ECC HW1

2021年10月4日　　下午 09:42

100

2.4 Construct the prime field $GF(11)$ with modulo-11 addition and multiplication. Find all the primitive elements, and determine the orders of other elements.

The remainder of the power of each elements is summarized as follows:

Power

Element values

	1	2	3	4	5	6	7	8	9	10
0	0									
1	1									
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1					
4	4	5	9	3	1					
5	5	3	4	9	1					
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1					
10	10	1								

Therefore, the order of each elements are

1: 1　　3: 5　　5: 5　　7: 10　　9: 5

2: 10　　4: 5　　6: 10　　8: 10　　10: 1 #

and the primitive elements are 2, 6, 7, 8 #

2.7 Let λ be the characteristic of a Galois field $GF(q)$. Let 1 be the unit element of $GF(q)$. Show that the sums

$$1,\ \sum_{i=1}^{2} 1,\ \sum_{i=1}^{3} 1,\ \cdots,\ \sum_{i=1}^{\lambda-1} 1,\ \sum_{i=1}^{\lambda} 1 = 0$$

form a subfield of $GF(q)$.

We define the group $1, \sum_{i=1}^{2} 1, \dots, \sum_{i=1}^{\lambda} 1$ as I

To prove that I forms a subfield of $GF(q)$, we will prove

① I is a group under addition of $GF(q)$

② $I \setminus \{0\}$ is a group under multiplication of $GF(q)$

① I is a group under addition of GF(q)

$\because \sum_{\lambda=1}^{l} 1 + \sum_{\lambda=1}^{\lambda-l} 1 = \sum_{\lambda=1}^{\lambda} = 0$

$\therefore \sum_{\lambda=1}^{\lambda-l} 1$ is the inverse of $\sum_{\lambda=1}^{l} 1$ under addition operation

Also, since all elements are originally in GF(q)

The assotiative law is satisfy

Therefore, I forms a group under addition operation in GF(q)

② I is a group under multiplication of GF(q)

$\because \lambda$ is prime $\therefore \forall\, 1 \le l \le \lambda,\ (l, \lambda) = 1$

There exist a, b s.t. $al + b\lambda = 1$

$\Rightarrow 1 = \lambda\left(b + \frac{a - a \bmod \lambda}{\lambda} l\right) + l(a \bmod \lambda)$

$$\therefore \left(\sum_{\lambda=1}^{l} 1\right)\left(\sum_{\lambda=1}^{a \bmod \lambda} 1\right) = \sum_{\lambda=1}^{l(a \bmod \lambda)} 1$$

$$= \sum_{\lambda=1}^{1 - \lambda\left(b + \frac{a - a \bmod \lambda}{\lambda} l\right)} 1$$

$$= \sum_{\lambda=1}^{1} 1 - \left(\cancel{\sum_{\lambda=1}^{\lambda} 1}^{\,0}\right)\left(\sum_{\lambda=1}^{b + \frac{a - a \bmod \lambda}{\lambda} l} 1\right) = 1$$

Therefore, the multiplication inverse of $\sum_{\lambda=1}^{l} 1$

is $\sum_{\lambda=1}^{a \bmod \lambda} 1$

Also, since all elements are originally in GF(q)

they all satisfy the associative law

$\Rightarrow$ I is a group under multiplication in GF(q)

#

2.10 Show that $X^5 + X^3 + 1$ is irreducible over $GF(2)$.

To show it is irreducible, we need to show that x^5+x^3+1 can't be divide by all polynomials under degree $\lfloor \frac{5}{2} \rfloor = 2$.

These polynomials are x, $x+1$, x^2+1, x^2+x, x^2+x+1

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

Remainders

※

2.11 Let $f(X)$ be a polynomial of degree n over $GF(2)$. The reciprocal of $f(X)$ is defined as

$$f^*(X) = X^n f\left(\frac{1}{X}\right).$$

a. Prove that $f^*(X)$ is irreducible over $GF(2)$ if and only if $f(X)$ is irreducible over $GF(2)$.

b. Prove that $f^*(X)$ is primitive if and only if $f(X)$ is primitive.

a. This is equivalent to prove:

$f^*(X)$ is reducible over $GF(2)$ iff $f(X)$ is irreducible over $GF(2)$

"$\Leftarrow$" Supposed $f(x) \triangleq \sum_{i=0}^{n} \alpha_i x^i$ and

$f(x) = p(x)q(x)$ where

$p(x) = \sum_{i=0}^{k} \beta_i x^i$ and $q(x) = \sum_{i=0}^{n-k} \gamma_i x^i$

Then, $f^*(x) = x^n f\left(\frac{1}{x}\right) = x^n\left(\sum_{i=0}^{k} \beta_i x^{-i}\right)\left(\sum_{i=0}^{n-k} \gamma_i x^{-i}\right)$

$$= \left(x^k \sum_{i=0}^{k} \beta_i x^{-i}\right)\left(x^{n-k} \sum_{i=0}^{n-k} \gamma_i x^{-i}\right)$$

$$= \left(\sum_{i=0}^{k} \beta_{k-i} x^i\right)\left(\sum_{i=0}^{n-k} \gamma_{n-k-i} x^i\right)$$

is reducible

"$\Rightarrow$" The reverse side can be proved in the same concept. #

b. This is equivalent to prove that $f(X)$ is primitive iff $f^*(X)$ is primitive.

"$\Rightarrow$" $f(x)$ is not primitive $\Rightarrow \exists k < 2^n - 1$ s.t.

$$f(X)\,g(x) = x^k + 1$$

$$\Rightarrow f\left(\tfrac{1}{X}\right) g\left(\tfrac{1}{X}\right) = X^{-k} + 1$$

$$\Rightarrow f^*(X)\, g\left(\tfrac{1}{X}\right) = X^n f\left(\tfrac{1}{X}\right) g\left(\tfrac{1}{X}\right) = X^{n-k} + X^n$$

$$\Rightarrow f^*(X)\, x^{k-n} g\left(\tfrac{1}{x}\right) = x^k + 1$$

$$\Rightarrow f^*(X) \text{ is not primitive}$$

"$\Leftarrow$" The inverse side can be proof in the same way #

2.13 Construct a table for $GF(2^3)$ based on the primitive polynomial $p(X) = 1 + X + X^3$. Display the power, polynomial, and vector representations of each element. Determine the order of each element.

$GF(2^3)$ has $2^3 = 8$ elements

Power	Polynomial	Vector
0	0	$(0\,0\,0)$
1	1	$(1\,0\,0)$
α	α	$(0\,1\,0)$
α^2	α^2	$(0\,0\,1)$
α^3	$1+\alpha$	$(1\,1\,0)$
α^4	$\alpha+\alpha^2$	$(0\,1\,1)$
α^5	$1+\alpha+\alpha^2$	$(1\,1\,1)$
α^6	$1+\alpha^2$	$(1\,0\,1)$

2.19 Let α be a primitive element in $GF(2^4)$. Use Table 2.8 to solve the following simultaneous equations for X, Y, and Z:

$$\begin{aligned} X + \alpha^5 Y + Z &= \alpha^7, \\ X + \alpha Y + \alpha^7 Z &= \alpha^9, \\ \alpha^2 X + Y + \alpha^6 Z &= \alpha. \end{aligned}$$

$$\begin{cases} X + \alpha^5 Y + Z = \alpha^7 & — ① \\ X + \alpha Y + \alpha^7 Z = \alpha^9 & — ② \\ \alpha^2 X + Y + \alpha^6 Z = \alpha & — ③ \end{cases}$$

$$\begin{cases} X + \alpha^5 Y + Z = \alpha^7 & — ① \\ +(\alpha+\alpha^5)Y + (\alpha^7+1)Z = \alpha^9 + \alpha^7 & — ②+① — ④ \\ +(1+\alpha^7)Y + (\alpha^6+\alpha^2)Z = \alpha + \alpha^9 & — ②+\alpha^2\times① — ⑤ \end{cases}$$

$(1+\alpha^7)\times④ + (\alpha+\alpha^5)\times⑤$:

$$(\cancel{\alpha^7}+\alpha^{14}+1+\cancel{\alpha^7}+\cancel{\alpha^7}+\alpha^3+\alpha^{11}+\cancel{\alpha^7})Z$$

$$= \alpha^9+\alpha^{16}+\alpha^7+\cancel{\alpha^{14}}+\alpha^2+\alpha^{10}+\alpha^6+\cancel{\alpha^{14}}$$

$$(\cancel{1}+\cancel{\alpha^3}+\cancel{1}+\cancel{\alpha^3}+\alpha+\alpha^2+\alpha^3)Z = \cancel{\alpha}+\cancel{\alpha^3}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha}+\cancel{\alpha^3}$$

$$+\cancel{\alpha^2}+\cancel{1}+\cancel{\alpha}+\cancel{\alpha^2}+\alpha^2+\alpha^3$$

$$(1+\alpha+\alpha^2)Z = \alpha+\alpha^2$$

$$\alpha^{10}Z = \alpha^5 = \alpha^{20} \Rightarrow Z = \alpha^{10}$$

substitute into ⑤:

$$(1+\alpha^7)Y + \alpha^{16} + \alpha^{12} = \alpha + \alpha^9$$

$$(\cancel{1}+\cancel{1}+\alpha+\alpha^3)Y = \cancel{\alpha}+1+\cancel{\alpha}+\alpha^2+\cancel{\alpha^3}+\cancel{\alpha}+\cancel{\alpha}+\cancel{\alpha^3}$$

$$\therefore \alpha^9 Y = \alpha^8 = \alpha^{23} \Rightarrow Y = \alpha^{14}$$

Substitute into ①

$$X+\alpha^{19}+\alpha^{10}=\alpha^{7}$$

$$X=\cancel{1}+\cancel{\alpha}+\cancel{1}+\cancel{\alpha}+\alpha^2+1+\alpha+\alpha^3=\alpha^{12}$$

$\therefore X=\alpha^{12},\ Y=\alpha^{14},\ Z=\alpha^{10}$ #