1. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $3x \equiv 2 \pmod{7}$
(b) $5x + 1 \equiv 13 \pmod{23}$
(c) $5x + 1 \equiv 13 \pmod{26}$
(d) $9x \equiv 3 \pmod{5}$
(e) $5x \equiv 1 \pmod{6}$
(f) $3x \equiv 1 \pmod{6}$

2. Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

3. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

4. Describe the symmetries of a rhombus and prove that the set of symmetries forms a group. Give Cayley tables for both the symmetries of a rectangle and the symmetries of a rhombus. Are the symmetries of a rectangle and those of a rhombus the same?

5. Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

6. Give a multiplication table for the group $U(12)$.

7. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

8. Give an example of two elements A and B in $GL_2(\mathbb{R})$ with $AB \neq BA$.

9. Prove that the product of two matrices in $SL_2(\mathbb{R})$ has determinant one.

10. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

is a group under matrix multiplication. This group, known as the *Heisenberg group*, is important in quantum physics. Matrix multiplication in the Heisenberg group is defined by

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & y+y'+xz' \\ 0 & 1 & z+z' \\ 0 & 0 & 1 \end{pmatrix}.$$

11. Prove that $\det(AB) = \det(A)\det(B)$ in $GL_2(\mathbb{R})$. Use this result to show that the binary operation in the group $GL_2(\mathbb{R})$ is closed; that is, if A and B are in $GL_2(\mathbb{R})$, then $AB \in GL_2(\mathbb{R})$.

12. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on $\mathbb{Z}_2^n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Prove that $\mathbb{Z}_2^n$ is a group under this operation. This group is important in algebraic coding theory.

13. Show that $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under the operation of multiplication.

14. Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation $\circ$ on G by $(a, m) \circ (b, n) = (ab, m + n)$. Show that G is a group under this operation.

15. Prove or disprove that every group containing six elements is abelian.

16. Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$.

17. Give an example of three different groups with eight elements. Why are the groups different?

18. Show that there are $n!$ permutations of a set containing n items.

19. Show that

$$0 + a \equiv a + 0 \equiv a \pmod{n}$$

for all $a \in \mathbb{Z}_n$.

20. Prove that there is a multiplicative identity for the integers modulo n:

$$a \cdot 1 \equiv a \pmod{n}.$$

21. For each $a \in \mathbb{Z}_n$ find a $b \in \mathbb{Z}_n$ such that

$$a + b \equiv b + a \equiv 0 \pmod{n}.$$

22. Show that addition and multiplication mod n are well defined operations. That is, show that the operations do not depend on the choice of the representative from the equivalence classes mod n.

23. Show that addition and multiplication mod n are associative operations.

24. Show that multiplication distributes over addition modulo n:

$$a(b + c) \equiv ab + ac \pmod{n}.$$

25. Let a and b be elements in a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$.

26. Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

27. Prove that the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

28. Prove the remainder of Proposition 3.6: if G is a group and $a, b \in G$, then the equation $xa = b$ has unique solutions in G.

29. Prove Theorem 3.8.

30. Prove the right and left cancellation laws for a group G; that is, show that in the group G, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$ for elements $a, b, c \in G$.

31. Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

32. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$.

33. Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

34. Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$. (See Example 40 for a short description of the product of groups.)

35. Find all the subgroups of the symmetry group of an equilateral triangle.

36. Compute the subgroups of the symmetry group of a square.

37. Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$.

38. Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

39. Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

40. Let G consist of the 2×2 matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta \in \mathbb{R}$. Prove that G is a subgroup of $SL_2(\mathbb{R})$.

41. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

42. Let G be the group of 2×2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Prove that H is a subgroup of G.

43. Prove or disprove: $SL_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries and determinant one, is a subgroup of $SL_2(\mathbb{R})$.

44. List the subgroups of the quaternion group, Q_8.

45. Prove that the intersection of two subgroups of a group G is also a subgroup of G.

46. Prove or disprove: If H and K are subgroups of a group G, then $H \cup K$ is a subgroup of G.

47. Prove or disprove: If H and K are subgroups of a group G, then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G. What if G is abelian?

48. Let G be a group and $g \in G$. Show that

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

is a subgroup of G. This subgroup is called the *center* of G.

49. Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

50. Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

51. Give an example of an infinite group in which every proper subgroup is finite.

52. If $xy = x^{-1}y^{-1}$ for all x and y in G, prove that G must be abelian.

53. Prove or disprove: Every nontrivial subgroup of an nonabelian group is nonabelian.

54. Let H be a subgroup of G and

$$C(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

[width=2in]images/UPCcode.pdf images/UPCcode.png

FIGURE 1. A UPC code

Prove $C(H)$ is a subgroup of G. This subgroup is called the *centralizer* of H in G.

55. Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{g^{-1}hg : h \in H\}$ is also a subgroup of G.

Additional Exercises: Detecting Errors. Credit card companies, banks, book publishers, and supermarkets all take advantage of the properties of integer arithmetic modulo n and group theory to obtain error detection schemes for the identification codes that they use.

(1) **UPC Symbols.** Universal Product Code (UPC) symbols are found on most products in grocery and retail stores. The UPC symbol is a 12-digit code identifying the manufacturer of a product and the product itself (Figure 1). The first 11 digits contain information about the product; the twelfth digit is used for error detection. If $d_1 d_2 \cdots d_{12}$ is a valid UPC number, then

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

(a) Show that the UPC number 0-50000-30042-6, which appears in Figure 1, is a valid UPC number.
(b) Show that the number 0-50000-30043-6 is not a valid UPC number.
(c) Write a formula to calculate the check digit, d_{12}, in the UPC number.
(d) The UPC error detection scheme can detect most transposition errors; that is, it can determine if two digits have been interchanged. Show that the transposition error 0-05000-30042-6 is not detected. Find a transposition error that is detected. Can you find a general rule for the types of transposition errors that can be detected?
(e) Write a program that will determine whether or not a UPC number is valid.

(2) It is often useful to use an inner product notation for this type of error detection scheme; hence, we will use the notion

$$(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$$

to mean

$$d_1 w_1 + d_2 w_2 + \cdots + d_k w_k \equiv 0 \pmod{n}.$$

Suppose that $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ is an error detection scheme for the k-digit identification number $d_1 d_2 \cdots d_k$, where $0 \leq d_i < n$. Prove that all single-digit errors are detected if and only if $\gcd(w_i, n) = 1$ for $1 \leq i \leq k$.

(3) Let $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ be an error detection scheme for the k-digit identification number $d_1 d_2 \cdots d_k$, where $0 \leq d_i < n$. Prove that all transposition errors of two digits d_i and d_j are detected if and only if $\gcd(w_i - w_j, n) = 1$ for i and j between 1 and k.

(4) **ISBN Codes.** Every book has an International Standard Book Number (ISBN) code. This is a 10-digit code indicating the book's publisher and title. The tenth digit is a check digit satisfying

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

One problem is that d_{10} might have to be a 10 to make the inner product zero; in this case, 11 digits would be needed to make this scheme work. Therefore, the character X is used for the eleventh digit. So ISBN 3-540-96035-X is a valid ISBN code.

(a) Is ISBN 0-534-91500-0 a valid ISBN code? What about ISBN 0-534-91700-0 and ISBN 0-534-19500-0?
(b) Does this method detect all single-digit errors? What about all transposition errors?

(c) How many different ISBN codes are there?

(d) Write a computer program that will calculate the check digit for the first nine digits of an ISBN code.

(e) A publisher has houses in Germany and the United States. Its German prefix is 3-540. If its United States prefix will be 0-abc, find abc such that the rest of the ISBN code will be the same for a book printed in Germany and in the United States. Under the ISBN coding method the first digit identifies the language; German is 3 and English is 0. The next group of numbers identifies the publisher, and the last group identifies the specific book.