Homework for section#5A (approximate due date Sept 14th, 2020)

1-Arithmetic in extended Galois field with $\boldsymbol{GF}_{2^8}$; $\boldsymbol{P}_{(x)} = x^8 + x^4 + x^3 + x + 1$

Compute the following elements:

1/21; 1/9f; 1/ab; 1/cd

1/21 = 6e

1/9f = 9a

1/ab = 4a

1/cd = fc

2-Arithmetic in extended Galois Field with $\boldsymbol{GF}_{2^3}$; $\boldsymbol{P}_{(x)} = x^3 + x + 1$

Represented by polynomials: $\boldsymbol{A}_{(x)} = \boldsymbol{a}_2\, x^2 + \boldsymbol{a}_1\, x + \boldsymbol{a}_0$

Elements: *(0, 1, x, x +1, x^2, x^2+1, x^2+ x, x^2+ x +1)*

Find the 8 inverses:

Multiplication Table

	000 (0)	001 (1)	010 (x)	011 (x+1)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	0	0	0	0	0	0	0	0
001 (1)	0	**1**	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010 (x)	0	x	x^2	x^2+x	$x+1$	**1**	x^2+x+1	x^2+x
011 (x+1)	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	**1**	x
100 (x^2)	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+x	**1**
101 (x^2+1)	0	x^2+1	**1**	x^2	x	x^2+x+1	$x+1$	x^2+x
110 (x^2+x)	0	x^2+x	x^2+x+1	**1**	x^2+1	$x+1$	x	x^2
111 (x^2+x+1)	0	x^2+x+1	x^2+1	x	**1**	x^2+x	x^2	$x+1$

Inverse Table

$A_{(x)}$	$A^{-1}{}_{(x)}$
1	1
x	x^2+1
x+1	x^2+x
x^2	x^2+x+1
x^2+1	x
x^2+x	x+1
x^2+x+1	x^2

Compute the following:

$x^2+1 \odiv x^2+x$ =?

= (x^2+1) * (x + 1) [Inverse of x^2+x is x +1]

= $x^3 + x^2 + x + 1$

Now, $x^3 + x^2 + x + 1$ mod (x^3+x+1)

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

Remainder = x^2

$x^3 + x^2 + x + 1 \equiv x^2$ mod (x^3+x+1)

$x^2+1 \odiv x^2+x$ = 101 $\odiv 110 = 100$

$x^2+x \odiv x^2+1$ =?

$(x^2+x) * (x)$ [Inverse of x^2+1 is x]

= $x^3 + x^2$

Now, $x^3 + x^2$ mod (x^3+x+1)

$x^3 + x^2$= (x^3+x+1) * 1 + (x^2 - x - 1)

Remainder (x^2 - x - 1)

$x^3 + x^2 \equiv$ (x^2 - x - 1) mod (x^3+x+1)

$\equiv$ (x^2 + x + 1) mod (x^3+x+1)

$x^2 + x \odiv x^2 + 1$ = 110 $\odiv 101 = 001$