

$GF(2)$

Values =  $\{0, 1\}$

Operations =  $+, \times$

+	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Inverse : For  $+$ , the element itself  
For  $\times$ , no inverse for 0  
Inverse of 1 is 1

$GF(5)$

Values =  $\{0, 1, 2, 3, 4\}$

Operations =  $+, \times$

+	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

$\times$	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

### Additive Inverse

a	0	1	2	3	4
-a	0	4	3	2	1

### Multiplicative Inverse

a	0	1	2	3	4
a <sup>-1</sup>	-	1	3	2	4

GF(2<sup>n</sup>) Fields :

GF(2<sup>2</sup>)

Values = {00, 01, 10, 11}

### Addition

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity : 00

### Multiplication

X	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity : 01

Multiply  $P_1$   $(x^5+x^2+x)$  and  $P_2$   $(x^7+x^4+x^3+x^2+x)$   
in  $GF(2^8)$  with the irreducible polynomial  
 $(x^8+x^4+x^3+x+1)$

$$\begin{aligned}
 P_1 \times P_2 &= x^5(x^7+x^4+x^3+x^2+x) + \\
 &\quad x^2(x^7+x^4+x^3+x^2+x) + \\
 &\quad x(x^7+x^4+x^3+x^2+x) \\
 &= x^{12} + \cancel{x^9} + \cancel{x^8} + x^7 + \cancel{x^6} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + x^2 \\
 &= \underline{x^{12} + x^7 + x^2}
 \end{aligned}$$

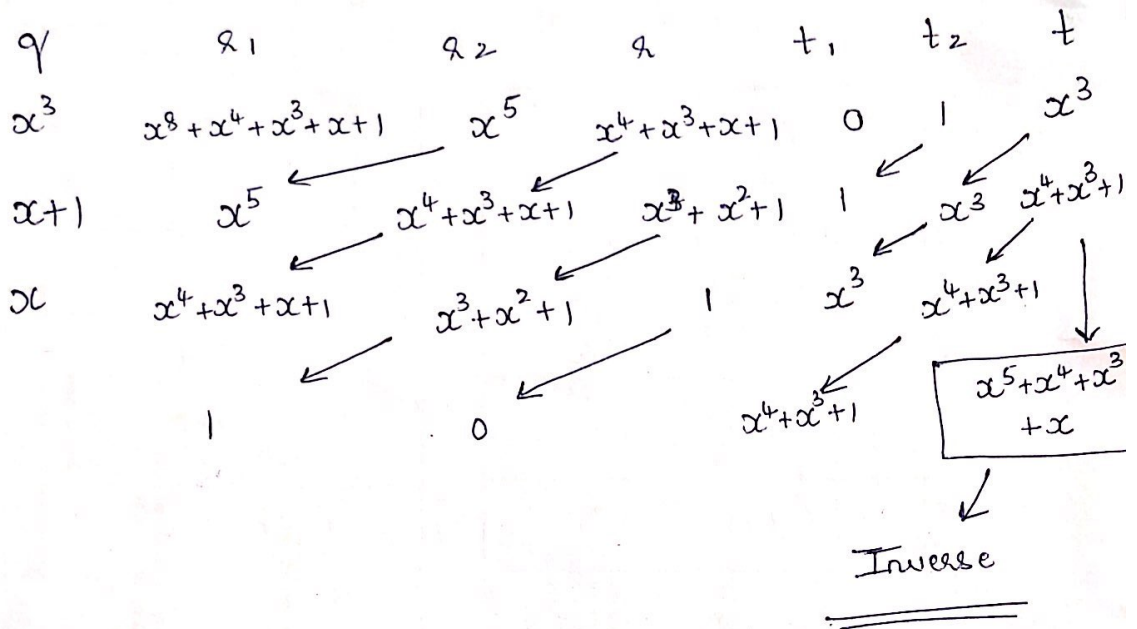
$$(x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\begin{array}{r}
 x^8 + x^4 + x^3 + x + 1 \overline{) x^{12} + x^7 + x^2} \\
 \underline{x^{12} + x^8 + x^7 + x^5 + x^4} \phantom{+ x^2} \\
 x^6 + x^5 + x^4 + x^2 \\
 \underline{x^8 + x^4 + x^3 + x + 1} \\
 x^5 + x^3 + x^2 + x + 1
 \end{array}$$

↳ Remainder

Inverse of  $x^5$  modulo  $x^8+x^4+x^3+x+1$  in  $GF(2^8)$

Using Extended Euclidean algorithm



Inverse of  $(x^5)^{-1}$  is  $x^5+x^4+x^3+x$

Verification:

$$x^5 \times (x^5+x^4+x^3+x)$$

$$= (x^{10}+x^9+x^8+x^6) \bmod x^8+x^4+x^3+x+1$$

$$\begin{array}{r}
 x^8+x^4+x^3+x+1 \overline{) x^{10}+x^9+x^8+x^6} \\
 \underline{x^{10}+x^6+x^5+x^3+x^2} \phantom{+x} \\
 x^9+x^8+x^5+x^3+x^2 \\
 \underline{x^9+x^5+x^4+x^2+x} \\
 x^8+x^4+x^3+x^2+x \\
 \underline{x^8+x^4+x^3+x+1} \\
 1
 \end{array}$$

Remainder

Step 1 :

$$\begin{array}{r}
 x^3 \xrightarrow{\text{Quotient}} \\
 x^5 \overline{) x^8 + x^4 + x^3 + x + 1} \\
 \underline{x^8} \phantom{+ x^4 + x^3 + x + 1} \\
 x^4 + x^3 + x + 1 \xrightarrow{\text{Remainder}}
 \end{array}$$

Step 2 :

$$\begin{array}{r}
 x+1 \xrightarrow{\text{Quotient}} \\
 x^4 + x^3 + x + 1 \overline{) x^5} \\
 \underline{x^5 + x^4 + x^2 + x} \phantom{+ 1} \\
 x^4 + x^3 + x + 1 \xrightarrow{\text{Remainder}}
 \end{array}$$

To calculate 't' :

$$\begin{aligned}
 t_1 &= q \times t_2 \\
 &= 1 - (x+1) \times x^3 \\
 &= 1 - x^4 - x^3 \\
 &= \underline{x^4 + x^3 + 1}
 \end{aligned}$$

Step 3 :

$$\begin{array}{r}
 x \xrightarrow{\text{Quotient}} \\
 x^3 + x^2 + 1 \overline{) x^4 + x^3 + x + 1} \\
 \underline{x^4 + x^3 + x} \phantom{+ 1} \\
 1 \xrightarrow{\text{Remainder}}
 \end{array}$$

To calculate 't' :

$$\begin{aligned}
 t_1 &= q \times t_2 \\
 &= x^3 - x(x^4 + x^3 + 1) \\
 &= x^3 - x^5 - x^4 - x \\
 &= \underline{x^5 + x^4 + x^3 + x}
 \end{aligned}$$



Multiplication using a computer:

Find  $(\alpha \times (\alpha \times P_2))$  instead of  $(\alpha^2 \times P_2)$

Multiply  $P_1$  and  $P_2$  in  $GF(2^8)$  with the irreducible polynomial  $(x^8 + x^4 + x^3 + x + 1)$

$$P_1 = x^5 + x^2 + x$$

$$P_2 = x^7 + x^4 + x^3 + x^2 + x$$

Powers	Operation	New Result	Reduction
$\alpha^0 \times P_2$		$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	No
$\alpha^1 \times P_2$	$\alpha \times (\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha)$	$\alpha^5 + \alpha^2 + \alpha + 1$	Yes
$\alpha^2 \times P_2$	$\alpha \times (\alpha^5 + \alpha^2 + \alpha + 1)$	$\alpha^6 + \alpha^3 + \alpha^2 + \alpha$	No
$\alpha^3 \times P_2$	$\alpha \times (\alpha^6 + \alpha^3 + \alpha^2 + \alpha)$	$\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2$	No
$\alpha^4 \times P_2$	$\alpha \times (\alpha^7 + \alpha^4 + \alpha^3 + \alpha^2)$	$\alpha^5 + \alpha + 1$	Yes
$\alpha^5 \times P_2$	$\alpha \times (\alpha^5 + \alpha + 1)$	$\alpha^6 + \alpha^2 + \alpha$	No

$$\begin{aligned}
 P_1 \times P_2 &= (\cancel{\alpha^7} + \cancel{\alpha^4} + \cancel{\alpha^3}) + (\cancel{\alpha^6} + \alpha^3 + \cancel{\alpha^2} + \cancel{\alpha}) + (\alpha^5 + \alpha^2 + \alpha + 1) \\
 &= \underline{\alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1}
 \end{aligned}$$

$$\underline{x^1 \times P_2}$$

$$x \times (x^7 + x^4 + x^3 + x^2 + x)$$

$$= x^8 + x^5 + x^4 + x^3 + x^2$$

$$x^8 + x^4 + x^3 + x + 1 \quad \begin{array}{r} 1 \\ \hline \cancel{x^8} + x^5 + \cancel{x^4} + \cancel{x^3} + x^2 \\ \hline x^5 + x^2 + x + 1 \end{array}$$

→ new result

$$\underline{x^4 \times P_2}$$

$$x \times (x^7 + x^4 + x^3 + x^2)$$

$$= x^8 + x^5 + x^4 + x^3$$

$$x^8 + x^4 + x^3 + x + 1 \quad \begin{array}{r} 1 \\ \hline \cancel{x^8} + x^5 + \cancel{x^4} + \cancel{x^3} \\ \hline x^5 + x + 1 \end{array}$$

→ new result

$$P_1 = x^5 + x^2 + x = 000100110 \text{ (8 bits)}$$

$$P_2 = x^7 + x^4 + x^3 + x^2 + x = 10011110 \text{ (8 bits)}$$

$$\text{modulus} = x^8 + x^4 + x^3 + x + 1$$

$$= 100011010 \text{ (9 bits)}$$

Algorithm:

1. If MSB of previous result = 0, shift previous result one bit to the left.

2. If MSB of previous result = 1,

(a) Shift one bit to the left

(b) XOR with modulus without MSB

Powers	Shift - Left	XOR
$x^0 \times P_2$		$10011110 = P_2$
$x^1 \times P_2$	00111100	$00111100 \oplus 00011011$ $= 00100111$
$x^2 \times P_2$	01001110	01001110
$x^3 \times P_2$	10011100	10011100
$x^4 \times P_2$	00111000	$00111000 \oplus 00011010$ $= 00100011$
$x^5 \times P_2$	01000110	01000110

$$P_1 \times P_2 = (00100111) + (01001110) + (01000110) = \underline{\underline{00101111}}$$