Modular Polynomial Arithmetic Over GF(2^n)

Dr. E.SURESH BABU

Assistant Professor

Computer Science and Engineering Department

National Institute of Technology, Warangal

Warangal

Outline

- ❖ Modular Polynomial Arithmetic Over $GF(2^n)$
- ❖ Arithmetic Polynomials Over $GF(2^n)$
  - ✓ Example : Arithmetic Polynomials Over $GF(2^8)$
- ❖ Finding Multiplicative Inverses in $GF(2^n)$
- ❖ Using A Generator : To Represent The Elements in $GF(2^n)$

Modular Polynomial Arithmetic Over GF(2^n)

Modular Polynomial Arithmetic Over GF(2^n)

- In **GF(2^n)**, when the **degree of the result** is more than **n-1**, it needs to be **reduced modulo a irreducible polynomial.**
  - ✓ This can be implemented as **BIT-SHIFT and XOR.**

Example : Modular Polynomial Arithmetic Over GF(2^3)

- We will first choose a particular **irreducible polynomial**, as

$$x^3 + x + 1$$

- (By the way there exist only **two irreducible polynomials of degree 3** over GF(2). The other is

$$x^3 + x^2 + 1.$$

For Example: $x^4+x^3+x+1 \equiv x^2+x \bmod (x^3+x+1)$.

- The bit-string representation of

  $x^4+x^3+x+1 \rightarrow 11011$

  $x^3+x+1 \rightarrow 1011.$

- The **degree of 11011**(x^4+x^3+x+1) **is 4** and the **degree of the irreducible polynomial is 3** (x^3+x+1).

For Example: $x^4+x^3+x+1 \equiv x^2+x \bmod (x^3+x+1)$.

- The **reduction starts by shifting** the irreducible polynomial **1011 one bit left**, you get **10110**, then

$$\begin{array}{r} 11011 \\ \oplus\, 10110 \\ \hline 1101. \end{array} \quad (x^3+x^2+1)$$

For Example: $x^4+x^3+x+1 \equiv x^2+x \mod (x^3+x+1)$.

- The **degree of 1101 is 3** which is still **greater than $n-1=2$,**
  - ✓ so you need **another XOR**. But you **don't need to shift** the irreducible polynomial this time.

$$
\begin{array}{r}
1101 \\
\oplus\ 1011 \\
\hline
0110
\end{array}
= x^2+x.
$$

Arithmetic Polynomials Over GF(2^n)

Recap...

❖ Keep in mind that we will **not use modular arithmetic**, as we have seen that **modular arithmetic (Z_8) not result in a field.**

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	[illegible]	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	[illegible]	7	4	1	[illegible]	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	[illegible]	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

Polynomials in GF(2^n)

- we will see how **polynomial arithmetic** provides a means for **constructing the desired Finite field.**

How to Find All the Polynomials in GF(2^n)

- To find all the polynomials in GF(2^n),
  - ✓ we need an **irreducible polynomial** of degree n.
- **For Example : AES** arithmetic is based on GF(2^8) which uses the following irreducible polynomial

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

Polynomials Over GF(2^n)

- ❖ There are **2^n polynomials** in the Finite field and the **degree of each polynomial** is **no more than n-1.**
- ❖ **GF(2^3) contains 8 element**

  { 0, 1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1 }.

  { 000, 001, 010, 011, 100, 101, 110, 111 }

  - ✓ **$x+1$ is actually $0x^2+1x+1$ ➔ 011.**
  - ✓ **$x^2+x = 1x^2+1x+0$ ➔ 110.**

Polynomials Over GF(2^3) : Example

- To construct the **finite field GF(2^3),** we need to choose an **irreducible polynomial of degree 3.**
- **Only Two Irreducible Polynomials**

$$\mathbf{x^3 + x + 1} \text{ and } \mathbf{x^3 + x^2 + 1}.$$

- We will consider first Irreducible Polynomials : $\mathbf{x^3 + x + 1}$

Addition Polynomial Operation in $GF(2^n)$

❖ Already We have seen that **addition of polynomials** over **GF(2)** is performed by **adding corresponding coefficients**

- ✓ **Addition** is just the **XOR operation.**

❖ **Addition of two polynomials** in **$GF(2^n)$** corresponds to a **bitwise XOR operation.**

Addition Operation in GF(2^n) : Bit Representation

	+	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	[illegible]	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

$$100 + 010 = 110$$

$$\begin{array}{r} 100 \\ \oplus\ 010 \\ \hline 110 \end{array}$$

equivalent to Polynomial

$$x^2+x$$

Addition Polynomial Operation in $GF(2^n)$

		000	001	010	011	100	101	110	111
	+	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$
000	0	0	1	x	$x + 1$	x^2	$x^2 + 1$	$x^2 + 1$	$x^2 + x + 1$
001	1	1	0	$x + 1$	x	$x^2 + 1$	x^2	$x^2 + x + 1$	$x^2 + x$
010	x	x	$x + 1$	0	1	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$
011	$x + 1$	$x + 1$	x	1	0	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2
100	x^2	x^2	$x^2 + 1$	$x^2 + x$	$x^2 + x + 1$	0	1	x	$x + 1$
101	$x^2 + 1$	$x^2 + 1$	x^2	$x^2 +$ [illegible] $+ 1$	$x^2 + x$	1	0	$x + 1$	x
110	$x^2 + x$	$x^2 + x$	$x^2 + x + 1$	x^2	$x^2 + 1$	x	$x + 1$	0	1
111	$x^2 + x + 1$	$x^2 + x + 1$	$x^2 + x$	$x^2 + 1$	x^2	$x + 1$	x	1	0

(a) Addition

$$\begin{array}{r} 100 \\ \oplus\ 010 \\ \hline 110 \end{array}$$

100 + 010 = 110

equivalent to Polynomial

x^2+x

Multiplication Polynomial Operation in GF(2^n)

- There is **no simple XOR operation w.r.t** multiplication in **GF(2^n)**.
- A **Reasonably Straightforward Technique** we will discuss.

Multiplication Polynomial Mechanism in $GF(2^n)$

- In general, In **$GF(2^n)$**, An **n^{th}-degree polynomial $p(x)$** we have

$$x^n \bmod p(x) = [p(x) - x^n]$$

- For Example : Consider a **irreducible polynomial** in **$GF(2^8)$ is**

$$\mathbf{m(x) = x^8 + x^4 + x^3 + x + 1}$$

$x^8 \bmod m(x) = [m(x) - x^8]$	$= x^4 + x^3 + x + 1$

$GF(2^8)$ is used in AES Encryption Algorithm

Multiplication Polynomial Mechanism in $GF(2^n)$

- Now, consider a polynomial in **$GF(2^8)$,** which has the form

$$f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

- If we **multiply f (x) by x** , we have

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x)$$

If **$b_7=0$**, then the result is a polynomial of **degree less than 8**, which is already in **reduced form**, and **no further computation** is necessary

If **$b_7 = 1$**, then reduction modulo m(x) is achieved using **$x^4 + x^3 + x + 1$**

Continuation

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x)$$

- If the **bit b_7 = 0** then the right hand above is already in the set of polynomials in GF(2^8) and nothing further needs to be done.
- In this case, the output bit pattern is **$b_6b_5b_4b_3b_2b_1b_0$0.,**

Continuation

❖ If **b_7 = 1**, then **reduction modulo m(x)** is achieved using **$x^4 + x^3 + x + 1$**

$$(f(x) \times x) \;\; mod \;\; m(x)$$

$$= (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \; mod \; m(x)$$

$$= (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \;\; + \;\; (x^8 \; mod \; m(x))$$

$$= (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x \; + 1)$$

$$= (b_6b_5b_4b_3b_2b_1b_00) \quad \otimes \quad (00011011)$$

Continuation

- If $b_7 = 1$, then **reduction modulo m(x)** is achieved using $x^4 + x^3 + x + 1$

$$x \times f(x) = (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x + 1)$$

- The above Equation follows that **multiplication by (i.e., 00000001)** can be implemented as a **1-bit left shift** followed by a **conditional bitwise XOR** with **(00011011)**, which represents $x^4 + x^3 + x + 1$

In General

- To summarize, **Multiplication by a higher power** of can be achieved by **repeated application** of following Equation

$$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_00) & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_00) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}$$

- By **adding intermediate results**, **multiplication by any constant in GF(2^8) can be achieved.**

Multiplication Polynomial in $GF(2^3)$

			000	001	010	011	100	101	110	111
	×		0	1	2	3	4	5	6	7
000	0		0	0	0	0	0	0	0	0
001	1		0	1	2	3	4	5	6	7
010	2		0	2	4	6	3	1	7	5
011	3		0	3	6	5	7	4	1	2
100	4		0	4	3	7	6	2	5	1
101	5		0	5	1	4	2	7	3	6
110	6		0	6	7	1	5	3	2	4
111	7		0	7	5	2	1	6	4	3

(b) Multiplication

$m(x)$: $x^3 + x + 1$

$x^3 \text{ Mod } m(x) = m(x) - x^3$

$m(x) = x + 1 = 011$

$100 \text{ X } 010 = ?$

x^1: $100 \text{ X } 010 = 000 \oplus 011$

$= 011$

Shift

x^2: $100 \text{ X } 100 = 110$

Finally $100 \text{ X } 010$

$= 011 = 3$

Multiplication Polynomial Operation in GF(2^n)

	×	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	$x^2 + x + 1$	$x^2 + 1$
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	$x^2 + 1$	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	$x^2 + 1$	x^2	$x + 1$

(b) Multiplication

Finally 100 X 010

= 011 = 3 = x+1

Additive and multiplicative inverses Does Exist for all Elements in GF(2^3)

w	$-w$	w^{-1}
0	0	—
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

(c) Additive and multiplicative inverses

Observation : Polynomials Over GF(2^3)

- **Hence GF(2^3) is a finite field** because
  - ✓ it is a finite set and
  - ✓ it contains a **unique multiplicative inverse** for every non-zero element.

Example : Arithmetic Polynomials Over GF(2^8)

Exercise : Fast Bit Multiplication Polynomial in GF(2^8)

❖ **Construct the Multiplication Polynomial in GF(2^8)**

$$f(x) = x^6 + x^4 + x^2 + x + 1$$

$$g(x) = x^7 + x + 1$$

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

$$f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1.$$

Solution: Multiplication Polynomial in GF(2^8)

❖ **Construct the Multiplication Polynomial in GF(2^8)**

we need to compute (01010111) × (10000011). First, we determine the results of multiplication by powers of x:

$$
\begin{aligned}
(01010111) \times (00000010) &= (10101110) \\
(01010111) \times (00000100) &= (01011100) \oplus (00011011) = (01000111) \\
(01010111) \times (00001000) &= (10001110) \\
(01010111) \times (00010000) &= (00011100) \oplus (00011011) = (00000111) \\
(01010111) \times (00100000) &= (00001110) \\
(01010111) \times (01000000) &= (00011100) \\
(01010111) \times (10000000) &= (00111000)
\end{aligned}
$$

So,

$$
\begin{aligned}
(01010111) \times (10000011) &= (01010111) \times [(00000001) \oplus (00000010) \oplus (10000000)] \\
&= (01010111) \oplus (10101110) \oplus (00111000) = (11000001)
\end{aligned}
$$

which is equivalent to $x^7 + x^6 + 1$.

Another Example

- Find the result of multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$

Another Example:

- **Step-1 :** We first find the **partial result of multiplying** x^0, x^1, x^2, x^3, x^4, **and** x^5 by P_2.

- We have **P1 = 000100110, P2 = 10011110, modulus = 100011010 (nine bits).** We show the exclusive or operation by $\otimes$

Example

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1 \times P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

Example :

❖ An efficient algorithm for **multiplication using n-bit words**

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	$(00111100) \oplus (00011010) = \underline{\mathbf{00100111}}$
$x^2 \otimes P_2$	01001110	$\underline{\mathbf{01001110}}$
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	$(00111000) \oplus (00011010) = 00100011$
$x^5 \otimes P_2$	01000110	$\underline{\mathbf{01000110}}$
$\mathbf{P_1 \otimes P_2 = (00100111) \oplus (01001110) \oplus (01000110) = 00101111}$		

Finding Multiplicative Inverses in $GF(2^n)$

Finding Multiplicative Inverses in GF(2^n)

- We will use same **Extended Euclid's Algorithm** for finding the **multiplicative inverse (MI)** of a bit pattern in GF(2^n)

Extended Euclid's Algorithm

$r_1 \leftarrow a; \qquad r_2 \leftarrow b;$
$s_1 \leftarrow 1; \qquad s_2 \leftarrow 0;$
$t_1 \leftarrow 0; \qquad t_2 \leftarrow 1;$

(Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2; \; r_2 \leftarrow r;$

(Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2; \; s_2 \leftarrow s;$

(Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2; \; t_2 \leftarrow t;$

(Updating t's)

}

gcd $(a, b) \leftarrow r_1; \; s \leftarrow s_1; \; t \leftarrow t_1$

Finding Multiplicative Inverses in GF(2^8)Using Extended Euclid Function

- In GF (2^8), Find the **inverse of** **($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$$r = r_1 - q \times r_2 \qquad s = s_1 - q \times s_2 \qquad t = t_1 - q \times t_2$$

Finding Multiplicative Inverses in GF(2^n)

- In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

q	r_1	r_2	r	t_1	t_2	t

Finding Multiplicative Inverses in GF(2^n)

- In GF (2^8), find the **inverse of (x^7 + x^4 + x^2 + 1)** modulo **(x^8 + x^4 + x^3 + x + 1).**

$$\begin{array}{ll} r_1 \leftarrow a; & r_2 \leftarrow b; \\ s_1 \leftarrow 1; & s_2 \leftarrow 0; \\ t_1 \leftarrow 0; & t_2 \leftarrow 1; \end{array} \quad \text{(Initialization)}$$

q	r_1	r_2	r	t_1	t_2	t

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^8), find the **inverse of (x^7 +x^4 +x^2 +1)** modulo **(x^8 + x^4 + x^3 + x + 1).**

$$\begin{array}{ll} r_1 \leftarrow a; & r_2 \leftarrow b; \\ s_1 \leftarrow 1; & s_2 \leftarrow 0; \\ t_1 \leftarrow 0; & t_2 \leftarrow 1; \end{array} \quad \text{(Initialization)}$$

q	r1	r2	r	t1	t2	t
	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$				

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^8), find the **inverse of (x^7 +x^4 +x^2 +1)** modulo **(x^8 + x^4 + x^3 + x + 1).**

$$r_1 \leftarrow a; \quad r_2 \leftarrow b;$$
$$s_1 \leftarrow 1; \quad s_2 \leftarrow 0; \qquad \text{(Initialization)}$$
$$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$$

q	r_1	r_2	r	t_1	t_2	t
	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$		0	1	

Finding Multiplicative Inverses in GF(2^n)

- In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$$q \leftarrow r_1 / r_2;$$

q	r_1	r_2	r	t_1	t_2	t
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$		0	1	

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;\ r_2 \leftarrow r;$

(Updating r's)

q	**r_1**	**r_2**	**r**	**t_1**	**t_2**	**t**
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$$r \leftarrow r_1 - q \times r_2 ;$$
$$r_1 \leftarrow r_2 ;\ r_2 \leftarrow r ;$$

(Updating r's)

q	r_1	r_2	r	t_1	t_2	t
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	
	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$				

Finding Multiplicative Inverses in GF(2^n)

- In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;\ t_2 \leftarrow t;$ (Updating t's)

q	r_1	r_2	r	t_1	t_2	t
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	x
	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$				

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo **($x^8 + x^4 + x^3 + x + 1$).**

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;\ t_2 \leftarrow t;$
(Updating t's)

q	**r_1**	**r_2**	**r**	**t_1**	**t_2**	**t**
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	x
	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$		1	x	

Repeat the Process to Find the Multiplicative Inverse

Finding Multiplicative Inverses in GF(2^n)

- In GF (2^8), find the **inverse of ($x^7 + x^4 + x^2 + 1$)** modulo ($x^8 + x^4 + x^3 + x + 1$).

q	r_1	r_2	r	t_1	t_2	t
x	$x^8 + x^4 + x^3 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	0	1	x
$x^2 + x + 1$	$x^7 + x^4 + x^2 + 1$	$x^5 + x^4 + 1$	x	1	x	$x^3 + x^2 + x + 1$
$x^4 + x^3$	$x^5 + x^4 + 1$	x	1	x	$x^3 + x^2 + x + 1$	$x^7 + x^3 + x$
x	x	1	0	$x^3 + x^2 + x + 1$	$x^7 + x^3 + x$	$x^8 + x^4 + x^3 + x + 1$
	1	0		$x^7 + x^3 + x$		

The answer is ($x^7 + x^3 + x$)

Finding Multiplicative Inverses in GF(2^n)

❖ In GF (2^4), find the **inverse of (x^2 + 1)** modulo ($x^4 + x + 1$).

r = r_1 – q x r_2 ; s = s_1 – q x s_2 ; t = t_1 – q x t_2

q	r_1	r_2	r	t_1	t_2	t
(x^2+1)	(x^4+x+1)	(x^2+1)	(x)	(0)	(1)	(x^2+1)
(x)	(x^2+1)	(x)	(1)	(1)	(x^2+1)	(x^3+x+1)
(x)	(x)	(1)	(0)	(x^2+1)	(x^3+x+1)	(0)
	(1)	(0)		(x^3+x+1)	(0)	

The answer is **($x^3 + x + 1$)**

Finding Multiplicative Inverses in GF(2^n)

❖ In GF(2^8), find the **inverse of (x^5) modulo ($x^8 + x^4 + x^3 + x + 1$).**

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)	$(x^5+x^4+x^3+x)$
(x^3+x^2+1)	(x^3+x^2+1)	(1)	(0)	(x^4+x^3+1)	$(x^5+x^4+x^3+x)$	(0)
	(1)	(0)		$(x^5+x^4+x^3+x)$	(0)	

The answer is **$(x^5 + x^4 + x^3 + x)$**

Using A Generator : To Represent The Elements in GF(2^n)

Using A Generator: To Represent The Elements Of GF(2^n)

- It is particularly convenient to represent the elements of a Galois Field GF(2^n) with the help of a generator element.
- If **g is a generator element**, then every element of GF(2^n), except for the 0 element, can be expressed as some power of g.

$$\boxed{\{0, g, g, g^2, \ldots, g^N\}, \text{ where } N = 2^n - 2}$$

Example :

- Generate the **elements of the field** GF(2^3) using the irreducible polynomial $f(x) = x^3 + x + 1$.

Solution

- The elements **0, g^0, g^1, and g^2** can be easily generated
  - ✓ because they are the **3-bit representations of 0, 1, x, and x^2**
- Elements **g^3 through g^6 (2^3-2= 8-2 = 6),** which represent **x^3 though x^6** need to be divided by the **irreducible polynomial.**

Observation

- To avoid the **polynomial division**, we use
  - ✓ The relation $f(g) = g^3 + g + 1 = 0$

$$g^3 = -g - 1$$

$$= g + 1$$

- We now show that **'g' generates all of the polynomials** of **degree less than 3.**

Generator for GF(2^3) using $x^3 + x + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5
$g^0 (= g^7)$	1	001	1

Operations on Generator in GF(2^3) :

- This **Power Representation** makes **multiplication easy.**
- To multiply in the power notation, **add exponents modulo 7.**

$$g^k = g^{k \bmod 7} \text{ for any integer } k$$

- **For Example:**

$$g^4 \times g^6 = g^{(10 \bmod 7)} = g^3 = g + 1$$

- The same result is achieved using **polynomial arithmetic**

Polynomial Arithmetic in GF(2^3) : Previous Example

- **For Example:**

$$g^4 \times g^6 = g^{(10 \bmod 7)} = g^3 = g + 1$$

- The same result is achieved using **polynomial arithmetic, We have**

$$g^4 = g^2 + g \text{ and } g^6 = g^2 + 1.$$

$$(g^2 + g) \times (g^2 + 1) = g^4 + g^3 + g^2 + 1.$$

Next, we need to determine $(g^4 + g^3 + g^2 + 1) \bmod (g^3 + g + 1)$ by division:

Polynomial Arithmetic in GF(2^3) : Previous Example

Next, we need to determine $(g^4 + g^3 + g^2 + 1) \bmod (g^3 + g + 1)$ by division:

$$
\begin{array}{r|l}
 & g \quad + 1 \\
\cline{2-2}
g^3 + g + 1 & g^4 + g^3 + g^2 + g \\
 & g^4 + \qquad\; g^2 + g \\
\cline{2-2}
 & \qquad g^3 \\
 & \qquad g^3 + \qquad\; g + 1 \\
\cline{2-2}
 & \qquad\qquad\quad\; g + 1
\end{array}
$$

Both
Provides
Same
Results

$g^4 \, X \, g^6 = g^{(10 \bmod 7)} = g^3 = g + 1$

Addition tables for GF(2^3) using the Power Representation.

GF(2^3) Arithmetic Using Generator for the Polynomial $(x^3 + x + 1)$

		000	001	010	100	011	110	111	101
	+	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	1	G	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
001	1	1	0	$g + 1$	$g^2 + 1$	g	$g^2 + g + 1$	$g^2 + g$	g^2
010	g	g	$g + 1$	0	$g^2 + g$	1	g^2	$g^2 + 1$	$g^2 + g + 1$
100	g^2	g^2	$g^2 + 1$	$g^2 + g$	0	$g^2 + g + 1$	g	$g + 1$	1
011	g^3	$g + 1$	g	1	$g^2 + g + 1$	0	$g^2 + 1$	g^2	$g^2 + g$
110	g^4	$g^2 + g$	$g^2 + g + 1$	g^2	g	$g^2 + 1$	0	1	$g + 1$
111	g^5	$g^2 + g + 1$	$g^2 + g$	$g^2 + 1$	$g + 1$	g^2	1	0	g
101	g^6	$g^2 + 1$	g^2	$g^2 + g + 1$	1	$g^2 + g$	$g + 1$	g	0

Multiplication tables for GF(2^3) using the Power Representation.

		000	001	010	100	011	110	111	101
	$\times$	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
010	g	0	g	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1
100	g^2	0	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g
011	g^3	0	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g	g^2
110	g^4	0	g^2+g	g^2+g+1	g^2+1	1	g	g^2	$g+1$
111	g^5	0	g^2+g+1	g^2+1	1	g	g^2	$g+1$	g^2+g
101	g^6	0	g^2+1	1	g	g^2	$g+1$	g^2+g	g^2+g+1

In general, for GF(2^n) with irreducible polynomial $f(x)$, determine $g^n = \mathrm{f}(g) - g^n$. Then calculate all of the powers of g from g^{n+1} through g^{2^n-2}. The elements of the field correspond to the powers of g from g^0 through g^{2^n-2} plus the value 0. For multiplication of two elements in the field, use the equality $g^k = g^{k \bmod (2^n-1)}$ for any integer k.

Outline

- **Modular Polynomial Arithmetic Over GF(2^n)**
- **Arithmetic Polynomials Over GF(2^n)**
  - ✓ **Example : Arithmetic Polynomials Over GF(2^8)**
- **Finding Multiplicative Inverses in GF(2^n)**
- **Using A Generator : To Represent The Elements in GF(2^n)**

Thank U