HW4

Monday, October 24, 2022 2:07 PM

Q15: 1 → order 1.

primitive 2 → 4, 8, 5, 10, 9, 7, 3, 6, 1

order = 10

3 → 9, 5, 4, 1.

order = 5

4 → 5, 9, 3, 1

order = 5

5 → 3, 4, 9, 1

order = 5

primitive 6 → 3, 7, 9, 10, 5, 8, 4, 2, 1

order = 10

primitive 7 → 5, 2, 3, 10, 4, 6, 9, 8, 1

order = 10

primitive 8 → 9, 6, 4, 10, 3, 2, 5, 7, 1 primitive $8 \to 9, 6, 4, 10, 3, 2, 5, 7, 1$

order $= 10$

$9 \to 4, 3, 5, 1$

order $= 5$.

$10 \to 1$

order $= 2$

Q16 $f(0) = 1 \quad f(1) = 1 \Rightarrow$ No deg $= 1$ factor.

The deg $= 2$ irreducible polynomial in GF(2)

is $x^2 + x + 1$ only.

```
             1 1 1 0
      ______________
111 ) 1 0 1 0 0 1
      1 1 1
      ----------
        1 0 0
        1 1 1
      ----------
          1 1 0
          1 1 1
          ------
```

$$\Rightarrow x^5+x^3+1 \text{ is irreducible.}$$

Q17.1 We prove

$f(x)$ is reducible $\Longleftrightarrow f^*(x)$ is reducible.

proof: Suppose $g(x) \mid f(x)$ is a ~~factor~~ of $f(x)$ and $m = \deg(g(x)) < \underbrace{\deg(f(x))}_{=n}$

$$\Rightarrow f(x) = g(x)\cdot h(x).$$

Claim: $f^*(x) = g^*(x)\cdot h^*(x)$

proof: $f^*(x) = x^n \cdot f(x^{-1})$

$$= x^n \cdot g(x^{-1}) \cdot h(x^{-1})$$

$$= \left(x^m \cdot g(x^{-1})\right)\cdot\left(x^{n-m} h(x^{-1})\right)$$

$$= g^*(x)\cdot h^*(x).$$

$\rightharpoondown$ If $f(x)$ is reducible $\Rightarrow f^*(x)$ is

$\Rightarrow$ If $f(x)$ is reducible $\Rightarrow f^{*}(x)$ is reducible.

The "$\Leftarrow$" direction is proven by noting $f^{**}(x) = f(x)$. Q.E.D.

Q17.2 Suppose $f(x)$ is primitive.

$\Rightarrow$ ① $f(x)$ is irreducible $\overset{①'}{\Rightarrow} f^{*}(x)$ is irreducible

② $f(x) \cdot \ell(x) = x^{2^n - 1} - 1 = x^{2^n-1} + 1$

for some $\ell(x)$. w. $\deg(\ell(x)) = 2^n - 1 - n$

③ $f(x) \nmid x^m + 1$ for all $m < 2^n - 1$.

By ②. $\Rightarrow f^{*}(x) \cdot \ell^{*}(x) = x^{2^n-1} + 1$ ②'

Finally we prove that

$f^{*}(x) \nmid x^m + 1$ for all

$$m < 2^n - 1 \text{ ———— } ③'$$

Suppose not.

$$f^*(x) \cdot d(x) = x^m + 1 \quad \text{for some } m < 2^n - 1$$

Taking the reciprocal.

$$f(x) \cdot d^*(x) = x^m + 1,$$ which contradicts ③ $\Rightarrow$ ③' is true.

By ①', ②', ③' $\Rightarrow f^*(x)$ is primitive.

The "$\Leftarrow$" direction is by noting

$$f^{**}(x) = f(x).$$

$1 \rightarrow 0001 = 1$

$\alpha \rightarrow 0010 = 2$

$\alpha^2 \rightarrow 0100 = 4$

$\alpha^3 \rightarrow 1000 = 8$

$\alpha^{10} = 0111 = 7$

$\alpha^{11} = 1110 = 14$

$\alpha^{12} = 1111 = 15$

$\alpha^3 \rightarrow 1000 = 8$

$\alpha^4 \rightarrow 0011 = 3$

$\alpha^5 \rightarrow 0110 = 6$

$\alpha^6 \rightarrow 1100 = 12$

$\alpha^7 \rightarrow 1011 = 11$

$\alpha^8 \rightarrow 0101 = 5$

$\alpha^9 \rightarrow 1010 = 10$

α[illegible] $= 1111 = 15$

$\alpha^{13} = 1101 = 13$

$\alpha^{14} = 1001 = 9$

$(\alpha^{15} = 0001 = 1)$

8, 2, 12, 13

1, 0, 8, 6, 1 | 8, 2, 0, 11, 0, 4, 14, 1

8, 0, 12, 5, 8

2, 12, 14, 8 4

2, 0, 3, 12, 2

12, 13, 4, 6, 14,

12, 0, 10, 14, 12

13, 14, 8, 2, 1

13, 0, 2, 8, 13

$$\frac{13,0,2,8,13}{14,10,10,12}$$

$\Rightarrow$ quotient polynomial: $8x^3+2x^2+12x+13$

$$= \alpha^3 x^3 + \alpha x^2 + \alpha^6 x + \alpha^{13}$$

remainder polynomial: $14x^3+10x^2+10x+12$

$$= \alpha^{11} x^3 + \alpha^9 x^2 + \alpha^9 x + \alpha^6$$