CS-527 Assignment - 6

(1) a) degree 5 over GF(2)

The general form for writing degree 5 equation is,

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e$$

where, $a, b, c, d, e \in (0, 1)$.

The above polynomial equation is irreducible if it cannot be reduced by any other irreducible polynomials of degree m or n where

$$m + n = 5.$$

The total no. of 5 degree polynomials are 2^5 i.e., 32.

Out of 32, 24 polynomials will have root 0 or 1 i.e., divisible by x or (x+1).

The remaining 8 polynomials are,

$x^5 + x^4 + x^3 + x^2 + 1$

$x^5 + x^3 + x^2 + x + 1$

$x^5 + x^4 + x^2 + x + 1$

$x^5 + x^4 + x^3 + x + 1$

$x^5 + x^4 + 1$

$x^5 + x^3 + 1$

$x^5 + x^2 + 1$

$x^5 + x + 1$

checking the irreducibility,

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

$\Rightarrow$ It's irreducible. ✓

b) $x^5+x^3+x^2+x+1 = (x^2+x+1)(x^3+x^2+x+1)+x$

$\Rightarrow$ Irreducible ✓

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

$\Rightarrow$ Irreducible ✓

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

$\Rightarrow$ Irreducible ✓

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

$\Rightarrow$ Reducible

f) $x^5+x^3+1 = (x^3+x^2+x)(x^2+x+1)+(x+1)$

$\Rightarrow$ Irreducible ✓

g) $x^5+x^2+1 = (x^3+x^2)(x^2+x+1)+1$

$\Rightarrow$ Irreducible ✓

h) $x^5+x+1 = (x^3+x^2+1)(x^2+x+1)$

$\Rightarrow$ Reducible

There are 6 irreducible polynomials of degree 5 over GF(2).

They are, $x^5+x^4+x^3+x^2+1$, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, x^5+x^3+1, x^5+x^2+1.

b) degree 3 over $GF(3)$.

General form:-

x^3+ax^2+bx+c where, $a,b,c \in [0,1,2)$.

Assuming three cases with $c=0$, $c=1$ and $c=2$.

(i) if $c=0$,

$x^3+ax^2+bx \quad \forall \; a,b \in [0,1,2]$.

The polynomials will have root 0.

which is divisible by x.

So it will be reducible polynomial.

(ii) if $c=1$,

a) x^3+x^2+x+1 is divisible by root 1. given.

$x^2(x+1)+1(x+1) \Rightarrow (x^2+1)(x+1)$. reducible //

b) x^3+x^2+1 root = 1 reducible //

c) x^3+x+1. root = 1 reducible //

d) x^3+2x^2+2x+1 root = 1 reducible //

e) x^3+2x^2+1 no root irreducible.

f) x^3+2x+1 no root irreducible

g) x^3+2x^2+x+1 no root irreducible

h) x^3+x^2+2x+1 no root irreducible.

i) x^3+1 root 2 reducible.

iii) if $C=2$,

a) x^3+2, root $=1$ reducible.

b) x^3+x^2+x+2, no root irreducible.

c) x^3+x^2+2, no root, irreducible.

d) x^3+x+2, root $=2$, reducible

e) x^3+2x^2+2, root $=2$, reducible.

f) x^3+2x+2, no root, irreducible

g) x^3+2x^2+x+2, root $=1$, reducible.

h) x^3+x^2+2x+2, root $=1$, reducible

i) x^3+2x^2+2x+2, no root, irreducible

⇒ The irreducible polynomials of degree 3 over $GF(3)$ are,

x^3+2x+1,

x^3+2x+2,

x^3+x^2+2x+1,

x^3+2x^2+1,

x^3+2x^2+x+1,

x^3+x^2+x+2,

x^3+x^2+2,

x^3+2x^2+2x+2.

(2) a) 23 mod 101.

assuming, a=23 and b=101.

$s_{-1}=1$, $s_0=0$, $t_{-1}=0$, $t_0=1$, $r_{-1}=101$, $r_0=23$.

i	r_i	q_i	s_i	t_i
-1	101	-	1	0
0	23	-	0	1
1	9	4	1	-4
2	5	2	-2	9
3	4	1	3	-13
4	1	1	-5	23

$1 = -5 \times 101 + 23 \times 22$

$1 = (23 \times 22) \bmod 101$

22 is the multiplicative inverse of 23 under mod 101.

b) $(x^6+x^4+x^2+x+1) \bmod x^8$ over GF(2).

$a \to x^8$, $b \to x^6+x^4+x^2+x+1$.

Now, constructing the table for i, r_i, q_i, s_i, t_i.

i	r_i	q_i	s_i	t_i
-1	x^8	-	1	0
0	$x^6+x^4+x^2+x+1$	-	0	1
1	x^3+x+1	x^2+1	1	x^2+1
2	x^2	x^3+1	x^3+1	$x^5+x^3+x^2$
3	$x+1$	x	x^4+x+1	$x^6+x^4+x^3+x^2+1$
4	1	$x+1$	$x^5+x^4+x^3+x^2$	$x^7+x^6+x^3+x+1$

$1 = (x^5+x^4+x^3+x^2)x^8 + (x^7+x^6+x^3+x+1)(x^6+x^4+x^2+x+1)$

$\Rightarrow x^7+x^6+x^3+x+1$ is the multiplicative inverse of $x^6+x^4+x^2+x+1$ over mrd x^8 over GF(2).

③ Given,

$t_i = t_{i-2} - q_i \cdot t_{i-1}$ —①

$s_i = s_{i-2} - q_i \cdot s_{i-1}$ —②

also, $r_i = r_{i-2} - q_i \cdot r_{i-1}$ —③.

a) $t_i r_{i-1} - t_{i-1} r_i = (-1)^i a.$

by ① & ③

$$q_i = \frac{t_{i-2} - t_i}{t_{i-1}} = \frac{r_{i-2} - r_i}{r_{i-1}}$$

$$\Rightarrow t_{i-2} \cdot r_{i-1} - t_i r_{i-1} = t_{i-1} \cdot r_{i-2} - t_i \cdot r_i$$

$$\Rightarrow t_i r_{i-1} - t_{i-1} \cdot r_i = t_{i-2} \cdot r_{i-1} - t_{i-1} \cdot r_{i-2}.$$

$$= (-1)[t_{i-1} \cdot r_{i-2} - t_{i-2} \cdot r_{i-1}]$$

$$= (-1)^2 [t_{i-2} \cdot r_{i-3} - t_{i-3} \cdot r_{i-2}]$$

$$\vdots$$

$$= (-1)^i [t_{i-i} \cdot r_{i-(i+1)} - t_{i-(i+1)} \cdot r_{i-1}]$$

$$= (-1)^i [t_0 \cdot r_{-1} - t_{-1} \cdot r_0]$$

$$= (-1)^i [1 \times a - 0 \times b]$$

$$= (-1)^i \cdot a.$$

$$\therefore t_i r_{i-1} - t_{i-1} \cdot r_i = (-1)^i \cdot a.$$ //

b) To prove,

$$s_i \cdot r_{i-1} - s_{i-1} \cdot r_i = (-1)^{i+1} \cdot b$$

from ① & ③

$$q_i = \frac{s_{i-2} - s_i}{s_{i-1}} = \frac{r_{i-2} - r_i}{r_{i-1}}$$

$$s_{i-2} \cdot r_{i-1} - s_i \cdot r_{i-1} = s_{i-1} \cdot r_{i-2} - s_{i-1} \cdot r_i$$

$$\Rightarrow s_i r_{i-1} - s_{i-1} \cdot r_i = s_{i-2} \cdot r_{i-1} - s_{i-1} \cdot r_{i-2}$$

$$= (-1)\left[s_{i-1} \cdot r_{i-2} - s_{i-2} \cdot r_{i-1}\right]$$

$$= (-1)^2 \left(s_{i-2} \cdot r_{i-3} - s_{i-3} \cdot r_{i-2}\right]$$

$$= \vdots$$

$$= (-1)^i \left[s_{i-i} \cdot r_{i-(i+1)} - s_{i-(i+1)} \cdot r_{i-1}\right.$$

$$= (-1)^i \left[s_0 \cdot r_1 - s_{-1} \cdot r_0\right]$$

$$= (-1)^i \left[0 \times a - 1 \times b\right]$$

$$= (-1)^i \left[-b\right]$$

$$= (-1)^{i+1} \cdot b$$

$$\Rightarrow \boxed{s_i r_{i-1} - s_{i-1} \cdot r_i = (-1)^{i+1} \cdot b}$$

c) $s_i \cdot t_{i-1} - s_{i-1} \cdot t_i = (-1)^{i+1}$

from ① & ②.

$$q_i = \frac{t_{i-2} - t_i}{t_{i-1}} = \frac{s_{i-2} - s_i}{s_{i-1}}$$

$$s_{i-1} \cdot t_{i-2} - s_{i-1} \cdot t_i = s_{i-2} \cdot t_{i-1} - s_i \cdot t_{i-1}$$

$$s_i \cdot t_{i-1} - s_{i-1} \cdot t_i = (-1)\left[s_{i-1} \cdot t_{i-2} - s_{i-2} \cdot t_{i-1}\right]$$

$$= (-1)^2 \left[s_{i-2} \cdot t_{i-3} - s_{i-3} \cdot t_{i-2}\right]$$

$$\vdots$$

$$= (-1)^i \left[s_{i-i} \cdot t_{i-(i+1)} - s_{i-(i+1)} \cdot t_{i-i}\right]$$

$$= (-1)^i \left[s_0 \cdot t_{-1} - s_{-1} \cdot t_0\right]$$

$$= (-1)^i \left[0 - 1\right]$$

$$= (-1)^i \left[-1\right]$$

$$= (-1)^{i+1}$$

$$\Rightarrow \boxed{s_{i-1} \cdot t_{i-1} - s_{i-1} \cdot t_i = (-1)^{i+1}} \quad //$$

d) $s_i \cdot a + t_i \cdot b = r_i$ //

$s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$, $t_0 = 1$, $r_{-1} = a$, $r_0 = b$.

Proof by induction:

Base cases:-

① $i=-1$ LHS $s_{-1}a + t_{-1}b$.

$= 1 \times a + 0 \times b = a$

RHS $= r_{-1} = a$

L.H.S = R.H.S

② $i=0$

LHS $= s_0 a + t_0 b$

$= 0 \times a + 1 \times b = b$

R.H.S $= s_0 r_0 = b$

L.H.S = R.H.S

Assume, it is true for upto $i-1$

$\Rightarrow s_{i-1}a + t_{i-1}b = r_{i-1}$

also,

$\therefore s_{i-2}a + t_{i-2}b = r_{i-2}$ ....

Proving for i,

i.e., $s_i a + t_i b = r_i$

LHS $= s_i a + t_i b$ from ① & ②

$= (s_{i-2} - q_i s_{i-1})a + (t_{i-2} - q_i t_{i-1})b$

$= [s_{i-2} \cdot a + t_{i-2} b] - q_i [s_{i-1} \cdot a + t_{i-2} b]$

$= r_{i-2} - q_i r_{i-1}$

$= r_i$ // by (3).

R.H.S $= r_i$.

$\Rightarrow$ L.H.S = R.H.S.

$$\boxed{s_i \cdot a + t_i b = r_i.}$$

e) $\deg(s_i) + \deg(r_{i-1}) = \deg(b)$.

for $(1 \le i \le n+1)$.

we know from GCD.

$\deg(s_i) > \deg(s_{i-1})$

$\deg(r_{i-1}) > \deg(r_i)$

$\Rightarrow \deg(s_i \times r_{i-1}) > \deg(s_{i-1} \times r_i)$ — (1)

$s_i r_{i-1} - s_{i-1} r_i = (-1)^{i+1} b$ — (2)

from (1) & (2)

$\deg(s_i r_{i-1}) = \deg(b)$.

$$\boxed{\Rightarrow \deg(s_i) + \deg(r_{i-1}) = \deg(b)}$$

f) To prove,

$\deg(t_i) + \deg(r_{i-1}) = \deg(a)$.

for i, $1 \le i \le n+1$.

Similarly,

$$\deg(t_i) > \deg(t_{i-1})$$

$$\deg(r_{i-1}) > \deg(r_i).$$

$$\Rightarrow \deg(t_i\, r_{i-1}) > \deg(t_{i-1} \cdot r_i) \quad -①$$

$$t_i \cdot r_{i-1} - t_{i-1} \cdot r_i = (-1)^i \cdot a \quad -②$$

from ① & ②

$$\deg(t_i\, r_{i-1}) = \deg(a).$$

$$\Rightarrow \boxed{\deg(t_i) + \deg(r_{i-1}) = \deg(a).}$$

④ a) $x^{15} - 1$ over GF(2).

$$x^{15} - 1 = x^{2^4 - 1} - 1$$

$\Rightarrow$ GF(2^4) $\Rightarrow$ $x^4 + x + 1 = 0$

irreducible polynomial.

let α be a root of the polynomial.

$$\alpha^4 + \alpha + 1 = 0.$$

(GF(2)) $\Rightarrow \alpha^4 \geq \alpha + 1$

	α^3	α^2	α	1
α^0				1
α^1			α	
α^2		α^2		
α^3	α^3			
α^4			$\alpha+1$	
α^5		$\alpha^2+\alpha$		
α^6	$\alpha^3+\alpha^2$			
α^7	$\alpha^3+\alpha+1$			
α^8		α^2+1		
α^9	$\alpha^3+\alpha$			
α^{10}		$\alpha^2+\alpha+1$		
α^{11}	$\alpha^3+\alpha^2+\alpha$			
α^{12}	$\alpha^3+\alpha^2+\alpha+1$			
α^{13}	$\alpha^3+\alpha^2+1$			
α^{14}	α^3+1			

$\therefore \alpha^{15} = \alpha^0 = 1.$

Solutions will be $1, \alpha, \alpha^2$ or 3.

degree = 4.

$\alpha^4 = \alpha + 1.$

$\alpha^5 = \alpha \cdot \alpha^4 = \alpha^2 + \alpha.$

$\alpha^6 = \alpha^4 \cdot \alpha^2$

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

$= \alpha^3 + \alpha^2.$

$\alpha^7 = \alpha \cdot \alpha^6$

$= \alpha(\alpha^3 + \alpha^2)$

$= \alpha^4 + \alpha^3$

$= \alpha + 1 + \alpha^3$.

Conjugate classes

① $\alpha \quad (\alpha)^2 = \alpha^2 \quad (\alpha)^{2^2} = (\alpha)^4 \cdot (\alpha)^{2^3} = \alpha^8$

$(\alpha)^{2^4} = \alpha^{16} = \alpha^1$.

$\Rightarrow \alpha, \alpha^2, \alpha^4, \alpha^8$ //.

② $\alpha^3, \quad (\alpha^3)^2 = \alpha^6, \quad (\alpha^3)^{2^2} \cdot \alpha^{12}, (\alpha^3)^{2^3} = \alpha^{24}$

$= \alpha^9$

$(\alpha^3)^{2^4} = \alpha^{48} = \alpha^3$

~~$3 = 48 \bmod$~~

$\Rightarrow \alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ //. $3 < 48$ mod 15.

③ $\alpha^5, \quad (\alpha^5)^{2^1} = \alpha^{10}, \quad (\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$

$\Rightarrow \alpha^5, \alpha^{10}$ //.

④ $\alpha^7, (\alpha^7)^{2^1} = \alpha^{14}, \quad (\alpha^7)^{2^2} = \alpha^{28} = \alpha^{13},$

$(\alpha^7)^2 = \alpha^{56} = \alpha^{11}$, $(\alpha^7)^{24} = \alpha^7$

$\Rightarrow \alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ ||.

(5) α^0

(1) $(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$
$= x^4+x+1$.

(2) $(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$
$= x^4+x^3+x^2+x+1$

(3) $(x-\alpha^5)(x-\alpha^{10}) = x^2+x+1$

(4) $(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$
$= x^4+x^3+1$

(5) $(x-\alpha^8) = x-1 \Rightarrow x+1$. over GF(2).

$\Rightarrow (x^{15}-1) = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$
$= (x^4+x^3+1)(x+1)$.

b) $x^9 - x$ over GF(3).

$x^9-x = x(x^8-1) = x(x^{3^2-1}-1)$.

over $GF(3^2)$.

x^2+x+2 → irreducible polynomial.

let α be the root.

$\Rightarrow \alpha^2+\alpha+2=0$.

$\alpha^2 = -\alpha - 2 = 2\alpha + 1$ over GF(3).

	α
α^0	1
α^1	α
α^2	$2\alpha+1$
α^3	$2\alpha+2$
α^4	2
α^5	2α
α^6	$\alpha+2$
α^7	$\alpha+1$

$\alpha^2 = 2\alpha + 1$

$\alpha^3 = \alpha \cdot \alpha^2$

$= 2\alpha^2 + \alpha$

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

$= 4\alpha + 2 + \alpha$

$= 2\alpha + 2.$

$\therefore \alpha^8 = \alpha^0$

~~Conjugate classes~~

Conjugate classes

(1) $\alpha, (\alpha)^3 = \alpha^3, (\alpha)^{3^2} = \alpha^9 = \alpha$

$\Rightarrow \alpha, \alpha^3$

(2) α^2, α^6

(3) α^4

(4) α^5, α^7

(5) α^0

(1) $(x-\alpha)(x-\alpha^3) = x^2+x+2$

(2) $(x-\alpha^2)(x-\alpha^6) = x^2+1$

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

④ $(x-\alpha^5)(x-\alpha^7) = x^2+2x+2$

⑤ $x-\alpha^0 = x-1 = x+2$

$$x^9-x = x(x^8-1) = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

⑤

$$x^{2^{10}}-x = x(x^{2^{10}-1}-1)$$

$2^{10}-1 = 1023.$

$1023 = 3\times11\times31$

order = divisions

$\phi(p^n) = p^n - p^{n-1}$ where, p is a prime number.

order	no. of elements = ϕ(order)
1	$\phi(1) = 1^1-1^0 = 1$
3	$\phi(3) = 3^1-3^0 = 2$
11	$\phi(11) = 11^1-11^0 = 10$
31	$\phi(31) = 31^1-31^0 = 30$
33	$\phi(33) = \phi(3).\phi(11) = 20$
93	$\phi(93) = \phi(3).\phi(31) = 60$
341	$\phi(341) = \phi(11).\phi(31) = 300$
1023	$\phi(1023) = \phi(3).\phi(341) = 600$

degree	no. of polynomials
1	1/1=1
2	2/2=2
10	10/10=1
5	30/5=6
10	20/10=2
10	~~300/10~~ = 60/10 = 6
10	300/10 = 30
10	600/10 = 60.

To calculate the degree of mini. polynomial
x. order $/2^n - 1$.

finding min. x shows that order divides

eg: $3/2^2 - 1 = 3/3$. $2^n - 1$.

Akhil Sai Chintala
934409906.