Solutions to Chapter 8, Susanna Epp Discrete Math 5th Edition

https://github.com/spamegg1

October 6, 2023

Contents

1 Exercise Set 8.1

1.1 Exercise 1

As in Example 8.1.2, the **congruence modulo 2** relation E is defined from $\mathbb{Z}$ to $\mathbb{Z}$ as follows: For every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, $m \; E \; n \iff m - n$ is even.

1.1.1 (a)

Is $0 \; E \; 0$? Is $5 \; E \; 2$? Is $(6, 6) \in E$? Is $(21, 7) \in E$?

Proof. $0 \; E \; 0$ because $0 - 0 = 0 = 2 \cdot 0$, so $2 \mid (0 - 0)$. $5 \not{E} \; 2$ because $5 - 2 = 3$ and $3 \neq 2k$ for any integer k, so $2 \nmid (5 - 2)$. $(6, 6) \in E$ because $6 - 6 = 0 = 2 \cdot 0$, so $2 \mid (6 - 6)$.$(-1, 7) \in E$ because $-1 - 7 = -8 = 2 \cdot (-4)$, so $2 \mid (-1 - 7)$. □

1.1.2 (b)

Prove that for any even integer n, $n \; E \; 0$.

Proof. Assume n is even. By definition of even, $n = 2k$ for some integer k. Then $n - 0 = 2k - 0 = 2k$ is also even. Therefore by definition of E, $n \; E \; 0$. □

1.2 Exercise 2

Prove that for all integers m and n, $m - n$ is even if, and only if, both m and n are even or both m and n are odd.

Proof. $\Longrightarrow$: Assume $m - n$ is even. *[We want to prove that both m and n are even or both m and n are odd.]* By definition of even, $m - n = 2k$ for some integer k. There are 4 cases:

Case 1: both m and n are even: Nothing to prove.

Case 2: both m and n are odd: Nothing to prove.

Case 3: m **is even,** n **is odd:** By definitions of even and odd, $m = 2k, n = 2l + 1$ for some integers k, l. So $m - n = 2k - 2l - 1 = 2(k - l - 1) + 1$ where $k - l - 1$ is an integer. So by definition of odd, $m - n$ is odd, a contradiction. So this case is impossible.

Case 4: m **is odd,** n **is even:** By definitions of even and odd, $m = 2k + 1, n = 2l$ for some integers k, l. So $m - n = 2k + 1 - 2l = 2(k - l) + 1$ where $k - l$ is an integer. So by definition of odd, $m - n$ is odd, a contradiction. So this case is impossible.

$\Longleftarrow$: Assume both m and n are even or both m and n are odd. *[We want to prove that $m - n$ is even.]* There are 2 cases:

Case 1: both m **and** n **are even:** By definition of even, $m = 2k, n = 2l$ for some integers k, l. Then $m - n = 2k - 2l = 2(k - l)$ where $k - l$ is an integer. So by definition, $m - n$ is even.

Case 2: both m **and** n **are odd:** By definition of even, $m = 2k + 1, n = 2l + 1$ for some integers k, l. Then $m - n = 2k + 1 - 2l - 1 = 2(k - l)$ where $k - l$ is an integer. So by definition, $m - n$ is even. □

1.3 Exercise 3

The congruence modulo 3 relation, T, is defined from $\mathbb{Z}$ to $\mathbb{Z}$ as follows: For all integers m and n, $m\ T\ n \iff 3 \mid (m - n)$.

1.3.1 (a)

Is $10\ T\ 1$? Is $1\ T\ 10$? Is $(2, 2) \in T$? Is $(8, 1) \in T$?

Proof. $10\ T\ 1$ because $10 - 1 = 9 = 3 \cdot 3$, and so $3 \mid (10 - 1)$.

$1\ T\ 10$ because $1 - 10 = -9 = 3 \cdot (-3)$, and so $3 \mid (1 - 10)$.

$2\ T\ 2$ because $2 - 2 = 0 = 3 \cdot 0$, and so $3 \mid (2 - 2)$.

$8 \not T\ 1$ because $8 - 1 = 7 \neq 3k$, for any integer k. So $3 \nmid (8 - 1)$. □

1.3.2 (b)

List five integers n such that $n\ T\ 0$.

Proof. One possible answer: 3, 6, 9, −3, −6 □

1.3.3 (c)

List five integers n such that $n\ T\ 1$.

Proof. One possible answer: 4, 7, 10, −2, −5 □

1.3.4 (d)

List five integers n such that $n\ T\ 2$.

Proof. One possible answer: 5, 8, 11, -1, -4 □

1.3.5 (e)

Make and prove a conjecture about which integers are related by T to 0, which integers are related by T to 1, and which integers are related by T to 2.

All integers of the form $3k+1$, for some integer k, are related by T to 1.

Proof. All integers of the form $3k$, for some integer k, are related by T to 0.

All integers of the form $3k+1$, for some integer k, are related by T to 1.

All integers of the form $3k+2$, for some integer k, are related by T to 2. □

1.4 Exercise 4

Define a relation P on $\mathbb{Z}$ as follows: For every ordered pair $(m,n) \in \mathbb{Z}\times\mathbb{Z}$, $m\ P\ n \iff$ m and n have a common prime factor.

1.4.1 (a)

Is 15 P 25?

Proof. Yes, because 15 and 25 are both divisible by 5, which is prime. □

1.4.2 (b)

Is 22 P 27?

Proof. No, because 22 and 27 have no common prime factor. □

1.4.3 (c)

Is 0 P 5?

Proof. Yes, because 0 and 5 are both divisible by 5, which is prime. □

1.4.4 (d)

Is 8 P 8?

Proof. Yes, because 8 and 8 are both divisible by 2, which is prime. □

1.5 Exercise 5

Let $X = \{a, b, c\}$. Recall that $\mathscr{P}(X)$ is the power set of X. Define a relation $\mathbf{S}$ on $\mathscr{P}(X)$ as follows: For all sets A and B in $\mathscr{P}(X)$, $A \ \mathbf{S} \ B \iff A$ has the same number of elements as B.

1.5.1 (a)

Is $\{a, b\}$ $\mathbf{S}$ $\{b, c\}$?

Proof. Yes, because both $\{a, b\}$ and $\{b, c\}$ have two elements. □

1.5.2 (b)

Is $\{a\}$ $\mathbf{S}$ $\{a, b\}$?

Proof. No, one has 1 element, the other has 2 elements. □

1.5.3 (c)

Is $\{c\}$ $\mathbf{S}$ $\{b\}$?

Proof. Yes, because both $\{c\}$ and $\{b\}$ have one element. □

1.6 Exercise 6

Let $X = \{a, b, c\}$. Define a relation $\mathbf{J}$ on $\mathscr{P}(X)$ as follows: For all sets A and B in $\mathscr{P}(X)$, $A \ \mathbf{J} \ B \iff A \cap B \neq \varnothing$.

1.6.1 (a)

Is $\{a\}$ $\mathbf{J}$ $\{c\}$?

Proof. No, because $\{a\} \cap \{c\} = \varnothing$. □

1.6.2 (b)

Is $\{a, b\}$ $\mathbf{J}$ $\{b, c\}$?

Proof. Yes, because $\{a, b\} \cap \{b, c\} = \{b\} \neq \varnothing$. □

1.6.3 (c)

Is $\{a, b\}$ $\mathbf{J}$ $\{a, b, c\}$?

Proof. Yes, because $\{a, b\} \cap \{a, b, c\} = \{a, b\} \neq \varnothing$. □

1.7 Exercise 7

Define a relation R on $\mathbb{Z}$ as follows: For all integers m and n, $m \; R \; n \iff 5 \mid (m^2 - n^2)$.

1.7.1 (a)

Is $1 \; R \; (-9)$?

Proof. Yes. $1 \; R \; (-9) \iff 5 \mid (1^2 - (-9)^2)$. But $1^2 - (-9)^2 = 1 - 81 = -80$, and $5 \mid (-80)$ because $-80 = 5 \cdot (-16)$. □

1.7.2 (b)

Is $2 \; R \; 13$?

Proof. Yes, $2^2 - (13)^2 = 4 - 169 = -165 = 5 \cdot (-33)$. So $5 \mid 2^2 - (13)^2$. □

1.7.3 (c)

Is $2 \; R \; (-8)$?

Proof. Yes, $2^2 - (-8)^2 = 4 - 64 = -60 = 5 \cdot (-12)$. So $5 \mid 2^2 - (-8)^2$. □

1.7.4 (d)

Is $(-8) \; R \; 2$?

Proof. Yes, $(-8)^2 - 2^2 = 64 - 4 = 60 = 5 \cdot 12$. So $5 \mid (-8)^2 - 2^2$. □

1.8 Exercise 8

Let A be the set of all strings of a's and b's of length 4. Define a relation R on A as follows: For every $s, t \in A$, $s \; R \; t \iff s$ has the same first two characters as t.

1.8.1 (a)

Is $abaa \; R \; abba$?

Proof. Yes, because both $abaa$ and $abba$ have the same first two characters ab. □

1.8.2 (b)

Is $aabb \; R \; bbaa$?

Proof. No, because the first two characters of $aabb$ are different from the first two characters of $bbaa$. □

1.8.3 (c)

Is *aaaa* R *aaab*?

Proof. Yes, because both *aaaa* and *aaab* have the same first two characters *aa*. □

1.8.4 (d)

Is *baaa* R *abaa*?

Proof. No, because the first two characters of *baaa* are different from the first two characters of *abaa*. □

1.9 Exercise 9

Let A be the set of all strings of 0's, 1's, and 2's of length 4. Define a relation R on A as follows: For every $s, t \in A$, $s \; R \; t \iff$ the sum of the characters in s equals the sum of the characters in t.

1.9.1 (a)

Is 0121 R 2200?

Proof. Yes, because the sum of the characters in 0121 is 4 and the sum of the characters in 2200 is also 4. □

1.9.2 (b)

Is 1011 R 2101?

Proof. No, because the sum of the characters in 1011 is 3, whereas the sum of the characters in 2101 is 4. □

1.9.3 (c)

Is 2212 R 2121?

Proof. No, because the sum of the characters in 2212 is 7, whereas the sum of the characters in 2121 is 6. □

1.9.4 (d)

Is 1220 R 2111?

Proof. Yes, because the sum of the characters in 1220 is 5 and the sum of the characters in 2111 is also 5. □

1.10 Exercise 10

Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let R be the "less than" relation. That is, for every ordered pair $(x, y) \in A \times B, x\,R\,y \iff x < y$. State explicitly which ordered pairs are in R and R^{-1}.

Proof. $R = \{(3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$

$R^{-1} = \{(4, 3), (5, 3), (6, 3), (5, 4), (6, 4), (6, 5)\}$ □

1.11 Exercise 11

Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and let S be the "divides" relation. That is, for every ordered pair $(x, y) \in A \times B, x\,S\,y \iff x \mid y$. State explicitly which ordered pairs are in S and S^{-1}.

Proof. $S = \{(3, 6), (4, 4), (5, 5)\}, S^{-1} = \{(6, 3), (4, 4), (5, 5)\}$ □

1.12 Exercise 12

1.12.1 (a)

Suppose a function $F : X \to Y$ is one-to-one but not onto. Is F^{-1} (the inverse relation for F) a function? Explain your answer.

Proof. No. If $F : X \to Y$ is not onto, then F fails to be defined on all of Y. In other words, there is an element y in Y such that $(y, x) \notin F^{-1}$ for any $x \in X$. Consequently, F^{-1} does not satisfy property (1) of the definition of function. □

1.12.2 (b)

Suppose a function $F : X \to Y$ is onto but not one-to-one. Is F^{-1} (the inverse relation for F) a function? Explain your answer.

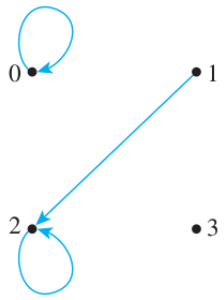
Proof. No. If $F : X \to Y$ is not one-to-one, then F for some y in Y, there will be multiple potential values for $F^{-1}(y)$. In other words, there is an element y in Y and elements $x_1, x_2 \in X$ such that $(y, x_1) \in F^{-1}$ and $(y, x_2) \in F^{-1}$. Consequently, F^{-1} does not satisfy property (2) of the definition of function. □

Draw the directed graphs of the relations defined in 13 – 18.

1.13 Exercise 13

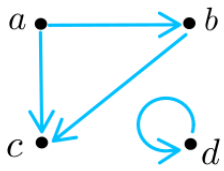
Define a relation R on $A = \{0, 1, 2, 3\}$ by $R = \{(0, 0), (1, 2), (2, 2)\}$.

Proof. □



1.14 Exercise 14

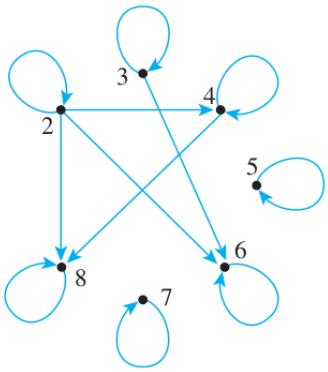
Define a relation S on $B = \{a, b, c, d\}$ by $S = \{(a, b), (a, c), (b, c), (d, d)\}$.



Proof. □

1.15 Exercise 15

Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation R on A as follows: For every $x, y \in A, x\,R\,y \iff x \mid y$.



Proof. □

1.16 Exercise 16

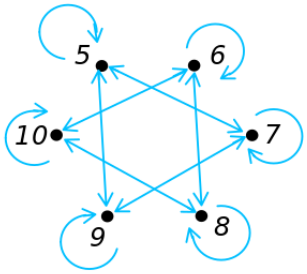
Let $A = \{5, 6, 7, 8, 9, 10\}$ and define a relation S on A as follows: For every $x, y \in A, x\,S\,y \iff 2 \mid (x - y)$.

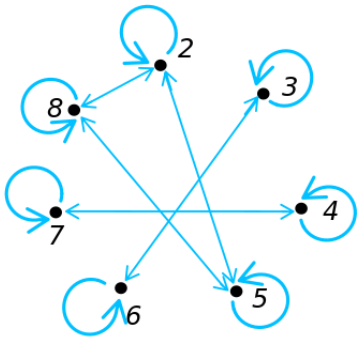
Proof. □

1.17 Exercise 17

Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as follows: For every $x, y \in A, x\,T\,y \iff 3 \mid (x - y)$.

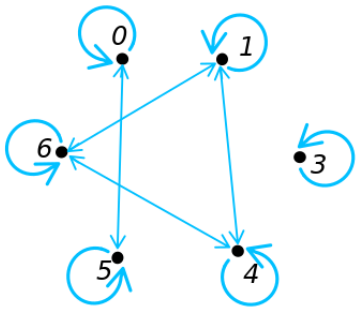
Proof. □





1.18 Exercise 18

Let $A = \{0, 1, 3, 4, 5, 6\}$ and define a relation V on A as follows: For every $x, y \in A, x\,V\,y \iff 5 \mid (x^2 - y^2)$.



Proof. □

1.19 Exercise 19

Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B, x\,R\,y \iff x \mid y$ and $x\,S\,y \iff y - 4 = x$. State explicitly which ordered pairs are in $A \times B, R, S, R \cup S$, and $R \cap S$.

Proof. $A \times B = \{(2, 6), (2, 8), (2, 10), (4, 6), (4, 8), (4, 10)\}$

$R = \{(2, 6), (2, 8), (2, 10), (4, 8)\}$, $S = \{(2, 6), (4, 8)\}$, $R \cup S = R, R \cap S = S$ □

1.20 Exercise 20

Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For every $(x, y) \in A \times B, x\,R\,y \iff |x| \mid |y|$ and $x\,S\,y \iff x - y$ is even. State explicitly which ordered pairs are in $A \times B, R, S, R \cup S$, and $R \cap S$.

Proof. $A \times B = \{(-1,1),(-1,2),(1,1),(1,2),(2,1),(2,2),(4,1),(4,2)\}$

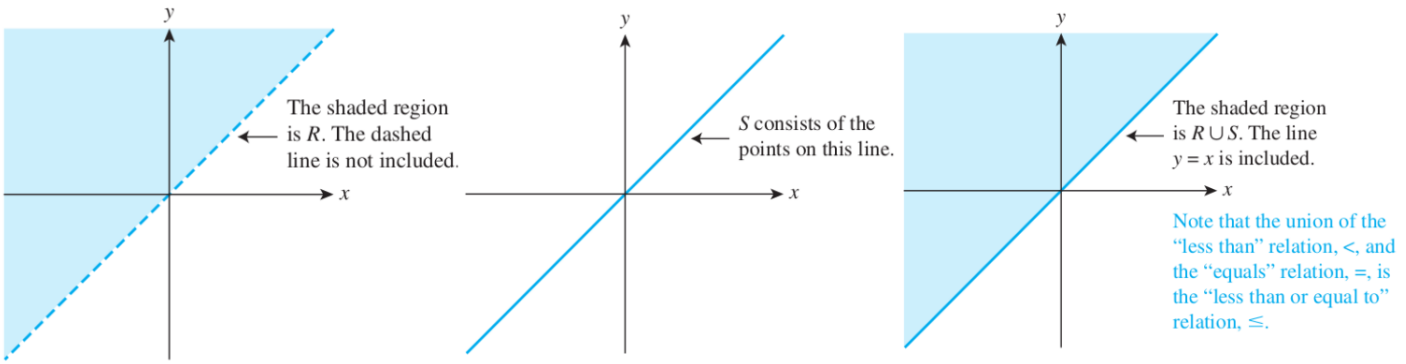
$R = \{(-1,1),(1,1),(2,2)\}$, $S = \{(-1,1),(1,1),(2,2),(4,2)\}$, $R \cup S = S, R \cap S = R$ □

1.21 Exercise 21

Define relations R and S on R as follows: $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, x < y\}$ and

$S = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, x = y\}$. That is, R is the "less than" relation and S is the "equals" relation on $\mathbb{R}$. Graph $R, S, R \cup S$, and $R \cap S$ in the Cartesian plane.

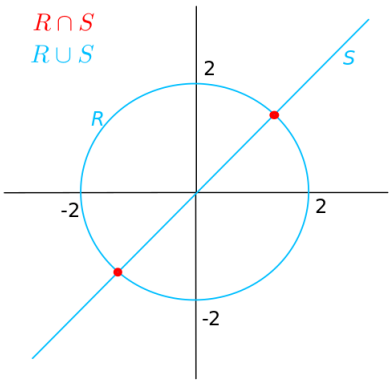
Proof. The graph of the intersection of R and S is obtained by finding the set of all points common to both graphs. But there are no points for which both $x < y$ and $x = y$. Hence $R \cap S = \varnothing$ and the graph consists of no points at all.



□

1.22 Exercise 22

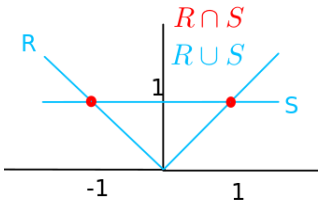
Define relations R and S on R as follows: $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, x^2 + y^2 = 4\}$ and $S = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, x = y\}$. Graph $R, S, R \cup S$, and $R \cap S$ in the Cartesian plane.



Proof. □

1.23 Exercise 23

Define relations R and S on R as follows: $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, y = |x|\}$ and $S = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, y = 1\}$. Graph $R, S, R \cup S$, and $R \cap S$ in the Cartesian plane.



Proof. □

1.24 Exercise 24

In Example 8.1.7 consider the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = X. The response to the query is the projection onto the first two coordinates of the intersection of the database with the set $A_1 \times A_2 \times A_3 \times \{X\}$.

1.24.1 (a)

Find the result of the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = pneumonia.

Proof. 574329 Tak Kurosawa, 011985 John Schmidt □

1.24.2 (b)

Find the result of the query SELECT Patient_ID#, Name FROM S WHERE Primary_Diagnosis = appendicitis.

Proof. 466581 Mary Lazars, 778400 Jamal Baskers □

2 Exercise Set 8.2

In $1-8$, a number of relations are defined on the set $A = \{0, 1, 2, 3\}$. For each relation:

a. Draw the directed graph.

b. Determine whether the relation is reflexive.

c. Determine whether the relation is symmetric.

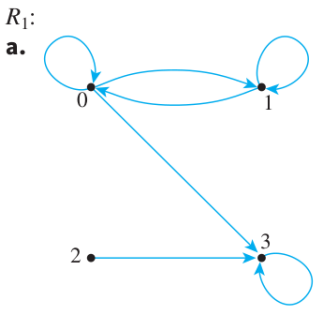
d. Determine whether the relation is transitive.

Give a counterexample in each case in which the relation does not satisfy one of the properties.

2.1 Exercise 1

$R_1 = \{(0,0), (0,1), (0,3), (1,1), (1,0), (2,3), (3,3)\}$

2.1.1 (a)



Proof. □

2.1.2 (b)

Proof. R_1 is not reflexive: $2 \not R_1 2$. □

2.1.3 (c)

Proof. R_1 is not symmetric: $2 R_1 3$ but $3 \not R_1 2$. □

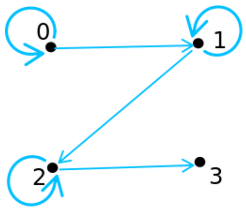
2.1.4 (d)

Proof. R_1 is not transitive: $1 R_1 0$ and $0 R_1 3$ but $1 \not R_1 3$. □

2.2 Exercise 2

$R_2 = \{(0,0), (0,1), (1,1), (1,2), (2,2), (2,3)\}$

2.2.1 (a)



Proof. □

2.2.2 (b)

Proof. R_2 is not reflexive: $3 \not R_2 3$. □

2.2.3 (c)

Proof. R_2 is not symmetric: $2 R_2 3$ but $3 \not R_2 2$. □

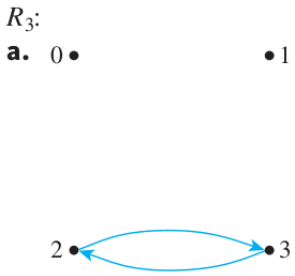
2.2.4 (d)

Proof. R_2 is not transitive: $0 R_2 1$ and $1 R_2 2$ but $0 \not R_2 2$. □

2.3 Exercise 3

$R_3 = \{(2,3),(3,2)\}$

2.3.1 (a)



Proof. □

2.3.2 (b)

Proof. R_3 is not reflexive: $0 \not R_3 0$. □

2.3.3 (c)

Proof. R_3 is symmetric. □

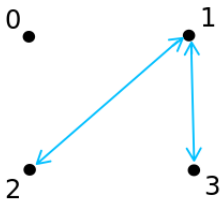
2.3.4 (d)

Proof. R_3 is not transitive: $2 R_3 3$ and $3 R_3 2$ but $2 \not R_3 2$. □

2.4 Exercise 4

$R_4 = \{(1,2),(2,1),(1,3),(3,1)\}$

2.4.1 (a)



Proof. □

2.4.2 (b)

Proof. R_4 is not reflexive: $0 \not R_4 0$. □

2.4.3 (c)

Proof. R_4 is symmetric. □

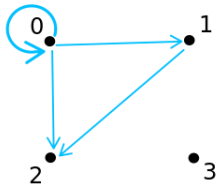
2.4.4 (d)

Proof. R_4 is not transitive: $2\,R_4\,1$ and $1\,R_4\,3$ but $2\,\not{R_4}\,3$. □

2.5 Exercise 5

$R_5 = \{(0,0),(0,1),(0,2),(1,2)\}$

2.5.1 (a)



Proof. □

2.5.2 (b)

Proof. R_5 is not reflexive: $3\,\not{R_5}\,3$. □

2.5.3 (c)

Proof. R_5 is not symmetric: $1\,R_5\,2$ but $2\,\not{R_5}\,1$. □

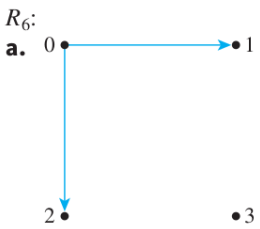
2.5.4 (d)

Proof. R_5 is transitive. □

2.6 Exercise 6

$R_6 = \{(0,1),(0,2)\}$

2.6.1 (a)



Proof. □

2.6.2 (b)

Proof. R_6 is not reflexive: $3\,\not{R_6}\,3$. □

2.6.3 (c)

Proof. R_6 is not symmetric: $0\,R_6\,1$ but $1\,\not{R_6}\,0$. □

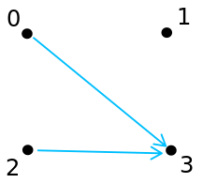
2.6.4 (d)

Proof. R_6 is transitive. □

2.7 Exercise 7

$R_7 = \{(0,3),(2,3)\}$

2.7.1 (a)



Proof. □

2.7.2 (b)

Proof. R_7 is not reflexive: $3\,\not{R_7}\,3$. □

2.7.3 (c)

Proof. R_7 is not symmetric: $0\,R_7\,3$ but $3\,\not{R_7}\,0$. □

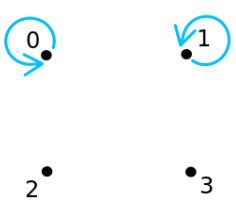
2.7.4 (d)

Proof. R_7 is transitive. □

2.8 Exercise 8

$R_8 = \{(0,0),(1,1)\}$

2.8.1 (a)



Proof. □

2.8.2 (b)

Proof. R_8 is not reflexive: $3 \not R_8 3$. □

2.8.3 (c)

Proof. R_8 is symmetric. □

2.8.4 (d)

Proof. R_8 is transitive. □

In 9–33, determine whether the given relation is reflexive, symmetric, transitive, or none of these. Justify your answers.

2.9 Exercise 9

R is the "greater than or equal to" relation on the set of real numbers: For every $x, y \in \mathbb{R}, x\,R\,y \iff x \geq y$.

Proof. ***R* is reflexive:** R is reflexive iff for every real number $x, x\,R\,x$. By definition of R, this means that for every real number $x, x \geq x$. In other words, for every real number $x, x > x$ or $x = x$, which is true.

***R* is not symmetric:** R is symmetric iff for all real numbers x and y, if $x\,R\,y$ then $y\,R\,x$. By definition of R, this means that for all real numbers x and y, if $x \geq y$ then $y \geq x$. The following counterexample shows that this is false. $x = 1$ and $y = 0$. Then $x \geq y$, but $y \not\geq x$ because $1 \geq 0$ and $0 \not\geq 1$.

***R* is transitive:** R is transitive iff for all real numbers x, y, and z, if $x\,R\,y$ and $y\,R\,z$ then $x\,R\,z$. By definition of R, this means that for all real numbers x, y, and z, if $x \geq y$ and $y \geq z$ then $x \geq z$. This is true by definition of $\geq$ and the transitive property of order for the real numbers. (See Appendix A, T18.) □

2.10 Exercise 10

C is the circle relation on the set of real numbers: For every $x, y \in \mathbb{R}, x\,C\,y \iff x^2 + y^2 = 1$.

Proof. ***C* is not reflexive:** Let $x = 0$. Then $0^2 + 0^2 = 0 \neq 1$, therefore $0 \not C 0$.

***C* is symmetric:** Assume $x\,C\,y$. Then $x^2 + y^2 = 1$. So $y^2 + x^2 = 1$. So $y\,C\,x$.

***C* is not transitive:** Let $x = 1, y = 0, z = 1$. Then $x\,C\,y$ because $1^2 + 0^2 = 1$, and $y\,C\,z$ because $0^2 + 1^2 = 1$. However $x \not C\, z$ because $1^2 + 1^2 = 2 \neq 1$. □

2.11 Exercise 11

D is the relation defined on $\mathbb{R}$ as follows: For every $x, y \in \mathbb{R}, x\,D\,y \iff xy \geq 0$.

Proof. ***D* is reflexive:** For all real numbers $x, x \cdot x = x^2 \geq 0$ so $x\,D\,x$.

***D* is symmetric:** Assume $x\,D\,y$. Then $xy \geq 0$. So $yx \geq 0$. So $y\,D\,x$.

***D* is not transitive:** Let $x = 1, y = 0, z = -1$. Then $xy = 0 \geq 0$ so $x\,D\,y$, and $yz = 0 \geq 0$ so $y\,D\,z$, but $xz = -1 \ngeq 0$ so $x \not D z$. □

2.12 Exercise 12

E is the congruence modulo 4 relation on $\mathbb{Z}$: For every $m, n \in \mathbb{Z}, m\,E\,n \iff 4 \mid (m-n)$.

Proof. ***E* is reflexive:** For all $m \in \mathbb{Z}, (m - m) = 0 = 4 \cdot 0$ so $4 \mid (m - m)$ thus $m\,E\,m$.

***E* is symmetric:** Assume $m\,E\,n$. Then $4 \mid (m - n)$. So $m - n = 4 \cdot k$ for some integer k. So $n - m = 4 \cdot (-k)$ where $-k$ is an integer. So $4 \mid (n - m)$ and $n\,E\,m$.

***E* is transitive:** Assume $m\,E\,n$ and $n\,E\,o$. Then $4 \mid (m - n)$ and $4 \mid (n - o)$. So $m - n = 4k$ and $n - o = 4l$ for some integers k, l. So $m - o = (m - n) + (n - o) = 4k + 4l = 4(k + l)$ where $k + l$ is an integer. Thus $4 \mid (m - o)$ and $m\,E\,o$. □

2.13 Exercise 13

F is the congruence modulo 5 relation on $\mathbb{Z}$: For every $m, n \in \mathbb{Z}, m\,F\,n \iff 5 \mid (m-n)$.

Proof. ***F* is reflexive:** The proof is the same as in exercise 12.

***F* is symmetric:** The proof is the same as in exercise 12.

***F* is transitive:** The proof is the same as in exercise 12. □

2.14 Exercise 14

O is the relation defined on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}, m\,O\,n \iff m - n$ is odd.

Proof. ***O* is not reflexive:** $0 - 0 = 0$ is even, therefore $0 \not O 0$.

***O* is symmetric:** Assume $m\,O\,n$. So $m - n$ is odd. So $m - n = 2k + 1$ for some integer k. So $n - m = -2k - 1 = 2(-k - 1) + 1$ where $-k - 1$ is an integer. So $n - m$ is odd and $n\,O\,m$.

***O* is not transitive:** $2 - 1 = 1$ is odd so $2\,O\,1$, and $1 - 0 = 1$ is odd so $1\,O\,0$, but $2 - 0 = 2$ is even so $2 \not O 0$. □

2.15 Exercise 15

D is the "divides" relation on Z^+: For all positive integers m and $n, m\,D\,n \iff m \mid n$.

Proof. **D is reflexive:** For all $m \in \mathbb{Z}^+$ $m = m \cdot 1$ therefore $m \mid m$, so $m\,D\,m$.

D is not symmetric: $3\,D\,6$ because $3 \mid 6$ because $6 = 3 \cdot 2$, but $6 \not D 3$ because $6 \nmid 3$ since $3/6 = 1/2$ is not an integer.

D is transitive: Assume $m\,D\,n$ and $n\,D\,o$. Then $m \mid n$ and $n \mid o$. So $n = mk$ and $o = nl$ for some integers k, l. So $o = nl = (mk)l = m(kl)$ where kl is an integer. So $m \mid o$ and $m\,D\,o$. □

2.16 Exercise 16

A is the "absolute value" relation on $\mathbb{R}$: For all real numbers x and y, $x\,A\,y \iff |x| = |y|$.

Proof. **A is reflexive:** For all real numbers x, $|x| = |x|$ so $x\,A\,x$.

A is symmetric: Assume $x\,A\,y$ so $|x| = |y|$. Then $|y| = |x|$ so $y\,A\,x$.

A is transitive: Assume $x\,A\,y$ and $y\,A\,z$, so $|x| = |y|$ and $|y| = |z|$. Then $|x| = |y| = |z|$ so $x\,A\,z$. □

2.17 Exercise 17

Recall that a prime number is an integer that is greater than 1 and has no positive integer divisors other than 1 and itself. (In particular, 1 is not prime.) A relation P is defined on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}, m\,P\,n \iff \exists$ a prime number p such that $p \mid m$ and $p \mid n$.

Proof. **P is not reflexive:** There is no prime number p such that $p \mid 1$ and $p \mid 1$. Thus $1 \not P 1$.

P is symmetric: Assume $m\,P\,n$. So there is a prime number p such that $p \mid m$ and $p \mid n$. So $p \mid n$ and $p \mid m$, and thus $n\,P\,m$.

P is not transitive: Let $m = 6, n = 15, o = 35$. Then the prime $p = 3$ divides both m and n, so $m\,P\,n$, and the prime $q = 5$ divides both n and o, so $n\,P\,o$, but there is no prime that divides both $m = 2 \cdot 3$ and $o = 5 \cdot 7$, so $m \not P o$. □

2.18 Exercise 18

Define a relation Q on $\mathbb{R}$ as follows: For all real numbers x and y, $x\,Q\,y \iff x - y$ is rational.

Proof. **Q is reflexive:** For all reals $x \in \mathbb{R}, x - x = 0$ and 0 is rational, so $x\,Q\,x$.

***Q* is symmetric:** Assume $x\,Q\,y$. Then $x-y$ is rational. Then $y-x=-(x-y)$ is rational (being the negative of a rational). So $y\,Q\,x$.

***Q* is transitive:** Assume $x\,Q\,y$ and $y\,Q\,z$. Then $x-y$ and $y-z$ are rational. So $x-z=(x-y)+(y-z)$ is also rational (being the sum of two rationals). Thus $x\,Q\,z$. □

2.19 Exercise 19

Define a relation I on $\mathbb{R}$ as follows: For all real numbers x and y, $x\,I\,y \iff x-y$ is irrational.

Proof. ***I* is not reflexive:** For all reals $x\in\mathbb{R}, x-x=0$ and 0 is not irrational, so $x\not I x$.

***I* is symmetric:** Assume $x\,I\,y$. Then $x-y$ is irrational. So $y-x=-(x-y)$ is irrational (being the negative of an irrational). So $y\,I\,x$.

***I* is not transitive:** Let $x=\sqrt{2}, y=0, z=\sqrt{2}$. Then $x\,I\,y$ because $x-y=\sqrt{2}$ is irrational. Also $y\,I\,z$ because $y-z=-\sqrt{2}$ is irrational. But $x-z=0$ is not irrational, thus $x\not I z$. □

2.20 Exercise 20

Let $X=\{a,b,c\}$ and $\mathscr{P}(X)$ be the power set of X (the set of all subsets of X). A relation $\mathbf{E}$ is defined on $\mathscr{P}(X)$ as follows: For every $A,B\in\mathscr{P}(X), A\,\mathbf{E}\,B \iff$ the number of elements in A equals the number of elements in B.

Proof. **E is reflexive:** For every $A\in\mathscr{P}(X)$, the number of elements in A equals the number of elements in A. So $A\,\mathbf{E}\,A$.

E is symmetric: Assume $A\,\mathbf{E}\,B$. Then the number of elements in A equals the number of elements in B. So, the number of elements in B equals the number of elements in A. So $B\,\mathbf{E}\,A$.

E is transitive: Assume $A\,\mathbf{E}\,B$ and $B\,\mathbf{E}\,C$. Then the number of elements in A equals the number of elements in B, and the number of elements in B equals the number of elements in C. So the number of elements in A equals the number of elements in C. So $A\,\mathbf{E}\,C$. □

2.21 Exercise 21

Let $X=\{a,b,c\}$ and $\mathscr{P}(X)$ be the power set of X. A relation $\mathbf{L}$ is defined on $\mathscr{P}(X)$ as follows: For every $A,B\in\mathscr{P}(X), A\,\mathbf{L}\,B \iff$ the number of elements in A is less than the number of elements in B.

Proof. **L is not reflexive:** For all $A\in\mathscr{P}(X)$, the number of elements in A is not less than the number of elements in A. So $A\not\mathbf{L}\,A$.

L is not symmetric: Let $A = \varnothing, B = \{a\}$. Then the number of elements in A (which is 0) is less than the number of elements in B (which is 1). So $A \,\mathbf{L}\, B$. But the number of elements in B (which is 1) is not less than the number of elements in A (which is 0). So $B \not\mathbf{L} A$.

L is transitive: Assume $A \,\mathbf{L}\, B$ and $B \,\mathbf{L}\, C$. Then the number of elements in A is less than the number of elements in B, and the number of elements in B is less than the number of elements in C. Then the number of elements in A is less than the number of elements in C. So $A \,\mathbf{L}\, C$. □

2.22 Exercise 22

Let $X = \{a, b, c\}$ and $\mathscr{P}(X)$ be the power set of X. A relation $\mathbf{N}$ is defined on $\mathscr{P}(X)$ as follows: For every $A, B \in \mathscr{P}(X), A\mathbf{N}B \iff$ the number of elements in A is not equal to the number of elements in B.

Proof. **N is not reflexive:** Let $A = \{a\}$ which has 1 element. Then the number of elements in A is equal to the number of elements in A. So $A \not\mathbf{N} A$.

N is symmetric: Assume $A \,\mathbf{N}\, B$. Then the number of elements in A is not equal to the number of elements in B. So the number of elements in B is not equal to the number of elements in A, and $B \,\mathbf{N}\, A$.

N is not transitive: Let $A = \{a\}, B = \varnothing, C = \{c\}$. Then $A \,\mathbf{N}\, B$ because A has 1 element and B has 0 elements, and $0 \neq 1$. Similarly $B \,\mathbf{N}\, C$. But $A \not\mathbf{N} C$ because both A and C have 1 element, and $1 = 1$. □

2.23 Exercise 23

Let X be a nonempty set and $\mathscr{P}(X)$ the power set of X. Define the "subset" relation $\mathbf{S}$ on $\mathscr{P}(X)$ as follows: For every $A, B \in \mathscr{P}(X), A \,\mathbf{S}\, B \iff A \subseteq B$.

Proof. **S is reflexive:** For all $A \in \mathscr{P}(X), A \subseteq A$ therefore $A \,\mathbf{S}\, A$.

S is not symmetric: Let $A = \{a\}, B = \{a, b\}$. Then $A \subseteq B$, so $A \,\mathbf{S}\, B$. But $B \nsubseteq A$ therefore $B \not\mathbf{S} A$.

S is transitive: Assume $A \,\mathbf{S}\, B$ and $B \,\mathbf{S}\, C$. So $A \subseteq B$ and $B \subseteq C$. Then by transitivity of subsets, $A \subseteq C$, and $A \,\mathbf{S}\, C$. □

2.24 Exercise 24

Let X be a nonempty set and $\mathscr{P}(X)$ the power set of X. Define the "not equal to" relation $\mathbf{U}$ on $\mathscr{P}(X)$ as follows: For every $A, B \in \mathscr{P}(X), A\mathbf{U}B \iff A \neq B$.

Proof. **U is not reflexive:** For every $A \in \mathscr{P}(X), A = A$ therefore $A \not\mathbf{U} A$.

U is symmetric: Assume $A \,\mathbf{U}\, B$. Then $A \neq B$. So $B \neq A$, and $B \,\mathbf{U}\, A$.

U is not transitive: Let $X = \{x\}, A = \{x\}, B = \varnothing, C = \{x\}$. Then $A \,\mathbf{U}\, B$ because $A \neq B$, and $B \,\mathbf{U}\, C$ because $B \neq C$, but $A = C$ so $A \not\mathbf{U} C$. □

2.25 Exercise 25

Let A be the set of all strings of a's and b's of length 4. Define a relation R on A as follows: For every $s, t \in A, s \,R\, t \iff s$ has the same first two characters as t.

Proof. ***R* is reflexive:** For every string $s \in A$, s has the same first two characters as s. Thus $s \,R\, s$.

***R* is symmetric:** Assume $s \,R\, t$. Then s has the same first two characters as t. Then t has the same first two characters as s, so $t \,R\, s$.

***R* is transitive:** Assume $s \,R\, t$ and $t \,R\, r$. Then s has the same first two characters as t, and t has the same first two characters as r. So s has the same first two characters as r, and $s \,R\, r$. □

2.26 Exercise 26

Let A be the set of all strings of 0's, 1's, and 2's that have length 4 and for which the sum of the characters in the string is less than or equal to 2. Define a relation R on A as follows: For every $s, t \in A, s \,R\, t \iff$ the sum of the characters of s equals the sum of the characters of t.

Proof. ***R* is reflexive:** For every $s, \in A$, the sum of the characters of s equals the sum of the characters of s. So $s \,R\, s$.

***R* is symmetric:** Assume $s \,R\, t$. Then the sum of the characters of s equals the sum of the characters of t. So the sum of the characters of t equals the sum of the characters of s, and $s \,R\, t$.

***R* is transitive:** Assume $s \,R\, t$ and $t \,R\, r$. Then the sum of the characters of s equals the sum of the characters of t, and the sum of the characters of t equals the sum of the characters of r. So the sum of the characters of s equals the sum of the characters of r, and $s \,R\, r$. □

2.27 Exercise 27

Let A be the set of all English statements. A relation $\mathbf{I}$ is defined on A as follows: For every $p, q \in A, p \,\mathbf{I}\, q \iff p \implies q$ is true.

Proof. **I is reflexive:** For every $p \in A, p \implies p$ is true, therefore $p \,\mathbf{I}\, p$.

I is not symmetric: Let p be "$1 is greater than 2$" and let q be "2 is greater than 1". So p is false and q is true. Therefore $p \implies q$ is true and $q \implies p$ is false. So $p \,\mathbf{I}\, q$ but $q \not\mathbf{I}\, p$.

I is transitive: Assume $p\,\mathbf{I}\,q$ and $q\,\mathbf{I}\,r$. So $p \implies q$ is true and $q \implies r$ is true. By transitivity of implication, $p \implies r$ is true, and $p\,\mathbf{I}\,r$. □

2.28 Exercise 28

Let $A = \mathbb{R} \times \mathbb{R}$. A relation $\mathbf{F}$ is defined on A as follows: For every (x_1, y_1) and (x_2, y_2) in A, $(x_1, y_1)\mathbf{F}(x_2, y_2) \iff x_1 = x_2$.

Proof. **F is reflexive:** For every $(x, y) \in A, x = x$, therefore $(x, y)\mathbf{F}(x, y)$.

F is symmetric: Assume $(x_1, y_1)\mathbf{F}(x_2, y_2)$. Then $x_1 = x_2$. Then $x_2 = x_1$. So $(x_2, y_2)\mathbf{F}(x_1, y_1)$.

F is transitive: Assume $(x_1, y_1)\mathbf{F}(x_2, y_2)$ and $(x_2, y_2)\mathbf{F}(x_3, y_3)$. Then $x_1 = x_2$ and $x_2 = x_3$. Thus $x_1 = x_3$ and so $(x_1, y_1)\mathbf{F}(x_3, y_3)$. □

2.29 Exercise 29

Let $A = \mathbb{R} \times \mathbb{R}$. A relation $\mathbf{S}$ is defined on A as follows: For every (x_1, y_1) and (x_2, y_2) in $A, (x_1, y_1)\mathbf{S}(x_2, y_2) \iff y_1 = y_2$.

Proof. **S is reflexive:**

S is symmetric:

S is transitive: □

2.30 Exercise 30

Let A be the "punctured plane"; that is, A is the set of all points in the Cartesian plane except the origin (0, 0). A relation R is defined on A as follows: For every p_1 and p_2 in $A, p_1\,R\,p_2 \iff p_1$ and p_2 lie on the same half line emanating from the origin.

Proof. ***R* is reflexive:** For all $p \in A, p$ and p lie on the same half line emanating from the origin. So $p\,R\,p$.

***R* is symmetric:** Assume $p_1\,R\,p_2$. Then p_1 and p_2 lie on the same half line emanating from the origin. Then p_2 and p_1 lie on the same half line emanating from the origin. So $p_2\,R\,p_1$.

***R* is transitive:** First notice that for any $p \in A$ there is exactly one half line emanating from the origin on which p lies.

Assume $p_1\,R\,p_2$ and $p_2\,R\,p_3$. Then p_1 and p_2 lie on the same half line emanating from the origin, say l_1. And p_2 and p_3 lie on the same half line emanating from the origin, say l_2. Since p_2 lies on both l_1 and l_2, by the previous paragraph $l_1 = l_2$. Then p_1 and p_3 lie on the same half line emanating from the origin. So $p_1\,R\,p_3$. □

2.31 Exercise 31

Let A be the set of people living in the world today. A relation R is defined on A as follows: For all people p and q in $A, p\,R\,q \iff p$ lives within 100 miles of q.

Proof. **R is reflexive:** For every person p, p lives within 0 miles of p, so in particular p lives within 100 miles of p. Therefore $p\,R\,p$.

R is symmetric: Assume $p\,R\,q$. So p lives within 100 miles of q. Then q lives within 100 miles of p. Thus $q\,R\,p$.

R is not transitive: As a counterexample, take p to be an inhabitant of Chicago, Illinois, q an inhabitant of Kankakee, Illinois, and r an inhabitant of Champaign, Illinois. Then $p\,R\,q$ because Chicago is less than 100 miles from Kankakee, and $q\,R\,r$ because Kankakee is less than 100 miles from Champaign, but $p \not R\, r$ because Chicago is not less than 100 miles from Champaign. □

2.32 Exercise 32

Let A be the set of all lines in the plane. A relation R is defined on A as follows: For every l_1 and l_2 in $A, l_1\,R\,l_2 \iff l_1$ is parallel to l_2. (Assume that a line is parallel to itself.)

Proof. **R is reflexive:** For every line $l \in A, l$ is parallel to itself, therefore $l\,R\,l$.

R is symmetric: Assume $l_1\,R\,l_2$. Then l_1 is parallel to l_2. Then l_2 is parallel to l_1, so $l_2\,R\,l_1$.

R is transitive: Assume $l_1\,R\,l_2$ and $l_2\,R\,l_3$. Then l_1 is parallel to l_2 and l_2 is parallel to l_3. By transitivity of parallelism l_1 is parallel to l_3 so $l_1\,R\,l_3$. □

2.33 Exercise 33

Let A be the set of all lines in the plane. A relation R is defined on A as follows: For every l_1 and l_2 in $A, l_1\,R\,l_2 \iff l_1$ is perpendicular to l_2.

Proof. **R is not reflexive:** For evert line l in A, l is not perpendicular to itself (l is parallel to itself). Therefore $l \not R\, l$.

R is symmetric: Assume $l_1\,R\,l_2$. Then l_1 is perpendicular to l_2. Then l_2 is perpendicular to l_1. So $l_2\,R\,l_1$.

R is not transitive: Let l_1 be the line $y = 0$, let l_2 be the line $x = 0$ and l_3 be the line $y = 1$. Then l_2 is perpendicular to both l_1 and l_3 so $l_1\,R\,l_2$ and $l_2\,R\,l_3$. But l_1 is parallel to l_3 so $l_1 \not R\, l_3$. □

In 34 – 36, assume that R is a relation on a set A. Prove or disprove each statement.

2.34 Exercise 34

If R is reflexive, then R^{-1} is reflexive.

Proof. Suppose R is any reflexive relation on a set A. *[We must show that R^{-1} is reflexive. To show this, we must show that for every x in A, $x\,R^{-1}x$.]* Given any element x in A, since R is reflexive, $x\,R\,x$, and by definition of relation, this means that $(x, x) \in R$. It follows, by definition of the inverse of a relation, that $(x, x) \in R^{-1}$, and so, by definition of relation, $x\,R^{-1}\,x$ *[as was to be shown].* □

2.35 Exercise 35

If R is symmetric, then R^{-1} is symmetric.

Proof. Assume R is symmetric. *[We want to show R^{-1} is symmetric.]* Assume $x\,R^{-1}\,y$. We need to show $y\,R^{-1}\,x$. By definition of R^{-1}, $y\,R\,x$. Since R is symmetric, $x\,R\,y$. By definition of R^{-1} again, $y\,R^{-1}\,x$. □

2.36 Exercise 36

If R is transitive, then R^{-1} is transitive.

Proof. Assume R is transitive. *[We want to show R^{-1} is transitive.]* Assume $x\,R^{-1}\,y$ and $y\,R^{-1}\,z$. We need to show $x\,R^{-1}\,z$. By definition of R^{-1}, $y\,R\,x$ and $z\,R\,y$. Since R is transitive, $z\,R\,x$. By definition of R^{-1} again, $x\,R^{-1}\,z$. □

In 37 – 42, assume that R and S are relations on a set A. Prove or disprove each statement.

2.37 Exercise 37

If R and S are reflexive, is $R \cap S$ reflexive? Why?

Proof. Yes. Suppose R and S are reflexive. *[To show that $R \cap S$ is reflexive, we must show that $\forall x \in A, (x, x) \in R \cap S$.]* So suppose $x \in A$. Since R is reflexive, $(x, x) \in R$, and since S is reflexive, $(x, x) \in S$. Thus, by definition of intersection, $(x, x) \in R \cap S$ *[as was to be shown].* □

2.38 Exercise 38

If R and S are symmetric, is $R \cap S$ symmetric? Why?

Proof. Yes. Suppose R and S are symmetric. *[To show that $R \cap S$ is symmetric, we must show that $\forall x, y \in A$, if $(x, y) \in R \cap S$ then $(y, x) \in R \cap S$.]* So suppose $x, y \in A$ and $(x, y) \in R \cap S$. By definition of intersection $(x, y) \in R$ and $(x, y) \in S$. Since R is symmetric, $(y, x) \in R$, and since S is symmetric, $(y, x) \in S$. Thus, by definition of intersection, $(y, x) \in R \cap S$ *[as was to be shown].* □

2.39 Exercise 39

If R and S are transitive, is $R \cap S$ transitive? Why?

Proof. Yes. Suppose R and S are transitive. *[To show that $R \cap S$ is transitive, we must show that $\forall x, y, z \in A$, if $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$ then $(x, z) \in R \cap S$.]* So suppose $x, y, z \in A$ and $(x, y) \in R \cap S$ and $(y, z) \in R \cap S$. By definition of intersection $(x, y) \in R$ and $(x, y) \in S$ and $(y, z) \in R$ and $(y, z) \in S$. Since R is transitive, $(x, z) \in R$, and since S is transitive, $(x, z) \in S$. Thus, by definition of intersection, $(x, z) \in R \cap S$ *[as was to be shown].* □

2.40 Exercise 40

If R and S are reflexive, is $R \cup S$ reflexive? Why?

Proof. Yes. To prove this we must show that for all x in A, $(x, x) \in R \cup S$. So suppose x is a particular but arbitrarily chosen element in A. *[We must show that $(x, x) \in R \cup S$.]* Then $(x, x) \in R$ because R is reflexive, and hence $(x, x) \in R \cup S$ by definition of union, *[as was to be shown].* □

2.41 Exercise 41

If R and S are symmetric, is $R \cup S$ symmetric? Why?

Proof. Yes. To prove this we must show that for all x and y in A, if $(x, y) \in R \cup S$ then $(y, x) \in R \cup S$. So suppose (x, y) is a particular but arbitrarily chosen element in $R \cup S$. *[We must show that $(y, x) \in R \cup S$.]* By definition of union, $(x, y) \in R$ or $(x, y) \in S$. In case $(x, y) \in R$, then $(y, x) \in R$ because R is symmetric, and hence $(y, x) \in R \cup S$ by definition of union. In case $(x, y) \in S$ then $(y, x) \in S$ because S is symmetric, and hence $(y, x) \in R \cup S$ by definition of union. Thus, in both cases, $(y, x) \in R \cup S$ *[as was to be shown].* □

2.42 Exercise 42

If R and S are transitive, is $R \cup S$ transitive? Why?

Proof. No. Let $A = \{a, b, c, d\}, R = \{(a, b), (b, c), (a, c)\}, S = \{(c, a), (a, d), (c, d)\}$. Then R and S are transitive but $R \cup S$ is not: $(a, c) \in R \cup S$ and $(c, a) \in R \cup S$ but $(a, a) \notin R \cup S$. □

In $43 - 50$, the following definitions are used: a relation on a set A is defined to be irreflexive if, and only if, for every $x \in A, x \not R x$; asymmetric if, and only if, for every $x, y \in A$ if $x \, R \, y$ then $y \not R x$; intransitive if, and only if, for every $x, y, z \in A$, if xRy and yRz then $x \not R z$. For each of the relations in the referenced exercise, determine whether the relation is irreflexive, asymmetric, intransitive, or none of these.

2.43 Exercise 43

Exercise 1

Proof. R_1 is not irreflexive because $(0,0) \in R_1$. R_1 is not asymmetric because $(0,1) \in R_1$ and $(1,0) \in R_1$. R_1 is not intransitive because $(0,1) \in R_1$ and $(1,0) \in R_1$ and $(0,0) \in R_1$. □

2.44 Exercise 44

Exercise 2

Proof. Recall $R_2 = \{(0,0),(0,1),(1,1),(1,2),(2,2),(2,3)\}$.

R_2 is not irreflexive because $(0,0) \in R_2$.

R_2 is not asymmetric because $(0,0) \in R_2$ and $(0,0) \in R_2$.

R_2 is not intransitive because $(0,0) \in R_2$ and $(0,1) \in R_2$ and $(0,1) \in R_2$. □

2.45 Exercise 45

Exercise 3

Proof. R_3 is irreflexive because no element of A is related by R_3 to itself. R_3 is not asymmetric because $(2,3) \in R_3$ and $(3,2) \in R_3$. R_3 is intransitive. To see why, observe that R_3 consists only of $(2,3)$ and $(3,2)$. Now $(2,3) \in R_3$ and $(3,2) \in R_3$ but $(2,2) \notin R_3$. Also $(3,2) \in R_3$ and $(2,3) \in R_3$ but $(3,3) \notin R_3$. □

2.46 Exercise 46

Exercise 4

Proof. Recall $R_4 = \{(1,2),(2,1),(1,3),(3,1)\}$.

R_4 is irreflexive.

R_4 is not asymmetric because $(1,2) \in R_4$ and $(2,1) \in R_4$.

R_4 is intransitive. □

2.47 Exercise 47

Exercise 5

Proof. Recall $R_5 = \{(0,0),(0,1),(0,2),(1,2)\}$.

R_5 is not irreflexive because $(0,0) \in R_5$.

R_5 is not asymmetric because $(0,0) \in R_5$ and $(0,0) \in R_5$.

R_5 is not intransitive because $(0,1) \in R_5$ and $(1,2) \in R_5$ and $(0,2) \in R_5$. □

2.48 Exercise 48

Exercise 6

Proof. Recall $R_6 = \{(0,1),(0,2)\}$. R_6 is irreflexive because no element of A is related by R_6 to itself. R_6 is asymmetric because R_6 consists only of $(0,1)$ and $(0,2)$ and neither $(1,0)$ nor $(2,0)$ is in R_6. R_6 is intransitive. □

2.49 Exercise 49

Exercise 7

Proof. Recall $R_7 = \{(0,3),(2,3)\}$.

R_7 is irreflexive, asymmetric and intransitive. □

2.50 Exercise 50

Exercise 8

Proof. Recall $R_8 = \{(0,0),(1,1)\}$. R_8 is not irreflexive because $(0,0) \in R_8$. R_8 is not asymmetric because $(0,0) \in R_8$ and $(0,0) \in R_8$. R_8 is intransitive. □

In $51-53$, R, S, and T are relations defined on $A = \{0,1,2,3\}$.

2.51 Exercise 51

Let $R = \{(0,1),(0,2),(1,1),(1,3),(2,2),(3,0)\}$. Find R^t, the transitive closure of R.

Proof. $R^t = R \cup \{(0,0),(0,3),(1,0),(3,1),(3,2),(3,3),(0,2),(1,2)\} =$

$\{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,2),(3,0),(3,1),(3,2),(3,3)\}$. □

2.52 Exercise 52

Let $S = \{(0,0),(0,3),(1,0),(1,2),(2,0),(3,2)\}$. Find S^t, the transitive closure of S.

Proof. $S^t = S \cup \{(0,2),(1,3),(2,2),(2,3),(3,3)\}$

$= \{(0,0),(0,2),(0,3),(1,0),(1,2),(1,3),(2,0),(2,2),(2,3),(3,2),(3,3)\}$ □

2.53 Exercise 53

Let $T = \{(0,2),(1,0),(2,3),(3,1)\}$. Find T^t, the transitive closure of T.

Proof. $T^t = T \cup \{(0,3),(0,1),(0,0),(1,2),(1,3),(1,1),(2,1),(2,0),(2,2),(3,0),(3,2),$

$(3,3)\} = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),(2,0),(2,1),(2,2),(2,3),$

$(3,0),(3,1),(3,2),(3,1)\}$ □

2.54 Exercise 54

Write a computer algorithm to test whether a relation R defined on a finite set A is reflexive, where $A = \{a[1], a[2], \ldots, a[n]\}$.

Algorithm: Test for Reflexivity
[The input for this algorithm is a binary relation R defined on a set A, that is represented as the one- dimensional array $a[1], a[2], \ldots, a[n]$. To test whether R is reflexive, a variable called answer is initially set equal to "yes," and each element $a[i]$ of A is examined in turn to see whether it is related by R to itself. If any element is not related to itself by R, then answer is set equal to "no," the while loop is not repeated, and processing terminates.]

Input: *n [a positive integer], $a[1], a[2], \ldots, a[n]$ [a one-dimensional array representing a set A], R [a subset of $A \times A$]*
Algorithm Body:
    $i := 1$, answer := "yes"
    while (answer = "yes" and $i \leq n$)
        if $(a[i], a[i]) \notin R$ **then** answer := "no"
        $i := i + 1$
    end while
Output: answer *[a string]*

2.55 Exercise 55

Write a computer algorithm to test whether a relation R defined on a finite set A is symmetric, where $A = \{a[1], a[2], \ldots, a[n]\}$.

Algorithm: Test for Symmetry
Input: *n [a positive integer], $a[1], a[2], \ldots, a[n]$ [a one-dimensional array representing a set A], R [a subset of $A \times A$]*
Algorithm Body:
    $i := 1, j := 1$, answer := "yes"
    while (answer = "yes" and $i \leq n$)
        while (answer = "yes" and $j \leq n$)
            if $(a[i], a[j]) \in R$ and $(a[j], a[i]) \notin R$ **then** answer := "no"
            $j := j + 1$
        end while
        $i := i + 1$
    end while
Output: answer *[a string]*

2.56 Exercise 56

Write a computer algorithm to test whether a relation R defined on a finite set A is transitive, where $A = \{a[1], a[2], \ldots, a[n]\}$.

Algorithm: Test for Transitivity
Input: *n [a positive integer], $a[1], a[2], \ldots, a[n]$ [a one-dimensional array representing a set A], R [a subset of $A \times A$]*
Algorithm Body:
$i := 1, j := 1, k := 1$, answer := "yes"

while (answer = "yes" and $i \leq n$)
  while (answer = "yes" and $j \leq n$)
    while (answer = "yes" and $k \leq n$)
      if $(a[i], a[j]) \in R$ and $(a[j], a[k]) \in R$ and $(a[i], a[k]) \notin R$
      then answer := "no"
      $k := k + 1$
    end while
    $j := j + 1$
  end while
  $i := i + 1$
end while
Output: answer *[a string]*

3 Exercise Set 8.3

3.1 Exercise 1

Suppose that $S = \{a, b, c, d, e\}$ and R is a relation on S such that $a\,R\,b, b\,R\,c$, and $d\,R\,e$. List all of the following:

$$c\,R\,b, c\,R\,c, a\,R\,c, b\,R\,a, a\,R\,d, e\,R\,a, e\,R\,d, c\,R\,a$$

that must be true if R is:

3.1.1 (a)

reflexive (but not symmetric or transitive)

Proof. $c\,R\,c$

□

3.1.2 (b)

symmetric (but not reflexive or transitive)

Proof. $b\,R\,a, c\,R\,b, e\,R\,d$ □

3.1.3 (c)

transitive (but not reflexive or symmetric)

Proof. $a\,R\,c$ □

3.1.4 (d)

an equivalence relation.

Proof. $c\,R\,c, b\,R\,a, c\,R\,b, e\,R\,d, a\,R\,c, c\,R\,a$ □

3.2 Exercise 2

Each of the following partitions of $\{0, 1, 2, 3, 4\}$ induces a relation R on $\{0, 1, 2, 3, 4\}$. In each case, find the ordered pairs in R.

3.2.1 (a)

$\{0, 2\}, \{1\}, \{3, 4\}$

Proof. $R = \{(0, 0), (0, 2), (2, 0), (2, 2), (1, 1), (3, 3), (3, 4), (4, 3), (4, 4)\}$ □

3.2.2 (b)

$\{0\}, \{1, 3, 4\}, \{2\}$

Proof. $R = \{(0, 0), (1, 1), (3, 3), (4, 4), (1, 3), (3, 1), (1, 4), (4, 1), (3, 4), (4, 3), (2, 2)\}$ □

3.2.3 (c)

$\{0\}, \{1, 2, 3, 4\}$

Proof. $R = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (2, 3),$
$(3, 2), (2, 4), (4, 2), (3, 4), (4, 3)\}$ □

In each of $3-6$, the relation R is an equivalence relation on A. As in example 8.3.5, first find the specified equivalence classes. then state the number of distinct equivalence classes for R and list them.

3.3 Exercise 3

$A = \{0, 1, 2, 3, 4\}, R = \{(0, 0), (0, 4), (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 0), (4, 4)\}$, equivalence classes: [0], [1], [2], [3]

Proof. $[0] = \{0, 4\}, [1] = \{1, 3\}, [2] = \{2\}, [3] = \{1, 3\}$. So there are three distinct equivalence classes: $[0] = \{0, 4\} = [4], [1] = \{1, 3\} = [3], [2] = \{2\}$ □

3.4 Exercise 4

$A = \{a, b, c, d\}, R = \{(a, a), (b, b), (b, d), (c, c), (d, b), (d, d)\}$, classes: $[a], [b], [c], [d]$

Proof. $[a] = \{a\}, [b] = \{b, d\}, [c] = \{c\}, [d] = \{b, d\}$. So there are four distinct equivalence classes: $[a] = \{a\}, [b] = \{b, d\} = [d], [c] = \{c\}$. □

3.5 Exercise 5

$A = \{1, 2, 3, 4, \ldots, 20\}$. R is defined on A as follows: for all $x, y \in A, x\,R\,y \iff 4 \mid (x - y)$. Equivalence classes: [1], [2], [3], [4], [5]

Proof. $[1] = \{1, 5, 9, 13, 17\}, [2] = \{2, 6, 10, 14, 18\}, [3] = \{3, 7, 11, 15, 19\}, [4] = \{4, 8, 12, 16, 20\}, [5] = \{5, 9, 13, 17, 1\} = [1]$, four distinct equivalence classes: [1], [2], [3], [4] □

3.6 Exercise 6

$A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R is defined on A as follows: for all $x, y \in A, x\,R\,y \iff 3 \mid (x - y)$. Equivalence classes: [0], [1], [2], [3]

Proof. $[0] = \{-3, 0, 3\}, [1] = \{-2, 1, 4\}, [2] = \{-4, -1, 2, 5\}, [3] = \{-3, 0, 3\}$

There are 3 distinct equivalence classes: [0], [1], [2] □

In each of 7 – 14, the relation R is an equivalence relation on the set A. Find the distinct equivalence classes of R.

3.7 Exercise 7

$A = \{(1, 3), (2, 4), (-4, -8), (3, 9), (1, 5), (3, 6)\}$. R is defined on A as follows: For every $(a, b), (c, d) \in A, (a, b)\,R\,(c, d) \iff ad = bc$.

Proof. $\{(1, 3), (3, 9)\}, \{(2, 4), (24, 28), (3, 6)\}, \{(1, 5)\}$ □

3.8 Exercise 8

$X = \{a, b, c\}$ and $A = \mathscr{P}(X)$. R is defined on A as follows: For all sets u, v in $\mathscr{P}(X)$, $u\,R\,v \iff N(u) = N(v)$. (That is, the number of elements in u equals the number of elements in v.)

Proof. $\{\varnothing\}, \{\{a\}, \{b\}, \{c\}\}, \{\{a, b\}, \{a, c\}, \{b, c\}\}, \{\{a, b, c\}\}$ □

3.9 Exercise 9

$X = \{-1, 0, 1\}$ and $A = \mathscr{P}(X)$. R is defined on $\mathscr{P}(X)$ as follows: For all sets s and t in $\mathscr{P}(X), s\,R\,t \iff$ the sum of the elements in s equals the sum of the elements in t.

Proof. $\{\varnothing, \{0\}, \{-1, 1\}, \{-1, 0, 1\}\}, \{\{-1\}, \{-1, 0\}\}, \{\{1\}, \{0, 1\}\}$ □

3.10 Exercise 10

$A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R is defined on A as follows: For all $m, n \in \mathbb{Z}, m\,R\,n \iff 3 \mid (m^2 - n^2)$.

Proof. $\{-5, -4, -2, -1, 1, 2, 4, 5\}, \{-3, 0, 3\}$ □

3.11 Exercise 11

$A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R is defined on A as follows: For every $(m, n) \in A, m\,R\,n \iff 4 \mid (m^2 - n^2)$.

Proof. $\{-4, -2, 0, 2, 4\}, \{-3, -1, 1, 3\}$ □

3.12 Exercise 12

$A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R is defined on A as follows: For all $(m, n) \in A, m\,R\,n \iff 5 \mid (m^2 - n^2)$.

Proof. $\{-4, -1, 1, 4\}, \{-3, -2, 2, 3\}, \{0\}$ □

3.13 Exercise 13

A is the set of all strings of length 4 in a's and b's. R is defined on A as follows: For all strings s and t in $A, s\,R\,t \iff s$ has the same first two characters as t.

Proof. $\{aaaa, aaab, aaba, aabb\}$, $\{abaa, abab, abba, abbb\}$, $\{baaa, baab, baba, babb\}$,

$\{bbaa, bbab, bbba, bbbb\}$ □

3.14 Exercise 14

A is the set of all strings of 0's, 1's, and 2's that have length 4 and for which the sum of the characters in the string is less than or equal to 2. R is defined on A as follows: For every $s, t \in A, s\,R\,t \iff$ the sum of the characters of s equals the sum of the characters of t.

Proof. $\{0000\}, \{0001, 0010, 0100, 1000\}, \{0011, 0101, 1001, 0110, 1010, 1100, 0002, 0020, 0200, 2000\}$ □

3.15 Exercise 15

Determine which of the following congruence relations are true and which are false.

3.15.1 (a)

$17 \equiv 2 \pmod 5$

Proof. True. $17 - 2 = 15 = 5 \cdot 3$ □

3.15.2 (b)

$4 \equiv -5 \pmod 7$

Proof. False. $4 - (-5) = 9$ is not divisible by 7. □

3.15.3 (c)

$-2 \equiv -8 \pmod 3$

Proof. True. $-2 - (-8) = 6 = 3 \cdot 2$ □

3.15.4 (d)

$-6 \equiv -2 \pmod 2$

Proof. True. $-6 - (-2) = -4 = 2 \cdot (-2)$ □

3.16 Exercise 16

3.16.1 (a)

Let R be the relation of congruence modulo 3. Which of the following equivalence classes are equal? $[7], [-4], [-6], [17], [4], [27], [19]$

Proof. $[7] = [4] = [19], [-4] = [17], [-6] = [27]$ □

3.16.2 (b)

Let R be the relation of congruence modulo 7. Which of the following equivalence classes are equal? $[35], [3], [-7], [12], [0], [-2], [17]$

Proof. $[35] = [0] = [-7], [3] = [17], [12] = [-2]$ □

3.17 Exercise 17

3.17.1 (a)

Prove that for all integers m and n, $m \equiv n \pmod 3$ iff $m \mod 3 = n \mod 3$.

Proof. ($\implies$) Suppose m, n are integers such that $m \equiv n \pmod 3$. *[We want to show that* $m \mod 3 = n \mod 3$*]*. By definition of congruence, $3 \mid (m - n)$, and so, by definition of divisibility, $m - n = 3a$ for some integer a. Let $r = m \mod 3$. Then $m = 3b + r$ for some integer b. Since $m - n = 3a$, it follows that $m - n = (3b + r) - n = 3a$, or, equivalently, $n = 3(b - a) + r$. Now $b - a$ is an integer and $0 \leq r < 3$. So, by definition of mod, $n \mod 3 = r$, which equals $m \mod 3$.

($\impliedby$) Suppose m, n are integers such that $m \mod 3 = n \mod 3$. *[We want to show that* $m \equiv n \pmod 3$*]*. Let $r = m \mod 3 = n \mod 3$. Then, by definition of mod, $m = 3p + r$ and $n = 3q + r$ for some integers p and q. By substitution, $m - n = (3p + r) - (3q + r) = 3(p - q)$. Since $p - q$ is an integer, it follows that $3 \mid (m - n)$, and so, by definition of congruence, $m \equiv n \pmod 3$. □

3.17.2 (b)

Prove for all integers $d > 0$ and m, n, $m \equiv n \pmod d$ iff $m \mod d = n \mod d$.

Proof. Assume m, n, d are integers with $d > 0$.

($\implies$) 1. Assume $m \equiv n \pmod d$.

2. By 1 and definition of congruence, $d \mid (m - n)$.

3. By 2 and definition of divisibility, $m - n = da$ for some integer a.

4. Let $r = m \mod d$. Then by definition of mod, $m = db + r$ for some integer b and $0 \leq r < d$.

5. By 3 and 4, $m - n = (db + r) - n = da$, so $n = (db + r) - da = d(b - a) + r$ where $b - a$ is an integer and $0 \leq r < d$.

6. By 5 and definition of mod, $r = n \mod d$. Therefore $n \mod d = r = m \mod d$.

($\impliedby$) 1. Assume $m \mod d = n \mod d$. Let $r = m \mod d = n \mod d$.

2. By 1 and definition of mod, $m = da + r$ and $n = db + r$ for some integers a, b.

3. By 2, $m - n = da + r - (db + r) = d(a - b)$ where $a - b$ is an integer. Thus $d \mid (m - n)$.

4. By 3 and definition of congruence, $m \equiv n \pmod d$. □

3.18 Exercise 18

3.18.1 (a)

Give an example of two sets that are distinct but not disjoint.

Proof. One possible answer: Let $A = \{1, 2\}$ and $B = \{2, 3\}$. Then $A \neq B$, so A and B are distinct. But A and B are not disjoint since $2 \in A \cap B$. □

3.18.2 (b)

Find sets A_1 and A_2 and elements x, y, and z such that x and y are in A_1 and y and z are in A_2 but x and z are not both in either of the sets A_1 or A_2.

Proof. Let $A_1 = \{x, y\}, A_2 = \{y, z\}$. □

In 19 – 31, (1) prove that the relation is an equivalence relation, and (2) describe the distinct equivalence classes of each relation.

3.19 Exercise 19

A is the set of all students at your college.

3.19.1 (a)

R is the relation defined on A as follows: For every x and y in A, $x\,R\,y \iff x$ has the same major (or double major) as y. (Assume "undeclared" is a major.)

Proof. (1) R is reflexive because it is true that for each student x at a college, x has the same major (or double major) as x.

R is symmetric because it is true that for all students x and y at a college, if x has the same major (or double major) as y, then y has the same major (or double major) as x.

R is transitive because it is true that for all students x, y, and z at a college, if x has the same major (or double major) as y and y has the same major (or double major) as z, then x has the same major (or double major) as z.

R is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each major and double major at the college. Each class consists of all students with that major (or double major). □

3.19.2 (b)

S is the relation defined on A as follows: For every $x, y \in A, x\,S\,y \iff x$ is the same age as y.

Proof. (1) S is reflexive because for each student x at a college, x is the same age as x.

S is symmetric because it is true that for all students x and y at a college, if x is the same age as y, then y is the same age as x.

S is transitive because it is true that for all students x, y, and z at a college, if x is the same age as y and y is the same age as z, then x is the same age as z.

S is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each age at the college. Each class consists of all students with that age. □

3.20 Exercise 20

E is the relation defined on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}, m\,E\,n \iff 4 \mid (m-n)$.

Proof. (1) The solution to exercise 12 in Section 8.2 proved that E is reflexive, symmetric, and transitive. Thus E is an equivalence relation.

(2) Observe that for any integer a, the equivalence class of a is

$$\begin{array}{rcll} [a] & = & \{x \in \mathbb{Z} \mid x\,E\,a\} & \text{by definition of equivalence class} \\ & = & \{x \in \mathbb{Z} \mid x - a \text{ is divisible by } 4\} & \text{by definition of } E \\ & = & \{x \in \mathbb{Z} \mid x - a = 4k \text{ for some integer } k\} & \text{by definition of divisibility} \\ & = & \{x \in \mathbb{Z} \mid x = 4k + a \text{ for some integer } k\} & \text{by algebra.} \end{array}$$

Now when any integer a is divided by 4, the only possible remainders are 0, 1, 2, and 3 and no integer has two distinct remainders when it is divided by 4. Thus every integer is contained in exactly one of the following four equivalence classes:

$\{x \in \mathbb{Z} \mid x = 4k \text{ for some integer } k\}$, $\{x \in \mathbb{Z} \mid x = 4k+1 \text{ for some integer } k\}$,

$\{x \in \mathbb{Z} \mid x = 4k+2 \text{ for some integer } k\}$, $\{x \in \mathbb{Z} \mid x = 4k+3 \text{ for some integer } k\}$ □

3.21 Exercise 21

R is the relation defined on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}, m\,R\,n \iff 7m - 5n$ is even.

Proof. (1) R is reflexive because for all $m \in \mathbb{Z}, 7m - 5m = 2m$ is even, therefore $m\,R\,m$.

R is symmetric: assume $m\,R\,n$. Then $7m - 5n$ is even. So $7m - 5n = 2k$ for some integer k. Then $7n - 5m = (-5n + 12n) + (7m - 12m) = (12n - 12m) + (7m - 5n) = 2(6n - 6m) + 2k = 2(6n - 6m + k)$ where $6n - 6m + k$ is an integer. Thus $7n - 5m$ is even and $n\,R\,m$.

R is transitive: assume $m\,R\,n$ and $n\,R\,o$. Then $7m - 5n = 2k$ and $7n - 5o = 2l$ for some integers k, l. So $7m - 5o = (7m - 5n + 5n) + (-7n + 7n - 5o) = (7m - 5n) + (5n - 7n) + (7n - 5o) = 2k - 2n + 2l = 2(k - n + l)$, where $k - n + l$ is an integer. So $7m - 5o$ is even and $m\,R\,o$.

(2) Assume $m\,R\,n$. So $7m-5n$ is even. By properties of even and odd integers, either $7m$ and $5n$ are both even, or they are both odd. Since 7 and 5 are odd, and odd times odd is odd, this means that either m and n are both even, or they are both odd. Thus R has two equivalence classes: the set of all even integers and the set of all odd integers. □

3.22 Exercise 22

Let A be the set of all statement forms in three variables p, q, and r. $\mathbf{R}$ is the relation defined on A as follows: For all P and Q in A, $P\,\mathbf{R}\,Q \iff P$ and Q have the same truth table.

Proof. (1) $\mathbf{R}$ is reflexive because for all $P \in A$, P and P have the same truth table, so $P\,\mathbf{R}\,P$.

$\mathbf{R}$ is symmetric: assume $P\,\mathbf{R}\,Q$. Then P and Q have the same truth table. Then Q and P have the same truth table, so $Q\,\mathbf{R}\,P$.

$\mathbf{R}$ is transitive: assume $P\,\mathbf{R}\,Q$ and $Q\,\mathbf{R}\,S$. Then P and Q, and Q and S have the same truth tables. So P and S have the same truth table, and $P\,\mathbf{R}\,S$.

(2) There is an equivalence class corresponding to every possible truth table in 3 variables p, q, r. There are 8 lines in every truth table, and each line has 2 options (true or false), so there are 2^8 equivalence classes. □

3.23 Exercise 23

Let P be a set of parts shipped to a company from various suppliers. S is the relation defined on P as follows: For every $x, y \in P, x\,S\,y \iff x$ has the same part number and is shipped from the same supplier as y.

Proof. (1) S is reflexive because for all $x \in P$, x has the same part number and is shipped from the same supplier as x, so $x\,S\,x$.

S is symmetric: assume $x\,S\,y$. Then x has the same part number and is shipped from the same supplier as y. So y has the same part number and is shipped from the same supplier as x. Thus $y\,S\,x$.

S is transitive: assume $x\,S\,y$ and $y\,S\,z$. So x has the same part number and is shipped from the same supplier as y and y has the same part number and is shipped from the same supplier as z, so x has the same part number and is shipped from the same supplier as z. Therefore $x\,S\,z$.

(2) For each distinct part number shipped from each distinct supplier, there is a distinct equivalence class corresponding to that part number. □

3.24 Exercise 24

Let A be the set of identifiers in a computer program. It is common for identifiers to be used for only a short part of the execution time of a program and not to be used

again to execute other parts of the program. In such cases, arranging for identifiers to share memory locations makes efficient use of a computer's memory capacity. Define a relation R on A as follows: For all identifiers x and y, $x\,R\,y \iff$ the values of x and y are stored in the same memory location during execution of the program.

Proof. (1) R is reflexive because for all identifiers x, the values of x and x are stored in the same memory location during execution of the program.

R is symmetric: assume $x\,R\,y$. Then the values of x and y are stored in the same memory location during execution of the program. So the values of y and x are stored in the same memory location during execution of the program. So $y\,R\,x$.

R is transitive: assume $x\,R\,y$ and $y\,R\,z$. So the values of x and y are stored in the same memory location during execution of the program, and the values of y and z are stored in the same memory location during execution of the program. Then the values of x and z are stored in the same memory location during execution of the program. So $x\,R\,z$.

(2) There is a distinct equivalence class corresponding to each distinct memory location during execution of the program. □

3.25 Exercise 25

A is the "absolute value" relation defined on $\mathbb{R}$ as follows: For every $x, y \in \mathbb{R}, x\,A\,y \iff |x| = |y|$.

Proof. (1) A is reflexive because for all $x \in \mathbb{R}, |x| = |x|$, so $x\,A\,x$.

A is symmetric: assume $x\,A\,y$. Then $|x| = |y|$. So $|y| = |x|$, and $y\,A\,x$.

A is transitive: assume $x\,A\,y$ and $y\,A\,z$. Then $|x| = |y|$ and $|y| = |z|$, so $|x| = |z|$ and therefore $x\,A\,z$.

(2) There is a distinct equivalence class for each nonnegative real number. Each class is a set of the form $\{x, -x\}$ where x is a nonnegative real number. □

3.26 Exercise 26

D is the relation defined on $\mathbb{Z}$ as follows: For every $m, n \in \mathbb{Z}, m\,D\,n \iff 3 \mid (m^2 - n^2)$.

Proof. (1) D is reflexive because for all $m \in \mathbb{Z}, m^2 - m^2 = 0 = 3 \cdot 0$, so $3 \mid (m^2 - m^2)$ and thus $m\,D\,m$.

D is symmetric: assume $m\,D\,n$. Then $3 \mid (m^2 - n^2)$. Then $m^2 - n^2 = 3r$ for some integer r. Then $n^2 - m^2 = 3 \cdot (-r)$ where $-r$ is an integer. So $3 \mid (n^2 - m^2)$ and thus $n\,D\,m$.

D is transitive: assume $m\,D\,n$ and $n\,D\,o$. So $3 \mid (m^2 - n^2)$ and $3 \mid (n^2 - o^2)$. So $m^2 - n^2 = 3r$ and $n^2 - o^2 = 3s$ for some integers r, s. Then $m^2 - o^2 = (m^2 - n^2) + (n^2 - o^2) = 3(r + s)$ where $r + s$ is an integer. Therefore $3 \mid (m^2 - n^2)$ and $m\,D\,o$.

(2) There are two distinct equivalence classes: $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ and $[1] = \{\ldots, -5, -4, -2, -1, 1, 2, 4, 5, \ldots\}$. □

3.27 Exercise 27

R is the relation defined on $\mathbb{Z}$ as follows: For every $(m, n) \in \mathbb{Z}, m\,R\,n \iff 4 \mid (m^2 - n^2)$.

Proof. (1) R is an equivalence relation, the proofs are exactly the same as above in Exercise 26 (replace 3 with 4).

(2) There are 2 distinct equivalence classes: $[0]$ = the set of all even integers, $[1]$ = the set of all odd integers. This is because, if we want $4 \mid (m-n)(m+n)$, it is sufficient that both $m-n$ and $m+n$ are even; this is the case when either both m, n are odd or both m, n are even. □

3.28 Exercise 28

I is the relation defined on $\mathbb{R}$ as follows: For every $x, y \in \mathbb{R}, m\,I\,n \iff x - y$ is an integer.

Proof. (1) I is reflexive because the difference between each real number and itself is 0, which is an integer.

I is symmetric because for all real numbers x and y, if $x - y$ is an integer, then $y - x = (-1)(x - y)$, which is also an integer.

I is transitive because for all real numbers x, y, and z, if $x - y$ is an integer and $y - z$ is an integer, then $x - z = (x - y) + (y - z)$ is the sum of two integers and thus is an integer.

I is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one class for each real number x with $0 \leq x < 1$. The distinct classes are all sets of the form $\{y \in \mathbb{R} \mid y = n + x, \text{ for some integer } n\}$, where x is a real number such that $0 \leq x < 1$. □

3.29 Exercise 29

Define P on the set $\mathbb{R} \times \mathbb{R}$ of ordered pairs of real numbers as follows: For every $(w, x), (y, z) \in \mathbb{R} \times \mathbb{R}, (w, x)\,P\,(y, z) \iff w = y$.

Proof. (1) P is reflexive because each ordered pair of real numbers has the same first element as itself.

P is symmetric for the following reason: Suppose (w, x) and (y, z) are ordered pairs of real numbers such that $(w, x)\,P\,(y, z)$. Then, by definition of P, $w = y$. Now by the symmetric property of equality, this implies that $y = w$, and so, by definition of P, $(y, z)\,P\,(w, x)$.

P is transitive for the following reason: Suppose $(u, v), (w, x)$, and (y, z) are ordered pairs of real numbers such that $(u, v)\,P\,(w, x)$ and $(w, x)\,P\,(y, z)$. Then, by definition of P, $u = w$ and $w = y$. It follows from the transitive property of equality that $u = y$. Hence, by definition of P, $(u, v)\,P\,(y, z)$.

P is an equivalence relation because it is reflexive, symmetric, and transitive.

(2) There is one equivalence class for each real number. The distinct equivalence classes are all sets of ordered pairs $\{(x, y) \in \mathbb{R}\times\mathbb{R} \mid x = a\}$, for each real number a. Equivalently, the equivalence classes consist of all vertical lines in the Cartesian plane. □

3.30 Exercise 30

Define Q on the set $\mathbb{R}\times\mathbb{R}$ as follows: For every $(w, x), (y, z) \in \mathbb{R}\times\mathbb{R}$, $(w, x)\, Q\, (y, z) \iff x = z$.

Proof. (1) Q is reflexive because for all $(w, x) \in \mathbb{R} \times \mathbb{R}$, $x = x$ so $(w, x)\, Q\, (w, x)$.

Q is symmetric: assume $(w, x)\, Q\, (y, z)$. Then $x = z$. So $z = x$ and thus $(y, z)\, Q\, (w, x)$.

Q is transitive: assume $(w, x)\, Q\, (y, z)$ and $(y, z)\, Q\, (s, t)$. Then $x = z$ and $z = t$. So $x = t$ and thus $(w, x)\, Q\, (s, t)$.

(2) Q has a distinct equivalence class, for each real number a, of the form $\{(w, x) \in \mathbb{R} \times \mathbb{R} \mid x = a\}$. □

3.31 Exercise 31

Let P be the set of all points in the Cartesian plane except the origin. R is the relation defined on P as follows: For every p_1 and p_2 in P, $p_1\, R\, p_2 \iff$ p_1 and p_2 lie on the same half-line emanating from the origin.

Proof. (1) R is reflexive: for every $p \in P$, p and p lie on the same half-line emanating from the origin (namely the half-line that connects p to the origin). Thus $p\, R\, p$.

R is symmetric: assume $p\, R\, q$. Then p and q lie on the same half-line l emanating from the origin. Then q and p lie on the same half-line l emanating from the origin. Thus $q\, R\, p$.

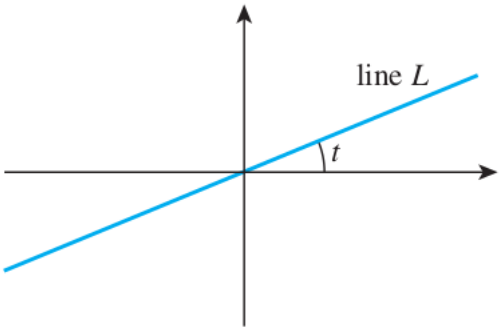
R is transitive: assume $p\, R\, q$ and $q\, R\, r$. Then p and q lie on the same half-line l_1 emanating from the origin and q and r lie on the same half-line l_2 emanating from the origin. Then it must be that $l_1 = l_2$ since q lies on both half-lines. Thus p and r lie on the same half-line emanating from the origin, and $p\, R\, r$.

(2) Each equivalence class is a half-line l emanating from the origin, containing all the points p that lie on l. □

3.32 Exercise 32

Let A be the set of all straight lines in the Cartesian plane. Define a relation $\parallel$ on A as follows: For every l_1 and l_2 in A, $l_1 \parallel l_2 \iff$ l_1 is parallel to l_2. Then $\parallel$ is an equivalence relation on A. Describe the equivalence classes of this relation.

Proof. There is one equivalence class for each real number t such that $0 \leq t < \pi$. One line in each class goes through the origin, and that line makes an angle of t with the positive horizontal axis.



Alternatively, there is one equivalence class for every possible slope: all real numbers plus "undefined." □

3.33 Exercise 33

Let A be the set of points in the rectangle with x and y coordinates between 0 and 1. That is,

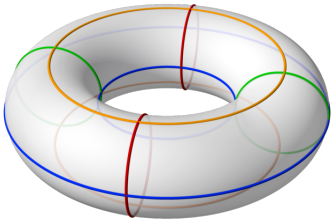
$$A = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, 0 \leq x \leq 1 \text{ and } 0 \leq y \leq 1\}.$$

Define a relation R on A as follows: For all (x_1, y_1) and (x_2, y_2) in A,

$$\begin{aligned}
(x_1, y_1)\, R\, (x_2, y_2) \iff\ & (x_1, y_1) = (x_2, y_2); \text{ or} \\
& x_1 = 0 \text{ and } x_2 = 1 \text{ and } y_1 = y_2; \text{ or} \\
& x_1 = 1 \text{ and } x_2 = 0 \text{ and } y_1 = y_2; \text{ or} \\
& y_1 = 0 \text{ and } y_2 = 1 \text{ and } x_1 = x_2; \text{ or} \\
& y_1 = 1 \text{ and } y_2 = 0 \text{ and } x_1 = x_2.
\end{aligned}$$

In other words, all points along the top edge of the rectangle are related to the points along the bottom edge directly beneath them, and all points directly opposite each other along the left and right edges are related to each other. The points in the interior of the rectangle are not related to anything other than themselves. Then R is an equivalence relation on A. Imagine gluing together all the points that are in the same equivalence class. Describe the resulting figure.

Proof. Gluing the top and bottom edges of the rectangle results in a horizontal cylinder. Then, if we also glue the left and right circular ends of this cylinder, we get a doughnut shaped figure:



□

3.34 Exercise 34

The documentation for the computer language Java recommends that when an "equals method" is defined for an object, it be an equivalence relation. That is, if R is defined as follows: $x\,R\,y \iff x.equals(y)$ for all objects in the class, then R should be an equivalence relation. Suppose that in trying to optimize some of the mathematics of a graphics application, a programmer creates an object called a point, consisting of two coordinates in the plane. The programmer defines an equals method as follows: If p and q are any points, then $p.equals(q)$ iff the distance from p to q is less than or equal to c where c is a small positive number that depends on the resolution of the computer display. Is the programmer's equals method an equivalence relation? Justify your answer.

Proof. No. If points p, q, and r all lie on a straight line with q in the middle, and if p is c units from q and q is c units from r, then p is more than c units from r. □

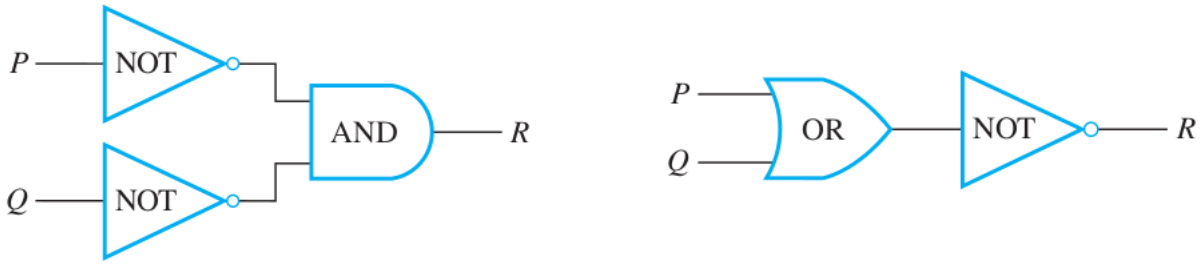
3.35 Exercise 35

Find an additional representative circuit for the input/output table of Example 8.3.9.

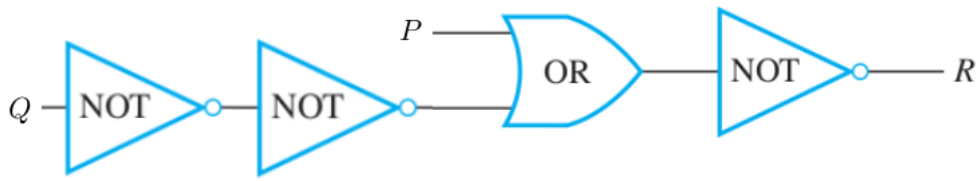
Proof. Recall that the output table is:

Input		Output
P	***Q***	***R***
1	1	0
1	0	0
0	1	0
0	0	1

And two representative circuits for this table were given:



Here is another:



□

Let R be an equivalence relation on a set A. Prove each of the statements in $36-41$ directly from the definitions of equivalence relation and equivalence class without using the results of Lemma 8.3.2, Lemma 8.3.3, or Theorem 8.3.4.

3.36 Exercise 36

For every a in A, $a \in [a]$.

Proof. Suppose R is an equivalence relation on a set A and $a \in A$. Because R is an equivalence relation, R is reflexive, and because R is reflexive, each element of A is related to itself by R. In particular $a\,R\,a$. Hence, by definition of equivalence class, $a \in [a]$. □

3.37 Exercise 37

For every a and b in A, if $b \in [a]$ then $a\,R\,b$.

Proof. Yes, by definition of $[a], b \in [a] \iff b\,R\,a$. So $b\,R\,a$. By symmetry, $a\,R\,b$. □

3.38 Exercise 38

For every a, b, and c in A, if $b\,R\,c$ and $c \in [a]$ then $b \in [a]$.

Proof. Suppose R is an equivalence relation on a set A and a, b, and c are elements of A with $b\,R\,c$ and $c \in [a]$. Since $c \in [a]$, then $c\,R\,a$ by definition of equivalence class. Now R is transitive because R is an equivalence relation. Thus, since $b\,R\,c$ and $c\,R\,a$, then $b\,R\,a$. It follows that $b \in [a]$ by definition of equivalence class. □

3.39 Exercise 39

For every a and b in A, if $[a] = [b]$ then $a\,R\,b$.

Proof. Assume $[a] = [b]$. By Exercise 36 $b \in [b]$, and since $[a] = [b]$ we have $b \in [a]$. So by Exercise 37 $a\,R\,b$. □

3.40 Exercise 40

For every a, b, and x in A, if $a\,R\,b$ and $x \in [a]$ then $x \in [b]$.

Proof. Suppose a, b, and x are in $A, a\,R\,b$, and $x \in [a]$. By definition of equivalence class, $x\,R\,a$. So $x\,R\,a$ and $a\,R\,b$, and thus, by transitivity, $x\,R\,b$. Hence $x \in [b]$. □

3.41 Exercise 41

For every a and b in A, if $a \in [b]$ then $[a] = [b]$.

Proof. Assume $x \in [a]$. Then $x \, R \, a$ by definition of $[a]$. Since $a \in [b]$, by Exercise 37 $b \, R \, a$. By symmetry, $a \, R \, b$. Then by transitivity $x \, R \, b$. So $x \in [b]$ by definition of $[b]$. Thus $[a] \subseteq [b]$.

Assume $x \in [b]$. Then $x \, R \, b$ by definition of $[b]$. Since $a \in [b]$, by Exercise 37 $b \, R \, a$. Then by transitivity $x \, R \, a$. So $x \in [a]$ by definition of $[a]$. Thus $[b] \subseteq [a]$.

So by definition of set equality $[a] = [b]$. □

3.42 Exercise 42

Let R be the relation defined in Example 8.3.12: $(a, b) \, R \, (c, d) \iff ad = bc$.

3.42.1 (a)

Prove that R is reflexive.

Proof. For all $a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}, ab = ba$, therefore $(a, b) \, R \, (a, b)$. So R is reflexive. □

3.42.2 (b)

Prove that R is symmetric.

Proof. Assume $(a, b) \, R \, (c, d)$. Then $ad = bc$. So $bc = ad$ and thus $(c, d) \, R \, (a, b)$. So R is symmetric. □

3.42.3 (c)

List four distinct elements in $[(1, 3)]$.

Proof. One possible answer: $(2, 6), (-2, -6), (3, 9), (-3, -9)$. □

3.42.4 (d)

List four distinct elements in $[(2, 5)]$.

Proof. One possible answer: $(4, 10), (6, 15), (8, 20), (10, 25)$. □

3.43 Exercise 43

In Example 8.3.12, define operations of addition $(+)$ and multiplication $(\cdot)$ as follows: For every $(a, b), (c, d) \in A, [(a, b)] + [(c, d)] = [(ad + bc, bd)]$ and $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$.

3.43.1 (a)

Prove that this addition is well defined. That is, show that if $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$, then $[(ad+bc,bd)] = [(a'd'+b'c',b'd')]$.

Proof. Suppose that $(a,b),(a',b'),(c,d)$, and (c',d') are any elements of A such that $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$. By definition of $R, ab' = ba'$ (*) and $cd' = dc'$ (**). We must show that $[(a,b)] + [(c,d)] = [(a',b')] + [(c',d')]$. By definition of the addition on A, this equation is true if, and only if, $[(ad+bc,bd)] = [(a'd'+b'c',b'd')]$. And, by definition of the relation, this equation is true if, and only if, $(ad+bc)b'd' = bd(a'd'+b'c')$. After multiplying out, this becomes $adb'd' + bcb'd' = bda'd' + bdb'c'$, and regrouping, turns it into $(ab')(dd') + (cd')(bb') = (ba')(dd') + (dc')(bb')$. Substituting the values from (*) and (**) shows that this last equation is true. □

3.43.2 (b)

Prove that this multiplication is well defined. That is, show that if $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$, then $[(ac,bd)] = [(a'c',b'd')]$.

Proof. 1. Assume $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$.

2. By 1 and the definition of equivalence classes of R, $(a,b)\,R\,(a',b')$ and $(c,d)\,R\,(c',d')$.

3. By 2 and definition of R, $ab' = ba'$ and $cd' = dc'$.

4. By 3, multiplying the left hand sides together and the right hand sides together, $ab'cd' = ba'dc'$.

5. By 4 and commutativity, reorganizing, $(ac)(b'd') = (bd)(a'c')$.

6. By 5 and definition of R, $(ad,bc)\,R\,(a'c',b'd')$.

7. By 6 and definition of equivalence classes of R, $[(ad,bc)] = [(a'c',b'd')]$. □

3.43.3 (c)

Show that $[(0,1)]$ is an identity element for addition. That is, show that for any $(a,b) \in A, [(a,b)] + [(0,1)] = [(0,1)] + [(a,b)] = [(a,b)]$.

Proof. Suppose that (a,b) is any element of A. We must show that $[(a,b)] + [(0,1)] = [(a,b)]$. By definition of the addition on A, this equation is true if, and only if, $[(a\cdot 1 + b\cdot 0, b\cdot 1)] = [(a,b)]$. And this last equation is true because $a\cdot 1 + b\cdot 0 = a$ and $b\cdot 1 = b$. □

3.43.4 (d)

Find an identity element for multiplication. That is, find (i,j) in A so that for every (a,b) in A, $[(a,b)]\cdot[(i,j)] = [(i,j)]\cdot[(a,b)] = [(a,b)]$.

Proof. The multiplicative identity is $(1,1)$. Indeed, by definition of multiplication on A, $[(a,b)]\cdot[(1,1)] = [(a\cdot 1, b\cdot 1)] = [(a,b)]$ and $[(1,1)]\cdot[(a,b)] = [(1\cdot a, 1\cdot b)] = [(a,b)]$. □

3.43.5 (e)

For any $(a, b) \in A$, show that $[(-a, b)]$ is an inverse for $[(a, b)]$ for addition. That is, show that $[(-a, b)] + [(a, b)] = [(a, b)] + [(-a, b)] = [(0, 1)]$.

Proof. Suppose that (a, b) is any element of A. We must show that $[(a, b)] + [(-a, b)] = [(-a, b)] + [(a, b)] = [(0, 1)]$. By definition of the addition on A, this equation is true if, and only if, $[(ab + b(-a), bb)] = [(0, 1)]$, or, equivalently, $[(0, bb)] = [(0, 1)]$. By definition of the relation, this last equation is true if, and only if, $0 \cdot 1 = bb \cdot 0$, which is true. □

3.43.6 (f)

Given any $(a, b) \in A$ with $a \neq 0$, find an inverse for $[(a, b)]$ for multiplication. That is, find (c, d) in A so that $[(a, b)] \cdot [(c, d)] = [(c, d)] \cdot [(a, b)] = [(i, j)]$, where $[(i, j)]$ is the identity element you found in part (d).

Proof. Given $[(a, b)]$ we want to find $[(c, d)]$ such that $[(a, b)] \cdot [(c, d)] = [(ac, bd)] = [(1, 1)]$.

So by the definition of equivalence classes of R on A, (ac, bd) is related to $(1, 1)$ by R, in other words $ac \cdot 1 = bd \cdot 1$, or $ac = bd$. Then let $(c, d) = (b, a)$. So $ac = ab = ba = bd$, therefore $(ac, bd)\, R\, (1, 1)$ and thus $[(ac, bd)] = [(1, 1)]$, in other words $[(a, b)] \cdot [(c, d)] = [(1, 1)]$.

Similarly we can prove that $[(c, d)] \cdot [(a, b)] = [(1, 1)]$. □

3.44 Exercise 44

Let $A = Z^+ \times Z^+$. Define a relation R on A as follows: For every (a, b) and (c, d) in A, $(a, b)\, R\, (c, d) \iff a + d = c + b$.

3.44.1 (a)

Prove that R is reflexive.

Proof. Let (a, b) be any element of $Z^+ \times Z^+$. We must show that $(a, b)\, R\, (a, b)$. By definition of R, this relationship holds if, and only if, $a + b = b + a$. But this equation is true by the commutative law of addition for real numbers. Hence R is reflexive. □

3.44.2 (b)

Prove that R is symmetric.

Proof. Assume $(a, b)\, R\, (c, d)$. Then by definition of R, $a + d = c + b$. So $c + b = a + d$. Thus $(c, d)\, R\, (a, b)$ by definition of R. So R is symmetric. □

3.44.3 (c)

Prove that R is transitive.

Proof. Assume $(a, b)\, R\, (c, d)$ and $(c, d)\, R\, (e, f)$. By definition of R, $a + d = c + b$ and $c + f = e + d$. Adding the two equations we get $a + d + c + f = c + b + e + d$. Canceling $c + d$ on both sides we get $a + f = e + b$, thus $(a, b)\, R\, (e, f)$ so R is transitive. □

3.44.4 (d)

List five elements in [(1, 1)].

Proof. One possible answer: (1, 1), (2, 2), (3, 3), (4, 4), (5, 5) □

3.44.5 (e)

List five elements in [(3, 1)].

Proof. One possible answer: (4, 2), (5, 3), (6, 4), (7, 5), (8, 6) □

3.44.6 (f)

List five elements in [(1, 2)].

Proof. One possible answer: (1, 2), (2, 3), (3, 4), (4, 5), (5, 6) □

3.44.7 (g)

Describe the distinct equivalence classes of R.

Proof. Observe that for any positive integers a and b, the equivalence class of (a, b) consists of all ordered pairs in $Z^+ \times Z^+$ for which the difference between the first and second coordinates equals $a - b$. Thus there is one equivalence class for each integer: positive, negative, and zero. Each positive integer n corresponds to the class of $(n+1, 1)$; each negative integer $-n$ corresponds to the class of $(1, n + 1)$; and zero corresponds to the class $(1, 1)$. □

3.45 Exercise 45

The following argument claims to prove that the requirement that an equivalence relation be reflexive is redundant. In other words, it claims to show that if a relation is symmetric and transitive, then it is reflexive. Find the mistake in the argument.

"Proof: Let R be a relation on a set A and suppose R is symmetric and transitive. For any two elements x and y in A, if $x\, R\, y$ then $y\, R\, x$ since R is symmetric. Thus it follows by transitivity that $x\, R\, x$, and hence R is reflexive."

Proof. The conclusion $x\, R\, x$ only follows under the assumption that $x\, R\, y$, which has not been discharged from the proof. (See next exercise.) □

3.46 Exercise 46

Let R be a relation on a set A and suppose R is symmetric and transitive. Prove the following: If for every x in A there is a y in A such that $x\,R\,y$, then R is an equivalence relation.

Proof. Let R be a relation on a set A and suppose R is symmetric and transitive. Assume x is any element in A. By the assumption, there exists y in A such that $x\,R\,y$. Then $y\,R\,x$ since R is symmetric. Thus it follows by transitivity that $x\,R\,x$, and hence R is reflexive. Hence R is an equivalence relation. □

3.47 Exercise 47

Refer to the quote at the beginning of this section to answer the following questions.

3.47.1 (a)

What is the name of the Knight's song called?

Proof. ... The name of the song is called 'Haddocks' Eyes.' □

3.47.2 (b)

What is the name of the Knight's song?

Proof. The name really is 'The Aged Aged Man.' □

3.47.3 (c)

What is the Knight's song called?

Proof. "Ways and Means" □

3.47.4 (d)

What is the Knight's song?

Proof. The song really is 'A-sitting on a Gate' □

3.47.5 (e)

What is your (full, legal) name?

Proof. Spam, Egg □

3.47.6 (f)

What are you called?

Proof. Spam □

3.47.7 (g)

What are you? (Do not answer this on paper; just think about it.)

Proof. *???* □

4 Exercise Set 8.4

4.1 Exercise 1

4.1.1 (a)

Use the Caesar cipher to encrypt the message WHERE SHALL WE MEET.

Proof. ZKHUH VKDOO ZH PHHW □

4.1.2 (b)

Use the Caesar cipher to decrypt the message LQ WKH FDIHWHULD.

Proof. IN THE CAFETERIA □

4.2 Exercise 2

4.2.1 (a)

Use the Caesar cipher to encrypt the message AN APPLE A DAY.

Proof. DQ DSSOH D GDB □

4.2.2 (b)

Use the Caesar cipher to decrypt the message NHHSV WKH GRFWRU DZDB.

Proof. KEEPS THE DOCTOR AWAY □

4.3 Exercise 3

Let $a = 25, b = 19, n = 3$.

4.3.1 (a)

Verify that $3 \mid (25 - 19)$.

Proof. The relation $3 \mid (25-19)$ is true because $25-19 = 6$ and $3 \mid 6$ (since $6 = 3 \cdot 2$). □

4.3.2 (b)

Explain why $25 \equiv 19 \pmod 3$.

Proof. By definition of congruence modulo n, to show that $25 \equiv 19 \pmod 3$, one must show that $3 \mid (25 - 19)$. This was verified in part (a). □

4.3.3 (c)

What value of k has the property that $25 = 19 + 3k$?

Proof. To show that $25 = 19 + 3k$ for some integer k, one solves the equation for k and checks that the result is an integer. In this case, $k = (25 - 19)/3 = 2$, which is an integer. Thus $25 = 19 + 2 \cdot 3$. □

4.3.4 (d)

What is the (nonnegative) remainder obtained when 25 is divided by 3? When 19 is divided by 3?

Proof. When 25 is divided by 3, the remainder is 1 because $25 = 3 \cdot 8 + 1$. When 19 is divided by 3, the remainder is also 1 because $19 = 3 \cdot 6 + 1$. Thus 25 and 19 have the same remainder when divided by 3. □

4.3.5 (e)

Explain why $25 \mod 3 = 19 \mod 3$.

Proof. By definition, $25 \mod 3$ is the remainder obtained when 25 is divided by 3, and $19 \mod 3$ is the remainder obtained when 19 is divided by 3. In part (d) these two numbers were shown to be equal. □

4.4 Exercise 4

Let $a = 68, b = 33, n = 7$.

4.4.1 (a)

Verify that $7 \mid (68 - 33)$.

Proof. The relation $7 \mid (68 - 33)$ is true because $68 - 33 = 35$ and $7 \mid 35$ (since $35 = 7 \cdot 5$). □

4.4.2 (b)

Explain why $68 \equiv 33 \pmod 7$.

Proof. By definition of congruence modulo n, to show that $68 \equiv 33 \pmod 7$, one must show that $7 \mid (68 - 33)$. This was verified in part (a). □

4.4.3 (c)

What value of k has the property that $68 = 33 + 7k$?

Proof. To show that $68 = 33 + 7k$ for some integer k, one solves the equation for k and checks that the result is an integer. In this case, $k = (68 - 33)/7 = 5$, which is an integer. Thus $68 = 33 + 7 \cdot 5$. □

4.4.4 (d)

What is the (nonnegative) remainder obtained when 68 is divided by 7? When 33 is divided by 7?

Proof. When 68 is divided by 7, the remainder is 5 because $68 = 7 \cdot 9 + 5$. When 33 is divided by 7, the remainder is also 5 because $33 = 7 \cdot 4 + 5$. Thus 68 and 33 have the same remainder when divided by 7. □

4.4.5 (e)

Explain why $68 \mod 7 = 33 \mod 7$.

Proof. By definition, $68 \mod 7$ is the remainder obtained when 68 is divided by 7, and $33 \mod 7$ is the remainder obtained when 33 is divided by 7. In part (d) these two numbers were shown to be equal. □

4.5 Exercise 5

Prove the transitivity of modular congruence. That is, prove that for all integers a, b, c, and n with $n > 1$, if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

Proof. 1. Assume $a \equiv b \pmod n$ and $b \equiv c \pmod n$.

2. By 1 and definition of modular congruence, $n \mid (a - b)$ and $n \mid (b - c)$.

3. By 2 and definition of divides, $a - b = en$ and $b - c = fn$ for some integers e, f.

4. By 3, adding the equations we get $a - c = (a - b) + (b - c) = en + fn = (e + f)n$ where $e + f$ is an integer.

5. By 4 and definition of divides, $n \mid (a - c)$.

6. By 5 and definition of modular congruence, $a \equiv c \pmod n$. □

4.6 Exercise 6

Prove that the distinct equivalence classes of the relation of congruence modulo n are the sets $[0], [1], [2], \ldots, [n-1]$, where for each $a = 0, 1, 2, \ldots, n-1$, $[a] = \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\}$.

Proof. Assume $a \in \mathbb{Z}$. By the quotient-remainder theorem, $a = nq + r$ for some integers q, r with $0 \leq r < n$. So $a \equiv r \pmod{n}$ and by definition of $[r], a \in [r]$. Since $0 \leq r < n$, a belongs to one of the sets $[0], [1], [2], \ldots, [n-1]$.

Now we need to show the sets $[0], [1], [2], \ldots, [n-1]$ are distinct equivalence classes. Assume $0 \leq a < n$ and $0 \leq b < n$. We need to show that if $[a] = [b]$ then $a = b$.

Assume $[a] = [b]$. Since $a \equiv a \pmod{n}$, by definition of $[a], a \in [a]$. Since $[a] = [b], a \in [b]$. Then by definition of $[b]$, $a \equiv b \pmod{n}$. So $n \mid (a - b)$. So $a - b = kn$ for some integer k. Notice that since $0 \leq a < n$ and $0 \leq b < n$, we have $-n < a - b < n$. Therefore $k = 0$. So $a = b$.

We have shown that every integer belongs to one of the classes $[0], [1], [2], \ldots, [n-1]$, and we have show that these classes are all distinct. □

4.7 Exercise 7

Verify the following statements.

4.7.1 (a)

$128 \equiv 2 \pmod{7}$ and $61 \equiv 5 \pmod{7}$

Proof. $128 \equiv 2 \pmod{7}$ because $128 - 2 = 126 = 7 \cdot 18$, $61 \equiv 5 \pmod{7}$ because $61 - 5 = 56 = 7 \cdot 8$ □

4.7.2 (b)

$(128 + 61) \equiv (2 + 5) \pmod{7}$

Proof. $128 + 61 \equiv (2 + 5) \pmod{7}$ because $128 + 61 = 189, 2 + 5 = 7$, and $189 - 7 = 182 = 7 \cdot 26$. □

4.7.3 (c)

$(128 - 61) \equiv (2 - 5) \pmod{7}$

Proof. $128 - 61 \equiv (2 - 5) \pmod{7}$ because $128 - 61 = 67, 2 - 5 = -3$, and $67 - (-3) = 70 = 7 \cdot 10$. □

4.7.4 (d)

$(128 \cdot 61) \equiv (2 \cdot 5) \pmod 7$

Proof. $128 \cdot 61 \equiv (2 \cdot 5) \pmod 7$ because $128 \cdot 61 = 7808, 2 \cdot 5 = 10$, and $7808 - (10) = 7798 = 7 \cdot 1114$. □

4.7.5 (e)

$128^2 \equiv 2^2 \pmod 7$

Proof. $128^2 \equiv 2^2 \pmod 7$ because $128^2 = 16384, 2^2 = 4$, and $16384 - 4 = 16380 = 7 \cdot 2340$. □

4.8 Exercise 8

Verify the following statements.

4.8.1 (a)

$45 \equiv 3 \pmod 6$ and $104 \equiv 2 \pmod 6$

Proof. $45 \equiv 3 \pmod 6$ because $45 - 3 = 42 = 6 \cdot 7$

$104 \equiv 2 \pmod 6$ because $104 - 2 = 102 = 6 \cdot 17$ □

4.8.2 (b)

$(45 + 104) \equiv (3 + 2) \pmod 6$

Proof. $45 + 104 \equiv (3 + 2) \pmod 6$ because $45 + 104 = 149, 3 + 2 = 5$, and $149 - 5 = 144 = 6 \cdot 24$. □

4.8.3 (c)

$(45 - 104) \equiv (3 - 2) \pmod 6$

Proof. $45 - 104 \equiv (3 - 2) \pmod 6$ because $45 - 104 = -59, 3 - 2 = 1$, and $-59 - (1) = -60 = 6 \cdot (-10)$. □

4.8.4 (d)

$(45 \cdot 104) \equiv (3 \cdot 2) \pmod 6$

Proof. $45 \cdot 104 \equiv (3 \cdot 2) \pmod 6$ because $45 \cdot 104 = 4680, 3 \cdot 2 = 6$, and $4680 - (6) = 4674 = 6 \cdot 779$. □

4.8.5 (e)

$45^2 \equiv 3^2 \pmod 6$

Proof. $45^2 \equiv 3^2 \pmod 6$ because $45^2 = 2025, 3^2 = 9$, and $2025 - 9 = 2016 = 6 \cdot 336$. □

In $9 - 11$, prove each of the given statements, assuming that a, b, c, d, and n are integers with $n > 1$ and that $a \equiv c \pmod n$ and $b \equiv d \pmod n$.

4.9 Exercise 9

$(a + b) \equiv (c + d) \pmod n$

4.9.1 (a)

Proof. Suppose a, b, c, d, and n are integers with $n > 1, a \equiv c \pmod n$, and $b \equiv d \pmod n$. By Theorem 8.4.1, $a - c = nr$ and $b - d = ns$ for some integers r and s. Then $(a + b) - (c + d) = (a - c) + (b - d) = nr + ns = n(r + s)$. Now $r + s$ is an integer, and so, by Theorem 8.4.1, $a + b \equiv (c + d) \pmod n$. □

4.9.2 (b)

$(a - b) \equiv (c - d) \pmod n$

Proof. Suppose a, b, c, d, and n are integers with $n > 1, a \equiv c \pmod n$, and $b \equiv d \pmod n$. By Theorem 8.4.1, $a - c = nr$ and $b - d = ns$ for some integers r and s. Then $(a - b) - (c - d) = (a - c) - (b - d) = nr - ns = n(r - s)$. Now $r - s$ is an integer, and so, by Theorem 8.4.1, $a - b \equiv (c - d) \pmod n$. □

4.10 Exercise 10

$a^2 \equiv c^2 \pmod n$

Proof. Suppose a, c, and n are integers with $n > 1$ and $a \equiv c \pmod n$. By Theorem 8.4.1, $a - c = nr$ for some integers r. Then $a^2 - c^2 = (a - c)(a + c) = nr(a + c)$. Now $r(a + c)$ is an integer, and so, by Theorem 8.4.1, $a^2 \equiv c^2 \pmod n$. □

4.11 Exercise 11

$a^m \equiv c^m \pmod n$ for every integer $m \geq 1$ (Use mathematical induction on m.)

Proof. Show that $a \equiv c \pmod n$: This holds by assumption.

Show that for every integer $m \geq 1$ *if* $a^m \equiv c^m \pmod n$ *then* $a^{m+1} \equiv c^{m+1} \pmod n$*:* Assume $m \geq 1$ and $a^m \equiv c^m \pmod n$. We also know that $a \equiv c \pmod n$ by assumption, so $a - c = ns$ for some integer s. Then

$$\begin{aligned} a^{m+1} - c^{m+1} &= (a-c)(a^m + a^{m-1}c + \ldots + ac^{m-1} + c^m) \\ &= ns(a^m + a^{m-1}c + \ldots + ac^{m-1} + c^m) \end{aligned}$$

therefore $n \mid (a^{m+1} - c^{m+1})$, so by definition of congruence, $a^{m+1} \equiv c^{m+1} \pmod{n}$. □

4.12 Exercise 12

4.12.1 (a)

Prove that for every integer $n \geq 0, 10^n \equiv 1 \pmod{9}$.

Proof. Let the property $P(n)$ be the congruence $10^n \equiv 1 \pmod{9}$.

Show that $P(0)$ is true: When $n = 0$, the left-hand side of the congruence is $10^0 = 1$ and the right- hand side is also 1.

Show that for every integer $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true: Let k be any integer with $k \geq 0$, and suppose $P(k)$ is true. That is, suppose $10^k \equiv 1 \pmod{9}$. (*) *[This is the inductive hypothesis.]* By Theorem 8.4.1, $10 \equiv 1 \pmod{9}$ (**) because $10 - 1 = 9 = 9 \cdot 1$. And by Theorem 8.4.3, we can multiply the left- and right-hand sides of (*) and (**) to obtain $10^k \cdot 10 \equiv 1 \cdot 1 \pmod{9}$, or, equivalently, $10^{k+1} \equiv 1 \pmod{9}$. Hence $P(k+1)$ is true.

Alternative Proof: Note that $10 \equiv 1 \pmod{9}$ because $10 - 1 = 9$ and $9 \mid 9$. Thus by Theorem 8.4.3(4), $10^n \equiv 1^n \equiv 1 \pmod{9}$. □

4.12.2 (b)

Use part (a) to prove that a positive integer is divisible by 9 if, and only if, the sum of its digits is divisible by 9.

Proof. Assume n is a positive integer. We can write n in base 10 expansion:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \cdot 10^0$$

where $a_k, \ldots, a_0$ are the decimal digits of n.

[We want to show n is divisible by 9 if and only if $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9.]

By part (a), $10^k \equiv 10^{k-1} \equiv \cdots \equiv 10^1 \equiv 10^0 \equiv 1 \pmod{9}$. Therefore

$$n \equiv a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \cdot 10^0 \equiv a_k \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \cdot 1 \pmod{9}$$

If n is divisible by 9, $n \equiv 0 \pmod{9}$, so by the above congruence, $a_k + \cdots + a_0 \equiv 0 \pmod{9}$, so $a_k + \cdots + a_0$ is divisible by 9. Similarly if $a_k + \cdots + a_0$ is divisible by 9 then n is divisible by 9 by the same reasoning. □

4.13 Exercise 13

4.13.1 (a)

Prove that for every integer $n \geq 1, 10^n \equiv (-1)^n \pmod{11}$.

Proof. Let the property $P(n)$ be the congruence $10^n \equiv (-1)^n \pmod{11}$.

Show that $P(0)$ is true: When $n = 0$, the left-hand side of the congruence is $10^0 = 1$ and the right- hand side is also $(-1)^n = 1$.

Show that for every integer $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true: Let k be any integer with $k \geq 0$, and suppose $P(k)$ is true. That is, suppose $10^k \equiv (-1)^k \pmod{11}$. (*) *[This is the inductive hypothesis.]* By Theorem 8.4.1, $10 \equiv -1 \pmod{11}$ (**) because $10 - (-1) = 11 = 11 \cdot 1$. And by Theorem 8.4.3, we can multiply the left- and right-hand sides of (*) and (**) to obtain $10^k \cdot 10 \equiv (-1)^k \cdot (-1) \pmod{11}$, or, equivalently, $10^{k+1} \equiv (-1)^{k+1} \pmod{11}$. Hence $P(k+1)$ is true. □

4.13.2 (b)

Use part (a) to prove that a positive integer is divisible by 11 if, and only if, the alternating sum of its digits is divisible by 11. (For instance, the alternating sum of the digits of 82,379 is $8 - 2 + 3 - 7 + 9 = 11$ and $82,379 = 11 \cdot 7489$.)

Proof. Assume n is a positive integer. We can write n in base 10 expansion:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \cdot 10^0$$

where $a_k, \ldots, a_0$ are the decimal digits of n.

[We want to show n is divisible by 11 if and only if $a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \cdots + a_1 \cdot (-1)^1 + a_0 \cdot (-1)^0$ is divisible by 11.]

By part (a), $10^k \equiv (-1)^k \pmod{11}$. Therefore

$$n \equiv a_k \cdot (-1)^k + a_{k-1} \cdot (-1)^{k-1} + \cdots + a_1 \cdot (-1)^1 + a_0 \cdot (-1)^0 \pmod{11}$$

If n is divisible by 11, $n \equiv 0 \pmod{11}$, so by the above congruence, $a_k \cdot (-1)^k + \cdots + a_0 \cdot (-1)^0 \equiv 0 \pmod{11}$, so $a_k \cdot (-1)^k + \cdots + a_0 \cdot (-1)^0$ is divisible by 11. Similarly if $a_k + \cdots + a_0$ is divisible by 11 then n is divisible by 11 by the same reasoning. □

4.14 Exercise 14

Use the technique of Example 8.4.4 to find $14^2 \mod 55, 14^4 \mod 55, 14^8 \mod 55$, and $14^{16} \mod 55$.

Proof.

$$\begin{aligned}
14^1 \bmod 55 &= 14 \\
14^2 \bmod 55 &= 196 \bmod 55 = 31 \\
14^4 \bmod 55 &= (14^2 \bmod 55)^2 \bmod 55 = 31^2 \bmod 55 = 26 \\
14^8 \bmod 55 &= (14^4 \bmod 55)^2 \bmod 55 = 26^2 \bmod 55 = 16 \\
14^{16} \bmod 55 &= (14^8 \bmod 55)^2 \bmod 55 = 16^2 \bmod 55 = 36
\end{aligned}$$

□

4.15 Exercise 15

Use the result of exercise 14 and the technique of Example 8.4.5 to find $14^{27} \mod 55$.

Proof. $14^{27} \mod 55 = 14^{16+8+2+1} \mod 55$

$= (14^{16} \mod 55)(14^8 \mod 55)(14^2 \mod 55)(14 \mod 55) \mod 55$

$= 36 \cdot 16 \cdot 31 \cdot 14 \mod 55 = 249985 \mod 55 = 9$ □

In 16 – 18, use the techniques of example 8.4.4 and example 8.4.5 to find the given numbers.

4.16 Exercise 16

$675^{307} \mod 713$

Proof. Note that $307 = 256 + 32 + 16 + 2 + 1$.

$675^1 \mod 713 = 675$

$675^2 \mod 713 = 455625 \mod 713 = 18$

$675^4 \mod 713 = 18^2 \mod 713 = 324$

$675^8 \mod 713 = 324^2 \mod 713 = 104976 \mod 713 = 165$

$675^{16} \mod 713 = 165^2 \mod 713 = 27225 \mod 713 = 131$

$675^{32} \mod 713 = 131^2 \mod 713 = 17161 \mod 713 = 49$

$675^{64} \mod 713 = 49^2 \mod 713 = 2401 \mod 713 = 262$

$675^{128} \mod 713 = 262^2 \mod 713 = 68644 \mod 713 = 196$

$675^{256} \mod 713 = 196^2 \mod 713 = 38416 \mod 713 = 627$

So $675^{307} \mod 713 = 675^{256+32+16+2+1} \mod 713 = (675^{256} \cdot 675^{32} \cdot 675^{16} \cdot 675^2 \cdot 675^1) \mod 713 = (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \mod 713 = 48900262950 \mod 713 = 3$ □

4.17 Exercise 17

$89^{307} \mod 713$

Proof. Note that $307 = 256 + 32 + 16 + 2 + 1$.

$$
\begin{aligned}
89^1 \bmod 713 &= 89 \\
89^2 \bmod 713 &= 7921 \bmod 713 = 78 \\
89^4 \bmod 713 &= 78^2 \bmod 713 = 380 \\
89^8 \bmod 713 &= 380^2 \bmod 713 = 144400 \bmod 713 = 374 \\
89^{16} \bmod 713 &= 374^2 \bmod 713 = 139876 \bmod 713 = 128 \\
89^{32} \bmod 713 &= 128^2 \bmod 713 = 16384 \bmod 713 = 698 \\
89^{64} \bmod 713 &= 698^2 \bmod 713 = 487204 \bmod 713 = 225 \\
89^{128} \bmod 713 &= 225^2 \bmod 713 = 50625 \bmod 713 = 2 \\
89^{256} \bmod 713 &= 2^2 \bmod 713 = 4
\end{aligned}
$$

So $89^{307} \bmod 713 = 89^{256+32+16+2+1} \bmod 713 = (89^{256} \cdot 89^{32} \cdot 89^{16} \cdot 89^2 \cdot 89^1) \bmod 713 = (4 \cdot 698 \cdot 128 \cdot 78 \cdot 89) \bmod 713 = 2480904192 \bmod 713 = 15$ □

4.18 Exercise 18

$48^{307} \bmod 713$

Proof. Note that $307 = 256 + 32 + 16 + 2 + 1$.

$$
\begin{aligned}
48^1 \bmod 713 &= 48 \\
48^2 \bmod 713 &= 2304 \bmod 713 = 165 \\
48^4 \bmod 713 &= 165^2 \bmod 713 = 131 \\
48^8 \bmod 713 &= 131^2 \bmod 713 = 17161 \bmod 713 = 49 \\
48^{16} \bmod 713 &= 49^2 \bmod 713 = 2401 \bmod 713 = 262 \\
48^{32} \bmod 713 &= 262^2 \bmod 713 = 68644 \bmod 713 = 196 \\
48^{64} \bmod 713 &= 196^2 \bmod 713 = 38416 \bmod 713 = 627 \\
48^{128} \bmod 713 &= 627^2 \bmod 713 = 393129 \bmod 713 = 266 \\
48^{256} \bmod 713 &= 266^2 \bmod 713 = 70756 \bmod 713 = 169
\end{aligned}
$$

So $48^{307} \bmod 713 = 48^{256+32+16+2+1} \bmod 713 = (48^{256} \cdot 48^{32} \cdot 48^{16} \cdot 48^2 \cdot 48^1) \bmod 713 = (169 \cdot 196 \cdot 262 \cdot 165 \cdot 48) \bmod 713 = 68733624960 \bmod 713 = 12$ □

In 19 – 24, use the RSA cipher from examples 8.4.9 and 8.4.10. In 19 – 21, translate the message into its numeric equivalent and encrypt it. In 22 – 24, decrypt the ciphertext and translate the result into letters of the alphabet to discover the message.

4.19 Exercise 19

HELLO

Proof. The letters in HELLO translate numerically into 08, 05, 12, 12, and 15. By Example 8.4.9, the H is encrypted as 17. To encrypt E, we compute $5^3 \bmod 55 = 15$. To encrypt L, we compute $12^3 \bmod 55 = 23$. And to encrypt O, we compute 15^3

mod 55 = 20. Thus the ciphertext is 17 15 23 23 20. (In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.) □

4.20 Exercise 20

WELCOME

Proof. The letters in WELCOME translate numerically into 23, 05, 12, 03, 15, 13 and 05. To encrypt W, we compute $23^3 \mod 55 = 12$. To encrypt E, we compute $5^3 \mod 55 = 15$. To encrypt L, we compute $12^3 \mod 55 = 23$. To encrypt C, we compute $3^3 \mod 55 = 27$. To encrypt O, we compute $15^3 \mod 55 = 20$. And to encrypt M, we compute $13^3 \mod 55 = 52$. Thus the ciphertext is 12 15 23 27 20 52 15. □

4.21 Exercise 21

EXCELLENT

Proof. The letters in EXCELLENT translate numerically into 05, 24, 03, 05, 12, 12, 05, 14 and 20. To encrypt E, we compute $5^3 \mod 55 = 15$. To encrypt X, we compute $24^3 \mod 55 = 19$. To encrypt C, we compute $3^3 \mod 55 = 27$. To encrypt L, we compute $12^3 \mod 55 = 23$. To encrypt N, we compute $14^3 \mod 55 = 49$. To encrypt T, we compute $20^3 \mod 55 = 25$. Thus the ciphertext is 15 19 27 15 23 23 15 49 25. □

4.22 Exercise 22

13 20 20 09

Proof. By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for $13^{27}, 20^{27}$, and 9^{27} must be found and then translated into letters of the alphabet. Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$13^1 \equiv 13 \pmod{55}$	$20^1 \equiv 20 \pmod{55}$	$9^1 \equiv 9 \pmod{55}$
$13^2 \equiv 4 \pmod{55}$	$20^2 \equiv 15 \pmod{55}$	$9^2 \equiv 26 \pmod{55}$
$13^4 \equiv 4^2 \equiv 16 \pmod{55}$	$20^4 \equiv 15^2 \equiv 5 \pmod{55}$	$9^4 \equiv 26^2 \equiv 16 \pmod{55}$
$13^8 \equiv 16^2 \equiv 36 \pmod{55}$	$20^8 \equiv 5^2 \equiv 25 \pmod{55}$	$9^8 \equiv 16^2 \equiv 36 \pmod{55}$
$13^{16} \equiv 36^2 \equiv 31 \pmod{55}$	$20^{16} \equiv 25^2 \equiv 20 \pmod{55}$	$9^{16} \equiv 36^2 \equiv 31 \pmod{55}$

Then we compute

$$\begin{aligned} 13^{27} \mod 55 &= (31 \cdot 36 \cdot 4 \cdot 13) \mod 55 = 7 \\ 20^{27} \mod 55 &= (20 \cdot 25 \cdot 15 \cdot 20) \mod 55 = 15 \\ 9^{27} \mod 55 &= (31 \cdot 36 \cdot 26 \cdot 9) \mod 55 = 4 \end{aligned}$$

Finally, because 7, 15, and 4 translate into letters as G, O, and D, we see that the message is GOOD. □

4.23 Exercise 23

08 05 15

Proof. By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for $8^{27}, 5^{27}$, and 15^{27} must be found and then translated into letters of the alphabet. Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$8^1 \equiv 8 \pmod{55}$	$5^1 \equiv 5 \pmod{55}$	$15^1 \equiv 15 \pmod{55}$
$8^2 \equiv 9 \pmod{55}$	$5^2 \equiv 25 \pmod{55}$	$15^2 \equiv 5 \pmod{55}$
$8^4 \equiv 9^2 \equiv 26 \pmod{55}$	$5^4 \equiv 25^2 \equiv 20 \pmod{55}$	$15^4 \equiv 5^2 \equiv 25 \pmod{55}$
$8^8 \equiv 26^2 \equiv 16 \pmod{55}$	$5^8 \equiv 20^2 \equiv 15 \pmod{55}$	$15^8 \equiv 25^2 \equiv 20 \pmod{55}$
$8^{16} \equiv 16^2 \equiv 36 \pmod{55}$	$5^{16} \equiv 15^2 \equiv 5 \pmod{55}$	$15^{16} \equiv 20^2 \equiv 15 \pmod{55}$

Then we compute

$$\begin{aligned} 8^{27} \bmod 55 &= (36 \cdot 16 \cdot 9 \cdot 8) \bmod 55 = 2 \\ 5^{27} \bmod 55 &= (5 \cdot 15 \cdot 25 \cdot 5) \bmod 55 = 25 \\ 15^{27} \bmod 55 &= (15 \cdot 20 \cdot 5 \cdot 15) \bmod 55 = 5 \end{aligned}$$

Finally, because 2, 25, and 5 translate into letters as B, Y, and E, we see that the message is BYE. □

4.24 Exercise 24

51 14 49 15

Proof. By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for $51^{27}, 14^{27}$, and 49^{27} must be found and then translated into letters of the alphabet (15^{27} translates to E). Because $27 = 16+8+2+1$, we first perform the following computations:

$51^1 \equiv 51 \pmod{55}$	$14^1 \equiv 14 \pmod{55}$	$49^1 \equiv 49 \pmod{55}$
$51^2 \equiv 16 \pmod{55}$	$14^2 \equiv 31 \pmod{55}$	$49^2 \equiv 36 \pmod{55}$
$51^4 \equiv 16^2 \equiv 36 \pmod{55}$	$14^4 \equiv 31^2 \equiv 26 \pmod{55}$	$49^4 \equiv 36^2 \equiv 31 \pmod{55}$
$51^8 \equiv 36^2 \equiv 31 \pmod{55}$	$14^8 \equiv 26^2 \equiv 16 \pmod{55}$	$49^8 \equiv 31^2 \equiv 26 \pmod{55}$
$51^{16} \equiv 31^2 \equiv 26 \pmod{55}$	$14^{16} \equiv 16^2 \equiv 36 \pmod{55}$	$49^{16} \equiv 26^2 \equiv 16 \pmod{55}$

Then we compute

$$\begin{aligned} 51^{27} \bmod 55 &= (26 \cdot 31 \cdot 16 \cdot 51) \bmod 55 = 6 \\ 14^{27} \bmod 55 &= (36 \cdot 16 \cdot 31 \cdot 14) \bmod 55 = 9 \\ 49^{27} \bmod 55 &= (16 \cdot 26 \cdot 36 \cdot 49) \bmod 55 = 14 \end{aligned}$$

Finally, because 6, 9, 24 and 15 translate into letters as F, I, N, and E, we see that the message is FINE. □

4.25 Exercise 25

Use Theorem 5.2.2 to prove that if a and n are integers greater than 1 and $a^n - 1$ is prime, then $a = 2$ and n is prime.

Proof. By Theorem 5.2.2, using a in place of r and $n-1$ in place of n, we have $1+a+\cdots+a^{n-1} = \frac{a^n-1}{a-1}$. Multiplying both sides by $a-1$ gives $a^n-1 = (a-1)(1+a+a^2+\cdots+a^{n-1})$. So $a-1 \mid (a^n-1)$. Since a^n-1 is prime, this forces $a-1=1$ so $a=2$.

So 2^n-1 is prime. Argue by contradiction and assume n is not prime. So $n = ab$ for some integers $1 < a, b < n$. Then by Theorem 5.2.2,

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

where both $2^a - 1 > 1$ and $(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1 > 1$, so $2^n - 1$ is not prime, a contradiction. So n is prime. □

In 26 and 27, use the extended euclidean algorithm to find the greatest common divisor of the given numbers and express it as a linear combination of the two numbers.

4.26 Exercise 26

6664 and 765

Proof. Step 1: $6664 = 765 \cdot 8 + 544$, and so $544 = 6664 - 765 \cdot 8$

Step 2: $765 = 544 \cdot 1 + 221$, and so $221 = 765 - 544$

Step 3: $544 = 221 \cdot 2 + 102$, and so $102 = 544 - 221 \cdot 2$

Step 4: $221 = 102 \cdot 2 + 17$, and so $17 = 221 - 102 \cdot 2$

Step 5: $102 = 17 \cdot 6 + 0$

Thus $\gcd(6664, 765) = 17$ (which is the remainder obtained just before the final division). Substitute back through steps $4-1$ to express 17 as a linear combination of 6664 and 765:

$$\begin{aligned} 17 &= 221 - 102 \cdot 2 && = \\ &= 221 - (554 - 221 \cdot 2) && = 221 \cdot 5 - 544 \cdot 2 \\ &= (765 - 544) \cdot 5 - 544 \cdot 2 && = 765 \cdot 5 - 544 \cdot 7 \\ &= 765 \cdot 5 - (6664 - 765 \cdot 8) \cdot 7 && = (-7) \cdot 6664 + 61 \cdot 765. \end{aligned}$$

(When you have finished this final step, it is wise to verify that you have not made a mistake by checking that the final expression really does equal the greatest common divisor.) □

4.27 Exercise 27

4158 and 1568

Proof. Step 1: $4158 = 1568 \cdot 2 + 1022$, and so $1022 = 4158 - 1568 \cdot 2$

Step 2: $1568 = 1022 \cdot 1 + 546$, and so $546 = 1568 - 1022$

Step 3: $1022 = 546 \cdot 1 + 476$, and so $476 = 1022 - 546$

Step 4: $546 = 476 \cdot 1 + 70$, and so $70 = 546 - 476$

Step 5: $476 = 70 \cdot 6 + 56$, and so $56 = 476 - 70 \cdot 6$

Step 6: $70 = 56 \cdot 1 + 14$, and so $14 = 70 - 56$

Step 7: $56 = 14 \cdot 4 + 0$.

Thus $\gcd(4158, 1568) = 14$ (which is the remainder obtained just before the final division). Substitute back through steps $7 - 1$ to express 14 as a linear combination of 4158 and 1568:

$$
\begin{array}{rcl@{\qquad}rcl}
14 & = & 70 - 56 & = & \\
 & = & 70 - (476 - 70 \cdot 6) & = & 70 \cdot 7 - 476 \\
 & = & (546 - 476) \cdot 7 - 476 & = & 546 \cdot 7 - 476 \cdot 8 \\
 & = & 546 \cdot 7 - (1022 - 546) \cdot 8 & = & 546 \cdot 15 - 1022 \cdot 8 \\
 & = & (1568 - 1022) \cdot 15 - 1022 \cdot 8 & = & 1568 \cdot 15 - 1022 \cdot 23 \\
 & = & 1568 \cdot 15 - (4158 - 1568 \cdot 2) \cdot 23 & = & 1568 \cdot 61 - 4158 \cdot 23
\end{array}
$$

□

Exercises 28 and 29 refer to the following formal version of the extended euclidean algorithm.

Algorithm 8.4.1 Extended Euclidean Algorithm
Input: A, B *[integers with* $A > B > 0$*]*
Algorithm Body:
$a := A, b := B, s := 1, t := 0, u := 0, v := 1$
[pre-condition: $a = sA + tB$ *and* $b = uA + vB$*]*
while $(b \neq 0)$ *[loop invariant:* $a = sA + tB, b = uA + vB, gcd(a, b) = gcd(A, B)$*]*
  $r := a \mod b, q := a \operatorname{div} b, a := b, b := r$
  $u_{new} := s - uq, v_{new} := t - vq$
  $s := u, t := v, u := u_{new}, v := v_{new}$
end while
gcd $:= a$, *[post-condition:* $gcd(A, B) = a = sA + tB$*]*
Output: gcd *[a positive integer]*, s, t *[integers]*

In 28 and 29, for the given values of A and B, make a table showing the value of s, t, and $sA + tB$ before the start of the while loop and after each iteration of the loop.

4.28 Exercise 28

Proof.

$\boldsymbol{a}$	330	156	18	12	6
$\boldsymbol{b}$	156	18	12	6	0
$\boldsymbol{r}$		18	12	6	0
$\boldsymbol{q}$		2	8	1	2
$\boldsymbol{s}$	1	0	1	-8	9
$\boldsymbol{t}$	0	1	-2	17	-19
$\boldsymbol{u}$	0	1	-8	9	-26
$\boldsymbol{v}$	1	-2	17	-19	55
$\boldsymbol{u_{new}}$		1	-8	9	-26
$\boldsymbol{v_{new}}$		-2	17	-19	55
$\boldsymbol{sA+tB}$	330	156	18	12	6

□

4.29 Exercise 29

Proof.

$\boldsymbol{a}$	284	168	116	52	12	4
$\boldsymbol{b}$	168	116	52	12	4	0
$\boldsymbol{r}$		116	52	12	4	0
$\boldsymbol{q}$		1	1	2	4	3
$\boldsymbol{s}$	1	0	1	-1	3	-13
$\boldsymbol{t}$	0	1	-1	2	-5	22
$\boldsymbol{u}$	0	1	-1	3	-13	42
$\boldsymbol{v}$	1	-1	2	-5	22	-71
$\boldsymbol{u_{new}}$		1	-1	3	-13	42
$\boldsymbol{v_{new}}$		-1	2	-5	22	-71
$\boldsymbol{sA+tB}$	284	168	116	52	12	4

□

4.30 Exercise 30

Finish the proof of Theorem 8.4.5 by proving that if a, b, and c are as in the proof, then $c \mid b$.

Proof. By the quotient-remainder theorem $b = cp + r$ for some integers p, r with $0 \leq r < c$. Then $r = b - cp$ and substituting $c = as + bt$, we get $r = b - cp = b - (as + bt)p = b - asp - bpt = b(1 - pt) - asp$, so r is a linear combination of a and b. If $r > 0$ then r would be in S, so r would be a smaller element of S than c, a contradiction. Hence $r = 0$ and $b = cp$ which implies $c \mid b$. □

4.31 Exercise 31

4.31.1 (a)

Find an inverse for 210 modulo 13.

Proof. Step 1: $210 = 13 \cdot 16 + 2$, and so $2 = 210 - 16 \cdot 13$

Step 2: $13 = 2 \cdot 6 + 1$, and so $1 = 13 - 2 \cdot 6$

Step 3: $6 = 1 \cdot 6 + 0$, and so $gcd(210, 13) = 1$

Substitute back through steps 2 and 1: $1 = 13 - 2 \cdot 6 = 13 - (210 - 16 \cdot 13) \cdot 6 = (-6) \cdot 210 + 97 \cdot 13$

Thus $210 \cdot (-6) \equiv 1 \pmod{13}$, and so -6 is an inverse for 210 modulo 13. □

4.31.2 (b)

Find a positive inverse for 210 modulo 13.

Proof. Compute $13 - 6 = 7$. Note that $7 \equiv -6 \pmod{13}$ because $7 - (-6) = 13 = 13 \cdot 1$. Thus, by Theorem 8.4.3(3), $210 \cdot 7 \equiv 210 \cdot (-6) \pmod{13}$. By part (a), -6 is an inverse for 210 modulo 13, and so $210 \cdot (-6) \equiv 1 \pmod{13}$. It follows, by the symmetric and transitive properties of congruence, that $210 \cdot 7 \equiv 1 \pmod{13}$, and so 7 is a positive inverse for 210 modulo 13. □

4.31.3 (c)

Find a positive solution for the congruence $210x \equiv 8 \pmod{13}$.

Proof. This problem can be solved using either the result of part (a) or that of part (b). By part (b) $210 \cdot 7 \equiv 1 \pmod{13}$. Multiply both sides by 8 and apply Theorem 8.4.3(3) to obtain $210 \cdot 56 \equiv 8 \pmod{13}$. Thus a positive solution for $210x \equiv 8 \pmod{13}$ is $x = 56$. Note that the least positive residue corresponding to this solution is also a solution. By Theorem 8.4.1, $56 \equiv 4 \pmod{13}$ because $56 = 13 \cdot 4 + 4$, and so, by Theorem 8.4.3(3), $210 \cdot 56 \equiv 210 \cdot 4 \equiv 9 \pmod{13}$. This shows that 4 is also a solution for the congruence, and because $0 \leq 4 < 13$, 4 is the least positive solution for the congruence. □

4.32 Exercise 32

4.32.1 (a)

Find an inverse for 41 modulo 660.

Proof. Step 1: $660 = 41 \cdot 16 + 4$, and so $4 = 660 - 41 \cdot 16$

Step 2: $41 = 4 \cdot 10 + 1$, and so $1 = 41 - 4 \cdot 10$

Step 3: $4 = 1 \cdot 4 + 0$, and so $gcd(660, 41) = 1$

Substitute back through steps 2 and 1: $1 = 41 - 4 \cdot 10 = 41 - (660 - 41 \cdot 16) \cdot 10 = (-10) \cdot 660 + 161 \cdot 41$

Thus $41 \cdot 161 \equiv 1 \pmod{660}$, and so 161 is an inverse for 41 modulo 660. □

4.32.2 (b)

Find the least positive solution for the following congruence: $41x \equiv 125 \pmod{660}$.

Proof. By part (a) $41 \cdot 161 \equiv 1 \pmod{660}$. Multiply both sides by 125 and apply Theorem 8.4.3(3) to obtain $41 \cdot 20125 \equiv 125 \pmod{660}$. Thus a positive solution for $41x \equiv 125 \pmod{660}$ is $x = 20125$. Note that the least positive residue corresponding to this solution is also a solution. By Theorem 8.4.1, $20125 \equiv 325 \pmod{660}$ because $20125 = 660 \cdot 30 + 325$, and so, by Theorem 8.4.3(3), $41 \cdot 20125 \equiv 41 \cdot 325 \equiv 125 \pmod{660}$. This shows that 325 is also a solution for the congruence, and because $0 \leq 325 < 660$, 325 is the least positive solution for the congruence. □

4.33 Exercise 33

Use Theorem 8.4.5 to prove that for all integers a, b, and c, if $gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

Proof. Since $gcd(a, b) = 1$, by Theorem 8.4.5 $1 = as + bt$ for some integers s, t.

Since $a \mid c, au = c$ for some integer u. Since $b \mid c, bv = c$ for some integer v.

Since $1 = as + bt$, multiplying by c we get $c = cas + cbt = (bv)as + (au)bt = ab(sv + tu)$.

Notice that $sv + tu$ is an integer, thus $ab \mid c$. □

4.34 Exercise 34

Give a counterexample to show that the statement of exercise 33 is false if the hypothesis that $gcd(a, b) = 1$ is removed.

Proof. Let $a = 4, b = 6, c = 12$. Then $gcd(a, b) = gcd(4, 6) = 2 \neq 1$. And $a \mid c$ because $12 = 4 \cdot 3$ and $b \mid c$ because $12 = 6 \cdot 2$. But $ab \nmid c$ because $4 \cdot 6 = 24 \nmid 12$. □

4.35 Exercise 35

Corollary 8.4.7 guarantees the existence of an inverse modulo n for an integer a when a and n are relatively prime. Use Euclid's lemma to prove that the inverse is unique modulo n. In other words, show that if s and t are any two integers whose product with a is congruent to 1 modulo n, then s and t are congruent to each other modulo n.

Proof. Let a be any integer and let n be any positive integer, and suppose s and t are any inverses for a modulo n. Thus $as \equiv 1 \pmod{n}$ and $at \equiv 1 \pmod{n}$. Note that $ast = (as) \cdot t = (at) \cdot s$. By Theorem 8.4.3(3), $(as) \cdot t \equiv t \pmod{n}$ and $(at) \cdot s \equiv s \pmod{n}$. Thus, by symmetry and transitivity of congruence modulo n, $s \equiv t \pmod{n}$.

Because s and t were chosen arbitrarily, we conclude that any two inverses for a are congruent modulo n. □

In 36, 37, 39, and 40, use the RSA cipher with public key $n = 713 = 23 \cdot 31$ and $e = 43$. In 36 and 37, encode the messages into their numeric equivalents and encrypt them. In 39 and 40, decrypt the given ciphertext and find the original messages.

4.36 Exercise 36

HELP

Proof. The numeric equivalents of H, E, L, and P are 08, 05, 12, and 16. To encrypt these letters, the following quantities must be computed: $8^{43} \mod 713, 5^{43} \mod 713, 12^{43} \mod 713$, and $16^{43} \mod 713$. We use the fact that $43 = 32 + 8 + 2 + 1$.

$$\begin{aligned}
8^1 &= 8 = && \mod 713\\
8^2 &= 64 = && \mod 713\\
8^4 &= 64^2 = 531 && \mod 713\\
8^8 &= 531^2 = 326 && \mod 713\\
8^{16} &= 326^2 = 39 && \mod 713\\
8^{32} &= 39^2 = 95 && \mod 713
\end{aligned}$$

Thus the ciphertext is $8^{43} \mod 713 = (95 \cdot 326 \cdot 64 \cdot 8) \mod 713 = 233$.

$$\begin{aligned}
5^1 &= 5 = && \mod 713\\
5^2 &= 25 = && \mod 713\\
5^4 &= 625 = && \mod 713\\
5^8 &= 625^2 = 614 && \mod 713\\
5^{16} &= 614^2 = 532 && \mod 713\\
5^{32} &= 532^2 = 676 && \mod 713
\end{aligned}$$

Thus the ciphertext is $5^{43} \mod 713 = (676 \cdot 614 \cdot 25 \cdot 5) \mod 713 = 129$.

$$\begin{aligned}
12^1 &= 12 = && \mod 713\\
12^2 &= 144 = && \mod 713\\
12^4 &= 144^2 = 59 && \mod 713\\
12^8 &= 59^2 = 629 && \mod 713\\
12^{16} &= 629^2 = 639 && \mod 713\\
12^{32} &= 639^2 = 485 && \mod 713
\end{aligned}$$

Thus the ciphertext is $12^{43} \mod 713 = (485 \cdot 629 \cdot 144 \cdot 12) \mod 713 = 48$.

$$
\begin{array}{lllll}
16^1 & = & 16 & = & \mod 713 \\
16^2 & = & 256 & = & \mod 713 \\
16^4 & = & 256^2 & = 653 & \mod 713 \\
16^8 & = & 653^2 & = 35 & \mod 713 \\
16^{16} & = & 35^2 & = 512 & \mod 713 \\
16^{32} & = & 512^2 & = 473 & \mod 713
\end{array}
$$

Thus the ciphertext is $12^{43} \mod 713 = (473 \cdot 35 \cdot 256 \cdot 16) \mod 713 = 128$.

Therefore, the encrypted message is 233 129 048 128. (Again, note that in practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words. We kept them separate so that the numbers in the computations would be smaller and easier to work with.) □

4.37 Exercise 37

COME

Proof. The numeric equivalents of C, O, M, and E are 03, 15, 13, and 05. The letter E was encrypted in Exercise 36 as 129. To encrypt the other letters, the following quantities must be computed: $3^{43} \mod 713, 15^{43} \mod 713$, and $13^{43} \mod 713$. We use the fact that $43 = 32 + 8 + 2 + 1$.

$$
\begin{array}{lllll}
3^1 & = & 3 & = & \mod 713 \\
3^2 & = & 9 & = & \mod 713 \\
3^4 & = & 9^2 & = 81 & \mod 713 \\
3^8 & = & 81^2 & = 144 & \mod 713 \\
3^{16} & = & 144^2 & = 59 & \mod 713 \\
3^{32} & = & 59^2 & = 629 & \mod 713
\end{array}
$$

Thus the ciphertext is $3^{43} \mod 713 = (629 \cdot 144 \cdot 9 \cdot 3) \mod 713 = 675$.

$$
\begin{array}{lllll}
15^1 & = & 15 & = & \mod 713 \\
15^2 & = & 225 & = & \mod 713 \\
15^4 & = & 225^2 & = 2 & \mod 713 \\
15^8 & = & 2^2 & = 4 & \mod 713 \\
15^{16} & = & 4^2 & = 16 & \mod 713 \\
15^{32} & = & 16^2 & = 256 & \mod 713
\end{array}
$$

Thus the ciphertext is $15^{43} \mod 713 = (256 \cdot 4 \cdot 225 \cdot 15) \mod 713 = 89$.

$$
\begin{array}{lllll}
13^1 & = & 13 & = & \mod 713 \\
13^2 & = & 169 & = & \mod 713 \\
13^4 & = & 169^2 & = 41 & \mod 713
\end{array}
$$

$$
\begin{aligned}
13^8 &= 41^2 &&= 255 && \mod 713 \\
13^{16} &= 255^2 &&= 142 && \mod 713 \\
13^{32} &= 142^2 &&= 200 && \mod 713
\end{aligned}
$$

Thus the ciphertext is $13^{43} \mod 713 = (200 \cdot 255 \cdot 169 \cdot 13) \mod 713 = 476$.

Therefore, the encrypted message is 675 089 476 129. □

4.38 Exercise 38

Find the least positive inverse for 43 modulo 660.

Proof. Step 1: $660 = 43 \cdot 15 + 15$, so $15 = 660 - 43 \cdot 15$

Step 2: $43 = 15 \cdot 2 + 13$, so $13 = 43 - 15 \cdot 2$

Step 3: $15 = 13 \cdot 1 + 2$, so $2 = 15 - 13 \cdot 1$

Step 4: $13 = 2 \cdot 6 + 1$, so $1 = 13 - 2 \cdot 6$

Step 5: $2 = 1 \cdot 2 + 0$, so $gcd(660, 43) = 1$.

Stepping back through steps 4-1 we get: $1 = 13 - 2 \cdot 6 = 13 - (15 - 13) \cdot 6 = 7 \cdot 13 - 6 \cdot 15$

$= 7 \cdot (43 - 15 \cdot 2) - 6 \cdot 15 = 7 \cdot 43 - 20 \cdot 15$

$= 7 \cdot 43 - 20 \cdot (660 - 43 \cdot 15) = 307 \cdot 43 - 20 \cdot 660$

So $307 \cdot 43 \equiv 1 \pmod{660}$ and since $0 \leq 307 < 660$, 307 is the least positive inverse of 43. □

4.39 Exercise 39

675 089 089 048

Proof. By Exercise 37, 675 decrypts to C and 089 decrypts to O. By Exercise 36, 048 decrypts to L. So the plaintext is COOL. □

4.40 Exercise 40

028 018 675 129

Proof. Similarly, 675 = C, 129 = E. We must decrypt 028 and 018. By exercise 38, the decryption key, d, is 307. So we must compute $28^{307} \mod 713$ and $18^{307} \mod 713$. We use the fact $307 = 256 + 32 + 16 + 2 + 1$.

$$
\begin{array}{lllll}
28^1 & = & 28 & = & \mod 713 \\
28^2 & = & 784 & = 71 & \mod 713 \\
28^4 & = & 71^2 & = 50 & \mod 713 \\
28^8 & = & 50^2 & = 361 & \mod 713 \\
28^{16} & = & 361^2 & = 555 & \mod 713 \\
28^{32} & = & 555^2 & = 9 & \mod 713 \\
28^{64} & = & 9^2 & = 81 & \mod 713 \\
28^{128} & = & 81^2 & = 144 & \mod 713 \\
28^{256} & = & 144^2 & = 59 & \mod 713
\end{array}
$$

Thus the ciphertext is $28^{307} \mod 713 = (59 \cdot 9 \cdot 555 \cdot 71 \cdot 28) \mod 713 = 14$, which is N.

$$
\begin{array}{lllll}
18^1 & = & 18 & = & \mod 713 \\
18^2 & = & 324 & = & \mod 713 \\
18^4 & = & 324^2 & = 165 & \mod 713 \\
18^8 & = & 165^2 & = 131 & \mod 713 \\
18^{16} & = & 131^2 & = 49 & \mod 713 \\
18^{32} & = & 49^2 & = 262 & \mod 713 \\
18^{64} & = & 262^2 & = 196 & \mod 713 \\
18^{128} & = & 196^2 & = 627 & \mod 713 \\
18^{256} & = & 627^2 & = 266 & \mod 713
\end{array}
$$

Thus the ciphertext is $18^{307} \mod 713 = (266 \cdot 262 \cdot 49 \cdot 324 \cdot 18) \mod 713 = 9$, which is I.

So the plaintext is NICE. □

4.41 Exercise 41

4.41.1 (a)

Use mathematical induction and Euclid's lemma to prove that for every positive integer s, if p and $q_1, q_2, \ldots, q_s$ are prime numbers and $p \mid q_1 q_2 \cdots q_s$, then $p = q_i$ for some i with $1 \leq i \leq s$.

Proof. Let $P(s)$ be the statement: "if p and $q_1, q_2, \ldots, q_s$ are prime numbers and $p \mid q_1 q_2 \cdots q_s$, then $p = q_i$ for some i with $1 \leq i \leq s$."

Show $P(1)$ is true: Assume $p \mid q_1$. Since p and q_1 are both prime, $p = q_1$ as needed.

Show that for any integer $s \geq 1$ if $P(s)$ is true then $P(s+1)$ is true: Assume $P(s)$, and assume p and $q_1, q_2, \ldots, q_{s+1}$ are prime numbers and $p \mid q_1 q_2 \cdots q_s q_{s+1}$.

Let $a = q_1 q_2 \cdots q_s$. Then $p \mid a q_{s+1}$, and either $p = q_{s+1}$, or by Euclid's lemma $p \mid q_1 q_2 \cdots q_s$, in which case $p = q_i$ for some $1 \leq i \leq s$ by the inductive hypothesis. □

4.41.2 (b)

The uniqueness part of the unique factorization theorem for the integers says that given any integer n, if $n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$ for some positive integers r and s and prime numbers $p1 \leq p2 \leq \cdots \leq p_r$ and $q1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$ and $p_i = q_i$ for every integer i with $1 \leq i \leq r$.

Use the result of part (a) to fill in the details of the following sketch of a proof: Suppose that n is an integer with two different prime factorizations: $n = p_1p_2 \cdots p_t = q_1q_2 \cdots q_u$. All the prime factors that appear on both sides can be canceled (as many times as they appear on both sides) to arrive at the situation where $p_1p_2 \cdots p_r = q_1q_2 \cdots q_s, p_1 \leq p_2 \leq \cdots \leq p_r, q_1 \leq q_2 \leq \cdots \leq q_s$, and $p_i \neq q_j$ for any integers i and j. Then use part (a) to deduce a contradiction, and conclude that the prime factorization of n is unique except, possibly, for the order in which the prime factors are written.

Proof. Assume $p_1p_2 \cdots p_r = q_1q_2 \cdots q_s, p_1 \leq p_2 \leq \cdots \leq p_r, q_1 \leq q_2 \leq \cdots \leq q_s$, and $p_i \neq q_j$ for any integers i and j.

Notice $p_1 \mid q_1q_2 \cdots q_s$. Then by part (a), $p_1 = q_i$ for some $1 \leq i \leq s$. This contradicts the fact that $p_1 \neq q_j$ for any integer and j.

Conclusion: Our supposition was false, so n does not have two different prime factorizations. Thus the prime factorization of n is unique except, possibly, for the order in which the prime factors are written. □

4.42 Exercise 42

According to Fermat's little theorem, if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1 \pmod{p}$. Verify that this theorem gives correct results for the following:

4.42.1 (a)

$a = 15$ and $p = 7$

Proof. $a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod{7}$ because $11390625 - 1 = 7 \cdot 1627232$. □

4.42.2 (b)

$a = 8$ and $p = 11$

Proof. $a^{p-1} = 8^{10} = 1073741824 \equiv 1 \pmod{1}1$ because $1073741824 - 1 = 11 \cdot 97612893$. □

4.43 Exercise 43

Fermat's little theorem can be used to show that a number is not prime by finding a number a relatively prime to p with the property that $a^{p-1} \not\equiv 1 \pmod{p}$. However, it cannot be used to show that a number is prime. Find an example to illustrate this

fact. That is, find integers a and p such that a and p are relatively prime and $a^{p-1} \equiv 1 \pmod{p}$ but p is not prime.

Proof. Let $a = 5, p = 4$. Then a and p are relatively prime, and $a^{p-1} = 5^{4-1} = 5^3 = 125 \equiv 1 \pmod{4}$ because $125 - 1 = 124 = 4 \cdot 31$, but p is not prime because $4 = 2 \cdot 2$. □

5 Exercise Set 8.5

5.1 Exercise 1

5.1.1 (a)

Proof. □

5.1.2 (b)

Proof. □

5.1.3 (c)

Proof. □

5.1.4 (d)

Proof. □

5.2 Exercise 2

Proof. □

5.3 Exercise 3

Proof. □

5.4 Exercise 4

Proof. □

5.5 Exercise 5

Proof. □

5.6 Exercise 6

Proof. □

5.7 Exercise 7

Proof. □

5.8 Exercise 8

Proof. □

5.9 Exercise 9

Proof. □

5.10 Exercise 10

Proof. □

5.11 Exercise 11

5.11.1 (a)

Proof. □

5.11.2 (b)

Proof. □

5.11.3 (c)

Proof. □

5.11.4 (d)

Proof. □

5.11.5 (e)

Proof. □

5.11.6 (f)

Proof. □

5.11.7 (g)

Proof. □

5.12 Exercise 12

Proof. □

5.13 Exercise 13

Proof. □

5.14 Exercise 14

5.14.1 (a)

Proof. □

5.14.2 (b)

Proof. □

5.15 Exercise 15

Proof. □

5.16 Exercise 16

5.16.1 (a)

Proof. □

5.16.2 (b)

Proof. □

5.17 Exercise 17

Proof. □

5.18 Exercise 18

Proof. □

5.19 Exercise 19

Proof. □

5.20 Exercise 20

Proof. □

5.21 Exercise 21

5.21.1 (a)

Proof. □

5.21.2 (b)

Proof. □

5.22 Exercise 22

Proof. □

5.23 Exercise 23

Proof. □

5.24 Exercise 24

Proof. □

5.25 Exercise 25

Proof. □

5.26 Exercise 26

Proof. □

5.27 Exercise 27

Proof. □

5.28 Exercise 28

Proof. □

5.29 Exercise 29

Proof. □

5.30 Exercise 30

5.30.1 (a)

Proof. □

5.30.2 (b)

Proof. □

5.30.3 (c)

Proof. □

5.30.4 (d)

Proof. □

5.31 Exercise 31

Proof. □

5.32 Exercise 32

Proof. □

5.33 Exercise 33

Proof. □

5.34 Exercise 34

Proof. □

5.35 Exercise 35

Proof. □

5.36 Exercise 36

Proof. □

5.37 Exercise 37

Proof. □

5.38 Exercise 38

Proof. □

5.39 Exercise 39

Proof. □

5.40 Exercise 40

5.40.1 (a)

Proof. □

5.40.2 (b)

Proof. □

5.41 Exercise 41

5.41.1 (a)

Proof. □

5.41.2 (b)

Proof. □

5.42 Exercise 42

Proof. □

5.43 Exercise 43

Proof. □

5.44 Exercise 44

Proof. □

5.45 Exercise 45

Proof. □

5.46 Exercise 46

Proof. □

5.47 Exercise 47

Proof. □

5.48 Exercise 48

Proof. □

5.49 Exercise 49

5.49.1 (a)

Proof. □

5.49.2 (b)

Proof. □

5.50 Exercise 50

5.50.1 (a)

Proof. □

5.50.2 (b)

Proof. □

5.51 Exercise 51

5.51.1 (a)

Proof. □

5.51.2 (b)

Proof. □