CHAPTER 2

Mathematics of Cryptography Part I

(Solution to Odd-Numbered Problems)

Review Questions

1. The set of integers is **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 **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 **Z** to $\mathbf{Z}_n$, we need to divide the integer by n and use the remainder; to map a negative integer from **Z** to $\mathbf{Z}_n$, we need to repeatedly add n to the integer to move it to the range 0 to $n - 1$.

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.

5. A linear Diophantine equation of two variables is of the form $a\boldsymbol{x} + b\boldsymbol{y} = c$. 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. One of them is called the particular solution; the rest, are called the general solutions.

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 (nonnegative) residue. The set of all of these least residues is $\mathbf{Z}_n$.

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 **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.

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.

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. $\gcd(200, 180, 450, 600) = \gcd(\gcd(200, 180, 450), 600) = \gcd(10, 600) = 10$

15.

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

b.

$\gcd(301, 201) = \gcd(3 \times 100 + 1, 2 \times 100 + 1) = 1$
$\gcd(121, 81) = \gcd(3 \times 40 + 1, 2 \times 40 + 1) = 1$

17.

a. $22 \bmod 7 = 1$

b. $291 \bmod 42 = 39$

c. $84 \bmod 320 = 84$

d. $400 \bmod 60 = 40$

19.

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

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

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

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

21. $a \bmod 5 = (a_n \times 10^n + \ldots + a_1 \times 10^1 + a_0) \bmod 5$
$= [(a_n \times 10^n) \bmod 5 + \ldots + (a_1 \times 10^1) \bmod 5 + a_0 \bmod 5] \bmod 5$
$= [0 + \ldots + 0 + a_0 \bmod 5] =$ $\boldsymbol{a_0 \bmod 5}$

23. $a \bmod 4 = (a_n \times 10^n + \ldots + a_1 \times 10^1 + a_0) \bmod 4$
$= [(a_n \times 10^n) \bmod 4 + \ldots + (a_1 \times 10^1) \bmod 4 + a_0 \bmod 4] \bmod 4$
$= [0 + \ldots + 0 + (a_1 \times 10^1) \bmod 4 + a_0 \bmod 4] =$ $\mathbf{(a_1 \times 10^1 + a_0) \bmod 4}$

25. $a \bmod 9 = (a_n \times 10^n + \ldots + a_1 \times 10^1 + a_0) \bmod 9$
$= [(a_n \times 10^n) \bmod 9 + \ldots + (a_1 \times 10^1) \bmod 9 + a_0 \bmod 9] \bmod 9$
$=$ $\mathbf{(a_n + \ldots + a_1 + a_0) \bmod 9}$

27. $a \bmod 11 = (a_n \times 10^n + \ldots + a_1 \times 10^1 + a_0) \bmod 11$
$= [(a_n \times 10^n) \bmod 11 + \ldots + (a_1 \times 10^1) \bmod 11 + a_0 \bmod 11] \bmod 11$
$= \ldots + a_3 \times (-1) + a_2 \times (1) + a_1 \times (-1) + a_0 \times (1)] \bmod 11$

For example, 631453672 mod 11 = [(1)6 + (–1)3 + (1)1 + (–1)4 + (1)5 + (–1)3 + (1)6 + (–1)7 + (1)2] mod 11 = –8 mod 11 = 5 mod 11

29.

a. (A + N) mod 26 = (0 + 13) mod 26 = 13 mod 26 = **N**

b. (A + 6) mod 26 = (0 + 6) mod 26 = 6 mod 26 = **G**

c. (Y – 5) mod 26 = (24 –5) mod 26 = 19 mod 26 = **T**

d. (C – 10) mod 26 = (2 –10) mod 26 = –8 mod 26 = 18 mod 26 = **S**

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

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)

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

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

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

$x_1 = 8 + 50/2 = 33$

39.

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

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

$$A^{-1} = 7 \times \underbrace{\begin{bmatrix} 1 & 0 \\ 9 & 3 \end{bmatrix}}_{\text{adj}(A)} \longrightarrow A^{-1} = \begin{bmatrix} 7 & 0 \\ 3 & 1 \end{bmatrix}$$

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

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

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

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

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