
CHAPTER 2

Mathematics of Cryptography *Part I*

(Solution to Practice Set)

Review Questions

1. The set of integers is \mathbf{Z} . It contains all integral numbers from negative infinity to positive infinity. The set of residues modulo n is \mathbf{Z}_n . It contains integers from 0 to $n - 1$. The set \mathbf{Z} has non-negative (positive and zero) and negative integers; the set \mathbf{Z}_n has only non-negative integers. To map a nonnegative integer from \mathbf{Z} to \mathbf{Z}_n , we need to divide the integer by n and use the remainder; to map a negative integer from \mathbf{Z} to \mathbf{Z}_n , we need to repeatedly add n to the integer to move it to the range 0 to $n - 1$.
2. We mentioned four properties:
 - Property 1:** if $a \mid 1$, then $a = \pm 1$.
 - Property 2:** if $a \mid b$ and $b \mid a$, then $a = \pm b$.
 - Property 3:** if $a \mid b$ and $b \mid c$, then $a \mid c$.
 - Property 4:** if $a \mid b$ and $a \mid c$, then $a \mid (m \times b + n \times c)$, where m and n are arbitrary integers.
3. The number 1 is an integer with only one divisor, itself. A prime has only two divisors: 1 and itself. For example, the prime 7 has only two divisor 7 and 1. A composite has more than two divisors. For example, the composite 42 has several divisors: 1, 2, 3, 6, 7, 14, 21, and 42.
4. The greatest common divisor of two positive integers, $\gcd(a, b)$, is the largest positive integer that divides both a and b . The *Euclidean algorithm* can find the greatest common divisor of two positive integers.
5. A linear Diophantine equation of two variables is of the form $ax + by = c$. We need to find integer values for x and y that satisfy the equation. This type of equation has either no solution or an infinite number of solutions. Let $d = \gcd(a, b)$. If d does not divide c then the equation have no solitons. If d divides c , then we have an infinite number of solutions. Oné of them is called the particular solution; the rest, are called the general solutions.

6. The modulo operator takes an integer a from the set \mathbf{Z} and a positive modulus n . The operator creates a nonnegative residue, which is the remainder of dividing a by n . We mentioned three properties for the modulo operator:
- **First:** $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
 - **Second:** $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
 - **Third:** $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$
7. A residue class $[a]$ is the set of integers congruent modulo n . It is the set of all integers such that $x = a \pmod{n}$. In each set, there is one element called the least (non-negative) residue. The set of all of these least residues is \mathbf{Z}_n .
8. The set \mathbf{Z}_n is the set of all positive integer between 0 and $n - 1$. The set \mathbf{Z}_n^* is the set of all integers between 0 and $n - 1$ that are relatively prime to n . Each element in \mathbf{Z}_n has an additive inverse; each element in \mathbf{Z}_n^* has a multiplicative inverse. The extended Euclidean algorithm is used to find the multiplicative inverses in \mathbf{Z}_n^* .
9. A matrix is a rectangular array of $l \times m$ elements, in which l is the number of rows and m is the number of columns. If a matrix has only one row ($l = 1$), it is called a row matrix; if it has only one column ($m = 1$), it is called a column matrix. A square matrix is a matrix with the same number of rows and columns ($l = m$). The determinant of a square matrix \mathbf{A} is a scalar defined in linear algebra. The multiplicative inverse of a square matrix exists only if its determinant has a multiplicative inverse in the corresponding set.
10. A linear equation is an equation in which the power of each variable is 1. A linear congruence equation is a linear equation in which calculations are done modulo n . An equation of type $ax = b \pmod{n}$ can be solved by finding the multiplicative inverse of a . A set of linear equations can be solved by finding the multiplicative inverse of a matrix.

Exercises

- 11.
- a. It is false because $26 = 2 \times 13$.
 - b. It is true because $123 = 3 \times 41$.
 - c. It is true because 127 is a prime.
 - d. It is true because $21 = 3 \times 7$.
 - e. It is false because $96 = 2^5 \times 3$.
 - f. It is false because 8 is greater than 5.
- 12.

- a. $\gcd(88, 220) = 44$, as shown in the following table:

q	r_1	r_2	r
0	88	220	88
2	220	88	44
2	88	44	0
	44	0	

- b. $\gcd(300, 42) = 6$, as shown in the following table:

q	r_1	r_2	r
7	300	42	6
7	42	6	0
	6	0	

- c. $\gcd(24, 320) = 8$, as shown in the following table:

q	r_1	r_2	r
0	24	320	24
13	320	24	8
3	24	8	0
	8	0	

- d. $\gcd(401, 700) = 1$ (coprime), as shown in the following table:

q	r_1	r_2	r
0	401	700	401
1	700	401	299
1	401	299	102
2	299	102	95
1	102	95	7
13	95	7	4
1	7	4	3
1	4	3	1
3	3	1	0
	1	0	

13.

- a. $\gcd(a, b, 16) = \gcd(\gcd(a, b), 16) = \gcd(24, 16) = 8$
 b. $\gcd(a, b, c, 16) = \gcd(\gcd(a, b, c), 16) = \gcd(12, 16) = 4$
 c. $\gcd(200, 180, 450) = \gcd(\gcd(200, 180), 450) = \gcd(20, 450) = 10$
 d. $\gcd(200, 180, 450, 600) = \gcd(\gcd(200, 180, 450), 600) = \gcd(10, 600) = 10$

14.

a. $\gcd(2n + 1, n) = \gcd(n, 1) = 1$

b.

$$\gcd(201, 100) = \gcd(2 \times 100 + 1, 100) = 1$$

$$\gcd(81, 40) = \gcd(2 \times 40 + 1, 40) = 1$$

$$\gcd(501, 250) = \gcd(2 \times 250 + 1, 250) = 1$$

15.

a. $\gcd(3n + 1, 2n + 1) = \gcd(2n + 1, n) = 1$

b.

$$\gcd(301, 201) = \gcd(3 \times 100 + 1, 2 \times 100 + 1) = 1$$

$$\gcd(121, 81) = \gcd(3 \times 40 + 1, 2 \times 40 + 1) = 1$$

16.

a. We use the following table:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	4	7	4	1	0	1	0	1	0
1	7	4	3	0	1	-1	1	0	1
1	4	3	1	1	-1	2	0	1	-1
3	3	1	0	-1	2	-7	1	-1	4
	1	0		2	-7		-1	4	
	↑			↑			↑		
	gcd			s			t		

$$\gcd(4, 7) = 1 \quad \rightarrow \quad (4)(2) + (7)(-1) = 1$$

b. We use the following table:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	291	42	39	1	0	1	0	1	-6
1	42	39	3	0	1	-1	1	-6	7
13	39	3	0	1	-1	14	-6	7	-97
	3	0		-1	14		7	-97	
	↑			↑			↑		
	gcd			s			t		

$$\gcd(291, 42) = 3 \quad \rightarrow \quad (291)(-1) + (42)(7) = 3$$

c. We use the following table:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	84	320	84	1	0	1	0	1	0
3	320	84	68	0	1	-3	1	0	1
1	84	68	16	1	-3	-4	0	1	-1
4	68	16	4	-3	4	-19	1	-1	5
4	16	4	0	4	-19	80	-1	5	-21
	4	0		-19	80		5	-21	
	↑			↑			↑		
	gcd			s			t		

$$\gcd(84, 320) = 4 \rightarrow (84)(-19) + (320)(5) = 4$$

d. We use the following table:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	400	60	40	1	0	1	0	1	-6
1	60	40	20	0	1	-1	1	-6	7
2	40	20	0	1	-1	3	-6	7	-20
	20	0		-1	4		7	-20	
	↑			↑			↑		
	gcd			s			t		

$$\gcd(400, 60) = 20 \rightarrow (400)(-1) + (60)(7) = 20$$

17.

- $22 \bmod 7 = 1$
- $291 \bmod 42 = 39$
- $84 \bmod 320 = 84$
- $400 \bmod 60 = 40$

18.

- $(273 + 147) \bmod 10 = (273 \bmod 10 + 147 \bmod 10) \bmod 10 = (3 + 7) \bmod 10 = 0 \bmod 10$
- $(4223 + 17323) \bmod 10 = (4223 \bmod 10 + 17323 \bmod 10) \bmod 10 = (3 + 3) \bmod 10 = 6 \bmod 10$
- $(148 + 14432) \bmod 12 = (148 \bmod 12 + 14432 \bmod 12) \bmod 12 = (4 + 8) \bmod 12 = 0 \bmod 12$
- $(2467 + 461) \bmod 12 = (2467 \bmod 12 + 461 \bmod 12) \bmod 12 = (7 + 5) \bmod 12 = 0 \bmod 12$

19.

$$\text{a. } (125 \times 45) \bmod 10 = (125 \bmod 10 \times 45 \bmod 10) \bmod 10 = (5 \times 5) \bmod 10 = 5 \bmod 10$$

$$\text{b. } (424 \times 32) \bmod 10 = (424 \bmod 10 \times 32 \bmod 10) \bmod 10 = (4 \times 2) \bmod 10 = 8 \bmod 10$$

$$\text{c. } (144 \times 34) \bmod 10 = (144 \bmod 10 \times 34 \bmod 10) \bmod 10 = (4 \times 4) \bmod 10 = 6 \bmod 10$$

$$\text{d. } (221 \times 23) \bmod 10 = (221 \bmod 10 \times 23 \bmod 10) \bmod 10 = (1 \times 3) \bmod 10 = 3 \bmod 10$$

20.

$$\begin{aligned} \text{a. } a \bmod 10 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 10 \\ &= [(a_n \times 10^n) \bmod 10 + \dots + (a_1 \times 10^1) \bmod 10 + a_0 \bmod 10] \bmod 10 \\ &= [0 + \dots + 0 + a_0 \bmod 10] = \mathbf{a_0 \bmod 10} \end{aligned}$$

$$\begin{aligned} \text{b. } a \bmod 100 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 100 \\ &= [(a_n \times 10^n) \bmod 100 + \dots + (a_1 \times 10^1) \bmod 100 + a_0 \bmod 100] \bmod 100 \\ &= [0 + \dots + 0 + (a_1 \times 10^1) \bmod 100 + a_0 \bmod 100] \\ &= (a_1 \times 10^1) \bmod 100 + a_0 \bmod 100 = \mathbf{[a_1 \times 10^1 + a_0] \bmod 100}. \end{aligned}$$

$$\text{c. Similarly } a \bmod 1000 = \mathbf{[a_2 \times 10^2 + a_1 \times 10^1 + a_0] \bmod 1000}.$$

$$\begin{aligned} \text{21. } a \bmod 5 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 5 \\ &= [(a_n \times 10^n) \bmod 5 + \dots + (a_1 \times 10^1) \bmod 5 + a_0 \bmod 5] \bmod 5 \\ &= [0 + \dots + 0 + a_0 \bmod 5] = \mathbf{a_0 \bmod 5} \end{aligned}$$

$$\begin{aligned} \text{22. } a \bmod 2 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 2 \\ &= [(a_n \times 10^n) \bmod 2 + \dots + (a_1 \times 10^1) \bmod 2 + a_0 \bmod 2] \bmod 2 \\ &= [0 + \dots + 0 + a_0 \bmod 2] = \mathbf{a_0 \bmod 2} \end{aligned}$$

$$\begin{aligned} \text{23. } a \bmod 4 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 4 \\ &= [(a_n \times 10^n) \bmod 4 + \dots + (a_1 \times 10^1) \bmod 4 + a_0 \bmod 4] \bmod 4 \\ &= [0 + \dots + 0 + (a_1 \times 10^1) \bmod 4 + a_0 \bmod 4] = \mathbf{(a_1 \times 10^1 + a_0) \bmod 4} \end{aligned}$$

$$\begin{aligned} \text{24. } a \bmod 8 &= (a_n \times 10^n + \dots + a_2 \times 10^2 + a_1 \times 10^1 + a_0) \bmod 8 \\ &= [(a_n \times 10^n) \bmod 8 + \dots + (a_2 \times 10^2) \bmod 8 + (a_1 \times 10^1) \bmod 8 \\ &\quad + a_0 \bmod 8] \bmod 8 \\ &= [0 + \dots + 0 + (a_1 \times 10^2) \bmod 8 + (a_1 \times 10^1) \bmod 8 + a_0 \bmod 8] \\ &= \mathbf{(a_2 \times 10^2 + a_1 \times 10^1 + a_0) \bmod 8} \end{aligned}$$

$$\begin{aligned} \text{25. } a \bmod 9 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 9 \\ &= [(a_n \times 10^n) \bmod 9 + \dots + (a_1 \times 10^1) \bmod 9 + a_0 \bmod 9] \bmod 9 \\ &= \mathbf{(a_n + \dots + a_1 + a_0) \bmod 9} \end{aligned}$$

$$\begin{aligned} \text{26. } a \bmod 7 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 7 \\ &= [(a_n \times 10^n) \bmod 7 + \dots + (a_1 \times 10^1) \bmod 7 + a_0 \bmod 7] \bmod 7 \\ &= \dots + \mathbf{a_5 \times (-2) + a_4 \times (-3) + a_3 \times (-1) + a_2 \times (2) + a_1 \times (3) + a_0 \times (1)} \bmod 7 \end{aligned}$$

$$\text{For example, } 631453672 \bmod 13 = [(-1)6 + (2)3 + (1)1 + (-2)4 + (-3)5 + (-1)3 + (2)6 + (3)7 + (1)2] \bmod 7 = 3 \bmod 7$$

$$\begin{aligned}
 27. \quad a \bmod 11 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 11 \\
 &= [(a_n \times 10^n) \bmod 11 + \dots + (a_1 \times 10^1) \bmod 11 + a_0 \bmod 11] \bmod 11 \\
 &= \dots + a_3 \times (-1) + a_2 \times (1) + a_1 \times (-1) + a_0 \times (1) \bmod 11
 \end{aligned}$$

For example, $631453672 \bmod 11 = [(1)6 + (-1)3 + (1)1 + (-1)4 + (1)5 + (-1)3 + (1)6 + (-1)7 + (1)2] \bmod 11 = -8 \bmod 11 = 5 \bmod 11$

$$\begin{aligned}
 28. \quad a \bmod 13 &= (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0) \bmod 13 \\
 &= [(a_n \times 10^n) \bmod 13 + \dots + (a_1 \times 10^1) \bmod 13 + a_0 \bmod 13] \bmod 13 \\
 &= \dots + a_5 \times (4) + a_4 \times (3) + a_3 \times (-1) + a_2 \times (-4) + a_1 \times (-3) + a_0 \times (1) \bmod 13
 \end{aligned}$$

For example, $631453672 \bmod 13 = [(-4)6 + (-3)3 + (1)1 + (4)4 + (3)5 + (-1)3 + (-4)6 + (-3)7 + (1)2] \bmod 13 = 3 \bmod 13$

29.

$$a. \quad (A + N) \bmod 26 = (0 + 13) \bmod 26 = 13 \bmod 26 = \mathbf{N}$$

$$b. \quad (A + 6) \bmod 26 = (0 + 6) \bmod 26 = 6 \bmod 26 = \mathbf{G}$$

$$c. \quad (Y - 5) \bmod 26 = (24 - 5) \bmod 26 = 19 \bmod 26 = \mathbf{T}$$

$$d. \quad (C - 10) \bmod 26 = (2 - 10) \bmod 26 = -8 \bmod 26 = 18 \bmod 26 = \mathbf{S}$$

$$30. \quad (0, 0), (1, 19), (2, 18), (3, 17), (4, 16), (5, 15), (6, 14), (7, 13), (8, 12), (9, 11), (10, 10)$$

$$31. \quad (1, 1), (3, 7), (9, 9), (11, 11), (13, 17), (19, 19)$$

32.

a. We use the following table:

q	r_1	r_2	r	t_1	t_2	t
4	180	38	28	0	1	-4
1	18	28	10	1	-4	5
2	28	10	8	-4	5	-14
1	10	8	2	5	-14	19
4	8	2	0	-14	19	90
	2	0		19		
	gcd			t		

$$\gcd(180, 38) = 2 \neq 1 \quad \rightarrow \quad 38 \text{ has no inverse in } \mathbf{Z}_{180}.$$

b. We use the following table:

q	r_1	r_2	r	t_1	t_2	t
25	180	7	5	0	1	
1	7	5	2	1	-25	
2	5	2	1	-25	26	
2	2	1	0	26	-77	
	1	0		-77	180	
	gcd			t		

$$\gcd(180, 7) = 1 \rightarrow 7^{-1} \bmod 180 = -77 \bmod 180 = 103 \bmod 180.$$

c. We use the following table:

q	r_1	r_2	r	t_1	t_2	t
1	180	132	48	0	1	-1
2	132	48	36	1	-1	3
1	48	36	12	-1	3	-4
3	36	12	0	3	-4	15
	12	0		-4	15	
	gcd			t		

$$\gcd(180, 132) = 12 \neq 1 \rightarrow 132 \text{ has no inverse in } \mathbf{Z}_{180}.$$

d. We use the following table:

q	r_1	r_2	r	t_1	t_2	t
7	180	24	12	0	1	-7
2	24	12	0	1	-7	15
	12	0		-7	15	
	gcd			t		

e. $\gcd(180, 24) = 12 \neq 1 \rightarrow 24$ has no inverse in \mathbf{Z}_{180} .

33.

a. We have $a = 25$, $b = 10$ and $c = 15$. Since $d = \gcd(a, b) = 5$ divides c , there is an infinite number of solutions. The reduced equation is $5x + 2y = 3$. We solve the equation $5s + 2t = 1$ using the extended Euclidean algorithm to get $s = 1$ and $t = -2$. The particular and general solutions are

Particular:	$x_0 = (c/d) \times s = 3$	$y_0 = (c/d) \times t = -6$
General:	$x = 3 + 2 \times k$	$y = -6 - 5 \times k$ (k is an integer)

b. We have $a = 19$, $b = 13$ and $c = 20$. Since $d = \gcd(a, b) = 1$ and divides c , there is an infinite number of solutions. The reduced equation is $19x + 13y = 20$. We

solve the equation $19s + 13t = 1$ to get $s = -2$ and $t = 3$. The particular and general solutions are

Particular:	$x_0 = (c/d) \times s = -40$	$y_0 = (c/d) \times t = 60$
General:	$x = -40 + 13 \times k$	$y = 60 - 19 \times k$ (k is an integer)

- c. We have $a = 14$, $b = 21$ and $c = 77$. Since $d = \gcd(a, b) = 7$ divides c , there is an infinite number of solutions. The reduced equation is $2x + 3y = 11$. We solve the equation $2s + 3t = 1$ to get $s = -1$ and $t = 1$. The particular and general solutions are

Particular:	$x_0 = (c/d) \times s = -11$	$y_0 = (c/d) \times t = 11$
General:	$x = -11 + 3 \times k$	$y = 11 - 2 \times k$ (k is an integer)

- d. We have $a = 40$, $b = 16$ and $c = 88$. Since $d = \gcd(a, b) = 8$ divides c , there is an infinite number of solutions. The reduced equation is $5x + 2y = 11$. We solve the equation $5s + 2t = 1$ to get $s = 1$ and $t = -2$. The particular and general solutions are

Particular:	$x_0 = (c/d) \times s = 11$	$y_0 = (c/d) \times t = -22$
General:	$x = 11 + 2 \times k$	$y = -22 - 5 \times k$ (k is an integer)

34.

- a. Since $\gcd(15, 12) = 3$ and 3 does not divide 13, there is no solution.
 b. Since $\gcd(18, 30) = 6$ and 6 does not divide 20, there is no solution.
 c. Since $\gcd(15, 25) = 5$ and 5 does not divide 69, there is no solution.
 d. Since $\gcd(40, 30) = 10$ and 10 does not divide 98, there is no solution.

35. We have the equation $39x + 15y = 270$. We have $a = 39$, $b = 15$ and $c = 270$. Since $d = \gcd(a, b) = 3$ divides c , there is an infinite number of solutions. The reduced equation is $13x + 5y = 90$. We solve the equation $13s + 5t = 1$: $s = 2$ and $t = -5$. The particular and general solutions are

Particular:	$x_0 = (c/d) \times s = 180$	$y_0 = (c/d) \times t = -450$
General:	$x = 180 + 5 \times k$	$y = -450 - 13 \times k$

To find an acceptable solution (nonnegative values) for x and y , we need to start with negative values for k . Two acceptable solutions are

$k = -35 \rightarrow x = 5$ and $y = 5$	$k = -36 \rightarrow x = 0$ and $y = 18$
---	--

36. In each case, we follow three steps discussed in Section 2.4 of the textbook.

a.

Step 1: $a = 3, b = 4, n = 5 \rightarrow d = \gcd(a, n) = 1$

Since d divides b , there is only **one** solution.

Step 2: Reduction: $3x \equiv 4 \pmod{5}$

Step 3: $x_0 = (3^{-1} \times 4) \pmod{5} = 2$

b.

Step 1: $a = 4, b = 4, n = 6 \rightarrow d = \gcd(a, n) = 2$

Since d divides b , there are **two** solutions.

Step 2: Reduction: $2x \equiv 2 \pmod{3}$

Step 3: $x_0 = (2^{-1} \times 2) \pmod{3} = 1 \quad x_1 = 1 + 6 / 2 = 4$

c.

Step 1: $a = 9, b = 12, n = 7 \rightarrow d = \gcd(a, n) = 1$

Since d divides b , there is only **one** solution.

Step 2: Reduction: $9x \equiv 12 \pmod{7}$

Step 3: $x_0 = (9^{-1} \times 12) \pmod{7} = (2^{-1} \times 5) \pmod{7} = 4$

d.

Step 1: $a = 256, b = 442, n = 60 \rightarrow d = \gcd(a, n) = 4$

Since d does not divide b , there is **no** solution.

37.

a.

$3x + 5 \equiv 4 \pmod{5} \rightarrow 3x \equiv (-5 + 4) \pmod{5} \rightarrow 3x \equiv 4 \pmod{5}$

$a = 3, b = 4, n = 5 \rightarrow d = \gcd(a, n) = 1$

Since d divides b , there is only **one** solution.

Reduction: $3x \equiv 4 \pmod{5}$

$x_0 = (3^{-1} \times 4) \pmod{5} = 2$

b.

$$4x + 6 \equiv 4 \pmod{6} \rightarrow 4x \equiv (-6 + 4) \pmod{6} \rightarrow 4x \equiv 4 \pmod{6}$$

$$a = 4, b = 4, n = 6 \rightarrow d = \gcd(a, n) = 2$$

Since d divides b , there are **two** solutions.

Reduction: $2x \equiv 2 \pmod{3}$

$$x_0 = (2^{-1} \times 2) \pmod{3} = 1$$

$$x_1 = 1 + 6 / 2 = 4$$

c.

$$9x + 4 \equiv 12 \pmod{7} \rightarrow 9x \equiv (-4 + 12) \pmod{7} \rightarrow 9x \equiv 1 \pmod{7}$$

$$a = 9, b = 1, n = 7 \rightarrow d = \gcd(a, n) = 1$$

Since d divides b , there is only **one** solution.

Reduction: $9x \equiv 1 \pmod{7}$

$$x_0 = (9^{-1} \times 1) \pmod{7} = 4$$

d.

$$232x + 42 \equiv 248 \pmod{50} \rightarrow 232x \equiv 206 \pmod{50}$$

$$a = 232, b = 206, n = 50 \rightarrow d = \gcd(a, n) = 2$$

Since d divides b , there are **two** solutions.

Reduction: $116x \equiv 103 \pmod{25} \rightarrow 16x \equiv 3 \pmod{25}$

$$x_0 = (16^{-1} \times 3) \pmod{25} = 8$$

$$x_1 = 8 + 50/2 = 33$$

38.

- a. The result of multiplying the first two matrices is a 1×1 matrix, as shown below:

$$\begin{bmatrix} 3 & 7 & 10 \end{bmatrix} \times \begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix} = \left[(3 \times 2 + 7 \times 4 + 10 \times 12) \pmod{16} \right] = \left[10 \right]$$

- b. The result of multiplying the second two matrices is a 3×3 matrix, as shown below:

$$\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix} \times \begin{bmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 5 & 2 & 4 \end{bmatrix} = \begin{bmatrix} 8 & 0 & 11 \\ 11 & 1 & 1 \\ 1 & 14 & 1 \end{bmatrix}$$

39.

- a. The determinant and the inverse of matrix A are shown below:

$$A = \begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix} \rightarrow \det(A) = 3 \pmod{10} \rightarrow (\det(A))^{-1} = 7 \pmod{10}$$

$$A^{-1} = 7 \times \begin{bmatrix} 1 & 0 \\ 9 & 3 \end{bmatrix} \rightarrow A^{-1} = \begin{bmatrix} 7 & 0 \\ 3 & 1 \end{bmatrix}$$

$\text{adj}(A)$

- b. Matrix B has no inverse because $\det(B) = (4 \times 1 - 2 \times 1) \pmod{10} = 2 \pmod{10}$, which has no inverse in \mathbf{Z}_{10} .

- c. The determinant and the inverse of matrix C are shown below:

$$C = \begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix} \rightarrow \det(C) = 3 \pmod{10} \rightarrow (\det(C))^{-1} = 7 \pmod{10}$$

$$C^{-1} = \begin{bmatrix} 3 & 2 & 2 \\ 9 & 3 & 4 \\ 1 & 2 & 3 \end{bmatrix}$$

In this case, $\det(C) = 3 \pmod{10}$; its inverse in \mathbf{Z}_{10} is $7 \pmod{10}$. It can be proved that $C \times C^{-1} = \mathbf{I}$ (identity matrix).

40. Although we give the general method for every case using matrix multiplication, in cases *a* and *c*, there is no need for matrix multiplication because the coefficient of *y* (in *a*) or *x* (in *c*) is actually 0 in these two cases. These cases can be solved much easier.

- a. In this particular case, the answer can be found easier because the coefficient of y is 0 in the first equation. The solution is shown below:

$$\begin{aligned} \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 4 \\ 3 \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 2 & 1 \end{bmatrix}^{-1} \times \begin{bmatrix} 4 \\ 3 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow \begin{bmatrix} x = 3 \pmod{5} \\ y = 2 \pmod{5} \end{bmatrix} \end{aligned}$$

- b. The solution is shown below:

$$\begin{aligned} \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix}^{-1} \times \begin{bmatrix} 5 \\ 4 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 2 & 4 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 5 \\ 4 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \end{bmatrix} \rightarrow \begin{bmatrix} x = 5 \pmod{7} \\ y = 2 \pmod{7} \end{bmatrix} \end{aligned}$$

- c. The solution is shown below:

$$\begin{aligned} \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 3 \\ 5 \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}^{-1} \times \begin{bmatrix} 3 \\ 5 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 1 & 2 \\ 5 & 0 \end{bmatrix} \times \begin{bmatrix} 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} x = 6 \pmod{7} \\ y = 1 \pmod{7} \end{bmatrix} \end{aligned}$$

- d. The solution is shown below:

$$\begin{aligned} \begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 5 \\ 3 \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 6 \end{bmatrix}^{-1} \times \begin{bmatrix} 5 \\ 3 \end{bmatrix} \\ \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 6 & 5 \\ 7 & 2 \end{bmatrix} \times \begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 5 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} x = 5 \pmod{8} \\ y = 1 \pmod{8} \end{bmatrix} \end{aligned}$$

