Galois, Évariste (1811-1832)

Aritmética em corpos finitos binários GF(2^n) incluindo cálculo do inverso multiplicativo e considerações computacionais

Thaysa Bello

Agenda

- Motivação
- Pré requisito
- Aritmética em corpos finitos binários GF(2^n)
- Inverso Multiplicativo
- Considerações Computacionais
- Gerador
- Resumo

Motivação

- Por que estudar corpos finitos na forma GF(p^n) ?

  Importante na criptografia

  - Diversos algoritmos de criptografia contam com as propriedades dos corpos finitos:
    - Advanced Encryption Standard (AES)
    - Criptografia de curva elíptica

Corpo (Field), {F, +, x}

- O que é?
  - Conjunto de elementos com duas operações binárias – adição e multiplicação.
- Axiomas obedecidos
  - A1-A5 e M1- M7
- Exemplos conhecidos de corpos
  - Números racionais
  - Números reais
  - Números complexos

Axiomas do tipo A (Adição)

- (A1) Fechamento sob adição
- (A2) Associatividade da adição $a + (b + c) = (a + b) + c$
- (A3) Identidade aditiva $a + 0 = 0 + a = a$
- (A4) Inverso aditivo $a + (-a) = (-a) + a = 0$
- (A5) Comutatividade da adição $a + b = b + a$

Axiomas do tipo M (Multiplicação)

- (M1) Fechamento sob multiplicação
- (M2) Associatividade da multiplicação $a(bc) = (ab)c$
- (M3) Leis distributivas $a(b + c) = ab + ac$ $(a + b)c = ac + bc$
- (M4) Comutatividade da multiplicação $ab = ba$
- (M5) Identidade multiplicativa $a1 = 1a = a$
- (M6) Sem divisores zero
- (M7) Inverso multiplicativo $aa^{-1} = a^{-1}a = 1$

Corpo Finito

- O que é?
  - Um corpo com um número finito de elementos.

- Ordens e Aritmética utilizada
  - Corpos finitos de ordem p
    - Aritmética *mod* p
  - Corpos finitos de ordem p^n , para n >1
    - Aritmética polinomial modular

Aritmética **módulo 8 (Zn)** versus **em GF(2^3)**

Adição

Módulo 8

+	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

GF(2^3)

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

Multiplicação

Módulo 8

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

GF(2^3)

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

Inversos aditivos e multiplicativos

Módulo 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

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

Aritmética **módulo 8 (Zn)** versus **em GF(2^3)**

Adição

Módulo 8

+	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

GF(2^3)

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

Aritmética **módulo 8** (Zn) versus **em GF(2^3)**

Adição

Módulo 8

+	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

GF(2^3)

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

Multiplicação

Módulo 8

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

GF(2^3)

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

Inversos aditivos e multiplicativos

Módulo 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

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

Aritmética polinomial modular

- Considerar conjunto S
  - Todos os polinômios de grau n-1 ou menos sobre o corpo de Zp
- Forma dos polinômios do conjunto S

$$f(x) = \sum_{i=0}^{n-1} a_i x^i$$

a_i → Assume um valor no conjunto {0,1, ..., p-1}

Aritmética polinomial modular

- Considerar conjunto S
  - Todos os polinômios de grau n-1 ou menos sobre o corpo de Zp
- Forma dos polinômios do conjunto S

$$f(x) = \sum_{i=0}^{n-1} a_i x^i = a_0 x^0 + a_1 x^1 + \cdots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1}$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^i = a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0$$

Aritmética polinomial modular

- Quantidade dos elementos do conjunto S ?
- Cada elemento é um polinômio
- Quantos são esses polinômios?
  - Um total de polinômios p^n diferentes em S.
  - Para p = 3 e n = 2 → 9 polinômios diferentes ($3^2 = 9$)
  - Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)
  - Para p = 2 e n = 8 → 256 polinômios diferentes ($2^8 = 256$)

Aritmética polinomial modular - Exemplo

- Para p = 3 e n = 2 → 9 polinômios diferentes ($3^2 = 9$)
  - Quais sãos os polinômios do conjunto S ?

Aritmética polinomial modular - Exemplo

- Para p = 3 e n = 2 → 9 polinômios diferentes ($3^2 = 9$)
  - Quais sãos os polinômios do conjunto S ?

$$f(x) = \sum_{i=0}^{n-1} a_i x^i = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

a_i → Assume um valor no conjunto {0,1, ..., p-1} ; para p = 3 =>{0,1,2}

Para p = 3 e n = 2 → 9 polinômios diferentes ($3^2 = 9$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = \sum_{i=0}^{n-1} a_i x^i = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

a_i → Assume um valor no conjunto {0,1, ..., p-1} ; para p = 3 =>{0,1,2}

n'=1 $a_0 x^0$ ou a_0

- $a_0 = 0$; f(x) = 0
- $a_0 = 1$; f(x) = 1
- $a_0 = 2$; f(x) = 2

n'=2 $a_0 x^0 + a_1 x^1$ ou $a_1 x + a_0$

- $a_0 = 0$; $a_1 = 1$; f(x) = x
- $a_0 = 0$; $a_1 = 2$; f(x) = 2x
- $a_0 = 1$; $a_1 = 1$; f(x) = x+1
- $a_0 = 1$; $a_1 = 2$; f(x) = 2x+1
- $a_0 = 2$; $a_1 = 1$; f(x) = x + 2
- $a_0 = 2$; $a_1 = 2$; f(x) = 2x + 2

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

$a_2 = 0$; $a_1 = 0$; $a_0 = 0$; **f(x) = ?**

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

$a_2 = 0$; $a_1 = 0$; $a_0 = 0$; **f(x) = $0x^2 + 0x^1 + 0x^0$**

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

$a_2 = 0$; $a_1 = 0$; $a_0 = 0$; **f(x) = 0**

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

$a_2 = 0$; $a_1 = 0$; $a_0 = 0$; **f(x) = 0**

$a_2 = 0$; $a_1 = 0$; $a_0 = 1$; **f(x) = 1**

$a_2 = 0$; $a_1 = 1$; $a_0 = 0$; **f(x) = x**

$a_2 = 0$; $a_1 = 1$; $a_0 = 1$; **f(x) = x+1**

$a_2 = 1$; $a_1 = 0$; $a_0 = 0$; **f(x) = x^2**

$a_2 = 1$; $a_1 = 0$; $a_0 = 1$; **f(x) = $1x^2 + 0x^1 + 1x^0$**

Para p = 2 e n = 3 → 8 polinômios diferentes ($2^3 = 8$)

- Quais sãos os polinômios do conjunto S ?

$$f(x) = a_2x^2 + a_1x^1 + a_0x^0$$

$a_2 = 0$; $a_1 = 0$; $a_0 = 0$; **f(x) = 0**

$a_2 = 0$; $a_1 = 0$; $a_0 = 1$; **f(x) = 1**

$a_2 = 0$; $a_1 = 1$; $a_0 = 0$; **f(x) = x**

$a_2 = 0$; $a_1 = 1$; $a_0 = 1$; **f(x) = x+1**

$a_2 = 1$; $a_1 = 0$; $a_0 = 0$; **f(x) = x^2**

$a_2 = 1$; $a_1 = 0$; $a_0 = 1$; **f(x) = x^2 +1**

$a_2 = 1$; $a_1 = 1$; $a_0 = 0$; **f(x) = x^2 +x**

$a_2 = 1$; $a_1 = 1$; $a_0 = 1$; **f(x) = x^2 +x +1**

Aritmética polinomial modular

- Segue as regras comuns da aritmética polinomial com 2 refinamentos
- A aritmética sobre os coeficientes é realizada no módulo p. (usamos regras da aritmética para corpo finito Zp)
- Se a multiplicação resultar em um polinômio de grau maior que n -1, então o polinômio será reduzido módulo algum polinômio irredutível m(x) de grau n. (r(x) = f(x) mod m(x))

Aritmética polinomial modular

- Exemplo: AES utiliza a aritmética no corpo finito $GF(2^8)$.
  - Polinômio irredutível
    - $m(x) = x^8 + x^4 + x^3 + x + 1$
  - Considere polinômio 1
    - $f(x) = x^6 + x^4 + x^2 + x + 1$
  - Considere polinômio 2
    - $g(x) = x^7 + x + 1$

Aritmética polinomial modular ADIÇÃO

- Adição (Equivalente a operação XOR)
  - f(x) + g(x)
    - f(x) = $x^6 + x^4 + x^2 + x + 1$
    - g(x) = $x^7 + x + 1$
  - $f(x) + g(x) = x^7 + x^6 + x^4 + x^2$

Aritmética polinomial modular MULTIPLICAÇÃO

- Multiplicação (Equivalente a operação AND lógico)
  - f(x) x g(x)
    - f(x) = $x^6 + x^4 + x^2 + x + 1$
    - g(x) = $x^7 + x + 1$
  - f(x) x g(x) =?

Aritmética polinomial modular MULTIPLICAÇÃO

- f(x) x g(x)

$$
\begin{array}{rr}
 & x^6 + x^4 + x^2 + x + 1 \\
x & x^7 + x + 1 \\
\hline
 & x^6 + x^4 + x^2 + x + 1
\end{array}
$$

Aritmética polinomial modular MULTIPLICAÇÃO

- f(x) x g(x)

$$
\begin{array}{r}
x^6 + x^4 + x^2 + x + 1 \\
\times \quad x^7 + x + 1 \\
\hline
x^6 + x^4 + x^2 + x + 1 \\
x^7 + x^5 + x^3 + x^2 + x
\end{array}
$$

Aritmética polinomial modular MULTIPLICAÇÃO

- f(x) x g(x)

$$
\begin{array}{r}
x^6 + x^4 + x^2 + x + 1 \\
\times \quad x^7 + x + 1 \\
\hline
x^6 + x^4 + x^2 + x + 1 \\
x^7 + x^5 + x^3 + x^2 + x \\
\hline
x^{13} + x^{11} + x^9 + x^8 + x^7
\end{array}
$$

Aritmética polinomial modular MULTIPLICAÇÃO

- f(x) x g(x)

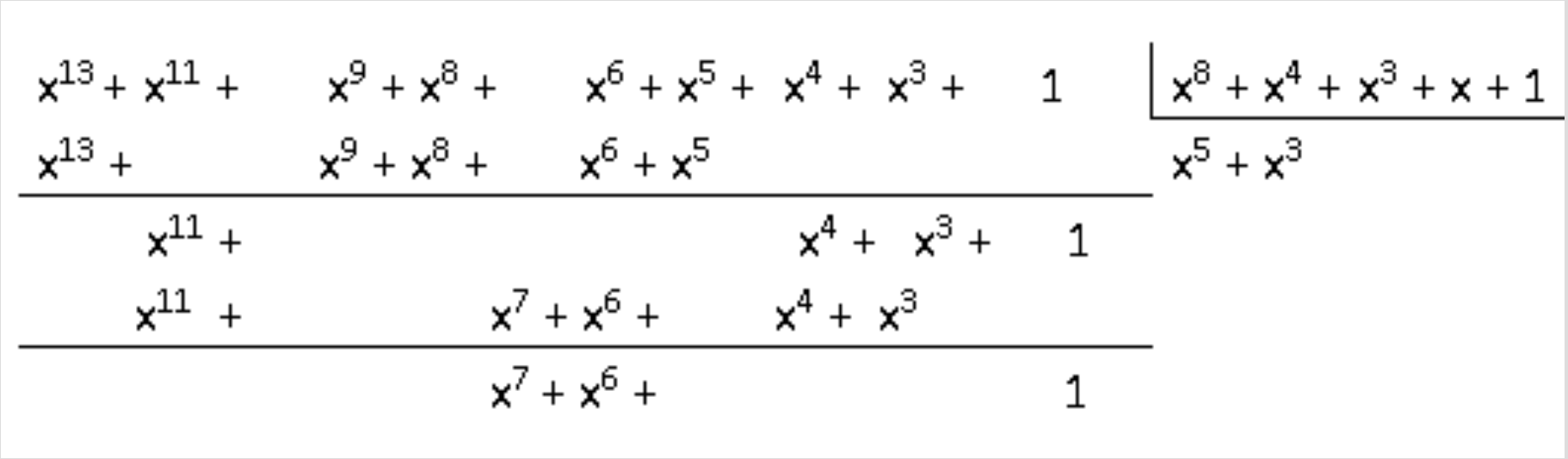
$$
\begin{array}{r}
x^6 + x^4 + x^2 + x + 1 \\
\times \quad x^7 + x + 1 \\
\hline
x^6 + x^4 + x^2 + x + 1 \\
x^7 + x^5 + x^3 + x^2 + x \\
\hline
x^{13} + x^{11} + x^9 + x^8 + x^7 \\
\hline
x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{array}
$$

Aritmética polinomial modular MULTIPLICAÇÃO

- f(x) x g(x) mod m(x)

$f(x) \times g(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$

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



- f(x) x g(x) mod m(x) = $x^7 + x^6 + 1$

ADIÇÃO (operação XOR)

+		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	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+x+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

MULTIPLICAÇÃO

Polinômio irredutível $x^3 + x + 1$

	×	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	$x+1$

Inverso multiplicativo de um polinômio

- mdc[m(x),f(x)] = 1
- Grau de f(x) < m(x)
- m(x) → polinômio irredutível
- Exemplo: f(x) mod m(x)

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

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

Verificando o graus do 2 polinômios

$x^7 < x^8$

Inverso multiplicativo de um polinômio

- mdc[m(x),f(x)] = 1
- Grau de f(x) < m(x)
- m(x) → polinômio irredutível
- Exemplo: $(x^7 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1)$

Verificando o grau do 2 polinômios

$x^7 < x^8$

Inverso multiplicativo de um polinômio

$a(x) = x^8 + x^4 + x^3 + x + 1$
$b(x) = x^7 + x + 1$

$q(x) = x$
$r(x) = x^4 + x^3 + x^2 + 1$

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

$a(x) = x^7 + x + 1$
$b(x) = x^4 + x^3 + x^2 + 1$

$q(x) = x^3 + x^2 + 1$
$r(x) = x$

$$\begin{array}{l|l} x^7 + \quad x + 1 & x^4 + x^3 + x^2 + 1 \\ \hline x^7 + x^6 + x^5 + \quad x^3 & x^3 + x^2 + 1 \\ \hline x^6 + x^5 + \quad x^3 + \quad x + 1 & \\ x^6 + x^5 + x^4 + \quad x^2 & \\ \hline x^4 + x^3 + x^2 + x + 1 & \\ x^4 + x^3 + x^2 + \quad 1 & \\ \hline x & \end{array}$$

$a(x) = x4 + x3 + x2 + 1$
$b(x) = x$

$q(x) = x^3 + x^2 + x$
$r(x) = 1$

$$\begin{array}{l|l} x^4 + x^3 + x^2 + \quad 1 & x \\ \hline x^4 & x^3 + x^2 + x \\ \hline x^3 + x^2 + \quad 1 & \\ x^3 & \\ \hline x^2 + \quad 1 & \\ x^2 & \\ \hline 1 & \end{array}$$

Inverso multiplicativo de um polinômio

a (x) = $x^4 + x^3 + x^2 + 1$ b(x) = x q(x) = $x^3 + x^2 + x$ **r(x) =1**	$x^4 + x^3 + x^2 + 1 \mid x$ $x^4 \quad\quad x^3 + x^2 + x$ $x^3 + x^2 + 1$ x^3 $x^2 + 1$ x^2 1
a (x) = x b(x) = 1 q(x) = x r(x) = 0	$x \mid 1$ $x \quad x$ 0

Inverso multiplicativo de um polinômio

- $a(x) = q(x).b(x) + r(x)$
  $x^8 + x^4 + x^3 + x + 1 = x.(x^7 + x + 1) + x^4 + x^3 + x^2 + 1$

- $v_{-1} = 1$
- $w_{-1} = 0$

$$r_{-1} = a(x) = a(x).v_{-1}(x) + b(x).w_{-1}(x)$$

- $v_0 = 0$
- $w_0 = 1$

$$r_0 = b(x) = a(x).v_0(x) + b(x).w_0(x)$$

- $v_1 = v_{-1} - q(x).v_0(x) = 1$
- $w_1 = w_{-1} - q(x).w_0(x) = q(x)$

$$r_1 = a(x).v_1(x) + b(x).w_1(x)$$

Inverso multiplicativo de um polinômio

$a(x) = x^8 + x^4 + x^3 + x + 1$ $b(x) = x^7 + x + 1$ $q(x) = x$ $r(x) = x^4 + x^3 + x^2 + 1$	$v_1 = v_{-1} - q(x).v_0(x) = 1 - (x).0$ $v_1 = 1$ $w_1 = w_{-1} - q(x).w_0(x) = 0 - (x).1$ $w_1 = x$
$a(x) = x^7 + x + 1$ $b(x) = x^4 + x^3 + x^2 + 1$ $q(x) = x^3 + x^2 + 1$ $r(x) = x$	$v_2 = v_0 - q(x).v_1(x) = 0 - (x^3 + x^2 + 1).1$ $V_2 = x^3 + x^2 + 1$ $w_2 = w_0 - q(x).w_1(x) = 1 - (x^3 + x^2 + 1).x$ $w_2 = x^4 + x^3 + x + 1$
$a(x) = x^4 + x^3 + x^2 + 1$ $b(x) = x$ $q(x) = x^3 + x^2 + x$ **$r(x) = 1$**	$v_3 = v_1 - q(x).v_2(x) = 1 - (x^3 + x^2 + x)(x^3 + x^2 + 1)$ $v_3 = x^6 + x^2 + x + 1$ $w_3 = w_1 - q(x).w_2(x) = x - (x^3 + x^2 + x)(x^4 + x^3 + x + 1)$ **$w_3 = x^7$**

Inverso multiplicativo de um polinômio

$a(x) = x^4 + x^3 + x^2 + 1$ $b(x) = x$ $q(x) = x^3 + x^2 + x$ **$r(x) = 1$**	$v_3 = v_1 - q(x).v_2(x) = 1 - (x^3 + x^2 + x)(x^3 + x^2 + 1)$ $v_3 = x^6 + x^2 + x + 1$ $w_3 = w_1 - q(x).w_2(x) = x - (x^3 + x^2 + x)(x^4 + x^3 + x + 1)$ **$w_3 = x^7$**
$a(x) = x$ $b(x) = 1$ $q(x) = x$ $r(x) = 0$	$V_4 = v_2 - q(x).v_3(x)$ $v_4 = (x^3 + x^2 + 1) - (x)(x^6 + x^2 + x + 1)$ $V_4 = x^7 + x + 1$ $w_4 = w_2 - q(x).w_3(x)$ $w_4 = (x^4 + x^3 + x + 1) - (x)(x^7)$ $w_4 = x^8 + x^4 + x^3 + x + 1$

$$w(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$$

Considerações Computacionais

- Cada polinômio em $GF(2^n)$ pode ser representado por um número de *n* bits.
- Exemplo: para 2^3, cada polinômio pode ser representado por 3 bits
- Adição: Para polinômios em $GF(2^n)$ é a operação XOR
- Multiplicação: Técnica baseia-se em $x^n \bmod p(x) = [p(x) - x^n]$

Considerações computacionais
Adição

Em Z_2 → a adição é a operação XOR

$\mathrm{GF}(2^8)$

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

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

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

$$(01010111) \oplus (10000011) = (11010100)$$

$$\{57\} \oplus \{83\} = \{D4\}$$

Considerações computacionais Multiplicação

- Multiplicação: Técnica baseia-se em $x^n \bmod p(x) = [p(x) - x^n]$

Em GF(2^8) e $m(x) = \mathbf{x^8} + x^4 + x^3 + x + 1$, tem -se:

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

$x^4 + x^3 + x + 1$ equivalente a 00011011 em binário

X equivalente a 00000010 em binário

Considerações computacionais Multiplicação

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

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

Redução de módulo m(x)

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

Considerações computacionais Multiplicação

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

Se $b_7 = 0$

Polinômio de grau menor que 8, que já está na forma reduzida

Se $b_7 = 1$

Redução de módulo m(x) é obtida

- Multiplicação por x (00000010)
  - deslocamento a esquerda de 1 bit seguido por XOR 00011011

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

Considerações computacionais
Multiplicação

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

$$(01010111)$$

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

$$(10000011)$$

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

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

$$(00011011)$$

$$(01010111) \times (10000011) = f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$$

Considerações computacionais
Multiplicação

$$x \times f(x) = \begin{cases} (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) & \text{if } b_7 = 0 \\ (b_6 b_5 b_4 b_3 b_2 b_1 b_0 0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}$$

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

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

Gerador

$GF(2^3)$

$$f(g) = g^3 + g + 1 = 0$$

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

$$g^4 = g(g^3) = g(g + 1) = g^2 + g$$
$$g^5 = g(g^4) = g(g^2 + g) = g^3 + g^2 = g^2 + g + 1$$
$$g^6 = g(g^5) = g(g^2 + g + 1) = g^3 + g^2 + g = g^2 + g + g + 1 = g^2 + 1$$
$$g^7 = g(g^6) = g(g^2 + 1) = g^3 + g = g + g + 1 = 1 = g^0$$

Gerador

$GF(2^3)$

Utilizando o polinômio irredutível: $x^3 + x + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
$g^0 (= g^7)$	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

Resumo do que foi apresentado

- Aritmética polinomial modular
  - Existe um total de p^n polinômios diferentes
  - Um conjunto S é um corpo finito
  - Adição equivale ao XOR
  - Multiplicação r(x) = f(x) mod m(x)
- Inverso multiplicativo
  - Se mdc[m(x),f(x)] = 1 existe o inverso multiplicativo
- Considerações computacionais
  - Um polinômio em $GF(2^n)$ pode ser representado pelos coeficientes binários
- Gerador
  - Técnica equivalente para definir um corpo finito na forma $GF(2^n)$