Introduction to Cryptology

Tutorial-04

Mathematical Background: Extension Finite Fields

28.03.2023, v42

Irreducible Polynomials and extension Fields GF(2^m)

g(x) is called Irreducible Polynomial of degree m over GF(2)

$g(x) = a_0 + a_1 x + a_2 x^2 + .. a_n x^n$

where $a_i \in$ GF(2) and Factorization is not possible over GF(2)

- The period **e** of g(x) is the **smallest** e such that **$x^e = 1$** [mod g(x)]
- **e** is actually the order of x modulo g(x). e **divides** **2^m -1**
- If e = **2^m -1** the the polynomial is called **primitive**
- The **reciprocal** polynomial is defined as $g^*(x) = x^n g(1/x)$
- The **period of the reciprocal** polynomial $g^*(x)$ is equal to that of g(x)

GF (2^m)
The ring of polynomials $Z_{g(x)}$ modulo an irreducible polynomial of degree m over GF(2) is an extension field with 2^m elements
The order of any element in GF(2^m) is a divisor of 2^m -1 (Lagrange theorem)

Problem 4-1: Polynomials over a field

Give the corresponding vector representation of the polynomials

1. $1 + x^2 + x^5 + x^9$
2. $1 + x^3 + x^8 + x^{12}$
3. $x^2 + x^5 + x^7$
4. $x + x^9 + x^{10}$
5. $1 + x^8$
6. $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$

Solution 4-1:

LSB MSB

1. $1 + x^2 + x^5 + x^9$ = 1010010001
2. $1 + x^3 + x^8 + x^{12}$ = 1001000010001
3. $x^2 + x^5 + x^7$ = 00100101
4. $x + x^9 + x^{10}$ = 01000000011
5. $1 + x^8$ = 100000001
6. $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$ = 11111111

Problem 4-2: Polynomials over a field

Compute the following polynomial products over **GF(2)**

1. $(1 + x^2)(1 + x^2 + x^5)$
2. $(x^3 + x^4)(1 + x^3 + x^8 + x^{12})$
3. $x^3 (1 + x^3 + x^5 + x^6)$

Compute the following polynomial products over **GF(3)**

1. $(1 + 2x^2)(1 + x^2 + 2x^5)$
2. $(x + 2x^3)(1 + 2x^3 + x^8 + x^{12})$

Compute the following polynomial products over **GF(7)**

1. $(2 + 4x^2)(1 + 3x^2 + 5x^5)$
2. $(3x + 5x^3)(6 + 2x^3 + 3x^8)$

Solution 4-2:

products over **GF(2)**

1. $(1 + x^2)(1 + x^2 + x^5) = 1 + x^2 + x^5 + x^2 + x^4 + x^7 = 1 + 2x^2 + x^4 + x^5 + x^7 = 1 + x^4 + x^5 + x^7$
2. $(x^3 + x^4)(1 + x^3 + x^8 + x^{12}) = x^3 + x^6 + x^{11} + x^{15} + x^4 + x^7 + x^{12} + x^{16} = x^3 + x^4 + x^6 + x^7 + x^{11} + x^{12} + x^{15} + x^{16}$
3. $x^3 (1 + x^3 + x^5 + x^6) = x^3 + x^6 + x^8 + x^9$

Solution 4-2 cont.:

products over **GF(3)**

1. $(1 + 2x^2)(1 + x^2 + 2x^5) = 1 + x^2 + 2x^5 + 2x^2 + 2x^4 + 4x^7 = 1 + 3x^2 + 2x^4 + 2x^5 + 4x^7 = 1 + 2x^4 + 2x^5 + 1x^7$
2. $(x + 2x^3)(1 + 2x^3 + x^8 + x^{12}) =$

products over **GF(7)**

1. $(2 + 4x^2)(1 + 3x^2 + 5x^5) = 2 + 6x^2 + 10x^5 + 4x^2 + 12x^4 + 20x^7 = 2 + 10x^2 + 12x^4 + 10x^5 + 20x^7$
   $= 2 + 3x^2 + 5x^4 + 3x^5 + 6x^7$
2. $(3x^2 + 5x^3)(6x^2 + 2x^3 + 3x^8) =$

Problem 4-3: Polynomials division over a finite field

Compute the following polynomial divisions over **GF(2)**

$(x^{12} + x^8 + x^6 + x^2 + 1) \div (x^5 + x^2 + 1)$

Solution 4-3:

$(x^{12} + x^8 + x^6 + x^2 + 1) \div (x^5 + x^2 + 1)$

$- \; (x^{12} + x^9 + x^7)$ | $x^7 + x^4 + x^3 + x^2 + 1$ ← **Q(x)**

$x^9 + x^8 + x^7 + x^6 + x^2 + 1$
$x^9 + x^6 + x^4$

$x^8 + x^7 + x^4 + x^2 + 1$
$x^8 + x^5 + x^3$

$x^7 + x^5 + x^4 + x^3 + x^2 + 1$
$x^7 + x^4 + x^2$

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

$x^3 + x^2$ ← **Remainder of the division R(x)**

in GF(2):
1+1=2=0
=> 1=-1
=>Addition
Is equal to
subtraction

Problem 4-4: Find the multiplicative inverse of **x + 1** modulo **$x^5 + x^3 + 1$**

Solution 4-4: <u>Compute</u> gcd [$P_1(x)$, $P_2(x)$] = $A(x) P_1(x)$ + **B(x)** $P_2(x)$

if **gcd =1**, then the inverse is **B(x)**

<u>Extended gcd Algorithm:</u>

A2 = A1 – q A2

B2 = B1 – q B2

$P_1(x)$	$P_2(x)$	A1(x)	A2(x)	B1(x)	B2(x)	Q(x)	R(x)
$x^5 + x^3 + 1$	$x + 1$	1	0	0	1	$x^4 + x^3$	1
$x + 1$	1	0	1	1	$0 - (x^4 + x^3)*1$ = $x^4 + x^3$	$x + 1$	0

=> $(x^4 + x^3) \equiv (x + 1)^{-1}$ modulo $(x^5 + x^3 + 1)$

$x^5 + x^3 + 1 = 0$
$x^5 = x^3 + 1$

Check: $(x + 1)(x^4 + x^3) = x^5 + x^4 + x^4 + x^3 \equiv 1$ modulo $(x^5 + x^3 + 1)$

Problem 4-5: Elements order over an extension field

Compute the exponents of the element x from 1 to 16 and 31 over **GF(2^5)** which is generated by the irreducible polynomial $P(x) = (x^5 + x^2 + 1)$

Solution 4-5:

If $P(x)= x^5 + x^2 + 1$ is the modulus then it is equal to zero

That is $x^5 + x^2 + 1 = 0$ Thus $x^5 = x^2 + 1$

Let us compute the exponents of **x** over this field:

$x^1 = x$ mod $(x^5 + x^2 + 1)$
$x^2 = x^2$ mod $(x^5 + x^2 + 1)$
$x^3 = x^3$ mod $(x^5 + x^2 + 1)$
$x^4 = x^4$ mod $(x^5 + x^2 + 1)$
$x^5 = x^2 + 1$ mod $(x^5 + x^2 + 1)$
$x^6 = x(x^2 + 1) = x^3 + x$ mod $(x^5 + x^2 + 1)$
$x^7 = x(x^3 + x) = x^4 + x^2$ mod $(x^5 + x^2 + 1)$
$x^8 = x^5 + x^3 = x^3 + x^2 + 1$ mod $(x^5 + x^2 + 1)$
$x^9 = x^4 + x^3 + x$ mod $(x^5 + x^2 + 1)$
$x^{10} = x^5 + x^4 + x^2 = x^4 + x^2 + x^2 + 1 = x^4 + 1$ mod $(x^5 + x^2 + 1)$
$x^{11} = x^5 + x = x^2 + x + 1$ mod $(x^5 + x^2 + 1)$
$x^{12} = x^3 + x^2 + x$ mod $(x^5 + x^2 + 1)$

Solution 4-5 cont.:

$x^{13} = x^4 + x^3 + x^2$ mod $(x^5 + x^2 + 1)$
$x^{14} = x^5 + x^4 + x^3 = x^4 + x^3 + x^2 + 1$ mod $(x^5 + x^2 + 1)$
$x^{15} = x^5 + x^4 + x^3 + x = x^4 + x^3 + x^2 + x + 1$ mod $(x^5 + x^2 + 1)$
$x^{16} = x^5 + x^4 + x^3 + x^2 + x = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1$ mod $(x^5 + x^2 + 1)$
…
$x^{31} = x(x^{15})^2 = x(x^4 + x^3 + x^2 + x + 1)^2 = x^9 + x^7 + x^5 + x^3 + x =$
$= x^4 + x^4 + x^3 + x^3 + x^2 + x^2 + x + x + 1 = 1$ mod $(x^5 + x^2 + 1)$

$\Rightarrow$ **The order of x is 31 !**

<u>Important notice:</u>
In GF (2^5): the order of any element
Is a divisor of 2^5-1=31
Divisors of 31 are 1 and 31 !
=> The order can be either 1 or 31 !

Problem 4-6: sample Hardware Structure for Multiplication and division in GF(2^5)

Given GF(2^5) generated by the irreducible polynomial **$g(x) = x^5 + x^3 + 1$**

Design a circuit which multiplies any serial data stream I(x) by the inverse of the polynomial **$b(x)= x + 1$** in GF(2^5).

Check the circuit by multiplying **$I(x) = (1 + x^2 + x^3)$ by $H(x)= (x + 1)^{-1}$**

Solution 4-6: First computing the multiplicative inverse of b(x) modulo g(x)

the inverse is **$H(x) = b(x)^{-1}$ mod $g(x) = (x + 1)^{-1}$ mod $(x^5 + x^3 + 1)$**

<u>Computing H(x) by the Extended gcd Algorithm:</u>

A2 = A1 – q A2

B2 = B1 – q B2

$P_1(x)$	$P_2(x)$	A1(x)	A2(x)	B1(x)	B2(x)	Q(x)	R(x)
$x^5 + x^3 + 1$	$x + 1$	1	0	0	1	$x^4 + x^3$	1
$x + 1$	1	0	1	1	$0 - (x^4 + x^3)*1$ $= x^4 + x^3$	$x + 1$	0

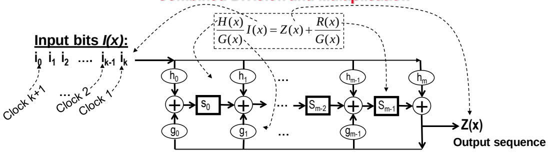
=> $H(x)= (x + 1)^{-1}$ mod $(x^5 + x^3 + 1) = (x^4 + x^3)$

$x^5 + x^3 + 1 = 0$
$x^5 = x^3 + 1$

Check: $(x + 1)(x^4 + x^3) = x^5 + x^4 + x^4 + x^3 = x^3 + 1 + x^4 + x^4 + x^3 \equiv 1$ mod $(x^5 + x^3 + 1)$ q.e.d

<u>Use the following implementation template:</u>

Hardware Architectures for Arithmetic in GF (2^m)
Combined Division and Multiplication



<u>Multiplier</u>: $H(x) = h_0 + h_1x^1 + h_2x^2 \cdots + h_mx^m$

<u>Divisor</u>: $G(x) = g_0 + g_1x^1 + g_2x^2 \cdots + g_mx^m$

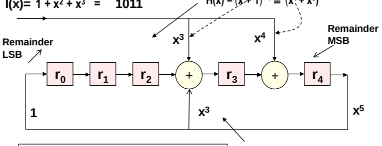
<u>Input</u>: $I(x) = i_0 + i_1x^1 + i_2x^2 \cdots + i_kx^k$

<u>Remainder</u>: $R(x) = r_0 + r_1x^1 + r_2x^2 \cdots + r_{m-1}x^{m-1}$
R(x)=H(x) • I(x) mod G(x) $= s_0 + s_1x^1 + s_2x^2 \cdots + s_{m-1}x^{m-1}$ *after clock k+1*

Solution 4-6 cont.:

A circuit which multiplies any serial data stream I(x) by the inverse of the polynomial $b(x)= x + 1$ that is $b(x)^{-1} = H(x)= x^3 + x^4$ modulo the irreducible polynomial $g(x) = x^5 + x^3 + 1$

$I(x)= 1 + x^2 + x^3$ = 1011 (LSB .. MSB)



<u>Check:</u>
$I(x) \times H(x) =$
$= (1 + x^2 + x^3)(x^4 + x^3)$
$= x^4 + x^6 + x^7 + x^3 + x^5 + x^6$
$= x^4 + x^7 + x^3 + x^5$
$= x^4 + x^2 + 1 + x^3 + x^3 + 1 + x^3$
$= x^4 + x^2 + x^3$

$x^5 = 1 + x^3$
$x^6 = x + x^4$
$x^7 = x^2 + x^5 = x^2 + 1 + x^3$

Clocking in the data stream I(x)= 1011
States before clocking each input
<u>Clock</u> LSB .. MSB
1. Input 1 register state 00000 ← Initial state = 0
2. Input 1 register state 00011 ← next state
3. Input 0 register state 10000
4. Input 1 register state 01000
Input x register state 00111 ← State after clock 4

Result of multiplication= $x^2 + x^3 + x^4$

Problem 4-7: ad-hoc Class exercise

Select a polynomial as a modulus for **GF(2^8)**

Compute a primitive element

- Wich are the possible multiplicative orders in **GF(2^8)**
- How many elements do exist from each possible order
- Compute a primitive element
- Compute other 5 primitive elements
- Compute one element for each possible multiplicative order

Solution 4-7:

Problem 4-8: ad-hoc Class exercise, Online-Example: ad-hoc Class exercise

Compute the multiplicative inverse of $x^4 + x^2 + 1$ modulo $x^5 + x + 1$

$P_1(x)$	$P_2(x)$	B1(x)	B2(x)	Q(x)	R(x)
$X^5 + x + 1$	$x^4 + x^2 + 1$	0	1	x	X^3+1
$x^4 + x^2 + 1$	X^3+1	1	X	x	X^2+X+1
X^3+1	X^2+X+1	X	x^2+1	X+1	0

As gcd [$P_1(x)$, $P_2(x)$] ≠ 1 => a multiplicative inverse do not exist.

Trying another $P_2(x) = x^2 + 1$

$P_1(x)$	$P_2(x)$	B1(x)	B2(x)	Q(x)	R(x)
$X^5 + x + 1$	x^2+1	0	1	x^3+x	1
x^2+1	1	1	x^3+x	x^2+1	0

As gcd [$P_1(x)$, $P_2(x)$] = 1, => the multiplicative inverse is $P_2(x)^{-1}$ = B2(x) = x^3+x

Check: $(x^2 + 1)(x^3+x) = x^5+x^3+x^3+x = x + 1 + x = 1$ q.e.d

Online-Example: ad-hoc Class exercise

Compute the multiplicative inverse of $x^2 + 1$ modulo $x^7 + x^6 + 1$

P1(x)	P2(x)	B1(x)	B2(x)	Q(x)	R(x)
$x^7 + x^6 + 1$	$x^2 + 1$	0	1	$x^5+x^4+x^3$ $+x^2+x+1$	x
$x^2 + 1$	x	1	$x^5+x^4+x^3+x^2+x+1$	x	1
x	1	$x^5+x^4+x^3+x^2+x+1$	$x^6+x^5+x^4+x^3+x^2+x+1$	x	0

Check: $(x^2 + 1)(x^6+x^5+x^4+x^3+x^2+x+1)$

$= x^8+x^7+x^6+x^5+x^4+x^3+x^2 + x^6+x^5+x^4+x^3+x^2+x+1$

$= x^6 + x + 1 + x^6 + 1 + x + 1$

$= 1$

$x^7 = x^6 + 1$

$x^8 = x^7 + x = x^6 + x + 1$