

پاسخ تمرینات رمزنگاری فصل چهارم

Algebraic Structures

تهیه و تنظیم:

سید رسول موسوی – رادنوش بدریان

۱. ساختار جبری را تعریف کنید و سه ساختار جبری بحث شده در این فصل را شرح دهید.

1. The combination of the set and the operations that are applied to the elements of the set is called an *algebraic structure*. We have defined three common algebraic structures: *groups*, *rings*, and *fields*.

۲. گروه را تعریف کنید و تفاوت بین گروه و گروه جابجایی را بنویسید.

2. A group is a set of elements with a binary operation that satisfies four properties: closure, associativity, existence of identity, and existence of inverse. A commutative group, also called an abelian group, is a group in which the operator satisfies the four properties for groups plus an extra property, commutativity.

۳. حلقه را تعریف کنید و تفاوت بین حلقه و حلقه‌ی تعویض‌پذیر را توضیح دهید.

3. A ring is an algebraic structure with two operations. The first operation must satisfy all five properties required for an abelian group. The second operation must satisfy only the first two. In addition, the second operation must be distributed over the first. A commutative ring is a ring in which the commutative property is also satisfied for the second the operation.

۴. میدان را تعریف کنید و تفاوت بین میدان محدود و میدان نامحدود را توضیح دهید.

4. A field is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation (sometimes called the zero element) has no inverse. A finite field is a field with a finite number of elements. An infinite field is a field with an infinite number of elements.

۵. تعداد عوامل در میدان‌های گالویس به عنوان یک عدد اول را نشان دهید.

5. A Galois field, $GF(p^n)$, is a finite field with p^n elements. If $n = 1$, the field is sometimes referred to as $GF(p)$.

۶. یک مثال از گروه که از مجموعه‌ای از باقی‌مانده‌ها استفاده می‌کند را بیاورید.

6. An example of a group is $\mathbf{G} = \langle \mathbf{Z}_n, + \rangle$. The identity element is 0; the inverse of an element a is $-a$.

۷. یک مثال از حلقه که از مجموعه‌ای از باقی‌مانده‌ها استفاده می‌کند را بیاورید.

7. An example of a ring is $\mathbf{R} = \langle \mathbf{Z}, +, \times \rangle$. For the first operation, the identity element is 0; the inverse of an element a is $-a$. Neither the identity element nor the inverse of an element is defined for the second operation.

۸. یک مثال از میدان که از مجموعه‌ای از باقی‌مانده‌ها استفاده می‌کند بیاورید.

8. An example of a field is $\mathbf{F} = \langle \mathbf{Z}_p, +, \times \rangle$. For the first operation, the identity element is 0; the inverse of an element a is $-a$. For the second operation, the identity element is 1 and the inverse of an element a is a^{-1} . The identity element of the first operation, however, has no inverse with regard to the second operation.

۹. نحوه نمایش کلمات n بیتی را با استفاده از چندجمله‌ای را نشان دهید.

9. A polynomial of degree $n - 1$ with coefficient in $GF(2)$ can represent an n -bit word with power of each term defining the position of the bit and the coefficients of the terms defining the value of the bits.

۱۰. چندجمله‌ای‌های ساده نشدنی را تعریف کنید.

10. In $GF(2^n)$, a *reducible polynomial* of degree n is a polynomial with coefficient in $GF(2)$ that cannot be factored into a polynomial with degree of less than n . A reducible polynomial is sometimes referred to as a prime polynomial.

۱۱. برای گروه $G = \langle \mathbb{Z}_4, + \rangle$:

a. ثابت کنید که یک گروه آبلیان است

b. نتیجه $3+2$ و $3-2$ را نشان دهید

11. The group $G = \langle \mathbb{Z}_4, + \rangle$ has only four members: 0, 1, 2, and 3.

- a. For all a 's and b 's members of G , we need to prove that $a + b = b + a$. The following shows the proof (all operations are modulo 4).

$$(0 + 1) = (1 + 0)$$

$$(0 + 2) = (2 + 0)$$

$$(0 + 3) = (3 + 0)$$

$$(1 + 2) = (2 + 1)$$

$$(1 + 3) = (3 + 1)$$

$$(2 + 3) = (3 + 2)$$

b.

$$(3 + 2) \bmod 4 = 1 \bmod 4$$

$$(3 - 2) \bmod 4 = -1 \bmod 4 = 3 \bmod 4$$

۱۲. برای گروه $G = \langle \mathbb{Z}_6^*, \times \rangle$

a. ثابت کنید که یک گروه آبلیان است

b. نتیجه‌ی 5×1 و $1/5$ را نشان دهید

c. نشان دهید که چرا نباید در مورد تقسیم بر صفر در این گروه نگران نباشیم.

12. The group $\mathbf{G} = \langle \mathbb{Z}_6^*, \times \rangle$ has only two members: 1 and 5.

a. For all a 's and b 's members of G , we need to prove that $a \times b = b \times a$. Since this group has only two members, we can see that $(1 \times 5) \bmod 6 = (5 \times 1) \bmod 6$.

b.

$$(5 \times 1) \bmod 6 = 5 \bmod 6$$

$$(1 \div 5) \bmod 6 = (1 \times 5^{-1}) \bmod 6 = (1 \times 5) \bmod 6 = 5 \bmod 6$$

c. There is no need to worry about division by zero in this group, because 0 is not the member of this group.

۱۳. تنها یک عملگر برای گروه در جدول ۴-۱ تعریف شده بود. فرض کنید که این عملگر، جمع است. جدول را برای عملگر تفریق نشان دهید.

13. Assume that the operation is $(\diamond)$. We can say that $(x \diamond y)$ is the same as $x \bullet (-y)$, in which $(-y)$ is the inverse of y with respect to operation $(\bullet)$. Using Table 4.1, we can create the following table:

$\diamond$	a	b	c	d
a	a	d	c	b
b	b	a	d	c
c	c	b	a	d
d	d	c	b	a

Another way to solve the problem is to think about similarity between the group represented in Table 4.1 and the group $\mathbf{G} = \langle \mathbf{Z}_4, + \rangle$. Make the table for subtraction operation in the group $\mathbf{G} = \langle \mathbf{Z}_4, + \rangle$ and replace 0 with a , 1 with b , 2 with c , and 3 with d .

۱۴. ثابت کنید که گروه جایگشت در جدول ۴-۲ تعویض پذیر نیست.

14. It is enough to prove one single case $(a \circ b \neq b \circ a)$:

$$[1 \ 3 \ 2] \circ [2 \ 1 \ 3] = [3 \ 1 \ 2] \quad \text{but} \quad [2 \ 1 \ 3] \circ [1 \ 3 \ 2] = [2 \ 3 \ 1]$$

۱۵. تا حدودی ثابت کنید که گروه جایگشت در جدول ۴-۲ شرکت پذیری را از طریق در اختیار گذاشتن چندین مورد حل و برطرف کنید.

15. We use only two cases:

a. We first prove that

$$([1 \ 3 \ 2] \circ [2 \ 1 \ 3]) \circ [3 \ 1 \ 2] = [1 \ 3 \ 2] \circ ([2 \ 1 \ 3] \circ [3 \ 1 \ 2])$$

$$([1 \ 3 \ 2] \circ [2 \ 1 \ 3]) \circ [3 \ 1 \ 2] = [3 \ 1 \ 2] \circ [3 \ 1 \ 2] = [2 \ 3 \ 1]$$

$$[1 \ 3 \ 2] \circ ([2 \ 1 \ 3] \circ [3 \ 1 \ 2]) = [1 \ 3 \ 2] \circ [3 \ 2 \ 1] = [2 \ 3 \ 1]$$

b. We then prove that

$$([1 \ 2 \ 3] \circ [2 \ 1 \ 3]) \circ [3 \ 1 \ 2] = [1 \ 2 \ 3] \circ ([2 \ 1 \ 3] \circ [3 \ 1 \ 2])$$

$$([1 \ 2 \ 3] \circ [2 \ 1 \ 3]) \circ [3 \ 1 \ 2] = [2 \ 1 \ 3] \circ [3 \ 1 \ 2] = [3 \ 2 \ 1]$$

$$[1 \ 2 \ 3] \circ ([2 \ 1 \ 3] \circ [3 \ 1 \ 2]) = [1 \ 2 \ 3] \circ [3 \ 2 \ 1] = [3 \ 2 \ 1]$$

۱۶. جدول جایگشت را برای دو ورودی و دو خروجی مشابه جدول ۲-۴ ایجاد کنید.

16. The following shows the composition with identify elements.

$\circ$	[1 2]	[2 1]
[1 2]	[1 2]	[2 1]
[2 1]	[2 1]	[1 2]

۱۷. آلیس از سه جایگشت متوالی [1 3 2] و [3 2 1] و [2 1 3] استفاده می-کند. نشان دهید که باب چگونه می تواند فقط از یک جایگشت برای معکوس کردن فرایند استفاده کند. از جدول ۲-۴ استفاده کنید.

17. The result of $([1\ 3\ 2] \circ [3\ 2\ 1]) \circ [2\ 1\ 3] = [3\ 2\ 1]$. Bob can use the permutation [3 2 1] to reverse the operation. This proves that double or multiple permutation does not help; Alice could have used one single permutation.

۱۸. تمام زیرگروه‌های، گروه‌های زیر را پیدا کنید؟

a. $G = \langle \mathbb{Z}_{16}, + \rangle$

b. $G = \langle \mathbb{Z}_{23}, + \rangle$

c. $G = \langle \mathbb{Z}_{16}^*, \times \rangle$

d. $G = \langle \mathbb{Z}_{17}^*, \times \rangle$

18.

- a. In this case, $|G| = 16$, which means the order of each subgroup should divide 16. We can have subgroups with orders 1, 2, 4, 8, 16. The following shows some of these subgroups.

$$\begin{array}{ll} |H| = 1 & \rightarrow H = \langle \{1\}, \times \rangle \\ |H| = 2 & \rightarrow H = \langle \{1, 7\}, \times \rangle \quad H = \langle \{1, 9\}, \times \rangle \quad H = \langle \{1, 15\}, \times \rangle \\ |H| = 4 & \rightarrow H = \langle \{1, 3, 9, 11\}, \times \rangle \quad H = \langle \{1, 7, 9, 15\}, \times \rangle \\ |H| = 8 & \rightarrow H = G \end{array}$$

- b. In this case, $|G| = 23$, which means the order of each subgroup should divide 23. We can have subgroups with orders 1 and 23. The following shows some of these subgroups.

$$\begin{array}{ll} |H| = 1 & \rightarrow H = \langle \{0\}, + \rangle \\ |H| = 23 & \rightarrow H = G \end{array}$$

- c. In this case, $|G| = 8$, which means the order of each subgroup should divide 8. We can have subgroups with orders 1, 2, 4, 8. The following shows some of these subgroups.

$$\begin{array}{ll}
 |H| = 1 & \rightarrow H = \langle \{1\}, \times \rangle \\
 |H| = 2 & \rightarrow H = \langle \{1, 7\}, \times \rangle \quad H = \langle \{1, 9\}, \times \rangle \quad H = \langle \{1, 15\}, \times \rangle \\
 |H| = 4 & \rightarrow H = \langle \{1, 3, 9, 11\}, \times \rangle \quad H = \langle \{1, 7, 9, 15\}, \times \rangle \\
 |H| = 8 & \rightarrow H = G
 \end{array}$$

- d. In this case, $|G| = 16$, which means the order of each subgroup should divide 16. We can have subgroups with orders 1, 2, 4, 8, 16. The following shows some of these subgroups.

$$\begin{array}{ll}
 |H| = 1 & \rightarrow H = \langle \{1\}, \times \rangle \\
 |H| = 2 & \rightarrow H = \langle \{1, 16\}, \times \rangle \\
 |H| = 4 & \rightarrow H = \langle \{1, 4, 13, 16\}, \times \rangle \\
 |H| = 16 & \rightarrow H = G
 \end{array}$$

۱۹. با استفاده از قضیه‌ی لاگرانژ مرتبه تمام زیرگروه‌های پتانسیل زیرگروه‌های،

گروه‌های زیر را بدست آورید.

a. $G = \langle Z_{18}, + \rangle$

b. $G = \langle Z_{29}, + \rangle$

c. $G = \langle Z_{12}^*, \times \rangle$

d. $G = \langle Z_{19}^*, \times \rangle$

19.

- a. The order of the group is $|G| = 18$. The order of potential subgroups should divide 18, which means $|H|$ can be 1, 2, 3, 6, 9, and 18.
- b. The order of the group is $|G| = 29$. The order of potential subgroups should divide 29, which means $|H|$ can be 1 and 29.
- c. The order of the group is $|G| = 4$. The order of potential subgroups should divide 4, which means $|H|$ can be 1, 2, and 4.
- d. The order of the group is $|G| = 18$. The order of potential subgroups should divide 18, which means $|H|$ can be 1, 2, 3, 6, 9, and 18.

۲۰. درجات تمام عوامل در گروه‌های زیر را بدست آورید.

a. $G = \langle \mathbb{Z}_8, + \rangle$

b. $G = \langle \mathbb{Z}_7, + \rangle$

c. $G = \langle \mathbb{Z}_9^*, \times \rangle$

d. $G = \langle \mathbb{Z}_7^*, \times \rangle$

20.

a. For $G = \langle \mathbb{Z}_8, + \rangle$, we have

ord (0) = 0	ord (1) = 8	ord (2) = 4	ord (3) = 8	ord (4) = 2
ord (5) = 8	ord (6) = 4	ord (7) = 8		

b. For $G = \langle \mathbb{Z}_7, + \rangle$, we have

ord (0) = 0	ord (1) = 7	ord (2) = 7	ord (3) = 7	ord (4) = 7
ord (5) = 7	ord (6) = 7			

c. For $G = \langle \mathbb{Z}_9^*, \times \rangle$, we have

ord (1) = 0	ord (2) = 6	ord (4) = 3	ord (5) = 6	ord (7) = 3
ord (8) = 2				

d. For $G = \langle \mathbb{Z}_7^*, \times \rangle$, we have

ord (1) = 0	ord (2) = 3	ord (3) = 6	ord (4) = 6	ord (5) = 6
ord (6) = 2				

۲۱. مثال ۴-۲۵ را با استفاده از چندجمله‌ای ساده نشدنی $F(x)=x^4+x^3+1$ یکبار دیگر انجام دهید.

21. The elements $0, g^0, g^1, g^2$, and g^3 can be easily be generated, because they are the 4-bit representations of $0, 1, x^2$, and x^3 . We use the relation $f(g) = g^4 + g^3 + 1 = 0$ to generate other powers. Using this relation, we have $g^4 = g^3 + 1$. We use this relation to find the value of all elements as 4-bit words:

0	$= 0$	$= 0$	$= 0$	$\longrightarrow$	0	$= (0000)$
g^0	$= g^0$	$= g^0$	$= g^0$	$\longrightarrow$	g^0	$= (0001)$
g^1	$= g^1$	$= g^1$	$= g^1$	$\longrightarrow$	g^1	$= (0010)$
g^2	$= g^2$	$= g^2$	$= g^2$	$\longrightarrow$	g^2	$= (0100)$
g^3	$= g^3$	$= g^3$	$= g^3$	$\longrightarrow$	g^3	$= (1000)$
g^4	$= g^4$	$= g^4$	$= g^3 + 1$	$\longrightarrow$	g^4	$= (1001)$
g^5	$= g(g^4)$	$= g(g^3 + 1)$	$= g^3 + g + 1$	$\longrightarrow$	g^5	$= (1011)$
g^6	$= g(g^5)$	$= g(g^3 + g + 1)$	$= g^3 + g^2 + g + 1$	$\longrightarrow$	g^6	$= (1111)$
g^7	$= g(g^6)$	$= g(g^3 + g^2 + g + 1)$	$= g^2 + g + 1$	$\longrightarrow$	g^7	$= (0111)$
g^8	$= g(g^7)$	$= g(g^2 + g + 1)$	$= g^3 + g^2 + g$	$\longrightarrow$	g^8	$= (1110)$
g^9	$= g(g^8)$	$= g(g^3 + g^2 + g)$	$= g^2 + 1$	$\longrightarrow$	g^9	$= (0101)$
g^{10}	$= g(g^9)$	$= g(g^2 + 1)$	$= g^3 + g$	$\longrightarrow$	g^{10}	$= (1010)$
g^{11}	$= g(g^{10})$	$= g(g^3 + g)$	$= g^3 + g^2 + 1$	$\longrightarrow$	g^{11}	$= (1101)$
g^{12}	$= g(g^{11})$	$= g(g^3 + g^2 + 1)$	$= g + 1$	$\longrightarrow$	g^{12}	$= (0011)$
g^{13}	$= g(g^{12})$	$= g(g + 1)$	$= g^2 + g$	$\longrightarrow$	g^{13}	$= (0110)$
g^{14}	$= g(g^{13})$	$= g(g^2 + g)$	$= g^3 + g^2$	$\longrightarrow$	g^{14}	$= (1100)$

۲۲. مثال ۴-۲۶ را با استفاده از چندجمله‌ای ساده نشدنی $F(x)=x^4+x^3+1$ یکبار دیگر انجام دهید.

22. The following shows a few examples of addition and subtraction. Note that modulus for the exponent is $2^n - 1$ or 15.

a. We show two examples of addition (using the results of Exercise 21):

$$\begin{aligned} g^3 + g^{12} &= g^3 + (g + 1) = g^3 + g + 1 & \rightarrow & \quad (1011) = (1000) + (0011) \\ g^{10} + g^{12} &= (g^3 + g) + (g + 1) = g^3 + 1 & \rightarrow & \quad (1001) = (1010) + (0011) \end{aligned}$$

b. We show two examples of subtraction (using the results of Exercise 21):

$$\begin{aligned} g^3 - g^9 &= g^3 - (g^2 + 1) = g^3 + g^2 + 1 & \rightarrow & \quad (1101) = (1000) - (0101) \\ g^{10} - g^4 &= (g^3 + g) - (g^3 + 1) = g + 1 & \rightarrow & \quad (0011) = (1010) - (1001) \end{aligned}$$

۲۳. مثال ۴-۲۷ را با استفاده از چندجمله‌ای ساده نشدنی $F(x)=x^4+x^3+1$ یکبار دیگر انجام دهید.

23.

a. We show two examples of multiplication (using the results of Exercise 21):

$$\begin{aligned} g^3 \times g^{12} &= g^{15 \bmod 15} = g^0 = 1 & \rightarrow & \quad (0001) = (1000) \times (0011) \\ g^{10} \times g^{12} &= g^{22 \bmod 15} = g^7 = g^2 + g + 1 & \rightarrow & \quad (0111) = (1010) + (0011) \end{aligned}$$

b. We show two examples of division (using the results of Exercise 21):

$$\begin{aligned} g^3 \div g^9 &= g^{-6 \bmod 15} = g^9 = g^2 + 1 & \rightarrow & \quad (0101) = (1000) \div (0101) \\ g^{10} \div g^4 &= g^{6 \bmod 15} = g^6 = g^3 + g^2 + g + 1 & \rightarrow & \quad (1111) = (1010) - (1001) \end{aligned}$$

۲۴. کدام یک از گروه‌های زیر، میدان گالویس معتبر است؟

GH (12) .a

GF(13) .b

GF(16) .c

GF(17) .d

24.

- a. GF(12) is **not** a Galois field, because 12 cannot be written in the form p^n .
- b. GF(13) is a Galois field; 13 can be written in the form p^n ($p=13$ and $n=1$).
- c. GF(16) is a Galois field; 16 can be written in the form p^n ($p=2$ and $n=4$).
- d. GF(17) is a Galois field; 17 can be written in the form p^n ($p=17$ and $n=1$).

۲۵. برای هر کدام از کلمات n بیتی، چند جمله‌ای متناظر آن را بنویسید

10010 .a

10 .b

100001 .c

00011 .d

25.

a. $x^4 + x$

b. x

c. $x^5 + 1$

d. $x + 1$

۲۶. کلمه n بیتی را که توسط هر کدام از چندجمله‌ای‌های زیر نشان داده می‌شود را پیدا کنید.

26.

- a. 0101
- b. 00101
- c. 011
- d. 10000000

a. x^2+1 در $GF(2^4)$

b. x^2+1 در $GF(2^5)$

c. $x+1$ در $GF(2^3)$

d. x^7 در $GF(2^8)$

۲۷. در میدان $GF(7)$ نتایج را بدست آورید.

27.

- a. $5 + 3 = 8 \bmod 7 = 1 \bmod 7$
- b. $5 - 4 = 1 \bmod 7$
- c. $5 \times 3 = 15 \bmod 7 = 1 \bmod 7$
- d. $5 \div 3 = 5 \times (3^{-1}) = 5 \times 5 = 25 \bmod 7 = 4 \bmod 7$

a. $5+3$

b. $5-4$

c. 5×3

d. $5 \div 3$

۲۸. ثابت کنید که (x) و $(x+1)$ چندجمله‌ای‌های ساده نشدنی درجه 1 هستند.

28. A polynomial $f(x)$ of degree n is irreducible if $f(x) = g(x) \times h(x)$, where g and h are two polynomials, each with the degree greater than zero. According to this definition we have **degree** $(f) = \mathbf{degree} (g) + \mathbf{degree} (h)$. Based on this, we can prove that every polynomial of degree 1 is a reducible polynomial because the integer 1 cannot be sum of two integers greater than 0. Since the only two polynomials of degree 1 are $f_1(x) = x$ and $f_2(x) = x + 1$, these two polynomials are irreducible.

۲۹. ثابت کنید که (x^2+x+1) چندجمله‌ای‌های ساده نشدنی درجه ۲ هستند.

29. A polynomial $f(x)$ of degree n is irreducible if $f(x) = g(x) \times h(x)$, where g and h are two polynomials, each with the degree greater than zero. According to this defini-

tion we have **degree** $(f) = \mathbf{degree} (g) + \mathbf{degree} (h)$. Based on this, a reducible polynomial of degree 2 can be factored only as two polynomials of degree 1 ($2 = 1 + 1$). In other words, a factors of a reducible polynomial of degree 2 can be only x or $(x + 1)$ (the only two polynomials of degree 1). We can check all polynomials of degree 2 to see which one can be factored as such.

$(x^2) = (x) \times (x)$	$\rightarrow$	(x^2) is reducible
$(x^2 + 1) = (x + 1) \times (x + 1)$	$\rightarrow$	$(x^2 + 1)$ is reducible
$(x^2 + x) = (x) \times (x + 1)$	$\rightarrow$	$(x^2 + x)$ is reducible
$(x^2 + x + 1)$ cannot be factored.	$\rightarrow$	$(x^2 + x + 1)$ is irreducible

It can also be proved that $f(x) = x^2 + x + 1$ cannot be evenly divided by x or $x + 1$ because this implies that $x = 0$ or $x = -1$ must be the root of the $f(x)$, which are not $f(0) = 1$ and $f(-1) = 1$.

- 30.** A polynomial $f(x)$ of degree n is irreducible if $f(x) = g(x) \times h(x)$, where g and h are two polynomials, each with the degree greater than zero. According to this definition we have **degree** $(f) = \mathbf{degree} (g) + \mathbf{degree} (h)$. Based on this, a reducible polynomial of degree 3 can be factored only as two polynomials of degree 1 and 2 ($3 = 1 + 2$). In other words, one of the factors of a reducible polynomial of degree 3 must be x or $(x + 1)$ (the only two polynomials of degree 1). We can check all polynomials of degree 3 to see which one can be factored as such.

$(x^3) = (x) \times (x^2)$	$\rightarrow$	(x^3) is reducible
$(x^3 + 1) = (x + 1) \times (x^2 + x + 1)$	$\rightarrow$	$(x^3 + 1)$ is reducible
$(x^3 + x) = (x) \times (x^2 + 1)$	$\rightarrow$	$(x^3 + x)$ is reducible
$(x^3 + x + 1)$ cannot be factored	$\rightarrow$	$(x^3 + x + 1)$ is irreducible
$(x^3 + x^2) = (x^2) \times (x + 1)$	$\rightarrow$	$(x^3 + x^2)$ is reducible
$(x^3 + x^2 + 1)$ cannot be factored	$\rightarrow$	$(x^3 + x^2 + 1)$ is irreducible
$(x^3 + x^2 + x) = (x) \times (x^2 + x + 1)$	$\rightarrow$	$(x^3 + x^2 + x)$ is reducible
$(x^3 + x^2 + x + 1) = (x + 1) \times (x^2 + x + 1)$	$\rightarrow$	$(x^3 + x^2 + x + 1)$ is reducible

It is clear that $f_1(x) = x^3 + x + 1$ can not be factored as (x) or $(x + 1)$ because neither 0 nor -1 are the root for this polynomial. This is true for $f_2(x) = x^3 + x^2 + 1$.

۳۱. کلمات n بیتی زیر را با استفاده از چندجمله‌ای‌ها، ضرب کنید.

a. $(11) \times (10)$

b. $(1010) \times (1000)$

c. $(11100) \times (10000)$

31. We first write each number as a polynomial with coefficient in $GF(2)$. We then multiply the polynomials. Finally, we convert the result to the binary pattern.

a. $(x + 1) \times (x + 1) \rightarrow (x^2 + x + x + 1) \rightarrow (x^2 + 1) \rightarrow 101$

b. $(x^3 + x) \times (x^3) \rightarrow (x^6 + x^4) \rightarrow 1010000$

c. $(x^4 + x^3 + x^2) \times (x^4) \rightarrow (x^{16} + x^7 + x^6) \rightarrow 10000000011000000$

۳۲. معکوس ضریب زیر را در $GF(2^2)$ پیدا کنید. نکته اینکه تنها یک پیمانه برای

این میدان وجود دارد.

a. 1

b. x

c. x+1

32. The only irreducible polynomial of degree 2 is $x^2 + x + 1$. We can guess that the inverse of 1 is 1 and the other two polynomials are inverses of each other, but we use the extended Euclidean algorithm to find them.

- a. The inverse of 1 is 1, as shown in the following table.

q	r_1	r_2	r	t_1	t_2	t
$x^2 + x + 1$	$x^2 + x + 1$	1	0	0	1	1
	1	0		1	1	

- b. The inverse of x is $x + 1$, as shown in the following table.

q	r_1	r_2	r	t_1	t_2	t
$x + 1$	$x^2 + x + 1$	x	1	0	1	$x + 1$
x	x	1	0	1	$x + 1$	1
	1	0		$x + 1$	1	

- c. The inverse of $x + 1$ is x , as shown in the following table.

q	r_1	r_2	r	t_1	t_2	t
x	$x^2 + x + 1$	$x + 1$	1	0	1	x
$x + 1$	$x + 1$	1	0	1	x	1
	1	0		x	1	

۳۳. از الگوریتم اقلیدسی گسترده برای بدست آوردن معکوس (x^4+x^3+1) در $GF(2^5)$ با استفاده از واحدهای (x^5+x^2+1) استفاده کنید.

33. The inverse is $x^3 + x$, as shown below (using the extended Euclidean algorithm).

q	r_1	r_2	r	t_1	t_2	t
$x + 1$	$x^5 + x^2 + 1$	$x^4 + x^3 + 1$	$x^3 + x^2 + x$	0	1	$x + 1$
x	$x^4 + x^3 + 1$	$x^3 + x^2 + x$	$x^2 + 1$	1	$x + 1$	$x^2 + x + 1$
$x + 1$	$x^3 + x^2 + x$	$x^2 + 1$	1	$x + 1$	$x^2 + x + 1$	$x^3 + x$
$x^2 + 1$	$x^2 + 1$	1	0	$x^2 + x + 1$	$x^3 + x$	1
	1	0		$x^3 + x$	1	

۳۴. جدولی را برای جمع و ضرب $GF(2^4)$ با استفاده از (X^4+X^3+1) به عنوان پیمانه، ایجاد کنید.

34. We use the irreducible polynomial $(x^4 + x^3 + 1)$.

a. The following shows the addition table. We have used hexadecimal values to make the table shorter.

$\oplus$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	D	C
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	D	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

- b. The following shows the multiplication table. We have used hexadecimal values to make the table shorter.

$\otimes$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	9	B	D	F	1	3	5	7
3	0	3	6	5	C	F	A	9	1	2	7	4	D	E	B	8
4	0	4	8	C	9	D	1	5	B	F	3	7	2	6	A	E
5	0	5	A	F	D	8	7	2	3	6	9	C	E	D	4	1
6	0	6	C	A	1	7	D	B	2	4	E	8	3	5	F	9
7	0	7	E	9	5	2	B	C	A	D	4	3	F	8	1	6
8	0	8	9	1	B	3	2	A	F	7	6	E	4	C	D	5
9	0	9	B	2	F	6	4	D	7	E	C	5	8	1	3	A
A	0	A	D	7	3	9	E	4	6	C	B	1	5	F	8	2
B	0	B	F	4	7	C	8	3	E	5	1	A	9	2	6	D
C	0	C	1	D	2	E	3	F	4	8	5	9	6	A	7	B
D	0	D	3	E	6	B	5	8	C	1	F	2	A	7	9	4
E	0	E	5	B	A	4	F	1	D	3	8	6	7	9	2	C
F	0	F	7	8	E	1	9	6	5	A	2	D	B	4	C	3

۳۵. با استفاده از جدول ۴-۱۰ عملگرهای زیر را اجرا کنید:

- a. $(100) \div (10)$
- b. $(100) \div (000)$
- c. $(101) \div (011)$
- d. $(000) \div (111)$

35. We use Table 4.10 to find the multiplicative inverse of the second word. We then use the same table to multiply the first word with the inverse of the second word.

a. $(100) \div (010) = (100) \times (010)^{-1} = (100) \times \mathbf{(110)} = (010)$

b. $(100) \div (000) \rightarrow$ This operation is impossible because (000) has no inverse.

c. $(101) \div (011) = (101) \times (011)^{-1} = (101) \times \mathbf{(100)} = (011)$

d. $(000) \div (111) = (000) \times (111)^{-1} = (000) \times \mathbf{(101)} = (111)$

۳۶. نشان دهید که چگونه (x^3+x^2+x+1) توسط (x^2+1) در $GF(2^4)$ با استفاده از الگوریتم در جدول ۷-۴ ضرب می‌شود. از (x^4+x^3+1) به عنوان پیمانه استفاده کنید؟

36. We let $P_1 = (x^2 + 1)$, $P_2 = (x^3 + x^2 + x + 1)$, and modulus $= (x^4 + x^3 + 1)$. The following table shows the process. Note that we only need to add the modulus with the new result (if the degree of the result is greater than the degree of the modulus); no division is needed.

<i>Powers</i>	<i>Operation</i>	<i>New Result</i>	<i>Reduction</i>
$x^0 \otimes P_2$		$x^3 + x^2 + x + 1$	No
$x^1 \otimes P_2$	$x \otimes (x^3 + x^2 + x + 1)$	$x^2 + x + 1$	Yes
$x^2 \otimes P_2$	$x \otimes (x^2 + x + 1)$	$x^3 + x^2 + x$	No
$P_1 \otimes P_2 = (x^0 \otimes P_2) \oplus (x^2 \otimes P_2) = (x^3 + x^2 + x + 1) \oplus (x^3 + x^2 + x) = \mathbf{(1)}$			

The result is **(1)**, which can be proved using multiplication and division by the modulus.

۳۷. نشان دهید که چگونه (10101) توسط (10000) در $GF(2^5)$ با استفاده از الگوریتم در جدول ۸-۴ ضرب می‌شود. از (x^5+x^2+1) به عنوان پیمانه استفاده کنید.

37. We let $P_1 = (10000)$, $P_2 = (10101)$, and modulus = (100101). The following table shows the process:

<i>Powers</i>	<i>Shift-Let Operation</i>	<i>Exclusive-Or</i>
$x^0 \otimes P_2$		10101
$x^1 \otimes P_2$	01010 01010	$\oplus 00101 = 01111$
$x^2 \otimes P_2$	11110	11110
$x^3 \otimes P_2$	11100 11100	$\oplus 00101 = 11001$
$x^4 \otimes P_2$	10010 10010	$\oplus 00101 = \mathbf{10111}$
$P_1 \otimes P_2 = (x^4 \otimes P_2) = 10111$		

The result is **(10111)** or $(x^4 + x^2 + x + 1)$, which can be proved using multiplication and division by the modulus.

پایان