is shown here. This graph has both an Euler circuit and a Hamilton cycle. However, for each vertex v in K_4, $\deg(v) = 3$, so K_4 does not have an Euler circuit.

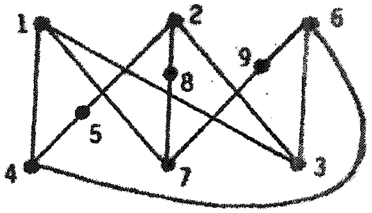
(e) Suppose that $G = (V, E)$ has a Hamilton cycle $v_1 \to v_2 \to v_3 \to \ldots \to v_n \to v_1$ and let $e_i = \{v_i, v_{i+1}\}$, $1 \le i \le n-1$, and $e_n = \{v_n, v_1\}$. Then there is a cycle in $L(G)$ on the vertices e_i, $1 \le i \le n$. If $|E| = n$, then this cycle is a Hamilton cycle. If $|E| > n$, let $e \in E$, where $e \neq e_i$, $1 \le i \le n$, and let $e = \{v_i, v_j\}$, $1 \le i < j \le n$. (This also takes care of the case where G is a multigraph.) In $L(G)$ there are edges $\{e_{i-1}, e\}$, where $e_{i-1} = e_n$ if $i = 1$, and $\{e, e_i\}$, and we can extend the cycle in $L(G)$ by replacing $\{e_{i-1}, e_i\}$ by the edges $\{e_{i-1}, e\}$ and $\{e, e_i\}$. Since $|E|$ is finite, as we continue enlarging our present cycle in this way, we obtain a Hamilton cycle for $L(G)$.

(f) The graph in Fig. 11.99(b) has no Hamilton cycle, but its line graph, as seen in part (a), has a Hamilton cycle.

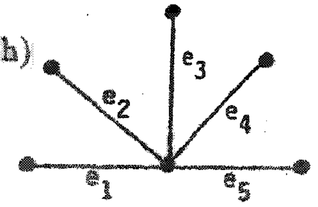
(g) For $G = K_5$, $L(G)$ has 10 vertices and 30 edges. Since G is connected, $L(G)$ is connected. But since $30 > 3(10) - 6$, it follows by Corollary 11.3 that $L(G)$ is nonplanar.

For $G = K_{3,3}$ we number the edges as shown in the first figure. Then in $L(G)$ we find the subraph shown in the second figure, so $L(G)$ is nonplanar.





(h)

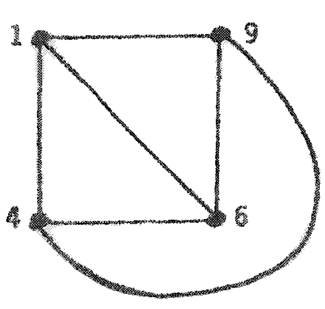


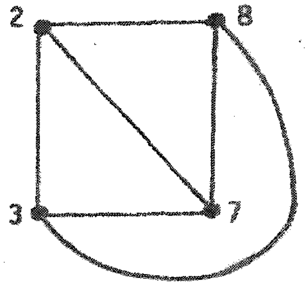
Let G be the graph shown here with six vertices (five pendant and one of degree 5). Then in $L(G)$ there are five vertices each of degree four, and $L(G) = K_5$, a nonplanar graph.

19. (a) The constant term is 3, not 0. This contradicts Theorem 11.11.
(b) The leading coefficient is 3, not 1. This contradicts the result in Exercise 17 of Section 11.6.
(c) The sum of the coefficients in -1, not 0. This contradicts Theorem 11.12.

20. (a) $x^3y - xy^3 = xy(x^2 - y^2) = xy(x - y)(x + y)$
If x or y is even then xy and $xy(x - y)(x + y)$ are both even. When x, y are both odd, then $x - y$ and $x + y$ are both even, as is $xy(x - y)(x + y)$.

(b)





(c) From part (a) $x^3y - xy^3 = xy(x-y)(x+y)$ is always even. If the units digit of either x or y is 0 or 5, then the result follows. Also, if x, y have the same units digit, then $x - y$ is a multiple of 10 and so is $x^3y - xy^3$. In all other cases we have three positive integers x, y, z with distinct units digits in the set $V = \{1, 2, 3, 4, 6, 7, 8, 9\}$. By the pigeonhole principle two of these integers, say x and y, must be in the same component (K_4) of G. Since the component is complete, $\{x, y\}$ is an edge, so either $x + y$ or $x - y$ is divisible by 5. Hence $x^3y - xy^3$ is divisible by 10.

21. (a) $a_1 = 2$, $a_2 = 3$. For $n \geq 3$ label the vertices of P_n as $v_1, v_2, v_3, \ldots, v_n$ where the edges are $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}$. In constructing an independent subset S from P_n we consider two cases:

(1) $v_n \notin S$: Then S is an independent subset of P_{n-1} and there are a_{n-1} such subsets.

(2) $v_n \in S$: Then $v_{n-1} \notin S$ and $S - \{v_n\}$ is one of the a_{n-2} independent subsets of P_{n-2}.

Hence $a_n = a_{n-1} + a_{n-2}$, $n \geq 3$, $a_1 = 2$, $a_2 = 3$, *or* $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$, $a_0 = 1$, $a_1 = 2$. So $a_n = F_{n+2}$, the $(n+2)$nd Fibonacci number.

(b) Consider the subgraph of G_1 induced by the vertices 1,2,3,4. From part (a) we know that this subgraph determines 8 ($= F_6$, the sixth (nonzero) Fibonacci number) independent subsets of {1,2,3,4}. Therefore, the graph G_1 has $1 + F_6$ independent subsets of vertices.

Likewise the graph G_2 has $1 + F_7$ independent subsets (of vertices), and the graph G_n determines $1 + F_{n+2}$ such subsets.

(c) $H_1 : 3 + F_6 = (2^2 - 1) + F_6$
$H_2 : 3 + F_7 = (2^2 - 1) + F_7$
$H_3 : 3 + F_{n+2} = (2^2 - 1) + F_{n+2}$

(d) There are $2^s - 1 + m$ independent subsets of vertices for graph $G' = (V', E')$.

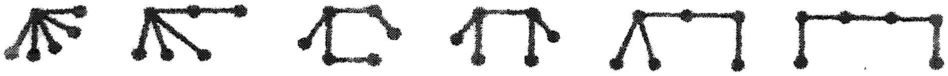
22. Proof: First we prove that G is connected. If not, let C_1, C_2 be two of the components of G and let $v_1, v_2 \in V$ with v_1 a vertex in C_1 and v_2 a vertex in C_2. If C_1 has n_1 vertices and C_2 has n_2 vertices, then $10 = \deg(v_1) + \deg(v_2) \leq (n_1 - 1) + (n_2 - 1) = (n_1 + n_2) - 2 \leq 8$. This contradiction tells us that G is connected.

Here $|E| = (\frac{1}{2})\sum_v \deg(v) = (\frac{1}{2})(50) = 25$. If G were planar, then we would have $25 = |E| \leq 3|V| - 6 = 3(10) - 6 = 24$, according to Corollary 11.3. This contradiction now tells us that G is nonplanar.

CHAPTER 12
TREES

Section 12.1

1. (a)



(b) 5

2. $|E_1| = 17 \Longrightarrow |V_2| = 18$. $|V_2| = 2|V_1| = 36 \Longrightarrow |E_2| = 35$.

3. (a) Let $e_1, e_2, \ldots, e_7$ denote the numbers of edges for the seven trees, and let $v_1, v_2, \ldots v_7$, respectively, denote the numbers of vertices. Then $v_i = e_i + 1$, for all $1 \leq i \leq 7$, and $|V_1| = v_1 + v_2 + \ldots + v_7 = (e_1 + e_2 + \ldots + e_7) + 7 = 40 + 7 = 47$.

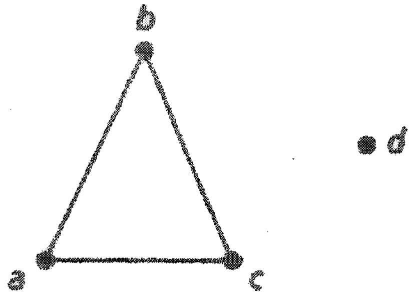
(b) Let n denote the number of trees in F_2. Then if e_i, v_i, $1 \leq i \leq n$, denote the numbers of edges and vertices, respectively, in these trees, it follows that $v_i = e_i + 1$, for all $1 \leq i \leq n$, and $62 = v_1 + v_2 + \ldots + v_n = (e_1+1)+(e_2+1)+\ldots+(e_n+1) = (e_1+e_2+\ldots+e_n)+n = 51+n$, so $n = 62 - 51 = 11$ trees in F_2.

4. $e = v - \kappa$

5. A path is a tree with only two pendant vertices.

6. (a) Since a tree contains no cycles it cannot have a subgraph homeomorphic to either K_5 or $K_{3,3}$.
(b) If $T = (V, E)$ is a tree then T is connected and, by part (a), T is planar. By Theorem 11.6, $|V| - |E| + 1 = 2$ or $|V| = |E| + 1$.

7.



8. (a) Let x be the number of pendant vertices. Then $2|E| = \sum_{v \in V} \deg(v) = x + 4(2) + 1(3) + 2(4) + 1(5)$ and $|E| = |V| - 1 = x + 4 + 1 + 2 + 1 - 1 = x + 7$.
So $2(x+7) = x + 24$ and $x = 10$.

(b) $2|E| = \sum_{v \in V} \deg(v) = v_1 + v_2(2) + v_3(3) + \ldots + v_m(m)$
$|E| = |V| - 1 = (v_1 + v_2 + \ldots v_m) - 1$
$2(v_1 + v_2 + \ldots + v_m - 1) = v_1 + 2v_2 + \ldots + mv_m$, so $v_1 = v_3 + 2v_4 + 3v_5 + \ldots + (m-2)v_m + 2$, and $|V| = v_1 + v_2 + \ldots + v_m = [v_3 + 2v_4 + \ldots + (m-2)v_m + 2] + v_2 + v_3 + \ldots + v_m = v_2 + 2v_3 + 3v_4 + \ldots + (m-1)v_m + 2$, $|E| = |V| - 1 = v_2 + 2v_3 + \ldots + (m-1)v_m + 1$.

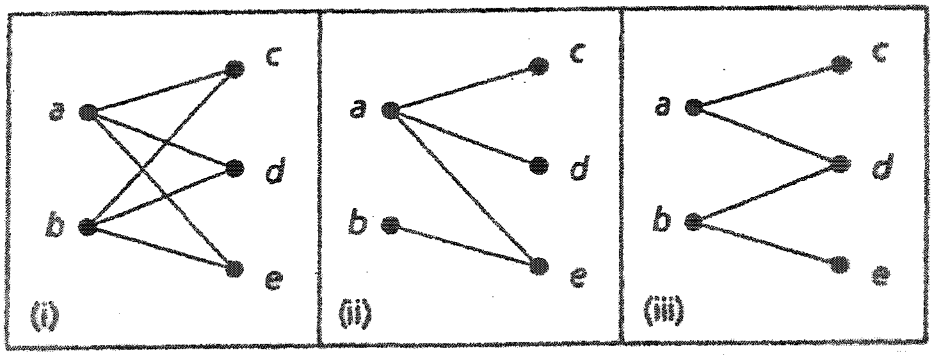
9. If there is a (unique) path between each pair of vertices in G then G is connected. If G contains a cycle then there is a pair of vertices x, y with two distinct paths connecting x and y. Hence, G is a loop-free connected undirected graph with no cycles, so G is a tree.

10. 31

11. Since T is a tree, there is a unique path connecting any two distinct vertices of T. Hence there are $\binom{n}{2}$ distinct paths in T.

12. If G contains no cycles then G is a tree. But then G must have at least two pendant vertices. This graph has only one pendant vertex.

13. (a) In part (i) of the given figure we find the complete bipartite graph $K_{2,3}$. Parts (ii) and (iii) of the figure provide two nonisomorphic spanning trees for $K_{2,3}$.
(b) Up to isomorphism these are the only spanning trees for $K_{2,3}$.



14. Let $V = \{x, y, w_1, w_2, \ldots, w_n\}$ be the vertices for $K_{2,n}$, where $V_1 = \{x, y\}$, $V_2 = \{w_1, w_2, \ldots, w_n\}$ and all edges have one vertex in V_1 and the other in V_2. If T is a spanning tree for $K_{2,n}$, then T has $n+1$ edges and $\deg(x) + \deg(y) = n + 1$. So the number of nonisomorphic spanning trees for $K_{2,n}$ is the number of partitions of n into two (nonzero) summands. This number is $\lfloor (n+1)/2 \rfloor$.

15. (a) 6: Any one of the six spanning trees for C_6 (the cycle on six vertices) together with the path connecting f to k.
(b) $6 \cdot 6 = 36$

16. (1) This graph has $9 = 3 \cdot 4 - 3 = 3 + 3(4-2)$ vertices, so any spanning tree for it will have eight edges. There are $12 = 3 \cdot 4$ edges (in total) so we shall remove four edges. Two edges must be removed from one 4-cycle (a cycle on four vertices) and one edge from each of the other two 4-cycles. When two edges from a 4-cycle are removed one must be from the 3-cycle (induced by a, b, and c) – otherwise, we get a disconnected subgraph. There are three ways to select the 4-cycle for removing two edges and three ways to select the edge not on the 3-cycle. We then select one edge from each of the remaining 4-cycles in $4 \cdot 4$ ways. So the number of nonidentical spanning trees for this graph is $3(4-1)(4^2) = 144$.

(2) Here the graph has $8 = 4 \cdot 3 - 4 = 4 + 4(3-2)$ vertices and $12 = 4 \cdot 3$ edges. There are $4(3-1)(3^3) = 216$ nonidentical spanning trees.

(3) This graph has $16 = 4 \cdot 5 - 4 = 4 + 4(5-2)$ vertices and $20 = 4 \cdot 5$ edges. There are $4(5-1)(5^3) = 2000$ nonidentical spanning trees.

17. (a) $n \geq m+1$
(b) Let k be the number of pendant vertices in T. From Theorem 11.2 and Theorem 12.3 we have

$$2(n-1) = 2|E| = \sum_{v \in V} \deg(v) \geq k + m(n-k).$$

Consequently, $[2(n-1) \geq k + m(n-k)] \Rightarrow [2n - 2 \geq k + mn - mk] \Rightarrow [k(m-1) \geq 2 - 2n + mn = 2 + (m-2)n \geq 2 + (m-2)(m+1) = 2 + m^2 - m - 2 = m^2 - m = m(m-1)]$, so $k \geq m$.

18. $\sum_{v \in V} \deg(v) = 2|E| = 2(|V| - 1) = 2(999) = 1998.$

19. (a) If the complement of T contains a cut set, then the removal of these edges disconnects G and there are vertices x, y with no path connecting them. Hence T is not a spanning tree for G.

(b) If the complement of C contains a spanning tree, then every pair of vertices in G has a path connecting them and this path includes no edges of C. Hence the removal of the edges in C from G does not disconnect G, so C is not a cut set for G.

20. $(d) \Longrightarrow (e)$: Let C be a cycle (in G) with r vertices and r edges. Since G is connected, the remaining vertices of G can each be connected to a vertex in C by a path (in G). Each such connection requires at least one new edge. Consequently, in G, $|E| \geq |V|$, contradicting $|V| = |E| + 1$. So G has no cycles and is connected, and G is a tree. Let G' be the graph obtained by adding edge $\{a, b\}$ to G. Since $\{a, b\} \notin E$, there is a unique path P, of length at least 2 in G, that connects a to b. In

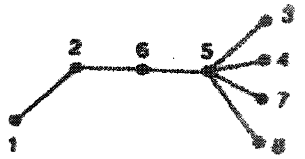
G', $P \cup \{\{a,b\}\}$ is a cycle. If G' contains a second cycle C_1, then C_1 must contain edge $\{a,b\}$. If not, then G would contain a cycle. This second cycle $C_1 = P_1 \cup \{\{a,b\}\}$, where P_1 is a path in G and $P_1 \neq P$. This contradicts Theorem 12.1.

$(e) \Longrightarrow (a)$: If G is not connected, let C_1, C_2 be components of G with $a \in C_1, b \in C_2$. Then adding the edge $\{a,b\}$ to G would not result in a cycle. Consequently, G is connected with no cycles, so G is a tree.

21. (a) (i) 3,4,6,3,8,4 (ii) 3,4,6,6,8,4

(b) No pendant vertex of the given tree appears in the sequence so the result is true for these vertices. When an edge $\{x,y\}$ is removed and y is a pendant vertex (of the tree or one of the resulting subtrees), then the $\deg(x)$ is decreased by 1 and x is placed in the sequence. As the process continues either (i) this vertex x becomes a pendant vertex in a subtree and is removed but not recorded in the sequence, or (ii) the vertex x is left as one of the last two vertices of an edge. In either case x has been listed in the sequence $(\deg(x) - 1)$ times.

(c)



(d) Input: The given Prüfer code $x_1, x_2, \ldots, x_{n-2}$.
Output: The unique tree T with n vertices labeled with $1, 2, \ldots, n$. (This tree T has the Prüfer code $x_1, x_2, \ldots, x_{n-2}$.)

```
$C := [x_1, x_2, \ldots, x_{n-2}]$        {Initializes $C$ as a list (ordered set).}
$L := [1, 2, \ldots, n]$                 {Initializes $L$ as a list (ordered set).}
$T := \emptyset$
for $i := 1$ to $n - 2$ do
    $v :=$ smallest element in $L$ not in $C$
    $w :=$ first entry in $C$
    $T := T \cup \{\{v, w\}\}$           {Add the new edge $\{v, w\}$ to the present forest.}
    delete $v$ from $L$
    delete the first occurrence of $w$ from $C$
$T := T \cup \{\{y, z\}\}$               {The vertices $y, z$ are the last two remaining entries in $L$.}
```

22. Let V be the vertex set for K_n. From the previous exercise we know that there are $(n-1)^{n-3}$ spanning trees for the subgraph of K_n induced by $V - v$ (namely, the complete graph K_{n-1}). For v to be a pendant vertex it can be adjacent to only one of the $n - 1$ vertices in $V - v$. Consequently, there are $(n-1)[(n-1)^{n-3}]$ spanning trees of K_n where v is a pendant vertex.

23. (a) If the tree contains $n+1$ vertices then it is (isomorphic to) the complete bipartite graph $K_{1,n}$ – often called the *star* graph.
(b) If the tree contains n vertices then it is (isomorphic to) a path on n vertices.

24. Consider the Prüfer codes for the n^{n-2} labeled trees on n vertices. For a given labeled tree, the pendant vertices (of degree 1) have the labels which do *not* appear in the Prüfer code for that tree. If there are k pendant vertices, then there are k labels missing from the code and these can be selected in $\binom{n}{k}$ ways. That leaves $n-k$ labels that must *all* be placed in the $n-2$ positions of the Prüfer code. This can be counted as the number of *onto* functions from the set of $n-2$ positions to the set of $n-k$ labels – that is,
$(n-k)!\ S(n-2, n-k)$.

The result then follows by the rule of product.

25. Let $E_1 = \{\{a,b\}, \{b,c\}, \{c,d\}, \{d,e\}, \{b,h\}, \{d,i\}, \{f,i\}, \{g,i\}\}$ and
$E_2 = \{\{a,h\}, \{b,i\}, \{h,i\}, \{g,h\}, \{f,g\}, \{c,i\}, \{d,f\}, \{e,f\}\}$.

Section 12.2

1.
(a) f,h,k,p,q,s,t (b) a (c) d
(d) e,f,j,q,s,t (e) q,t (f) 2
(g) k,p,q,s,t

2. (a)

Vertex	Level Number
p	35
s	36
t	36
v	37
w	38
x	38
y	39
z	39

(b) The vertex u has 37 ancestors.
(c) The vertex y has 39 ancestors.

3. (a) $1 + w - x\ y * \pi \uparrow z\ 3$ (b) 0.4

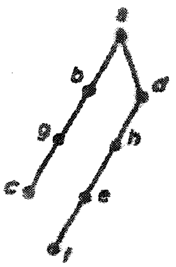
4. (a) 5 (b) 2.1.3 (c) 4 (including the root)
(d) 2.1.3.x, $1 \leq x \leq 5$; 2.1.3, 2.1.2, 2.1.1, 2.1, 2, 1.

5. Preorder: r,j,h,g,e,d,b,a,c,f,i,k,m,p,s,n,q,t,v,w,u
Inorder: h,e,a,b,d,c,g,f,j,i,r,m,s,p,k,n,v,t,w,q,u
Postorder: a,b,c,d,e,f,g,h,i,j,s,p,m,v,w,t,u,q,n,k,r

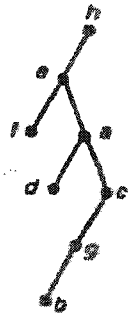
6. Preorder: 1,2,5,9,14,15,10,16,17,3,6,4,7,8,11,12,13
Postorder: 14,15,9,16,17,10,5,2,6,3,7,11,12,13,8,4,1

7. (a)

(i) & (iii)

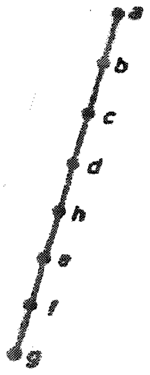


(ii)

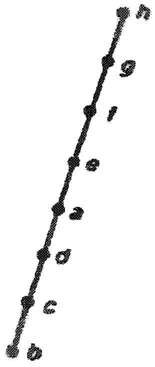


(b)

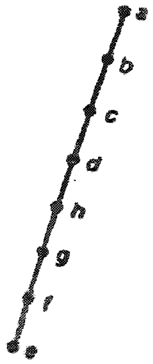
(i)



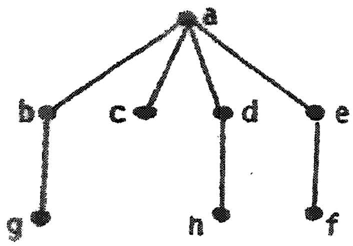
(ii)



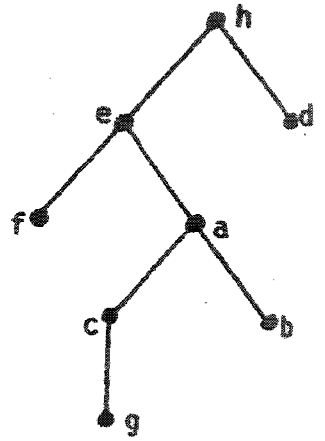
(iii)



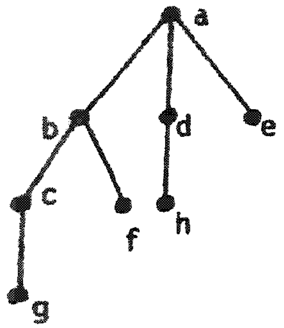
8. (a) (i) & (iii)



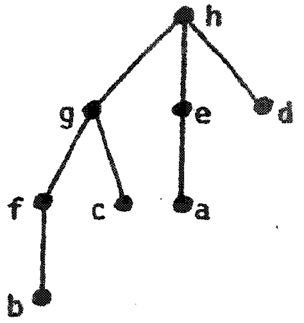
(ii)



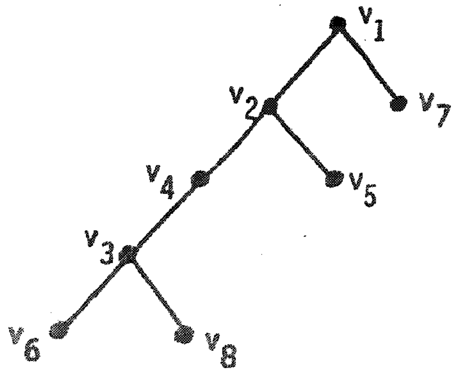
(b) (i) & (iii)



(ii)



9.



G is connected.

10. (a) Here the maximum height is $n-1$.
(b) In this case n must be odd and the maximum height is $(n-1)/2$.

11. Theorem 12.6
(a) Each internal vertex has m children so there are mi vertices that are the children of some other vertex. This accounts for all vertices in the tree except the root. Hence $n = mi + 1$
(b) $\ell + i = n = mi + 1 \Longrightarrow \ell = (m-1)i + 1$

(c) $\ell = (m-1)i + 1 \Longrightarrow i = (\ell - 1)/(m-1)$
$n = mi + 1 \Longrightarrow i = (n-1)/m$.

(Corollary 12.1)
Since the tree is balanced $m^{h-1} < \ell \leq m^h$ by Theorem 12.7.
$m^{h-1} < \ell \leq m^h \Longrightarrow \log_m(m^{h-1}) < \log_m(\ell) \leq \log_m(m^h) \Longrightarrow$
$(h-1) < \log_m \ell \leq h \Longrightarrow h = \lceil \log_m \ell \rceil$.

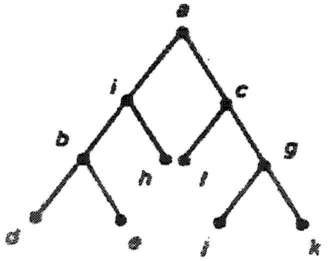
12. From Theorem 12.6 (c) we have
(a) $(\ell-1)/(m-1) = (n-1)/m \Longrightarrow (n-1)(m-1) = m(\ell-1) \Longrightarrow$
$n - 1 = (m\ell - m)/(m-1) \Longrightarrow n = [(m\ell - m)/(m-1)] + 1 =$
$[(m\ell - m) + (m-1)]/(m-1) = (m\ell - 1)/(m-1)$.

(b) $(\ell-1)/(m-1) = (n-1)/m \Longrightarrow \ell - 1 = (m-1)(n-1)/m \Longrightarrow$
$\ell = [(m-1)(n-1) + m]/m = [(m-1)n + 1]/m$.

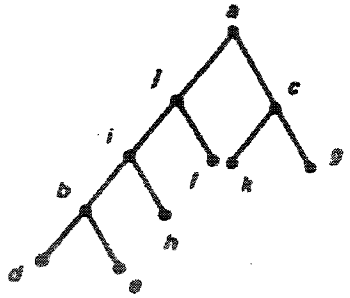
13. (a) From part (a) of Theorem 12.6 we have $|V|$ = number of vertices in $T = 3i + 1 = 3(34) + 1 = 103$. So T has $103 - 1 = 102$ edges. From part (b) of the same theorem we find that the number of leaves in T is $(3-1)(34) + 1 = 69$. [We can also obtain the number of leaves as $|V| - i = 103 - 34 = 69$.]

(b) It follows from part (c) of Theorem 12.6 that the given tree has $(817 - 1)/(5 - 1) = 816/4 = 204$ internal vertices.

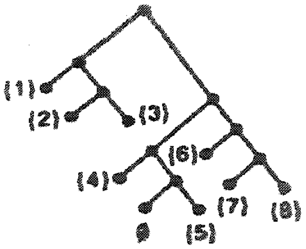
14. (a)



(b)



15. (a)



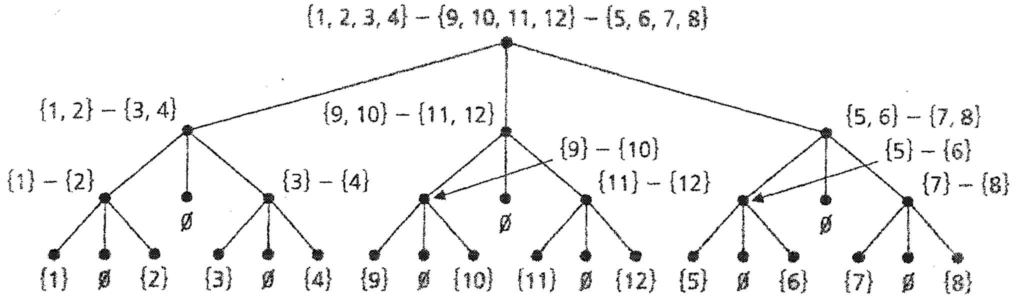
(b) 9; 5 (c) $h(m-1)$; $(h-1) + (m-1)$

16. (a) From Theorem 12.6 (c), with $\ell = 25$, $m = 2$, it follows that $i = (25-1)/(2-1) = 24$. Hence 24 cans of tennis balls are opened and 24 matches are played.
(b) Either 4 or 5.

17. 21845; $1 + m + m^2 + \ldots + m^{h-1} = (m^h - 1)/(m-1)$.

18. $2[5 + 5^2 + 5^3 + 5^4 + 5^5 + 5^6 + 5^7]$; $2[5^5 + 5^6 + 5^7]$

19.



20. The number of vertices at level $h-1$ is m^{h-1}. Among these we find $m^{h-1} - b_{h-1}$ of the l leaves of T. Each of the b_{h-1} branch nodes account for m leaves (at level h). Therefore, $l = m^{h-1} - b_{h-1} + mb_{h-1} = m^{h-1} + (m-1)b_{h-1}$.

21. Let T be a complete binary tree with 31 vertices. The left and right subtrees of T are then *complete binary trees* on $2k+1$ and $30-(2k+1)$ vertices, respectively, with $0 \leq k \leq 14$.

The number of ways the left subtree can have $11 (= 2 \cdot 5 + 1)$ vertices is $(\frac{1}{6})\binom{10}{5}$. This leaves $19 (= 2 \cdot 9 + 1)$ vertices for the right subtree where there are $(\frac{1}{10})\binom{18}{9}$ possibilities. So by the rule of product there are $(\frac{1}{6})\binom{10}{5}(\frac{1}{10})\binom{18}{9} = 204,204$ complete binary trees on 31 vertices with 11 vertices in the left subtree of the root. A similar argument tells us that there are $(\frac{1}{11})\binom{20}{10}(\frac{1}{5})\binom{8}{4} = 235,144$ complete binary trees on 31 vertices with 21 vertices in the right subtree of the root.

22. $a_{n+1} = a_0a_n + a_1a_{n-1} + a_2a_{n-2} + \cdots + a_{n-1}a_1 + a_na_0$
[Compare with the equation for b_{n+1} in Section 10.5.]

23. (a) 1,2,5,11,12,13,14,3,6,7,4,8,9,10,15,16,17
(b) The preorder traversal of the rooted tree.

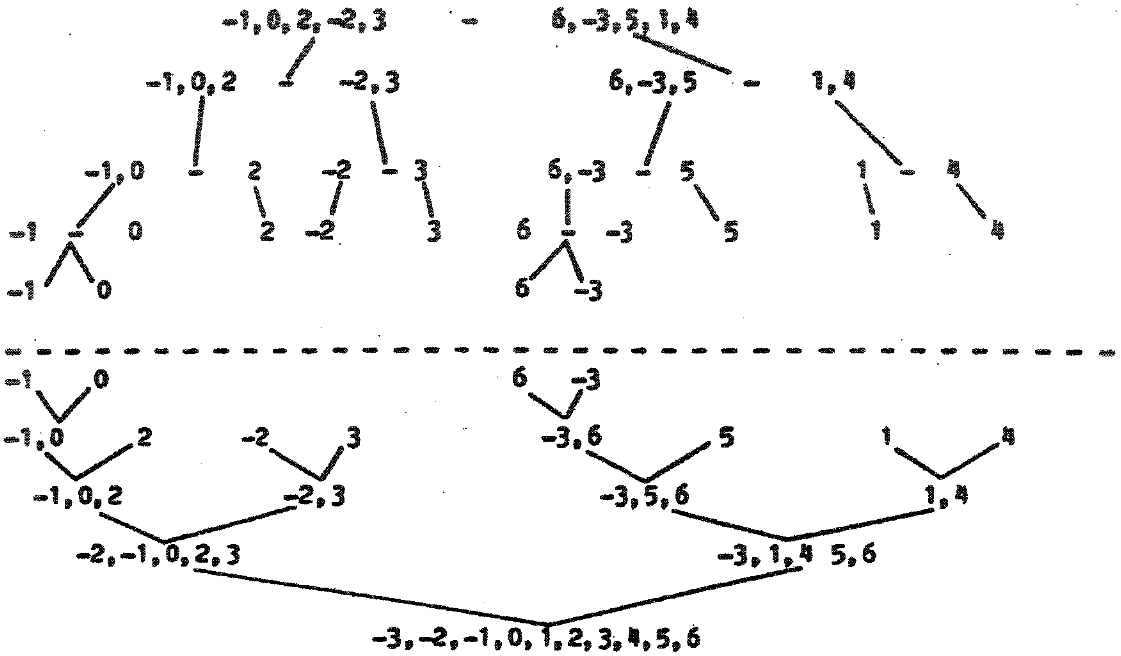
24. (a) 11,12,13,14,5,2,6,7,3,8,9,15,16,17,10,4,1
(b) The postorder traversal of the rooted tree.

Here the algorithm is iterative, while the one given in Definition 12.3 is recursive.

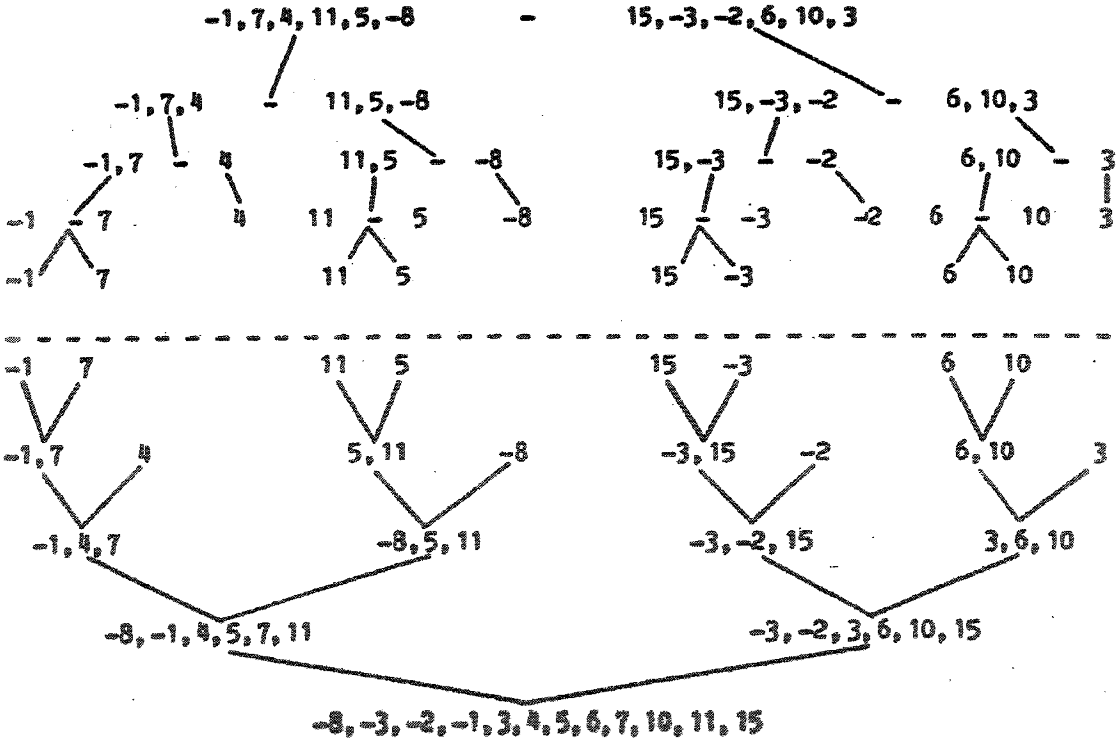
Section 12.3

1. (a) $L_1:\ 1,3,5,7,9 \qquad L_2:\ 2,4,6,8,10$
   (b) $L_1:\ 1,3,5,7,\ldots,2m-3,m+n$
   $L_2:\ 2,4,6,8,\ldots,2m-2,2m-1,2m,2m+1,\ldots,m+n-1$

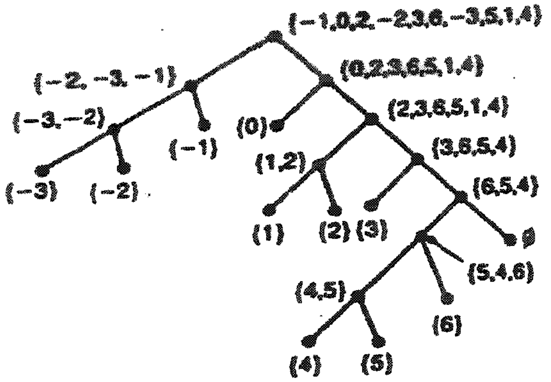
2. (a)



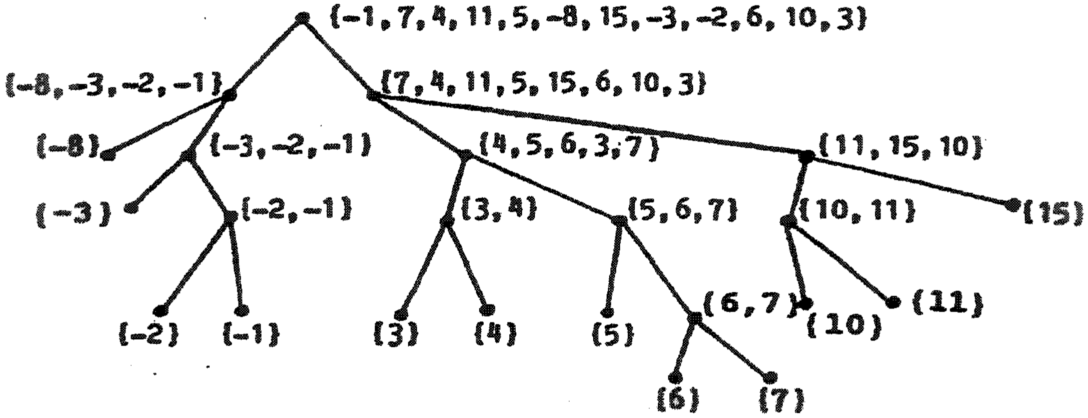
(b)



3. (a)



(b)



4. To establish this result we use mathematical induction (the alternative form). We know that $g(1) \leq g(2) \leq g(3) \leq g(4)$. So we assume that for all $i, j \in \{1, 2, 3, \ldots, n\}$, $i < j \Longrightarrow g(i) \leq g(j)$. Considering the case for $n+1$ we have two results to examine.

(1) If $n+1$ is odd then $n+1 = 2k+1$ for some $k \in \mathbf{Z}^+$. In the worst case, $g(n+1) = g(2k+1) = g(k)+g(k+1)+[k+(k+1)-1] = g(k)+g(k+1)+2k \geq g(k)+g(k)+(2k-1) = g(2k) = g(n)$, since $g(k+1) \geq g(k)$ by the induction hypothesis.

(2) If $n+1$ is even, then $n+1 = 2t$ for some $t \in \mathbf{Z}^+$. In the worst case, $g(n+1) = g(2t) = g(t)+g(t)+[t+t-1] = g(t)+g(t)+(2t-1) \geq g(t)+g(t-1)+(2t-2) = g(2t-1) = g(n)$, because $g(t) \geq g(t-1)$ by the induction hypothesis.

Consequently g is a monotone increasing function.

Section 12.4

1. (a) tear (b) tatener (c) rant

2. $x = y = z = 1$

3.

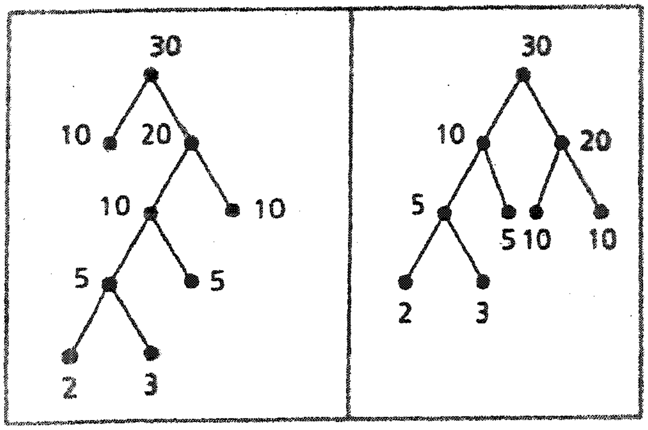
a:	111	e:	10	h:	010
b:	110101	f:	0111	i:	00
c:	0110	g:	11011	j:	110100
d:	0001				

4. (a) 2^3 (b) 2^7 (c) 2^{12} (d) 2^h

5. Since the tree has $m^7 = 279,936$ leaves, it follows that $m = 6$. From part(c) of Theorem 12.6 we find that there are $(m^7 - 1)/(m - 1) = (279,935)/5 = 55,987$ internal vertices.

6. $v = 1+m+m^2+\cdots+m^h = (1-m^{h+1})/(1-m) = (m^{h+1}-1)/(m-1)$, so $v(m-1)+1 = m^{h+1}$. Consequently, $h + 1 = \log_m[v(m-1)+1]$ and $h = \log_m[v(m-1)+1] - 1$.

7.



Amend part (a) of Step 2 for the Huffman tree algorithm as follows. If there are $n(> 2)$ such trees with smallest root weights w and w', then

(i) if $w < w'$ and $n - 1$ of these trees have root weight w', select a tree (of root weight w') with smallest height; and

(ii) if $w = w'$ (and all n trees have the same smallest root weight), select two trees (of root weight w) of smallest height.

8. (a) To merge lists L_1 and L_2 requires at most $75 + 40 - 1 = 114$ comparisons (from Lemma 12.1), for L_3 and L_4 at most $110 + 50 - 1 = 159$ comparisons. Merging the two resulting lists then requires at most $115 + 160 - 1 = 274$ comparisons for a total of at most $114 + 159 + 274 = 547$ comparisons.

(b) At most 114; at most 224 (338 at most, in total); at most 274 (in total, at most 612).

(c) Merge L_2 and L_4, then merge the resulting list (for L_2, L_4) with L_1, and finally merge the resulting list (for L_1, L_2, L_4) with L_3. This requires at most a total of $89+164+274 = 527$ comparisons.

(d) In order to minimize the number of comparisons in the sorting process construct an optimal tree with the weights w_i, $1 \leq i \leq n$, given by $w_i = |L_i|$.

Section 12.5

1. The articulation points are b, e, f, h, j, k. The biconnected components are
$B_1 : \{\{a, b\}\}$; $B_2 : \{\{d, e\}\}$;
$B_3 : \{\{b, c\}, \{c, f\}, \{f, e\}, \{e, b\}\}$; $B_4 : \{\{f, g\}, \{g, h\}, \{h, f\}\}$;
$B_5 : \{\{h, i\}, \{i, j\}, \{j, h\}\}$; $B_6 : \{\{j, k\}\}$;
$B_7 : \{\{k, p\}, \{p, n\}, \{n, m\}, \{m, k\}, \{p, m\}\}$.

2. If every path from x to y contains the vertex z, then splitting the vertex z will result in at least two components C_x, C_y where $x \in C_x$, $y \in C_y$. If not, there is a path that still connects x and y and this path does not include vertex z. Conversely, if z is an articulation point of G then the splitting of z results in at least two components C_1, C_2 for G. Select $x \in C_1$, $y \in C_2$. Since G is connected there is at least one path from x to y, but since x and y become separated upon the splitting of z, every path connecting x and y in G contains the vertex z.

3. (a) T can have as few as one or as many as $n-2$ articulation points. If T contains a vertex of degree $(n-1)$, then this vertex is the only articulation point. If T is a path with n vertices and $n-1$ edges, then the $n-2$ vertices of degree 2 are all articulation points.
(b) In all cases, a tree on n vertices has $n-1$ biconnected components. Each edge is a biconnected component.

4. (a) From Exercise 2, if v is an articulation point in T then there are vertices x, y where every path from x to y includes vertex v. Hence $\deg(v) > 1$. Conversely, if $\deg(v) > 1$, let $a, b \in V$ such that $\{a, v\}$, $\{v, b\} \in E$. Then in splitting vertex v, the tree is separated into components C_a, C_b containing a, b, respectively. If not, there is another path from a to b that does not include v. This contradicts Theorem 12.1.

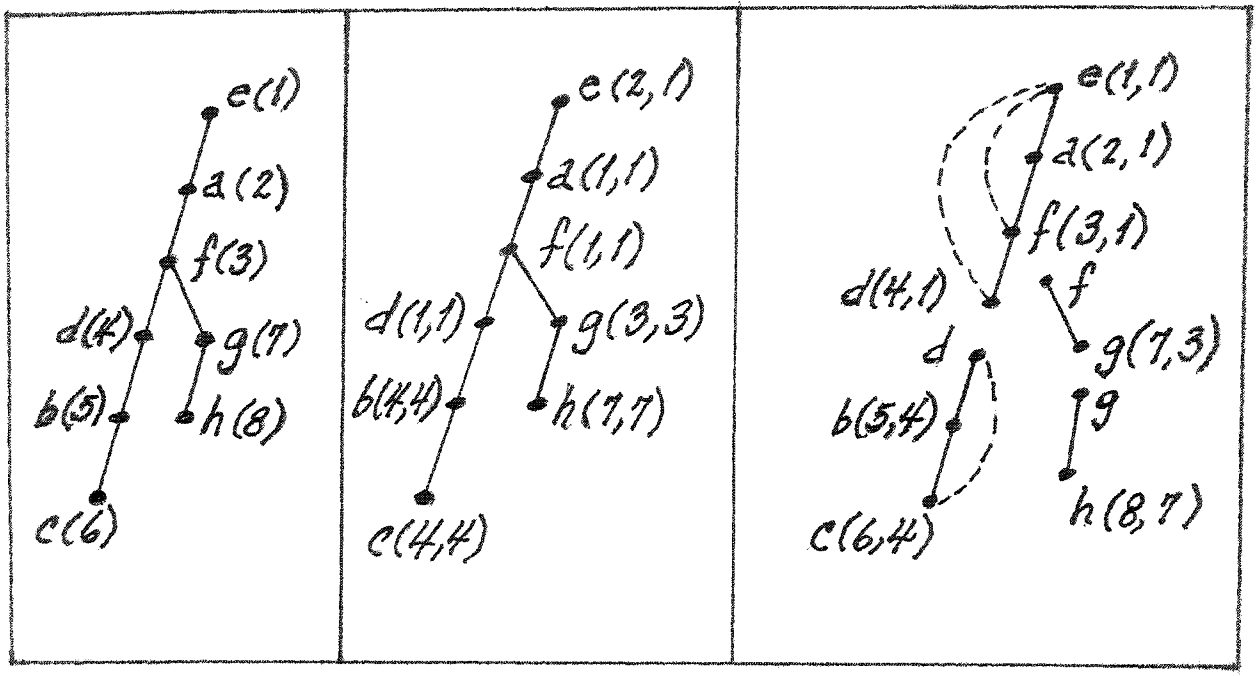
(b) Since G is connected, G has a spanning tree $T = (V, E')$. This tree has at least two pendant vertices. Let v be a pendant vertex in T. If v is an articulation point of G, then there are vertices x, y in G such that every path connecting x and y contains v. But then one of these paths must be in T. So $\deg_T(v) > 1$, contradicting v being a pendant vertex.

5. $\chi(G) = \max\{\chi(B_i) | 1 \leq i \leq k\}$.

6. The graph G has $n_1 \cdot n_2 \cdots n_8$ distinct spanning trees.

7. Proof: Suppose that G has a pendant vertex, say x, and that $\{w, x\}$ is the (unique) edge in E incident with x. Since $|V| \geq 3$ we know that $\deg(w) \geq 2$ and that $\kappa(G - w) \geq 2 > 1 = \kappa(G)$. Consequently, w is an articulation point of G.

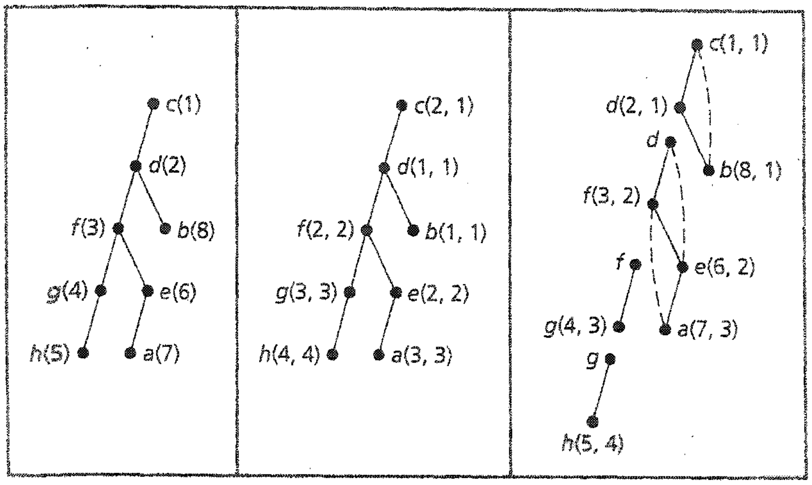
8.



(a) The first tree provides the depth-first spanning tree T for G with e as the root.
(b) The second tree provides $(\text{low}'(v), \text{low}(v))$ for each vertex v of G (and T). These results follow from step (2) of the algorithm.

For the third tree we find $(\text{dfi}(v), \text{low}(v))$ for each vertex v. Applying step (3) of the algorithm we find the articulation points d, f, and g, and the four biconnected components.

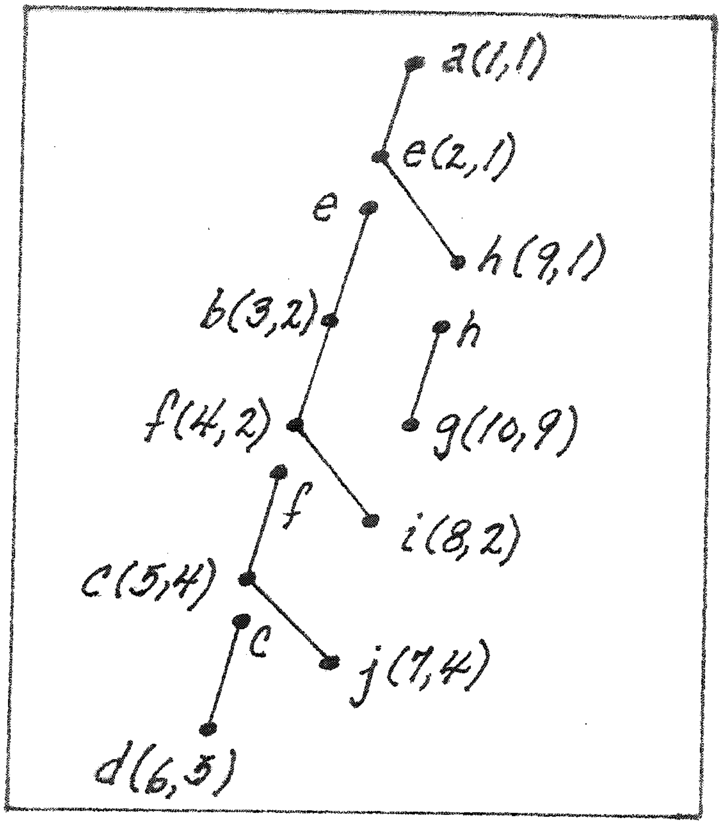
9.



(a) The first tree provides the depth-first spanning tree T for G where the order prescribed for the vertices is reverse alphabetical and the root is c.
(b) The second tree provides $(\text{low}'(v), \text{low}(v))$ for each vertex v of G (and T). These results follow from step (2) of the algorithm.

For the third tree we find $(\text{dfi}(v), \text{low}(v))$ for each vertex v. Applying step (3) of the algorithm we find the articulation points d, f, and g, and the four biconnected components.

10. The ordered pair next to each vertex v in the figure provides $(\text{dfi}(v), \text{low}(v))$. Following step (3) of the algorithm for determining the articulation points of G we see here that this graph has four articulation points – namely, c, e, f, and h. There are five biconnected components – the figure shows the spanning trees for these components.



11. No! For any loop-free connected undirected graph $G = (V, E)$ where $|V| \geq 2$, we have $\text{low}(x_1) = \text{low}(x_2) = 1$. (Note: Vertices x_1 and x_1 are always on the same biconnected component.)

12. (a) The vertex set for each graph is $V - \{v\}$. If $e = \{x, y\}$ is an edge in $\overline{G - v}$ then e is not in $G - v$, and since $x, y \neq v$, e is an edge in $\overline{G} - v$. For the opposite inclusion if $e = \{x, y\}$ is an edge in $\overline{G} - v$, then $x, y \neq v$ and e is not an edge in G, nor the subgraph $G - v$. Here e is an edge in $\overline{G - v}$.

Since $\overline{G - v}$ and $\overline{G} - v$ have the same vertex and edge sets, these graphs are equal.

(b) If v is an articulation point of G, then $\kappa(G - v) > \kappa(G)$, so $G - v$ is not connected. But then $\overline{G - v}$ is connected. So $\kappa(\overline{G} - v) = \kappa(\overline{G - v}) = 1 \leq \kappa(\overline{G})$, and consequently v cannot be an articulation point of $\overline{G}$.

13. Proof: If not, let $v \in V$ where v is an articulation point of G. Then $\kappa(G - v) > \kappa(G) = 1$. (From Exercise 19 of Section 11.6 we know that G is connected.) Now $G - v$ is disconnected with components $H_1, H_2, \ldots, H_t$, for $t \geq 2$. For $1 \leq i \leq t$, let $v_i \in H_i$. Then $H_i + v$ is a subgraph of $G - v_{i+1}$, and $\chi(H_i + v) \leq \chi(G - v_{i+1}) < \chi(G)$. (Here $v_{t+1} = v_1$.) Now let $\chi(G) = n$ and let $\{c_1, c_2, \ldots, c_n\}$ be a set of n colors. For each subgraph $H_i + v$, $1 \leq i \leq t$, we can properly color the vertices of $H_i + v$ with at most $n - 1$ colors — and can use c_1 to color vertex v for all of these t subgraphs. Then we can join these t subgraphs together at vertex v and obtain a proper coloring for the vertices of G where we use less than $n (= \chi(G))$ colors.

14. No! Consider the graph and breadth-first spanning tree shown in the figure. Here $\{c,d\} \in E$ and $\{c,d\} \notin E'$, but c is neither an ancestor nor a descendant of d in the tree T.

Supplementary Exercises

1. If G is a tree, consider G as a rooted tree. Then there are λ choices for coloring the root of G and $(\lambda - 1)$ choices for coloring each of its descendants. The result then follows by the rule of product.

Conversely, if $P(G,\lambda) = \lambda(\lambda-1)^{n-1}$, then since the factor λ only occurs once, the graph G is connected. $P(G,\lambda) = \lambda(\lambda-1)^{n-1} = \lambda^n - (n-1)\lambda^{n-1} + \ldots + (-1)^{n-1}\lambda \Longrightarrow G$ has n vertices and $(n-1)$ edges. Therefore by part (d) of Theorem 12.5, G is a tree.

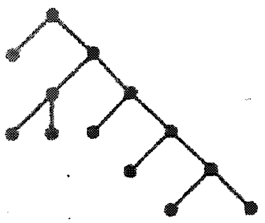
2. Model the problem with a complete quaternary tree rooted at the president.

(a) Since there are 125 executives (vertices) there are 124 edges (phone calls).

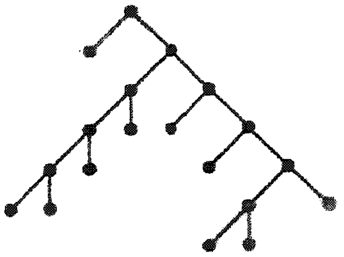
(b) The total number of executives making calls is the number of internal vertices. From Theorem 12.6 (c), $i = (125-1)/4 = 61$. So 60 executives, in addition to the president, make calls.

3. (a) 1011001010100

(b) (i)



(ii)



(c) Since the last two vertices visited in a preorder traversal are leaves, the last two symbols in the characteristic sequence of every complete binary tree are 00.

4. (a) {1,11} {3,23} {4,9} {6,15} {-5,18} {2,7} {-10,35} {-2,5}
{-5,1,11,18} {2,3,7,23} {-10,4,9,35} {-2,5,6,15}
{-10,-5,1,4,9,11,18,35} {-2,2,3,5,6,7,15,23}
{-10,-5,-2,1,2,3,4,5,6,7,9,11,15,18,23,35}

(b) $\sum_{i=1}^{k}(2^i - 1)2^{k-i}$

5. We assume that $G = (V,E)$ is connected – otherwise we work with a component of G. Since G is connected, and $\deg(v) \geq 2$ for all $v \in V$, it follows from Theorem 12.4 that G is not a tree. But every connected graph that is not a tree must contain a cycle.

6. From the first part of the definition of $\mathcal{R}$ the relation is reflexive. To establish the antisym-

metric property let $x\mathcal{R}y$ and $y\mathcal{R}x$ for $x, y \in V$. $x\mathcal{R}y \Longrightarrow x$ is on the path from r to y. If $x \neq y$ then x is encountered before y as we traverse the (unique) path from r to y. Hence by the uniqueness of such a path we cannot have $y\mathcal{R}x$. Hence $(x\mathcal{R}y \wedge y\mathcal{R}x) \Longrightarrow x = y$. Lastly, let $x, y, z \in V$ with $x\mathcal{R}y$ and $y\mathcal{R}z$. Then x is on the unique path from r to y and y is on the unique path from r to z. Since these paths are unique the path from r to z must include x so $x\mathcal{R}z$ and $\mathcal{R}$ is transitive.

7. For $1 \leq i(< n)$, let $x_i =$ the number of vertices v where $\deg(v) = i$. Then $x_1 + x_2 + \ldots + x_{n-1} = |V| = |E| + 1$, so $2|E| = 2(-1 + x_1 + x_2 + \ldots + x_{n-1})$. But $2|E| = \sum_{v\in V} \deg(v) = (x_1 + 2x_2 + 3x_3 + \ldots + (n-1)x_{n-1})$. Solving $2(-1 + x_1 + x_2 + \ldots + x_{n-1}) = x_1 + 2x_2 + \ldots + (n-1)x_{n-1}$ for x_1, we find that $x_1 = 2 + x_3 + 2x_4 + 3x_5 + \ldots + (n-3)x_{n-1} = 2 + \sum_{\deg(v_i)\geq 3}[\deg(v_i) - 2]$.

8. (a) For all $e \in E$, $e = e$, so $e\mathcal{R}e$ and $\mathcal{R}$ is reflexive.
If $e_1, e_2 \in E$ with $e_1 \neq e_2$ and $e_1\mathcal{R}e_2$, then e_1 and e_2 are edges of a cycle C of G. Hence e_2 and e_1 are edges of the cycle C, so $e_2\mathcal{R}e_1$ and $\mathcal{R}$ is symmetric.

Let e_1, e_2, e_3 be three distinct edges with $e_1\mathcal{R}e_2$ and $e_2\mathcal{R}e_3$. Let C_1 be a cycle of G containing e_1, e_2 and let C_2 be a cycle of G containing e_2, e_3. If $C_1 \neq C_2$, let C be the cycle of G made up from the edges of C_1, C_2, where common edges are removed. (In terms of edges, $C = C_1 \Delta C_2$.) Since e_1, e_3 are on C we have $e_1\mathcal{R}e_3$, and $\mathcal{R}$ is transitive.

(b) The partition of E induced by $\mathcal{R}$ provides the biconnected components of G.

9. (a) G^2 is isomorphic to K_5.
(b) G^2 is isomorphic to K_4.
(c) G^2 is isomorphic to K_{n+1}, so the number of new edges is $\binom{n+1}{2} - n = \binom{n}{2}$.

(d) If G^2 has an articulation point x, then there exists $u, v \in V$ such that every path (in G^2) from u to v passes through x. (This follows from Exercise 2 of Section 12.5.) Since G is connected, there exists a path P (in G) from u to v. If x is not on this path (which is also a path in G^2), then we contradict x being an articulation point in G^2. Hence the path P (in G) passes through x, and we can write $P: u \rightarrow u_1 \rightarrow \ldots \rightarrow u_{n-1} \rightarrow u_n \rightarrow x \rightarrow v_m \rightarrow v_{m-1} \rightarrow \ldots \rightarrow v_1 \rightarrow v$. But then in G^2 we add the edge $\{u_n, v_m\}$, and the path P' (in G^2) given by $P': u \rightarrow u_1 \rightarrow \ldots \rightarrow u_{n-1} \rightarrow u_n \rightarrow v_m \rightarrow v_{m-1} \rightarrow \ldots \rightarrow v_1 \rightarrow v$ does not pass through x. So x is not an articulation point of G^2, and G^2 has no articulation points.

10. (a) For the minimum value of $|V|$ we have six leaves at level 8 and the other $6^7 - 1$ leaves are at level 7. Since there are $6^7 + 5$ leaves, it follows from part (c) of Theorem 12.6 that $|V| = (6/5)[(6^7 + 5) - 1] + 1 = 335,929$.
For the maximum value of $|V|$ we have one leaf at level 7 and the other $(6^7 - 1)(6)$ leaves are at level 8. So there are $(6^8 - 6) + 1 = 6^8 - 5$ leaves in total. Once again we use part (c) of Theorem 12.6 to find that $|V| = (6/5)[(6^8 - 5) - 1] + 1 = 2,015,533$.
(b) Let ℓ denote the number of leaves in T. For the minimum case $\ell = (m^{h-1} - 1) + m =$

$m^{h-1} + (m-1)$ and $|V| = [m/(m-1)][m^{h-1} + (m-1) - 1] + 1$. For the maximum case we have $\ell = m(m^{h-1} - 1) + 1 = m^h - m + 1$ and $|V| = [m/(m-1)][m^h - m] + 1$.

11. (a) $\ell_n = \ell_{n-1} + \ell_{n-2}$, for $n \geq 3$ and $\ell_1 = \ell_2 = 1$. Since this is precisely the Fibonacci recurrence relation, we have $l_n = F_n$, the nth Fibonacci number, for $n \geq 1$.
(b) $i_n = i_{n-1} + i_{n-2} + 1$, $n \geq 3$, $i_1 = i_2 = 0$. The summand "+1" arises when we count the root, an internal vertex.
(Homogeneous part of solution):

$$i_n^{(h)} = i_{n-1}^{(h)} + i_{n-2}^{(h)},\ n \geq 3$$

$$i_n^{(h)} = A\alpha^n + B\beta^n, \text{ where } \alpha = (1+\sqrt{5})/2 \text{ and } \beta = (1-\sqrt{5})/2.$$

(Particular part of solution):

$$i_n^{(p)} = C, \text{ a constant}$$

Upon substitution into the recurrence relation $i_n = i_{n-1} + i_{n-2} + 1$, $n \geq 3$, we find that

$$C = C + C + 1,$$

so $C = -1$,
and $i_n = A\alpha^n + B\beta^n - 1$.
With $i_1 = i_2 = 0$ we have

$$0 = i_1 = A\alpha + B\beta - 1$$

$$0 = i_2 = A\alpha^2 + B\beta^2 - 1,$$

and consequently,
$B = (\alpha - 1)/[\beta(\alpha - \beta)] = [((1+\sqrt{5})/2) - 1]/[((1-\sqrt{5})/2)(\sqrt{5})] =$ $[1 + \sqrt{5} - 2]/[(1-\sqrt{5})(\sqrt{5})] = -1/\sqrt{5}$, and $A = [1 - B\beta]/\alpha = 1/\sqrt{5}$. Therefore,

$$i_n = (1/\sqrt{5})\alpha^n - (1/\sqrt{5})\beta^n - 1 = F_n - 1,$$

where F_n denotes the nth Fibonacci number, for $n \geq 1$.
(c) $v_n = \ell_n + i_n$, for all $n \in \mathbf{Z}^+$. Consequently, $v_n = F_n + F_n - 1 = 2F_n - 1$, where, as in parts (a) and (b), F_n denotes the nth Fibonacci number.

12. (a) For the graph G_3 in Fig. 12.48 (d) there are 12 nonidentical spanning trees in total.
(b) Consider the graph G_{n+1}. Here the nonidentical spanning trees arise from the following three cases any two of which are mutually exclusive.

(1) The edge $\{a, n+1\}$ is used: Here we can then use any of the t_n nonidentical spanning trees for G_n, and the result is a spanning tree for G_{n+1}.

(2) The edge $\{n+1, b\}$ is used: Here we have a situation similar to that in (1) and we get t_n additional nonidentical spanning trees for G_{n+1}.

(3) The edges $\{a, n+1\}$, $\{n+1, b\}$ are both used: Now for each vertex i, where $1 \leq i \leq n$, we have two choices — include the edge $\{a, i\}$ or the edge $\{i, b\}$ (but *not* both). In this way we obtain the final 2^n nonidentical spanning trees for G_{n+1}.

The results in (1), (2), and (3) lead us to the following recurrence relation:

$$(*) \qquad t_{n+1} = 2t_n + 2^n, \qquad t_1 = 1, \qquad n \geq 1.$$

(Homogeneous Solution): $t_{n+1} = 2t_n$

$$t_n^{(h)} = A(2^n),\ A \text{ a constant.}$$

(Particular Solution): $t_n^{(p)} = Bn(2^n)$, B a constant.

Substituting $t_n^{(p)}$ into equation $(*)$ we find that

$$B(n+1)(2^{n+1}) = 2Bn(2^n) + 2^n$$

$$Bn(2^{n+1}) + B(2^{n+1}) = Bn(2^{n+1}) + 2^n$$

Consequently, $2B(2^n) = 2^n$ and $2B = 1$, or $B = 1/2$. Therefore, $t_n = A(2^n) + (1/2)n(2^n) = A(2^n) + n2^{n-1}$.

Since $t_1 = 1 = A(2) + 1$, $A = 0$ and $t_n = n2^{n-1}$, $n \geq 1$.

13. (a) For the spanning trees of G there are two mutually exclusive and exhaustive cases:

(i) The edge $\{x_1, y_1\}$ is in the spanning tree: These spanning trees are counted in b_n.

(ii) The edge $\{x_1, y_1\}$ is not in the spanning tree: In this case the edges $\{x_1, x_2\}$, $\{y_1, y_2\}$ are both in the spanning tree. Upon removing the edges $\{x_1, x_2\}, \{y_1, y_2\}$, and $\{x_1, y_1\}$, from the original ladder graph, we now need a spanning tree for the resulting smaller ladder graph with $n-1$ rungs. There are a_{n-1} spanning trees in this case.

(b) Here there are three mutually exclusive and exhaustive cases:

(i) The edges $\{x_1, x_2\}$ and $\{y_1, y_2\}$ are both in the spanning tree: Delete $\{x_1, x_2\}$, $\{y_1, y_2\}$, and $\{x_1, y_1\}$ from the graph. Then b_{n-1} counts those spanning trees for ladders with $n-1$ rungs where $\{x_2, y_2\}$ is included. For each of these delete $\{x_2, y_2\}$ and add $\{x_1, x_2\}$, $\{y_1, y_2\}$ and $\{x_1, y_1\}$.

(ii) The edge $\{x_1, x_2\}$ is in the spanning tree but the edge $\{y_1, y_2\}$ is not: Now the removal of the edges $\{x_1, y_1\}, \{x_1, x_2\}$, and $\{y_1, y_2\}$ from G results in a subgraph that is a ladder graph on $n-1$ rungs. This subgraph has a_{n-1} spanning trees.

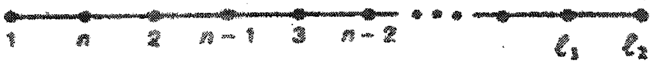
(iii) Here the edge $\{y_1, y_2\}$ is in the spanning tree but the edge $\{x_1, x_2\}$ is not: As in case (ii) there are a_{n-1} spanning trees.

On the basis of the preceding argument we have $b_n = b_{n-1} + 2a_{n-1}$, $n \geq 2$.

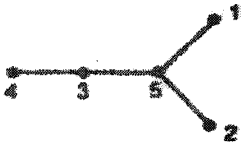
(c) $a_n = a_{n-1} + b_n$
$b_n = b_{n-1} + 2a_{n-1}$
$a_n = a_{n-1} + b_{n-1} + 2a_{n-1} = 3a_{n-1} + b_{n-1}$
$b_n = a_n - a_{n-1}$, so $b_{n-1} = a_{n-1} - a_{n-2}$
$a_n = 3a_{n-1} + a_{n-1} - a_{n-2} = 4a_{n-1} - a_{n-2}$, $n \geq 3$, $a_1 = 1$, $a_2 = 4$
$a_n - 4a_{n-1} + a_{n-2} = 0$
$r^2 - 4r + 1 = 0$
$r = (1/2)(4 \pm \sqrt{16-4}) = 2 \pm \sqrt{3}$
So $a_n = A(2+\sqrt{3})^n + B(2-\sqrt{3})^n$
$a_0 = 0 \Longrightarrow A + B = 0 \Longrightarrow B = -A.$

$a_1 = 1 = A(2+\sqrt{3}) - A(2-\sqrt{3}) = 2A\sqrt{3} \Longrightarrow A = 1/2\sqrt{3}$ and $B = -1/2\sqrt{3}$.
Therefore $a_n = (1/(2\sqrt{3}))[(2+\sqrt{3})^n - (2-\sqrt{3})^n], n \geq 0$.

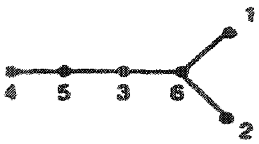
14. (a)

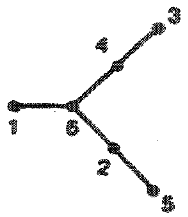


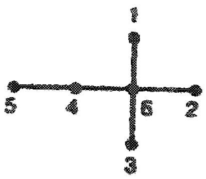
For n even, $\ell_1 = n/2$ and $\ell_2 = \ell_1 + 1$
For n odd, $\ell_1 = \ell_2 + 1$ and $\ell_2 = \lceil n/2 \rceil$
(b) Label the vertex of degree 1 with the label 1. Label the other n vertices (one vertex per label) with the labels $2, 3, \ldots, n, n+1$.
(c) For $|V| = 4$ the only trees are a path of length 3 and $K_{1,3}$. These are handled by parts (a) and (b), respectively.
For $|V| = 5$ there are three trees: (1) A path of length 4; (2) $K_{1,4}$; and (3) The tree with a vertex of degree 3. Trees (1) and (2) are handled by parts (a) and (b), respectively. The third tree may be labeled as follows.

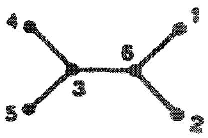


For $|V| = 6$, there are six trees. The path of length 5 and $K_{1,5}$ are dealt with by parts (a) and (b), respectively. The other four trees may be labeled as follows.





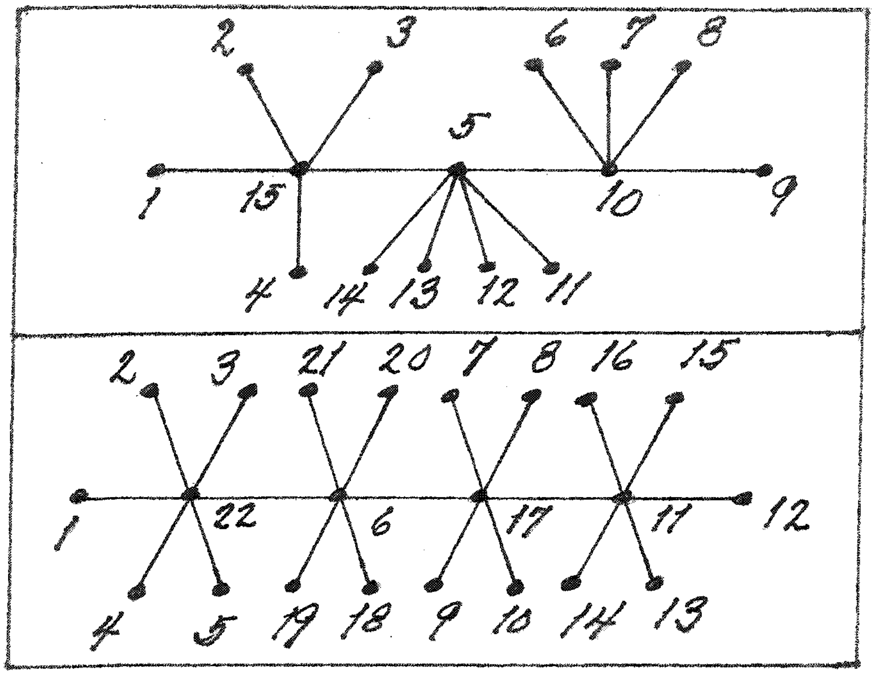




15. (a) (i) 3 (ii) 5

(b) $a_n = a_{n-1} + a_{n-2}$, $n \geq 5$, $a_3 = 2$, $a_4 = 3$.
$a_n = F_{n+1}$, the $(n+1)$st Fibonacci number.

16.

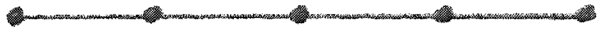


17. Here the input consists of
(a) the k (≥ 3) vertices of the spine – ordered from left to right as $v_1, v_2, \ldots, v_k$;
(b) $\deg(v_i)$, in the caterpillar, for all $1 \leq i \leq k$; and
(c) n, the number of vertices in the caterpillar, with $n \geq 3$.

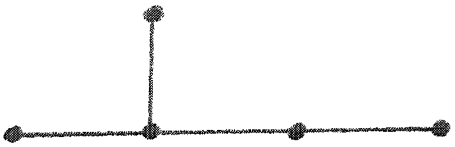
If $k = 3$, the caterpillar is the complete bipartite graph (or, star) $K_{1,n-1}$, for some $n \geq 3$. We label v_1 with 1 and the remaining vertices with $2, 3, \ldots, n$. This provides the edge labels (the absolute value of the difference of the vertex labels) $1, 2, 3, \ldots, n-1$ – a graceful labeling.

```
For $k > 3$ we consider the following.
$\ell := 2$          {$\ell$ is the largest low label}
$h := n - 1$    {$h$ is the smallest high label}
label $v_1$ with 1
label $v_2$ with $n$
for $i := 2$ to $k - 1$ do
    if $2\lfloor i/2 \rfloor = i$ then                {$i$ is even}
        begin
            if  $v_i$ has unlabeled leaves that are not on the spine then
                assign the $\deg(v_i) - 2$ labels from $\ell$
                to $\ell + \deg(v_i) - 3$ to these leaves of $v_i$
            assign the label $\ell + \deg(v_i) - 2$ to $v_{i+1}$
            $\ell := \ell + \deg(v_i) - 1$
        end
    else
        begin
            if  $v_i$ has unlabeled leaves that are not on the spine then
                assign the $\deg(v_i) - 2$ labels from $h - [\deg(v_i) - 3]$
                to $h$ to these leaves of $v_i$
            assign the label $h - \deg(v_i) + 2$ to $v_{i+1}$
            $h := h - \deg(v_i) + 1$
        end
```

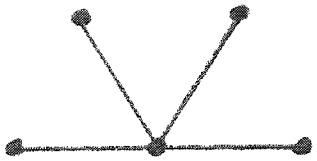
18. (a) Fig. 12.50 10001000010001
Fig. 12.51 100001000010000100001
(b) Yes, when the caterpillar is a path.
(c) Yes, when the caterpillar is the complete bipartite graph (or, star) $K_{1,n-1}$, where $n \geq 3$.
(d)



1111



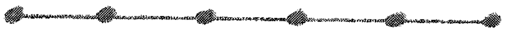
1011



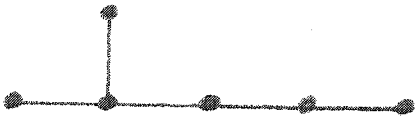
1001

There are three nonisomorphic caterpillars on five vertices. Two of the corresponding binary strings are palindromes.

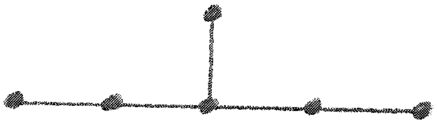
(e)



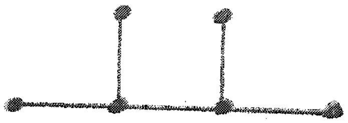
11111



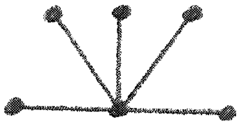
10111



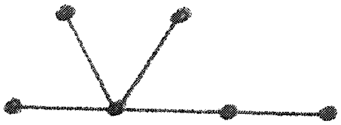
11011



10101



10001



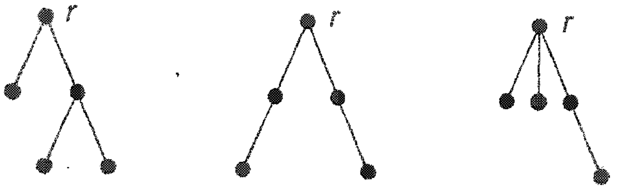
10011

There are six nonisomorphic caterpillars on six vertices. Four of the corresponding binary strings are palindromes.

(f) Since the caterpillar has n vertices it has $n-1$ edges, and its binary string has $n-1$ bits, where the first and last bits are 1s. For each of the remaining $n-3$ bits there are two choices – 0 or 1. This gives us 2^{n-3} binary strings. However, for each binary string s that is not a palindrome, the reversal of that string – namely, s^R – corresponds with a caterpillar that is isomorphic to the caterpillar determined by s. So each pair of these strings – s and s^R – determines only one (nonisomorphic) caterpillar. Further, each palindrome also determines a unique caterpillar. For the palindromes we have two choices for each of the first $\lceil (n-3)/2 \rceil$ positions (after the first 1). So there are $2^{\lceil (n-3)/2 \rceil}$ binary strings that are palindromes. Consequently, $2^{n-3} + 2^{\lceil (n-3)/2 \rceil}$ counts each of the nonisomorphic caterpillars on n vertices twice. Therefore, the number of nonisomorphic caterpillars on n vertices, for $n \geq 3$, is $(1/2)(2^{n-3} + 2^{\lceil (n-3)/2 \rceil})$.

19. (a) $1, -1, 1, 1, -1, -1$ $\quad$ $1, 1, -1, 1, -1, -1$ $\quad$ $1, -1, 1, -1, 1, -1$

(b)



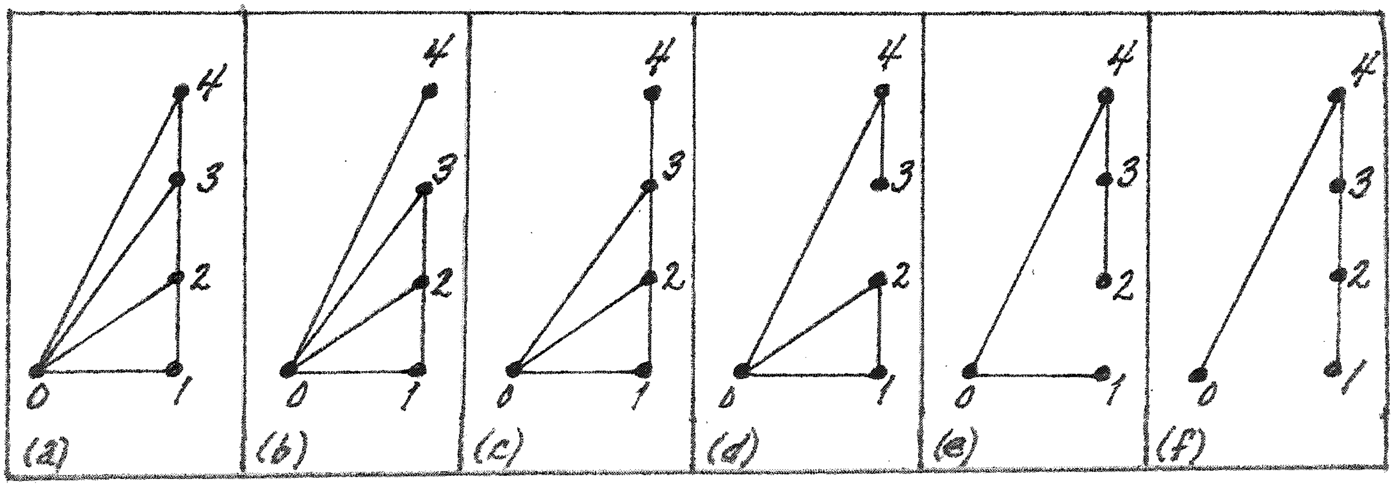
In total there are 14 ordered rooted trees on five vertices.

(c) This is another example where the Catalan numbers arise. There are $(\frac{1}{n+1})\binom{2n}{n}$ ordered rooted trees on $n+1$ vertices.

20. (a) Consider the case for $n = 4$, shown in part (a) of the figure. The five spanning subgraphs in parts (b)–(f) of the figure provide pairwise mutually exclusive situations that account for all the spanning trees of the graph given in part (a). As we scan the figure from left to right we find that

$$t_4 = t_3 + t_3 + t_2 + t_1 + t_0 = t_3 + \sum_{i=0}^{3} t_i.$$

This result generalizes to provide $t_{n+1} = t_n + \sum_{i=0}^{n} t_i$.



(b)

$$\begin{aligned} t_{n+1} &= t_n + \textstyle\sum_{i=0}^{n} t_i \\ &= 2t_n + \textstyle\sum_{i=0}^{n-1} t_i \\ &= 2t_n + [t_{n-1} + \textstyle\sum_{i=0}^{n-1} t_i] - t_{n-1} \\ &= 3t_n - t_{n-1}, n \geq 2 \end{aligned}$$

(c) $t_{n+1} = 3t_n - t_{n-1}, n \geq 2, t_2 = 3, t_1 = 1.$
Let $t_n = Ar^n$, $A \neq 0, r \neq 0.$
$r^2 - 3r + 1 = 0$
$r = (3 \pm \sqrt{5})/2$
So $t_n = B[(3+\sqrt{5})/2]^n + C[(3-\sqrt{5})/2]^n$.
Since $1 = t_1 = B[(3+\sqrt{5})/2] + C[(3-\sqrt{5})/2]$ and
$3 = t_2 = B[(3+\sqrt{5})/2)]^2 + C[(3-\sqrt{5})/2]^2$,
we find that
$B = 1/\sqrt{5}, C = -1/\sqrt{5}.$
Consequently, $t_n = (1/\sqrt{5})[(3+\sqrt{5})/2]^n - (1/\sqrt{5})[(3-\sqrt{5})/2]^n$, $n \geq 1$, $t_0 = 1$.

Recall that the nth Fibonacci number F_n is given by

$$F_n = (1/\sqrt{5})[(1+\sqrt{5})/2]^n - (1/\sqrt{5})[(1-\sqrt{5})/2]^n, n \geq 0.$$

For $n \geq 1$, $F_{2n} = (1/\sqrt{5})[(1+\sqrt{5})/2]^{2n} - (1/\sqrt{5})[(1-\sqrt{5})/2]^{2n} = (1/\sqrt{5})[(1+\sqrt{5})^2/4]^n - (1/\sqrt{5})[(1-\sqrt{5})^2/4]^n = (1/\sqrt{5})[(3+\sqrt{5})/2]^n - (1/\sqrt{5})[(3-\sqrt{5})/2]^n = t_n$.

21. (a) There are $\binom{5}{3} - 2 = 8$ nonidentical (though some are isomorphic) spanning trees for the kite induced by a, b, c, d. Since there are four vertices, a spanning tree has three edges and the only selections of three edges that do not provide a spanning tree are $\{a,c\}, \{b,c\}, \{a,b\}$ and $\{a,b\}, \{a,d\}, \{b,d\}$.

(b) There are $8 \cdot 1 \cdot 8 \cdot 1 \cdot 8 \cdot 1 \cdot 8 = 8^4$ nonidentical (though some are isomorphic) spanning trees of G that do not contain edge $\{c,h\}$. These spanning trees must include the edges $\{g,k\}$, $\{l,p\}$, and $\{d,o\}$, and there are eight nonidentical (though some are isomorphic) spanning trees for each of the four subgraphs that are kites.

(c) Consider the kite induced by a, b, c, d. There are eight two-tree forests for this kite that have no path between c and d. These forests can be obtained from the five edges of the kite by removing three edges at a time, as follows:

(i) $\{a,b\}, \{a,c\}, \{b,c\}$
(ii) $\{a,c\}, \{b,c\}, \{b,d\}$
(iii) $\{a,c\}, \{a,d\}, \{b,c\}$
(iv) $\{a,b\}, \{a,d\}, \{b,d\}$
(v) $\{a,d\}, \{b,c\}, \{b,d\}$
(vi) $\{a,c\}, \{a,d\}, \{b,d\}$
(vii) $\{a,b\}, \{a,d\}, \{b,c\}$
(viii) $\{a,b\}, \{a,c\}, \{b,d\}$

Vertex c is isolated for (i), (ii), (iii). For (iv), (v), (vi), vertex d is isolated. The forests for (vii), (viii) each contain two disconnected edges: $\{a,c\}, \{b,d\}$ for (vii) and $\{a,d\}, \{b,c\}$ for (viii).

Consequently, there are $4 \cdot 8 \cdot 1 \cdot 8 \cdot 1 \cdot 8 \cdot 1 \cdot 8 \cdot 1 = 4 \cdot 8^4$ nonidentical (though some are isomorphic) spanning trees for G that contain each of the four edges $\{c,h\}, \{g,k\}, \{l,p\}$, and $\{d,o\}$.

(d) In total there are $4 \cdot 8^4 + 4 \cdot 8^4 = 2(4 \cdot 8^4)$ nonidentical (though some are isomorphic) spanning trees for G.

(e) $2n8^n$

CHAPTER 13
OPTIMIZATION AND MATCHING

Section 13.1

1. (a) If not, let $v_i \in \overline{S}$, where $1 \leq i \leq m$ and i is the smallest such subscript. Then $d(v_0, v_i) < d(v_0, v_{m+1})$, and we contradict the choice of v_{m+1} as a vertex v in $\overline{S}$ for which $d(v_0, v)$ is a minimum.
(b) Suppose there is a shorter directed path (in G) from v_0 to v_k. If this path passes through a vertex in $\overline{S}$, then from part (a) we have a contradiction. Otherwise, we have a shorter directed path P'' from v_0 to v_k and P'' only passes through vertices in S. But then $P'' \cup \{(v_k, v_{k+1}), (v_{k+1}, v_{k+2}), \ldots, (v_{m-1}, v_m), (v_m, v_{m+1})\}$ is a directed path (in G) from v_0 to v_{m+1}, and it is shorter than path P.

2.

(a) Initialization: (Counter $= 0$) $a = v_0$, $S_0 = \{a\}$. Label a with $(0, -)$ and the other six vertices with $(\infty, -)$.

First Iteration: $\overline{S}_0 = \{b, c, f, g, h, i\}$
$L(b) = 14$, $L(g) = 10$, $L(h) = 17$.
So we have the labels: $g : (10, a)$; $b : (14, a)$; $h : (17, a)$.
$L(v) = \infty$ for $v = c, f$, and i. Hence $v_1 = g$, $S_1 = \{a, g\}$ and the counter is increased to 1.

Second Iteration: $\overline{S}_1 = \{b, c, f, h, i\}$
$L(b) = 13 = L(g) + wt(g, b) < 14$, so b is now labeled $(13, g)$.
$L(h) = 16 = L(g) + wt(g, h) < 17$, so h is now labeled $(16, g)$.
$L(i) = 14 = L(g) + wt(g, i) < \infty$, so i now has the label $(14, g)$.
The vertices c, f are still labeled by $(\infty, -)$. Now we find $v_2 = b$ and we set $S_2 = \{a, g, b\}$ and increase the counter to 2.

Third Iteration: $\overline{S}_2 = \{c, f, h, i\}$
$L(c) = 22 = L(b) + wt(b, c)$ and c is labeled $(22, b)$.
$L(f) = 23 = L(b) + wt(b, f)$ and f is labeled $(23, b)$.
$L(h) = 16$ and h is labeled $(16, g)$.
$L(i) = 14$ and i is labeled $(14, g)$.
Now we have $v_3 = i$ with $S_3 = \{a, g, b, i\}$ and the counter is increased to 3.

Fourth Iteration: $\overline{S}_3 = \{c, f, h\}$
$L(c) = 22$ and c is labeled $(22, b)$.
$L(h) = 15 = L(i) + wt(i, h) < 16$ and h is labeled $(15, i)$.
$L(f) = 21 = L(i) + wt(i, f) < 23$ and f is labeled $(21, i)$.
Here we have $v_4 = h$, $S_4 = \{a, g, b, i, h\}$ and counter is now assigned the value 4.

Fifth Iteration: $\overline{S}_4 = \{c, f\}$
$L(c) = 22$ and c is labeled $(22, b)$.
$L(f) = 21$ and f is labeled $(21, i)$.
Now $v_5 = f$, $S_5 = \{a, g, b, i, h, f\}$ and the counter is increased to 5.

Sixth Iteration: $\overline{S}_5 = \{c\}$
$L(c) = 22$ and c is labeled $(22, b)$.
Here $v_6 = c$, $S_6 = \{a, g, b, i, h, f, c\}$, and now counter $= 6 = 7 - 1 = |V| - 1$, so the algorithm terminates.

(b) $c:$ $\{a, g\}, \{g, b\}, \{b, c\}$ $f:$ $\{a, g\}, \{g, i\}, \{i, f\}$ $i:$ $\{a, g\}, \{g, i\}$

3. (a) $d(a, b) = 5$; $d(a, c) = 6$; $d(a, f) = 12$; $d(a, g) = 16$; $d(a, h) = 12$
(b) $f:$ $\{(a, c), (c, f)\}$ $g:$ $\{(a, b), (b, h), (h, g)\}$
$h:$ $\{(a, b), (b, h)\}$

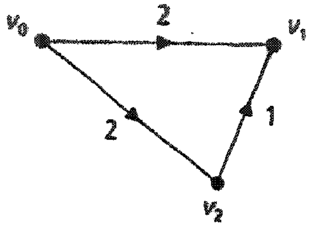
4. (a) Order the vertices of G as $[a, b, c, f, g, h]$.
For L_0 we get the following array of labels: $[\infty, \infty, 0, \infty, \infty, \infty]$, and $S_0 = \{c\}$.
In a similar manner we obtain the arrays:

$L_1: [\infty, \infty, 0, 6, \infty, 11]$; $S_1 = \{c, f\}$
$L_2: [11, \infty, 0, 6, 15, 10]$; $S_2 = \{c, f, h\}$
$L_3: [17, \infty, 0, 6, 14, 10]$; $S_3 = \{c, f, h, g\}$
$L_4: [17, \infty, 0, 6, 14, 10]$; $S_4 = \{c, f, h, g, a\}$
$L_5: [17, 22, 0, 6, 14, 10]$; $S_5 = \{c, f, h, g, a, b\}$

(b) Order the vertices of G as $[a, b, c, f, g, h, i]$.
We obtain the following arrays for the six iterations:

$L_0: [0, \infty, \infty, \infty, \infty, \infty, \infty]$; $S_0 = \{a\}$
$L_1: [0, 14, \infty, \infty, 10, 17, \infty]$; $S_1 = \{a, g\}$
$L_2: [0, 13, \infty, \infty, 10, 16, 14]$; $S_2 = \{a, g, b\}$
$L_3: [0, 13, 22, 23, 10, 16, 14]$; $S_3 = \{a, g, b, i\}$
$L_4: [0, 13, 22, 21, 10, 15, 14]$; $S_4 = \{a, g, b, i, h\}$
$L_5: [0, 13, 22, 21, 10, 15, 14]$; $S_5 = \{a, g, b, i, h, f\}$
$L_6: [0, 13, 22, 21, 10, 15, 14]$; $S_6 = \{a, g, b, i, h, f, c\}$

5. False – consider the weighted graph

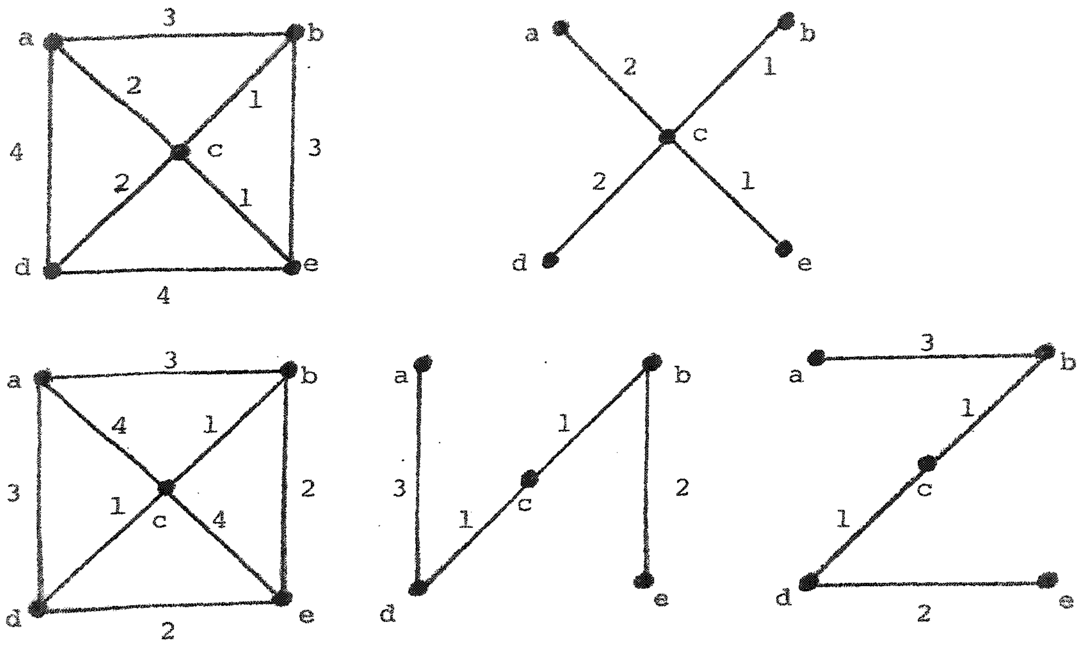


Section 13.2

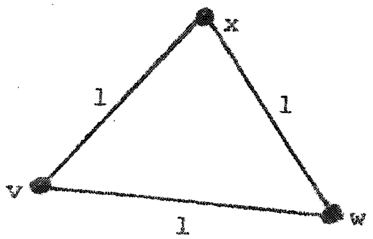
1. Kruskal's Algorithm generates the following sequence (of forests) which terminates in a minimal spanning tree T of weight 18:

(1) $F_1 = \{\{e, h\}\}$, (2) $F_2 = F_1 \cup \{\{a, b\}\}$,
(3) $F_3 = F_2 \cup \{\{b, c\}\}$, (4) $F_4 = F_3 \cup \{\{d, e\}\}$,
(5) $F_5 = F_4 \cup \{\{e, f\}\}$, (6) $F_6 = F_5 \cup \{\{a, e\}\}$,
(7) $F_7 = F_6 \cup \{\{d, g\}\}$, (8) $F_8 = T = F_7 \cup \{\{f, i\}\}$.

Note: The answer given here is not unique.

2. 

3. No! Consider the following counterexample:



Here $V = \{v, x, w\}$, $E = \{\{v, x\}, \{x, w\}, \{v, w\}\}$ and $E' = \{\{v, x\}, \{x, w\}\}$.

4. Gary – South Bend (58); South Bend – Fort Wayne (79); Fort Wayne – Indianapolis (121); Indianapolis – Bloomington (151); Bloomington – Terre Haute (58); Terre Haute – Evansville (113).

5. (a) Evansville – Indianapolis (168); Bloomington – Indianapolis (51); South Bend – Gary (58); Terre Haute – Bloomington (58); South Bend – Fort Wayne (79); Indianapolis – Forth Wayne (121).

(b) Fort Wayne – Gary (132); Evansville – Indianapolis (168); Bloomington – Indianapolis (51); Gary – South Bend (58); Terre Haute – Bloomington (58); Indianapolis – Fort Wayne (121).

6. Start with the prescribed edge(s), unless one or more cycles result. (If so, delete the edge of maximum weight in each such cycle.) Then apply Kruskal's Algorithm starting at Step (2).

7. (a) To determine an optimal tree of maximal weight replace the two occurrences of "small" in Kruskal's Algorithm by "large".

(b) Use the edges: South Bend – Evansville (303); Fort Wayne – Evansville (290); Gary –

Evansville (277); Fort Wayne – Terre Haute (201); Gary – Bloomington (198); Indianapolis – Evansville (168).

8. The proof for Prim's Algorithm is similar to that of Kruskal's Algorithm.
Proof: Let $|V| = n$, and let T be a spanning tree for G obtained by Prim's Algorithm. The edges in T are labeled as $e_1, e_2, \ldots, e_{n-1}$, where the subtree S_i of T, obtained after the ith iteration of the algorithm, contains the edges $e_1, e_2, \ldots, e_i$, for some $1 \leq i \leq n-1$. For each optimal tree T' of G define $d(T')$, as in the proof of Theorem 13.1. Let T_1 be an optimal tree for G where $d(T_1) = r$ is maximal. We shall prove that $T = T_1$.
If not, then $r < n-1$, and there exists an edge $e_r = \{x, y\}$ with $e_r \in T, e_r \notin T_1$. Since T_1 is a spanning tree for G, however, there is a unique path P connecting x and y in T_1. Assume that $x \in S_{r-1}$, $y \notin S_{r-1}$. Select an edge e'_r in P which joins a vertex in S_{r-1} with a vertex that is not in S_{r-1}. By the minimality condition in Step 2 of Prim's Algorithm $wt(e'_r) \geq wt(e_r)$. Adding the edge e_r to T_1, e_r together with the edges in P form a cycle. Deleting edge e'_r, the cycle becomes a path and a new subgraph of G is obtained. Since this subgraph is connected with n vertices and $n-1$ edges, it is a tree T_2, where $wt(T_2) = wt(T_1) + wt(e_r) - wt(e'_r)$. With $wt(e'_r) \geq wt(e_r)$, we find that $wt(T_2) \leq wt(T_1)$, and since T_1 is optimal it follows that $wt(T_2) = wt(T_1)$. But then T_2 is an optimal tree for the graph G with $d(T_2) > r$, and this contradicts the choice of T_1 (where $d(T_1)$ is maximal).

9. When the weights of the edges are all distinct, in each step of Kruskal's Algorithm a unique edge is selected.

Section 13.3

1. (a) $s = 2$; $t = 4$; $w = 5$; $x = 9$; $y = 4$ (b) 18

(c) (i) $P = \{a, b, h, d, g, i\}$; $\overline{P} = \{z\}$
(ii) $P = \{a, b, h, d, g\}$; $\overline{P} = \{i, z\}$
(iii) $P = \{a, h\}$; $\overline{P} = \{b, d, g, i, z\}$

2. Corollary 13.3: This result is a special case of Theorem 13.3.
Corollary 13:4: This result follows from the observation following the proof of Theorem 13.3, namely,

$$val(f) = \sum_{\substack{x \in P \\ y \in \overline{P}}} f(x, y) - \sum_{\substack{w \in P \\ v \in \overline{P}}} f(v, w).$$

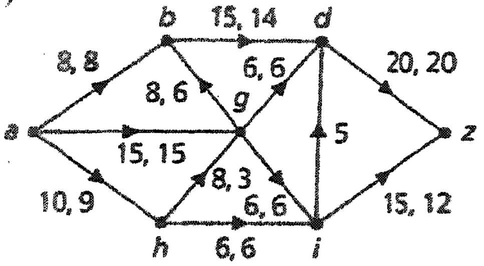
If $val(f) = c(P, \overline{P}) = \sum_{\substack{x \in P \\ y \in \overline{P}}} c(x, y)$, since $0 \leq f(x, y) \leq c(x, y)$, for

$x \in P$, $y \in \overline{P}$, it follows that $f(e) = c(e)$ for each $e = (x, y)$, $x \in P$, $y \in \overline{P}$, and

$f(e) = 0$ for each $e = (v, w)$, $v \in \overline{P}$, $w \in P$. Conversely if conditions (a) and (b) hold, then

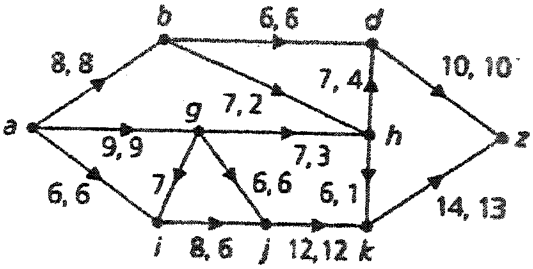
$$val(f) = \sum_{\substack{x\in P\\ y\in \overline{P}}} f(x,y) - \sum_{\substack{w\in P\\ v\in \overline{P}}} f(v,w) = \sum_{\substack{x\in P\\ y\in \overline{P}}} c(x,y) - 0 = c(P, \overline{P}).$$

3. (1)



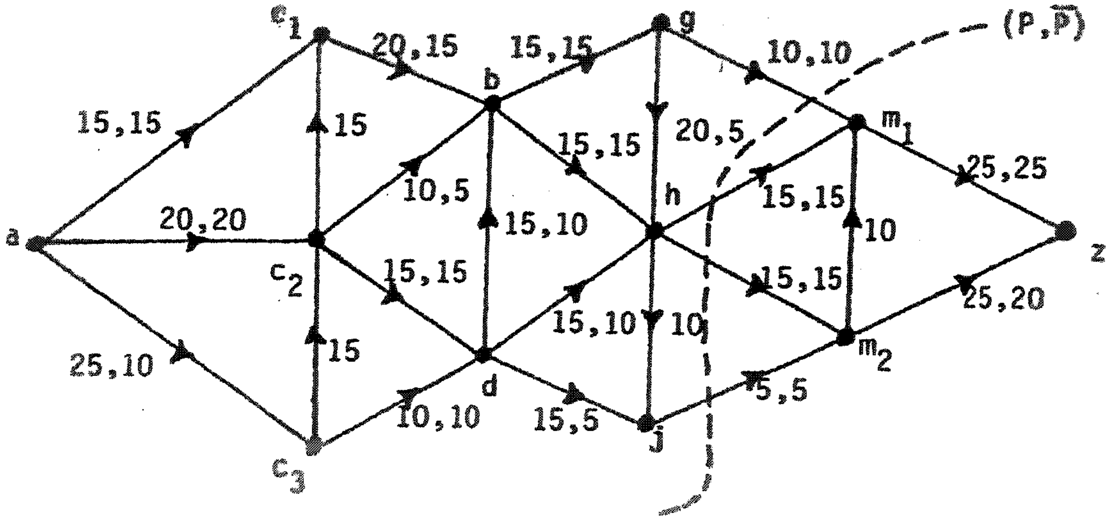
The maximal flow is 32, which is $c(P, \overline{P})$ for $P = \{a, b, d, g, h\}$ and $\overline{P} = \{i, z\}$.

(2)

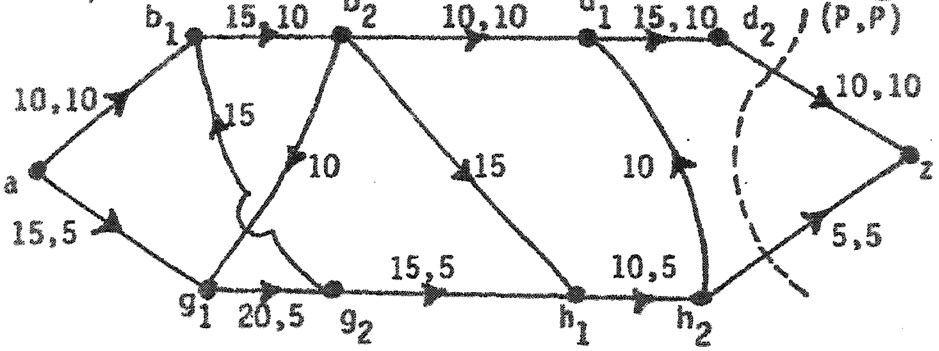


The maximal flow is 23, which is $c(P, \overline{P})$ for $P = \{a\}$ and $\overline{P} = \{b, g, i, j, d, h, k, z\}$.

4. (Example 13.12)



(Example 13.13)



(Example 13.14) Four messengers should be sent out – one for each of the following paths (which are mutually disjoint in pairs).

(1) $a \to b \to h \to p \to z$

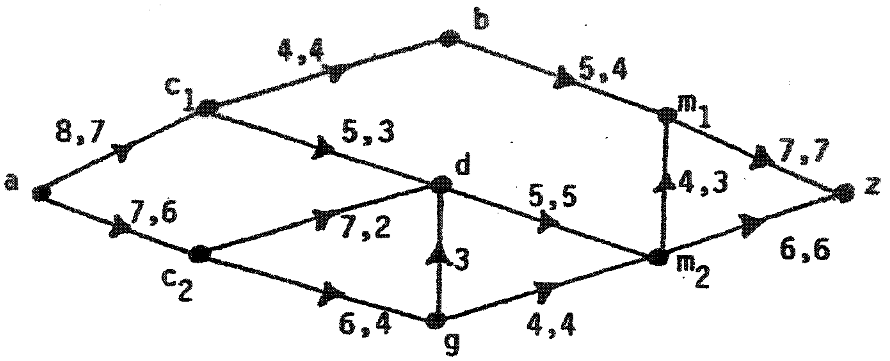
(2) $a \to d \to i \to m \to q \to z$

(3) $a \to f \to j \to n \to r \to z$

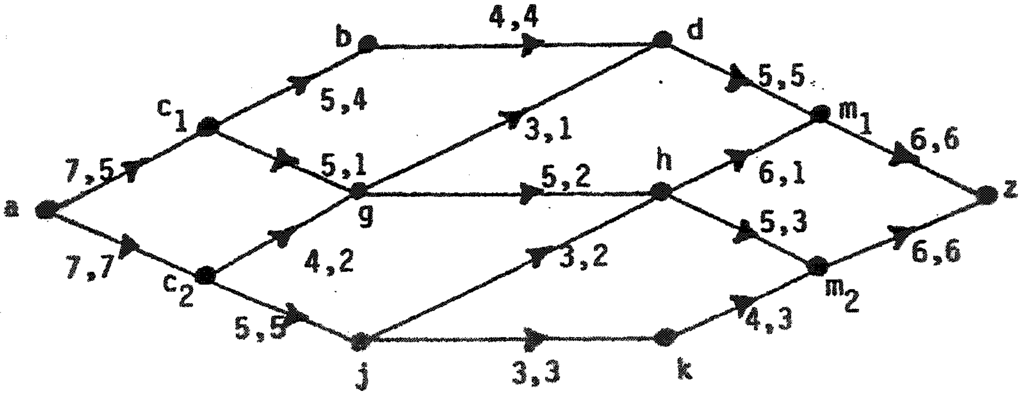
(4) $a \to g \to k \to s \to z$

5. Here $c(e)$ is a positive integer for each $e \in E$ and the initial flow is defined as $f(e) = 0$ for all $e \in E$. The result follows because Δ_p is a positive integer for each application of the Edwards-Karp algorithm and, in the Ford-Fulkerson algorithm, $f(e) - \Delta_p$ will not be negative for a backward edge.

6. (a)

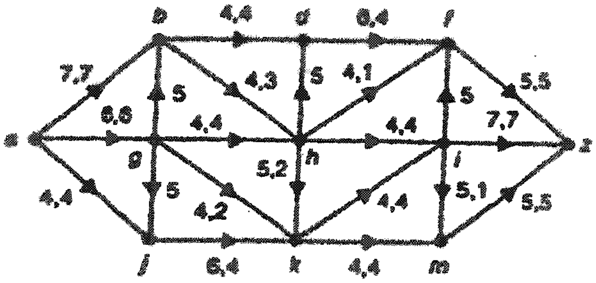


(b)



In either situation the supply will meet the manufacturers' demands.

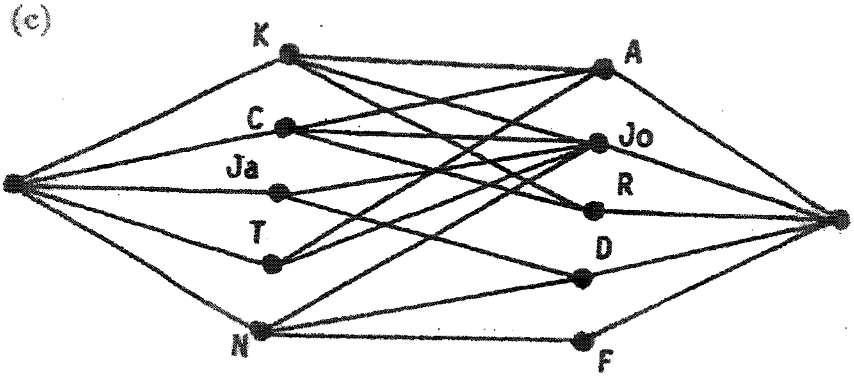
7.



Section 13.4

1. $5/\binom{8}{4} = 1/14$

2. (a), (b), and (c)



The edges $\{K, A\}$, $\{T, Jo\}$, $\{C, R\}$, $\{Ja, D\}$, and $\{N, F\}$ determine a complete matching which pairs Janice with Dennis and Nettie with Frank.

(d) No. Every complete matching must include $\{N, F\}$.

3. Let the committees be represented as $c_1, c_2, \ldots, c_6$, according to the way they are listed in the exercise.

(a) Select the members as follows: $c_1 - A$; $c_2 - G$; $c_3 - M$; $c_4 - N$; $c_5 - K$; $c_6 - R$.

(b) Select the nonmembers as follows: $c_1 - K$; $c_2 - A$; $c_3 - G$; $c_4 - J$; $c_5 - M$; $c_6 - P$.

4. (a) $(4)(3) = 12$ (b) $(4)(3)(2)(1) = 4! = 24$
(c) $(9)(8)(7)(6)(5) = 9!/4! = P(9,5)$
(d) $(n)(n-1)(n-2)\cdots(n-m+1) = n!/(n-m)! = P(n,m)$.

5. (a) A one-factor for a graph $G = (V, E)$ consists of edges which have no common vertex. So the one-factor contains an even number of vertices, and since it spans G we must have $|V|$ even.
(b) Consider the Petersen graph as shown in Figure 11.52 (a) of the text. The edges

$$\{e,a\} \qquad \{b,c\} \qquad \{d,i\} \qquad \{g,j\} \qquad \{f,h\}$$

provide a one-factor for this graph.
(c) There are $(5)(3) = 15$ one-factors for K_6.
(d) Label the vertices of K_{2n} with $1, 2, 3, \ldots, 2n-1, 2n$. We can pair vertex 1 with any of the other $2n-1$ vertices, and we are then confronted, in the case where $n \geq 2$, with finding a one-factor for the graph K_{2n-2}. Consequently,

$$a_n = (2n-1)a_{n-1}, \qquad a_1 = 1.$$

We find that

$$a_n = (2n-1)a_{n-1} = (2n-1)(2n-3)a_{n-2} = (2n-1)(2n-3)(2n-5)a_{n-3} = \ldots$$

$$= (2n-1)(2n-3)(2n-5)\cdots(5)(3)(1) = \frac{(2n)(2n-1)(2n-2)(2n-3)\cdots(4)(3)(2)(1)}{(2n)(2n-2)\cdots(4)(2)}$$

$$= \frac{(2n)!}{2^n(n!)}$$

6. (Corollary 13.6) Let $A \subseteq X$. Since $\deg(x) \geq k$ for all $x \in X$, there are at least $k|A|$ edges that are incident from the vertices in A. These edges are incident to $|R(A)|$ vertices in Y. Since $\deg(y) \leq k$ for all $y \in Y$, it follows that $k|A| \leq k|R(A)|$, so we have $|A| \leq |R(A)|$, and there is a complete matching of X into Y (by virtue of Theorem 13.7).

7. Yes, such an assignment can be made by Fritz. Let X be the set of student applicants and Y the set of part-time jobs. Then for all $x \in X$, $y \in Y$, draw the edge (x, y) if applicant x is qualified for part-time job y. Then $\deg(x) \geq 4 \geq \deg(y)$ for all $x \in X$, $y \in Y$, and the result follows from Corollary 13.6.

8. (a) $4 \in A_1$, $3 \in A_2$, $1 \in A_3$, $2 \in A_4$.

   (b) $2 \in A_1$, $4 \in A_2$, $5 \in A_3$, $1 \in A_4$, $3 \in A_5$.

   (c) Since $|\cup_{i=1}^{5} A_i| = 4 < 5$, there is no system of distinct representatives.

9. (a) (1) Select i from A_i, for $1 \leq i \leq 4$.

   (2) Select $i+1$ from A_i, for $1 \leq i \leq 3$, and 1 from A_4.

   (b) 2

10. (a) If there is a system of distinct representatives then $|\cup_{i=1}^{n} A_i| \geq n$, i.e., $k \geq n$, since $|\cup_{i=1}^{n} A_i| = |A_i| = k$, for all $1 \leq i \leq n$. Conversely, if there is no system of distinct representatives, then for some $1 \leq i \leq n$, the union of i of the sets $A_1, A_2, \ldots, A_n$ contains less than i elements. Hence $k < i \leq n$, or $k < n$.

    (b) $P(k, n)$.

11. Proof: For each subset A of X, let G_A be the subgraph of G induced by the vertices in $A \cup R(A)$. If e is the number of edges in G_A, then $e \geq 4|A|$ because $\deg(a) \geq 4$ for all $a \in A$. Likewise $e \leq 5|R(A)|$ because $\deg(b) \leq 5$ for all $b \in R(A)$. So $5|R(A)| \geq 4|A|$ and $\delta(A) = |A| - |R(A)| \leq |A| - (4/5)|A| = (1/5)|A| \leq (1/5)|X| = 2$. Then since $\delta(G) = \max\{\delta(A) | A \subseteq X\}$ we have $\delta(G) \leq 2$.

12. Let $\emptyset \neq A \subseteq X$ and $E_1 \subseteq E$ where $E_1 = \{\{a, b\} | a \in A, b \in R(A)\}$. Since $\deg(a) \geq 3$ for all $a \in A$, $|E_1| \geq 3|A|$. For each $b \in R(A) \subseteq Y$, $\deg(b) \leq 7$, so $|E_1| \leq 7|R(A)|$. Hence $3|A| \leq 7|R(A)|$ and $\delta(A) = |A| - |R(A)| \leq |A| - (3/7)|A| = (4/7)|A|$. Since $|X| \leq 50$ and $A \subseteq X$, $\delta(A) \leq (4/7)(50) = 200/7$ and $\delta(G) = \max\{\delta(A) | A \subseteq X\} \leq 28$.

13. (a) $\delta(G) = 1$. A maximal matching of X into Y is given by $\{\{x_1, y_4\}, \{x_2, y_2\}, \{x_3, y_1\}, \{x_5, y_3\}\}$.

(b) If $\delta(G) = 0$, there is a complete matching of X into Y, and $\beta(G) = |Y|$, or $|Y| = \beta(G) - \delta(G)$. If $\delta(G) = k > 0$, let $A \subseteq X$ where $|A| - |R(A)| = k$. Then $A \cup (Y - R(A))$ is a largest maximal independent set in G and $\beta(G) = |A| + |Y - R(A)| = |Y| + (|A| - |R(A)|) = |Y| + \delta(G)$, so $|Y| = \beta(G) - \delta(G)$.

(c) Figure 13.30 (a): $\{x_1, x_2, x_3, y_2, y_4, y_5\}$;
Figure 13.32: $\{x_3, x_4, y_2, y_3, y_4\}$.

14. Proof (By Mathematical Induction):
The hypercube Q_2 has vertex set $V = \{00, 01, 10, 11\}$ and edge set $E = \{\{00, 01\}, \{01, 11\}, \{11, 10\}, \{10, 00\}\}$. Here there are two perfect matchings: $\{\{10, 00\}, \{11, 01\}\}$ and $\{\{10, 11\}, \{00, 01\}\}$. So the result is true in this first case, where $n = 2$.

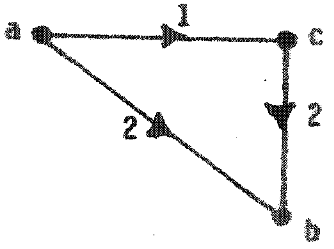
Assume the result is true for $n = k$ (≥ 2) – that is, that Q_k has at least $2^{(2^{k-2})}$ perfect matchings. Now consider the case for $n = k + 1$. In dealing with the hypercube Q_{k+1}, consider the subgraphs induced by the two sets of vertices $V^{(i)} = \{v | v \text{ is a vertex in } Q_{k+1} \text{ with first component } i\}$, $i = 0, 1$. The subgraph of Q_{k+1} induced by $V^{(0)}$ is (isomorphic to) Q_k – likewise, for the subgraph induced by $V^{(1)}$. From the induction hypothesis each of these subgraphs has at least $2^{(2^{k-2})}$ perfect matchings. Since the two subgraphs have no common edges, it follows from the rule of product that Q_{k+1} has at least $2^{(2^{k-2})} \cdot 2^{(2^{k-2})} = 2^{(2^{k-2} + 2^{k-2})} = 2^{[2(2^{k-2})]} = 2^{2^{(k+1)-2}}$ perfect matchings.

The result now follows for all $n \geq 2$ by the Principle of Mathematical Induction.

Supplementary Exercises

1. $d(a, b) = 5$; $d(a, c) = 11$; $d(a, d) = 7$; $d(a, e) = 8$;
$d(a, f) = 19$; $d(a, g) = 9$; $d(a, h) = 14$
(Note that the loop at vertex g and the edges (c, a) of weight 9 and (f, e) of weight 5 are of no significance.)

2. The algorithm is not correct. The following weighted directed graph provides a counterexample.



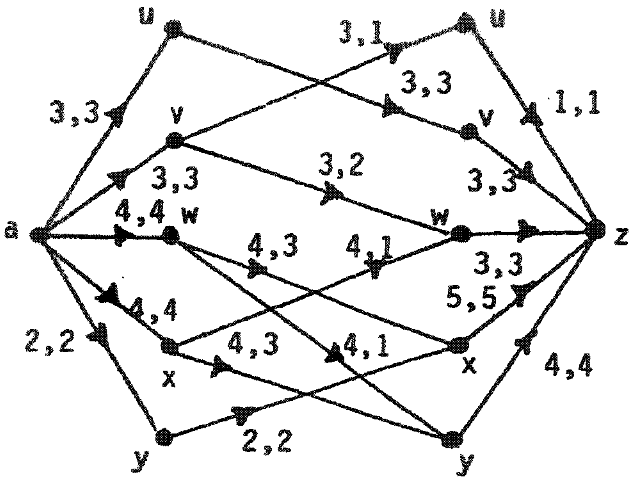
3. (a) The edge e_1 will always be selected in the first step of Kruskal's Algorithm.

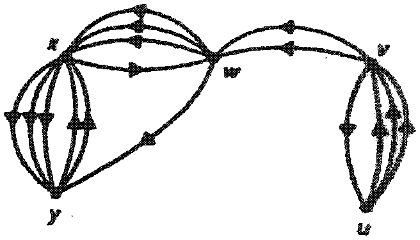
(b) Again using Kruskal's Algorithm, edge e_2 will be selected in the first application of Step (2) unless each of the edges e_1, e_2 is incident with the same two vertices, i.e., the edges e_1, e_2 form a circuit and G is a multigraph.

4. (a) In applying Kruskal's Algorithm, the only way we would have to consider edge e_1 as our last choice is if there is a vertex v in the graph where $e_1 = \{w, v\}$ and v is a pendant vertex of G. This cannot happen here since e_1 is part of a cycle.

(b) This result is false. Let G be the graph K_3 where the edges are assigned the weights $wt(e_1) = 3$, $wt(e_2) = 2$, $wt(e_3) = 1$.

5.





The transport network in the first diagram is determined by using the in degrees of the vertices for the capacities of the edges terminating at the sink z; the out degrees of the vertices are used for the capacities of the edges that originate at the source a.

6. (a) One possible selection is $qs : q$; $tq : t$; $ut : u$; $pqr : p$; $srt : r$.

(b) There are nine selections that each determine a system of distinct representatives. Consequently, the probability that the selection yields a system of distinct representatives is $9/[(2^3)(3^2)]$.

7. The number of different systems of distinct representatives is d_n, the number of derangements of $\{1, 2, 3, \ldots, n\}$.

8. (a) $5!$; $n!$

(b) Each entry in B is nonnegative and the sum of the entries in each row or column is 1.

(c)

$$B = (0.1)\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} + (0.2)\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + (0.3)\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} + (0.4)\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

(d) The r rows of B sum to r, since each row of B sums to 1. When we add the entries, considered in s columns, we get a result of s if we are dealing with all of the entries in the s columns. Hence here the entries sum to a number less than or equal to s. Consequently we have both $r > s$ and $r \leq s$, a contradiction.

Since this is a complete matching of X into Y we have n edges of the form $\{x_i, y_j\}$, where each of x_i and y_j, $1 \leq i, j \leq n$, appears exactly once. These edges are determined by the n nonnegative numbers b_{ij}, where no two of these numbers are in the same row or column of B. Writing $B = c_1P_1 + B_1$ where c_1 is the smallest entry in B and P_1 is an $n \times n$ permutation matrix, the sums of the entries in each row and column of B_1 is $1 - c_1$, where $0 \leq 1 - c_1 < 1$.

(e) We now repeat the argument in part (d) for the matrix B_1 and get $B = c_1P_1 + c_2P_2 + B_2$, where the sum of the entries in each row and column of B_2 is $1 - c_1 - c_2$, where $0 \leq 1 - c_1 - c_2 < 1 - c_1$. This process is continued until we obtain $B = c_1P_1 + c_2P_2 + \ldots + c_kP_k + B_k$ where all entries in B_k are 0.

9. The vertices (in the line graph $L(G)$) determined by E' form a maximal independent set.

PART 4

MODERN

APPLIED

ALGEBRA

CHAPTER 14
RINGS AND MODULAR ARITHMETIC

Section 14.1

1. (Example 14.5): $-a = a,\ -b = e,\ -c = d,\ -d = c,\ -e = b$
(Example 14.6): $-s = s,\ -t = y,\ -v = x,\ -w = w,\ -x = v,\ -y = t$

2. (a) This set is not a ring under ordinary addition and multiplication because there are no additive inverses.

(c) and (d) These sets are rings under ordinary addition and multiplication.

(d) This set is not a ring because it is not closed under multiplication.

3.

$$\begin{array}{lrcll}
\text{(a)} & (a+b)+c & = & (b+a)+c & \text{Commutative Law of } + \\
 & & = & b+(a+c) & \text{Associative Law of } + \\
 & & = & b+(c+a) & \text{Commutative Law of } + \\
\text{(b)} & d+a(b+c) & = & d+(ab+ac) & \text{Distributive Law of } \cdot \text{ over } + \\
 & & = & (d+ab)+ac & \text{Associative Law of } + \\
 & & = & (ab+d)+ac & \text{Commutative Law of } + \\
 & & = & ab+(d+ac) & \text{Associative Law of } + \\
\text{(c)} & c(d+b)+ab & = & ab+c(d+b) & \text{Commutative Law of } + \\
 & & = & ab+(cd+cb) & \text{Distributive Law of } \cdot \text{ over } + \\
 & & = & ab+(cb+cd) & \text{Commutative Law of } + \\
 & & = & (ab+cb)+cd & \text{Associative Law of } + \\
 & & = & (a+c)b+cd & \text{Distributive Law of } \cdot \text{ over } + \\
\text{(d)} & a(bc)+(ab)d & = & (ab)c+(ab)d & \text{Associate Law of } \cdot \\
 & & = & (ab)(c+d) & \text{Distributive Law of } \cdot \text{ over } + \\
 & & = & (ab)(d+c) & \text{Commutative Law of } +
\end{array}$$

4. No. Although there is an identity for this definition of $+$, namely $\emptyset$, there are no additive inverses.

5. (a) (i) The closed binary operation $\oplus$ is associative. For all $a, b, c \in \mathbf{Z}$ we find that

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = (a + b - 1) + c - 1 = a + b + c - 2,$$

and

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2.$$

(ii) For the closed binary operation $\odot$ and all $a, b, c \in \mathbf{Z}$, we have

$(a\odot b)\odot c = (a+b-ab)\odot c = (a+b-ab)+c-(a+b-ab)c = a+b-ab+c-ac-bc+abc = a+b+c-ab-ac-bc+abc$; and

$a\odot(b\odot c) = a\odot(b+c-bc) = a+(b+c-bc)-a(b+c-bc) = a+b+c-bc-ab-ac+abc = a+b+c-ab-ac-bc+abc$.

Consequently, this closed binary operation is also associative.

(iii) Given any integers a, b, c, we find that

$(b\oplus c)\odot a = (b+c-1)\odot a = (b+c-1)+a-(b+c-1)a = b+c-1+a-ba-ca+a = 2a+b+c-1-ba-ca$, and

$(b\odot a)\oplus(c\odot a) = (b+a-ba)\oplus(c+a-ca) = (b+a-ba)+(c+a-ca)-1 = 2a+b+c-1-ba-ca$.

Therefore the second distributive law holds. (The proof for the first distributive law is similar.)

(b) For all $a, b \in \mathbf{Z}$,

$$a\odot b = a+b-ab = b+a-ba = b\odot a,$$

because both ordinary addition and ordinary multiplication are commutative operations for $\mathbf{Z}$. Hence $(\mathbf{Z}, \oplus, \odot)$ is a commutative ring.

(c) Aside from 0 the only other unit is 2, since $2\odot 2 = 2+2-(2\cdot 2) = 0$, the unity for $(\mathbf{Z}, \oplus, \odot)$.

(d) This ring is an integral domain, but not a field. For all $a, b \in \mathbf{Z}$ we see that

$a\odot b = 1$ (the zero element) $\Rightarrow a+b-ab = 1 \Rightarrow a(1-b) = (1-b) \Rightarrow (a-1)(1-b) = 0 \Rightarrow a = 1$ or $b = 1$, so there are no proper divisors of zero in $(\mathbf{Z}, \oplus, \odot)$.

6. The trouble here is with the Distributive Laws. For $a, b, c \in \mathbf{Z}$ we find that

$$\begin{aligned} a\odot(b\oplus c) &= a\odot(b+c-7) = a+(b+c-7)-3a(b+c-7) \\ &= a+b+c-3ab-3ac+21a-7 \\ &= 22a+b+c-3ab-3ac-7, \end{aligned}$$

while

$$\begin{aligned} (a\odot b)\oplus(a\odot c) &= (a+b-3ab)\oplus(a+c-3ac) \\ &= (a+b-3ab)+(a+c-3ac)-7 \\ &= 2a+b+c-3ab-3ac-7. \end{aligned}$$

Hence, if $a \neq 0$, then $a\odot(b\oplus c) \neq (a\odot b)\oplus(a\odot c)$.

7. From the previous exercise we know that we need to determine the condition(s) on k, m for which the Distributive Laws will hold. Since $\odot$ is commutative we can focus on just one of these laws.

If $x, y, z \in \mathbf{Z}$, then

$x\odot(y\oplus z) = (x\odot y)\oplus(x\odot z) \Rightarrow$

$x\odot(y+z-k) = (x+y-mxy)\oplus(x+z-mxz)$

$\Rightarrow x+(y+z-k)-mx(y+z-k) = (x+y-mxy)+(x+z-mxz)-k$

$\Rightarrow x + y + z - k - mxy - mxz + mkx = x + y - mxy + x + z - mxz - k$
$\Rightarrow mkx = x \Rightarrow mk = 1 \Rightarrow m = k = 1$ or $m = k = -1$, since $m, k \in \mathbf{Z}$.

8.

(a) x
(b) $-s = t,\ -t = s,\ -x = x,\ -y = y$
(c) $t(s + xy) = y$
(d) Yes, the ring is commutative.
(e) No, there is no unity.
(f) The elements s, y are a pair of (proper) zero divisors.

9. (a) We shall verify one of the distributive laws. If $a, b, c \in \mathbf{Q}$, then

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c + 7) \\ &= a + (b + c + 7) + [a(b + c + 7)]/7 \\ &= a + b + c + 7 + (ab/7) + (ac/7) + a, \end{aligned}$$

while

$$\begin{aligned} (a \odot b) \oplus (a \odot c) &= (a \odot b) + (a \odot c) + 7 \\ &= a + b + (ab/7) + a + c + (ac/7) + 7 \\ &= a + b + c + 7 + (ab/7) + (ac/7) + a. \end{aligned}$$

Also, the rational number -7 is the zero element, and the additive inverse of each rational number a is $-14 - a$.

(b) Since $a \odot b = a + b + (ab/7) = b + a + (ba/7) = b \odot a$ for all $a, b \in \mathbf{Q}$, the ring $(\mathbf{Q}, \oplus, \odot)$ is commutative.

(c) For each $a \in \mathbf{Q}$, $a = a \odot u = a + u + (au/7) \Rightarrow u[1 + (a/7)] = 0 \Rightarrow u = 0$, because a is arbitrary. Hence the rational number 0 is the unity for this ring.
Now let $a \in \mathbf{Q}$, where $a \neq -7$, the zero element of the ring. Can we find $b \in \mathbf{Q}$ so that $a \odot b = 0$ – that is, so that $a + b + (ab/7) = 0$? It follows that $a + b + (ab/7) = 0 \Rightarrow b(1 + (a/7)) = -a \Rightarrow b = (-a)/[1 + (a/7)]$. Hence every rational number, other than -7, is a unit.

(d) From part (c) we know that $(\mathbf{Q}, \oplus, \odot)$ is a field. In order to verify that it is also an integral domain, let $a, b \in \mathbf{Q}$ with $a \odot b = -7$. Here we have $a \odot b = -7 \Rightarrow a + b + (ab/7) = -7$
$\Rightarrow a[1 + (b/7)] = -b - 7 \Rightarrow a[7 + b] = (-1)[7 + b](7)$
$\Rightarrow (a + 7)(b + 7) = 0 \Rightarrow a + 7 = 0$ or $b + 7 = 0 \Rightarrow a = -7$ or $b = -7$.
Consequently, there are no proper divisors of zero (the rational number -7) and $(\mathbf{Q}, \oplus, \odot)$ is an integral domain.

10. (a) $k = 3$; $m = -3$.
(b) The zero element is k. Hence we have $6 \oplus (-9) = k = 6 + (-9) - k$, so $2k = -3$ and $k = -3/2$. [Here $m = 3/2$.]
(c) The unity is the rational number 0. So we want $0 = 2 \odot (1/8) = 2 + (1/8) + [2(1/8)/m]$. This happens when $-17/8 = 1/4m$, or $4m = -8/17$. Hence $m = -2/17$ and $k = 2/17$.

11. (a) For example, $(a+bi)+(c+di)=(a+c)+(b+d)i=(c+a)+(d+b)i=(c+di)+(a+bi)$, because addition in $\mathbf{Z}$ is commutative. In like manner, each of the other properties for R to be a commutative ring with unity follow from the corresponding property of $(\mathbf{Z},+,\cdot)$. Finally, with respect to divisors of zero, if $(a+bi)(c+di)=(ac-bd)+(bc+ad)i=0$ and $a+bi\neq 0$, then at least one of a,b is nonzero. Assume, without loss of generality, that $a\neq 0$. $ac-bd=0\Longrightarrow c=bd/a$; $bc+ad=0\Longrightarrow d=-bc/a$. $cd=(bd/a)(-bc/a)=(-b^2/a^2)(cd)\Longrightarrow cd(1+(b^2/a^2))=0\Longrightarrow cd(a^2+b^2)=0\Longrightarrow c=0$ or $d=0$, since $a,b,c,d\in\mathbf{Z}$ and $a\neq 0$. $c=0$, $d=-bc/a\Longrightarrow d=0$. Also $d=0$, $c=bd/a\Longrightarrow c=0$. Hence $c+di=0$ and R is an integral domain.

(b) $a+bi$ is a unit in R if there is an element $c+di\in R$ with $(a+bi)(c+di)=1$. $1=(a+bi)(c+di)=(ac-bd)+(bc+ad)i\Longrightarrow ac-bd=1$, $bc+ad=0\Longrightarrow c=a/(a^2+b^2)$, $d=-b/(a^2+b^2)$. $c,d\in\mathbf{Z}\Longrightarrow a^2+b^2=1\Longrightarrow a=\pm1$, $b=0$; $a=0$, $b=\pm1$. Hence, the units of R are $1,-1,i$, and $-i$.

12. (a)
$$\begin{bmatrix}1&2\\3&7\end{bmatrix}\begin{bmatrix}a&b\\c&d\end{bmatrix}=\begin{bmatrix}1&0\\0&1\end{bmatrix}\Longrightarrow a+2c=1,\ 3a+7c=0,\ b+2d=0,\ 3b+7d=1\Longrightarrow$$
$a=7$, $b=-2$, $c=-3$, $d=1$.

(b) $$\begin{bmatrix}1&2\\3&8\end{bmatrix}^{-1}=\begin{bmatrix}4&-1\\(-3/2)&(1/2)\end{bmatrix}\in M_2(\mathbf{Q})$$ but this matrix is not in $M_2(\mathbf{Z})$.

13.
$$\begin{bmatrix}a&b\\c&d\end{bmatrix}^{-1}=(1/(ad-bc))\begin{bmatrix}d&-b\\-c&a\end{bmatrix},\quad\text{when } ad-bc\neq 0.$$

14. Let $\mathcal{U}=\{1,2,3\}$ and $R=\mathcal{P}(\mathcal{U})$. Then $(R,\Delta,\cap)$ is a ring with eight elements. To obtain a ring with 16 elements consider $\mathcal{U}=\{1,2,3,4\}$. In general, for each $n\in\mathbf{Z}^+$, if $\mathcal{U}=\{1,2,\ldots,n\}$ and $R=\mathcal{P}(\mathcal{U})$, then $(R,\Delta,\cap)$ is a ring with $|R|=2^n$.

15. (a) $xx=x(t+y)=xt+xy=t+y=x$
$yt=(x+t)t=xt+tt=t+t=s$
$yy=y(t+x)=yt+yx=s+s=s$
$tx=(y+x)x=yx+xx=s+x=x$
$ty=(y+x)y=yy+xy=s+y=y$

(b) Since $tx=x\neq t=xt$, this ring is not commutative.

(c) There is no unity, and consequently no units.

(d) The ring is neither an integral domain nor a field.

Section 14.2

1. (Theorem 14.5 (a)) Suppose that $u_1, u_2 \in R$ and that u_1, u_2 are both unity elements. Then $u_1 = u_1u_2 = u_2$. The first equality holds because u_2 is a unity element; the second equality follows since u_1 is a unity element.

   (Theorem 14.5 (b)) Let $y_1, y_2 \in R$ with $xy_1 = y_1x = u = xy_2 = y_2x$, where u is the unity of R. Then $y_1 = uy_1 = (y_2x)y_1 = y_2(xy_1) = y_2u = y_2$.

   (Theorem 14.10 (b)) If S is a subring of R, then $a, b \in S \Longrightarrow a + b,\ ab \in S$. Conversely, let $S = \{x_1, x_2, \ldots, x_n\}$. $T = \{x_i + x_1 | 1 \leq i \leq n\} \subseteq S$. $x_i + x_1 = x_j + x_1 \Longrightarrow x_i = x_j$, so $|T| = n$ and $T = S$. Hence $x_i + x_1 = x_1$ for some $1 \leq i \leq n$, and $x_i = z$, the zero element of R. For each $x \in S$, $x + S = \{x + x_i | 1 \leq i \leq n\} = S$. With $z \in S$, $x + x_j = z$ for some $x_j \in S$, so $x_j = -x \in S$. Consequently, by Theorem 14.9 S is a subring of R.

2. (a) $a(b - c) = a[b + (-c)] = ab + a(-c) = ab + [a(-c)] = ab + (-ac) = ab - (ac)$.

   (b) This part is verified in a similar way.

3. (a) $(ab)(b^{-1}a^{-1}) = aua^{-1} = aa^{-1} = u$ and $(b^{-1}a^{-1})(ab) = b^{-1}ub = b^{-1}b = u$, so ab is a unit. Since the multiplicative inverse of a unit is unique, it follows that $(ab)^{-1} = b^{-1}a^{-1}$.

   (b) $A^{-1} = \begin{bmatrix} 2 & -7 \\ -1 & 4 \end{bmatrix}$, $B^{-1} = \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix}$, $(AB)^{-1} = \begin{bmatrix} 4 & -15 \\ -9 & 34 \end{bmatrix}$,

   $(BA)^{-1} = \begin{bmatrix} 16 & -39 \\ -9 & 22 \end{bmatrix}$, $B^{-1}A^{-1} = \begin{bmatrix} 4 & -15 \\ -9 & 34 \end{bmatrix}$.

4. Let u be the unity of R and let x be a unit. Hence there is an element $y \in R$ with $xy = yx = u$. If $xw = z$, the zero of R, then $y(xw) = yz = z$ and $y(xw) = (yx)w = uw = w$. Hence x is not a zero divisor.

5. $(-a)^{-1} = -(a^{-1})$

6. (a) $S = \{z, w\}$

   $$\begin{array}{ll} s + s = s & s \cdot s = s \\ s + w = w + s = w & s \cdot w = w \cdot s = s \\ w + w = s & w \cdot w = w \end{array}$$

   $-s = s, -w = w$

   It follows from Theorem 14.9 that $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$.
   For all $r \in R$, $rs = sr = s$ and $rw = wr = s$ or w. Hence $(S, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

   (b) $T = \{s, v, x\}$.

$+$	s	v	x
s	s	v	x
v	v	x	s
s	x	s	v

$\cdot$	s	v	x
s	s	s	s
v	s	x	v
x	s	v	x

$-s = s$, $-v = x$, $-x = v$.

It follows from Theorem 14.9 that $(T, +, \cdot)$ is a subring of $(R, +, \cdot)$.
Also, for all $r \in R$ we have rs, sr, rv, vr, rx, and xr in T, so $(T, +, \cdot)$ is an ideal of $(R, +, \cdot)$.

7. $z \in S, T \Longrightarrow z \in S \cap T \Longrightarrow S \cap T \neq \emptyset$. $a, b \in S \cap T \Longrightarrow a, b \in S$ and $a, b \in T \Longrightarrow a + b, ab \in S$ and $a + b, ab \in T \Longrightarrow a + b, ab \in S \cap T$.
$a \in S \cap T \Longrightarrow a \in S$ and $a \in T \Longrightarrow -a \in S$ and $-a \in T \Longrightarrow -a \in S \cap T$.
So $S \cap T$ is a subring of R.

8. For $x = y = 0$ we have $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$, so S is *not* empty.

Now consider two elements of S — that is, two matrices of the form

$$\begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} v & v-w \\ v-w & w \end{bmatrix},$$

where $x, y, v, w \in \mathbf{Z}$. Then

(i) $\begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} - \begin{bmatrix} v & v-w \\ v-w & w \end{bmatrix} = \begin{bmatrix} x-v & (x-y)-(v-w) \\ (x-y)-(v-w) & y-w \end{bmatrix} =$

$$\begin{bmatrix} x-v & (x-v)-(y-w) \\ (x-v)-(y-w) & y-w \end{bmatrix},$$

an element of S; and

(ii)

$$\begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix}\begin{bmatrix} v & v-w \\ v-w & w \end{bmatrix} = \begin{bmatrix} xv+(x-y)(v-w) & x(v-w)+(x-y)w \\ (x-y)v+y(v-w) & (x-y)(v-w)+yw \end{bmatrix} =$$

$$\begin{bmatrix} xv+xv-yv-xw+yw & xv-xw+xw-yw \\ xv-yv+yv-yw & xv-yv-xw+yw+yw \end{bmatrix} =$$

$$\begin{bmatrix} xv+xv-yv-xw+yw & xv-yw \\ xv-yw & xv-yv-xw+yw+yw \end{bmatrix} = \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix}$$

for $a = xv + xv - yv - xw + yw$ and $b = xv - yv - xw + yw + yw$ — and this result is also in S.

Therefore, $S (\neq \emptyset)$ is closed under subtraction and multiplication, and it follows from Theorem 14.10 that S is a subring of R.

9. If not, there exist $a, b \in S$ with $a \in T_1, a \notin T_2$, and $b \in T_2, b \notin T_1$. Since S is a subring of R, it follows that $a + b \in S$. Hence $a + b \in T_1$ or $a + b \in T_2$.

Assume without loss of generality that $a + b \in T_1$. Since $a \in T_1$ we have $-a \in T_1$, so by the closure under addition in T_1 we now find that $(-a) + (a + b) = (-a + a) + b = b \in T_1$, a contradiction.

Therefore, $S \subseteq T_1 \cup T_2 \Longrightarrow S \subseteq T_1$ or $S \subseteq T_2$.

10. (a) If r is a proper divisor of zero we are finished. Otherwise, consider the function $f : R \to R$ where $f(a) = ar$, for all $a \in R$. This function f is one-to-one — if not, we have $f(a_1) = f(a_2)$ for distinct elements a_1, a_2 in R. But $f(a_1) = f(a_2) \Rightarrow a_1 r = a_2 r \Rightarrow (a_1 - a_2)r = z$, the zero element of R. And since $a_1 - a_2 \neq z$ and $r \neq z$ we find that r is a proper divisor of zero. Furthermore, with R finite it follows from Theorem 5.11 that f is also an onto function. Consequently, there is an element s in R such that $sr = f(s) = u$, and since R is commutative we have $rs = u$. With $rs = u = sr$ we find that r is a unit of R.
(b) The result in part (a) is not valid when R is infinite. Consider the commutative ring $(\mathbf{Z}, +, \cdot)$ with unity 1. For any integer n, if $n \neq -1, 0, 1$, then n is neither a proper divisor of zero nor a unit.

11. (a) Follows by Theorem 14.9.
(b) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

(d) S is an integral domain while R is a noncommutative ring with unity.

(e) S is not an ideal of R – for example, $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, and this result is not in S.

12. (a) Let
$A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, $B = \begin{bmatrix} d & 0 \\ e & f \end{bmatrix} \in S$. Then $A + B =$

$$\begin{bmatrix} a+d & 0 \\ b+e & c+f \end{bmatrix}, \quad \text{and} \quad AB = \begin{bmatrix} ad & 0 \\ bd+ce & cf \end{bmatrix} \quad \text{with}$$

$a + d$, $b + e$, $c + f$, ad, $bd + ce$, and $cf \in \mathbf{Z}$. So $A + B$, $AB \in S$. Also,

$$\begin{bmatrix} -a & 0 \\ -b & -c \end{bmatrix} \in S \quad \text{and} \quad \begin{bmatrix} -a & 0 \\ -b & -c \end{bmatrix} = -A.$$

Hence S is a subring of $M_2(\mathbf{Z})$, by Theorem 14.9.
However, S is not an ideal of $M_2(\mathbf{Z})$. We have

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in S \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in M_2(\mathbf{Z}) \quad \text{but}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} \notin S.$$

(b) Let $A = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$, $B = \begin{bmatrix} 2e & 2f \\ 2g & 2h \end{bmatrix} \in T$.

Then $A + B = \begin{bmatrix} 2a+2e & 2b+2f \\ 2c+2g & 2d+2h \end{bmatrix} = \begin{bmatrix} 2(a+e) & 2(b+f) \\ 2(c+g) & 2(d+h) \end{bmatrix}$

and $AB = \begin{bmatrix} 4ae+4bg & 4af+4bh \\ 4ce+4dg & 4cf+4dh \end{bmatrix} = \begin{bmatrix} 2(2ae+2bg) & 2(2af+2bh) \\ 2(2ce+2dg) & 2(2cf+2dh) \end{bmatrix}$

so $A+B$, $AB \in T$. Also $\begin{bmatrix} -2a & -2b \\ -2c & -2d \end{bmatrix} = \begin{bmatrix} 2(-a) & 2(-b) \\ 2(-c) & 2(-d) \end{bmatrix}$ is the additive inverse of A and it is in T. So by Theorem 14.9 T is a subring of $M_2(\mathbf{Z})$.

If $C = \begin{bmatrix} w & x \\ y & z \end{bmatrix} \in M_2(\mathbf{Z})$ then $CA = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix} =$

$\begin{bmatrix} 2aw+2cx & 2bw+2dx \\ 2ay+2cz & 2by+2dz \end{bmatrix} = \begin{bmatrix} 2(aw+cx) & 2(bw+dx) \\ 2(ay+cz) & 2(by+dz) \end{bmatrix}$ and

$AC = \begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} =$

$\begin{bmatrix} 2aw+2by & 2ax+2bz \\ 2cw+2dy & 2cx+2dz \end{bmatrix} = \begin{bmatrix} 2(aw+by) & 2(ax+bz) \\ 2(cw+dy) & 2(cx+dz) \end{bmatrix}$

and CA, $AC \in T$, so T is an ideal of $M_2(\mathbf{Z})$.

13. Since $za = z$, it follows that $z \in N(a)$ and $N(a) \neq \emptyset$. If $r_1, r_2 \in N(a)$, then $(r_1 - r_2)a = r_1a - r_2a = z - z = z$, so $r_1 - r_2 \in N(a)$. Finally, if $r \in N(a)$ and $s \in R$, then $(rs)a = (sr)a = s(ra) = sz = z$, so rs, $sr \in N(a)$. Hence $N(a)$ is an ideal – by Definition 14.6.

14. (a) $I \subseteq R$. For each $r \in R$, $ru = r \in I$, so $R \subseteq I$. Hence $I = R$.

(b) Let $x \in I$ with x a unit of R. Let $y \in R$ where $xy = yx = u$. Then $y \in R$, $x \in I \Longrightarrow yx = u \in I$ and the result follows by part (a).

15. Two ideals: R and $\{z\}$, where z is the zero of R.

16. (a) Since $u^{-1} = u$, $a^{-1} = b$, $b^{-1} = a$, each nonzero element of $(R, +, \cdot)$ is a unit, so $(R, +, \cdot)$ is a field.

(b) $\{u, z\}$ is a subring. However, $a \in R$ and $u \in \{u, z\}$ but $au = a \notin \{u, z\}$, so $\{u, z\}$ is not an ideal.

(c) $x + by = z \Longrightarrow x = -by$, so $u = y + b(-by) = y - ay = y + ay = (u + a)y = by$ and $y = ub^{-1} = b^{-1} = a$. Hence $x = -by = -ba = -u = u$.

17. (a) $a = au \in aR$, so $aR \neq \emptyset$. If $ar_1, ar_2 \in aR$, then $ar_1 - ar_2 = a(r_1 - r_2) \in aR$. Also, for $ar_1 \in aR$, $r \in R$, $r(ar_1) = (ar_1)r = a(r_1 r) \in aR$. Hence aR is an ideal of R.

(b) Let $a \in R$, $a \neq z$. Then $a = au \in aR$ so $aR = R$. Since $u \in R = aR$, $u = ar$ for some $r \in R$, and $r = a^{-1}$. Hence R is a field.

18. (a) If z_S, z_T denote the zero elements of S, T, respectively, then for all $s \in S$, $t \in T$, $(s,t) \oplus (z_S, z_T) = (s + z_S, t +' z_T) = (s,t) = (z_S + s, z_T +' t) = (z_S, z_T) \oplus (s,t)$, so (z_S, z_T) is the zero element for R. For $(s,t), (s_1,t_1), (s_2,t_2) \in R$, $(s,t) \odot [(s_1,t_1) \oplus (s_2,t_2)] = (s,t) \odot (s_1 + s_2, t_1 +' t_2)] = (s \cdot (s_1 + s_2), t \cdot' (t_1 +' t_2) = (s \cdot s_1 + s \cdot s_2, t \cdot' t_1 +' t \cdot' t_2) = (s \cdot s_1, t \cdot' t_1) \oplus (s \cdot s_2, t \cdot' t_2) = ((s,t) \odot (s_1,t_1)) \oplus ((s,t) \odot (s_2,t_2))$. Hence this distributive law follows from the corresponding law in each of the rings S, T. In the same way one finds that the remaining ring properties are also satisfied by $(R, \oplus, \odot)$.

(b) For all (s_1,t_1), $(s_2,t_2) \in R$, $(s_1,t_1) \odot (s_2,t_2) = (s_1 \cdot s_2, t_1 \cdot' t_2) = (s_2 \cdot s_1, t_2 \cdot' t_1) = (s_2,t_2) \odot (s_1,t_1)$.

(c) $u_R = (u_S, u_T)$

(d) No. Let S, T both be the field of rational numbers. In $S \times T$ there is no multiplicative inverse for (2,0). (Also, (2,0) and (0,2) are proper divisors of zero = (0,0).)

19. (a) $\binom{4}{2}(49)$ (b) 7^4 (d) Yes, the element (u,u,u,u). (d) 4^4

20. (a) By the given recursive definition the result is true for all $m \in \mathbf{Z}^+$ and $n = 1$. Assume the result for all $m \in \mathbf{Z}^+$ and $n = k$ (≥ 1). Now consider $m \in \mathbf{Z}^+$ and $n = k + 1$. $(m+n)a = (m + (k+1))a = ((m+1) + k)a = (m+1)a + ka$ (by the induction hypothesis) $= (ma+a) + ka$ (by the definition given in the exercise) $= ma + (ka+a) = ma + [(k+1)a] = ma + na$. Hence the result is true for all $m, n \in \mathbf{Z}^+$. If m or n is 0 the result remains true. If m, n are both negative we have $m = -m_1$, $n = -n_1$, for $m_1, n_1 \in \mathbf{Z}^+$ and $(m+n)(a) = (-m_1 - n_1)(a) = (m_1 + n_1)(-a) = m_1(-a) + n_1(-a) = (-m_1)a + (-n_1)(a) = ma + na$. Finally, suppose $mn < 0$. We consider the case $m > 0$, $n = -n_1 < 0$. Then $(m+n)a = (m - n_1)(a)$. If $m = n_1$ the result follows. If $m > n_1$, $m = s + n_1$ and $(m+n)a = ((s + n_1) - n_1)a = sa = sa + n_1 a - n_1 a = (s + n_1)a - n_1 a = ma + na$. For $m < n_1$, $n_1 = t + m$ and $(m+n)a = (m - (t+m))a = (-t)a = t(-a) = t(-a) + m(-a) - m(-a) = -m(-a) + (m+t)(-a) = ma + na$. (The proof is similar for the case where $m < 0$ and $n > 0$.) Consequently, for all $m, n \in \mathbf{Z}$, $(m+n)a = ma + na$.

(c) For $n = 1$, $n(a+b) = a + b = na + nb$. Assume the result for $n = k$ (≥ 1) and consider $n = k + 1$. $n(a+b) = (k+1)(a+b) = (k(a+b)) + (a+b) = (ka+kb) + (a+b) = (ka+a) + (kb+b) = (k+1)a + (k+1)b = na + nb$, so the result is true for all $n \in \mathbf{Z}^+$. If $n < 0$, let $n = -m$. Then $n(a+b) = (-m)(a+b) = m(-(a+b)) = m((-a) + (-b)) = m(-a) + m(-b) = (-m)(a) + (-m)(b) = na + nb$, so the result is true for all $n \in \mathbf{Z}$.

(b),(d), and (e). The proofs for these parts are done in a similar way.

21. (a) For each $m \in \mathbf{Z}^+, (a^m)(a^1) = a^m a = a^{m+1}$ so the result is true for $n = 1$. Assume the result for $m \in \mathbf{Z}^+$ and $n = k\ (\geq 1)$. For $m \in \mathbf{Z}^+, n = k+1, (a^m)(a^n) = (a^m)(a^{k+1}) = (a^m)(a^k a) = (a^m a^k)(a) = (a^{m+k})(a) = a^{(m+k)+1} = a^{m+(k+1)} = a^{m+n}$. Consequently, by the Principle of Mathematical Induction the result is true for all $m, n \in \mathbf{Z}^+$.
In like manner, $(a^m)^n = a^{mn}$ for all $m \in \mathbf{Z}^+$ and $n = 1$. Assuming the result for $m \in \mathbf{Z}^+$ and $n = k\ (\geq 1)$, we consider the case for $m \in \mathbf{Z}^+$ and $n = k+1$. Then $(a^m)^{(k+1)} = (a^m)^k(a^m) = (a^{mk})(a^m) = a^{mk+m}$ (from the first result) $= a^{m(k+1)} = a^{mn}$ and the result is true for all $m, n \in \mathbf{Z}^+$ by the Principle of Mathematical Induction.

(b) If R has a unity u, define $a^0 = u$, for $a \in R$, $a \neq z$. If a is a unit of R, define a^{-n} as $(a^{-1})^n$, for $n \in \mathbf{Z}^+$.

Section 14.3

1. (a) (i) $118 - 62 = 56 = 7(8)$, so $118 \equiv 62 \pmod 8$
(ii) $-237 - (-43) = -194$, but 8 does not divide -194, so -237 and -43 are *not* congruent modulo 8.
Also, $-43 \equiv 5 \pmod 8$ while $-237 \equiv 3 \pmod 8$, so -237 and -43 are *not* congruent modulo 8 .
(iii) $230 - (-90) = 320 = 40(8)$, so $230 \equiv -90 \pmod 8$.
Also, $230 = 28(8) + 6$ and $-90 = -12(8) + 6$ so $230 \equiv 6 \equiv -90 \pmod 8$.

b) (i) $243 - 76 = 167 = 18(9) + 5$ so 243 and 77 are *not* congruent modulo 9.
Also, $243 = 27(9) + 0$ while $76 = 8(9) + 4$. Since the remainders for 243 and 76 are different for division by 9, it follows that 243 and 76 are *not* congruent modulo 9.
(ii) $700 - (-137) = 837 = 93(9)$, so 700 and -137 are congruent modulo 9.
(iii) $056 - (-1199) = 1143 = 127(9)$, so -56 and -1199 are congruent modulo 9.

2. (a) $28 - 6 = 22$, so $n(> 1)$ is a divisor of 22. With $22 = 2 \cdot 11$, there are four divisors of 22 – including 1. Consequently, there are three possible values for n-namely, 2, 11, and 22.
(b) $68 - 37 = 31$, a prime. Consequently, $n = 31$ in this case.
(c) $301 - 233 = 68 = 2^2 \cdot 17$, so there are five possible values for $n(> 1)$ – namely, 2, 4, 17, 34, and 68.
(d) Since $49 - 1 = 48 = 2^4 \cdot 3$, there are nine possible values for $n(> 1)$ – namely, 2, 4, 8, 16, 3, 6, 12, 24, 48.

3. (a) $-6, 1, 8, 14$ (b) $-9, 2, 13, 24$ (c) $-7, 10, 27, 44$

4. Proof: Here we find the following: $b \equiv c \pmod n \Rightarrow b = c + mn$, for some $m \in \mathbf{Z} \Rightarrow ab = ac + m(an) \Rightarrow ab \equiv ac \pmod{an}$.

5. Proof: Since $a \equiv b \pmod n$ we may write $a = b + kn$ for some $k \in \mathbf{Z}$. And $m|n \Rightarrow n = \ell m$

for some $\ell \in \mathbf{Z}$. Consequently, $a = b + kn = b + (k\ell)m$ and $a \equiv b \pmod{m}$.

6. Proof: If $a \equiv b \pmod{m}$, then $a - b = km$, for some $k \in \mathbf{Z}$. Likewise, $a \equiv b \pmod{n} \Rightarrow a - b = \ell n$, for some $\ell \in \mathbf{Z}$. With $km = a - b = \ell n$, it follows that $n|km$.

   Now $\gcd(m, n) = 1 \Rightarrow mx + ny = 1$, for some $x, y \in \mathbf{Z}$. Consequently, $k = kmx + kny$, and since $n|kmx$ (because $n|km$) and $n|kny$, we have $n|k$. Therefore, $k = nk_1$, for some $k_1 \in \mathbf{Z}$, and $a - b = km = k_1(mn)$. Hence, $a \equiv b \pmod{mn}$.

   Conversely, suppose that $a \equiv b \pmod{mn}$. Then $a - b = tmn$, for some $t \in \mathbf{Z}$. Consequently, $a - b = (tm)n \Rightarrow a \equiv b \pmod{n}$, and $a - b = (tn)m \Rightarrow a \equiv b \pmod{m}$.
   [Note that this result does not require $\gcd(m, n) = 1$.]

7. Let $a = 8$, $b = 2$, $m = 6$, and $n = 2$. Then $\gcd(m, n) = \gcd(6, 2) = 2 > 1$, $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$. But $a - b = 8 - 2 = 6 \neq k(12) = k(mn)$, for some $k \in \mathbf{Z}$. Hence $a \not\equiv b \pmod{mn}$.

8. Proof: If $3|n$ then $n \equiv 0 \pmod{3}$ and $2n \equiv 0 \pmod{3}$. Hence $2n + 1 \equiv 1 \pmod{3}$ and $2n - 1 \equiv 2 \pmod{3}$.

   If $3 \not| n$, then exactly one of the following occurs:

   (a) $n \equiv 1 \pmod{3} \Longrightarrow 2n \equiv 2 \pmod{3}$, and so $2n + 1 \equiv 0 \pmod{3}$, while $2n - 1 \equiv 2 \pmod{3}$, so $3|(2n + 1)$.

   (b) $n \equiv 2 \pmod{3} \Longrightarrow 2n \equiv 1 \pmod{3}$, and so $2n - 1 \equiv 0 \pmod{3}$, while $2n + 1 \equiv 2 \pmod{3}$, so $3|(2n - 1)$.

9. Proof: For n odd consider the $n - 1$ numbers $1, 2, 3, \ldots, n - 3, n - 2, n - 1$ as $(n - 1)/2$ pairs: 1 and $(n - 1)$, 2 and $(n - 2)$, 3 and $(n - 3), \ldots, n - (\frac{n-1}{2}) - 1$ and $n - (\frac{n-1}{2})$. The sum of each pair is n which is congruent to 0 modulo n. Hence $\sum_{i=1}^{n-1} i \equiv 0 \pmod{n}$.

   When n is even we consider the $n - 1$ numbers $1, 2, 3, \ldots, (n/2) - 1, (n/2), (n/2) + 1, \ldots, n - 3, n - 2, n - 1$ as $(n/2) - 1$ pairs — namely, 1 and $n - 1$, 2 and $n - 2$, 3 and $n - 3, \ldots, (n/2) - 1$ and $(n/2) + 1$ — and the single number $(n/2)$. For each pair the sum is n, or 0 modulo n, so $\sum_{i=1}^{n-1} i \equiv (n/2) \pmod{n}$.

10. (Theorem 14.11) For each $a \in \mathbf{Z}$, $a - a = 0 \cdot n$ so $a \equiv a \pmod{n}$ and the relation is reflexive. If $a, b \in \mathbf{Z}$, then $a \equiv b \pmod{n} \Longrightarrow a - b = kn$, $k \in \mathbf{Z} \Longrightarrow b - a = (-k)n, -k \in \mathbf{Z} \Longrightarrow b \equiv a \pmod{n}$, so the relation is symmetric. Finally let $a, b, c \in \mathbf{Z}$ with $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $a - b = kn$, $b - c = mn$, for some $k, m \in \mathbf{Z}$ and $(a-b) + (b-c) = a - c = (k+m)n$, so $a \equiv c \pmod{n}$ and the relation is transitive.

    (Theorem 14.12) For all $[a], [b], [c] \in \mathbf{Z}_n$, $([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a+(b+c)]$ (since $a, b, c \in \mathbf{Z}$ and addition in $\mathbf{Z}$ is associative) $= [a]+[b+c] = [a]+([b]+[c])$. Hence the addition of equivalence classes in $\mathbf{Z}_n$ is associative. Likewise, all other properties for $(\mathbf{Z}_n, +, \cdot)$ to be a commutative ring with unity $[1]$ follow from the corresponding properties of the ring $(\mathbf{Z}, +, \cdot)$.

11. (a) For each $a \in \mathbf{Z}^+$ $\tau(a) = \tau(a)$, so the relation is reflexive. If $a, b \in \mathbf{Z}^+$, $\tau(a) = \tau(b) \Longrightarrow \tau(b) = \tau(a)$ so the relation is symmetric. Finally, for $a, b, c \in \mathbf{Z}^+$, $\tau(a) = \tau(b)$ and $\tau(b) = \tau(c) \Longrightarrow \tau(a) = \tau(c)$ so the relation is transitive.

(b) No, $2\mathcal{R}3$, $3\mathcal{R}5$ but $5 \not\mathcal{R} 8$. Also, $2\mathcal{R}3$, $2\mathcal{R}5$ but $4 \not\mathcal{R} 15$.

12. $\mathbf{Z}_{11}$: $[1]^{-1} = [1]$, $[2]^{-1} = [6]$, $[3]^{-1} = [4]$, $[4]^{-1} = [3]$, $[5]^{-1} = [9]$, $[6]^{-1} = [2]$, $[7]^{-1} = [8]$, $[8]^{-1} = [7]$, $[9]^{-1} = [5]$, $[10]^{-1} = [10]$.

$\mathbf{Z}_{13}$: $[1]^{-1} = [1]$, $[2]^{-1} = [7]$, $[3]^{-1} = [9]$, $[4]^{-1} = [10]$, $[5]^{-1} = [8]$, $[6]^{-1} = [11]$, $[7]^{-1} = [2]$, $[8]^{-1} = [5]$, $[9]^{-1} = [3]$, $[10]^{-1} = [4]$, $[11]^{-1} = [6]$, $[12]^{-1} = [12]$.

$\mathbf{Z}_{17}$: $[1]^{-1} = [1]$, $[2]^{-1} = [9]$, $[3]^{-1} = [6]$, $[4]^{-1} = [13]$, $[5]^{-1} = [7]$, $[6]^{-1} = [3]$, $[7]^{-1} = [5]$, $[8]^{-1} = [15]$, $[9]^{-1} = [2]$, $[10]^{-1} = [12]$, $[11]^{-1} = [14]$, $[12]^{-1} = [10]$, $[13]^{-1} = [4]$, $[14]^{-1} = [11]$, $[15]^{-1} = [8]$, $[16]^{-1} = [16]$.

13. (a)

$$\begin{aligned} 1009 &= 59(17) + 6 & \quad 0 < 6 < 17 \\ 17 &= 2(6) + 5 & \quad 0 < 5 < 6 \\ 6 &= 1(5) + 1 & \quad 0 < 1 < 5, \end{aligned}$$

so $1 = 6 - 5 = 6 - [17 - 2(6)] = 3(6) - 17 = 3[1009 - 59(17)] - 17 = 3(1009) - 178(17)$. Hence $1 \equiv (-178)(17) \pmod{1009}$, so $[17]^{-1} = [-178] = [-178 + 1009] = [831]$.

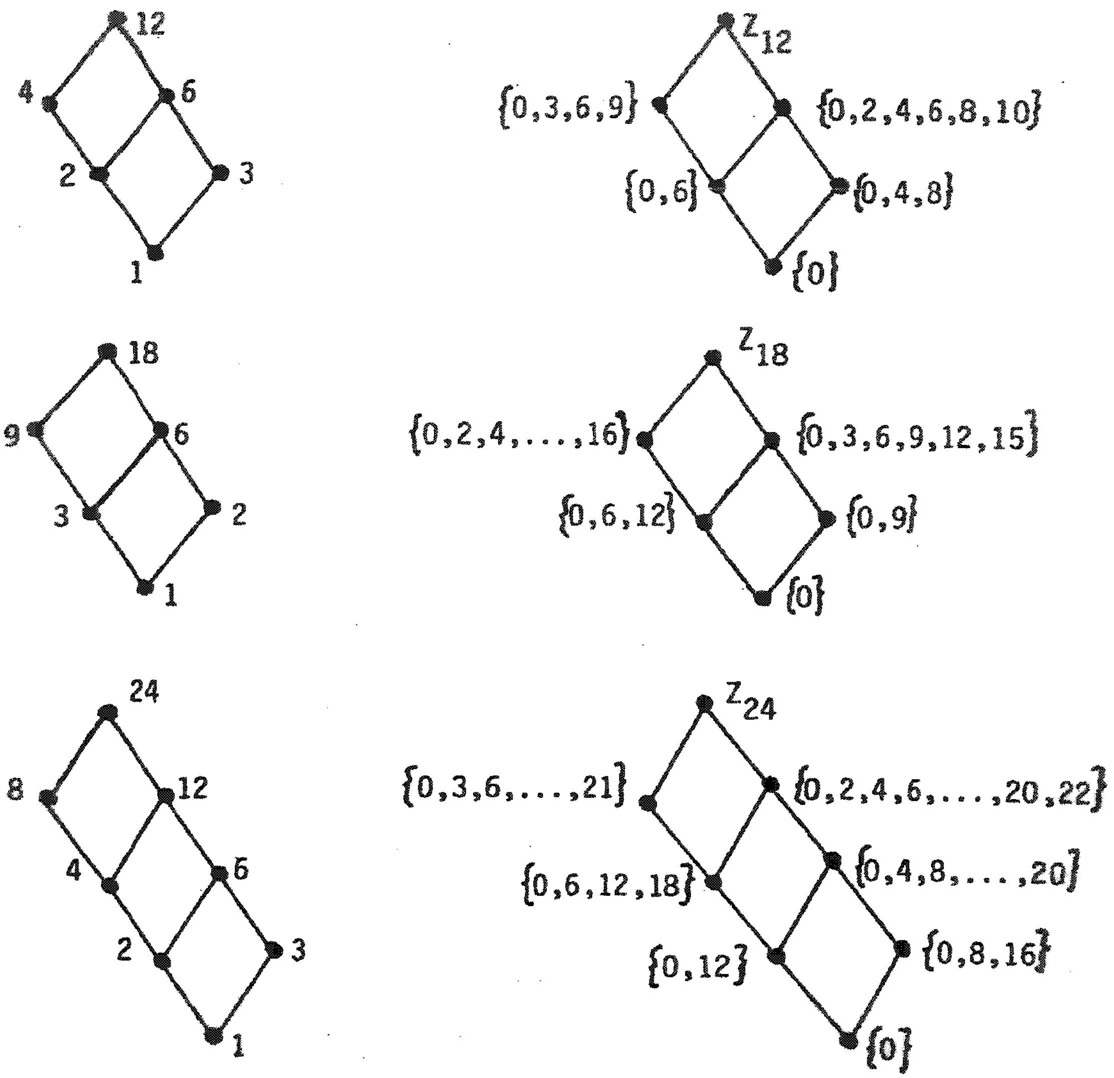
(b) $[100]^{-1} = [111]$ (c) $[777]^{-1} = [735]$.

14. (a) $\mathbf{Z}_{12}$: $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10, 12\}$, $\mathbf{Z}_{12}$.

$\mathbf{Z}_{18}$: $\{0\}$, $\{0, 9\}$, $\{0, 6, 12\}$, $\{0, 3, 6, 9, 12, 15\}$, $\{0, 2, 4, 6, \ldots, 16\}$, $\mathbf{Z}_{18}$.

$\mathbf{Z}_{24}$: $\{0\}$, $\{0, 12\}$, $\{0, 8, 16\}$, $\{0, 6, 12, 18\}$, $\{0, 4, 8, 12, 16, 20\}$, $\{0, 3, 6, \ldots, 18, 21\}$, $\{0, 2, 4, 6, \ldots, 20, 22\}$, $\mathbf{Z}_{24}$.

(b)



(c) The number of subrings of $\mathbf{Z}_n$ is $\tau(n)$, the number of positive divisors of n.

15. (a) 16 units; 0 proper zero divisors (b) 72 units; 44 proper zero divisors
(c) 1116 units; 0 proper zero divisors.

16. Let $a_1, a_2, \ldots, a_n$ be a list of n consecutive integers, $n \geq 1$. For $1 \leq i \leq n$, let b_i be the remainder upon division of a_i by n; $b_i \equiv a_i \pmod{n}$, $0 \leq b_i \leq n-1$. Then $\{b_1, b_2, \ldots, b_n\} = \{0,1,2,\ldots,n-1\}$, so $b_i = 0$ for some $1 \leq i \leq n$. $b_i = 0 \Longleftrightarrow a_i \equiv 0 \pmod{n} \Longleftrightarrow n|a_i$.

17. $\{1,2,3,\ldots,1000\} = \{1,4,7,10,\ldots,997,1000\} \cup \{2,5,8,\ldots,995,998\} \cup \{3,6,9,\ldots,999\}$. In this partition the first cell has 334 elements while the other two cells contain 333 elements each. If three elements are selected from the same cell then their sum will be divisible by three. If one number is selected from each of the three cells then their sum is divisible by three. Consequently the probability that the sum of three elements selected from $\{1,2,3,\ldots,999\}$ is divisible by three is $[\binom{334}{3} + 2\binom{333}{3} + \binom{334}{1}\binom{333}{1}^2]/\binom{1000}{3}$.

18. (a) For $m = 1$ the result is true. Assume the result true for $m = k$, i.e.,

$c \equiv d \pmod{n} \Longrightarrow c^k \equiv d^k \pmod{n}$, and consider the case of $m = k+1$. $c^m = c^{k+1} = (c^k)(c) \equiv (d^k)(d) \pmod{n}$, since $c \equiv d \pmod{n}$ and $(c^k) \equiv (d^k) \pmod{n}$. Hence $c^m = c^{k+1} \equiv d^{k+1} = d^m \pmod{n}$. By the Principle of Mathematical Induction the result follows for all $m \in \mathbf{Z}^+$.
The other result also follows by induction.

(b) Since $10 \equiv 1 \pmod{9}, 10^k \equiv 1^k = 1 \pmod{9}$ for all $k \geq 0$, and for all $0 \leq a \leq 9, (a)(10^k) \equiv a \pmod{9}$. Consequently, $x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_1 \cdot 10 + x_0 \equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod{9}$.

19. (a) For $n = 0$ we have $10^0 = 1 = 1(-1)^0$ so $10^0 \equiv (-1)^0 \pmod{11}$. [Since $10 - (-1) = 11$, $10 \equiv (-1) \pmod{11}$, or $10^1 \equiv (-1)^1 \pmod{11}$. Hence the result is true for $n = 0, 1$.] Assume the result true for $n = k \geq 1$ and consider the case for $k+1$. Then since $10^k \equiv (-1)^k \pmod{11}$ and $10 \equiv (-1) \pmod{11}$, we have $10^{k+1} = 10^k \cdot 10 \equiv (-1)^k(-1) = (-1)^{k+1} \pmod{11}$. The result now follows for all $n \in \mathbf{N}$ by the Principle of Mathematical Induction.

(b) If $x_n x_{n-1} \ldots x_2 x_1 x_0 = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10 + x_0$ denotes an $(n+1)$-st digit integer, then
$x_n x_{n-1} \ldots x_2 x_1 x_0 \equiv (-1)^n x_n + (-1)^{n-1} x_{n-1} + \cdots + x_2 - x_1 + x_0 \pmod{11}$.
Proof: $x_n x_{n-1} \ldots x_2 x_1 x_0 = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10 + x_0 \equiv x_n(-1)^n + x_{n-1}(-1)^{n-1} + \cdots + x_2(-1)^2 + x_1(-1) + x_0 = (-1)^n x_n + (-1)^{n-1} x_{n-1} + \cdots + x_2 - x_1 + x_0 \pmod{11}$.

20. If $a^2 = a$ in $\mathbf{Z}_p$, then $a^2 \equiv a \pmod{p}$, and it follows that $p|(a^2 - a)$. But $p|(a^2 - a) \Rightarrow p|a(a-1) \Rightarrow p|a$ or $p|(a-1)$, because p is prime. With $0 \leq a < p$, $p|a \Rightarrow a = 0$ and $p|(a-1) \Rightarrow a = 1$. So the only elements in $\mathbf{Z}_p$ that satisfy $a^2 = a$ are $a = 0, 1$. [Or $a = 0, 1$ are the only idempotent elements under multiplication in $\mathbf{Z}_p$.]

21. Let $g = \gcd(a, n)$, $h = \gcd(b, n)$. $a \equiv b \pmod{n} \Longrightarrow a = b + kn$, for some $k \in \mathbf{Z} \Longrightarrow g|b, h|a$. $g|b, g|n \Longrightarrow g|h$; $h|a, h|n \Longrightarrow h|g$. Since $g, h > 0$, $g = h$.

22. (a) $1 = 1$; $2^6 = 64 = 7(9) + 1$; $3^6 = 729 = 7(104) + 1$; $4^6 = 4096 = 7(585) + 1$; $5^6 = 15625 = 7(2232) + 1$; $6^6 = 46656 = 7(6665) + 1$.

(b) If $\gcd(n, 7) = 1$, then $n \equiv i \pmod{7}$, for $1 \leq i \leq 6$ and $n^6 \equiv i^6 \equiv 1 \pmod{7}$. $n^6 \equiv 1 \pmod{7} \Longleftrightarrow 7|(n^6 - 1)$.

23.

(1) Plaintext	a	ℓ	ℓ	g	a	u	ℓ	i	s	d	i	v	i	d	e	d
(2)	0	11	11	6	0	20	11	8	18	3	8	21	8	3	4	3
(3)	3	14	14	9	3	23	14	11	21	6	11	24	11	6	7	6
(4) Ciphertext	D	O	O	J	D	X	O	L	V	G	L	Y	L	G	H	G

i	*n*	*t*	*o*	*t*	*h*	*r*	*e*	*e*	*p*	*a*	*r*	*t*	*s*
8	13	19	14	19	7	17	4	4	15	0	17	19	18
11	16	22	17	22	10	20	7	7	18	3	20	22	21
L	*Q*	*W*	*R*	*W*	*K*	*U*	*H*	*H*	*S*	*D*	*U*	*W*	*V*

For each θ in row (2), the corresponding result below it in row (3) is $\theta + 3 \pmod{26}$.

24. Since the most frequently occurring letter in the English alphabet is *e*, we correspond the plaintext letter *e* with the ciphertext letter *Q*. As *Q* is 12 letters after *e* in the alphabet we have (a) $\kappa = 12$; (b) $E(\theta) \equiv \theta + 12 \pmod{26}$ and $D(\theta) \equiv \theta - 12 \pmod{26}$.

For part (c) consider the following:

(1) Ciphertext	*F*	*T*	*Q*	*I*	*M*	*K*	*I*	*Q*	*I*	*Q*	*D*	*Q*
(2)	5	19	16	8	12	10	8	16	8	16	3	16
(3)	19	7	4	22	0	24	22	4	22	4	17	4
(4) Plaintext	*t*	*h*	*e*	*w*	*a*	*y*	*w*	*e*	*w*	*e*	*r*	*e*

Here the results in row (3) are obtained from those in row (2) by applying the decryption function *D*.

The plaintext reveals the original message as 'The Way We Were'. [This is the title of an Academy award winning song sung by Barbra Streisand, as well as the title of a film starring Barbra Streisand and Robert Redford.]

25. From part (c) of Example 14.15 we know that for an alphabet of n letters there are $n \cdot \phi(n)$ affine ciphers. Here we have:
(a) $24\phi(24) = (24)[24(1 - \frac{1}{2})(1 - \frac{1}{3})] = (24)(8) = 192$
(b) $25\phi(25) = (25)[25(1 - \frac{1}{5})] = (25)(20) = 500$
(c) $27\phi(27) = (27)[27(1 - \frac{1}{3})] = (27)(18) = 486$
(d) $30\phi(30) = (30)[30(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})] = (30)(8) = 240$.

26. The nonnegative integers that correspond with the given plaintext and ciphertext letters are as follows:
$e: 4$ $W: 22$ $t: 19$ $X: 23$

The encryption function $E : \mathbf{Z}_{26} \to \mathbf{Z}_{26}$ is given by $E(\theta) \equiv \alpha\theta + \kappa \pmod{26}$, with $E(4) \equiv 4\alpha + \kappa \equiv 22 \pmod{26}$ and $E(19) \equiv 19\alpha + \kappa \equiv 23 \pmod{26}$. Therefore $(19\alpha + \kappa) - (4\alpha + \kappa) \equiv 15\alpha \equiv 23 - 22 \equiv 1 \pmod{26}$, and $\alpha \equiv 15^{-1} \pmod{26}$. The multiplicative inverse of 15 in $\mathbf{Z}_{26}$ is 7 since $15 \cdot 7 = 105 = 1 + 104 = 1 + 4(26) \equiv 1 \pmod{26}$, so $\alpha \equiv 7 \pmod{26}$ and $\kappa \equiv 22 - 4(7) \equiv -6 \equiv 20 \pmod{26}$. Consequently, $E(\theta) \equiv 7\theta + 20 \pmod{26}$.

Here $D(\theta) \equiv 7^{-1}(\theta - 20) \pmod{26}$. From above we see that $7^{-1} \equiv 15 \pmod{26}$, so $D(\theta) \equiv 15(\theta - 20) \pmod{26}$. Applying D to the nonnegative integers in row (2) of the following gives us the result in row (3), from which we extract the plaintext.

(1) Ciphertext	R	W	J	W	Q	T	O	O	M	Y	H	K	U	X	G	O	E	M	Y	P
(2)	17	22	9	22	16	19	14	14	12	24	7	10	20	23	6	14	4	12	24	15
(3)	7	4	17	4	18	11	14	14	10	8	13	6	0	19	24	14	20	10	8	3
(4) Plaintext	h	e	r	e	s	ℓ	o	o	k	i	n	g	a	t	y	o	u	k	i	d

So the original message is

'Here's looking at you, kid.' [Spoken by Humphrey Bogart to Ingrid Bergman in the Academy award winning film *Casablanca.*]

27. (a) $x_0 = 10$

$x_1 \equiv 5(x_0) + 3 \pmod{19} \equiv \quad \pmod{19} \equiv 15 \pmod{19}$, so $x_1 = 15$.
$x_2 \equiv 5(x_1) + 3 \pmod{19} \equiv 78 \pmod{19} \equiv 2 \pmod{19}$, so $x_2 = 2$.
$x_3 \equiv 5(x_2) + 3 \pmod{19} \equiv 13 \pmod{19}$, so $x_3 = 13$.
$x_4 \equiv 5(x_3) + 3 \pmod{19} \equiv 68 \pmod{19} \equiv 11 \pmod{19}$, so $x_4 = 11$.
Further computation tells us that $x_5 = 1$, $x_6 = 8$, $x_7 = 5$, $x_8 = 9$, and $x_9 = 10$, the seed.

So this linearcongruential generator produces nine distinct terms.
(b) $10, 15, 2, 13, 11, 1, 9, 5, 9, 10, 15, 2, \ldots$

28. $x_0 = 1$
$x_1 = 28$
$x_2 \equiv x_1 + x_0 \pmod{37} \equiv 28 + 1 \pmod{37} \equiv 29 \pmod{37}$, so $x_2 = 29$
$x_3 \equiv x_2 + x_1 \pmod{37} \equiv 29 + 28 \pmod{37} \equiv 57 \pmod{37}$, so $x_3 = 20$
Further computation leads to $x_4 = 12$, $x_5 = 32$, $x_6 = 7$, $x_7 = 2$, $x_8 = 9$, and $x_9 = 11$.

29. Proof: (By Mathematical Induction)
[Note that for $n \geq 1$, $(a^n - 1)/(a - 1) = a^{n-1} + a^{n-2} + \cdots + 1$, which can be computed in the ring $(\mathbf{Z}, +, \cdot)$.]

When $n - 0$, $a^0 x_0 + c[(a^0 - 1)/(a - 1)] \equiv x_0 + c[0/(a - 1)] \equiv x_0 \pmod{m}$, so the formula is true in thisfirst basis ($n = 0$) case. Assuming the result for n we have
$x_n \equiv a^n x_0 + c[(a^n - 1)/(a - 1)] \pmod{m}$, $0 \leq x_n < m$. Continuing to the next case we learn than

$$\begin{aligned} x_{n+1} &\equiv ax_n + c \pmod{m} \\ &\equiv a[a^n x_0 + c[(a^n - 1)/(a - 1)]] + c \pmod{m} \\ &\equiv a^{n+1} x_0 + ac[(a^n - 1)/(a - 1)] + c(a - 1)/(a - 1) \pmod{m} \\ &\equiv a^{n+1} x_0 + c[(a6n + 1 - a + a - 1)/(a - 1)] \pmod{m} \\ &\equiv a^{n+1} x_0 + c[(a^{n+1} - 1)/(a - 1)] \pmod{m} \end{aligned}$$

and we select x_{n+1} so that $0 \leq x_{n+1} < m$. It now follows by the Principle of Mathematical Induction that

$$x_n \equiv a^n x_0 + c[(a^n - 1)/(a - 1)] \pmod{m},\ 0 \leq x_n < m.$$

30. From the previous exercise we have

$$\begin{aligned} x_4 &\equiv a^4x_0 + c[(a^4-1)/(a-1)] \pmod{m} \\ &\equiv a^4x_0 + c(a^3+a^2+a+1) \pmod{m} \\ &\equiv 7^4x_0 + 4(7^3+7^2+7+1) \pmod{9} \\ &\equiv 7x_0 + 4)1+4+7+1) \pmod{9} \\ &\equiv 7x_0 + 4(13) \pmod{9} \\ &\equiv 7x_0 + 4(4) \pmod{9} \equiv 7x_0 + 7 \pmod{9} \end{aligned}$$

With $x_4 = 1$, it follows from $1 \equiv 7x_0 + 7 \pmod{9}$ that $3 \equiv 7x_0 \pmod{9}$. Since $7^{-1} \equiv 4 \pmod{9}$, we have $12 \equiv \pmod{9}$, so $x_0 = 3$, the seed.

31. Proof: Let $n, n+1$, and $n+2$ be three consecutive integers. Then $n^3+(n+1)^3+(n+2)^3 = n^3 + (n^3+3n^2+3n+1) + (n^3+6n^2+12n+8) = (3n^3+15n) + 9(n^2+1)$. So we consider $3n^3 + 15n = 3n(n^2+5)$. If $3|n$, then we are finished. If not, then $n \equiv 1 \pmod{3}$ or $n \equiv 2 \pmod{3}$. If $n \equiv 1 \pmod{3}$, then $n^2+5 \equiv 1+5 \equiv 0 \pmod{3}$, so $3|(n^2+5)$. If $n \equiv 2 \pmod{3}$, then $n^2+5 \equiv 9 \equiv 0 \pmod{3}$, and $3|(n^2+5)$. All cases are now covered, so we have $3|[n(n^2+5)]$. Hence $9|[3n(n^2+5)]$ and, consequently, 9 divides $(3n^3+15n) + 9(n^2+1) = n^3 + (n+1)^3 + (n+2)^3$.

32. Since $55 = 32+16+4+2+1 = (110111)2$, we have $3^{55} = 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1$.

Now, $3^1 \equiv 3 \pmod{10}$ and $3^2 \equiv 9 \pmod{10}$, so $3^2 \cdot 3^1 \equiv 7 \pmod{10}$. Further, $3^4 \equiv 81 \equiv 1 \pmod{10}$ so $3^4 \cdot 3^2 \cdot 3^1 \equiv 7 \pmod{10}$. With $3^4 \equiv 1 \pmod{10}$ it follows that $3^8 \equiv 1 \pmod{10}$, $3^{16} \equiv 1 \pmod{10}$ and $3^{32} \equiv 1 \pmod{10}$. Consequently,

$$3^{55} = 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1 \equiv 1 \cdot 1 \cdot 7 \equiv 7 \pmod{10},$$

so the last digit (that is, the units digit) in 3^{55} is 7.

33. From the presentation given in Example 14.18 it follows that for $n \in \mathbf{Z}^+$,

$$\sum_{k=0}^{n-1} p(k(n+1), n, n) = \frac{1}{n+1}\binom{2n}{n}, \text{the } n\text{th Catalan number.}$$

34.

$$\begin{aligned} (n-k+1)^2 &\equiv (-k+1)^2 \pmod{n} \\ &\equiv k^2 - 2k + 1 \pmod{n} \\ &\equiv k - 2k + 1 \pmod{n} - \text{because } k \text{ is idempotent} \\ &\equiv -k + 1 \pmod{n} \\ &\equiv n - k + 1 \pmod{n} \end{aligned}$$

Consequently, $n - k + 1$ is idempotent in $\mathbf{Z}_n$ whenever k is idempotent in $\mathbf{Z}_n$.

35. (a) $1+2+3 = 6 \equiv 1 \pmod{5}$; $0+4 = 4 \equiv 1 \pmod{3}$; $2+2+7+5 = 16 \equiv 2 \pmod{7}$. $h(123-04-2275) = 112$.

(b) Let $n = 112-43-8295$. Then $h(112-43-8295) = 413$.

36.

```
Program   Hashing (input,output);
Var
     ssnum:  array[1..9] of integer;
     i, a, b, c,  result:  integer;
Begin
     Writeln (‘Input the social security number, ’,
             ‘without hyphens, one digit at a time. ’);

     Writeln (‘Input the 1st digit and then type a return. ’);
     Read (ssnum[1]);
     Writeln (‘The 1st digit is ’, ssnum[1]:0);

     Writeln (‘Input the 2nd digit and then type a return. ’);
     Read (ssnum[2]);
     Writeln (‘The 2nd digit is ’, ssnum[2]:0);

     Writeln (‘Input the 3rd digit and then type a return. ’);
     Read (ssnum[3]);
     Writeln (‘The 3rd digit is ’, ssnum[3]:0);

     For i := 4 to 9 do
         Begin
         Writeln (‘Input the ’, i:0, ‘-th digit and then type a return. ’);
         Read (ssnum[i]);
         Writeln (‘The ’, i:0, ‘-th digit is ’, ssnum[i]:0)
         End;

     a := (ssnum[1] + ssnum[2] + ssnum[3]) Mod 5;
     b := (ssnum[4] + ssnum[5]) Mod 3;
     c := (ssnum[6] + ssnum[7] + ssnum[8] + ssnum[9]) Mod 7;
     result := 100*a + 10*b + c;

     Writeln (‘The hashing function assigns the result ’,
             result:0, ‘ to this social security number.’)
End.
```

37. (a) $h(206) = 1 \ \mathbf{mod}\ 41$, since $206 = 5(41)+1$. Likewise, $h(807) = 28 \ \mathbf{mod}\ 41$, $h(137) = 14 \ \mathbf{mod}\ 41$, $h(444) = 34 \ \mathbf{mod}\ 41$, $h(617) = 2 \ \mathbf{mod}\ 41$. Since $h(330) = 2 \ \mathbf{mod}\ 41$ but that parking space has been assigned, this patron is assigned to the next available space – here, it is 3. Likewise, the last two patrons are assigned to the spaces numbered $14 + 1 = 15$ and $3 + 1 = 4$.

(b) 1, 2, 3, 4, or 5.

38. (a) $3x \equiv 7 \pmod{31}$
Since $\gcd(3,31) = 1$, 3^{-1} exists in $\mathbf{Z}_{31}$. Using the Euclidean algorithm we have $31 = 10(3)+1$, so $1 = 31 - 10(3)$ and $3^{-1} = [3]^{-1} = [-10] = [21]$. (Note: $3 \cdot 21 = 63 = 2(31)+1$). Hence $3x \equiv 7 \pmod{31} \Rightarrow 21(3x) \equiv 21(7) \pmod{31} \Rightarrow x \equiv 147 \pmod{31} \Rightarrow x \equiv 23 \pmod{31}$.

(b) $5x \equiv 8 \pmod{37}$
With $\gcd(5,37) = 1$, we use the Euclidean algorithm to determine 5^{-1} in $\mathbf{Z}_{37}$.

$$\begin{aligned} 37 &= 7(5)+2, && 0 < 2 < 5 \\ 5 &= 2(2)+1, && 0 < 1 < 2 \end{aligned}$$

So $1 = 5 - 2(2) = 5 - 2[37 - 7(5)] = 5 - 2(37) + 14(15) = 37(-2) + 5(15)$. Consequently, $[1] = [5][15]$ in $\mathbf{Z}_{37}$ and $5^{-1} = [5]^{-1} = [15]$.

Therefore, $5x \equiv 8 \pmod{37} \Rightarrow 15(5x) \equiv 15(8) \pmod{37} \Rightarrow x \equiv 120 \pmod{137} \Rightarrow x \equiv 9 \pmod{37}$.

(c) $6x \equiv 97 \pmod{125}$
Since $6 \equiv 2 \cdot 3$ and $125 = 5^3$, it follows that $\gcd(6,125) = 1$. Using the Euclidean algorithm we learn that

$$\begin{aligned} 125 &= 20(6)+5, && 0 < 5 < 6 \\ 6 &= 1(5)+1, && 0 < 1 < 5 \end{aligned}$$

Consequently, $1 = 6 - 5 = 6 - [125 - 20(6)] = 6 - 125 + 20(6) = 21(6) + 125(-1) = 6(21) + 125(-1)$ and $[1] = [6][21]$ in $\mathbf{Z}_{125}$. So $6^{-1} = [6]^{-1} = [21]$ and $6x \equiv 97 \pmod{125} \Rightarrow x \equiv 21 \cdot 97 \pmod{125} \Rightarrow x \equiv 2037 \pmod{125} \Rightarrow x \equiv 37 \pmod{125}$.

Section 14.4

1. $s \to 0, t \to 1, v \to 2, w \to 3, x \to 4, y \to 5$

2. (Theorem 14.15 (d)) The result is true for $n = 1$. Assume the result for $n = k$ and consider $n = k+1$. Then $f(a^{k+1}) = f(a^k a) = f(a^k)f(a) = [f(a)]^k f(a) = [f(a)]^{k+1}$. Hence the result follows for all $n \in \mathbf{Z}^+$ by the Principle of Mathematical Induction.

(Theorem 14.16 (a)) For $s \in S$, there exists $r \in R$ with $f(r) = s$, since f is onto. $r = u_R r = r u_R$, so $s = f(r) = f(u_R r) = f(u_R)f(r) = f(u_r)s$ and $s = f(r) = f(r u_R) = f(r)f(u_R) = sf(u_R)$, so $f(u_R)$ is the unity of S.

(Theorem 14.16 (b)) Since a is a unit of R, there is an element $b \in R$ with $ab = ba = u_R$. Then $u_S = f(u_R)$ (by part(a)) $= f(ab) = f(a)f(b) = f(ba) = f(b)f(a)$, so $f(a)$ is a unit of S. Since $b = a^{-1}$, it follows that $f(b) = f(a^{-1})$ is a multiplicative inverse of $f(a)$. By Theorem 14.5 (b) we have $f(a^{-1}) = [f(a)]^{-1}$.

(Theorem 14.16 (c)) Let $s_1, s_2 \in S$. Then there exist $r_1, r_2 \in R$ with $f(r_i) = s_i, 1 \leq i \leq 2$. So $s_1 s_2 = f(r_1)f(r_2) = f(r_1 r_2) = f(r_2 r_1) = f(r_2)f(r_1) = s_2 s_1$, and consequently S is commutative.

3. Let $(R, +, \cdot), (S, \oplus, \odot), (T, +', \cdot')$ be the rings. For all $a, b \in R$, $(g o f)(a+b) = g(f(a+b)) = g(f(a) + f(b)) = g(f(a)) +' g(f(b)) = (g \circ f)(a) +' (g \circ f)(b)$. Also, $(g \circ f)(a \cdot b) = g(f(a \cdot b)) = g(f(a) \odot f(b)) = g(f(a)) \cdot' g(f(b)) = (g \circ f)(a) \cdot' (g \circ f)(b)$. Hence, $g \circ f$ is a ring homomorphism.

4. Define $f : \mathbf{R} \to S$ by $f(r) = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$, for each $r \in \mathbf{R}$. Then f is a one-to-one function from $\mathbf{R}$ onto S. For all $r, s \in \mathbf{R}$,

$$f(r+s) = \begin{bmatrix} r+s & 0 \\ 0 & r+s \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} + \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r) + f(s)$$

$$\text{and} \quad f(rs) = \begin{bmatrix} rs & 0 \\ 0 & rs \end{bmatrix} = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix} = f(r)f(s).$$

So f is a ring isomorphism and $\mathbf{R}$ is isomorphic to S.

5. (a) Since $f(z_R) = z_S$, it follows that $z_R \in K$ and $K \neq \emptyset$. If $x, y \in K$, then $f(x-y) = f(x + (-y)) = f(x) \oplus f(-y) = f(x) \ominus f(y) = z_S \ominus z_S = z_S$, so $x - y \in K$. Finally, if $x \in K$ and $r \in R$, then $f(rx) = f(r) \odot f(x) = f(r) \odot z_S = z_S$, and $f(xr) = f(x) \odot f(r) = z_S \odot f(r) = z_S$, so $rx, xr \in K$. Consequently, K is an ideal of R.

(b) The kernel is $\{6n | n \in \mathbf{Z}\}$.

(c) If f is one-to-one, then for each $x \in K, [f(x) = z_S = f(z_R)] \implies [x = z_R]$, so $K = \{z_R\}$. Conversely, if $K = \{z_R\}$, let $x, y \in R$ with $f(x) = f(y)$. Then $z_S = f(x) \ominus f(y) = f(x-y)$, so $x - y \in K = \{z_R\}$. Consequently, $x - y = z_R \implies x = y$, and f is one-to-one.

6. (a) $f[(12)(23) + 18] = f(13) \cdot f(23) + f(18) = (1,1,3) \cdot (1,2,3) + (0,0,3) = (1,2,4) + (0,0,3) = (1,2,2) = f(17)$, so $(13)(23) + 18 = 17$ in $\mathbf{Z}_{30}$.

(b) $f[(11)(21) - 20] = f(11) \cdot f(21) - f(20) = (1,2,1) \cdot (1,0,1) - (0,2,0) = (1,0,1) - (0,2,0) = (1,-2,1) = (1,1,1) = f(1)$, so $(11)(21) - 20 = 1$ in $\mathbf{Z}_{30}$.

(c) 24

(d) 29

7. (a)

x (in $\mathbf{Z}_{20}$)	$f(x)$ (in $\mathbf{Z}_4 \times \mathbf{Z}_5$)	x (in $\mathbf{Z}_{20}$)	$f(x)$ (in $\mathbf{Z}_4 \times \mathbf{Z}_5$)
0	(0,0)	10	(2,0)
1	(1,1)	11	(3,1)
2	(2,2)	12	(0,2)
3	(3,3)	13	(1,3)
4	(0,4)	14	(2,4)
5	(1,0)	15	(3,0)
6	(2,1)	16	(0,1)
7	(3,2)	17	(1,2)
8	(0,3)	18	(2,3)
9	(1,4)	19	(3,4)

(b) (i) $f((17)(19) + (12)(14)) = (1,2)(3,4) + (0,2)(2,4) = (3,3) + (0,3) = (3,1)$ and $f^{-1}(3,1) = 11$.

(ii) $f((18)(11) - (9)(15)) = (2,3)(3,1) - (1,4)(3,0) = (2,3) - (3,0) = (3,3)$ and $f^{-1}(3,3) = 3$.

8. $f(ma + tb) = mf(a) + tf(b) = m(1,0) + t(0,1) = (m,t)$

9. (a) 4 (b) 1 (c) No

10. (a) There are $\phi(15) = 15(2/3)(4/5) = 8$ units in both $\mathbf{Z}_{15}$ and $\mathbf{Z}_3 \times \mathbf{Z}_5$.

(b) Yes. Define $f : \mathbf{Z}_{15} \to \mathbf{Z}_3 \times \mathbf{Z}_5$ by $f(0) = (0,0)$; $f(1) = (1,1)$; $f(2) = (2,2)$; $f(3) = (0,3)$; $f(4) = (1,4)$; $f(5) = (2,0)$; $f(6) = (0,1)$; $f(7) = (1,2)$; $f(8) = (2,3)$; $f(9) = (0,4)$; $f(10) = (1,0)$; $f(11) = (2,1)$; $f(12) = (0,2)$; $f(13) = (1,3)$; $f(14) = (2,4)$. In general, $f(x) = (a,b)$, where $0 \le x \le 14$, and $x \equiv a \pmod 3$, $x \equiv b \pmod 5$, for $0 \le a \le 2$, $0 \le b \le 4$.

11. No, $\mathbf{Z}_4$ has two units, while the ring in Example 14.4 has only one unit.

12. Since $J \neq \emptyset$, $f^{-1}(J) \neq \emptyset$. If $a_1, a_2 \in f^{-1}(J)$ then $f(a_1), f(a_2) \in J$. Since J is an ideal, $f(a_1) + f(a_2) = f(a_1 + a_2) \in J$, so $a_1 + a_2 \in f^{-1}(J)$. Also, $f(a_1)f(a_2) = f(a_1a_2) \in J$, and $a_1a_2 \in f^{-1}(J)$. Finally, $a \in f^{-1}(J) \Longrightarrow f(a) \in J \Longrightarrow -f(a) \in J \Longrightarrow f(-a) \in J \Longrightarrow -a \in f^{-1}(J)$, so $f^{-1}(J)$ is a subring of R.

Now let $r \in R$ and $a \in f^{-1}(J)$. Then $f(ra) = f(r)f(a)$, where $f(r) \in S$ and $f(a) \in J$. Since J is an ideal of S, $f(ra) \in J$ and it follows that $ra \in f^{-1}(J)$. In a similar manner we find that $ar \in f^{-1}(J)$. So $f^{-1}(J)$ is an ideal of R.

13. Here $a_1 = 5$; $a_2 = 73$; $m_1 = 8$; $m_2 = 81$; $m = m_1m_2 = 8 \cdot 81 = 648$; $M_1 = m/m_1 = 81$; and $M_2 = m/m_2 = 8$.
$[x_1] = [M_1]^{-1} = [10(8) + 1]^{-1} = [1]^{-1} = [1]$ in $\mathbf{Z}_8$
$[x_2] = [M_2]^{-1} = [8]^{-1} = [-10] = [71]$ in $\mathbf{Z}_{81}$
$x - a_1M_1x_1 + a_2M_2x_2 = 5 \cdot 81 \cdot 1 + 73 \cdot 8 \cdot 71 = 41869 = 64(648) + 397$.

So the smallest positive solution is 397 and all other solutions are congruent to 397 modulo 648.
Check: $397 = 48(8) + 3 = 4(81) + 73$.

14. Here we want a simultaneous solution for the system of three congruences

$$\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15}. \end{aligned}$$

So $a_1 = 2$; $a_2 = 10$; $a_3 = 0$; $m_1 = 17$; $m_2 = 16$; $m_3 = 15$; $m = m_1 m_2 m_3 = 17 \cdot 16 \cdot 15 = 4080$; $M_1 = m/m_1 = 240$; $M_2 = m/m_2 = 255$; and $M_3 = m/m_3 = 272$.

$[x_1] = [M_1]^{-1} = [240]^{-1} = [14(17) + 2]^{-1} = [2]^{-1} = [9]$ in $\mathbf{Z}_{17}$
$[x_2] = [M_2]^{-1} = [255]^{-1} = [15(16) + 15]^{-1} = [15]^{-1} = [15]$ in $\mathbf{Z}_{16}$
$[x_3] = [M_3]^{-1} = [272]^{-1} = [18(15) + 2]^{-1} = [2]^{-1} = [8]$ in $\mathbf{Z}_{15}$
$x = 3 \cdot 9 \cdot 240 + 10 \cdot 15 \cdot 255 + 0 \cdot 8 \cdot 272 = 44730 \equiv 3930 \pmod{4080}$.

So the smallest number of (identical) gold coins that could have been in the treasure chest is 3930. Any other solution is congruent to 3930 modulo 4080.
Check: $3930 = 231(17) + 3 = 245(16) + 10 = 262(15)$.

15. Here $a_1 = 1$; $a_2 = 2$; $a_3 = 3$; $a_4 = 5$; $m_1 = 2$; $m_2 = 3$; $m_3 = 5$; $m_4 = 7$; $m = m_1 m_2 m_3 m_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$; $M_1 = m/m_1 = 105$; $M_2 = m/m_2 = 70$; $M_3 = m/m_3 = 42$ and $M_4 = m/m_4 = 30$.

$[x_1] = [M_1]^{-1} = [105]^{-1} = [52(2) + 1]^{-1} = [1]^{-1} = [1]$ in $\mathbf{Z}_2$
$[x_2] = [M_2]^{-1} = [70]^{-1} = [23(3) + 1]^{-1} = [1]^{-1} = [1]$ in $\mathbf{Z}_3$
$[x_3] = [M_3]^{-1} = [42]^{-1} = [8(5) + 2]^{-1} = [2]^{-1} = [3]$ in $\mathbf{Z}_5$
$[x_4] = [M_4]^{-1} = [30]^{-1} = [4(7) + 2]^{-1} = [2]^{-1} = [4]$ in $\mathbf{Z}_7$
$x = 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 5 \cdot 30 \cdot 4 = 1223 \equiv 173 \pmod{210}$.

So $x = 173$ is the smallest positive simultaneous solution for the four congruences. Any other solution would be congruent to 173 modulo 210.
Check: $173 = 86(2) + 1 = 57(3) + 2 = 34(5) + 3 = 24(7) + 5$.

Supplementary Exercises

1. (a) False. Let $R = \mathbf{Z}$ and $S = \mathbf{Z}^+$.
(b) False. Let $R = \mathbf{Z}$ and $S = \{2x | x \in \mathbf{Z}\}$.
(c) False. Let $R = M_2(\mathbf{Z})$ and $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbf{Z} \right\}$.
(d) True.
(e) False. $(\mathbf{Z}, +, \cdot)$ is a subring (but not a field) in $(\mathbf{Q}, +, \cdot)$.
(f) False. For each prime p, $\{a/(p^n) | a, n \in \mathbf{Z}, n \geq 0\}$ is a subring of $(\mathbf{Q}, +, \cdot)$.
(g) False. Consider the field in Table 14.6.

(h) True

2. R commutative $\iff ba = ab$ for all $a, b \in R \iff a^2 + ab + ba + b^2 = a^2 + 2ab + b^2$ for all $a, b \in R \iff (a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

3. (a) $a + a = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = (a+a) + (a+a) \Longrightarrow a + a = 2a = z$.

(b) For each $a \in R$, $a + a = z \Longrightarrow a = -a$. For $a, b \in R$, $(a+b) = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b \Longrightarrow ab + ba = z \Longrightarrow ab = -ba = ba$, so R is commutative.

4.

$$a + bi = c + di \iff a = c, b = d \iff \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix},$$

so f is a one-to-one function. It is also onto. (Why?)

Further,

$$\begin{aligned} f((a+bi)+(x+yi)) &= f((a+x)+(b+y)i) \\ &= \begin{bmatrix} a+x & b+y \\ -(b+y) & a+x \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \\ &= f(a+bi) + f(x+yi), \end{aligned}$$

and

$$\begin{aligned} f((a+bi)(x+yi)) &= f((ax-by)+(bx+ay)i) \\ &= \begin{bmatrix} ax-by & bx+ay \\ -(bx+ay) & ax-by \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \\ &= f(a+bi)f(x+yi), \end{aligned}$$

so f is a ring isomorphism.

5. Since $az = z = za$ for all $a \in R$, we have $z \in C$ and $C \neq \emptyset$. If $x, y \in C$, then $(x+y)a = xa + ya = ax + ay = a(x+y)$, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y$, and $(-x)a = -(xa) = -(ax) = a(-x)$, for all $a \in R$, so $x+y, xy$, and $-x \in C$. Consequently, C is a subring of R.

6. (a) (i) 2^4 (ii) 3^4 (iii) p^4

(b) (i) $(2^2-1)(2^2-2) = (3)(2) = 6$
(ii) $(3^2-1)(3^2-3) = (8)(6) = 48$
(iii) $(p^2-1)(p^2-p)$

7. (a) Since $a^3 = b^3$ and $a^5 = b^5$, it follows that $a^5 = (b^3)(b^2) = (a^3)(b^2)$. Consequently, $(a^3)(a^2) = (a^3)(b^2)$ with $a^3 \neq z$, so $a^2 = b^2$.

Now with $a^3 = b^3$ and $a^2 = b^2$ we have $(a^2)(a) = a^3 = b^3 = (b^2)(b) = (a^2)(b)$, and since $a^2 \neq z$ it follows that $a = b$.

(b) Since m, n are relatively prime we can write $1 = ms + nt$ where $s, t \in \mathbf{Z}$. With $m, n > 0$ it follows that one of s, t must be positive, and the other negative. Assume (without any loss of generality) that s is negative so that $1 - ms = nt > 0$.

Then $a^n = b^n \Longrightarrow (a^n)^t = (b^n)^t \Longrightarrow a^{nt} = b^{nt} \Longrightarrow a^{1-ms} = b^{1-ms} \Longrightarrow a(a^m)^{(-s)} = b(b^m)^{(-s)}$. But with $-s > 0$ and $a^m = b^m$, we have $(a^m)^{(-s)} = (b^m)^{(-s)}$. Consequently,

$$([(a^m)^{(-s)} = (b^m)^{(-s)} \neq z] \wedge [a(a^m)^{(-s)} = b(b^m)^{(-s)}]) \Longrightarrow a = b,$$

since we may use the Cancellation Law of Multiplication in an integral domain.

8. (a) $\mathbf{R}^+$ is closed under $\oplus$ and $\odot$. For all $a, b, c \in \mathbf{R}^+, a \oplus b = ab = ba = b \oplus a$; $a \oplus (b \oplus c) = a \oplus (bc) = a(bc) = (ab)c = (ab) \oplus c = (a \oplus b) \oplus c$; and $a \oplus 1 = 1 \oplus a = a$, so $\oplus$ is commutative and associative with additive identity 1. Also, for each $a \in \mathbf{R}^+$, $a^{-1} \in \mathbf{R}^+$, and a^{-1} is the (additive) inverse of a.

Now consider $\odot$. For $a, b, c \in \mathbf{R}^+$, $a \odot (b \odot c) = a \odot (b^{\log_2 c}) = a^{\log_2 (b^{\log_2 c})} = a^{(\log_2 c)(\log_2 b)}$ and $(a \odot b) \odot c = (a^{\log_2 b}) \odot c = a^{(\log_2 b)(\log_2 c)}$, so $\odot$ is associative. Also, for $a, b \in \mathbf{R}^+$, $\log_2 b \ \log_2 a = \log_2 a \ \log_2 b \Longrightarrow \log_2 [a^{\log_2 b}] = \log_2 [b^{\log_2 a}] \Longrightarrow a^{\log_2 b} = b^{\log_2 a} \Longrightarrow a \odot b = b \odot a$, so $\odot$ commutative. In addition, $a \odot 2 = a^{\log_2 2} = a^1 = a$ for all $a \in \mathbf{R}^+$ so 2 is the multiplicative identity. Finally, $a \odot (b \oplus c) = a \odot (bc) = a^{\log_2 (bc)} = a^{\log_2 b + \log_2 c} = (a^{\log_2 b})(a^{\log_2 c}) = (a \odot b) \oplus (a \odot c)$, so the distributive law holds and $(\mathbf{R}^+, \oplus, \odot)$ is a commutative ring with unity.

(b) For each $a \in \mathbf{R}^+$, $a \neq 1$, we find that $a \odot 2^{\log_2 a} = a^{\log_2 (2^{\log_2 a})} = a^{(\log_a 2)(\log_2 2)} = a^{\log_a 2} = 2$, the unity of the ring. So $(\mathbf{R}^+, \oplus, \odot)$ is a field.

9. Let $x = a_1 + b_1$, $y = a_2 + b_2$, for $a_1, a_2 \in A$, $b_1, b_2 \in B$. Then $x - y = (a_1 - a_2) + (b_1 - b_2) \in A + B$. If $r \in R$, and $a + b \in A + B$, with $a \in A$, $b \in B$, then $ra \in A$, $rb \in B$ and $r(a + b) \in A + B$. Similarly, $(a + b)r \in A + B$, and $A + B$ is an ideal of R.

10. (a) For $0 < k < p$, $\binom{p}{k} = (p!)/[k!(p-k)!] = p[(p-1)!/(k!(p-k)!)]$. $[(p-1)!/(k!(p-k)!)]$ is an integer because for any $0 < k < p$, none of $2, 3, \ldots, \max\{k, p-k\}$ divides p when p is prime.

(b) $(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$. By part (a) $\binom{p}{k} \equiv 0 \pmod{p}$ for $0 < k < p$, so $(a + b)^p \equiv a^p + b^p \pmod{p}$.

11. Consider the numbers x_1, $x_1 + x_2$, $x_1 + x_2 + x_3$, $\ldots, x_1 + x_2 + x_3 + \ldots + x_n$. If one of these numbers is congruent to 0 modulo n, the result follows. If not, there exist $1 \leq i < j \leq n$ with $(x_1 + x_2 + \ldots + x_i) \equiv (x_1 + \ldots + x_i + x_{i+1} + \ldots + x_j) \pmod{n}$. Hence n divides $(x_{i+1} + \ldots + x_j)$.

12. Since $2 = 1 + 1$ and $3 = 4 - 1$ we know that $(2, 1, 1)$ and $(3, 4, -1)$ are elements in S. However, $(2, 1, 1) \odot (3, 4 - 1) = (2 \cdot 3, 1 \cdot 4, 1 \cdot (-1)) = (6, 4 - 1)$, and $(6, 4, -1)$ is *not* in S because $6 \neq 4 + (-1)$. Consequently, S is *not* closed under multiplication so it is *not* a subring of $(\mathbf{Z}^3, \oplus, \odot)$.

[Note: The set S is nonempty and it is closed under subtraction.]

13. (a) For each $t \in \mathbf{N}$,

$$\begin{array}{llll} 7^{4t+1} \equiv 7 \pmod{10} & & 3^{4t+1} \equiv 3 \pmod{10} \\ 7^{4t+2} \equiv 9 \pmod{10} & & 3^{4t+2} \equiv 9 \pmod{10} \\ 7^{4t+3} \equiv 3 \pmod{10} & & 3^{4t+3} \equiv 7 \pmod{10} \\ 7^{4t+4} \equiv 1 \pmod{10} & & 3^{4t+4} \equiv 1 \pmod{10} \end{array}$$

So in order to get the units digit of $7^m + 3^n$ as 8 we must have (i) $m \equiv 1 \pmod 4$ and $n \equiv 0 \pmod 4$, or (ii) $m \equiv 0 \pmod 4$ and $n \equiv 3 \pmod 4$, or (iii) $m \equiv 2 \pmod 4$ and $n \equiv 2 \pmod 4$.

For case (i) there are 25 choices for m (namely, $1, 5, 9, \ldots, 93, 97$) and 25 choices for n (namely, $4, 8, 12, \ldots, 96, 100$) — a total of $25^2 = 625$ choices for the pair. There are also 625 choices for the pair in each of cases (ii) and (iii). Consequently, in total, there are 625 + 625 + 625 = 1875 ways to make the selection for m, n.
(b) For case (i) there are 32 choices for m and 31 choices for n, and $32 \times 31 = 992$ choices for the pair. There are 31 choices for each of m, n, resulting in $31^2 = 961$ possible pairs, for case (ii) and case (iii). Therefore we can select m, n in this situation in 992 + 961 + 961 = 2914 ways.
(c) There are $(100)^2 = 10,000$ ways in which one can select the pair m, n.
Here we consider three cases:
(i) $m \equiv 2 \pmod 4$ and $n \equiv 1 \pmod 4$;
(ii) $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$; and
(iii) $m \equiv 0 \pmod 4$ and $n \equiv 0 \pmod 4$.
For each case there are $(25)^2 = 625$ ways to select the pair m, n. Therefore, we have 1875 ways in total.
Consequently, the probability for the problem posed is $\frac{1875}{10,000} = 0.1875 = 3[(\frac{25}{100})(\frac{25}{100})] = 3/16$.

14. Proof:
(a) For $n = 2$ and $k = 1$ we have $1^3 = 1$, and $1^3 \equiv 1 \pmod 2$. When $n > 2$ then $k^3 - k = k(k^2 - 1) = k(k-1)(k+1) \neq 0$, where $k - 1$ and $k + 1$ are both even. Hence $n = 2k$ divides $k^3 - k$, so $k^3 \equiv k \pmod n$.
(b) When $n = 4k$ it follows that $(2k)^3 = (4k)(2k^2) = n(2k^2) \equiv 0 \pmod n$.
(c) Recall that for all real numbers x, y we have $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.
(i) If n is even with $n/2$ odd, then $\sum_{i=1}^{n-1} i^3 = 1^3 + 2^3 + \ldots + (\frac{n}{2} - 1)^3 + (\frac{n}{2})^3 + (\frac{n}{2} + 1)^3 + \ldots + (n-1)^3$.

Consider the following pairs:

$$\begin{array}{rcccl}
1^3+(n-1)^3 & = & [1+(n-1)][1^2-1(n-1)+(n-1)^2] & \equiv & 0 \pmod{n} \\
 & \vdots & & \vdots & \\
2^3+(n-2)^3 & = & [2+(n-2)][2^2-2(n-2)+(n-2)^2] & \equiv & 0 \pmod{n} \\
 & \vdots & & \vdots & \\
(\frac{n}{2}-1)^3+(\frac{n}{2}+1)^3 & = & [(\frac{n}{2}-1)+(\frac{n}{2}+1)][(\frac{n}{2}-1)^2-(\frac{n}{2}-1)(\frac{n}{2}+1)+(\frac{n}{2}+1)^2] & \equiv & 0 \pmod{n}.
\end{array}$$

Hence $\sum_{i=1}^{n-1} i^3 \equiv (\frac{n}{2})^3 \equiv (\frac{n}{2}) \pmod{n}$, for n even with $n/2$ odd — by virtue of part (a).

(ii) If n is even and divisible by 4, then by an argument similar to that in part (i) we have $\sum_{i=1}^{n-1} i^3 \equiv (\frac{n}{2})^3 \equiv 0 \pmod{n}$ — because of part (b).

(iii) Finally, consider the case where n is odd. By an argument similar to the one in part (i) we have $\sum_{i=1}^{n-1} i^3 = \sum_{i=1}^{(n-1)/2} [i^3+(n-i)^3] = \sum_{i=1}^{(n-1)/2} (i+(n-i))[i^2-i(n-i)+(n-i)^2]$, where each summand has the factor n — making it congruent to 0 modulo n. Consequently, $\sum_{i=1}^{n-1} i^3 \equiv 0 \pmod{n}$.

15. Proof: For all $n \in \mathbf{Z}$ we find that $n^2 \equiv 0 \pmod 5$ – when $5|n$ – or $n^2 \equiv 1 \pmod 5$ or $n^2 \equiv 4 \pmod 5$. Suppose that 5 does not divide any of a, b, or c. Then
(i) $a^2+b^2+c^2 \equiv 3 \pmod 5$ – when $a^2 \equiv b^2 \equiv c^2 \equiv 1 \pmod 5$;
(ii) $a^2+b^2+c^2 \equiv 1 \pmod 5$ – when each of two of a^2, b^2, c^2 is congruent to 1 modulo 5 and the other square is congruent to 4 modulo 5;
(iii) $a^2+b^2+c^2 \equiv 4 \pmod 5$ – when one of a^2, b^2, c^2 is congruent to 1 modulo 5 and each of the other two squares is congruent to 4 modulo 5; or,
(iv) $a^2+b^2+c^2 \equiv 2 \pmod 5$ – when $a^2 \equiv b^2 \equiv c^2 \equiv 4 \pmod 5$.

16.

```
Program  Reversal (input, output);
Var
          posint, rightdigit: integer;
Begin
          Writeln ('Input the positive integer whose digits are to be reversed.');
          Read (posint);
          Write ('The reversal of ', posint:0, '  is  ');
          While posint > 0 do
          Begin
                    rightdigit := posint Mod 10;
                    Write (rightdigit:0);
                    posint := posint Div 10
```

```
        End;
        Writeln
    End.
```

17. From Section 4.5 we know that $a-b$ has $(e_1+1)(e_2+1)\cdots(e_k+1)$ positive integer divisors. Consequently, there are $(e_1+1)(e_2+1)\cdots(e_k+1)-1$ possible values for n which will make $a \equiv b \pmod{n}$ true.

18. We use the Chinese Remainder Theorem to find a simultaneous solution for the system of three congruences:

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 4 \pmod{11} \\ x &\equiv 5 \pmod{15}. \end{aligned}$$

Here $a_1 = 3$; $a_2 = 4$; $a_3 = 5$; $m_1 = 8$; $m_2 = 11$; $m_3 = 15$; $m = m_1m_2m_3 = 8 \cdot 11 \cdot 15 = 1320$; $M_1 = m/m_1 = 165$; $M_2 = m/m_2 = 120$; and $M_3 = m/m_3 = 88$.

$[x_1] = [M_1]^{-1} = [165]^{-1} = [20(8)+5]^{-1} = [5]^{-1} = [5]$ in $\mathbf{Z}_8$

$[x_2] = [M_2]^{-1} = [120]^{-1} = [10(11)+10]^{-1} = [10]^{-1} = [10]$ in $\mathbf{Z}_{11}$

$[x_3] = [M_3]^{-1} = [88]^{-1} = [5(15)+13]^{-1} = [13]^{-1} = [7]$ in $\mathbf{Z}_{15}$

$x = 3 \cdot 165 \cdot 240 + 4 \cdot 120 \cdot 10 + 5 \cdot 88 \cdot 7 = 10355 = 7(1320) + 1115 \equiv 1115 \pmod{1320}.$

So $x = 1115$ is the smallest number of freshman that Jerina and Noor could be trying to organize for the pregame presentation.
Check: $1115 = 139(8) + 3 = 101(11) + 4 = 74(15) + 5$.

CHAPTER 15
BOOLEAN ALGEBRA AND SWITCHING FUNCTIONS

Section 15.1

1. (a) 1 (b) 1 (c) 1 (d) 1

2. (a) Since x has value 1, $x + xy + w$ has value 1 regardless of the values of y and w.
(b) Three assignments: (1) $y : 1,\ w : 1$; (2) $y : 0,\ w : 1$; and (3) $y : 1,\ w : 0$.
(c) Two assignments: (1) $y : 1,\ w : 1$; (2) $y : 0,\ w : 1$.
(d) Two assignments: (1) $y : 1,\ w : 1$; (2) $y : 0,\ w : 1$.

3. (a) 2^n (b) $2^{(2^n)}$

4.
a) (i) $\overline{w}\,\overline{x}yz$ (ii) $\overline{w}xy\overline{z}$
(iii) $\overline{w}xyz$ (iv) $\overline{w}\,\overline{x}\,\overline{y}\,\overline{z}$

b) (i) $w + x + \overline{y} + \overline{z}$ (ii) $w + \overline{x} + \overline{y} + z$
(iii) $w + \overline{x} + \overline{y} + \overline{z}$ (iv) $w + x + y + z$

5.

x	y	z	$\overline{x+y}$	$\overline{x}z$	$\overline{\overline{(x+y)} + (\overline{x}z)}$
0	0	0	1	0	0
0	0	1	1	1	0
0	1	0	0	0	1
0	1	1	0	1	0
1	0	0	0	0	1
1	0	1	0	0	1
1	1	0	0	0	1
1	1	1	0	0	1

(a) d.n.f. $xyz + x\overline{y}z + x\overline{y}\,\overline{z} + xy\overline{z} + \overline{x}y\overline{z}$
c.n.f. $(x + y + z)(x + y + \overline{z})(x + \overline{y} + \overline{z})$

(b) $f = \sum m(2, 4, 5, 6, 7) = \prod M(0, 1, 3)$

6. a) $g(w, x, y, z) = (wz + xyz)(x + \overline{x}\,\overline{y}z) = wxz + xyz + w\overline{x}\,\overline{y}z = wx(y + \overline{y})z +$ $(w + \overline{w})xyz + w\overline{x}\,\overline{y}z = wxyz + wx\overline{y}z + wxyz + \overline{w}xyz + w\overline{x}\,\overline{y}z$. Consequently, the d.n.f. for g is $wxyz + wx\overline{y}z + \overline{w}xyz + w\overline{x}\,\overline{y}z$, a sum of four minterms.

From the d.n.f. for g we know that the c.n.f. for g is a product of 12 maxterms. The binary labels for the above minterms are

$wxyz$:	$1111(=15)$	$wx\overline{y}z$:	$1101(=13)$
$\overline{w}xyz$:	$0111(=7)$	$w\overline{x}\,\overline{y}z$:	$1001(=9)$

Consequently we have the maxterms

$0000(=0)$	$w+x+y+z$	$0001(=1)$	$w+x+y+\overline{z}$	$0010(=2)$	$w+x+\overline{y}+z$
$0110(=3)$	$w+x+\overline{y}+\overline{z}$	$0100(=4)$	$w+\overline{x}+y+z$	$0101(=5)$	$w+\overline{x}+y+\overline{z}$
$0110(=6)$	$w+\overline{x}+\overline{y}+z$	$1000(=8)$	$\overline{w}+x+y+z$	$1010(=10)$	$\overline{w}+x+\overline{y}+z$
$1011(=11)$	$\overline{w}+x+\overline{y}+\overline{z}$	$1100(=12)$	$\overline{w}+\overline{x}+y+z$	$1110(=14)$	$\overline{w}+\overline{x}+\overline{y}+z$

and the c.n.f. for g is the product of these 12 maxterms.

b) $g = \sum m(7,9,13,15) = \prod M(0,1,2,3,4,5,6,8,10,11,12,14)$

7. (a) 2^{64} (b) 2^6 (c) 2^6

8. (a) $f(w,x,y,z) = \overline{w}x\overline{y}z + \overline{w}xy\overline{z} + w\overline{x}\,\overline{y}\,\overline{z} + w\overline{x}yz$

(b) $f(w,x,y,z) = \overline{w}\,\overline{x}yz + \overline{w}x\overline{y}z + \overline{w}xyz + w\overline{x}y\overline{z} + w\overline{x}yz + wx\overline{y}\,\overline{z} + wx\overline{y}z + wxy\overline{z} + wxyz$

9. $m + k = 2^n$

10. If $x = 0$, then $x+y+z = xyz \Longrightarrow x+y+z = 0 \Longrightarrow y = z = 0$.
If $x = 1$, then $x+y+z = xyz \Longrightarrow 1 = xyz \Longrightarrow y = z = 1$.

11. (a) $xy + (x+y)\overline{z} + y = y(x+1) + (x+y)\overline{z} = y + x\overline{z} + y\overline{z} = y(1+\overline{z}) + x\overline{z} = y + x\overline{z}$.

(b) $x + y + \overline{(\overline{x}+y+z)} = x + y + (x\overline{y}\,\overline{z}) = x(1+\overline{y}\,\overline{z}) + y = x + y$.

(c) $yz + wz + z + [wz(xy+wz)] = z(y+1) + wx + wxyz + wz = z + wx(1+yz) + wz = z + wx + wz = z(1+w) + wx = z + wx$.

12. $x+\overline{x}y = 0 \Longrightarrow x = 0 = \overline{x}y \Longrightarrow x = y = 0$; $\overline{x}y = \overline{x}z$, $x = y = 0 \Longrightarrow z = 0$; $\overline{x}y+\overline{x}\,\overline{z}+zw = \overline{z}w$, $x = y = z = 0 \Longrightarrow w = 1$.

13. (a)

(i)

f	g	h	fg	$\overline{f}h$	gh	$fg+\overline{f}h+gh$	$fg+\overline{f}h$
0	0	0	0	0	0	0	0
0	0	1	0	1	0	1	1
0	1	0	0	0	0	0	0
0	1	1	0	1	1	1	1
1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	0	1	0	0	1	1
1	1	1	1	0	1	1	1

Alternately, $fg+\overline{f}h = (fg+\overline{f})(fg+h) = (f+\overline{f})(g+\overline{f})(fg+h) = \mathbf{1}(g+\overline{f})(fg+h) = fgg+gh+\overline{f}fg+\overline{f}h = fg+gh+\mathbf{0}g+\overline{f}h = fg+gh+\overline{f}h$.

(ii) $fg+f\overline{g}+\overline{f}g+\overline{f}\overline{g} = f(g+\overline{g})+\overline{f}(g+\overline{g}) = f\cdot\mathbf{1}+\overline{f}\cdot\mathbf{1} = f+\overline{f} = \mathbf{1}$

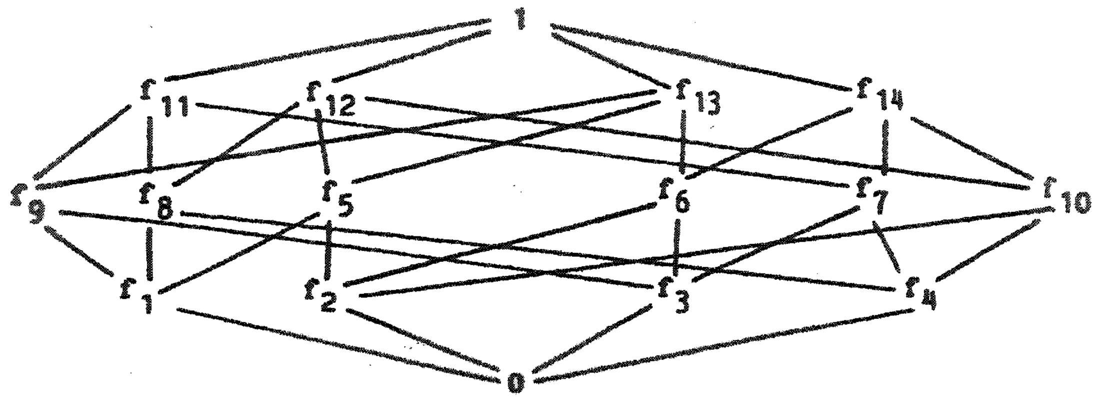
(b) (i) $(f+g)(f+h)(g+h) = (f+g)(\overline{f}+h)$

(ii) $(f+g)(f+\overline{g})(\overline{f}+g)(\overline{f}+\overline{g}) = \mathbf{0}$

14. (a) For any $f \in F_n$, f has value 1 whenever f has value 1 so the relation is reflexive. If $f, g \in F_n$ and $f \le g$ and $g \le f$, then if f has value 1 for a certain assignment of Boolean values to its n variables, g also has value 1 since $f \le g$. Likewise, when g has value 1, f does also, since $g \le f$. So f and g have the value 1 simultaneously and $f = g$, making the relation antisymmetric. Finally, if $f, g, h \in F_n$ with $f \le g$ and $g \le h$, then if f has the value 1 so does g (since $f \le g$) and so does h (since $g \le h$). Hence $f \le h$ and the relation is transitive.

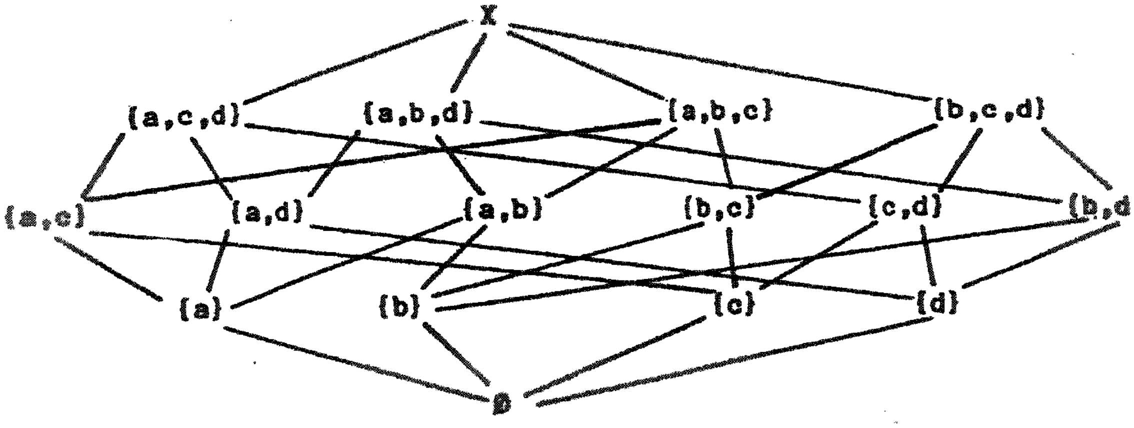
(b) fg has the value 1 iff f, g both have value 1 so $fg \le f$. When f has the value 1 so does $f+g$, so $f \le f+g$.

(c)



Minterms	Maxterms	
$f_1(x,y) = xy$	$f_{11}(x,y) = x + \overline{y}$	$f_5(x,y) = y,\ f_6(x,y) = \overline{x},$
$f_2(x,y) = \overline{x}y$	$f_{12}(x,y) = x + y$	$f_7(x,y) = \overline{y},\ f_8(x,y) = x,$
$f_3(x,y) = \overline{x}\,\overline{y}$	$f_{13}(x,y) = \overline{x} + y$	$f_9(x,y) = xy + \overline{x}\,\overline{y}$
$f_4(x,y) = x\overline{y}$	$f_{14}(x,y) = \overline{x} + \overline{y}$	$f_{10}(x,y) = \overline{x}y + x\overline{y}$

Let $X = \{a,b,c,d\}$



Ignoring the labels at the vertices, these Hasse diagrams are structurally the same.

15. (a) $f \oplus f = 0$; $f \oplus \overline{f} = 1$; $f \oplus 1 = \overline{f}$; $f \oplus 0 = f$

(b) (i) $f \oplus g = 0 \Leftrightarrow f\overline{g} + \overline{f}g = 0 \Rightarrow f\overline{g} + \overline{f}g = 0$. $[f = 1,$ and $f\overline{g} = 0] \Rightarrow g = 1$. $[f = 0$ and $\overline{f}g = 0] \Rightarrow g = 0$. Hence $f = g$.

(iii) $\overline{f} \oplus \overline{g} = \overline{f}\overline{\overline{g}} + \overline{\overline{f}}\overline{g} = \overline{f}g + f\overline{g} = f\overline{g} + \overline{f}g = f \oplus g$

(iv) This is the only result that is not true. When f has value 1, g has value 0 and h value 1 (or g has value 1 and h value 0), then $f \oplus gh$ has value 1 but $(f \oplus g)(f \oplus h)$ has value 0.

(v) $fg \oplus fh = \overline{fg}fh + fg\overline{fh} = (\overline{f} + \overline{g})fh + fg(\overline{f} + \overline{h}) = \overline{f}fh + f\overline{g}h + f\overline{f}g + fg\overline{h} =$

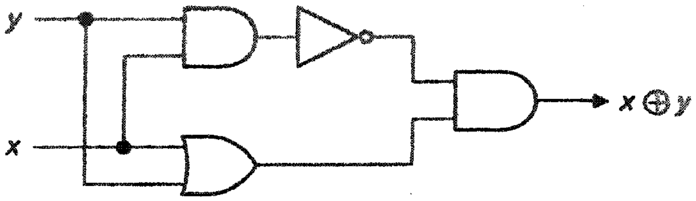
$f\bar{g}h + fg\bar{h} = f(\bar{g}h + g\bar{h}) = f(g \oplus h)$.

(vi) $\bar{f} \oplus g = \bar{f}\bar{g} + fg = fg + \bar{f}\bar{g} = f \oplus \bar{g}$.
$\overline{f \oplus g} = \overline{f\bar{g} + \bar{f}g} = (\bar{f} + g)(f + \bar{g}) = \bar{f}\bar{g} + fg = \bar{f} \oplus g$.

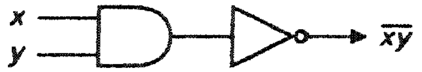
(vii) $[f \oplus g = f \oplus h] \Rightarrow [f \oplus (f \oplus g) = f \oplus (f \oplus h)] \Rightarrow [(f \oplus f) \oplus g = (f \oplus f) \oplus h] \Rightarrow [\mathbf{0} \oplus g = \mathbf{0} \oplus h] \Rightarrow [g = h]$.

Section 15.2

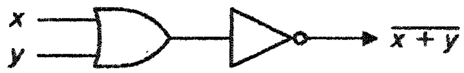
1. (a) $x \oplus y = (x + y)(\overline{xy})$



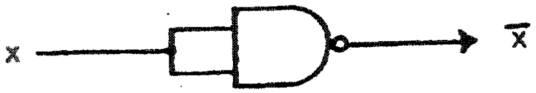
(b) $\overline{xy}$



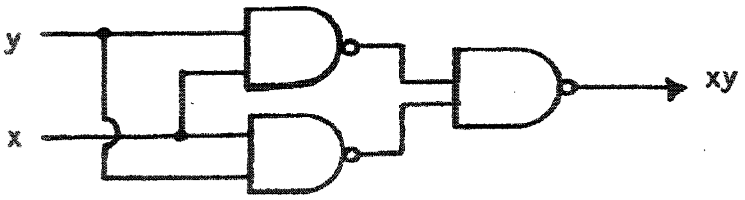
(c) $\overline{x + y}$



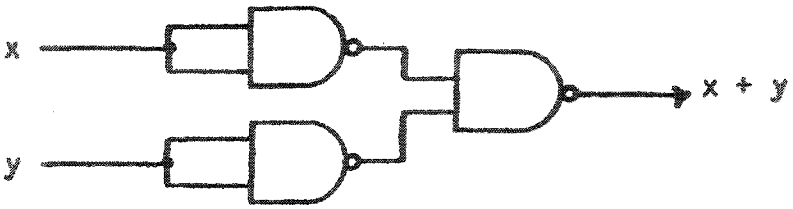
2. (a)



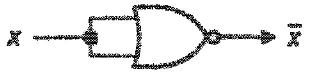
(b)



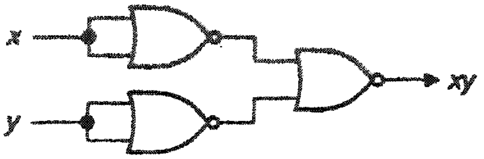
(c)



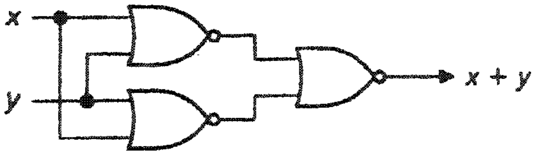
3. (a)



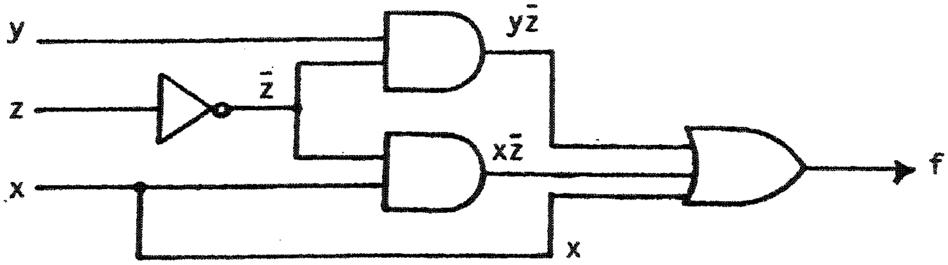
(b)



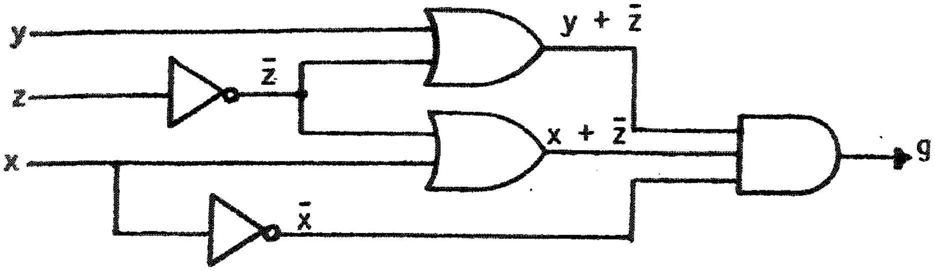
(c)



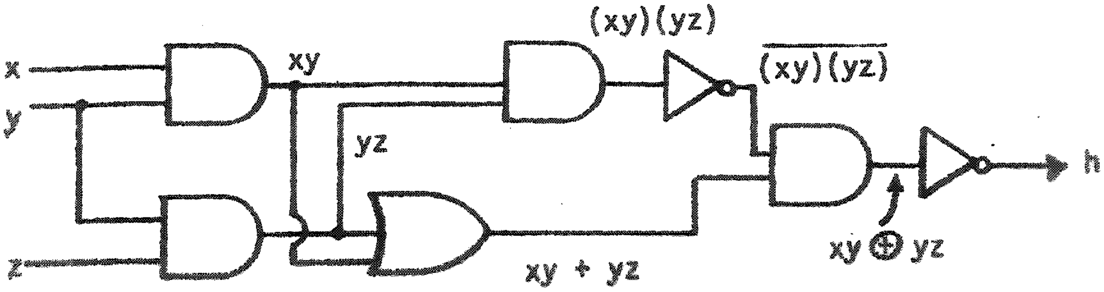
4. (a)



(b)

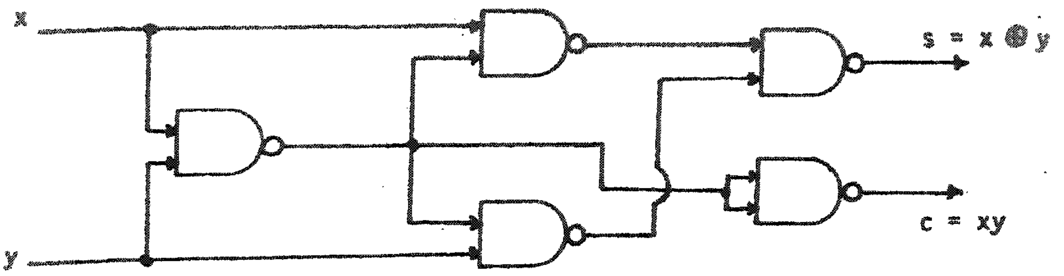


(c)

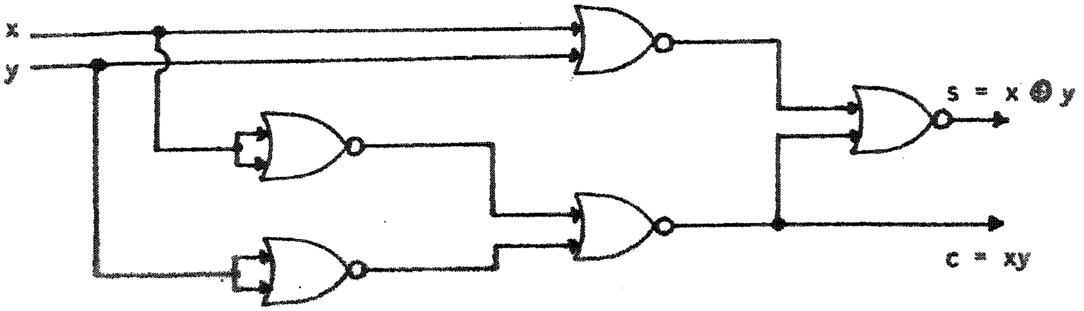


5. $f(w, x, y, z) = \overline{w}\ \overline{x}y\overline{z} + (w + x + \overline{y})z$

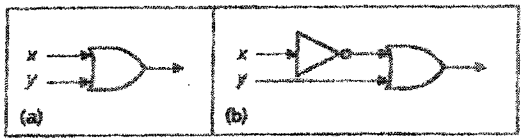
6. (a)



(b)

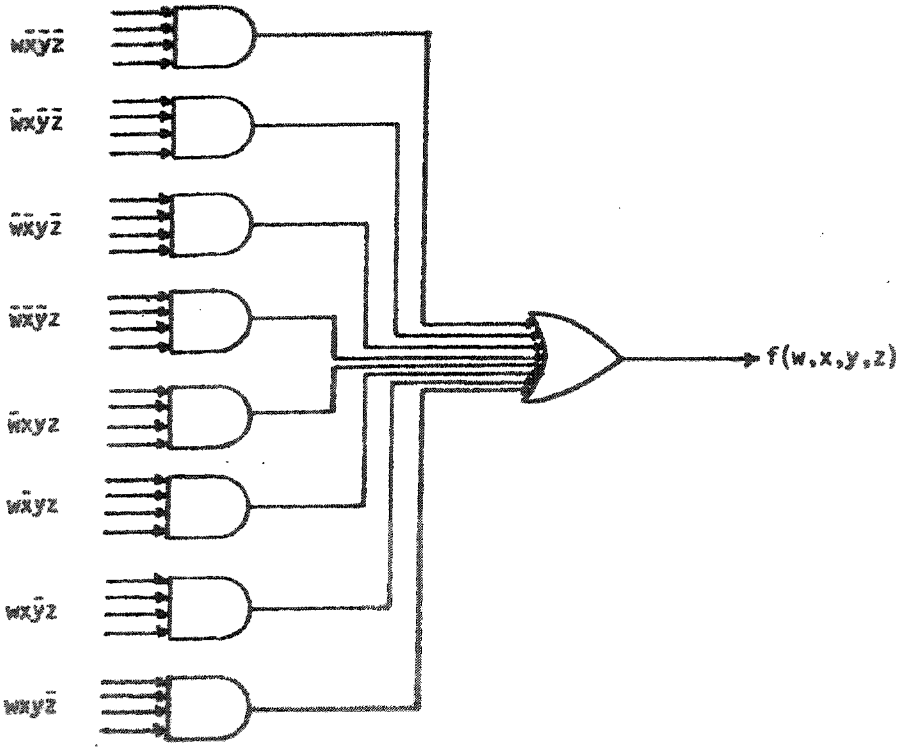


7. a) The output is $(x+\overline{y})(x+y)+y$. This simplifies to $x+(\overline{y}y)+y=x+0+y=x+y$ and provides us with the simpler equivalent network in part (a) of the figure.

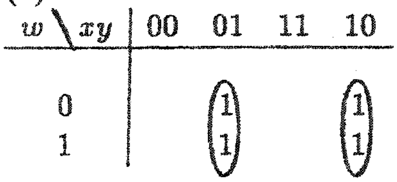


b) Here the output is $\overline{(x+\overline{y})}+(\overline{x}\,\overline{y}+y)$ which simplifies to $\overline{x}\,\overline{\overline{y}}+\overline{x}\,\overline{y}+y=\overline{x}y+\overline{x}\,\overline{y}+y=\overline{x}(y+\overline{y})+y=\overline{x}(1)+y=\overline{x}+y$. This accounts for the simpler equivalent network in part (b) of the figure.

8. (b)


$w\overline{x}\overline{y}\overline{z}$
$\overline{w}x\overline{y}\overline{z}$
$\overline{w}\overline{x}y\overline{z}$
$\overline{w}\overline{x}\overline{y}z$
$\overline{w}xyz$
$w\overline{x}yz$
$wx\overline{y}z$
$wxy\overline{z}$
f(w,x,y,z)

9. (a)

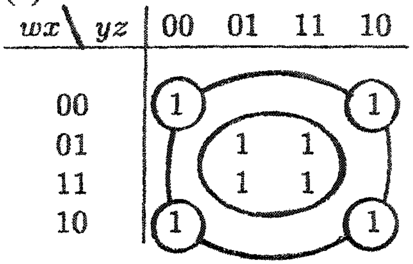


$w \backslash xy$	00	01	11	10
0		1		1
1		1		1

$f(w,x,y) = \overline{x}y + x\overline{y}$

(b) $f(w,x,y) = x$

(c)

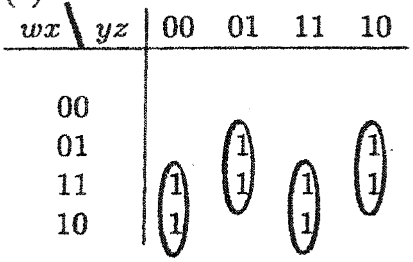


$wx \backslash yz$	00	01	11	10
00	1			1
01		1	1	
11		1	1	
10	1			1

$f(w,x,y,z) = xz + \overline{x}\,\overline{z}$

(d) $f(w,x,y,z) = xz + \overline{x}\,\overline{z} + w\overline{y}z$ or $xz + \overline{x}\,\overline{z} + w\overline{x}\,\overline{y}$

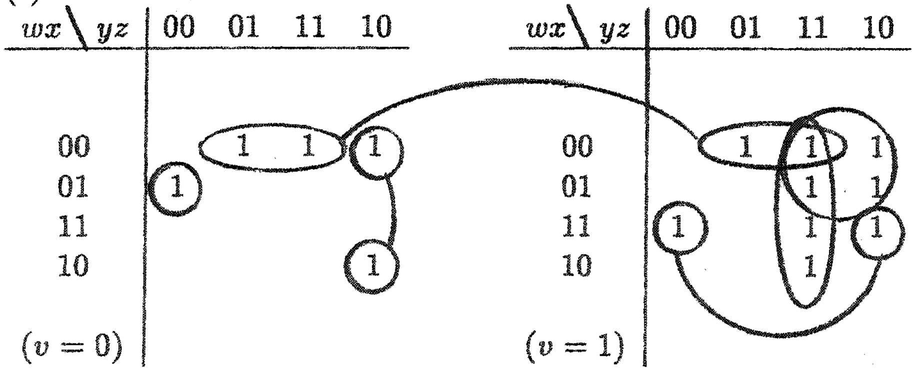
(e)



$wx \backslash yz$	00	01	11	10
00				
01		1		1
11	1	1	1	1
10	1		1	

$f(w,x,y,z) = w\overline{y}\,\overline{z} + x\overline{y}z + wyz + xy\overline{z}$

(f)



$wx \backslash yz$	00	01	11	10
00		1	1	1
01	1			
11				
10				1

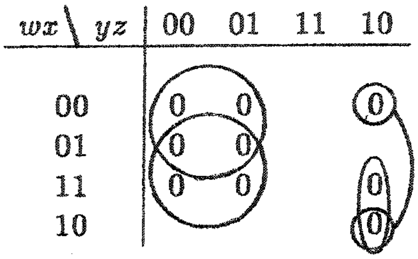
$(v = 0)$

$wx \backslash yz$	00	01	11	10
00		1	1	1
01			1	1
11	1		1	1
10			1	

$(v = 1)$

$f(v,w,x,y,z) = \overline{v}\,\overline{w}x\overline{y}\,\overline{z} + vwx\overline{z} + \overline{v}\,\overline{x}y\overline{z} + \overline{w}\,\overline{x}z + v\overline{w}y + vyz$

10.



$wx \backslash yz$	00	01	11	10
00	0	0		0
01	0	0		
11	0	0		0
10				0

$f(w,x,y,z) = (w+y)(\overline{x}+y)(\overline{w}+\overline{y}+z)(x+\overline{y}+z)$

11. (a) 2 (b) 3 (c) 4 (d) $k+1$

12. (a) 64 (b) 32 (c) 16 (d) 8

13.

(a) $|f^{-1}(0)| = |f^{-1}(1)| = 8$ (b) $|f^{-1}(0)| = 12, \quad |f^{-1}(1)| = 4$
(c) $|f^{-1}(0)| = 14, \quad |f^{-1}(1)| = 2$ (d) $|f^{-1}(0)| = 4, \quad |f^{-1}(1)| = 12$
(e) $|f^{-1}(0)| = 6, \quad |f^{-1}(1)| = 10$ (f) $|f^{-1}(0)| = 7, \quad |f^{-1}(1)| = 9$

Section 15.3

1. $f(u,v,w,x,y,z) = (v+w+x+y)(u+w)(v+z)(u+y+z) =$
$(uv+uw+ux+uy+vw+w+wx+wy)(v+z)(u+y+z) =$
$(uv+ux+uy+(u+v+1+x+y)w)(v+z)(u+y+z) =$
$(uv+ux+uy+w)(uv+vy+vz+uz+yz+z) =$
$(uv+ux+uy+w)(uv+vy+z) =$
$(uv+uvx+uvy+uvw+uvy+uvxy+uvy+wvy+uvz+uxz+uyz+wz) =$
$uv+wvy+uxz+uyz+wz$

2. Due to the size of this table we show only two of the simplifications.

$cd \backslash ef$	00	01	11	10
00	0	0	0	0
01	0	1	1	1
11	0	1	1	1
10	0	1	1	0

$(a=0, b=0)$

$cd \backslash ef$	00	01	11	10
00	0	1	1	1
01	0	1	1	1
11	0	1	1	1
10	0	1	1	1

$(a=0, b=1)$

$cd \backslash ef$	00	01	11	10
00	0	0	0	0
01	1	1	1	1
11	1	1	1	1
10	0	1	1	1

$(a=1, b=0)$

$cd \backslash ef$	00	01	11	10
00	0	1	1	1
01	1	1	1	1
11	1	1	1	1
10	0	1	1	1

$(a=1, b=1)$

$g(a,b,c,d,e,f) = bf + be + ad + df + de + cf + ace$

3. (a)

$wx \backslash yz$	00	01	11	10
00		1	1	
01		1	1	
11	✓	✓	✓	✓
10		1	✓	✓

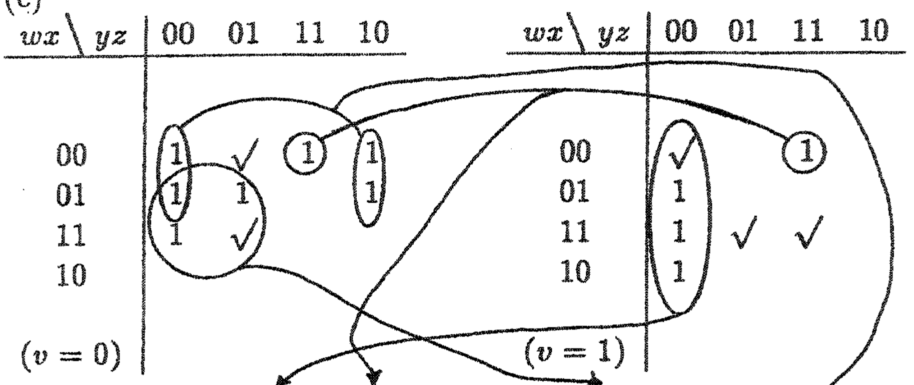
$f(w,x,y,z) = z$

(b)

$wx \backslash yz$	00	01	11	10
00	1			
01	✓	1		1
11		1		1
10	1	✓	✓	

$f(w,x,y,z) = \bar{x}\,\bar{y}\,\bar{z} + x\bar{y}z + xy\bar{z}$

(c)



$wx\backslash yz$	00	01	11	10
00	1	✓	1	1
01	1	1		1
11	1	✓		
10				

$(v=0)$

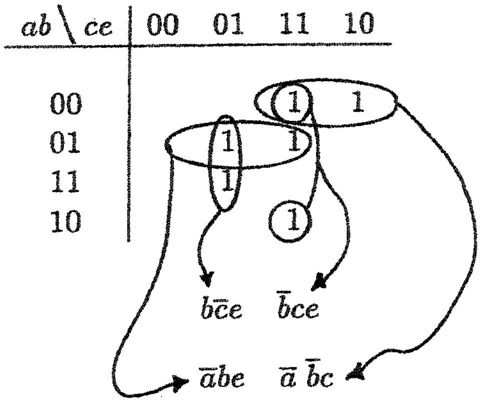
$wx\backslash yz$	00	01	11	10
00	✓		1	
01	1			
11	1	✓	✓	
10	1			

$(v=1)$

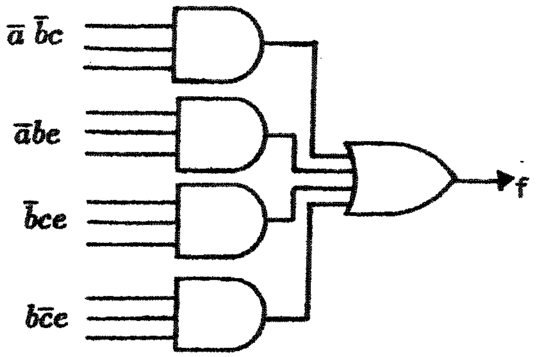
$f(v,w,x,y,z) = v\bar{y}\,\bar{z} + \bar{w}\,\bar{x}yz + \bar{v}\,\bar{w}\,\bar{z} + \bar{v}x\bar{y}$

4. (a) $f(a,b,c,e) = \bar{a}\bar{b}c\bar{e}\ (2) + \bar{a}\bar{b}ce\ (3) + \bar{a}b\bar{c}e\ (5) + \bar{a}bce\ (7) + a\bar{b}ce\ (11) + ab\bar{c}e\ (13)$

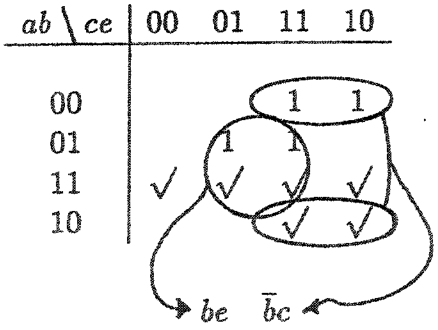
(b) $f = \sum m(2,3,5,7,11,13)$



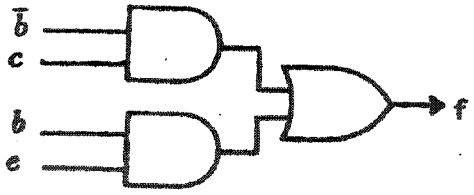
$ab\backslash ce$	00	01	11	10
00			1	1
01		1	1	
11		1		
10			1	



(c) $f = \sum m(2,3,5,7) + d(10,11,12,13,14,15)$



$ab\backslash ce$	00	01	11	10
00			1	1
01		1	1	
11	✓	✓	✓	✓
10			✓	✓



5. (a) $(a+b+c+d+e)(a+b+c+f)(a+b+c+d+f)(a+c+d+e+g)\cdot$
$(a+d+e+g)(b+c+f+g)(d+e+f+g) = (a+b+c+d+e)\cdot$
$(a+b+c+f)(a+d+e+g)(b+c+f+g)(d+e+f+g) =$
$(a+b+c+df+ef)(a+d+e+g)(b+c+f+g)(d+e+f+g) =$
$(a+b+c+df+ef)(d+e+g+af)(b+c+f+g) = [(b+c)+(a+df+ef)(f+g)](d+e+g+af) =$
$[b+c+af+df+ag+dfg+efg](d+e+g+af) = [b+c+af+df+ef+ag](d+e+g+af) =$

$bd+cd+adf+df+def+adg+be+ce+aef+def+ef+aeg+bg+cg+afg+dfg+efg+ag+abf + acf + af + adf + aef + afg = bd + cd + df + ag + ef + be + ce + af + bg + cg.$

Section 15.4

1. (The second Distributive Law). Let $x = 2^{k_1}3^{k_2}5^{k_3}$, $y = 2^{m_1}3^{m_2}5^{m_3}$, $z = 2^{n_1}3^{n_2}5^{n_3}$ where for $1 \le i \le 3$, $0 \le k_i, m_i, n_i \le 1$.
$\gcd(y,z) = 2^{s_1}3^{s_2}5^{s_3}$ where $s_i = \min\{m_i, n_i\}, 1 \le i \le 3$. $\operatorname{lcm}(x, \gcd(y,z)) = 2^{t_1}3^{t_2}5^{t_3}$ where $t_i = \max\{k_i, s_i\}$, $1 \le i \le 3$. Also, $\operatorname{lcm}(x,y) = 2^{u_1}3^{u_2}5^{u_3}$, $\operatorname{lcm}(x,z) = 2^{v_1}3^{v_2}5^{v_3}$ where $u_i = \max\{k_i, m_i\}$, $v_i = \max\{k_i, n_i\}$, $1 \le i \le 3$, and $\gcd(\operatorname{lcm}(x,y), \operatorname{lcm}(x,z)) = 2^{w_1}3^{w_2}5^{w_3}$ where $w_i = \min\{u_i, v_i\}$, $1 \le i \le 3$. To prove that $\operatorname{lcm}(x, \gcd(y,z)) = \gcd(\operatorname{lcm}(x,y), \operatorname{lcm}(x,z))$ we need to show that $t_i = w_i$, $1 \le i \le 3$. If $k_i = 0$, then $t_i = s_i$, $u_i = m_i$, $v_i = n_i$ and $w_i = \min\{u_i, v_i\} = \min\{m_i, n_i\} = s_i = t_i$. If $k_i = 1$, then $t_i = 1 = u_i = v_i = w_i$.

(The Identity Laws) $x + 0 =$ the lcm of x and 1 (the zero element) $= x$; $x \cdot 1 =$ the gcd of x and 30 (the one element) $= x$, since x is a divisor of 30.

(The Inverse Laws) $x + \overline{x} =$ the lcm of x and $30/x = 30$ (the one element of this Boolean algebra); $x\overline{x} =$ the gcd of x and $30/x = 1$ (the zero element of the Boolean algebra).

2. (b)$'$

$$\begin{aligned} x + xy &= x \cdot 1 + xy && \text{Def. 15.5 (c)}' \\ &= x(1 + y) && \text{Def. 15.5 (b)} \\ &= x \cdot 1 && \text{Th. 15.3 (a)}' \\ &= x && \text{Def. 15.5 (c)}' \end{aligned}$$

(b) Follows by duality.
(h) $\overline{0} = \overline{x\overline{x}} = \overline{x} + x = 1$
(h)$'$ Follows by duality.
(i) $x\overline{y} = 0 \Longrightarrow x = x \cdot 1 = x(y + \overline{y}) = xy + x\overline{y} = xy + 0 = xy$
$xy = x \Longrightarrow 0 = x\overline{x} = x(\overline{xy}) = x(\overline{x} + \overline{y}) = x\overline{x} + x\overline{y} = 0 + x\overline{y} = x\overline{y}$
(i)$'$ Follows by duality.

3. (a) 30 (b) 30 (c) 1 (d) 21 (e) 30 (f) 70

4. (a) $x + y = xy + y = y(x + 1) = y \cdot 1 = y$
(b) $x \le y \Longrightarrow x + y = y \Longrightarrow \overline{x + y} = \overline{y} \Longrightarrow \overline{x}\,\overline{y} = \overline{y} \Longrightarrow \overline{y} \le \overline{x}$.

5. (a) $w \le 0 \Rightarrow w \cdot 0 = w$. But $w \cdot 0 = 0$, by part (a) of Theorem 15.3.
(b) $1 \le x \Rightarrow 1 \cdot x = 1$, and $1 \cdot x = x$ from our defintion of a Boolean algebra.
(c) $y \le z \Rightarrow yz = y$, and $y \le \overline{z} \Rightarrow y\overline{z} = y$. Therefore $y = yz = (y\overline{z})z = y(\overline{z}z) = y \cdot 0 = 0$.

6. Proof:
(a) $w \leq x \Rightarrow wx = w$, and $y \leq z \Rightarrow yz = y$. Consequently, $(wx)(yz) = wy$, and we find that $wy = (wx)(yz) = (wy)(xz) \Rightarrow wy \leq xz$.
(b) As in part (a), $w \leq x \Rightarrow wx = w$, and $y \leq z \Rightarrow yz = y$. Therefore, $(w + y)(x + z) = wx + wz + yx + yz = (w + wz) + (y + yx) = w + y$, by the Absorption Law (Theorem 15.3 (b)$'$). But $(w + y)(x + z) = w + y \Rightarrow w + y \leq x + z$.

7. $x \leq y \Longleftrightarrow xy = x$. The dual of $xy = x$ is $x + y = x$.

$x + y = x \Longrightarrow xy = (x + y)y = xy + y = y(x + 1) = y \cdot 1 = y$, and $xy = y \Longleftrightarrow y \leq x$. Consequently, the dual of $x \leq y$ is $y \leq x$.

8. 2^n

9. From Theorem 15.5(a), with x_1, x_2 distinct atoms, if $x_1, x_2 \neq 0$, then $x_1 = x_1x_2 = x_2x_1 = x_2$, a contradiction.

10. If 0 and $0'$ are both zero elements of B then $0 = 0 + 0' = 0'$. In a similar way, if 1 and $1'$ are both one elements of B then $1 = 1 \cdot 1' = 1'$.

11. (d) Since x is an atom of $B_1, x \neq 0$ so $f(x) \neq 0$. Let $y \in B_2$ with $0 \neq y$ and $y \leq f(x)$. With f an isomorphism there exists $z \in B_1$ with $f(z) = y$. Also, $f^{-1} : B_2 \longrightarrow B_1$ is an isomorphism so $f(z) \leq f(x) \Longrightarrow z \leq x$. With x an atom and $0 < z \leq x$ we have $z = x$ so $f(z) = y = f(x)$, and $f(x)$ is an atom.

12. (a) $f(35) = f(5 + 7) = f(5) \cup f(7) = \{c\} \cup \{d\} = \{c, d\}$
$f(110) = f(2 + 5 + 11) = \{a, c, e\}$
$f(210) = f(2 + 3 + 5 + 7) = \{a, b, c, d\}$
$f(330) = f(2 + 3 + 5 + 11) = \{a, b, c, e\}$

(b) 5! (Since any isomorphism of finite Boolean algebras must correspond atoms.)

13. (a) $f(xy) = f(\overline{\overline{x} + \overline{y}}) = \overline{f(\overline{x} + \overline{y})} = \overline{f(\overline{x}) + f(\overline{y})} = \overline{f(\overline{x})} \cdot \overline{f(\overline{y})} = f(\overline{\overline{x}}) \cdot f(\overline{\overline{y}}) = f(x) \cdot f(y)$.
(b) Let B_1, B_2 be Boolean algebras with $f : B_1 \longrightarrow B_2$ one-to-one and onto. Then f is an isomorphism if $f(\overline{x}) = \overline{f(x)}$ and $f(xy) = f(x)f(y)$ for all $x, y \in B_1$. [Follows from part (a) by duality.]

14. Let $S \subseteq \mathcal{U}$. If $S = \emptyset$, then $f(0) = S$. If $S \neq \emptyset$, then let $x = \sum_{i=1}^{n} c_i x_i$ where $c_i = 1$ if $i \in S$ and $c_i = 0$ if $i \notin S$. Then $f(x) = S$. Hence f is onto.
Since $|B| = |\mathcal{P}(\mathcal{U})| = 2^n$, it follows from Theorem 5.11 that f is also one-to-one.

15. For each $1 \leq i \leq n$, $(x_1 + x_2 + \ldots + x_n)x_i = x_1x_i + x_2x_i + \ldots + x_{i-1}x_i + x_ix_i + x_{i+1}x_i + \ldots + x_nx_i = 0 + 0 + \ldots + 0 + x_i + 0 + \ldots + 0 = x_i$, by part (b) of Theorem 15.5. Consequently, it follows from Theorem 15.7 that $(x_1 + x_2 + \ldots + x_n)x = x$ for all $x \in B$. Since the one element is unique (from Exercise 10) we conclude that $1 = x_1 + x_2 + \ldots + x_n$.

Supplementary Exercises

1. (a) When $n = 2$, $x_1 + x_2$ denotes the Boolean sum of x_1 and x_2. For $n \geq 2$, we define $x_1 + x_2 + \ldots + x_n + x_{n+1}$ recursively by $(x_1 + x_2 + \ldots + x_n) + x_{n+1}$. [A similar definition can be given for the Boolean product.]
For $n = 2$, $\overline{x_1 + x_2} = \overline{x}_1\overline{x}_2$ is true, for this is one of the DeMorgan Laws. Assume the result for $n = k\ (\geq 2)$ and consider the case of $n = k + 1$. $\overline{(x_1 + x_2 + \ldots + x_k + x_{k+1})} = \overline{(x_1 + x_2 + \ldots + x_k) + x_{k+1}} = \overline{(x_1 + x_2 + \ldots + x_k)} \cdot \overline{x_{k+1}} = \overline{x}_1\overline{x}_2 \cdots \overline{x}_k\overline{x_{k+1}}$. Consequently, the result follows for all $n \geq 2$ by the Principle of Mathematical Induction.
(b) Follows from part (a) by duality.

2. $y = 4$, $z = 7$; $x = 16$ or 25

3. Let v, w, x, y, z indicate that Eileeen invites Margaret, Joan, Kathleen, Nettie, and Cathy, respectively. The conditons in (a) – (e) can then be expressed as

(a) $(v \rightarrow w) \Longleftrightarrow (\overline{v} + w)$ (b) $(x \rightarrow vy) \Longleftrightarrow (\overline{x} + vy)$

(c) $\overline{w}z + w\overline{z}$ (d) $yz + \overline{y}\,\overline{z}$ (e) $x + y + xy \Longleftrightarrow x + y$

$$(\overline{v} + w)(\overline{x} + vy)(\overline{w}z + w\overline{z})(yz + \overline{y}\,\overline{z})(x + y) \Longleftrightarrow (\overline{v} + w)(\overline{x}y + vy)(\overline{w}z + w\overline{z})(yz + \overline{y}\,\overline{z})$$
$$\Longleftrightarrow (\overline{v} + w)(\overline{x}y + vy)(\overline{w}yz + w\overline{y}\,\overline{z}) \Longleftrightarrow (\overline{v} + w)(\overline{w}\,\overline{x}yz + \overline{w}vyz) \Longleftrightarrow \overline{v}\,\overline{w}\,\overline{x}yz$$

Consequently, the only way Eileen can have her party and satisfy conditions (a) – (e) is to invite only Nettie and Cathy out of this group of five of her friends.

4. $h = \sum m(2, 4, 6, 8) + d(0, 10, 12, 14)$

5. Proof: If $x \leq z$ and $y \leq z$ then from Exercise 6(b) of Section 15.4 we have $x + y \leq z + z$. And by the idempotent law we have $z + z = z$.
Conversely, suppose that $x + y \leq z$. We find that $x \leq x + y$, because $x(x + y) = x + xy$ (by the idempotent law) $= x$ (by the absorption law). Since $x \leq x + y$ and $x + y \leq z$ we have $x \leq z$, because a partial order is transitive. [The proof that $y \leq z$ follows in a similar way.]

6. Statement: Let $\mathcal{B}$ be a Boolean algebra partially ordered by $\leq$. If $x, y, z \in \mathcal{B}$, then $xy \geq z$ if and only if $x \geq z$ and $y \geq z$.
Proof: If $x \geq z$ and $y \geq z$, then from Exercise 6(a) of Section 15.4 we have $xy \geq zz$. The result now follows from the idempotent law because $zz = z$.
Conversely, suppose that $xy \geq z$. We claim that $x \geq xy$. This follows because $(xy)x = x(yx) = x(xy) = (xx)y = xy$. Since $\leq$ is transitive, $x \geq xy$ and $xy \geq z \Rightarrow x \geq z$. [The proof that $y \geq z$ follows in a similar manner.]

7. Proof:
(a) $x \leq y \Rightarrow x + \overline{x} \leq y + \overline{x} \Rightarrow 1 \leq y + \overline{x} \Rightarrow y + \overline{x} = \overline{x} + y = 1$. Conversely, $\overline{x} + y = 1 \Rightarrow x(\overline{x} + y) = x \cdot 1 \Rightarrow x\overline{x}(= 0) + xy = x \Rightarrow xy = x \Rightarrow x \leq y$.
(b) $x \leq \overline{y} \Rightarrow x\overline{y} = x \Rightarrow xy = (x\overline{y})y = x(\overline{y}y) = x \cdot 0 = 0$. Conversely, $xy = 0 \Rightarrow x = x \cdot 1 =$

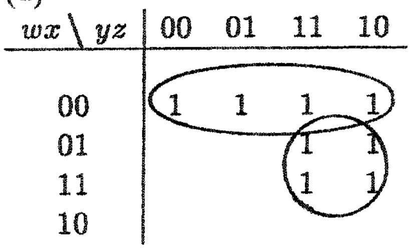
$x(y+\overline{y}) = xy + x\overline{y} = x\overline{y}$, and $x = x\overline{y} \Rightarrow x \leq \overline{y}$.

8. Proof: If $x = y$ then $x\overline{y} + \overline{x}y = x\overline{x} + \overline{x}x = 0 + 0 = 0$.

Conversely, suppose that $x\overline{y} + \overline{x}y = 0$. Then

$$\begin{aligned}
x = x + 0 &= x + (x\overline{y} + \overline{x}y) \\
&= (x + x\overline{y}) + \overline{x}y, \text{ by the Associative Law of } + \\
&= x + x\overline{y}, \text{ by the Absorption Law (Theorem 15.3 (b)')} \\
&= (x + \overline{x})(x + y), \text{ by the Distributive Law of } + \text{ over } \cdot \\
&= 1(x + y) \\
&= x + y \\
&= (x + y)1 \\
&= (x + y)(\overline{y} + y) \\
&= x\overline{y} + y, \text{ by the Distributive Law of } + \text{ over } \cdot \\
&\quad \text{(and the Commutative Law of } +) \\
&= x\overline{y} + (\overline{x}y + y), \text{ by the Absorption Law (Theorem 15.3 (b)')} \\
&= (x\overline{y} + \overline{x}y) + y, \text{ by the Associative Law of } + \\
&= 0 + y = y.
\end{aligned}$$

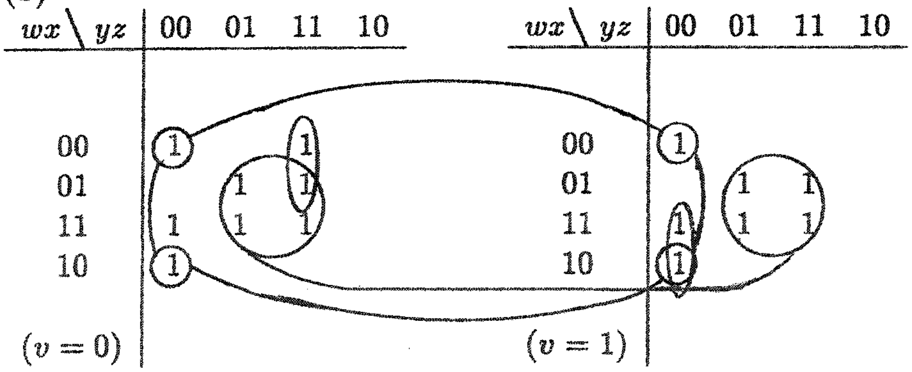
9. (a)



$wx \backslash yz$	00	01	11	10
00	1	1	1	1
01			1	1
11			1	1
10				

$f(w,x,y,z) = \overline{w}\,\overline{x} + xy$

(b)



$wx \backslash yz$	00	01	11	10
00	1		1	
01		1	1	
11	1	1	1	
10	1			
$(v=0)$				

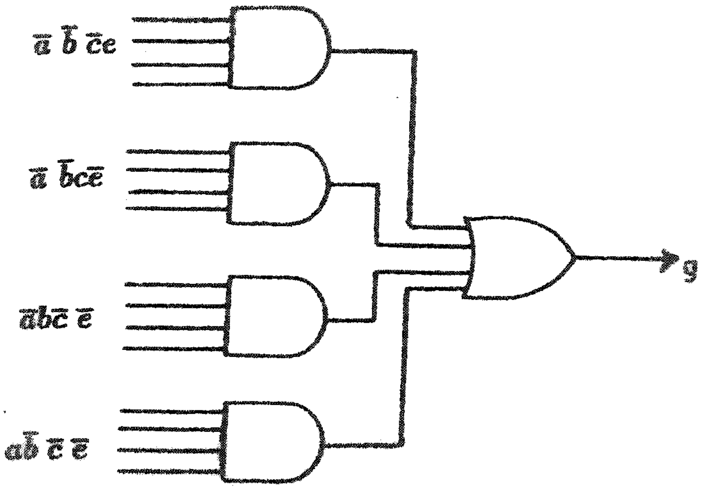
$wx \backslash yz$	00	01	11	10
00	1			
01		1	1	
11	1	1	1	
10	1			
$(v=1)$				

$g(v,w,x,y,z) = \overline{v}\,\overline{w}yz + xz + w\overline{y}\,\overline{z} + \overline{x}\,\overline{y}\,\overline{z}$

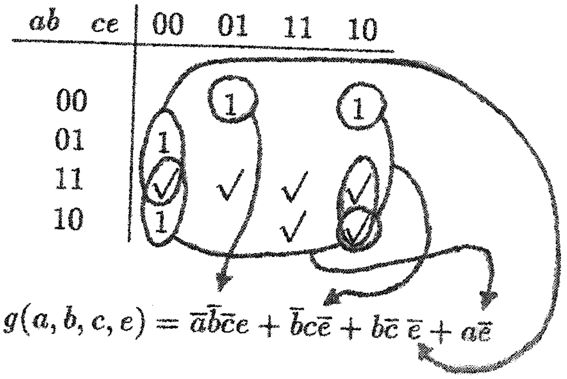
10.

(a) $g(a,b,c,e) = \overline{a}\overline{b}\overline{c}e\ (1) + \overline{a}\overline{b}c\overline{e}\ (2) + \overline{a}b\overline{c}\,\overline{e}\ (4) + a\overline{b}\overline{c}\,\overline{e}\ (8)$

(b)

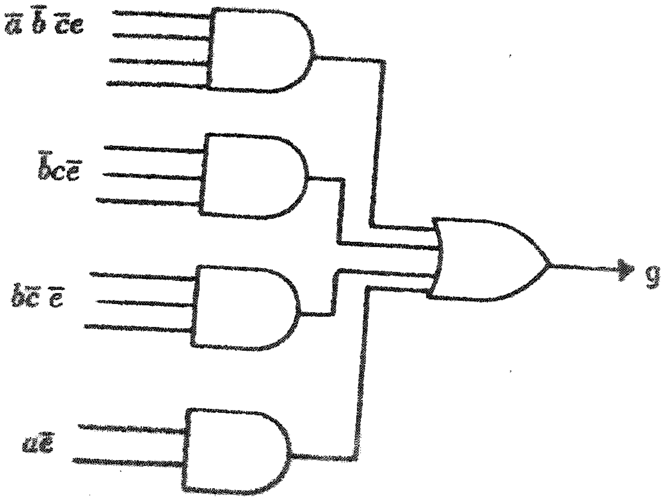


(c) $g(a,b,c,e) = \sum m(1,2,4,8) + d(10,11,12,13,14,15)$



ab \ ce	00	01	11	10
00		1		1
01	1			
11	✓	✓	✓	✓
10	1		✓	✓

$g(a,b,c,e) = \bar a\bar b\bar c e + \bar b c\bar e + b\bar c\,\bar e + a\bar e$



11. (a) $2^{(2^{n-1})}$ (b) 2^4; 2^{n+1}

12. 4!

13. (a) $60 = 2^2 \cdot 3 \cdot 5$ so there are 12 divisors of 60. Since 12 is not a power of 2 these divisors cannot yield a Boolean algebra.
(b) $120 = 2^3 \cdot 3 \cdot 5$ and there are 16 divisors of 60. Let $x = 4$. Then $\overline{x} = 120/4 = 30$ and $x \cdot \overline{x} =$ gcd of x and $\overline{x} = \gcd(4, 30) = 2$, not 1. Hence although $16 = 2^4$ the divisors of 120 do not yield a Boolean algebra.

14. If $c \leq a$, then $ac = c$, so $ab+c = ab+ac = a(b+c)$. Conversely, if $ab+c = a(b+c) = ab+ac$, then $ac = ac + 0 = ac + (ab + \overline{ab}) = (ab + ac) + \overline{ab} = (ab + c) + \overline{ab} = c + (ab + \overline{ab}) = c$, and $ac = c \Longrightarrow c \leq a$.

CHAPTER 16
GROUPS, CODING THEORY, AND POLYA'S METHOD OF ENUMERATION

Section 16.1

1. (a) Yes. The identity is 1 and each element is its own inverse.
   (b) No. The set is not closed under addition and there is no identity.
   (c) No. The set is not closed under addition.
   (d) Yes. The identity is 0; the inverse of $10n$ is $10(-n)$ or $-10n$.
   (e) Yes. The identity is 1_A and the inverse of $g: A \to A$ is $g^{-1}: A \to A$.
   (f) Yes. The identity is 0; the inverse of $a/(2^n)$ is $(-a)/(2^n)$.

2. (c) $ab = ac \Longrightarrow a^{-1}(ab) = a^{-1}(ac) \Longrightarrow (a^{-1}a)b = (a^{-1}a)c \Longrightarrow eb = ec \Longrightarrow b = c$
   (d) $ba = ca \Longrightarrow (ba)a^{-1} = (ca)a^{-1} \Longrightarrow b(aa^{-1}) = c(aa^{-1}) \Longrightarrow be = ce \Longrightarrow b = c$

3. Subtraction is not an associative (closed) binary operation – e.g., $(3-2)-4 = -3 \neq 5 = 3-(2-4)$.

4. (i) For all $a, b, c \in G$,
$(a \circ b) \circ c = (a+b+ab) \circ c = a+b+ab+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$
$a \circ (b \circ c) = a \circ (b+c+bc) = a+b+c+bc+a(b+c+bc) = a+b+c+bc+ab+ac+abc.$
Since $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ it follows that the (closed) binary operation is associative.
(ii) If $x, y \in G$, then $x \circ y = x+y+xy = y+x+yx = y \circ x$, so the (closed) binary operation is also commutative.
(iii) Can we find $a \in G$ so that $x = x \circ a$ for all $x \in G$?
$x = x \circ a \Longrightarrow x = x+a+xa \Longrightarrow 0 = a(1+x) \Longrightarrow a = 0$, because x is arbitrary, so 0 is the identity for this (closed) binary operation.
(iv) For $x \in G$, can we find $y \in G$ with $x \circ y = 0$? Here $0 = x \circ y = x+y+xy \Longrightarrow -x = y(1+x) \Longrightarrow y = -x(1+x)^{-1}$, so the inverse of x is $-x(1+x)^{-1}$.
It follows from (i) - (iv) that $(G, \circ)$ is an abelian group.

5. Since $x, y \in \mathbf{Z} \Longrightarrow x+y+1 \in \mathbf{Z}$, the operation is a (closed) binary operation (or $\mathbf{Z}$ is closed under $\circ$). For all $w, x, y \in \mathbf{Z}$, $w \circ (x \circ y) = w \circ (x+y+1) = w+(x+y+1)+1 = (w+x+1)+y+1 = (w \circ x) \circ y$, so the (closed) binary operation is associative. Furthermore, $x \circ y = x+y+1 = y+x+1 = y \circ x$, for all $x, y \in \mathbf{Z}$, so $\circ$ is also commutative. If $x \in \mathbf{Z}$ then $x \circ (-1) = x+(-1)+1 = x[= (-1) \circ x]$, so -1 is the identity element for $\circ$. And finally, for

each $x \in \mathbf{Z}$, we have $-x-2 \in \mathbf{Z}$ and $x \circ (-x-2) = x + (-x-2) + 1 = -1[= (-x-2)+x]$, so $-x-2$ is the inverse for x under $\circ$. Consequently, $(\mathbf{Z}, \circ)$ is an abelian group.

6. (i) For all $(a,b),(u,v),(x,y) \in S$ we have
$(a,b) \circ [(u,v) \circ (x,y)] = (a,b) \circ (ux, vx+y) = (aux, bux+vx+y)$
$[(a,b) \circ (u,v)] \circ (x,y) = (au, bu+v) \circ (x,y) = (aux, (bu+v)x+y) = (aux, bux+vx+y)$,
so the given (closed) binary operation is associative.
(ii) To find the identity element we need $(a,b) \in S$ such that $(a,b) \circ (u,v) = (u,v) = (u,v) \circ (a,b)$ for all $(u,v) \in S$.
$(u,v) = (u,v) \circ (a,b) = (ua, va+b) \Longrightarrow u = ua$ and $v = va + b \Longrightarrow a = 1$ and $b = 0$.
In addition, $(1,0) \circ (u,v) = (1 \cdot u, 0 \cdot u + v) = (u,v)$, so $(1,0)$ is the identity for this (closed) binary operation.
(iii) Given $(a,b) \in S$ can we find $(c,d) \in S$ so that $(a,b) \circ (c,d) = (c,d) \circ (a,b) = (1,0)$?
$(1,0) = (a,b) \circ (c,d) = (ac, bc+d) \Longrightarrow 1 = ac,\ 0 = bc + d \Longrightarrow c = a^{-1},\ d = -ba^{-1}$.
Since $(a^{-1}, -ba^{-1}) \circ (a,b) = (a^{-1}a, (-ba^{-1})a + b) = (1,0)$, $(a^{-1}, -ba^{-1})$ is the inverse of (a,b) for this (closed) binary operation.
From (i)-(iii) it follows that $(S, \circ)$ is a group. Since $(1,2),(2,3) \in S$ and $(1,2) \circ (2,3) = (2,7)$, while $(2,3) \circ (1,2) = (2,5)$, this group is nonabelian.

7. $U_{20} = \{1,3,7,9,11,13,17,19\}$

$U_{24} = \{1,5,7,11,13,17,19,23\}$

8. Proof: Suppose that G is abelian and that $a,b \in G$. Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$, by using the associative property for a group and the fact that this group is abelian.
Conversely, suppose that G is a group where $(ab)^2 = a^2b^2$ for all $a,b \in G$. If $x,y \in G$, then $(xy)^2 = x^2y^2 \Rightarrow (xy)(xy) = x^2y^2 \Rightarrow x(yx)y = x(xy^2) \Rightarrow (yx)y = xy^2$ (by Theorem 16.1 (c)) $\Rightarrow (yx)y = (xy)y \Rightarrow yx = xy$ (by Theorem 16.1 (d)). Therefore, the group G is abelian.

9. (a) The result follows from Theorem 16.1(b) since both $(a^{-1})^{-1}$ and a are inverses of a^{-1}.
(b) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is an inverse of ab, and by Theorem 16.1(b), $(ab)^{-1} = b^{-1}a^{-1}$.

10. G abelian $\Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$. By Exercise 9(b), $b^{-1}a^{-1} = (ab)^{-1}$, so G abelian $\Longrightarrow a^{-1}b^{-1} = (ab)^{-1}$. Conversely, if $a,b \in G$, then $a^{-1}b^{-1} = (ab)^{-1} \Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Longrightarrow ba^{-1}b^{-1} = a^{-1} \Longrightarrow ba^{-1} = a^{-1}b \Longrightarrow b = a^{-1}ba \Longrightarrow ab = ba \Longrightarrow G$ is abelian.

11. (a) $\{0\}$; $\{0,6\}$; $\{0,4,8\}$; $\{0,3,6,9\}$; $\{0,2,4,6,8,10\}$; $\mathbf{Z}_{12}$.
(b) $\{1\}$; $\{1,10\}$; $\{1,3,4,5,9\}$; $\mathbf{Z}_{11}^*$.
(c) $\{\pi_0\}$; $\{\pi_0, \pi_1, \pi_2\}$; $\{\pi_0, r_1\}$; $\{\pi_0, r_2\}$; $\{\pi_0, r_3\}$; S_3

12. (a) There are eight rigid motions for a square: π_0, π_1, π_2, π_3, where π_i is the

counterclockwise rotation through $i(90°)$, $0 \leq i \leq 3$; r_1 is the reflectin in the vertical; r_2 is the reflection in the horizontal; r_3 the reflection in the diagonal from lower left to upper right; and r_4 the reflection in the diagonal from upper left to lower right.

(b)

$\circ$	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_0	π_0	π_1	π_2	π_3	r_1	r_2	r_3	r_4
π_1	π_1	π_2	π_3	π_0	r_3	r_4	r_2	r_1
π_2	π_2	π_3	π_0	π_1	r_2	r_1	r_4	r_3
π_3	π_3	π_0	π_1	π_2	r_4	r_3	r_1	r_2
r_1	r_1	r_4	r_2	r_3	π_0	π_2	π_3	π_1
r_2	r_2	r_3	r_1	r_4	π_2	π_0	π_1	π_3
r_3	r_3	r_1	r_4	r_2	π_1	π_3	π_0	π_2
r_4	r_4	r_2	r_3	r_1	π_3	π_1	π_2	π_0

π_0 is the group identity.

The inverse of each reflection is the same reflection. The inverse of the rotation π_1 is the rotation π_3, and conversely. The inverse of the rotation π_2 is itself. Also, the inverse of π_0 is π_0.

13. (a) There are 10: five rotations through $i(72°), 0 \leq i \leq 4$, and five reflections about lines containing a vertex and the midpoint of the opposite side.
(b) For a regular n-gon ($n \geq 3$) there are $2n$ rigid motions. There are the n rotations through $i(360°/n)$, $0 \leq i \leq n-1$. There are n reflections. For n odd each reflection is about a line through a vertex and the midpoint of the opposite side. For n even, there are $n/2$ reflections about lines through opposite vertices and $n/2$ reflections about lines through the midpoints of opposite sides.

14.

$$\alpha\beta = \binom{12345}{15234}, \qquad \beta\alpha = \binom{12345}{32514}, \qquad \alpha^3 = \binom{12345}{12345},$$

$$\beta^4 = \binom{12345}{12534}, \qquad \alpha^{-1} = \binom{12345}{31245}, \qquad \beta^{-1} = \binom{12345}{21453},$$

$$(\alpha\beta)^{-1} = \binom{12345}{13452}, \qquad (\beta\alpha)^{-1} = \binom{12345}{42153}, \qquad \beta^{-1}\alpha^{-1} = \binom{12345}{13452}.$$

15. Since $eg = ge$ for all $g \in G$, it follows that $e \in H$ and $H \neq \emptyset$. If $x, y \in H$, then $xg = gx$ and $yg = gy$ for all $g \in G$. Consequently, $(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$ for all $g \in G$, and we have $xy \in H$. Finally, for all $x \in H$ and $g \in G$, $xg^{-1} = g^{-1}x$. So $(xg^{-1})^{-1} = (g^{-1}x)^{-1}$, or $gx^{-1} = x^{-1}g$, and $x^{-1} \in H$. Therefore H is a subgroup of G.

16. (a)

$\omega = (1/\sqrt{2})(1+i)$	$\omega^2 = i$
$\omega^3 = (1/\sqrt{2})(-1+i)$	$\omega^4 = -1$
$\omega^5 = (1/\sqrt{2})(-1-i)$	$\omega^6 = -i$
$\omega^7 = (1/\sqrt{2})(1-i)$	$\omega^8 = 1$

(b) Let $S = \{\omega^n | 1 \leq n \leq 8\}$. Then for all $1 \leq j, k \leq 8$, $\omega^j \cdot \omega^k = \omega^m$, where $m \equiv j+k \pmod 8$ and $1 \leq m \leq 8$. So S is closed under the binary operation of multiplication, which is commutative and associative for all complex numbers – so, in particular, the complex numbers is S.
The element $\omega^8 = 1$ is the identity element and, for all $1 \leq n \leq 7$, we have $(\omega^n)^{-1} = \omega^{8-n}$, so every element of S has a multiplicative inverse in S.
Consequently, S is an abelian group under multiplication.

17. (a) Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$, where $g_1 \circ g_2 \in G$, $h_1 * h_2 \in H$, since $(G, \circ)$ and $(H, *)$ are closed. Hence $G \times H$ is closed.
For $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$, $[(g_1, h_1) \cdot (g_2, h_2)] \cdot (g_3, h_3) = (g_1 \circ g_2,\ h_1 * h_2) \cdot (g_3, h_3) = ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) = (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) = (g_1, h_1) \cdot (g_2 \circ g_3, h_2 * h_3) = (g_1, h_1) \cdot [(g_2, h_2) \cdot (g_3, h_3)]$, since the operations in G and H are associative. Hence, $G \times H$ is associative under $\cdot$.
Let e_G, e_H denote the identities for G, H, respectively. Then (e_G, e_H) is the identity in $G \times H$.
Finally, let $(g, h) \in G \times H$. If g^{-1} is the inverse of g in G and h^{-1} is the inverse of h in H, then (g^{-1}, h^{-1}) is the inverse of (g, h) in $G \times H$.

(b) (i) 216
(ii) $H_1 = \{(x, 0, 0) | x \in \mathbf{Z}_6\}$ is a subgroup of order 6; $H_2 = \{(x, y, 0) | x, y \in \mathbf{Z}_6,\ y = 0, 3\}$ is a subgroup of order 12; $H_3 = \{(x, y, 0) | x, y \in \mathbf{Z}_6\}$ has order 36.
(iii) $-(2,3,4) = (4,3,2)$; $-(4,0,2) = (2,0,4)$; $-(5,1,2) = (1,5,4)$.

18. (a) Since $e \in H$ and $e \in K$, we have $e \in H \cap K$ and $H \cap K \neq \emptyset$. Now let $x, y \in H \cap K$.
$x, y \in H \cap K \Longrightarrow x, y \in H$ and $x, y \in K \Longrightarrow xy \in H$ and $xy \in K$ (since H, K are subgroups) $\Longrightarrow xy \in H \cap K$
$x \in H \cap K \Longrightarrow x \in H$ and $x \in K \Longrightarrow x^{-1} \in H$ and $x^{-1} \in K$ (because H, K are subgroups) $\Longrightarrow x^{-1} \in H \cap K$.
Therefore by Theorem 16.2 we have $H \cap K$ a subgroup of G.
(b) Let G be the group of rigid motions of the equilateral triangle as given in Example 16.7. Let $H = \{\pi_0, \pi_1, \pi_2\}$ and $K = \{\pi_0, r_1\}$. Then H, K are subgroups of G. Here $H \cup K = \{\pi_0, \pi_1, \pi_2, r_1\}$ and, since $r_1 \pi_1 = r_2 \notin H \cup K$, it follows that $H \cup K$ is *not* a subgroup of G.

19. (a) $x = 1, x = 4$ (b) $x = 1, x = 10$

(c) $x = x^{-1} \Rightarrow x^2 \equiv 1 \pmod p \Rightarrow x^2 - 1 \equiv 0 \pmod p \Rightarrow (x-1)(x+1) \equiv 0 \pmod p \Rightarrow x - 1 \equiv 0 \pmod p$ or $x + 1 \equiv 0 \pmod p \Rightarrow x \equiv 1 \pmod p$ or $x \equiv -1 \equiv p-1$

(mod p).

(d) The result is true for $p = 2$, since $(2-1)! = 1! \equiv -1 \pmod 2$. For $p \geq 3$, consider the elements $1, 2, \ldots, p-1$ in $(\mathbf{Z}_p^*, \cdot)$, The elements $2, 3, \ldots, p-2$ yield $(p-3)/2$ pairs of the form x, x^{-1}. [For example, when $p = 11$ we find that $2, 3, 4, \ldots, 9$ yield the four pairs 2,6; 3,4; 5,9; 7,8.] Consequently, $(p-1)! \equiv (1)(1)^{(p-3)/2}(p-1) \equiv p-1 \equiv -1 \pmod p$.

20. (a) In $(U_8, \cdot)$ we have $3^2 = 1$, so $3 = 3^{-1}$, and $5^2 = 1$, so $5 = 5^{-1}$.
(b) In $(U_{16}, \cdot)$ we have $7^2 = 1$, so $7 = 7^{-1}$, and $9^2 = 1$, so $9 = 9^{-1}$.
(c) Let $x = (2^{k-1} - 1)$ in $(U_{2^k}, \cdot)$. One finds that $x^2 = (2^{k-1} - 1(2^{k-1} - 1) = 2^{2k-2} - 2 \cdot 2^{k-1} + 1 = (2^k)(2^{k-2}) - 2k + 1 = 0(2^{k-2}) - 0 + 1 = 1$, so $x = x^{-1}$. This is also true for $x = (2^{k-1} + 1)$.

Section 16.2

1. (c) If $n = 0$, the result follows from part (a) of Theorem 16.5. So consider $n \in \mathbf{Z}^+$.

For $n = 1$, $f(a^n) = f(a^1) = f(a) = [f(a)]^1 = [f(a)]^n$, so the result follows for $n = 1$. Now assume the result true for $n = k$ (≥ 1) and consider $n = k+1$. Then $f(a^n) = f(a^{k+1}) = f(a^k \cdot a) = f(a^k) \cdot f(a) = [f(a)]^k \cdot f(a) = [f(a)]^{k+1} = [f(a)]^n$. So by the Principle of Mathematical Induction, the result is true for all $n \geq 1$.

For $n \geq 1$, we have $a^{-n} = (a^{-1})^n$ – as defined in the material following Theorem 16.1. So $f(a^{-n}) = f[(a^{-1})^n] = [f(a^{-1})]^n$ by our previous work. Then $[f(a^{-1})]^n = [(f(a))^{-1}]^n = [f(a)]^{-n}$ – by part (b) of Theorem 16.1. Hence $f(a^{-n}) = [f(a)]^{-n}$.

Consequently, $f(a^n) = [f(a)]^n$, for all $a \in G$ and all $n \in \mathbf{Z}$.

2. (a)
$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$
(b) For all $1 \leq m, n \leq 4$, $A^m \cdot A^n = A^{m+n} = A^r$, where $1 \leq r \leq 4$ and $m+n \equiv r \pmod 4$. Hence the set $\{A, A^2, A^3, A^4\}$ is closed under the binary operation of matrix multiplication. Matrix multiplication is an associative binary operation for all 2×2 real matrices. Consequently, it is associative when restricted to these four matrices.
The matrix $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element, and $A^{-1} = A^3$, $(A^2)^{-1} = A^{-2} = A^2$, $(A^3)^{-1} = A^{-3} = A$, and $(A^4)^{-1} = A^{-4} = A^4 = A^0$, so every element has a multiplicative inverse.
Finally, for all $1 \leq m, n \leq 4$, $A^m \cdot A^n = A^{m+n} = A^{n+m} = A^n \cdot A^m$, so $\{A, A^2, A^3, A^4\}$ is an abelian group under ordinary matrix multiplication.
(c) Define $f : \{A, A^2, A^3, A^4\} \longrightarrow G$ by

$$\begin{array}{lllll} f: & A \longrightarrow i & \quad or \quad & f: & A \longrightarrow -i \\ & A^2 \longrightarrow -1 = i^2 & & & A^2 \longrightarrow -1 = (-i)^2 \\ & A^3 \longrightarrow -i = i^3 & & & A^3 \longrightarrow i = (-i)^3 \\ & A^4 \longrightarrow 1 = i^4 & & & A^4 \longrightarrow 1 = (-i)^4 \end{array}$$

In either case f is an isomorphism for the two given cyclic groups of order 4.

3. $f(0) = (0,0) \quad f(1) = (1,1) \quad f(2) = (2,0)$
$f(3) = (0,1) \quad f(4) = (1,0) \quad f(5) = (2,1)$

4. Let $x, y \in H$. Since f is onto, there exist $a, b \in G$ with $f(a) = x$, $f(b) = y$. Then $xy = f(a)f(b) = f(ab) = f(ba)$ (since G is abelian) $= f(b)f(a) = yx$, so H is abelian.

5. We need to express the element $(4,6)$ of $\mathbf{Z} \times \mathbf{Z}$ in terms of the elements $(1,3)$ and $(3,7)$, so let us write

$$(4,6) = a(1,3) \oplus b(3,7), \quad \text{where } a, b \in \mathbf{Z}.$$

Then $f(4,6) = f(a(1,3) \oplus b(3,7)) = f(a(1,3)) + f(b(3,7)) = af(1,3) + bf(3,7)$.
With $(4,6) = a(1,3) \oplus b(3,7)$ we have $4 = a + 3b$ and $6 = 3a + 7b$, from which it follows that $a = -5$ and $b = 3$.
Consequently, $f(4,6) = -5g_1 + 3g_2$.

6. (a) For each $k \in \mathbf{Z}$, we find that $(k,0) \in \mathbf{Z} \times \mathbf{Z}$ and $f(k,0) = k - 0 = k$, so the function f is onto $\mathbf{Z}$. Furthermore, if (a,b), $(c,d) \in \mathbf{Z} \times \mathbf{Z}$, then $f((a,b) \oplus (c,d)) = f(a+c, b+d) = (a+c) - (b+d) = (a-b) + (c-d) = f(a,b) + f(c,d)$. Consequently, the function f is a homomorphism onto $\mathbf{Z}$.

(b) If $f(a,b) = 0$, then since $f(a,b) = a - b$, it follows that $a = b$. Also, $a = b \Rightarrow a - b = 0 \Rightarrow f(a,b) = 0$. Hence $f(a,b) = 0$ if and only if $a = b$, or $f^{-1}(0) = \{(a,a) | a \in \mathbf{Z}\}$.

(c) Since $f^{-1}(7) = \{(a,b) | f(a,b) = a - b = 7\}$, here we may also write $f^{-1}(7) = \{(b+7, b) | b \in \mathbf{Z}\} = \{(a, a-7) | a \in \mathbf{Z}\}$.

(d) Let $(a,b) \in \mathbf{Z} \times \mathbf{Z}$. We find that $(a,b) \in f^{-1}(E)$ if and only if $f(a,b) = a - b$ is an even integer.
[We may also write $f^{-1}(E) = \{(2m, 2n) | m, n \in \mathbf{Z}\} \cup \{(2m+1, 2n+1) | m, n \in \mathbf{Z}\}$.]

7. (a) $o(\pi_0) = 1$, $o(\pi_1) = o(\pi_2) = 3$, $o(r_1) = o(r_2) = o(r_3) = 2$.

(b) (See Fig. 16.6) $o(\pi_0) = 1$, $o(\pi_1) = o(\pi_3) = 4$, $o(\pi_2) = o(r_1) = o(r_2) = o(r_3) = o(r_4) = 2$.

8. $n = 2 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ has order 2 and generates the cyclic subgroup

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\} \quad \text{of } S_5.$$

$n = 3: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ has order 3 and generates the cyclic subgroup

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\} \quad \text{of} \quad S_5.$$

$n = 4: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$ has order 4 and generates the cyclic subgroup

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\} \quad \text{of} \quad S_5.$$

$n = 5: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ has order 5 and generates the cyclic subgroup

$$\left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\} \quad \text{of} \quad S_5.$$

9. (a) The elements of order 10 are 4, 12, 28, and 36.

(b) The elements of order 10 are a^4, a^{12}, a^{28}, and a^{36}.

10. (a) $U_{14} = \{1, 3, 5, 9, 11, 13\} = \{a \in \mathbf{Z}^+ \mid 1 \leq a \leq 13 \text{ and } \gcd(a, 14) = 1\}$.

(b) Since

$$\begin{array}{lll} 3^1 = 3 & 3^2 = 9 & 3^3 = 13 \\ 3^4 = 11 & 3^5 = 5 & 3^6 = 1, \end{array}$$

we know that U_{14} is cyclic and $U_{14} = \langle 3 \rangle$.

We also find that

$$\begin{array}{lll} 5^1 = 5 & 5^2 = 11 & 5^3 = 13 \\ 5^4 = 9 & 5^5 = 3 & 5^6 = 1, \end{array}$$

so $U_{14} = \langle 5 \rangle$.

There are no other generators for this group.

11. $\mathbf{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle$; $\mathbf{Z}_7^* = \langle 3 \rangle = \langle 5 \rangle$; $\mathbf{Z}_{11}^* = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 8 \rangle$.

12. Let $f\colon G \to G$, defined by $f(a) = a^{-1}$, be an isomorphism. For all $a, b \in G$, $(ab)^{-1} = f(ab) = f(a)f(b) = a^{-1}b^{-1}$. Also $(ab)^{-1} = a^{-1}b^{-1} \implies (ab)^{-1} = (ba)^{-1} \implies ab = ba$, so G is abelian. Conversely, the function $f: G \to G$ defined by $f(a) = a^{-1}$ is one-to-one and onto for any group G. For G abelian $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$, and f is an isomorphism.

13. Let $(G,+)$, $(H,*)$, $(K,\cdot)$ be the given groups. For any $x,y \in G$, $(g\circ f)(x+y) = g(f(x+y)) = g(f(x)*f(y)) = (g(f(x))\cdot(g(f(y)) = ((g\circ f)(x))\cdot((g\circ f)(y))$, since f,g are homomorphisms. Hence, $g\circ f : G \to K$ is a group homomorphism.

14. (a) From Exercise 16 of Section 16.1 we know that $G = \langle\omega\rangle$. It is also true that $G = \langle\omega^3\rangle = \langle\omega^5\rangle = \langle\omega^7\rangle$.

(b) Define $f : G \to \mathbf{Z}_8$ by $f(\omega^n) = [n]$, $1 \le n \le 8$. If $1 \le k,m \le 8$, then $\omega^k = \omega^m \iff k = m \iff [k] = [m] \iff f(\omega^k) = f(\omega^m)$, so f is a one-to-one function. Since $|G| = |\mathbf{Z}_8|$, it follows from Theorem 5.11 that f is also onto. Finally, for $1 \le k,m \le 8$, $f(\omega^k\cdot\omega^m) = f(\omega^{k+m}) = [k+m] = [k]+[m] = f(\omega^k)+f(\omega^m)$, so f is an isomorphism. Note: Three other isomorphisms are also possible here. They are determined, in each case, by the image of ω. We find these to be:
$f_1 : G \to \mathbf{Z}_8$, where $f_1(\omega) = [3]$;
$f_2 : G \to \mathbf{Z}_8$, where $f_2(\omega) = [5]$; and
$f_3 : G \to \mathbf{Z}_8$, where $f_3(\omega) = [7]$.

15. (a) $(\mathbf{Z}_{12},+) = \langle 1\rangle = \langle 7\rangle = \langle 11\rangle$
$(\mathbf{Z}_{16},+) = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \langle 9\rangle = \langle 11\rangle = \langle 13\rangle = \langle 15\rangle$
$(\mathbf{Z}_{24},+) = \langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle = \langle 13\rangle = \langle 17\rangle = \langle 19\rangle = \langle 23\rangle$

(b) Let $G = \langle a^k\rangle$. Since $G = \langle a\rangle$, $a = (a^k)^s$ for some $s \in \mathbf{Z}$. Then $a^{1-ks} = e$, so $1-ks = tn$ since $o(a) = n$. $1-ks = tn \Longrightarrow 1 = ks+tn \Longrightarrow \gcd(k,n) = 1$. Conversely, let $G = \langle a\rangle$ where $a^k \in G$ and $\gcd(k,n) = 1$. Then $\langle a^k\rangle \subseteq G$. $\gcd(k,n) = 1 \Longrightarrow 1 = ks+tn$, for some $s,t \in \mathbf{Z} \Longrightarrow a = a^1 = a^{ks+nt} = (a^k)^s(a^n)^t = (a^k)^s(e)^t = (a^k)^s \in \langle a^k\rangle$. Hence $G \subseteq \langle a^k\rangle$. So $G = \langle a^k\rangle$, or a^k generates G.

(c) $\phi(n)$.

16. If $k \nmid n$, let $n = qk+r$, $0 < r < k$. Then $f(a^n) = f(e_G) = e_H$ and $f(a^n) = (f(a))^n = (f(a))^{qk+r} = (f(a)^k)^q(f(a)^r) = (f(a))^r$. But $(f(a))^r = e_H$ with $0 < r < k$ contradicts $o(f(a)) = k$. Consequently, $k|n$.

Section 16.3

1. (a) $\left\{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$

(b)

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}H = \left\{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}H = \left\{\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}H=\left\{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}H=H$$

2. Let $K=\langle\beta\rangle=\left\{\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}K=K$$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}$$

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}K=\left\{\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\right\}$$

3. 12

4. $H=\langle[3]\rangle=\langle 3\rangle=\{0,3,6,9,12,15,18,21\}$
$1+H=\{1,4,7,10,13,16,19,22\}$
$2+H=\{2,5,8,11,14,17,20,23\}$.

$K = \langle [4] \rangle = \langle 4 \rangle = \{0, 4, 8, 12, 16, 20\}$
$1 + K = \{1, 5, 9, 13, 17, 21\}$
$2 + K = \{2, 6, 10, 14, 18, 22\}$
$3 + K = \{3, 7, 11, 15, 19, 23\}$

5. From Lagrange's Theorem we know that $|K| = 66(= 2 \cdot 3 \cdot 11)$ divides $|H|$ and that $|H|$ divides $|G| = 660(= 2^2 \cdot 3 \cdot 5 \cdot 11)$. Consequently, since $K \neq H$ and $H \neq G$, it follows that $|H|$ is $2(2 \cdot 3 \cdot 11) = 132$ or $5(2 \cdot 3 \cdot 11) = 330$.

6. Let G be the set of units in R. $u \in G \Longrightarrow G \neq \emptyset$. Also, the elements of G are associative under multiplication (inherited from the multiplication in R). If $x, y \in G$ then $x^{-1}, y^{-1} \in R$ (and in G), and $(xy)(y^{-1}x^{-1}) = u = (y^{-1}x^{-1})(xy)$, so $xy \in G$. Consequently, G is a multiplicative group.

7. (a)

$\cdot$	(1)(2)(3)(4)	(12)(34)	(13)(24)	(14)(23)
(1)(2)(3)(4)	(1)(2)(3)(4)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)(2)(3)(4)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)(2)(3)(4)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)(2)(3)(4)

It follows from Theorem 16.3 that H is a subgroup of G. And since the entries in the above table are symmetric about the diagonal from the upper left to the lower right, we have H an abelian subgroup of G.

(b) Since $|G| = 4! = 24$ and $|H| = 4$, there are $24/4 = 6$ left cosets of H in G.

(c) Consider the function $f: H \to \mathbf{Z}_2 \times \mathbf{Z}_2$ defined by

$f:$ (1)(2)(3)(4) $\to (0,0)$, $f:$ (12)(34) $\to (1,0)$,
$f:$ (13)(24) $\to (0,1)$, $f:$ (14)(23) $\to (1,1)$.

This function f is one-to-one and onto, and for all $x, y \in H$ we find that

$$f(x \cdot y) = f(x) \oplus f(y).$$

Consequently, f is an isomorphism.
[Note: There are other possible answers that can be given here. In fact, there are six possible isomorphisms that one can define here.]

8. Let $o(a) = k$. Then $|\langle a \rangle| = k$, so by Lagrange's Theorem k divides n. Hence $a^n = a^{km} = (a^k)^m = e^m = e$.

9. (a) If H is a proper subgroup of G, then by Lagrange's Theorem $|H|$ is 2 or p. If $|H| = 2$, then $H = \{e, x\}$ where $x^2 = e$, so $H = \langle x \rangle$. If $|H| = p$, let $y \in H$, where $y \neq e$. Then $o(y) = p$, so $H = \langle y \rangle$.

(b) Let $x \in G$, $x \neq e$. Then $o(x) = p$ or $o(x) = p^2$. If $o(x) = p$, then $|\langle x \rangle| = p$. If $o(x) = p^2$, then $G = \langle x \rangle$ and $\langle x^p \rangle$ is a subgroup of G of order p.

10. Corollary 16.1. $o(a) = |\langle a\rangle|$. By Lagrange's Theorem $|\langle a\rangle|$ divides $|G|$, so $o(a)||G|$.

Corollary 16.2. Let G be a group with $|G| = p$, a prime. Let $x \in G$, $x \neq e$. By Corollary 16.1, $o(x) = p$, so $G = \langle x\rangle$ and G is cyclic.

11. (a) Let $x \in H \cap K$. $x \in H \Longrightarrow o(x)|10 \Longrightarrow o(x) = 1, 2, 5$, or 10. $x \in K \Longrightarrow o(x)|21 \Longrightarrow o(x) = 1, 3, 7$, or 21. Hence $o(x) = 1$ and $x = e$.

12. (a) For all $a \in G$, $a^{-1}a = e \in H$, so $a\mathcal{R}a$ and $\mathcal{R}$ is reflexive. If $a, b \in G$ and $a\mathcal{R}b$, then $a\mathcal{R}b \Longrightarrow a^{-1}b \in H \Longrightarrow (a^{-1}b)^{-1} \in H$ (because H is a subgroup) $\Longrightarrow b^{-1}a \in H \Longrightarrow b\mathcal{R}a$, so $\mathcal{R}$ is symmetric. Finally, let a, b, $c \in G$ with $a\mathcal{R}b$ and $b\mathcal{R}c$. Then we have $a^{-1}b, b^{-1}c \in H$ and since H is closed under the group operation, $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}(e)c = a^{-1}c \in H$, so $a\mathcal{R}c$ and $\mathcal{R}$ is transitive. Hence $\mathcal{R}$ is an equivalence relation.

(b) $a\mathcal{R}b \Longrightarrow a^{-1}b \in H \Longrightarrow a^{-1}b = h$, where $h \in H \Longrightarrow bH = (ah)H = a(hH) = aH$. Conversely, $aH = bH \Longrightarrow a \in bH \Longrightarrow a = bh$ for some $h \in H \Longrightarrow h^{-1} = a^{-1}b$, where $h^{-1} \in H \Longrightarrow a^{-1}b \in H$ and $a\mathcal{R}b$.

(c) Let $x \in [a]$. Then $x\mathcal{R}a$ so $x^{-1}a \in H$. Since H is a subgroup, $(x^{-1}a)^{-1} = a^{-1}x \in H$. So $a^{-1}x = h \in H$ and $x = ah \in aH$. Hence $[a] \subseteq aH$. Conversely, if $y \in aH$ then $y = ah_1$, for some $h_1 \in H$. $y = ah_1 \Longrightarrow a^{-1}y = h_1 \in H \Longrightarrow a\mathcal{R}y$. With $\mathcal{R}$ symmetric we also have $y\mathcal{R}a$, and so $y \in [a]$. So here we find $aH \subseteq [a]$. With both inclusions established it now follows that $aH = [a]$.

(d) Define $f : aH \to H$ by $f(ah) = h$, for $h \in H$. $ah_1 = ah_2 \Longleftrightarrow h_1 = h_2 \Longleftrightarrow f(ah_1) = f(ah_2)$, so f is a one-to-one function. Also, for $h \in H$, $f^{-1}(h) \supseteq \{ah\}$, so $f^{-1}(h) \neq \emptyset$, and f is onto. Hence f is bijective and $|aH| = |H|$.

(e) Since $\mathcal{R}$ is an equivalence relation on G, $\mathcal{R}$ induces a partition of G as

$$G = [a_1] \cup [a_2] \cup \ldots \cup [a_t].$$

Hence $[a_i] = a_iH$ for all $1 \leq i \leq t$, and $|a_iH| = |H| = m$ for all $1 \leq i \leq t$. Consequently, $|G| = t|H|$, and $|H|$ divides $|G|$.

13. (a) In $(\mathbf{Z}_p^*, \cdot)$ there are $p - 1$ elements, so by Exercise 8, for each $[x] \in (\mathbf{Z}_p^*, \cdot)$, $[x]^{p-1} = [1]$, or $x^{p-1} \equiv 1 \pmod p$, or $x^p \equiv x \pmod p$. For all $a \in \mathbf{Z}$, if $p \mid a$ then $a \equiv 0 \pmod p$ and $a^p \equiv 0 \equiv a \pmod p$. If $p \not| a$, then $a \equiv b \pmod p$, $1 \leq b \leq p-1$ and $a^p \equiv b^p \equiv b \equiv a \pmod p$.

(b) In the group G of units of $\mathbf{Z}_n$ there are $\phi(n)$ units. If $a \in \mathbf{Z}$ and $\gcd(a, n) = 1$ then $[a] \in G$ and $[a]^{\phi(n)} = [1]$ or $a^{\phi(n)} \equiv 1 \pmod n$

(c) and (d) These results follow from Exercises 6 and 8. They are special cases of Exercise 8.

Section 16.4

1. Here $n = 2573$ and $e = 7$.
The assignment for the given plaintext is:

IN	VE	ST	IN	ST	OC	KS
0813	2104	1819	0813	1819	1402	1018

Since

$(0813)^7 \textbf{ mod } 2573 = 0462$
$(2104)^7 \textbf{ mod } 2573 = 0170$
$(1819)^7 \textbf{ mod } 2573 = 1809$
$(0813)^7 \textbf{ mod } 2573 = 0462$
$(1819)^7 \textbf{ mod } 2573 = 1809$
$(1402)^7 \textbf{ mod } 2573 = 1981$
$(1018)^7 \textbf{ mod } 2573 = 0305,$

the ciphertext is
0462 0170 1809 0462 1809 1981 0305

2. Here $n = 1459$ and $e = 5$.
The assignment for the given plaintext is:

OR	DE	RA	PI	ZZ	AX
1417	0304	1700	1508	2525	0023

Since

$(1417)^5 \textbf{ mod } 1459 = 0152$
$(0304)^5 \textbf{ mod } 1459 = 0466$
$(1700)^5 \textbf{ mod } 1459 = 1318$
$(1508)^5 \textbf{ mod } 1459 = 1177$
$(2525)^5 \textbf{ mod } 1459 = 0055$
$(0023)^5 \textbf{ mod } 1459 = 0694$

the ciphertext is
0152 0466 1318 1177 0055 0694.

3. Here $n = 2501 = (41)(61)$, so $r = \phi(n) = (40)(60) = 2400$. Further, $e = 11$ is a unit in $\mathbf{Z}_{2400}$ and $d = e^{-1} = 1091$.

Since the encrypted ciphertext is
1418 1436 2370 1102 1805 0250,
we calculate the following:

$(1418)^{1091} \textbf{ mod } 2501 = 0317$
$(1436)^{1091} \textbf{ mod } 2501 = 0821$
$(2370)^{1091} \textbf{ mod } 2501 = 0418$
$(1102)^{1091} \textbf{ mod } 2501 = 0005$
$(1805)^{1091} \textbf{ mod } 2501 = 0411$
$(0250)^{1091} \textbf{ mod } 2501 = 2423$

Consequently, the assignment for the original message is
0317 0821 0418 0005 0411 2423
and this reveals the message as

DRIVE SAFELYX.

4. Here $n = 3053 = (43)(71)$, so $r = \phi(n) = (42)(70) = 2940$. Further, $e = 17$ is a unit in $\mathbf{Z}_{2940}$ and $d = e^{-1} = 173$.

Since the encrypted ciphertext is

0986 3029 1134 1105 1232 2281 2967 0272 1818 2398 1153,
we calculate the following:

$(0986)^{173}$ **mod** $3053 = 1907$
$(3029)^{173}$ **mod** $3053 = 0417$
$(1134)^{173}$ **mod** $3053 = 0408$
$(1105)^{173}$ **mod** $3053 = 1818$
$(1232)^{173}$ **mod** $3053 = 0005$
$(2281)^{173}$ **mod** $3053 = 0419$

$(2967)^{173}$ **mod** $3053 = 2408$
$(0272)^{173}$ **mod** $3053 = 1313$
$(1818)^{173}$ **mod** $3053 = 2012$
$(2398)^{173}$ **mod** $3053 = 0104$
$(1153)^{173}$ **mod** $3053 = 1718$

Consequently, the assignment for the original message is
1907 0417 0408 1818 0005 0419 2408 1313 2012 0104 1718
and this reveals the message as

THERE IS SAFETY IN NUMBERS.

5. Here $n = pq = 121,361$ and $r = \phi(n) = 120,432$.

Since $p + q = n - r + 1 = 930$ and $p - q = \sqrt{(n-r+1)^2 - 4n} = \sqrt{864,900 - 485,444} = \sqrt{379,456} = 616$, it follows that

$$p = 157 \text{ and } q = 773.$$

6. Here $n = pq = 5,446,367$ and $r = \phi(n) = 5,441,640$.

Since $p+q = n-r+1 = 4728$ and $p-q = \sqrt{(n-r+1)^2 - 4n} = \sqrt{22,353,984 - 21,785,468} = \sqrt{568516} = 754$, it follows that

$$p = 1987 \text{ and } q = 2741.$$

Section 16.5

1. (a) $e = 0001001$ (b) $r = 1111011$ (c) $c = 0101000$

2. (a) $(0.95)^8(0.05)$ (b) $(0.95)^7(0.05)^2$

(c) $\binom{9}{1}(0.95)^8(0.05)$ (d) $\binom{9}{2}(0.95)^7(0.05)^2$

(e) $\binom{9}{3}(0.95)^6(0.05)^3$ (f) $\binom{7}{3}(0.95)^6(0.05)^3$

3. (a) (i) $D(111101100) = 101$ (ii) $D(000100011) = 000$
(iii) $D(010011111) = 011$

(b) 000000000, 000000001, 100000000

(c) 64

4. (a) $(0.95)^5 + \binom{5}{1}(0.05)(0.95)^4 + \binom{5}{2}(0.05)^2(0.95)^3$

(b) $[(0.95)^5 + \binom{5}{1}(0.05)(0.95)^4 + \binom{5}{2}(0.05)^2(0.95)^3]^3$

(c) $D(r) = 01$ (d) 0000000000, 1000000000, 0000000001

(e) 256

Sections 16.6 and 16.7

1. $S(101010, 1) = \{101010, 001010, 111010, 100010, 101110, 101000, 101011\}$

   $S(111111, 1) = \{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$

2. $S(000000, 1) = \{000000, 100000, 010000, 001000, 000100, 000010, 000001\}$

   $S(010101, 1) = \{010101, 110101, 000101, 011101, 010001, 010111, 010100\}$

   (a) $D(110101) = 01$ (b) $D(101011) = 10$

   (c) $D(001111) = 00$ (d) $D(110000) = 00$

3. (a) $|S(x, 1)| = 11$; $|S(x, 2)| = 56$; $|S(x, 3)| = 176$

   (b) $|S(x, k)| = 1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{k} = \sum_{i=0}^{k} \binom{n}{i}$

4. $k = 8$; $n = 4$

5. (a) The minimum distance between code words is 3. The code can detect all errors of weight ≤ 2 or correct all single errors.
   (b) The minimum distance between code words is 5. The code can detect all errors of weight ≤ 4 or correct all errors of weight ≤ 2.
   (c) The minimum distance between code words is 2. The code detects all single errors but has no correction capability.
   (d) The minimum distance between code words is 3. The code can detect all errors of weight ≤ 2 or correct all single errors.

6. (a) (i) $H \cdot (111101)^{tr} = (101)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (ii) $H \cdot (110101)^{tr} = (000)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (iii) $H \cdot (001111)^{tr} = (010)^{tr}$, so $c = 001101$ and $D(c) = 001$
   (iv) $H \cdot (100100)^{tr} = (010)^{tr}$, so $c = 100110$ and $D(c) = 100$
   (v) $H \cdot (110001)^{tr} = (100)^{tr}$, so $c = 110101$ and $D(c) = 110$
   (vi) $H \cdot (111111)^{tr} = (111)^{tr}$, which doesn't appear among the columns of H.
   Assuming a double error,
   (1) if $111 = 110 + 001$, then $c = 011110$ and $D(c) = 011$;
   (2) if $111 = 011 + 100$, then $c = 101011$ and $D(c) = 101$; and
   (3) if $111 = 101 + 010$, then $c = 110101$ and $D(c) = 110$.

   (vii) $H \cdot (111100)^{tr} = (100)^{tr}$, so $c = 111000$ and $D(c) = 111$
   (viii) $H \cdot (010100)^{tr} = (111)^{tr}$, which doesn't appear among the columns of H.

Assuming a double error,
(1) if $111 = 110 + 001$, then $c = 110101$ and $D(c) = 110$;
(2) if $111 = 011 + 100$, then $c = 000000$ and $D(c) = 000$; and
(3) if $111 = 101 + 010$, then $c = 011110$ and $D(c) = 011$.

(b) No. The results in (vi) and (viii) are not unique.

7. (a) $C = \{00000, 10110, 01011, 11101\}$. The minimum distance between code words is 3, so the code can detect all errors of weight ≤ 2 or correct all single errors.

(b) $$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(c) (i) 01 (ii) 11 (v) 11 (vi) 10
For (iii) and (iv) the syndrome is $(111)^{tr}$ which is not a column of H. Assuming a double error, if $(111)^{tr} = (110)^{tr} + (001)^{tr}$, then the decoded received word is 01 (for (iii)) and 10 (for (iv)). If $(111)^{tr} = (011)^{tr} + (100)^{tr}$, we get 10 (for (iii)) and 01 (for (iv)).

8. (a) $$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$C = \{000000, 100111, 010010, 001101, 110101, 101010, 011111, 111000\}$
(b) No. The second and fifth columns of H are the same.

9. $G = [I_8|A]$ where I_8 is the 8×8 multiplicative identity matrix and A is a column of eight 1's. $H = [A^{tr}|1] = [11111111|1]$.

10. (a) For each $x \in \{0,1\}$, $xG = xxxxxxxxx$.
(b) $H = [A|I_8]$ where I_8 is the 8×8 multiplicative identity and A is a column of eight 1's.

11. Compare the generator (parity-check) matrix in Exercise 9 with the parity-check (generator) matrix in Exercise 10.

12. Let $c \in \mathbf{Z}_2^n$ be a code word. For all $x \in S(c,k)$ the decoding function of Theorem 16.13 decodes x, and if c_1, c_2 are code words $S(c_1,k) \cap S(c_2,k) = \emptyset$. $x \in S(c,k) \Longleftrightarrow d(x,c) \leq k$, so $|S(c,k)| = \sum_{i=0}^{k} \binom{n}{i}$. Consequently, $|M(n,k)|[\sum_{i=0}^{k} \binom{n}{i}]$ accounts for all received words in $\mathbf{Z}_n^2$ that are code words or differ from a code word in k or fewer positions. It follows then that $|M(n,k)|[\sum_{i=0}^{k} \binom{n}{i}] \leq |\mathbf{Z}_2^n| = 2^n$.

For the lower (Gilbert) bound we appeal to error detection. If $r \in \mathbf{Z}_2^n$ and $d(c,r) \leq 2k$, then by Theorem 16.12 we are able to detect r as an incorrect transmission. So for all code words c, $S(c,2k)$ accounts for the code word c as well as those received words r where $d(c,r) \leq 2k$, but here we may have $S(c_1,2k) \cap S(c_2,2k) \neq \emptyset$ for distinct code words

c_1, c_2. If $2^n > |M(n,k)|[\sum_{i=0}^{2k}\binom{n}{i}]$, then there is an element $c^* \in \mathbf{Z}_2^n$ where $d(c^*, c) > 2k$ for all code words c. So we can add c^* to the present set of code words and get a larger code where the minimal distance between code words is still $2k+1$. This, however, contradicts the maximal size $|M(n,k)|$ so $2^n \leq |M(n,k)|[\sum_{i=0}^{2k}\binom{n}{i}]$.

Sections 16.8 and 16.9

1. $\binom{256}{2}$ calculations are needed to find the minimum distance between code words. (A calculation here determines the distance between a pair of code words.) If E is a group homomorphism we need to calculate the weights of the 255 nonzero code words.

2. (a)

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Received word r	$H \cdot r^{tr}$	$c = r + e$	$D(c)$
000011	$(011)^{tr}$	010011	010
100011	$(101)^{tr}$	101011	101
111110	$(110)^{tr}$	011110	011
100001	$(111)^{tr}$	110101	110
001100	$(001)^{tr}$	001101	001
011110	$(000)^{tr}$	011110	011
001111	$(010)^{tr}$	001101	001
111100	$(100)^{tr}$	111000	111

(b) If 100001 is used (in the last row of Table 16.8) as the coset leader instead of 010100, then for $r = 100001$, $H \cdot r^{tr} = (111)^{tr}$. However, if $r = 100001$ and $x = 100001$, then $c = 000000$ (not 110101) and $D(c) = 000$ (not 110).

3. (a)

Syndrome	Coset Leader			
000	00000	10110	01011	11101
110	10000	00110	11011	01101
011	01000	11110	00011	10101
100	00100	10010	01111	11001
010	00010	10100	01001	11111
001	00001	10111	01010	11100
101	11000	01110	10011	00101
111	01100	11010	00111	10001

[The last two rows are not unique.]

(b)

Received Word	Code Word	Decoded Message
11110	10110	10
11101	11101	11
11011	01011	01
10100	10110	10
10011	01011	01
10101	11101	11
11111	11101	11
01100	00000	00

4.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(a)

$(1000)\,G = 1000110$

$(1011)\,G = 1011010$

$(1001)\,G = 1001001$

$(1100)\,G = 1100011$

$(1110)\,G = 1110000$

$(1111)\,G = 1111111$

(b)

Received word r	$H \cdot r^{tr}$	c	$D(c)$
1100001	$(010)^{tr}$	1100011	1100
1110111	$(111)^{tr}$	1111111	1111
0010001	$(010)^{tr}$	0010011	0010
0011100	$(000)^{tr}$	0011100	0011

(c)

Syndrome	Coset Leader
000	0000000
110	1000000
101	0100000
011	0010000
111	0001000
100	0000100
010	0000010
001	0000001

(d) Same results as in part (b).

5. (a) G is 57×63; H is 6×63
(b) The rate is 57/63.

6. The rate of the (3,1) triple repetition code is 1/3. The rate for the Hamming (7,4) code is 4/7. Since (4/7) > (1/3) the Hamming code is more efficient.

7. (a) The Hamming (7,4) code corrects all single errors in transmission, so the probability of the correct decoding of 1011 is $(0.99)^7 + \binom{7}{1}(0.99)^6(0.01)$

(b) $[(0.99)^7 + \binom{7}{1}(0.99)^6(0.01)]^5$

Section 16.10

1. (a) $\pi_3^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_5C_2C_3C_4C_9C_6C_7C_8C_{11}C_{10}C_{15}C_{12}C_{13}C_{14}C_{16} \end{pmatrix}$

$r_2^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_5C_4C_3C_2C_6C_9C_8C_7C_{11}C_{10}C_{13}C_{12}C_{15}C_{14}C_{16} \end{pmatrix}$

(b) $r_3^{-1} = r_3$

$r_3^* = (r_3^{-1})^* \;=\; \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_2C_5C_4C_3C_7C_6C_9C_8C_{10}C_{11}C_{14}C_{13}C_{12}C_{15}C_{16} \end{pmatrix}$

$= (r_3^*)^{-1}$

(c) $\pi_1^* r_1^* = \begin{pmatrix} C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11}C_{12}C_{13}C_{14}C_{15}C_{16} \\ C_1C_2C_5C_4C_3C_7C_6C_9C_8C_{10}C_{11}C_{14}C_{13}C_{12}C_{15}C_{16} \end{pmatrix}$

$= r_3^* = (\pi_1 r_1)^*$.

2. $\alpha = (1247365)$ $\qquad \beta = (135)(2674)$
$\gamma = (123)(476)(5)$ $\qquad \delta = (14)(2)(375)(6)$

3. (a) $o(\alpha) = 7$; $\quad o(\beta) = 12$; $\quad o(\gamma) = 3$; $\quad o(\delta) = 6$.

(b) Let $\alpha \in S_n$, with $\alpha = c_1c_2 \ldots c_k$, a product of disjoint cycles. Then $o(\alpha)$ is the lcm of $\ell(c_1), \ell(c_2), \ldots, \ell(c_k)$, where $\ell(c_i) =$ length of c_i, $1 \leq i \leq k$.

4. Here G is the group of Example 16.7.

(a)

$$\Psi(\pi_0^*) = 2^3 \qquad \Psi(\pi_1^*) = 2 \qquad \Psi(\pi_2^*) = 2$$
$$\Psi(r_1^*) = 2^2 \qquad \Psi(r_2^*) = 2^2 \qquad \Psi(r_3^*) = 2^2$$

The number of distinct colorings is $(1/6)[2^3 + 2 + 2 + 3(2^2)] = 4$.

(b)

$$\Psi(\pi_0^*) = 3^3 \qquad \Psi(\pi_1^*) = 3 \qquad \Psi(\pi_2^*) = 3$$
$$\Psi(r_1^*) = 3^2 \qquad \Psi(r_2^*) = 3^2 \qquad \Psi(r_3^*) = 3^2$$

The number of distinct colorings is $(1/6)[3^3 + 3 + 3 + 3(3^2)] = 10$.

5. For $0 \leq i \leq 4$, let π_i denote a clockwise rotation through $i(72°)$. Also, there are five reflections r_i, $1 \leq i \leq 5$, each about a line through a vertex and the midpoint of the opposite side. Here $|G| = 10$.

(a) $\Psi(\pi_0^*) = 2^5 \qquad \Psi(\pi_i^*) = 2, \quad 2 \leq i \leq 4$
$\Psi(r_i^*) = 2^3, \qquad 1 \leq i \leq 5.$

The number of distinct configurations is $(1/10)[2^5 + 4(2) + 5(2^3)] = 8$.

(b) 39

6. (a) (i) Free to move in two dimensions: Here $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ where the π_i, $0 \leq i \leq 3$, are as in Example 16.28.
$\Psi(\pi_0^*) = 3^4$, $\Psi(\pi_1^*) = \Psi(\pi_3^*) = 3$, $\Psi(\pi_2^*) = 3^2$.
The number of distinct configurations is $(1/4)[3^4 + 2(3) + 3^2] = 24$.

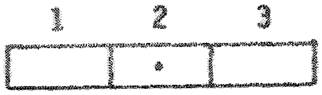
(ii) Free to move in three dimensions: Here G is the group of Example 16.28.
$\Psi(\pi_0^*) = 3^4$, $\Psi(\pi_1^*) = \Psi(\pi_3^*) = 3$, $\Psi(\pi_2^*) = 3^2$.
$\Psi(r_1^*) = 3^3 = \Psi(r_2^*)$, $\Psi(r_3^*) = 3^2 = \Psi(r_4^*)$.

The number of distinct configurations is $(1/8)[3^4 + 2(3) + 3^2 + 2(3^3) + 2(3^2)] = 21$.

(b) (i) Two dimensions: 51 (ii) Three dimensions: 39

7. (a) $G = \{\pi_i | 0 \leq i \leq 3\}$, where π_i is a clockwise rotation through $i \cdot 90°$. The number of distinct bracelets is $(1/4)[4^4 + 4 + 4^2 + 4] = 70$.

(b) $G = \{\pi_i | 0 \leq i \leq 3\} \cup \{r_i | 1 \leq i \leq 4\}$, where each r_i, $1 \leq i \leq 4$, is one of the two reflections about a line through two opposite beads of the midpoints of two opposite lengths of wire. Then the number of distinct bracelets is $(1/8)[4^4 + 4 + 4^2 + 4 + 4^3 + 4^3 + 4^2 + 4^2] = 55$.

8. (a) 

$G = \left\{\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\right\}$

$(1/2)[3^3 + 3^2] = 18$; $(1/2)[4^3 + 4^2] = 40$

(b) $G = \{\pi_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\}$

$(1/2)[3^4 + 3^2] = 45$; $(1/2)[4^4 + 4^2] = 136$

(c) n odd: $(1/2)[3^n + 3^{(n+1)/2}]$; $(1/2)[4^n + 4^{n+1)/2}]$
n even: $(1/2)[3^n + 3^{n/2}]$; $(1/2)[4^n + 4^{n/2}]$

(d) (a) $(1/2)[3 \cdot 2 \cdot 2 + 3 \cdot 2] = 9$; $(1/2)[4 \cdot 3 \cdot 3 + 4 \cdot 3] = 24$
(b) $(1/2)[3 \cdot 2 \cdot 2 \cdot 2 + 0] = 12$; $(1/2)[4 \cdot 3 \cdot 3 \cdot 3 + 0] = 54$.

9. Triangular Figure:
(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $(1/3)[2^4 + 2^2 + 2^2] = 8$
(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $(1/6)[2^4 + 2^2 + 2^2 + 3(2^3)] = 8$

Square Figure:
(a) $G = \{\pi_0, \pi_1, \pi_2 \pi_3\}$ $(1/4)[2^5 + 2(2^2) + 2^3] = 12$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $(1/8)[2^5 + 2(2^2) + 2^3 + 2(2^3) + 2(2^4)] = 12$

10. $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $(1/4)[4^5 + 2(4^2) + 4^3] = 280$
$(1/4)[4(3^4) + 2(4)(3) + 4(3^2)] = 96$

11. (a) 140 (b) 102

12. (a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $(1/4)[2^{16} + 2(2^4) + 2^8] = 16456$
(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$
$(1/8)[2^{16} + 2(2^4) + 2^8 + 2(2^8) + 2(2^{10})] = 8548$

13. $G = \{\pi_i | 0 \leq i \leq 6\}$, where π_i is the (clockwise) rotation through $i \cdot (360°/7)$.
$(1/7)[3^7 + 6(3)] = 315$

14. (a) If e is the identity of G, then $e^*(x) = x$, so $H = \{\pi \in G | \pi^*(x) = x\} \neq \emptyset$. If $\pi_1, \pi_2 \in G$ and $\pi_1^*(x) = x = \pi_2^*(x)$, then $\pi_1^* \pi_2^*(x) = x = (\pi_1 \pi_2)^*(x)$, so $\pi_1 \pi_2 \in H$. Also, if $\pi_1^*(x) = x$, then $(\pi_1^*)^{-1}(x) = x = (\pi_1^{-1})^*(x)$, so $\pi_1 \in H \Longrightarrow \pi_1^{-1} \in H$ and, consequently, H is a subgroup of G.

(b) C_1: The subgroup is $\{\pi_0, r_1\}$
C_{15}: The subgroup is $\{\pi_0, r_3\}$

Section 16.11

1. (a) $(1/4)[5^4 + 5^2 + 2(5)] = 165$
(b) $(1/8)[5^4 + 5^2 + 2(5) + 2(5^2) + 2(5^3)] = 120$

2. (a) $(1/5)[5^5 + 4(5)] = 629$

(b) $(1/10)[5^5 + 4(5) + 5(5^3)] = 377$

3. (Triangular Figure):

(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $\quad (1/3)[4^4 + 2(4^2)] = 96$

(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $\quad (1/6)[4^4 + 2(4^2) + 3(4^3)] = 80$

(Square Figure):

(a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$, $\quad (1/4)[4^5 + 2(4^2) + 4^3] = 280$

(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $\quad (1/8)[4^5 + 2(4^2) + 4^3 + 2(4^3) + 2(4^4)] = 220$

(Hexagonal Figure):

(a) $G = \{\pi_0, \pi_1\}$ where π_i is the rotation through $i \cdot 180°$, $i = 0, 1$.
$(1/2)[4^9 + 4^5] = 131,584$

(b) $G = \{\pi_0, \pi_1, r_1, r_2\}$ where $r_1(r_2)$ is the vertical (horizontal) reflection.
$(1/4)[4^9 + 4^5 + 4^5 + 4^7] = 70,144$

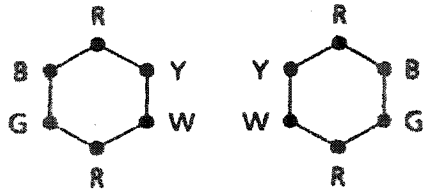
4. (a) $(1/12)[3^6 + 2(3) + 2(3^2) + 4(3^3) + 3(3^4)] = 92$

(b) $(1/12)[m^6 + 2m + 2m^2 + 4m^3 + 3m^4]$ is the number of ways to m-color the vertices of a regular hexagon that is free to move in space.

5. (a) $(1/6)[5^6 + 2(5) + 2(5^2) + 5^3] = 2635$

(b) $(1/12)[5^6 + 2(5) + 2(5^2) + 4(5^3) + 3(5^4)] = 1505$

(c)



6. (Triangular Figure):

(a) $G = \{\pi_0, \pi_1, \pi_2\}$ $\quad (1/3)[3^6 + 2(3^2)] = 249$

(b) $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ $\quad (1/6)[3^6 + 2(4^2) + 3(3^4)] = 165$

(Square Figure):

(a) $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$ $\quad (1/4)[3^8 + 2(3^2) + 3^4] = 1665$

(b) $G = \{\pi_0, \pi_1, \pi_2, \pi_3, r_1, r_2, r_3, r_4\}$ $\quad (1/8)[3^8 + 2(3^2) + (3^4) + 4(3^5)] = 954$

(Hexagonal Figure):

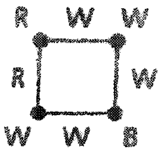
(a) $G = \{\pi_0, \pi_1\}$ $\quad (1/2)[3^{14} + 3^7] = 2,392,578$

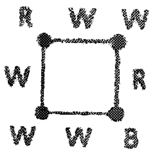
(b) $G = \{\pi_0, \pi_1, r_1, r_2\}$ $\quad (1/4)[3^{14} + 3^7 + 3^9 + 3^8] = 1,202,850$

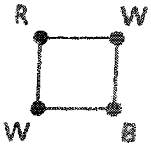
7. (a) $(1/8)[3^4 + 2(3) + 3^2 + 2(3^3) + 2(3^2)] = 21$

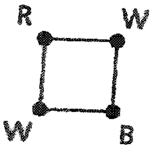
(b) $(1/8)[3^8 + 2(3^2) + 3^4 + 2(3^5) + 2(3^5)] = 954$

(c) No, $k = 21$, $m = 21$, so $km = 441 \neq 954 = n$. Here the location of a certain edge must be considered relative to the location of the vertices.

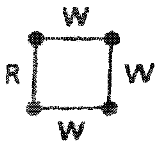
For example, 

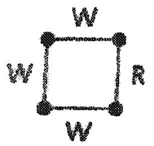
is not equivalent to 

even though 

is equivalent to 

and



is equivalent to 

.

Section 16.12

1. (a) (i) $(1/4)[(r+w)^4 + 2(r^4+w^4) + (r^2+w^2)^2] = r^4 + w^4 + r^3w + 2r^2w^2 + rw^3$
(ii) $(1/8)[(r+w)^4 + 2(r^4+w^4) + 3(r^2+w^2)^2 + 2(r+w)^2(r^2+w^2)] = r^4 + w^4 + r^3w + 2r^2w^2 + rw^3$

(b) (i) $(1/4)[(r+b+w)^4 + 2(r^4+b^4+w^4) + (r^2+b^2+w^2)^2]$
(ii) $(1/8)[(r+b+w)^4 + 2(r^4+b^4+w^4) + 3(r^2+b^2+w^2)^2 + 2(r+b+w)^2(r^2+b^2+w^2)]$

2. The cycle structure representations for the group elements are as follows:
(1) x_1^5 for the identity
(2) x_5 for the four (non-identity) rotations
(3) $x_1x_2^2$ for the five reflections.

The pattern inventory is $(1/10)[(r+b+w)^5 + 4(r^5+b^5+w^5) + 5(r+b+w)(r^2+b^2+w^2)^2]$.
For three red vertices we consider the coefficients of the summands that include r^3:
$(r+b+w)^5: \quad \binom{5}{3,1,1} + \binom{5}{3,2,0} + \binom{5}{3,0,2} = 40$
$(r+b+w)(r^2+b^2+w^2)^2: \quad \binom{2}{1,1,0} + \binom{2}{1,0,1} = 4$
The answer is $(1/10)[40 + 5(4)] = 6$.

For the two red, one white, and two blue vertices we consider
$(r+b+w)^5: \quad \binom{5}{2,1,2} = 30$
$(r+b+w)(r^2+b^2+w^2)^2: \; 2$

The answer is $(1/10)[30 + 5(2)] = 4$

3. (a) (See Example 16.35)

	Rigid Motion	Cycle Structure Representation
(1)	Identity	x_1^6
(2)	Rotation through 90°	$x_1^2x_4$
	Rotation through 180°	$x_1^2x_2^2$
	Rotation through 270°	$x_1^2x_4$
(3)	Rotations of 180°	x_2^3
(4)	Rotations of 120°	x_3^2

There are then $(1/24)[2^6 + 6(2^3) + 3(2^4) + 6(2^3) + 8(2^2)] = 10$ distinct 2-colorings of the faces of the cube.

(b) $(1/24)[(r+w)^6 + 6(r+w)^2(r^4+w^4) + 3(r+w)^2(r^2+w^2)^2 + 6(r^2+w^2)^3 + 8(r^3+w^3)^2]$

(c) For three red and three white faces we consider the coefficients of the summands that involve r^3w^3 :

$(r+w)^6$:	$\binom{6}{3} = 20$
$3(r+w)^2(r^2+w^2)^2$:	12
$8(r^3+w^3)^2$:	16

The answer is $(1/24)[20 + 12 + 16] = 2$

4. $(36) - (1/12)[3^4 + 8(3^2) + 3(3^2)] = 36 - (1/12)[180] = 21$ compounds have at least one bromine atom.

For the compounds with exactly three hydrogen atoms we need the coefficients of w^3x and w^3y in the pattern inventory.

$(w+x+y+z)^4$:	$\binom{4}{3,1,0,0} + \binom{4}{3,0,1,0} = 8$
$8(w+x+y+z)(w^3+x^3+y^3+z^3)$:	$8(1+1) = 16$

The answer is $(1/12)[8 + 16] = 2$

5. Let g denote green and y gold.

(Triangular Figure): $(1/6)[(g+y)^4 + 2(g+y)(g^3+y^3) + 3(g+y)^2(g^2+y^2)]$

(Square Figure): $(1/8)[(g+y)^5 + 2(g+y)(g^4+y^4) + (g+y)(g^2+y^2)^2 + 2(g+y)(g^2+y^2)^2 + 2(g+y)^3(g^2+y^2)]$

(Hexagonal Figure): $(1/4)[(g+y)^9 + (g+y)(g^2+y^2)^4 + (g+y)(g^2+y^2)^4 + (g+y)^5(g^2+y^2)^2]$.

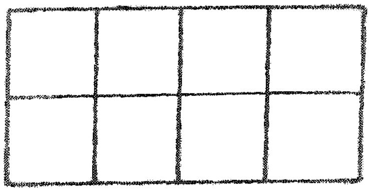
6. Here $G = \{\pi_i | 0 \leq i \leq 6\}$ where π_i is a clockwise rotation through $i \cdot (360°/7)$.
(a) Denote the colors by b: black; r: brown; and w: white.

The pattern inventory is $(1/7)[(b+r+w)^7 + 6(b^7+r^7+w^7)]$. In $(b+r+w)^7$ the coefficient of $b^3r^2w^2$ is $\binom{7}{3,2,2}$, so the answer is $(1/7)\binom{7}{3,2,2} = 30$.

(b) $(1/7)[7$ (for w^7) $+ \binom{7}{5,1,1}$ (for w^5br) $+ \binom{7}{3,2,2}$ (for $w^3b^2r^2$) $+ \binom{7}{1,3,3}$ (for wb^3r^3)$] =$ $(1/7)[7+42+210+140] = 57$

(c) For $n \in \mathbf{Z}^+$, $(1/7)[n^7+6n]$ is the number of ways to n-color the seven horses on the carousel. Since this is an integer, 7 divides (n^7+6n).

7. (a)



Here $G = \{\pi_0, \pi_1\}$, where π_1 denotes the 180° rotation.

$(1/2)[2^8 + 2^4] = 136$ distinct ways to 2-color the squares of the chessboard.

(b) $(1/2)[(r+w)^8 + (r^2+w^2)^4]$

(c) Four red and four white faces: $(1/2)[\binom{8}{4} + \binom{4}{2}] = 38$
Six red and two white faces: $(1/2)[\binom{8}{6} + \binom{4}{1}] = 16$

8. Here $G = \{\pi_i | 0 \leq i \leq 3\}$ where π_i is a (clockwise) rotation through $i(90°)$.

(a) $(1/4)[2^8 + 2(2^2) + 2^4] = 70$

(b) $(1/4)[3^8 + 2(3^2) + 3^4] = 1665$

(c) For the pattern inventory denote the colors as follows: b: black; g: gold; and u: blue. Then the pattern inventory is given by $(1/4)[(b+g+u)^8 + 2(b^4+g^4+u^4)^2 + (b^2+g^2+u^2)^4]$.

For four black, two gold, and two blue regions we need the coefficient of $b^4g^2u^2$ in the pattern inventory. This is $(1/4)[\binom{8}{4,2,2} + \binom{4}{2,1,1}] = 108$.

9. Let $c_1, c_2, \ldots, c_m$ denote the m colors. Since the term $(c_1 + c_2 + \ldots + c_m)^n$ is involved in the pattern inventory, there are $\binom{m+n-1}{n}$ distinct summands.

Supplementary Exercises

1. (a) Since $f(e_G) = e_H$, it follows that $e_G \in K$ and $K \neq \emptyset$. If $x, y \in K$, then $f(x) = f(y) = e_H$ and $f(xy) = f(x)f(y) = e_He_H = e_H$, so $xy \in K$. Also, for $x \in K$, $f(x^{-1}) = [f(x)]^{-1} = e_H^{-1} = e_H$, so $x^{-1} \in K$. Hence K is a subgroup of G.

(b) If $x \in K$, then $f(x) = e_H$. For all $g \in G$, $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_Hf(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$.

Hence, for all $x \in K, g \in G$, we find that $gxg^{-1} \in K$.

2. Let $+$ denote the operation in G, H, and K.

Let $S = \{(h,0)|h \in H\}$. Here 0 is the identity for H (and K) and (0,0) is the identity in G. S is a nonempty subset of G.

The function $f : G \to G$ defined by $f(h,k) = (h,0)$ is a homomorphism with $f(G) = S$, so by part (d) of Theorem 16.5 S is a subgroup of G. The function $g : S \to H$ defined by $g(h,0) = h$ provides an isomorphism between S and H.

In like manner, $\{(0,k)|k \in K\}$ is a subgroup of G that is isomorphic to K.

3. Let a, $b \in G$. Then $a^2b^2 = ee = e = (ab)^2 = abab$. But $a^2b^2 = abab \implies aabb = abab \implies ab = ba$, so G is abelian.

4. Since G has even order, $G - \{e\}$ is odd. For each $g \in G$, $g \neq e$, if $g \neq g^{-1}$, remove $\{g, g^{-1}\}$ from consideration. As we continue this process we must get to at least one element $a \in G$ where $a = a^{-1}$.

5. Let $G =< g >$ and let $h = f(g)$. If $h_1 \in H$, then $h_1 = f(g^n)$ for some $n \in \mathbf{Z}$, since f is onto. Therefore, $h_1 = f(g^n) = [f(g)]^n = h^n$, and $H = \langle h \rangle$.

6. (a) Since $(1,0) \oplus (0,1) = (1,1)$, it follows that $(1,0) \oplus (0,1) \oplus (1,1) = (1,1) \oplus (1,1) = (0,0)$.

(b) Here we have $((1,0,0) \oplus (0,1,1)) \oplus ((0,1,0) \oplus (1,0,1)) \oplus ((0,0,1) \oplus (1,1,0)) \oplus (1,1,1) = (1,1,1) \oplus (1,1,1) \oplus (1,1,1) \oplus (1,1,1) = (0,0,0)$.

(c) Let $n \in \mathbf{Z}^+, n > 1$. Consider the group $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \ldots \times \mathbf{Z}_2, \oplus)$, where we have n copies of $\mathbf{Z}_2$, and the group operation $\oplus$ is componentwise addition modulo 2. The sum of all the nonzero (or non-identity) elements in this group is $(0,0,\ldots,0)$, the identity element of the group.
Proof: In this group there are $2^n - 2$ elements where each such element contains at least one 0 and at least one 1. These $2^n - 2$ elements can be considered in $(1/2)(2^n - 2) = 2^{n-1} - 1$ pairs x, y where $x \oplus y = (1,1,\ldots,1)$, the group element where all n components are 1. Therefore the sum of these $2^n - 2$ elements results in $2^{n-1} - 1$ summands of $(1,1,\ldots,1)$, and this *odd* number of summands yields $(1,1,\ldots,1)$. When we add this result to the element $(1,1,\ldots,1)$ we conclude that the sum of all the nonzero elements in this group is the group identity.

7. Proof: For all $a, b \in G$,

$$(a \circ a^{-1}) \circ b^{-1} \circ b = b \circ b^{-1} \circ (a^{-1} \circ a) \implies$$
$$a \circ a^{-1} \circ b = b \circ a^{-1} \circ a \implies a \circ b = b \circ a,$$

and so it follows that $(G, \circ)$ is an abelian group.

8. For $i = 0$ we find that $n+1$ is in a cycle (of length 1) by itself. Here we have $Q(n,k)$ permutations.

Now let $i = 1$. Here $n+1$ is in a cycle of length 2. The other element can be selected in $n = \binom{n}{1}$ ways, and we have $\binom{n}{1}Q(n-1,k)$ permutations.

When $i = 2$, then $n+1$ is in a cycle of length 3. The other two elements can be selected in $\binom{n}{2}$ ways, and these three elements can be arranged in a cycle of length three in 2! ways. This gives us the $\binom{n}{2}2!Q(n-2,k)$ permutations of $1, 2, \ldots, n+1$ represented as a product of disjoint cycles of length at most k, where $n+1$ is in a cycle of length 3.

In general, for $i = t-1$, where $1 \leq t \leq k$, we find $n+1$ in a cycle of length t. The other $t-1$ elements can be selected in $\binom{n}{t-1}$ ways, and then these t elements can be arranged in a cycle of length t in $(t-1)!$ ways. Then $\binom{n}{t-1}(t-1)!Q(n-(t-1),k)$ counts the permutations of $1, 2, 3, \ldots, n+1$ represented as a product of disjoint cycles of length at most k, where $n+1$ is in a cycle of length t.

We have counted the same set of permutations in two ways, so it follows that

$$Q(n+1,k) = \sum_{i=0}^{k-1} \binom{n}{i}(i!)Q(n-i,k).$$

9. (a) Consider a permutation σ that is counted in $P(n+1,k)$. If $(n+1)$ is a cycle (of length 1) in σ, then σ (restricted to $\{1, 2, \ldots, n\}$) is counted in $P(n, k-1)$. Otherwise, consider any permutation τ that is counted in $P(n,k)$. For each cycle of τ, say $(a_1 a_2 \ldots a_r)$, there are r locations in which to place $n+1$ – (1) Between a_1 and a_2; (2) Between a_2 and $a_3; \ldots; (r-1)$ Between a_{r-1} and a_r; and (r) Between a_r and a_1. Hence there are n locations, in total, to locate $n+1$ in τ. Consequently, $P(n+1,k) = P(n,k-1) + nP(n,k)$.

(b) $\sum_{k=1}^{n} P(n,k)$ counts all of the permutations in S_n, which has $n!$ elements.

10. (a) (i) For all $\sigma, \tau \in S_n$ and $1 \leq i \leq n$, $|\sigma(i) - \tau(i)| \geq 0$, so $d(\sigma,\tau) \geq 0$.
(ii) $d(\sigma,\tau) = 0 \iff \max|\sigma(i) - \tau(i)| = 0$, $1 \leq i \leq n \iff |\sigma(i) - \tau(i)| = 0$, $1 \leq i \leq n \iff \sigma(i) = \tau(i)$, $1 \leq i \leq n \iff \sigma = \tau$.
(iii) $d(\sigma,\tau) = \max\{|\sigma(i) - \tau(i)||1 \leq i \leq n\} = \max\{|\tau(i) - \sigma(i)||1 \leq i \leq n\} = d(\tau,\sigma)$
(iv) Let $d(\rho,\tau) = |\rho(i) - \tau(i)|$ for some $1 \leq i \leq n$. Then $|\rho(i) - \tau(i)| = |(\rho(i) - \sigma(i)) + (\sigma(i) - \tau(i))| \leq |\rho(i) - \sigma(i)| + |\sigma(i) - \tau(i)| \leq d(\rho,\sigma) + d(\sigma,\tau)$.

(b) Since $d(\pi,\epsilon) = \max\{|\pi(i) - i||1 \leq i \leq n\}$, it follows that $d(\pi,\epsilon) \leq 1 \Longrightarrow \pi(n) = n$ or $\pi(n) = n-1$.

(c) If $\pi(n) = n$ then π restricted to $\{1, 2, 3, \ldots, n-1\}$ is also a permutation. Hence we may regard π as an element of S_{n-1}, with $d(\pi,\epsilon) \leq 1$ (ϵ in S_{n-1}), and there are a_{n-1} such permutations. Should $\pi(n) = n-1$, then we must also have $\pi(n-1) = n$. Then π restricted to $\{1, 2, 3, \ldots, n-2\}$ is a permutation. Regarding π as an element of S_{n-2} with $d(\pi,\epsilon) \leq 1$ (ϵ in S_{n-2}), there are a_{n-2} such permutations. Therefore, $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$, $a_1 = 1$, $a_2 = 2$ ($a_0 = 1$), and $a_n = F_{n+1}$, the $(n+1)$st Fibonacci number.

11. (a) Suppose that n is composite. We consider two cases.
(1) $n = m \cdot r$, where $1 < m < r < n$: Here $(n-1)! = 1 \cdot 2 \cdots (m-1) \cdot m \cdot (m+1) \cdots (r-1) \cdot r \cdot (r+1) \cdots (n-1) \equiv 0 \pmod{n}$. Hence $(n-1)! \not\equiv -1 \pmod{n}$.
(2) $n = q^2$, where q is a prime: If $(n-1)! \equiv -1 \pmod{n}$ then $0 \equiv q(n-1)! \equiv q(-1) \equiv n - q \not\equiv 0 \pmod{n}$. So in this case we also have $(n-1)! \not\equiv -1 \pmod{n}$.

(b) From Wilson's Theorem, when p is an odd prime, we find that

$$-1 \equiv (p-1)! \equiv (p-3)!(p-2)(p-1) \equiv (p-3)!(p^2-3p+2) \equiv 2(p-3)! \pmod{p}.$$

12. $G = \{\pi_0, \pi_1, \pi_2, \pi_3\}$

(a) $(1/4)[5^8 + 5^2 + 5^4 + 5^2] = 97,825$

(b) Here four colors are actually used. Nicole can select four colors in $\binom{5}{4} = 5$ ways. For one selection of four colors let $c_i, 1 \leq i \leq 4$, denote that the i-th color is not used. Then using the principle of inclusion and exclusion we have

$N = (1/4)[4^8 + 2(4^2) + 4^4] = 16,456$
$N(c_i) = (1/4)[3^8 + 2(3^2) + 3^4] = 1665,\ 1 \leq i \leq 4$
$N(c_ic_j) = (1/4)[2^8 + 2(2^2) + 2^4] = 70,\ 1 \leq i < j \leq 4$
$N(c_ic_jc_k) = (1/4)[1^8 + 2(1^2) + 1^4] = 1,\ 1 \leq i < j < k \leq 4$
$N(c_1c_2c_3c_4) = 0$
$N(\bar{c}_1\bar{c}_2\bar{c}_3\bar{c}_4) = N - S_1 + S_2 - S_3 + S_4 = 16,456 - \binom{4}{1}(1665) + \binom{4}{2}(70) - \binom{4}{3}(1) + 0 = 10,212.$

The answer then is $(5)(10,212) = 51,060$.

CHAPTER 17
FINITE FIELDS AND
COMBINATORIAL DESIGNS

Section 17.1

1. $f(x)+g(x) = 2x^4 + (2+3)x^3 + (3+5)x^2 + (1+6)x + (4+1) = 2x^4 + 5x^3 + 8x^2 + 7x + 5 = 2x^4 + 5x^3 + x^2 + 5$

$f(x) - g(x) = 2x^4 + (2-3)x^3 + (3-5)x^2 + (1-6)x + (4-1) =$
$2x^4 + (-1)x^3 + (-2)x^2 + (-5)x + 3 = 2x^4 + 6x^3 + 5x^2 + 2x + 3$

$f(x)g(x) = (2)(3)x^7 + [(2)(5) + (2)(3)]x^6 + [(2)(6) + (2)(5) + (3)(3)]x^5 + [(2)(1) + (2)(6) + (3)(5) + (1)(3)]x^4 + [(2)(1) + (3)(6) + (1)(5) + (4)(3)]x^3 + [(3)(1) + (1)(6) + (4)(5)]x^2 + [(1)(1) + (4)(6)]x + 4 = 6x^7 + 16x^6 + 31x^5 + 32x^4 + 37x^3 + 29x^2 + 25x + 4 =$
$6x^7 + 2x^6 + 3x^5 + 4x^4 + 2x^3 + x^2 + 4x + 4.$

2. There are four such polynomials:

(1) x^2 (2) $x^2 + x$ (3) $x^2 + 1$ (4) $x^2 + x + 1$

3. $(10)(11)^2$; $(10)(11)^3$; $(10)(11)^4$; $(10)(11)^n$

4. (a) $f(x) = 4x + 8,\ g(x) = 3x^2$
(b) $h(x) = 4x^5 + x,\ k(x) = 3x^2$

5. (Theorem 17.1) We shall prove one of the distributive laws. Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$, $h(x) = \sum_{k=0}^{p} c_k x^k$, where $m \geq p$. For $0 \leq t \leq m+n$, the coefficient of x^t in $f(x)[g(x) + h(x)]$ is $\sum a_i(b_j + c_j)$ where the sum is taken over all $0 \leq i \leq n$, $0 \leq j \leq m$ with $i + j = t$. But this is the same as $(\sum a_i b_j) + (\sum a_i c_j)$, for $0 \leq i \leq n$, $0 \leq j \leq m$, $i + j = t$, because $a_i(b_j + c_j) = a_i b_j + a_i c_j$ in ring R, and this is the coefficient of x^t in $f(x)g(x) + f(x)h(x)$.

(Corollary 17.1)

(a) Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$. For all $0 \leq t \leq m+n$ the coefficient of x^t in $f(x)g(x)$ is $\sum_{i+j=t} a_i b_j = \sum_{i+j=t} b_j a_i$ (since R is commutative), and this last summation is the coefficient of x^t in $g(x)f(x)$. Hence, $f(x)g(x) = g(x)f(x)$ and $R[x]$ is commutative.

(b) Let 1 denote the unity of R. Then 1 or $1x^0$ is the unity in $R[x]$.

(c) Let R be an integral domain and let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$ with $a_n \neq 0$, $b_m \neq 0$. If $f(x)g(x) = 0$, then $a_n b_m = 0$ contradicting R as an integral domain. Conversely, if $R[x]$ is an integral domain and $a, b \in R$ with $a \neq 0$ and $b \neq 0$, then $ab = (ax^0)(bx^0) \neq 0$ and R is an integral domain.

6. (a) $q(x) = x + 5$ $\quad r(x) = 25x^3 - 9x^2 - 30x - 3$
(b) $q(x) = x^2 + x$ $\quad r(x) = 1$
(c) $q(x) = x^2 + 4x + 2$ $\quad r(x) = x + 2$

7. (a) and (b) $f(x) = (x^2 + 4)(x - 2)(x + 2)$; the roots are ± 2.

(c) $f(x) = (x + 2i)(x - 2i)(x - 2)(x + 2)$; the roots are $\pm 2, \pm 2i$

(d) (a) $f(x) = (x^2 - 5)(x^2 + 5)$; no rational roots
(b) $f(x) = (x - \sqrt{5})(x + \sqrt{5})(x^2 + 5)$; the roots are $\pm\sqrt{5}$
(c) $f(x) = (x - \sqrt{5})(x + \sqrt{5})(x - \sqrt{5}i)(x + \sqrt{5}i)$; the roots are $\pm\sqrt{5}, \pm i\sqrt{5}$

8. (a) 0,2,6,8 $\quad$ (b) $x(x + 4) = (x - 0)(x - 8) = f(x) = (x - 2)(x - 6)$
(c) No – $\mathbf{Z}_{12}$ is *not* a field.

9. (a) $f(3) = 8060$ $\quad$ (b) $f(1) = 1$ $\quad$ (c) $f(-9) = f(2) = 6$

10. (a) $f(x) = x^3 + 5x^3 + 2x + 6 = (x - 1)(x - 3)(x - 5)$
(b) $f(x) = x^7 - x = x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)$

11. 4; 6; $p - 1$

12. (a) If $x - 1$ is a factor of $f(x)$, then 1 is a root of the polynomial. Consequently, $0 = f(1) = a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0$.

Conversely, $a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0 = 0 \Rightarrow$
$0 = a_n(1)^n + a_{n-1}(1)^{n-1} + \ldots + a_2(1)^2 + a_1(1)^1 + a_0(1)^0 = f(1) \Rightarrow$
1 is a root of $f(x) \Rightarrow x - 1$ is a factor of $f(x)$.

(b) If $x + 1$ is a factor of $f(x)$, then -1 is a root of $f(x)$. Therefore, $0 = a_n(-1)^n + a_{n-1}(-1)^{n-1} + a_{n-2}(-1)^{n-2} + a_{n-3}(-1)^{n-3} + \ldots + a_3(-1)^3 + a_2(-1)^2 + a_1(-1) + a_0$. Since n is even it follows that

$$0 = a_n - a_{n-1} + a_{n-2} - a_{n-3} + \ldots - a_3 + a_2 - a_1 + a_0,$$

so $a_n + a_{n-2} + \ldots + a_2 + a_0 = a_{n-1} + a_{n-3} + \ldots + a_3 + a_1$.

Conversely, under the conditions given,
$a_n + a_{n-2} + \ldots + a_2 + a_0 = a_{n-1} + a_{n-3} + \ldots + a_3 + a_1 \Rightarrow$
$0 = a_n - a_{n-1} + a_{n-2} - a_{n-3} + \ldots - a_3 + a_2 - a_1 + a_0 \Rightarrow$
$0 = a_n(-1)^n + a_{n-1}(-1)^{n-1} + a_{n-2}(-1)^{n-2} + a_{n-3}(-1)^{n-3} + \ldots + a_3(-1)^3 + a_2(-1)^2 + a_1(-1) + a_0 = f(-1) \Rightarrow$
-1 is a root of $f(x) \Rightarrow x - (-1) = x + 1$ is a factor of $f(x)$.

13. Let $f(x) = \sum_{i=0}^{m} a_i x^i$ and $h(x) = \sum_{i=0}^{k} b_i x^i$, where $a_i \in R$ for $0 \leq i \leq m$, and $b_i \in R$ for $0 \leq i \leq k$, and $m \leq k$. Then $f(x) + h(x) = \sum_{i=0}^{k}(a_i + b_i)x^i$, where $a_{m+1} = a_{m+2} = \ldots = a_k = z$, the zero of R, so $G(f(x) + h(x)) = G(\sum_{i=0}^{k}(a_i + b_i)x^i) = \sum_{i=0}^{k} g(a_i + b_i)x^i = \sum_{i=0}^{k}[g(a_i) + g(b_i)]x^i = \sum_{i=0}^{k} g(a_i)x^i + \sum_{i=0}^{k} g(b_i)x^i = G(f(x)) + G(h(x))$.

Also, $f(x)h(x) = \sum_{i=0}^{m+k} c_i x^i$, where $c_i = a_i b_0 + a_{i-1}b_1 + \ldots + a_1 b_{i-1} + a_0 b_i$, and

$$G(f(x)h(x)) = G(\sum_{i=0}^{m+k} c_i x^i) = \sum_{i=0}^{m+k} g(c_i)x^i.$$

Since $g(c_i) = g(a_i)g(b_0) + g(a_{i-1})g(b_1) + \ldots + g(a_1)g(b_{i-1}) + g(a_0)g(b_i)$,

$$\sum_{i=0}^{m+k} g(c_i)x^i = (\sum_{i=0}^{m} g(a_i)x^i)(\sum_{i=0}^{k} g(b_i)x^i) = G(f(x)) \cdot G(h(x)).$$

Consequently, $G : R[x] \longrightarrow S[x]$ is a ring homomorphism.

14. If $f(x)$ is a unit in $R[x]$ then there exists $g(x)$ in $R[x]$ where $f(x)g(x) = 1$ (the unity of $R[x]$). But $f(x)g(x) = 1$ and R an integral domain imply that $\deg 1 = 0 = \deg f(x)g(x) = \deg f(x) + \deg g(x)$. So $\deg f(x) = 0 = \deg g(x)$, and each of $f(x), g(x)$ are constants, and consequently units in R.

15. In $\mathbf{Z}_4[x]$, $(2x + 1)(2x + 1) = 1$, so $(2x + 1)$ is a unit. This does not contradict Exercise 14 because $(\mathbf{Z}_4, +, \cdot)$ is not an integral domain.

16. If $a \equiv b \pmod{n}$, then by mathematical induction it follows that $a^k \equiv b^k \pmod{n}$ for all $k \in \mathbf{Z}^+$. Also, $c(a^k) \equiv c(b^k) \pmod{n}$ for each $c \in \mathbf{Z}$, by the definition of multiplication in $\mathbf{Z}_n$. Finally, again by mathematical induction (on the degree of $f(x)$) and the definition of addition in $\mathbf{Z}_n$, it follows that $f(a) \equiv f(b) \pmod{n}$.

17. First note that for $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$, we have $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 = 0$ if and only if $f(1) = 0$. Since the zero polynomial is in S, the set S is not empty. With $f(x)$ as given here, let $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \in S$. (Here $m \leq n$, and for $m < n$ we have $b_{m+1} = b_{m+2} = \cdots = b_n = 0$.) Then $f(1) - g(1) = 0 - 0 = 0$ so $f(x) - g(x) \in S$.

Now consider $h(x) = \sum_{i=0}^{k} r_i x^i \in F[x]$. Here $h(x)f(x) \in F[x]$ and $h(1)f(1) = h(1) \cdot 0 = 0$, so $h(x)f(x) \in S$.

Consequently, S is an ideal in $F[x]$.

18. Let $f(x), g(x) \in I[x]$ where $f(x) = \sum_{i=0}^{m} a_i x_i$, $g(x) = \sum_{j=0}^{n} b_j x^j$, and $a_i \in I$ for $0 \leq i \leq m$, $b_j \in I$ for $0 \leq j \leq n$. Assume $m \leq n$ and that $a_{m+1} = a_{m+2} = \ldots = a_n = z$, the zero element of R. Then $f(x) - g(x) = \sum_{j=0}^{n}(a_j - b_j)x^j$, where $a_j - b_j \in I$ for $0 \leq j \leq n$ because I is an ideal. Now let $h(x) = \sum_{k=0}^{p} r_k x^k \in R[x]$. Then $h(x)f(x) = \sum_{t=0}^{m+p} c_t x^t$ where $c_t = r_0 a_t + r_1 a_{t-1} + r_2 a_{t-2} + \cdots + r_{t-1}a_1 + r_t a_0$. Since I is an ideal of R, $r_0 a_t$,

$r_1a_{t-1}, r_2a_{t-2}, \ldots, r_{t-1}a_1, r_ta_0 \in I$ and it then follows that $c_t \in I$ and $h(x)f(x) \in I[x]$. In a similar way it follows that $f(x)h(x) \in I[x]$. Consequently, $I[x]$ is an ideal in $R[x]$.

Section 17.2

1. (a) $x^2 + 3x - 1$ is irreducible over $\mathbf{Q}$. Over $\mathbf{R}$, $\mathbf{C}$,

$$x^2 + 3x - 1 = [x - ((-3 + \sqrt{13})/2)][x - ((-3 - \sqrt{13})/2)].$$

(b) $x^4 - 2$ is irreducible over $\mathbf{Q}$.
Over $\mathbf{R}$, $x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$;
$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$ over $\mathbf{C}$

(c) $x^2 + x + 1 = (x + 2)(x + 2)$ over $\mathbf{Z}_3$. Over $\mathbf{Z}_5, x^2 + x + 1$ is irreducible;
$x^2 + x + 1 = (x + 5)(x + 3)$ over $\mathbf{Z}_7$.

(d) $x^4 + x^3 + 1$ is irreducible over $\mathbf{Z}_2$.

(e) $x^3 + 3x^2 - x + 1$ is irreducible over $\mathbf{Z}_5$.

2. $f(x) = (x^2 + 1)^3$

3. Degree 1: x; $x + 1$
Degree 2: $x^2 + x + 1$
Degree 3: $x^3 + x^2 + 1$; $x^3 + x + 1$

4. $f(x) = (2x^2 + 1)(5x^3 - 5x + 3)(4x - 3) = 2(x^2 + 4)(5)(x^3 - x + 2)(4)(x - 6) =$
$5(x^2 + 4)(x^3 - x + 2)(x - 6)$, since $40 = 5$ in $\mathbf{Z}_7$.

5. 7^5

6. (Theorem 17.7)

(a) Let $f(x) \in F[x]$ with $\deg f(x) \leq 1$. If $f(x)$ were reducible then $f(x) = g(x)h(x)$ with $\deg g(x), h(x) \geq 1$. Then $1 \geq \deg f(x) = \deg g(x) + \deg h(x) \geq 2$.

(b) If $f(x)$ has a root r in F then $(x-r)$ is a factor of $f(x)$. Hence $f(x) = (x-r)g(x)$ where $\deg g(x) = 1$ or 2, so $f(x)$ is reducible. Conversely, for $f(x)$ reducible, $f(x) = h(x)k(x)$ where $\deg h(x), k(x) \geq 1$. With $\deg f(x) = 2$ or 3, one of $h(x), k(x)$ is a first degree (or linear) factor, say $h(x) = ax + b$, $a, b \in F$, $a \neq 0$. Then $-b/a$ is a root of $f(x)$.

7. (a) Yes, since the coefficients of the polynomials are from a field.

(b) $h(x)|f(x), g(x) \Longrightarrow f(x) = h(x)u(x)$, $g(x) = h(x)v(x)$, for some $u(x), v(x) \in F[x]$.
$m(x) = s(x)f(x) + t(x)g(x)$ for some $s(x), t(x) \in F[x]$, so
$m(x) = h(x)[s(x)u(x) + t(x)v(x)]$ and $h(x)|m(x)$.

(c) If $m(x) \not| f(x)$, then $f(x) = q(x)m(x) + r(x)$ where $r(x) \neq 0$ and $0 \leq \deg r(x) < \deg m(x)$. $m(x) = s(x)f(x) + t(x)g(x)$ so $r(x) = f(x) - q(x)[s(x)f(x) + t(x)g(x)] = (1-q(x))s(x)f(x) - q(x)t(x)g(x)$, so $r(x) \in S$. With $\deg r(x) < \deg m(x)$ we contradict the choice of $m(x)$. Hence $r(x) = 0$ and $m(x)|f(x)$.

8. (Theorem 17.9)

From the last equation $r_k(x)$ divides $r_{k-1}(x)$. The next to last equation yields $r_k(x)$ divides $r_{k-2}(x)$. Continuing backwards we find $r_k(x)$ divides $r_2(x)$ and $r_1(x)$, so $r_k(x)$ divides $r(x)$. From the second equation $r_k(x)$ divides $f(x); r_k(x)$ then divides $g(x)$ from the first equation. To establish condition (b) of Definition 17.6, let $k(x) \in F[x]$ where $k(x)$ divides $r(x)$. From the second equation, $k(x)$ divides $r_1(x)$ since it divides $f(x)$ and $r(x)$. Continuing down the list of equations we get to where $k(x)$ divides $r_{k-2}(x)$ and $r_{k-1}(x)$, and, consequently, $r_k(x)$.

(Theorem 17.10)

For all $f(x) \in F[x], f(x) - f(x) = 0 = 0 \cdot s(x)$, so $\mathcal{R}$ is reflexive. To show that $\mathcal{R}$ is symmetric, let $f(x), g(x) \in F[x]$ with $f(x)\mathcal{R}g(x)$. $f(x)\mathcal{R}g(x) \Longrightarrow f(x)-g(x) = t(x)s(x)$, for some $t(x) \in F[x] \Longrightarrow g(x) - f(x) = [-t(x)]s(x)$, $-t(x) \in F[x] \Longrightarrow g(x)\mathcal{R}f(x)$, so $\mathcal{R}$ is symmetric. Finally, let $f(x), g(x), h(x) \in F[x]$ with $f(x)\mathcal{R}g(x)$ and $g(x)\mathcal{R}h(x)$. Then $f(x) - g(x) = t(x)s(x)$, $g(x) - h(x) = u(x)s(x)$, so $[f(x) - g(x)] + [g(x) - h(x)] = f(x) - h(x) = [t(x) + u(x)]s(x)$ and $\mathcal{R}$ is transitive.

9. (a) By the long division of polynomials we have
$x^5 - x^4 + x^3 + x^2 - x - 1 = (x^3 - 2x^2 + 5x - 8)(x^2 + x - 2) + (17x - 17)$
$x^2 + x - 2 = (17x - 17)[(1/17)x + (2/17)x]$,
so the gcd of $f(x), g(x)$ is
$(x-1) = (1/17)(x^5 - x^4 + x^3 + x^2 - x - 1) - (1/17)(x^2 + x - 2)(x^3 - 2x^2 + 5x - 8)$.

(b) The gcd is $1 = (x+1)(x^4 + x^3 + 1) + (x^3 + x^2 + x)(x^2 + x + 1)$

(c) The gcd is $x^2 + 2x + 1 = (x^4 + 2x^2 + 2x + 2) + (x + 2)(2x^3 + 2x^2 + x + 1)$

10. If there were, then $x - a$ would be a factor of both $f(x)$ and $g(x)$, so $x - a$ would divide the gcd of $f(x)$, $g(x)$. This contradicts $f(x)$, $g(x)$ being relatively prime.

11. $f(x) = x^3 + 2x^2 + ax - b$
$g(x) = x^3 + x^2 - bx + a$
From the Division Algorithm for polynomials we find that $f(x) = g(x) + r(x)$, where $r(x) = x^2 + (a+b)x - (a+b)$, a polynomial of degree 2.
Since we want $r(x)$ to be the gcd, we must have $r(x)$ dividing $f(x)$.
Since $f(x) = r(x)[x+(2-a-b)]+[(2a+b)-(2-a-b)(a+b)]x+[-b+(a+b)(2-a-b)]$, we must have $(2a+b)-(2-a-b)(a+b) = 0$ and $-b+(a+b)(2-a-b) = 0$. Consequently,
$0 = (2a+b) - (2-a-b)(a+b) = a^2 + b^2 + 2ab - b$
$0 = -b+(a+b)(2-a-b) = -a^2 - b^2 - 2ab + 2a + b$. So $2a = 0$, or $a = 0$ and $b^2 - b = 0$.
There are two solutions:

$a = 0, b = 0; \quad a = 0, b = 1.$

12. (a) $x^2 \equiv x + 1 \pmod{s(x)} \Longrightarrow x^3 \equiv x^2 + x \equiv 1 \pmod{s(x)} \Longrightarrow x^4 \equiv x \pmod{s(x)}$.

$$x^4 + x^3 + x + 1 \equiv x + 1 + x + 1 \equiv 0 \pmod{s(x)}, \text{ so } x^4 + x^3 + x + 1 \in [0].$$

(Also note that $x^4 + x^3 + x + 1 = (x^2 + 1)(x^2 + x + 1)$.)

(b) $x^3 + x^2 + 1 \in [x + 1]$

(c) $x^4 + x^3 + x^2 + 1 = x^2(x^2 + x + 1) + 1$, so $x^4 + x^3 + x^2 + 1 \in [1]$.

13. (a) $f(x) \equiv f_1(x) \pmod{s(x)} \Longrightarrow f(x) = f_1(x) + h(x)s(x)$;
$g(x) \equiv g_1(x) \pmod{s(x)} \Longrightarrow g(x) = g_1(x) + k(x)s(x)$
Hence $f(x) + g(x) = f_1(x) + g_1(x) + (h(x) + k(x))s(x)$, so $f(x) + g(x) \equiv f_1(x) + g_1(x) \pmod{s(x)}$, and $f(x)g(x) = f_1(x)g_1(x) + (f_1(x)k(x) + g_1(x)h(x) + h(x)k(x)s(x))s(x)$, so $f(x)g(x) \equiv f_1(x)g_1(x) \pmod{s(x)}$.

(b) These properties follow from the corresponding properties for $F[x]$. For example, for the distributive law,

$$\begin{aligned}[f(x)]([g(x)] + [h(x)]) &= [f(x)][g(x) + h(x)] = [f(x)(g(x) + h(x))] \\ &= [f(x)g(x) + f(x)h(x)] = [f(x)g(x)] + [f(x)h(x)] \\ &= [f(x)][g(x)] + [f(x)][h(x)]\end{aligned}$$

(c) If not, there exists $g(x) \in F[x]$ where $\deg g(x) > 0$ and $g(x)|f(x), s(x)$. But then $s(x)$ would be reducible.

(d) A nonzero element of $F[x]/(s(x))$ has the form $[f(x)]$ where $f(x) \neq 0$ and $\deg f(x) < \deg s(x)$. With $f(x)$, $s(x)$ relatively prime, there exist $r(x)$, $t(x)$ with $1 = f(x)r(x) + s(x)t(x)$, so $1 \equiv f(x)r(x) \pmod{s(x)}$ or $[1] = [f(x)][r(x)]$. Hence $[r(x)] = [f(x)]^{-1}$.

(e) q^n

14. (a) $x^2 + 1 = (x + 1)(x + 1)$ in $\mathbf{Z}_2[x]$

(b) $[0]$, $[1]$, $[x]$, $[x + 1]$

(c) $\mathbf{Z}_2[x]/(s(x))$ is not an integral domain since $[x + 1][x + 1] = [0]$.

15. (a) $[x+2][2x+2]+[x+1] = [2x^2+1]+[x+1] = [2x^2+x+2] = [4x+2+x+2] = [2x+1]$ (Note: With $x^2 + x + 2 \equiv 0 \pmod{s(x)}$, it follows that $x^2 \equiv -x - 2 \equiv 2x + 1 \pmod{s(x)}$.)

(b) $[2x+1]^2[x+2] = [x^2+x+1][x+2] = [x^3+2] = [x(2x+1)+2] = [2x^2+x+2] = [2x+1]$

(c) Find $a, b \in \mathbf{Z}_3$ so that $[2x + 2][ax + b] = [1]$.
$[2ax^2 + (2a + 2b)x + 2b] = [1]$
$[2a(-x - 2) + (2a + 2b)x + 2b] = [2bx + (2b + 2a)] = [1]$
$2b \equiv 0 \pmod 3$, $(2b + 2a) \equiv 1 \pmod 3 \Longrightarrow b \equiv 0 \pmod 3$,

$a \equiv 2 \pmod 3$, so $(22)^{-1} = [2x+2]^{-1} = [2x]$.

16. (a) $s(0) = 1 = s(1)$, so $s(x)$ has no root in $\mathbf{Z}_2$ or linear factor in $\mathbf{Z}_2[x]$. But perhaps we can factor $s(x)$ as $f(x)g(x)$ where $\deg f(x) = \deg g(x) = 2$. If so we have $s(x) = x^4 + x^3 + 1 = f(x)g(x) = (x^2 + ax + b)(x^2 + cx + d)$, where $a, b, c, d \in \mathbf{Z}_2$. Then $(x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd = x^4+x^3+1 \Longrightarrow a+c = 1,\ b+ac+d = 0 = bc+ad,\ bd = 1$.

$bd = 1 \Longrightarrow b = d = 1$.

$b + ac + d = 0 \Longrightarrow ac = 0 \Longrightarrow a = c = 0$

But $a = c = 0 \Longrightarrow a + c = 0$, contradicting $a + c = 1$. Consequently, $s(x)$ is irreducible.

(b) The order of $\mathbf{Z}_2[x]/(s(x))$ is $2^4 = 16$ since $\mathbf{Z}_2[x]/(s(x)) = \{[ax^3 + bx^2 + cx + d] | a, b, c, d \in \mathbf{Z}_2\}$.

(c) $[x^2+x+1][ax^3+bx^2+cx+d] = [1] \Longrightarrow [ax^5+(a+b)x^4+(a+b+c)x^3+(b+c+d)x^2+(c+d)x+d] = [a(x^3+x+1)+(a+b)(x^3+1)+(a+b+c)x^3+(b+c+d)x^2+(c+d)x+d] = [(a+c)x^3+(b+c+d)x^2+(a+c+d)x+(b+d)] = [1] \Longrightarrow a+c \equiv 0 \equiv b+c+d \equiv a+c+d \pmod 2$, $b+d \equiv 1 \pmod 2$. $b+d \equiv 1 \pmod 2 \Longrightarrow c \equiv 1 \pmod 2 \Longrightarrow a \equiv 1 \pmod 2 \Longrightarrow d \equiv 0 \pmod 2 \Longrightarrow b \equiv 1 \pmod 2$. Hence $[x^2 + x + 1]^{-1} = [x^3 + x^2 + x]$.

(d) $[x^3+x+1][x^2+1] = [x^5+x^2+x+1] = [(x^3+x+1)+x^2+x+1] = [x^3+x^2]$

17. (a) $\mathbf{Z}_p[x]/(s(x)) = \{a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} | a_0, a_1, a_2, \ldots, a_{n-1} \in \mathbf{Z}_p\}$ which has order p^n.

(b) The multiplicative group of nonzero elements of this field is a cyclic group of order $p^n - 1$, so it has $\phi(p^n - 1)$ generators.

18. (a) 11 (b) 11 (c) 0 (d) 0

19. (a) 6 (b) 12 (c) 12 (d) $\text{lcm}(m, n)$ (e) 0

20. If not, $\ell_1 b + m_1 a + n_1 u = \ell_2 b + m_2 a + n_2 u$ where at least one of $(\ell_1 - \ell_2)$, $(m_1 - m_2)$, $(n_1 - n_2) \neq 0$. If $\ell_1 - \ell_2 = 0$, we have $m_1 a + n_1 u = m_2 a + n_2 u$ from which it follows (from the work on S_1) that $m_1 = m_2$ and $n_1 = n_2$ — or, $m_1 - m_2 = 0 = n_1 - n_2$ (A contradiction!) Hence $\ell_1 - \ell_2 \neq 0$. Should $m_1 - m_2 = 0$, then $\ell_1 b + n_1 u = \ell_2 b + n_2 u \Rightarrow b \in S_0$ (as in the proof for $|S_1| = p^2$) and this contradiction gives us $m_1 - m_2 \neq 0$. If $n_1 - n_2 = 0$ we find that $\ell_1 b + m_1 a = \ell_2 b + m_2 a \Rightarrow b \in S_1$, and this contradiction tells us that $n_1 - n_2 \neq 0$. With $\ell_1 - \ell_2$, $m_1 - m_2$, $n_1 - n_2$ all nonzero we obtain $b \in S_1$. This last contradiction tells us that $|S_2| = p^3$.

21. 101, 103, 107, 109, 113, 121, 125, 127, 128, 131, 137, 139, 149.

22. Let $s(x) = 2x^2 + 1 \in \mathbf{Z}_5[x]$. We find that $s(0) = 1$, $s(1) = 3$, $s(2) = 4$, $s(3) = 4$, and $s(4) = 3$, so by part (b) of Theorem 17.7 it follows that $s(x)$ is irreducible over $\mathbf{Z}_5$. And now parts (b) and (c) of Theorem 17.11 imply that $\mathbf{Z}_5[x]/(s(x))$ is a field containing $5^2 = 25$

elements.

23. For $s(x) = x^3 + x^2 + x + 2 \in \mathbf{Z}_3[x]$ one finds that $s(0) = 2$, $s(1) = 2$, and $s(2) = 1$. It then follows from part (b) of Theorem 17.7 and parts (b) and (c) of Theorem 17.11 that $\mathbf{Z}_3[x]/(s(x))$ is a finite field with $3^3 = 27$ elements.

24. (a) $h([a + bx]) = h([c + dx]) \Rightarrow a + bi = c + di \Rightarrow a = c$ and $b = d \Rightarrow a + bx = c + dx \Rightarrow [a + bx] = [c + dx]$, so h is one-to-one.
For all $a + bi \in \mathbf{C}$, where $a, b \in \mathbf{R}$, we find that $[a + bx] \in \mathbf{R}[x]/(x^2 + 1)$ and $h([a + bx]) = a + bi$. Consequently, the function h is also onto.
Finally, if $[a+bx], [c+dx] \in \mathbf{R}[x]/(x^2+1)$, then $h([a+bx]+[c+dx]) = h([(a+bx)+(c+dx)]) = h([(a + c) + (b + d)x]) = (a + c) + (b + d)i = (a + bi) + (c + di) = h([a + bx]) + h([c + dx])$, so h preserves the operation of addition.

(b) Let u_F, u_K denote the unity elements of fields F and K, respectively. Then $g(u_F) = g(u_F \cdot u_F) = g(u_F) \odot g(u_F)$, so $g(u_F) \odot u_K = g(u_F) = g(u_F) \odot g(u_F)$. If z_F, z_K denote the zero elements of F and K, respectively, then $g(z_F) = z_K$ (from part (a) of Theorem 14.15). Since g is one-to-one, $g(u_F) \neq z_K$, so by cancellation in K we have $g(u_F) \odot u_K = g(u_F) \odot g(u_F) \Rightarrow u_K = g(u_F)$.
Now if $a \in F$ and $a \neq z_F$, then $a^{-1} \in F$ and $g(u_F) = g(a \cdot a^{-1}) = g(a) \odot g(a^{-1})$. But $g(u_F) = u_K = g(a) \odot [g(a)]^{-1}$ because $g(a) \in K$. Since $g(a) \neq z_K$, by cancellation in K we have $g(a^{-1}) = [g(a)]^{-1}$.

25. (a) Since $0 = 0 + 0\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$, the set $\mathbf{Q}[2]$ is nonempty. For $a + b\sqrt{2}$, $c + d\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$, we have
$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$, with $(a - c), (b - d) \in \mathbf{Q}$; and
$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, with $ac + 2bd, ad + bc \in \mathbf{Q}$.
Consequently, it follows from part (a) of Theorem 14.10 that $\mathbf{Q}[\sqrt{2}]$ is a subring of $\mathbf{R}$.

(b) In order to show that $\mathbf{Q}[\sqrt{2}]$ is a subfield of $\mathbf{R}$ we need to find in $\mathbf{Q}[\sqrt{2}]$ a multiplicative inverse for each nonzero element in $\mathbf{Q}[\sqrt{2}]$.
Let $a + b\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$ with $a + b\sqrt{2} \neq 0$. If $b = 0$, then $a \neq 0$ and $a^{-1} \in \mathbf{Q}$ — and $a^{-1} + 0 \cdot \sqrt{2} \in \mathbf{Q}[\sqrt{2}]$. For $b \neq 0$, we need to find $c + d\sqrt{2} \in \mathbf{Q}[\sqrt{2}]$ so that

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

Now $(a + b\sqrt{2})(c + d\sqrt{2}) = 1 \Rightarrow (ac + 2bd) + (ad + bc)\sqrt{2} = 1 \Rightarrow ac + 2bd = 1$ and $ad + bc = 0 \Rightarrow c = -ad/b$ and $a(-ad/b) + 2bd = 1 \Rightarrow -a^2d + 2b^2d = b \Rightarrow d = b/(2b^2 - a^2)$ and $c = -a/(2b^2 - a^2)$. [Note: $2b^2 - a^2 \neq 0$ because $\sqrt{2}$ is irrational.]
Consequently, $(a + b\sqrt{2})^{-1} = [-a/(2b^2 - a^2)] + [b/(2b^2 - a^2)]\sqrt{2}$, with $[-a/(2b^2 - a^2)]$, $[b/(2b^2 - a^2)] \in \mathbf{Q}$. So $\mathbf{Q}[\sqrt{2}]$ is a subfield of $\mathbf{R}$.

(c) Since $s(x) = x^2 - 2$ is irreducible over $\mathbf{Q}$ we know from part (b) of Theorem 17.11 that $\mathbf{Q}[x]/(x^2 - 2)$ is a field.
Define the correspondence $f : \mathbf{Q}[x]/(x^2 - 2) \to \mathbf{Q}[2]$ by

$$f([a + bx]) = a + b\sqrt{2}.$$

By an argument similar to the one given in Example 17.10 and part (a) of Exercise 24 it follows that f is an isomorphism.

26. (a) Here we want to write $x^2 + bx + c$ as the product $(x - r_1)(x - r_2)$ where $r_1, r_2 \in \mathbf{Z}_p$. Since $(x - r_1)(x - r_2) = (x - r_2)(x - r_1)$, where we may have $r_1 = r_2$, here we seek the number of selections of size 2 from the set $\mathbf{Z}_p = \{0, 1, 2, \ldots, p - 1\}$, with repetitions allowed. Consequently, the number of these monic quadratic polynomials is $\binom{p+2-1}{2} = \binom{p+1}{2} = (\frac{1}{2})(p + 1)(p) = (\frac{1}{2})(p^2 + p)$.

(b) Since $ax^2 + bx + c$ is a quadratic polynomial we have $a \neq 0$. Then with $\mathbf{Z}_p$ a field it follows that $ax^2 + bx + c = a(x^2 + a^{-1}bx + a^{-1}c)$, so we want to be able to factor the monic quadratic polynomial $x^2 + a^{-1}bx + a^{-1}c(= x^2 + b_1x + c_1)$ into linear factors. We have returned to part (a) of the problem where we found the answer to be $(\frac{1}{2})(p^2 + p)$. So here the answer is $(p - 1)(\frac{1}{2})(p^2 + p) = (\frac{1}{2})p(p^2 - 1)$, because there are $p - 1$ nonzero choices for a.

(c) Since there are $(1)(p)(p) = p^2$ monic quadratic polynomials over $\mathbf{Z}_p$, by using the result from part (a) it follows that there are $p^2 - (\frac{1}{2})(p^2 + p) = \frac{1}{2}(p^2 - p)$ *irreducible* monic quadratic polynomials over $\mathbf{Z}_p$.

(d) Here we use the result from part (b), and find that there are $(p-1)(p)(p) - (\frac{1}{2})p(p^2 - 1) = (\frac{1}{2})p(p - 1)^2$ *irreducible* quadratic polynomials over $\mathbf{Z}_p$.

Section 17.3

1.

$$\text{(a)} \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \end{array} \qquad \text{(b)} \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{array} \qquad \text{(c)} \begin{array}{cccc} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 3 & 1 & 2 & 4 \\ 2 & 4 & 3 & 1 \end{array}$$

2. If not, there is an ordered pair (j, k), $1 \leq j, k \leq n$, that appears more than once when the Latin squares L_1^*, L_2^* are superimposed. Let π_i be the permutation of $\{1, 2, \ldots, n\}$ that standardizes L_i as L_i^*, $i = 1, 2$. The inverse permutation π_i^{-1}, $i = 1, 2$, changes L_i^* into L_i. In this process, the ordered pair $(\pi_1^{-1}(j), \pi_2^{-1}(k))$ will appear more than once when L_1, L_2 are superimposed. This contradicts L_1, L_2 being an orthogonal pair.

3. $a_{ri}^{(k)} = a_{rj}^{(k)} \Longrightarrow f_k f_r + f_i = f_k f_r + f_j \Longrightarrow f_i = f_j \Longrightarrow i = j.$

4. By virtue of Theorem 17.16, each 4×4 Latin square, in standard form, is equal to one of these three 4×4 Latin squares. In this sense, there are no others.

5.

$$L_3: \begin{array}{ccccc} 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 1 \\ 5 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{array} \qquad L_4: \begin{array}{ccccc} 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{array}$$

In standard form the Latin squares L_i, $1 \leq i \leq 4$, become

$$L_1': \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{array} \qquad L_2': \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{array}$$

$$L_3': \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 1 \\ 5 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 \end{array} \qquad L_4': \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{array}$$

6. $\mathbf{Z}_7 = \{1, 2, 3, \ldots, 7\}$, so $f_1 = 1$, $f_7 = 7$, as in the proof of Theorem 17.16. Here there are a total of six 7×7 Latin squares $L_k = (a_{ij}^{(k)})$, $1 \leq k \leq 6$, where $a_{ij}^{(k)} = f_k f_i + f_j$.
For $k = 1$, $a_{ij}^{(1)} = f_1 f_i + f_j = f_i + f_j$. This results in the Latin square L_1 (and L_1^* is L_1 in standard form).

$$L_1: \begin{array}{ccccccc} 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \qquad L_1^*: \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

For $k = 2$ we find $a_{ij}^{(2)} = f_2 f_i + f_j = 2f_i + f_j$, and this gives

$$L_2: \begin{array}{ccccccc} 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \qquad L_2^*: \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \end{array}$$

For $k = 3$, $a_{ij}^{(3)} = f_3 f_i + f_j = 3f_i + f_j$ and we have

$$L_3\colon\ \begin{array}{ccccccc} 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \qquad L_3^*\colon\ \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \end{array}$$

7. Introduce a third factor such as four types of transmission fluid or four types of tires.

8. (a) Neither of the 3×3 Latin squares in Example 17.15(b) is self-orthogonal.

(b) The 4×4 Latin square in Example 17.15(c) is self-orthogonal.

(c) If not, let $a_{kk} = a_{mm}$ for some $1 \leq k < m \leq n$. Then when L and L^{tr} are superimposed we get the ordered pair $(a_{kk}, a_{kk}) = (a_{mm}, a_{mm})$ and L, L^{tr} are not orthogonal.

Section 17.4

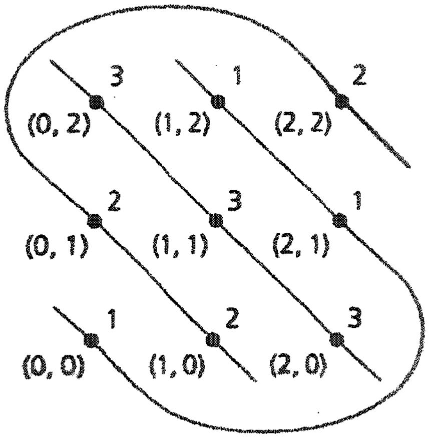
1.

Field	Number of	Number of	Number of Points	Number of Lines
	Points	Lines	on a Line	on a Point
$GF(5)$	25	30	5	6
$GF(3^2)$	81	90	9	10
$GF(7)$	49	56	7	8
$GF(2^4)$	256	272	16	17
$GF(31)$	961	992	31	32

2.

Field	Number of Parallel Classes	Number of Lines per Class
$GF(5)$	6	5
$GF(3^2)$	10	9
$GF(7)$	8	7
$GF(2^4)$	17	16
$GF(31)$	32	31

3. There are nine points and 12 lines. These lines fall into four parallel classes.



(i) Slope of 0.

$y = 0;\ y = 1;\ y = 2$

(ii) Infinite slope

$x = 0;\ x = 1;\ x = 2$

(iii) Slope 1

$y = x;\ y = x + 1;\ y = x + 2$

(iv) Slope 2 (as shown in the figure).

(1) $y = 2x$

(2) $y = 2x + 1$

(3) $y + 2x + 2$

The Latin square corresponding to the fourth parallel class is

3	1	2
2	3	1
1	2	3

4.

(0,4)	(1,4)	(2,4)	(3,4)	(4,4)
(0,3)	(1,3)	(2,3)	(3,3)	(4,3)
(0,2)	(1,2)	(2,2)	(3,2)	(4,2)
(0,1)	(1,1)	(2,1)	(3,1)	(4,1)
(0,0)	(1,0)	(2,0)	(3,0)	(4,0)

Here there are 25 points and 30 lines. These lines fall into six parallel classes.

(i) Slope 0:

$y = 0;\ y = 1;\ y = 2;$
$y = 3;\ y = 4$

(ii) Slope 1:

$y = x;\ y = x + 1;\ y = x + 2;$
$y = x + 3;\ y = x + 4.$

(iii) Slope 2: $y = 2x;\ y = 2x + 1;\ y = 2x + 2;\ y = 2x + 3;\ y = 2x + 4$
(iv) Slope 3: $y = 3x;\ y = 3x + 1;\ y = 3x + 2;\ y = 3x + 3;\ y = 3x + 4$
(v) Slope 4: $y = 4x;\ y = 4x + 1;\ y = 4x + 2;\ y = 4x + 3;\ y = 4x + 4$
(vi) Infinite Slope: $x = 0;\ x = 1;\ x = 2;\ x = 3;\ x = 4.$

The Latin square corresponding to the second parallel class is

5	4	3	2	1
4	3	2	1	5
3	2	1	5	4
2	1	5	4	3
1	5	4	3	2

5. (a) $y = 4x + 1$ (b) $y = 3x + 10$ or $2x + 3y + 3 = 0$
(c) $y = 10x$ or $10y = 11x$

6. (a) (A1) fails because the distinct points (2,4) and (5,4) are on both $y = 2x$ and $y = 4x + 2$.

(A2) fails because the point (2,4) is not on the line $y = 3$, yet this point is on both $y = 2x$ and $y = 4x + 2$. However, neither $y = 2x$ nor $y = 4x + 2$ has a point in common with the line $y = 3$.

(A3), however, still holds. The points (0,0), (1,0), (0,1), and (1,1) are such that no three of these points are on the same line.

(b) In this "geometry", each of the 42 lines contains six points, and each of the 36 points is on seven lines.

7. (a) Vertical line: $x = c$. The line $y = mx + b$ intersects this vertical line at the unique point $(c, mc + b)$. As b takes on the values of F, there are no two column entries (on the line $x = c$) that are the same.

Horizontal line: $y = c$. The line $y = mx + b$ intersects this horizontal line at the unique point $(m^{-1}(c - b), c)$. As b takes on the values of F, no two row entries (on the line $y = c$) are the same.

(b) Let L_i be the Latin square for the parallel class of slope m_i, $i = 1, 2$, $m_i \neq 0$, m_i finite. If an ordered pair (j, k) appears more than once when L_1, L_2 are superimposed, then there are two pairs of lines: (1) $y = m_1x + b_1$, $y = m_2x + b_2$; and (2) $y = m_1x + b_1'$, $y = m_2x + b_2'$ which both intersect at (j, k). But then $b_1 = k - m_1j = b_1'$ and $b_2 = k - m_2j = b_2'$.

Section 17.5

1. $v = 9$, $b = 12$, $r = 4$, $k = 3$, $\lambda = 1$.

2. 1 2 3 1 2 4 1 3 4 2 3 4 $(\lambda = 2)$

3. $\lambda = 2$
1 2 3 4 1 3 5 7 2 3 6 7 3 4 5 6
1 2 5 6 1 4 6 7 2 4 5 7

4.

v	b	r	k	λ
4	4	3	3	2
9	12	4	3	1
10	30	9	3	2
13	13	4	4	1
21	30	10	7	3

These results follow from the information given in the table and the equations (1) $vr = bk$; and (2) $\lambda(v-1) = r(k-1)$.

5. (a) $vr = bk \Longrightarrow 4v = 28(3) \Longrightarrow v = 21$; $\lambda(v-1) = r(k-1) \Longrightarrow 20\lambda = 4(2) \Longrightarrow \lambda \notin \mathbf{Z}^+$, so no such design can exist.
(b) $vr = bk \Longrightarrow (17)(8) = 5b \Longrightarrow b \notin \mathbf{Z}^+$, so no such design can exist in this case either.

6. With $v = b$ and $vr = bk$, we have $r = k$. Then $\lambda(v-1) = r(k-1) = k(k-1)$, where one of k and $k-1$ must be even. Hence $\lambda(v-1)$ is even. With v even, it follows that $v-1$ is odd, so $\lambda(v-1)$ even $\Longrightarrow \lambda$ even.

7. (a) $\lambda(v-1) = r(k-1) = 2r \Longrightarrow \lambda(v-1)$ is even. $\lambda v(v-1) = vr(k-1) = bk(k-1) = b(3)(2) \Longrightarrow 6|\lambda v(v-1)$.

(b) Here $\lambda = 1$. By part (a) $6|v(v-1) \Longrightarrow 3|v(v-1) \Longrightarrow 3|v$ or $3|(v-1)$, since 3 is prime. Also, by part (a) $\lambda(v-1) = (v-1)$ is even, so v is odd.
(i) $3|v \Longrightarrow v = 3t$, t odd $\Longrightarrow v = 3(2s+1) = 6s+3$ and $v \equiv 3 \pmod 6$.
(ii) $3|(v-1) \Longrightarrow v-1 = 3t$, t even $\Longrightarrow v-1 = 6x \Longrightarrow v = 6x+1$ and $v \equiv 1 \pmod 6$.

8. Here $v = 9$, $k = 3$, $b = 12$, $r = 4$ and $\lambda(v-1) = r(k-1) = 4(2) \Longrightarrow 8\lambda = 8 \Longrightarrow \lambda = 1$, so the design is a Steiner triple system.

9. $k = 3$, $\lambda = 1$, $b = 12 \Longrightarrow v = 9$, $r = 4$.

10. (a) P1) and P2)
(b) P1) and P3)
(c) P1), P2), and P3)

11. $v = 15$, $k = 5$, $\lambda = 2 \Longrightarrow$ (a) $b = 21$; (b) $r = 7$

12. Here we have a (v, b, r, k, λ) – design with $v = 28$, $k = 7$, and $\lambda = 2$. From Theorem 17.19 it follows that $6r = (k-1)r = \lambda(v-1) = 2(27)$, so $r = 9$, and consequently, there are $b = vr/k = (28)(9)/7 = 36$ students in Mrs. Mackey's class.

13. There are λ blocks that contain both x and y. Since r is the replication number of the design, it follows that $r - \lambda$ blocks contain x but not y. Likewise there are $r - \lambda$ blocks containing y but not x. Consequently, the number of blocks in the design that contain x or y is $(r-\lambda) + (r-\lambda) + \lambda = 2r - \lambda$.

14. Here $v = n$, $b = p$, $k = m$.

(a) $r = bk/v = pm/n$

(b) $\lambda(v-1) = r(k-1) \Longrightarrow \lambda(n-1) = (pm/n)(m-1) \Longrightarrow \lambda = [pm(m-1)]/[n(n-1)]$.

15. (a) $n+1 = 6 \Longrightarrow n = 5$, so there are $n^2+n+1 = 31$ points in this projective plane.

(b) $n^2+n+1 = 57 \Longrightarrow n = 7$, so there are $n+1 = 8$ points on each line of this plane.

16. The lines $y = x$ and $y = x + z$, for example, would intersect at the two distinct points (0,0,0) and (1,1,0). This contradicts conditions (P1) and (P2) of Definition 17.14.

17. (a) $v = b = 31$; $r = k = 6$; $\lambda = 1$

(b) $v = b = 57$; $r = k = 8$; $\lambda = 1$

(c) $v = b = 73$; $r = k = 9$; $\lambda = 1$

18. (a) There are nine points:

(0,0), (1,0), (2,0)
(0,1), (1,1), (2,1)
(0,2), (1,2), (2,2)

and 12 lines:

$$\begin{array}{llll} x = 0 & y = 0 & y = x & y = 2x \\ x = 1 & y = 1 & y = x+1 & y = 2x+1 \\ x = 2 & y = 2 & y = x+2 & y = 2x+2. \end{array}$$

Here there are four parallel classes, and the parameters for the associated balanced incomplete block design are $v = 9$, $b = 12$, $r = 4$, $k = 3$, $\lambda = 1$.

(b) From the nine points in part (a) we get

(0,0,1), (1,0,1), (2,0,1)
(0,1,1), (1,1,1), (2,1,1)
(0,2,1), (1,2,1), (2,2,1).

To these nine we adjoin the four additional points (1,0,0) and (0,1,0), (1,1,0), (2,1,0) for the line $z = 0$. Consequently, this projective plane has $9+3+1 = 3^2+3+1 = 13$ points and the following 13 lines.

$x = 0$:	$\{(0,0,1),(0,1,1),(0,2,1),(0,1,0)\}$
$y = 0$:	$\{(0,0,1),(1,0,1),(2,0,1),(1,0,0)\}$
$x = z$:	$\{(1,0,1),(1,1,1),(1,2,1),(0,1,0)\}$
$y = z$:	$\{(0,1,1),(1,1,1),(2,1,1),(1,0,0)\}$
$x = 2z$:	$\{(2,0,1),(2,1,1),(2,2,1),(0,1,0)\}$
$y = 2z$:	$\{(0,2,1),(1,2,1),(2,2,1),(1,0,0)\}$
$y = x$:	$\{(0,0,1),(1,1,1),(2,2,1),(1,1,0)\}$
$y = x + z$:	$\{(1,2,1),(2,0,1),(0,1,1),(1,1,0)\}$
$y = x + 2z$:	$\{(1,0,1),(0,2,1),(2,1,1),(1,1,0)\}$
$y = 2x$:	$\{(0,0,1),(1,2,1),(2,1,1),(2,1,0)\}$
$y = 2x + z$:	$\{(0,1,1),(1,0,1),(2,2,1),(2,1,0)\}$
$y = 2x + 2z$:	$\{(0,2,1),(1,1,1),(2,0,1),(2,1,0)\}$
$z = 0\ (\ell_\infty)$:	$\{(1,0,0),(0,1,0),(1,1,0),(2,1,0)\}$

Since there are four points on ℓ_∞ there are four parallel classes. Finally, the parameters for the associated balanced incomplete block design are $v = b = 13$, $r = k = 4$, $\lambda = 1$.

Supplementary Exercises

1. $n = 9$

2. (a) $0 = f(r/s) = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \ldots + a_1(r/s) + a_0 \Longrightarrow 0 = a_n r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n$. Since s divides 0 and s is a factor of all summands except the first, it follows that s divides $a_n r^n$. With $\gcd(r, s) = 1$, $s|a_n$. In similar fashion, $r|a_0$.

(b) (i) $f(x) = 2x^3 + 3x^2 - 2x - 3$.
From part (a) the possible rational roots are ±1, ±3, $\pm1/2$, $\pm3/2$.
$f(1) = 2(1^3) + 3(1^2) - 2(1) - 3 = 0$, so 1 is a root of $f(x)$ and $x - 1$ is a factor. By long division of polynomials (or synthetic division) $f(x) = (x-1)(2x^2 + 5x + 3) = (x-1)(2x+3)(x+1)$, so the other roots of $f(x)$ are $-3/2$ and -1.
(ii) $f(x) = x^4 + x^3 - x^2 - 2x - 2$.
The possible rational roots are ±1, ±2. $f(1) = -3$, $f(-1) = -1$, $f(2) = 14$, $f(-2) = 6$, so there are no rational roots. But can we find rational numbers a, b, c, d so that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$?
$(x^2+ax+b)(x^2+cx+d) = x^4+x^3-x^2-2x-2 \Longrightarrow a+c = 1$, $b+ac+d = -1$, $ad+bc = -2$, $bd = -2 \Longrightarrow a = 1$, $b = 1$, $c = 0$, $d = -2$, so
$f(x) = (x^2 + x + 1)(x^2 - 2)$.

(c) For $f(x) = x^{100} - x^{50} + x^{20} + x^3 + 1$, the only possible rational roots are ±1. But $f(1) = 3 \neq 0$ and $f(-1) = 1 \neq 0$, so $f(x)$ has no rational roots.

3. (a) Let $a, b \in \mathbf{Z}$ with $(x-a)(x+b) = x^2 + x - n$. Then $x^2 + (b-a)x - ab = x^2 + x - n \Longrightarrow b - a = 1$ and $ab = n$. For $1 \leq a \leq 31$ and $b = a + 1$, $n = ab \leq 992$. Hence there are 31 values of n, namely $a(a+1)$ for $1 \leq a \leq 31$.

(b) Here $(x-a)(x+b) = x^2+2x-n \Longrightarrow b-a = 2$ and $ab = n$. When $1 \leq a \leq 30$ and $b = a+2$ we find that $n = ab \leq 960$, so there are 30 such values of n in this case.

(c) In this case there are 29 values of n. Each n has the form $a(a+5)$ for $1 \leq a \leq 29$.

(d) If $(x-a)(x+b) = g(x)$, then $b-a = k$ and $ab = n$. When $k = 1000$, $b = a+1000$ and $ab = a^2+1000a > 1000$. For $k = 999$, with $a = 1$ and $b = 1000$ we have $n = ab = 1000$ and $x^2+999x-1000 = (x+1000)(x-1)$. In fact, for each $1 \leq k \leq 999$, let $a = 1$. Then $b = k+1$ and $n = ab = k+1$, and it follows that $x^2+kx-n = x^2+kx-(k+1) = [x+(k+1)](x-1)$. Hence the smallest positive integer k for which $g(x)$ cannot be so factored is $k = 1000$.

4. If $F = \mathbf{Z}_2$, then $f(1) = 1+1+1+1 = 0$, so 1 is a root of f and $(x-1) = (x+1)$ is a factor. If $F \neq \mathbf{Z}_2$ then $-1 \in F$ and $-1 \neq 1$. Here $f(-1) = 1-1-1+1 = 0$, so -1 is a root and $(x+1)$ is a factor.

5. For all $a \in \mathbf{Z}_p$, $a^p = a$ (See part (a) of Exercise 13 at the end of Section 16.3), so a is a root of $x^p - x$ and $x-a$ is a factor of $x^p - x$. Since $(\mathbf{Z}_p, +, \cdot)$ is a field, the polynomial $x^p - x$ can have at most p roots. Therefore $x^p - x = \prod_{a \in \mathbf{Z}_p}(x-a)$.

6. $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = (x-r_1)(x-r_2)\cdots(x-r_n)$.

(a) The coefficient of x^{n-1} in $(x-r_1)(x-r_2)\cdots(x-r_n)$ is $-r_1-r_2-\ldots-r_n$, so by comparing coefficients we have $a_{n-1} = -r_1-r_2-\cdots-r_n$, or

$$-a_{n-1} = r_1+r_2+\ldots+r_n.$$

(b) The constant term in $(x-r_1)(x-r_2)\cdots(x-r_n)$ is $(-1)^n r_1 r_2 \cdots r_n$. Again by comparison of coefficients we find that

$$a_0 = (-1)^n r_1 r_2 \cdots r_n, \quad \text{or}$$

$$(-1)^n a_0 = (-1)^{2n} r_1 r_2 \cdots r_n = r_1 r_2 \cdots r_n.$$

7. $\{1,2,4\}$, $\{2,3,5\}$, $\{4,5,7\}$

8. $k = 3$, $\lambda = 1$, $v = 63 \Longrightarrow r = 31$, $b = 651$

9. (a) $n^2+n+1 = 73 \Longrightarrow n = 8 \Longrightarrow n+1 = 9$, the number of points on each line.

(b) $n+1 = 10 \Longrightarrow n = 9 \Longrightarrow n^2+n+1 = 91$, the number of lines in this projective plane.

10. If $|F| = n$, then $n^2+n+1 = 91$ and $n = 9$. Since there is only one field (up to isomorphism) of order 9, it follows that $F = GF(3^2)$ which has characteristic 3.

11. (a) r 1's in each row; k 1's in each column.

(b) $A \cdot J_b$ is a $v \times b$ matrix whose (i,j) entry is r, since there are r 1's in each row of A and every entry in J_b is 1. Hence $A \cdot J_b = rJ_{v\times b}$. Likewise, $J_v \cdot A$ is a $v \times b$ matrix whose (i,j) entry is k, since there are k 1's in each column of A and every entry in J_v is 1. Hence $J_v \cdot A = kJ_{v\times b}$.

(c) The (i,j) entry in $A \cdot A^{tr}$ is obtained from the componentwise multiplication of rows i and j of A. If $i=j$ this results in the number of 1's in row i, which is r. For $i \neq j$, the number of 1's is the number of times x_i and x_j appear in the same block – this is given by λ. Hence $A \cdot A^{tr} = (r-\lambda)I_v + \lambda J_v$.

(d)

$$\begin{vmatrix} r & \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \lambda & \dots & r \end{vmatrix} \overset{(1)}{=} \begin{vmatrix} r & \lambda - r & \lambda - r & \lambda - r & \dots & \lambda - r \\ \lambda & r-\lambda & 0 & 0 & \dots & 0 \\ \lambda & 0 & r-\lambda & 0 & \dots & 0 \\ \lambda & 0 & 0 & r-\lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda & 0 & 0 & 0 & \dots & r-\lambda \end{vmatrix}$$

$$\overset{(2)}{=} \begin{vmatrix} r+(v-1)\lambda & 0 & 0 & 0 & \dots & 0 \\ \lambda & r-\lambda & 0 & 0 & \dots & 0 \\ \lambda & 0 & r-\lambda & 0 & \dots & 0 \\ \lambda & 0 & 0 & r-\lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda & 0 & 0 & 0 & \dots & r-\lambda \end{vmatrix}$$

$[r+(v-1)\lambda](r-\lambda)^{v-1} = (r-\lambda)^{v-1}[r+r(k-1)] = rk(r-\lambda)^{v-1}$

(1) Multiply column 1 by -1 and add it to the other $v-1$ columns.
(2) Add rows 2 through v to row 1.

12. (a) Here $V = \{1,2,\dots,9\}$ and the 12 blocks are

$$\begin{array}{cccccc@{\qquad}cccccc@{\qquad}cccccc} 3&4&5&7&8&9 & 1&5&6&7&8&9 & 1&2&4&5&6&9 \\ 2&4&6&7&8&9 & 1&3&4&6&7&9 & 1&2&3&6&7&8 \\ 2&3&5&6&8&9 & 1&3&4&5&6&8 & 1&2&3&5&7&8 \\ 2&3&4&5&6&7 & 1&2&4&5&7&8 & 1&2&3&4&8&9 \end{array}$$

Furthermore $r' = 8$, $k' = 6$, $\lambda' = 5$.

(b) In general we find that
$r' = b - r$, $\quad k' = v - k$, and $\quad \lambda' = b - [2r - \lambda] = b - 2r + \lambda$.

THE

APPENDICES

APPENDIX 1
EXPONENTIAL AND LOGARITHMIC FUNCTIONS

1. (a) $\sqrt{xy^3} = x^{1/2}y^{3/2}$ (b) $\sqrt[4]{81x^{-5}y^3} = 3x^{-5/4}y^{3/4} = \dfrac{3y^{3/4}}{x^{5/4}}$

(c) $5\sqrt[3]{8x^9y^{-5}} = 5(8^{1/3}x^{9/3}y^{-5/3}) = 5(2x^3y^{-5/3}) = \dfrac{10x^3}{y^{5/3}}$

2. (a) $125^{-4/3} = 1/(125)^{4/3} = 1/[(125)^{1/3}]^4 = 1/5^4 = 1/625$

(b) $0.027^{2/3} = [(0.027)^{1/3}]^2 = (0.3)^2 = 0.09$

(c) $(4/3)(1/8)^{-2/3} = (4/3)[1/(1/8)^{2/3}] = (4/3)[1/[(1/8)^{1/3}]^2] = (4/3)[1/(1/2)^2] = (4/3)[1/(1/4)] = (4/3)(4) = 16/3$

3. (a) $(5^{3/4})(5^{13/4}) = 5^{[(3/4)+(13/4)]} = 5^{16/4} = 5^4 = 625$

(b) $(7^{3/5})/(7^{18/5}) = 7^{[(3/5)-(18/5)]} = 7^{(3-18)/5} = 7^{-15/5} = 7^{-3} = 1/7^3 = 1/343$

(c) $(5^{1/2})(20^{1/2}) = (5^{1/2})(4 \cdot 5)^{1/2} = (5^{1/2})(4^{1/2})(5^{1/2}) = 2(5^{1/2})^2 = 2(5) = 10$

4. (a) $5^{3x^2} = 5^{5x+2} \Rightarrow 3x^2 = 5x + 2 \Rightarrow 3x^2 - 5x - 2 = 0 \Rightarrow (3x+1)(x-2) = 0 \Rightarrow x = -1/3$ or $x = 2$.

(b) $4^{x-1} = (1/2)^{4x-1} \Rightarrow 2^{2(x-1)} = 2^{-(4x-1)} \Rightarrow 2(x-1) = -(4x-1) \Rightarrow 2x - 2 = -4x + 1 \Rightarrow 6x = 3 \Rightarrow x = 1/2$

5.

(a) $\log_2 128 = 7$ (b) $\log_{125} 5 = 1/3$

(c) $\log_{10} 1/10,000 = -4$ (d) $\log_2 b = a$

6.

(a) 2 (b) -3 (c) 11

(d) -6 (e) $3/2$ (f) $1/3$

(g) 0 (h) $2/3$

7.

(a) $x^5 = 243 \Rightarrow x = 3$ (b) $x = 3^{-3} = 1/27$

(c) $10^x = 1000 \Rightarrow x = 3$ (d) $x^{5/2} = 32 \Rightarrow x = 32^{2/5} \Rightarrow x = 4$

8. Proof: Let $x = \log_b r$ and $y = \log_b s$. Then, because $x = \log_b r \iff b^x = r$ and $y = \log_b s \iff b^y = s$, we have

$$r/s = b^x/b^y = b^{x-y},$$

from part (2) of Theorem A1.1.
Since

$$r/s = b^{x-y} \iff \log_b(r/s) = x - y,$$

it follows that

$$\log_b(r/s) = x - y = \log_b r - \log_b s.$$

9. (a) Proof (by Mathematical Induction):
For $n = 1$ the statement is $\log_b r^1 = 1 \cdot \log_b r$, so the result is true for this first case. Assuming the result for $n = k$ (≥ 1) we have: $\log_b r^k = k \log_b r$. Now for the case where $n = k + 1$ we find that $\log_b r^{k+1} = \log_b(r \cdot r^k) = \log_b r + \log_b r^k$ (by part (a) of Theorem A1.2) $= \log_b r + k \log_b r$ (by the induction hypothesis) $= (1 + k) \log_b r = (k + 1) \log_b r$. Therefore the result follows for all $n \in \mathbf{Z}^+$ by the Principle of Mathematical Induction.

(b) For all $n \in \mathbf{Z}^+$, $\log_b r^{-n} = \log_b(1/r^n) = \log_b 1 - \log_b r^n$ (by part (b) of Theorem A1.2) $= 0 - n \log_b r$ (by part (a) above) $= (-n) \log_b r$.

10. (a) $\log_2 10 = \log_2(2 \cdot 5) = \log_2 2 + \log_2 5 = 1 + 2.3219 = 3.3219$

(b) $\log_2 100 = \log_2 10^2 = 2 \log_2 10 = 2(3.3219) = 6.6438$

(c) $\log_2(7/5) = \log_2 7 - \log_2 5 = 2.8074 - 2.3219 = 0.4855$

(d) $\log_2 175 = \log_2(7 \cdot 25) = \log_2 7 + 2 \log_2 5 = 2.8074 + 2(2.3219) = 7.4512$

11. (a) Let $x = \log_2 3$. Then $2^x = 3$ and $x(\ln 2) = \ln 2^x = \ln 3$, so $\log_2 3 = x = \ln 3/\ln 2 = 1.0986/0.6931 \doteq 1.5851$.

(b) $\log_5 2 = \ln 2/\ln 5 = 0.6931/1.6094 \doteq 0.4307$

(c) $\log_3 5 = \ln 5/\ln 3 = 1.6094/1.0986 \doteq 1.4650$

12. (a) $\log_{10} x = \log_{10}(2 \cdot 5) \Longrightarrow x = 10$

(b) $\log_4 3x = \log_4 7/5 \Longrightarrow 3x = 7/5 \Longrightarrow x = 7/15$.

13. (a) $1 = \log_{10} x + \log_{10} 6 = \log_{10} 6x \Longrightarrow 6x = 10^1 = 10 \Longrightarrow x = 10/6 = 5/3$.

(b) $\ln(x/(x-1)) = \ln 3 \Longrightarrow x/(x-1) = 3 \Longrightarrow x = 3(x-1) \Longrightarrow x = 3x - 3 \Longrightarrow$
$-2x = -3 \Longrightarrow x = 3/2$.

(c) $2 = \log_3(x^2+4x+4) - \log_3(2x-5) = \log_3[(x^2+4x+4)/(2x-5)] \Longrightarrow 3^2 = 9 = (x^2+4x+4)/(2x-5) \Longrightarrow 9(2x-5) = x^2+4x+4 \Longrightarrow 18x-45 = x^2+4x+4 \Longrightarrow x^2-14x+49 = 0 \Longrightarrow (x-7)^2 = 0 \Longrightarrow x = 7.$

14. $\log_2 x = (1/3)[\log_2 3 - \log_2 5] + (2/3)\log_2 6 + \log_2 17 = \log_2(3/5)^{1/3} + \log_2 6^{2/3} + \log_2 17 = \log_2[17(108/5)^{1/3}] \Longrightarrow x = 17(108/5)^{1/3}$

15. Proof: Let $x = a^{\log_b c}$ and $y = c^{\log_a b}$. Then
$x = a^{\log_b c} \Longrightarrow \log_b x = \log_b[a^{\log_b c}] = (\log_b c)(\log_b a)$, and
$y = c^{\log_a b} \Longrightarrow \log_b y = \log_b[c^{\log_b a}] = (\log_b a)(\log_b c)$.
Consequently, we find that $\log_b x = \log_b y$ from which it follows that $x = y$.

APPENDIX 2
PROPERTIES OF MATRICES

1.

(a) $$A + B = \begin{bmatrix} 3 & 2 & 5 \\ 0 & 2 & 7 \end{bmatrix}$$

(b) $$(A + B) + C = \begin{bmatrix} 3 & 3 & 7 \\ 5 & 6 & 4 \end{bmatrix}$$

(c) $$B + C = \begin{bmatrix} 1 & 2 & 3 \\ 6 & 6 & 1 \end{bmatrix}$$

(d) $$A + (B + C) = \begin{bmatrix} 3 & 3 & 7 \\ 5 & 6 & 4 \end{bmatrix}$$

(e) $$2A = \begin{bmatrix} 4 & 2 & 8 \\ -2 & 0 & 6 \end{bmatrix}$$

(f) $$2A + 3B = \begin{bmatrix} 7 & 5 & 11 \\ 1 & 6 & 18 \end{bmatrix}$$

(g) $$2C + 3C = \begin{bmatrix} 0 & 5 & 10 \\ 25 & 20 & -15 \end{bmatrix}$$

(h) $$5C = \begin{bmatrix} 0 & 5 & 10 \\ 25 & 20 & -15 \end{bmatrix}$$

(i) $$2B - 4C = \begin{bmatrix} 2 & -2 & -6 \\ -18 & -12 & 20 \end{bmatrix}$$

(j) $$A + 2B - 3C = \begin{bmatrix} 4 & 0 & 0 \\ -14 & -8 & 20 \end{bmatrix}$$

(k) $$2(3B) = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 12 & 24 \end{bmatrix}$$

(l) $$(2 \cdot 3)B = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 12 & 24 \end{bmatrix}$$

2. $3a + 4 = 2, \quad a = -2/3; \quad 3b - 8 = 0, \quad b = 8/3;$
$3c - 12 = 10, \quad c = 22/3; \quad 3d - 8 = 6, \quad d = 14/3$

3.

(a) [12], or 12

(b) $$\begin{bmatrix} 9 & 21 \\ 12 & 27 \end{bmatrix}$$

(c) $$\begin{bmatrix} -10 & -10 \\ 18 & 24 \end{bmatrix}$$

(d) $$\begin{bmatrix} -5 & -7 & 8 \\ 29 & 21 & 2 \\ -23 & -35 & 6 \end{bmatrix}$$

(e) $$\begin{bmatrix} a & b & c \\ d & e & f \\ 3g & 3h & 3i \end{bmatrix}$$

(f) $$\begin{bmatrix} a & b & c \\ 3g & 3h & 3i \\ d & e & f \end{bmatrix}$$

4. (a) $$AB + AC = \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & -4 \\ 1 & 3 & 5 \end{bmatrix} + \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 3 & -2 \\ -2 & -7 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 10 & 24 \\ 3 & 8 & 6 \\ 3 & 9 & 15 \end{bmatrix} + \begin{bmatrix} -8 & -31 & 26 \\ -4 & -11 & 10 \\ -6 & -21 & 18 \end{bmatrix} = \begin{bmatrix} -5 & -21 & 50 \\ -1 & -3 & 16 \\ -3 & -12 & 33 \end{bmatrix}$$

$$A(B+C) = \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} \left(\begin{bmatrix} 1 & 2 & -4 \\ 1 & 3 & 5 \end{bmatrix} + \begin{bmatrix} 0 & 3 & -2 \\ -2 & -7 & 6 \end{bmatrix} \right)$$

$$= \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 5 & -6 \\ -1 & -4 & 11 \end{bmatrix} = \begin{bmatrix} -5 & -21 & 50 \\ -1 & -3 & 16 \\ -3 & -12 & 33 \end{bmatrix}$$

(b) $BA + CA = \begin{bmatrix} 1 & 2 & -4 \\ 1 & 3 & 5 \end{bmatrix} \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} + \begin{bmatrix} 0 & 3 & -2 \\ -2 & -7 & 6 \end{bmatrix} \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix}$

$$= \begin{bmatrix} 1 & -4 \\ 2 & 25 \end{bmatrix} + \begin{bmatrix} 3 & 0 \\ -5 & -4 \end{bmatrix} = \begin{bmatrix} 4 & -4 \\ -3 & 21 \end{bmatrix}$$

$$(B+C)A = \left(\begin{bmatrix} 1 & 2 & -4 \\ 1 & 3 & 5 \end{bmatrix} + \begin{bmatrix} 0 & 3 & -2 \\ -2 & -7 & 6 \end{bmatrix} \right) \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 5 & -6 \\ -1 & -4 & 11 \end{bmatrix} \begin{bmatrix} -1 & 4 \\ 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 4 & -4 \\ -3 & 21 \end{bmatrix}$$

5. (a) $(-1/5)\begin{bmatrix} 1 & -2 \\ -3 & 1 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (c) The inverse does not exist.

(d) $\begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}$

6. (a) $A = \begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 1 & -5 \end{bmatrix} = (1/2)\begin{bmatrix} 3 & -2 \\ -2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & -5 \end{bmatrix} = (1/2)\begin{bmatrix} 1 & 10 \\ 0 & -10 \end{bmatrix}$

(b) $A = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}^{-1} \left(\begin{bmatrix} 3 & 2 \\ -1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \right) = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 17 & 19 \\ -10 & -11 \end{bmatrix}$

7. (a) $A^{-1} = (1/2)\begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix}$ (b) $B^{-1} = (1/5)\begin{bmatrix} 1 & -2 \\ 3 & -1 \end{bmatrix}$ (c) $AB = \begin{bmatrix} -4 & 3 \\ -6 & 2 \end{bmatrix}$

(d) $(AB)^{-1} = (1/10)\begin{bmatrix} 2 & -3 \\ 6 & -4 \end{bmatrix}$ (e) $B^{-1}A^{-1} = (1/10)\begin{bmatrix} 2 & -3 \\ 6 & -4 \end{bmatrix}$

8. (a) -2 (b) -10 (c) -10 (d) -50

9. (a) $\begin{bmatrix} 3 & -2 \\ 4 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \\ 6 \end{bmatrix}$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 4 & -3 \end{bmatrix}^{-1} \begin{bmatrix} 5 \\ 6 \end{bmatrix} = (-1) \begin{bmatrix} -3 & 2 \\ -4 & 3 \end{bmatrix} \begin{bmatrix} 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$

(b) $\begin{bmatrix} 5 & 3 \\ 3 & -2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 35 \\ 2 \end{bmatrix}$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & -2 \end{bmatrix}^{-1} \begin{bmatrix} 35 \\ 2 \end{bmatrix} = (-1/19) \begin{bmatrix} -2 & -3 \\ -3 & 5 \end{bmatrix} \begin{bmatrix} 35 \\ 2 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix}$$

10. (a) 21 (b) 21 (c) 21 (d) 63

11. $\det(2A) = 2^2(31) = 124$, $\det(5A) = 5^2(31) = 775$

12. (a) $\begin{vmatrix} 1 & 0 & -2 \\ 3 & 1 & -1 \\ 4 & 1 & 2 \end{vmatrix} = 3(-1)^{2+1} \begin{vmatrix} 0 & -2 \\ 1 & 2 \end{vmatrix} + 1(-1)^{2+2} \begin{vmatrix} 1 & -2 \\ 4 & 2 \end{vmatrix}$

$$+(-1)(-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 4 & 1 \end{vmatrix} = -3(2) + (10) + 1 = 5$$

$$\begin{vmatrix} 1 & 0 & -2 \\ 3 & 1 & -1 \\ 4 & 1 & 2 \end{vmatrix} = (-2)(-1)^{1+3} \begin{vmatrix} 3 & 1 \\ 4 & 1 \end{vmatrix} + (-1)(-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 4 & 1 \end{vmatrix}$$

$$+2(-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 3 & 1 \end{vmatrix} = -2(-1) + 1 + 2(1) = 5$$

(b) $\begin{vmatrix} 1 & 1 & 2 \\ 2 & 3 & -4 \\ 0 & 5 & 7 \end{vmatrix} = 1(-1)^{1+1} \begin{vmatrix} 3 & -4 \\ 5 & 7 \end{vmatrix} + 1(-1)^{1+2} \begin{vmatrix} 2 & -4 \\ 0 & 7 \end{vmatrix}$

$$+2(-1)^{1+3} \begin{vmatrix} 2 & 3 \\ 0 & 5 \end{vmatrix} = (21 + 20) - (14) + 2(10) = 47$$

$$\begin{vmatrix} 1 & 1 & 2 \\ 2 & 3 & -4 \\ 0 & 5 & 7 \end{vmatrix} = (1)(-1)^{1+2} \begin{vmatrix} 2 & -4 \\ 0 & 7 \end{vmatrix} + 3(-1)^{2+2} \begin{vmatrix} 1 & 2 \\ 0 & 7 \end{vmatrix}$$

$$+5(-1)^{3+2} \begin{vmatrix} 1 & 2 \\ 2 & -4 \end{vmatrix} = (-1)(14) + 3(7) - 5(-8) = 47$$

13. (a) $\begin{vmatrix} 1 & 0 & 2 \\ 6 & -2 & 1 \\ 4 & 3 & 2 \end{vmatrix} = (1)(-1)^{1+1}\begin{vmatrix} -2 & 1 \\ 3 & 2 \end{vmatrix} + 2(-1)^{1+3}\begin{vmatrix} 6 & -2 \\ 4 & 3 \end{vmatrix} =$

$(-4-3)+2(18+8) = -7+52 = 45$

(b) $\begin{vmatrix} 4 & 7 & 0 \\ 4 & 2 & 0 \\ 3 & 6 & 2 \end{vmatrix} = (2)(-1)^{3+3}\begin{vmatrix} 4 & 7 \\ 4 & 2 \end{vmatrix} = (2)(8-28) = -40$

(c) $\begin{vmatrix} 1 & 2 & -4 \\ 0 & 1 & 0 \\ 3 & 3 & 2 \end{vmatrix} = (1)(-1)^{1+1}\begin{vmatrix} 1 & -4 \\ 3 & 2 \end{vmatrix} = 2+12 = 14$

14. (a) (i) 0 (ii) 0 (iii) 0 (iv) 0

(b) Let A be a 3×3 matrix. If two rows of A are identical, or if two columns of A are identical, then $\det(A) = 0$. In fact, for each $n \in \mathbf{Z}^+$ where $n > 1$, if A is an $n \times n$ matrix with two identical rows or two identical columns, then $\det(A) = 0$.

15. (a) (i) $\begin{vmatrix} 1 & 2 & 1 \\ 0 & -1 & -1 \\ 2 & 3 & 0 \end{vmatrix} = 2(-1)^{3+1}\begin{vmatrix} 2 & 1 \\ -1 & -1 \end{vmatrix} + 3(-1)^{3+2}\begin{vmatrix} 1 & 1 \\ 0 & -1 \end{vmatrix}$

$= 2(-2-(-1)) - 3(-1) = 2(-1)+3 = 1.$

(ii) 5 (iii) 25

(b) (i) 51 (ii) 306 (iii) 510

16. There are n^2 entries in the matrix product AB. For each entry we perform n multiplications and $n-1$ additions. Therefore, in total, we perform n^3 multiplications and $n^2(n-1) = n^3 - n^2$ additions.

APPENDIX 3
COUNTABLE AND UNCOUNTABLE SETS

1. (a) True (b) False (c) True
(d) True (e) True (f) True
(g) False: Let $A = \mathbf{Z}^+ \cup (0,1]$ and $B = (0,1]$. Then A, B are both uncountable, but $A - B = \{2, 3, 4, \ldots\}$ is countable.

2. (a) The function $f : \mathbf{Z}^+ \rightarrow A$ defined by $f(n) = n^2$ is a one-to-one correspondence.
(b) Let $g : \mathbf{Z}^+ \rightarrow \{2, 6, 10, 14, \ldots\}$ be defined by $g(n) = (n-1)4+2$. Then g is a one-to-one correspondence.

3. If B were countable, then by Theorem A3.3 it would follow that A is countable. This leads us to a contradiction since we are given that A is uncountable.

4. The set I of irrational numbers is uncountable. If not, then $\mathbf{R} = \mathbf{Q} \cup I$ would be countable — by virtue of Theorems A3.8 and A3.9 (or, A3.7).

5. Since S, T are countably infinite, we know from Theorem A3.2 that we can write $S = \{s_1, s_2, s_3, \ldots\}$ and $T = \{t_1, t_2, t_3, \ldots\}$ — two (infinite) sequences of distinct terms. Define the function

$$f : S \times T \rightarrow \mathbf{Z}^+$$

by $f(s_i, t_j) = 2^i 3^j$, for all $i, j \in \mathbf{Z}^+$. If $i, j, k, \ell \in \mathbf{Z}^+$ with $f(s_i, t_j) = f(s_k, t_\ell)$, then $f(s_i, t_j) = f(s_k, t_\ell) \Rightarrow 2^i 3^j = 2^k 3^\ell \Rightarrow i = k, j = \ell$ (By the Fundamental Theorem of Arithmetic) $\Rightarrow s_i = s_k$ and $t_j = t_\ell \Rightarrow (s_i, t_j) = (s_k, t_\ell)$. Therefore f is a one-to-one function and $S \times T \sim f(S \times T) \subset \mathbf{Z}^+$. So from Theorem A3.3 we know that $S \times T$ is countable.

6. Let p, q, r be three distinct primes. Define the function $f : \mathbf{Z}^+ \times \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ by $f(a, b, c) = p^a q^b r^c$. If $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbf{Z}^+$ with $f(a_1, b_1, c_1) = f(a_2, b_2, c_2)$, then $f(a_1, b_1, c_1) = f(a_2, b_2, c_2) \Rightarrow p^{a_1} q^{b_1} r^{c_1} = p^{a_2} q^{b_2} r^{c_2} \Rightarrow a_1 = a_2, b_1 = b_2, c_1 = c_2$ (By the Fundamental Theorem of Arithmetic) $\Rightarrow (a_1, b_1, c_1) = (a_2, b_2, c_2)$. Consequently, f is a one-to-one function and $\mathbf{Z}^+ \times \mathbf{Z}^+ \times \mathbf{Z}^+ \sim f(\mathbf{Z}^+ \times \mathbf{Z}^+ \times \mathbf{Z}^+) \subset \mathbf{Z}^+$. By Theorem A3.3 it then follows that $\mathbf{Z}^+ \times \mathbf{Z}^+ \times \mathbf{Z}^+$ is countable.

7. The function $f : (\mathbf{Z} - \{0\}) \times \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Q}$ given by $f(a, b, c) = 2^a 3^b 5^c$ is one-to-one. (Verify this!) So by Theorems A3.3 and A3.8 it follows that $(\mathbf{Z} - \{0\}) \times \mathbf{Z} \times \mathbf{Z}$ is countable. Now for all $(a, b, c) \in (\mathbf{Z} - \{0\}) \times \mathbf{Z} \times \mathbf{Z}$ there are at most two (distinct) real solutions for the quadratic equation $ax^2 + bx + c = 0$. From Theorem A3.9 it then follows that the set of all real solutions of the quadratic equations $ax^2 + bx + c = 0$, where $a, b, c \in \mathbf{Z}$ and $a \neq 0$, is countable.

8. (a) $f(x) = 3x, \quad 0 < x < 1$
(b) $g(x) = 5x + 2, \quad 0 < x < 1$
(c) $h(x) = (b - a)x + a, \quad 0 < x < 1$