PART 5

有限域

多项式运算

多项式运算

- n次多项式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \sum a_i x^i$$

  - a_i组成的集合称为**系数集**

- 讨论三种多项式运算
  - 使用代数基本规则的普通多项式运算
  - 系数运算是模p运算的多项式运算，即系数在Z_p中
  - 系数在Z_p中，且多项式被定义为模一个n次多项式m(x)的多项式运算

普通多项式运算

- 对应系数相加减（+，-）
- 系数依次相乘（×）
- 如

$$f(x) = x^3 + x^2 + 2\ ,\quad g(x) = x^2 - x + 1$$

$$f(x) + g(x) = x^3 + 2x^2 - x + 3$$

$$f(x) - g(x) = x^3 + x + 1$$

$$f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$$

注意：定义在整数集上的多项式不支持除法运算，整数集不是域

系数在模Z_p中的多项式运算

- **系数是域F的元素时，构成多项式环（不构成整环，因为有可能有零因子）**
- **系数是Z_p的元素的多项式**
- **最感兴趣的是mod 2**
  - **所有系数是0 或 1**
  - **例如：$f(x) = x^3 + x^2$ 和 $g(x) = x^2 + x + 1$**

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

$$f(x) \times g(x) = x^5 + x^2$$

多项式的因式

- **对于任何多项式:**
  - $f(x) = q(x)\,g(x) + r(x)$，$r(x)$ 称为余式
  - $r(x) = f(x) \bmod g(x)$
- **若$r(x)=0$，则称$g(x)$整除$f(x)$**
- **若$r(x)\neq 0$，则称$f(x)$为不可约（既约）多项式，也叫素多项式。**
- **用一个不可约多项式作为模，则可构成一个域（可以定义除法了）**

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

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

(a) Addition

	×	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+x	x^2	$x+1$

(b) Multiplication

有限域GF（2^m）

- GF（2^m）表示有限域的阶（元素个数）为2^m

  其中元素通常用长度为m的二进制串表示

- GF（2^m）= $\{(a_{m-1},a_{m-2},\ldots a_1,a_0)\}$

  其中 $a_i \in \{0,1\}$

- 还可表示成多项式形式：

$$GF(2^m)=\left\{a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0\right\} \quad \text{其中，} a_i \in \{0,1\}$$

域元素（$a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$）通常表示为：

$$GF(2^m)=\{(a_{m-1}a_{m-2}\cdots a_1a_0)\} \quad \text{其中，} a_i \in \{0,1\}$$

GF（2^8）上的加法

- **在GF（2^8）上的加法定义为二进制多项式的加法，等同于按位异或运算。**

Example: '57' + '83' = 'D4', or with the polynomial notation:

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

In binary notation we have: "01010111" + "10000011" = "11010100". Clearly, the addition corresponds with the simple bitwise EXOR (denoted by $\oplus$) at the byte level.

1^1=0　0^0=0　1^0=1　0^1=1

在GF（2^8）上的乘法

- **在GF（2^8）上的乘法定义为二进制多项式的乘积模一个次数为8的不可约二进制多项式，此不可约二进制多项式为 $m(x)=x^8+x^4+x^3+x+1$：**

$$c(x)=a(x)\cdot b(x)=a(x)\times b(x)\bmod m(x)$$

- **什么是不可约多项式：**

当且仅当f(x)不能表示为两个多项式积（两个多项式都在 F 上，次数都低于f(x)），f(x)称为 F 上的不可约多项式，也叫素多项式。

- **$m(x)=x^8+x^4+x^3+x+1$是GF（2^8）上的一个不可约多项式，是在30个8次不可约多项式中选择的一个。**

乘法“·”

$$c(x) = a(x) \cdot b(x) = a(x) \times b(x) \bmod m(x)$$

$$a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

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

$$c(x) = c_7x^7 + c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

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

- **是普通多项式乘法，但系数运算可看作比特的乘法和异或运算，即看作域{0,1}上的运算。**

在GF（2^8）上的乘法

（01110011）·（10010101）=?

$$(x^6+x^5+x^4+x+1)\cdot(x^7+x^4+x^2+1) \quad \text{Mod} \quad (x^8+x^4+x^3+x+1)$$

一个乘法例子

$$(x^6+x^5+x^4+x+1)\cdot(x^7+x^4+x^2+1) \quad \text{Mod} \quad (x^8+x^4+x^3+x+1)$$

- **73*95=（01110011）·（10010101）**

$$(x^6+x^5+x^4+x+1)\cdot(x^7+x^4+x^2+1)$$

$$=x^{13}+x^{12}+x^{11}+x^{10}+x^9+3x^8+2x^7+2x^6+2x^5+2x^4+x^3+x^2+x+1$$

$$=x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^3+x^2+x+1$$
$$+2(x^8+x^4+x^3+x+1)$$

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

- **所以，（01110011）·（10010101）=（01110000）**

在GF（2^8）上的乘法例子2

Example: '57' • '83' = 'C1', or:

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^{13} + x^{11} + x^9 + x^8 + x^7 +$$
$$x^7 + x^5 + x^3 + x^2 + x +$$
$$x^6 + x^4 + x^2 + x + 1$$
$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \text{ modulo } x^8 + x^4 + x^3 + x + 1$$
$$= x^7 + x^6 + 1$$

多项式乘法逆

- **定义4：在GF（2^8）上的二进制多项式b(x)的乘法逆为满足下列方程式的二进制多项式a(x)，记为$b^{-1}(x)$**

$$a(x)b(x) \bmod m(x)=1$$

$$a(x) = x^3+1$$

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


海南大学
Hainan university