CS527

HW6; Fenghuan Li; 93363807.

1. a. degree 5 over GF(2).
   b. degree 3 over GF(3).

a. Let $f(x) \in GF$ for all polynomials over GF(2).
So, list all the possible polynomials of degree 5 over GF(2).

$a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$.

Because degree 5 over GF(2), So we can know that $a_5 = 1$, if $a_0 = 0$, it is a factor,
So, we can get that: $x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + 1$;
for a_4, a_3, a_2, a_1 will have 16 possibilities.
as the table show:

index		$f(x)$	index		$f(x)$
1	100001	x^5+1	9	110001	x^5+x^4+1
2	100011	x^5+x+1	10	110011	x^5+x^4+x+1
3	100101	x^5+x^2+1	11	110101	$x^5+x^4+x^2+1$
4	100111	x^5+x^2+x+1	12	110111	$x^5+x^4+x^2+x+1$
5	101001	x^5+x^3+1	13	111001	$x^5+x^4+x^3+1$
6	101011	x^5+x^3+x+1	14	111011	$x^5+x^4+x^3+x+1$
7	101101	$x^5+x^3+x^2+1$	15	111101	$x^5+x^4+x^3+x^2+1$
8	101111	$x^5+x^3+x^2+x+1$	16	111111	$x^5+x^4+x^3+x^2+x+1$

Because at index = {1, 4, 6, 7, 10, 11, 13, 16}, the $f(a) = 0$ when $a \in GF(2)$. That meaning these polynomials has root in F. So, these polynomials can't be irreducible.

Therefor, because index = {2, 9} we get the

$x^5 + x + 1 = (x^2 + x + 1) \cdot (x^3 + x^2 + 1)$ ... ①

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

As ① ② show, these two polynomials can be factored, so they are reducible.

Then, we can know that polynomials are irreducible

So, we can know that monic irreducible polynomials of degree 5 over GF(2) are:

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

.... a answer.

b. same like a part, let $f(x) \in F$ for all polynomials over GF(3). Then, list the all possible polynomials about degree 3 over GF(3):

We can know that $a_3 x^3 + a_2 x^2 + a_1 x + a_0$.

Because degree 3 over GF(3).

So we can get that $a_3 = 1$, $a_0 = 1$ or 2

So $x^3 + a_2 x^2 + a_1 x + a_0$ will have 18 possibles as this table show.

index		f(x)	index		f(x)
1	1001	x^3+1	10	1112	x^3+x^2+x+2
2	1002	x^3+2	11	1121	x^3+x^2+2x+1
3	1011	x^3+x+1	12	1122	x^3+x^2+2x+2
4	1012	x^3+x+2	13	1201	x^3+2x^2+1
5	1021	x^3+2x+1	14	1202	x^3+2x^2+2
6	1022	x^3+2x+2	15	1211	x^3+2x^2+x+1
7	1101	x^3+x^2+1	16	1212	x^3+2x^2+x+2
8	1102	x^3+x^2+2	17	1221	x^3+2x^2+2x+1
9	1111	x^3+x^2+x+1	18	1222	x^3+2x^2+2x+2

Same like a, we can find that some equal to 0, which meaning these polynomials have root.

For index = 5, 6, 8, 10, 11, 13, 15, 17 have no root. and these can't be factored over GF(3).

So, x^3+2x+1; x^3+2x+2; x^3+2x^2+1; x^3+x^2+2; x^3+x^2+x+2; x^3+x^2+2x+1; x^3+2x^2+x+1; x^3+2x^2+2x+1;

these are the irreducible polynomials of degree 3 over GF(3).

2. a. 23 mod 101.

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

a. Because we need to find the multiplicative inverse of 23 mod 101.

So, we need to define: $r_{-1} = 101$; $r_0 = 23$;
$r_{i-2} = q_i r_{i-1} + r_i$; $t_i = t_{i-2} - q_i t_{i-1}$;
$r_i = 101 s_i + 23 t_i$;

Using extended GCD algorithm:

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	22

So, as the table show, we can get that:

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

$\Rightarrow 1 \bmod 101 = 23 \times 22 \bmod 101$.

Therefor, the multiplicative inverse of 23 mod 101 is 22.

---

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

Because find the multiplicative inverse and use extended GCD algorithm.

let $r_{i-1}(x) = q_i(x) r_i(x) + r_{i+1}(x)$.

As the table show:

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	x	x	$-x^5-x^3-x^2-x-1$	$x^7+x^4+x^2+x$
5	1	1	$x^5+x^4+x^3+x^2$	$-x^7-x^6-x^3-x-1$

So, we can get that:

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

$\Rightarrow 1 = (x^7+x^6+x^3+x+1)\cdot(x^6+x^4+x^2+x+1) \bmod x^8$ GF(2).

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

3.

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

prove by induction: Let $i=0$, $t_0 r_{-1} - t_{-1} r_0 = a$

$\Rightarrow$ when $t_{-1}=0$ & $t_0=1$ get $r_{-1} = r_{i-1} = a$.

Since $t_i = t_{i-2} - q_i t_{i-1}$, when $t_{-1}=0$ & $t_0=1$ get $t_2 = t_0 + q_0 t_{-1} = 1$

Then, let $i=-1$, $t_{-1} r_{-2} - t_{-2} r_{-1} = -a$

($t_{-1}=0$, $t_0=1$, $r_{-1}=a$, $t_{-2}=1$) so we can get that:

$t_{-1} r_{-2} - t_{-2} r_{-1} = -a \Rightarrow -a = -a$.

Inductive steps:

Assume it is true for $i=k$;

Then, $i=k+1$;

$$t_{k+1}r_k - t_k r_{k+1} = (t_{k-1} - q_{k+1}t_k)r_k - t_k(r_{k-1} - q_{k+1}r_k)$$

$$= t_{k-1}r_k - t_k r_{k-1}$$

$$= (-1)^{k+1}a.$$

Then, we can know this assume is true for $i=k+1$;

so we prove that $t_i r_{i-1} - t_{i-1}r_i = (-1)^i a$ is true.

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

prove by induction:

when $i=0$, $s_0 r_{-1} - s_{-1}r_0 = b$.

Since $s_0=0$ & $s_{-1}=1$ we can get $\underline{r_0 = b}$

when $i=1$, $s_1 r_0 - s_0 r_1 = b$.

$$s_1 r_0 - s_0 r_1 = (s_{-1} - q_1 s_0)r_0 - s_0 r_1 = r_0 = (-1)^{(+1)} b.$$

Inductive steps:

Asume that the property is true for $i=k$.

Then we need to know $i=k+1$;

$$s_{k+1}r_k - s_k r_{k+1} = (s_{k-1} - q_{k+1}s_k)r_k - s_k(r_{k-1} - q_{k+1}r_k)$$

$$= -(s_k r_{k-1} - s_{k-1} r_k)$$
$$= (-1)^{((k+1)+1)} b.$$

For that steps, we can prove it also true for $i=k+1$, So, this property is true.

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

prove by induction:

$i=0$, $s_0 t_{-1} - s_{-1} t_0 = (-1)^{0+1}$

Since $s_0=0$ & $s_{-1}=1$, get $t_0=-1 \Rightarrow -1=-1$.

Inductive steps:

Assume it is true for $i=k$;

$$s_k t_{k-1} - s_{k-1} t_k = (-1)^{k+1} \quad \cdots ①$$

$i=k+1$;

$$s_{k+1} t_k - s_k t_{k+1} = (-1)^{k+2} \quad \cdots ②.$$

$$s_{k+1} = s_{k-1} - q_{k+1} s_k \quad \cdots ③.$$

$$t_{k+1} = t_{k-1} - q_{k+1} t_k \quad \cdots ④.$$

Put ③ ④ in ② we can get:

$$(s_{k-1} - q_{k+1} s_k) t_k - s_k (t_{k-1} - q_{k+1} t_k)$$

$$= -(s_k t_{k-1} - s_{k-1} t_k) = -1 \cdot (-1)^{k+1} = (-1)^{(k+1)+1}$$

So, this property is true for $i=k+1$, our prove is true.

d. $s_i a + t_i b = r_i$

prove by induction:

when $i=-1$, $s_{-1}a + t_{-1}b = r_{-1} \xrightarrow[s_{-1}=1]{t_{-1}=0} r_{-1}=a$.

when $i=0$, $s_0 a + t_0 b = r_0 \xrightarrow[s_0=0]{t_0=1} r_0 = b$.

when $i=1$, $s_1 a + t_1 b = r_1$.

when $i=2$ $s_2 a + t_2 b = (s_0 - q_2 s_1)a + (t_0 - q_2 t_1)b$

$= (0 - q_2 - 1)a + (1 - q_2(-q_1))b$

$= b - q_2(a - q_1 b) = b - q_2(r_1) = r_2$.

Inductive steps:

Assume the property is true for $i=k$;

we get $s_k a + t_k b = r_k$;

For $i=k+1$;

$s_{k+1} a + t_{k+1} b = (s_{k-1} - q_{k+1} s_k) a + (t_{k-1} - q_{k+1} t_k) b$

$= s_{k-1} a - q_{k+1} s_k a + t_{k-1} b - q_{k+1} t_k b$

$= s_{k-1} a + t_{k-1} b - q_{k+1}(s_k a + t_k b)$

$= r_{k-1} - q_{k+1}(r_k)$

$= r_{k+1}$.

So, it is true for $i=k+1$, we prove the property is true.

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

prove by induction:

when $i=1$, $\deg(s_1) + \deg(r_0) = \deg(b)$

since $s_1 = 1$. $\deg(1) + \deg(r_0) = \deg(b)$.

when $i=2$. $\deg(s_2) + \deg(r_1) = \deg(s_0 - q_2 s_1) + \deg(r_1)$

$= \deg(q_2 r_1) + \deg(1)$

since $\deg(r_i) = \deg(q_{i+2} r_{i+1})$

$\deg(q_2 r_1) = \deg(r_0) = \deg(b)$.

Assume the property is true for $i=k$,

$\deg(s_k) + \deg(r_{k-1}) = \deg(b)$.

For $i=k+1$;

$\deg(s_{k+1}) + \deg(r_{k+1}) = \deg(s_{k-1} - q_{k+1} s_k) + \deg(r_k)$

$= \deg(q_{k+1} s_k) + \deg(r_k)$

$= \deg(q_{k+1} r_k) + \deg(s_k) = \deg(r_{k-1}) + \deg(s_k)$

$= \deg(b)$.

So, it is also true for $i=k+1$; prove the property is true.

3. $\deg(t_i) + \deg(r_{i-1}) = \deg(a)$ for $0 \le i \le n+1$.

when $i=0$, $\deg(t_0) + \deg(r_{-1}) = \deg(a) = \deg(1) + \deg(r_{-1}) = \deg(a)$.

when $i=1$, $\deg(t_1) + \deg(r_0) = \deg(t_{-1} - q_1 t_0) + \deg(r_0)$

$= \deg(q_1 r_0) = \deg(r_{-1}) = \deg(a)$

Assume this is true for $i=k$; $\deg(t_k) + \deg(r_{k-1}) = \deg(a)$.

$i=k+1$; $\deg(t_{k+1}) + \deg(r_k) = \deg(t_{k-1} - q_{k+1} t_k) + \deg(r_k)$

$= \deg(q_{k+1} t_k) + \deg(r_k) = \deg(q_{k+1} r_k) + \deg(t_k)$

$= \deg(r_{k-1}) + \deg(t_k) = \deg(a)$.

So, is true for $i=k+1$; prove that this property is true.

4. a. $X^5 - 1$ over $GF(2)$.

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

a. Assume $\alpha \in GF(2)$. be a root of primitive polynomial

$p(x) = x^4 + x + 1$

other step at next page.

we can get that:

α^0	1	0001
α^1	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001
α^{15}	1	α^0

For conjugate classes:

$g_1(x) = (x-\alpha)(x-\alpha^2)\cdot(x-\alpha^4)\cdot(x-\alpha^8)$

$= (x^2+\alpha^5 x+\alpha^3)(x-\alpha^4)\cdot(x-\alpha^8)$

$= \underline{x^4+x+1}$

$g_2(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$

$= (x^3+\alpha^7x^2+\alpha^4x+\alpha^6)(x-\alpha^9) = \underline{x^4+x^3+x^2+x+1}$

$g_3(x) = (x-\alpha^5)(x-\alpha^{10})$

$= \underline{x^2+x+1}$

$$g_4(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{56})$$

$$= (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$$

$$= \underline{x^4+x^3+1}.$$

$$g_5(x) = x-\alpha^{15} = \underline{x+1}.$$

$$x^{15}-1 = g_1(x)\,g_2(x)\,g_3(x)\,g_4(x)\,g_5(x)$$

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

b. Same as a part. Let $\alpha \in GF(3)$ be a root of the primitive polynomial $p(x) = x^2+x+2$; we can get:

α^0	1	01
α^1	α	10
α^2	$-\alpha-2 = 2\alpha+1$	21
α^3	$\alpha\cdot\alpha^2 = 2\alpha+2$	22
α^4	2	02
α^5	2α	20
α^6	$\alpha+2$	12
α^7	$\alpha+1$	11
α^8	1	α^0

By the conjugate classes:

$g_1(x) = (x-\alpha)(x-\alpha^3) = x^2 - \alpha^4 x + \alpha^4 = x^2+x+2$.

$g_2(x) = (x-\alpha^2)(x-\alpha^6) = x^2+1$.

$g_3(x) = x-\alpha^4 = x+1$.

$g_4(x) = (x-\alpha^5)(x-\alpha^7) = x^2+2x+2$

$g_5(x) = x-\alpha^0 = x+2$.

So, $x^8+1 = g_1(x)\,g_2(x)\,g_3(x)\,g_4(x)\,g_5(x)$

$x^9-x = x\cdot(x^8+1) = x\,(g_1(x)\,g_2(x)\,g_3(x)\,g_4(x)\,g_5(x))$

$= x(x^2+x+2)(x^2+1)(x+1)(x^2+2x+2)(x+2)$

5. Because we need to find the degrees of the irreducible polynomials by $x^{2^{10}}-x$ over GF(2).

So, $x^{2^{10}}-x = x(x^{1023}-1)$.

Let α be a primitive root in $GF(2^{10})$

we can know the divisor of $1023 = \{1, 3, 11, 31, 33, 93, 341, 1023\}$.

We can know that the degree of minimum polynomial:

$\min(k)$ where $t \mid 2^k - 1$.

for the number of these polynomials:

$n = \frac{\phi(t)}{k}$; so we can get this table:

order.	number of elements $\varphi(t)$.	degree of minimum polym.	number of these polym
1	1	1	1
3	2	2	1
11	10	10	1
31	30	5	6
33	20.	10	2
93	60	10	6
341	300	10	30
1023	600	10	60.

So. the 1 polynomial of degree 1.
the 1 polynomial of degree 2.
the 6 polynomial of degree 5
the 99 polynomial of degree 10.