Prajjwal Dangal
CS 5920 - HW 3

1.a. Since we have GF(5), it will be a mod 5 operation.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table I : Addition modulo 5

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table II : Multiplication modulo 5

w	0	1	2	3	4
-w	0	4	3	2	1
w^{-1}	-	1	3	2	4

Table III : Additive and multiplicative inverses modulo 5

b.

i. By inspection, we know that x^3+1 does not have x as one of its factors.

Checking with $x+1$,

$$
\begin{array}{r}
x^2-x+1 \\
x+1 \;\overline{)\; x^3+1} \\
-x^3+x^2 \\
\hline
1-x^2 \\
-x-x^2 \\
\hline
1+x \\
1+x \\
\hline
0
\end{array}
$$

$x^3+1 = (x^2+x+1)(x+1)$ in GF(2)

$\therefore$ It is reducible.

(ii) By inspection, x is not a factor of x^3+x^2+1.
Checking with $x+1$,

$$\begin{array}{r} x^2 \\ x+1 \overline{)\ x^3+x^2+1} \\ \underline{x^3+x^2} \\ 1 \end{array}$$

Since we expect the factors to be in the form,
$x^3+x^2+1 = (x+\dots)(x^2+\dots)$,
x^3+x^2+1 is irreducible.

(iii) By inspection, x is not a factor.
Checking with $x+1$

$$\begin{array}{r} x^3+x^2+x+1 \\ x+1 \overline{)\ x^4+1} \\ \underline{x^4+x^3} \\ 1+x^3 \\ \underline{x^2+x^3} \\ 1+x^2 \\ \underline{x+x^2} \\ 1+x \\ \underline{1+x} \\ 0 \end{array}$$

Since, $x^4+1 = (x+1)(x^3+x^2+x+1)$
$\therefore$ x^4+1 is reducible.

2. a. Soln
We know,
$GF(4) = GF(2^2)$

+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x+1	x^2+x	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x	x^2+1	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2+1	x^2	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2	x^2+1	$x+1$	x	1	0

Table I: Polynomial Arithmetic Modulo (x^2+x+1) – Addition

x	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2+1	x^2+1	x^2+x	x^2+x+1	x^2	0
$x+1$	0	$x+1$	x^2+x+1	x^2+x				
x^2	0							
x^2+1	0							
x^2+x	0							
x^2+x+1	0							

Table II: Polynomial Arithmetic Modulo (x^2+x+1) – Multiplication

2b. Sol^{n}

Let the generator be g.

$m(g) = 0 \Rightarrow g^4 + g + 1 = 0 \Rightarrow g^4 = g + 1 \pmod 2$

Power	Polynomial	Binary	Hex
0	0	0000	0
g^0	1	0001	1
g_1	g	0010	2
g_2	g^2	0100	4
g_3	g^3	1000	8
g_4	$g+1$	0011	3
g_5	g^2+g	0110	6
g_6	g^3+g^2	1100	12
g_7	g^3+g+1	1011	11
g_8	g^2+1	0101	5
g_9	g^3+g	1010	10
g_{10}	g^2+g+1	0111	7
g_{11}	g^3+g^2+g	1110	14
g_{12}	g^3+g^2+g+1	1111	15
g_{13}	g^3+g^2+1	1101	13
g_{14}	g^3+1	1001	9

3a. solution (Sol^{n})

Since it's $GF(2^4)$, the block length is 16 bits.

The state array will be:

$$\begin{bmatrix} \text{nibble 1} & \text{nibble 3} \\ \text{nibble 2} & \text{nibble 4} \end{bmatrix}$$

3.

b. One prime polynomial in $GF(x^4)$ is $m(x) = x^4 + x + 1$.
or 10011

c. Here,

$$\begin{bmatrix} x^3+1 & x \\ x & x^3+1 \end{bmatrix} \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x^3+1+x^3 & x^5+1+x^3+x \end{bmatrix}$$

$$= \begin{bmatrix} x^3+1+x^3 & x^5+x^2+x \\ x^5+x^2+x & x^3+x^3+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Please note, $(x^5+x^2+x) \bmod (x^4+x+1) = 0$