Homework Assignment 1, Solutions

Problem 1.

(a) Let $\alpha = [0 \quad 1 \quad 0 \quad 0]$, then $ord(\alpha) \mid 15 \Rightarrow ord(\alpha)$ is 1, 3, 5 or 15.
$\alpha = [0 \quad 1 \quad 0 \quad 0] \neq [1 \quad 0 \quad 0 \quad 0]$, $\alpha^3 = [0 \quad 0 \quad 0 \quad 1] \neq [1 \quad 0 \quad 0 \quad 0]$,
$\alpha^5 = [1 \quad 0 \quad 0 \quad 0]$. $\therefore ord(\alpha) = 5$.

(b) We use trial and error. Try $[1 \quad 1 \quad 0 \quad 0]$.
$[1 \quad 1 \quad 0 \quad 0]^3 = [1 \quad 1 \quad 1 \quad 1]$, $[1 \quad 1 \quad 0 \quad 0]^5 = [1 \quad 0 \quad 1 \quad 1]$,
$\therefore$ The order of $[1 \quad 1 \quad 0 \quad 0]$ must be 15.

Problem 2.

(a) $ord(\alpha) \mid (49-1) \Rightarrow ord(\alpha)$ can only be 1, 2, 3, 4, 6, 8, 12, 16, 24, or 48.

I	1	2	3	4	6	8	12
$x^i \bmod (x^2-3)$	x	3	$3x$	2	6	4	1

$\therefore$ The order of α is 12.

(b) There are quite a few interesting ways to solve this problem. We give 3 examples below.

1. A systematic procedure to find a primitive root is by using Gauss's algorithm. Gauss's algorithm can be found on page 38, RJM Finite Field notes.
2. Use trial and error. Try $\beta = 1 + x$. And we found $\beta^4 = 2x = \alpha^5$. Let $t = ord(\beta)$. Then
$$t = \gcd(t,4) \cdot ord(\beta^4) = \gcd(t,4) \cdot ord(\alpha^5) = \gcd(t,4) \cdot \frac{12}{\gcd(12,5)} = 12 \cdot \gcd(t,4)$$
$\Rightarrow \gcd(t,4) = 4 \Rightarrow t = 48 \Rightarrow \beta = 1 + x$ is a primitive root.
$\alpha = \alpha^{25} = (\alpha^5)^5 = (\beta^4)^5 = \beta^{20}$.
3. Use trial and error. Let $\gamma_0 = 2 + x$, $\gamma_1 = 1 + 2x$. Then
$\gamma_0^4 = 6$, $\gamma_1^4 = 6x \Rightarrow (\gamma_0\gamma_1)^4 = \gamma_0^4\gamma_1^4 = 36x = x = \alpha$.
$\therefore$ *Let* $\beta = \gamma_0\gamma_1 = 1 + 5x$, then $\beta^4 = \alpha$.
$ord(\beta) = \gcd(ord(\beta),4) \cdot ord(\beta^4) = \gcd(ord(\beta),4) \cdot ord(\alpha) = 12 \cdot \gcd(ord(\beta),4)$
$\Rightarrow \gcd(ord(\beta),4) = 4 \Rightarrow ord(\beta) = 48 \Rightarrow \beta = 1 + 5x$ is a primitive root.

(c) 1. For $\beta = 1 + x$, 1 and β are linearly independent. And 1, $\beta = 1 + x$ and $\beta^2 = 4 + 2x$ are linearly dependent— $\beta^2 - 2\beta - 2 = 0$.
$\therefore$ The minimal polynomial of β is $x^2 - 2x - 2 = x^2 + 5x + 5$.

2. For $\beta = 1 + 5x$, with the same method we find:
The minimal polynomial of β is $x^2 + 5x + 3$.

Problem 3.

i	α^i	$ord(\alpha^i)$	$\deg(\alpha)$	Minimal polynomial

7	1011	15	4	$(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11}) = x^4+x^3+1$
8	0101	15	4	x^4+x+1
9	1010	5	4	$x^4+x^3+x^2+x+1$
10	0111	3	2	x^2+x+1
11	1110	15	4	x^4+x^3+1
12	1111	5	4	$x^4+x^3+x^2+x+1$
13	1101	15	4	x^4+x^3+1
14	1001	15	4	x^4+x^3+1

Problem 4.

(a) n=15, m=4. Let α be a primitive root in GF(16), then the conjugate class of α is $\{\alpha,\alpha^2,\alpha^4,\alpha^8\}$, the conjugate class of α^3 is $\{\alpha^3,\alpha^6,\alpha^{12},\alpha^9\}$, the conjugate class of α^5 is $\{\alpha^5,\alpha^{10}\}$, the conjugate class of α^7 is $\{\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}\}$.

$\because$ The generator polynomial $g(x) = lcm(mp(\alpha), mp(\alpha^3), \cdots, mp(\alpha^{2t-1}))$, $\therefore$

t	1	2	3	4	5	6	7
$\deg(g(x))$	4	8	10	14	14	14	14
Dimension	11	7	5	1	1	1	1

(b)

t	Generator polynomial g(x)
1	$g(x) = mp(\alpha) = x^4+x+1$
2	$g(x) = mp(\alpha)\cdot mp(\alpha^3) = x^8+x^7+x^6+x^4+1$
3	$g(x) = mp(\alpha)\cdot mp(\alpha^3)\cdot mp(\alpha^5) = x^{10}+x^8+x^5+x^4+x^2+x+1$
$4 \le t \le 7$	$g(x) = mp(\alpha)\cdot mp(\alpha^3)\cdot mp(\alpha^5)\cdot mp(\alpha^7) = x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9$ $+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

Problem 5.

(a) For n=7, $\beta^7 = 1$, the conjugate class of β is $\{\beta,\beta^2,\beta^4\}$, $\therefore r=3,\ k=n-r=4$.

For n=9, $\beta^9 = 1$, the conjugate class of β is $\{\beta,\beta^2,\beta^4,\beta^8,\beta^7,\beta^5\}$,

$\therefore r=6,\ k=n-r=3$.

For n=11, $\beta^{11} = 1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^5,\beta^{10},\beta^9,\beta^7,\beta^3,\beta^6\}$, $\therefore r=10,\ k=n-r=1$.

For n=13, $\beta^{13} = 1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^3,\beta^6,\beta^{12},\beta^{11},\beta^9,\beta^5,\beta^{10},\beta^7\}$, $\therefore r=12,\ k=n-r=1$.

For n=15, $\beta^{15} = 1$, the conjugate class of β is $\{\beta,\beta^2,\beta^4,\beta^8\}$,

$\therefore r=4,\ k=n-r=11$.

For n=17, $\beta^{17} = 1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^{15},\beta^{13},\beta^9\}$, $\therefore r=8,\ k=n-r=9$.

For n=19, $\beta^{19}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^{13},\beta^7,\beta^{14},\beta^9,\beta^{18},\beta^{17},\beta^{15},\beta^{11},\beta^3,\beta^6,\beta^{12},\beta^5,\beta^{10}\}$,

$\therefore r=18,\ k=n-r=1$.

For n=21, $\beta^{21}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^{11}\}$, $\therefore r=6,\ k=n-r=15$.

For n=23, $\beta^{23}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^9,\beta^{18},\beta^{13},\beta^3,\beta^6,\beta^{12}\}$, $\therefore r=11,\ k=n-r=12$.

For n=25, $\beta^{25}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^7,\beta^{14},\beta^3,\beta^6,\beta^{12},\beta^{24},\beta^{23},\beta^{21},$

$\beta^{17},\beta^9,\beta^{18},\beta^{11},\beta^{22},\beta^{19},\beta^{13}\}$,

$\therefore r=20,\ k=n-r=5$.

For n=27, $\beta^{27}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16},\beta^5,\beta^{10},\beta^{20},\beta^{13},\beta^{26},\beta^{25},\beta^{23},\beta^{19},\beta^{11},$

$\beta^{22},\beta^{17},\beta^7,\beta^{14}\}$,

$\therefore r=18,\ k=n-r=9$.

For n=29, $\beta^{29}=1$, the conjugate class of β is $\bigcup_{i=1}^{28}\{\beta^i\}$, $\therefore r=28,\ k=n-r=1$.

For n=31, $\beta^{31}=1$, the conjugate class of β is

$\{\beta,\beta^2,\beta^4,\beta^8,\beta^{16}\}$, $\therefore r=5,\ k=n-r=26$.

(b)

n	m	d	Note
7	3	d=3	Hamming code.
9	6	d≥3	
11	10	d=11	Repetition code.
13	12	d=13	Repetition code.
15	4	d=3	Hamming code.
17	8	d≥3	
19	18	d=19	Repetition code.
21	6	d≥3	
23	11	d≥5 (d=7)	Golay (23,12,d=7) code.
25	20	d≥5	
27	18	d≥3	
29	28	d=29	Repetition code.
31	5	d=3	Hamming code.