

1. It is given that  $f(x) = x^4 + x + 1$  is irreducible and primitive over  $GF(2)$ . Define  $\alpha$  by  $f(\alpha) = 0$ .
- (a) Set up a table for  $GF(16)$  containing the binary, exponential and polynomial representation of every element in  $GF(16)$ .
  - (b) Solve for  $x$  and  $y$ :  $\begin{cases} x + \alpha^7 y = \alpha^{10} \\ \alpha^2 x + y = \alpha^5 \end{cases}$ . Write all elements of  $GF(16)$  in exponential form.
  - (c) Find the quotient and remainder of  $x^5 + \alpha^2 x^4$  divided by  $x^2 + \alpha x + \alpha^2$ . Write all elements of  $GF(16)$  in exponential form.

*Solution* : (a) We know that  $\alpha^4 + \alpha + 1 = 0$ . So

$$\begin{aligned} \alpha^4 &= \alpha + 1 = 0011 \\ \alpha^5 &= \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 0110 \\ \alpha^6 &= \alpha\alpha^5 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = 1100 \\ \alpha^7 &= \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha + 1 + \alpha^3 = \alpha^3 + \alpha + 1 = 1011 \\ \alpha^8 &= \alpha\alpha^7 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1 = 0101 \\ \alpha^9 &= \alpha\alpha^8 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = 1010 \\ \alpha^{10} &= \alpha\alpha^9 = \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha + 1 + \alpha^2 = \alpha^2 + \alpha + 1 = 0111 \\ \alpha^{11} &= \alpha\alpha^{10} = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = 1110 \\ \alpha^{12} &= \alpha\alpha^{11} = \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1 = 1111 \\ \alpha^{13} &= \alpha\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1 = 1101 \\ \alpha^{14} &= \alpha\alpha^{13} = \alpha(\alpha^3 + \alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha = \alpha + 1 + \alpha^3 + \alpha = \alpha^3 + 1 = 1001 \\ \alpha^{15} &= \alpha\alpha^{14} = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha + 1 + \alpha = 1 \end{aligned}$$

Hence we get the following table :

binary	$GF(16)$	Polynomial in $\alpha$
0000	0	0
0001	1	1
0010	$\alpha$	$\alpha$
0100	$\alpha^2$	$\alpha^2$
1000	$\alpha^3$	$\alpha^3$
0011	$\alpha^4$	$\alpha + 1$
0110	$\alpha^5$	$\alpha^2 + \alpha$
1100	$\alpha^6$	$\alpha^3 + \alpha^2$
1011	$\alpha^7$	$\alpha^3 + \alpha + 1$
0101	$\alpha^8$	$\alpha^2 + 1$
1010	$\alpha^9$	$\alpha^3 + \alpha$
0111	$\alpha^{10}$	$\alpha^2 + \alpha + 1$
1110	$\alpha^{11}$	$\alpha^3 + \alpha^2 + \alpha$
1111	$\alpha^{12}$	$\alpha^3 + \alpha^2 + \alpha + 1$
1101	$\alpha^{13}$	$\alpha^3 + \alpha^2 + 1$
1001	$\alpha^{14}$	$\alpha^3 + 1$

(b) There are several methods of solving this system of linear equations : Cramer's rule, substitution method, elimination method. We illustrate the elimination method.

$$\begin{cases} x + \alpha^7 y = \alpha^{10} & \left| \begin{array}{c} \alpha^2 \\ 1 \end{array} \right| \left| \begin{array}{c} 1 \\ \alpha^7 \end{array} \right| \\ \alpha^2 x + y = \alpha^5 \end{cases}$$

This means that we get the first new equation by multiplying the first equation by  $\alpha^2$  and adding the second equation; we get the second new equation by multiplying the second equation by  $\alpha^7$  and adding the first equation. Hence we find

$$\begin{cases} (\alpha^9 + 1)y = \alpha^{12} + \alpha^5 \\ (1 + \alpha^9)x = \alpha^{10} + \alpha^{12} \end{cases}$$

Using the table, we find

$$\begin{aligned} \alpha^9 + 1 &= 1010 + 0001 = 1011 = \alpha^7 \\ \alpha^{12} + \alpha^5 &= 1111 + 0110 = 1001 = \alpha^{14} \\ \alpha^{10} + \alpha^{12} &= 0111 + 1111 = 1000 = \alpha^3 \end{aligned}$$

So

$$\begin{cases} \alpha^7 y = \alpha^{14} \\ \alpha^7 x = \alpha^3 \end{cases}$$

Hence

$$y = \frac{\alpha^{14}}{\alpha^7} = \alpha^7$$

and

$$x = \frac{\alpha^3}{\alpha^7} = \alpha^{-4} = \alpha^{11}$$

$$\boxed{(x, y) = (\alpha^{11}, \alpha^7)}$$

(c) Using the table and standard long division, we find

$$\begin{array}{r} x^2 + \alpha x + \alpha^2 \quad \left( \begin{array}{r} x^5 + \alpha^2 x^4 \\ x^5 + \alpha x^4 + \alpha^2 x^3 \\ \hline \alpha^5 x^4 + \alpha^2 x^3 \\ \alpha^5 x^4 + \alpha^6 x^3 + \alpha^7 x^2 \\ \hline \alpha^3 x^3 + \alpha^7 x^2 \\ \alpha^3 x^3 + \alpha^4 x^2 + \alpha^5 x \\ \hline \alpha^3 x^2 + \alpha^5 x \\ \alpha^3 x^2 + \alpha^4 x + \alpha^5 \\ \hline \alpha^8 x + \alpha^5 \end{array} \right) \end{array}$$

since

$$\begin{aligned} \alpha^2 + \alpha &= 0100 + 0010 = 0110 = \alpha^5 \\ \alpha^2 + \alpha^6 &= 0100 + 1100 = 1000 = \alpha^3 \\ \alpha^7 + \alpha^4 &= 1011 + 0011 = 1000 = \alpha^3 \\ \alpha^5 + \alpha^4 &= 0110 + 0011 = 0101 = \alpha^8 \end{aligned}$$

So

$$\boxed{x^5 + \alpha^2 x^4 = (x^2 + \alpha x + \alpha^2) \underbrace{(x^3 + \alpha^5 x^2 + \alpha^3 x + \alpha^3)}_{\text{quotient}} + \underbrace{(\alpha^8 x + \alpha^5)}_{\text{remainder}}}$$

2. Let  $\beta$  be a primitive 5-th root of unity in  $GF(16)$ . Then over  $GF(16)$ , we can factor  $x^5 - 1$  as

$$x^5 - 1 = (x - 1)(x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

Let  $\alpha$  be defined as in Exercise 1. Write all elements of  $GF(16)$  in exponential form.

- What are the choices for  $\beta$  in terms of  $\alpha$ ?
- Use cyclotomic cosets to find the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(2)$ .
- Use the table from Exercise 1 to expand the appropriate combinations of  $x - 1$ ,  $x - \beta$ ,  $x - \beta^2$ ,  $x - \beta^3$  and  $x - \beta^4$  to get the irreducible factors of  $x^5 - 1$  over  $GF(2)$ .
- We can view  $GF(4)$  as a subfield of  $GF(16)$ . Which elements of  $GF(16)$  form  $GF(4)$ ?
- Use cyclotomic cosets to find the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(4)$ .
- Use the table from Exercise 1 to expand the appropriate combinations of  $x - 1$ ,  $x - \beta$ ,  $x - \beta^2$ ,  $x - \beta^3$  and  $x - \beta^4$  to get the irreducible factors of  $x^5 - 1$  over  $GF(4)$ .

*Solution :* (a) Recall that if  $G$  is a group then for all  $g \in G$  and all  $k \in \mathbb{N}$ , we have that  $|g^k| = \frac{|g|}{\gcd(k, |g|)}$ .

Here we know that  $|\alpha| = 15$ . So for which  $1 \leq k \leq 15$  is  $|\alpha^k| = 5$ . This is equivalent with  $\gcd(k, 15) = 3$ . Hence  $k \in \{3, 6, 9, 12\}$ . So

$$\boxed{\beta \in \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}}$$

(b) We easily find that the cyclotomic cosets depending on  $n = 5$  and  $q = 2$  are

$$\{0\} \quad \text{and} \quad \{1, 2, 4, 3\}$$

Hence the irreducible factors over  $GF(2)$  are

$$x - \beta^0 \quad \text{and} \quad (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

So the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(2)$  are one and four.

(c) Note that we can find the irreducible factors of  $x^5 - 1$  over  $GF(2)$  without using any tables. Since

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

and since we know there are two irreducible factors over  $GF(2)$  (one of degree one and one of degree four), we must have that the irreducible factors are

$$x - 1 \quad \text{and} \quad (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4) = x^4 + x^3 + x^2 + x + 1$$

But we check this using the table from Ex.#1. We choose  $\beta = \alpha^3$ . Then

$$\begin{aligned} (x - \beta^1)(x - \beta^2)(x - \beta^3)(x - \beta^4) &= (x + \alpha^3)(x + \alpha^6)(x + \alpha^9)(x + \alpha^{12}) \\ &= [x^2 + (\alpha^3 + \alpha^6)x + \alpha^9] [x^2 + (\alpha^9 + \alpha^{12})x + \alpha^{21}] \\ &= [x^2 + \alpha^2 x + \alpha^9] [x^2 + \alpha^8 x + \alpha^6] \\ &= x^4 + (\alpha^2 + \alpha^8)x^3 + (\alpha^6 + \alpha^{10} + \alpha^9)x^2 + (\alpha^8 + \alpha^{17})x + \alpha^{15} \\ &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Since

$$\begin{aligned} \alpha^3 + \alpha^6 &= 1000 + 1100 = 0100 = \alpha^2 \\ \alpha^9 + \alpha^{12} &= 1010 + 1111 = 0101 = \alpha^8 \\ \alpha^2 + \alpha^8 &= 0100 + 0101 = 0001 = 1 \\ \alpha^6 + \alpha^{10} + \alpha^9 &= 1100 + 0111 + 1010 = 0001 = 1 \\ \alpha^8 + \alpha^{17} &= \alpha^8 + \alpha^2 = 1 \end{aligned}$$

The irreducible factor of  $x^5 - 1$  over  $GF(2)$  are  $x + 1$  and  $x^4 + x^3 + x^2 + x + 1$ .

(d) We know that the multiplicative group of  $GF(4)$  is a cyclic group of order 3. So if  $\gamma \in GF(16)$  has order 3, then  $GF(4) = \{0, 1, \gamma, \gamma^2\}$ . Similarly as in (a), we are looking for  $1 \leq k \leq 15$  with  $\gcd(k, 15) = 5$ . So we can choose  $\gamma = \alpha^5$ . Then

$$GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$$

(e) We easily find that the cyclotomic cosets depending on  $n = 5$  and  $q = 4$  are

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

Hence the irreducible factors over  $GF(4)$  are

$$x - \beta^0, (x - \beta^1)(x - \beta^4) \text{ and } (x - \beta^2)(x - \beta^3)$$

So the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(4)$  are one, two and two.

(f) The irreducible factors of  $x^5 - 1$  over  $GF(4)$  are (where we choose  $\beta = \alpha^3$ ) :

$$\begin{aligned} x - \beta^0 &= x + 1 \\ (x - \beta^1)(x - \beta^4) &= (x + \alpha^3)(x + \alpha^{12}) \\ &= x^2 + (\alpha^3 + \alpha^{12})x + \alpha^{15} \\ &= x^2 + \alpha^{10}x + 1 \\ (x - \beta^2)(x - \beta^3) &= (x + \alpha^6)(x + \alpha^9) \\ &= x^2 + (\alpha^6 + \alpha^9)x + \alpha^{15} \\ &= x^2 + \alpha^5x + 1 \end{aligned}$$

since

$$\begin{aligned} \alpha^3 + \alpha^{12} &= 1000 + 1111 = 0111 = \alpha^{10} \\ \alpha^6 + \alpha^9 &= 1100 + 1010 = 0110 = \alpha^5 \end{aligned}$$

The irreducible factors of  $x^5 - 1$  over  $GF(4)$  are  $x + 1$ ,  $x^2 + \alpha^5x + 1$  and  $x^2 + \alpha^{10}x + 1$ .

**3.** This exercise is about the ‘Squaring Rule’ in characteristic 2.

(a) Let  $a, b \in GF(2^n)$ . Prove that  $(a + b)^2 = a^2 + b^2$ .

(b) Let  $a_1, \dots, a_k \in GF(2^n)$ . Prove that  $(a_1 + a_2 + \dots + a_k)^2 = a_1^2 + a_2^2 + \dots + a_k^2$ .

(c) Let  $f(x)$  be a polynomial over  $GF(2)$ . Prove that  $\alpha^2$  is a root of  $f(x)$  if  $\alpha$  is a root of  $f(x)$ .

Proof : (a) We easily get that

$$(a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$$

since we are working in characteristic two.

(b) We prove this statement by induction on  $k$ . The result is obvious for  $k = 1$  and was proven in (a) for  $k = 2$ . So assume the statement is true for  $k = 1, 2, \dots, m - 1$  for some  $m \geq 3$ . Then we get that

$$\begin{aligned} (a_1 + a_2 + \dots + a_{m-1} + a_m)^2 &= [(a_1 + a_2 + \dots + a_{m-1}) + a_m]^2 \\ &= (a_1 + a_2 + \dots + a_{m-1})^2 + a_m^2 && \text{by the case ‘} k = 2 \text{’} \\ &= a_1^2 + a_2^2 + \dots + a_{m-1}^2 + a_m^2 && \text{by induction} \end{aligned}$$

(c) Put  $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$ . Note that  $a_0, a_1, a_2, \dots, a_{n-1}, a_n \in \{0, 1\}$ . Since  $0^2 = 0$  and  $1^2 = 1$ , we have that  $a_i^2 = a_i$  for  $i = 0, 1, \dots, n-1, n$ . Suppose that  $\alpha$  is a root of  $f(x)$ . So  $f(\alpha) = 0$ . Hence

$$\begin{aligned}
 0 &= [f(\alpha)]^2 \\
 &= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n)^2 \\
 &= (a_0)^2 + (a_1\alpha)^2 + (a_2\alpha^2)^2 + \cdots + (a_{n-1}\alpha^{n-1})^2 + (a_n\alpha^n)^2 && \text{by (b)} \\
 &= a_0^2 + a_1^2\alpha^2 + a_2^2(\alpha^2)^2 + \cdots + a_{n-1}^2(\alpha^{n-1})^2 + a_n^2(\alpha^n)^2 \\
 &= a_0 + a_1\alpha^2 + a_2(\alpha^2)^2 + \cdots + a_{n-1}(\alpha^2)^{n-1} + a_n(\alpha^2)^n && \text{since } a_i^2 = a_i \text{ for all } i \\
 &= f(\alpha^2)
 \end{aligned}$$

So  $f(\alpha^2) = 0$ . Hence  $\alpha^2$  is a root of  $f(x)$ . □

---



---