GF(2)

Values = {0, 1}

Operations = +, X

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| X | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

Inverse : For +, the element itself

For X, no inverse for 0

Inverse of 1 is 1

GF(5)

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

Operations = +, X

| + | 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 |

| 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 |

Additive Inverse

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

Multiplicative Inverse

| a | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a^{-1}$ | - | 1 | 3 | 2 | 4 |

## GF($2^n$) Fields :

GF($2^2$)

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

$$P_1 \times P_2 = x^5(x^7+x^4+x^3+x^2+x) + x^2(x^7+x^4+x^3+x^2+x) + x(x^7+x^4+x^3+x^2+x)$$

$$= x^{12}+x^9+x^8+x^7+x^6+x^9+x^6+x^5+x^4+x^3+x^8+x^5+x^4+x^3+x^2$$

$$= \underline{x^{12}+x^7+x^2}$$

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

$$\begin{array}{r|l} & x^4+1 \\ \hline x^8+x^4+x^3+x+1 & x^{12}+x^7+x^2 \\ & x^{12}+x^8+x^7+x^5+x^4 \\ \hline & x^8+x^5+x^4+x^2 \\ & x^8+x^4+x^3+x+1 \\ \hline & x^5+x^3+x^2+x+1 \end{array}$$

↳ Remainder

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

Using Extended Euclidean algorithm

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| $x^3$ | $x^8+x^4+x^3+x+1$ | $x^5$ | $x^4+x^3+x+1$ | 0 | 1 | $x^3$ |
| $x+1$ | $x^5$ | $x^4+x^3+x+1$ | $x^3+x^2+1$ | 1 | $x^3$ | $x^4+x^3+1$ |
| $x$ | $x^4+x^3+x+1$ | $x^3+x^2+1$ | 1 | $x^3$ | $x^4+x^3+1$ | $x^5+x^4+x^3+x$ |
| | 1 | 0 | | $x^4+x^3+1$ | | |

Inverse

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

Verification:

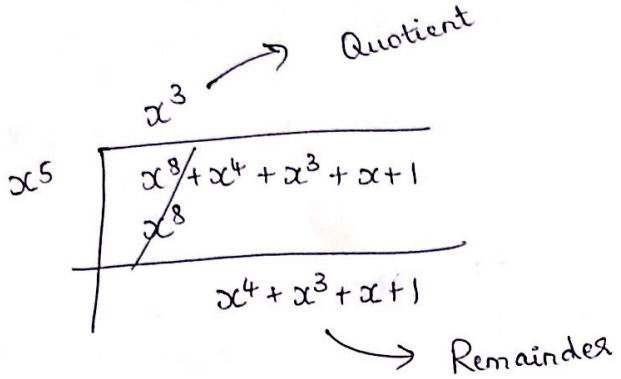
$$x^5 \times (x^5+x^4+x^3+x)$$

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

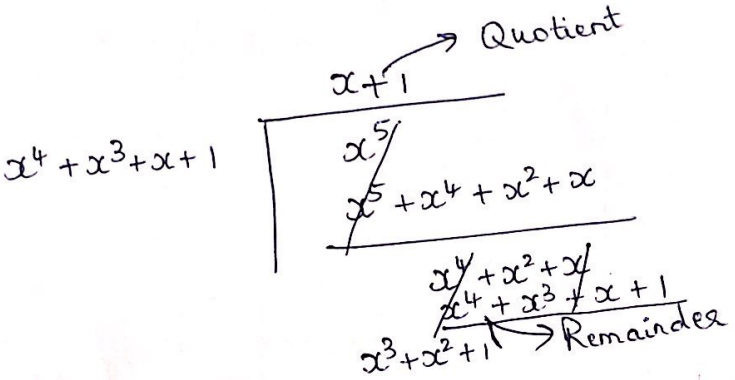
$$\begin{array}{r|l} & x^2+x+1 \\ \hline x^8+x^4+x^3+x+1 & x^{10}+x^9+x^8+x^6 \\ & x^{10}+x^6+x^5+x^3+x^2 \\ \hline & x^9+x^8+x^5+x^3+x^2 \\ & x^9+x^5+x^4+x^2+x \\ \hline & x^8+x^4+x^3+x \\ & x^8+x^4+x^3+x+1 \\ \hline & 1 \end{array}$$

Remainder

**Step 1 :**



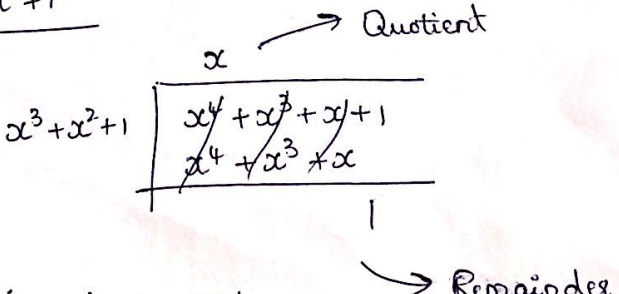

**Step 2 :**




To calculate 't' :

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

**Step 3**




To calculate 't' : $t_1 - q \times t_2$

$$= x^3 - x(x^4+x^3+1)$$
$$= x^3 - x^5 - x^4 - x$$
$$= \underline{x^5+x^4+x^3+x}$$

## Multiplication using a computer:

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

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 |
|---|---|---|---|
| $x^0 \times P_2$ | | $x^7 + x^4 + x^3 + x^2 + x$ | No |
| $x^1 \times P_2$ | $x \times (x^7 + x^4 + x^3 + x^2 + x)$ | $x^5 + x^2 + x + 1$ | Yes |
| $x^2 \times P_2$ | $x \times (x^5 + x^2 + x + 1)$ | $x^6 + x^3 + x^2 + x$ | No |
| $x^3 \times P_2$ | $x \times (x^6 + x^3 + x^2 + x)$ | $x^7 + x^4 + x^3 + x^2$ | No |
| $x^4 \times P_2$ | $x \times (x^7 + x^4 + x^3 + x^2)$ | $x^5 + x + 1$ | Yes |
| $x^5 \times P_2$ | $x \times (x^5 + x + 1)$ | $x^6 + x^2 + x$ | No |

$$P_1 \times P_2 = (x^4 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1)$$

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

$x^1 \times P_2$

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

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

$x^8 + x^4 + x^3 + x + 1$ | 1

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

$x^8 + x^4 + x^3 + x + 1$

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

↳ new result

$x^4 \times P_2$

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

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

$x^8 + x^4 + x^3 + x + 1$ | 1

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

$x^8 + x^4 + x^3 + x + 1$

$x^5 + x + 1$

↳ new result

$P_1 = x^5 + x^2 + x = 000100110$ (9 bits)

$P_2 = x^7 + x^4 + x^3 + x^2 + x = 10011110$ (8 bits)

modulus $= x^8 + x^4 + x^3 + x + 1$

$= 100011010$ (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 ⊕ 00011010 = 00100111 |
| $x^2 \times P_2$ | 01001110 | 01001110 |
| $x^3 \times P_2$ | 10011100 | 10011100 |
| $x^4 \times P_2$ | 00111000 | 00111000 ⊕ 00011010 = 00100011 |
| $x^5 \times P_2$ | 01000110 | 01000110 |

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