



# 现代密码学

## 第二十六讲 有限域基础

信息与软件工程学院



## 第二十六讲 有限域基础

---



A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the title.

# 什么是域

- $F$ 是一个非空集合，定义了加法、乘法两个二元运算，对这两个运算封闭
- 加法满足：对于任意 $a, b, c \in F$ 
  - $a+b=b+a$ ；交换律
  - $(a+b)+c=a+(b+c)$ ；结合律
  - 存在 $0 \in F$ ，使得 $a+0=a$ ；有零元
  - 存在 $-a \in F$ ，使得 $a+(-a)=0$ ；有负元
- 乘法满足：对于任意 $a, b, c \in F$ 
  - $a \cdot b=b \cdot a$ ；交换律
  - $(a \cdot b) \cdot c=a \cdot (b \cdot c)$ ；结合律
  - 存在 $e \in F$ ，使得 $a \cdot e=a$ ；有单位元
  - 存在 $a^{-1} \in F$ ，使得 $a \cdot a^{-1}=e$ ；有逆元
- 乘法对加法满足分配率
  - $a \cdot (b+c)=a \cdot b+a \cdot c$

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the section header.

## 域的例子

---

- $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}_{\text{mod } n}$ , 加法和乘法都是模 $n$ 的运算, 运算封闭
  - 加法满足结合律和交换律, 有零元 $0$ , 有负元
  - 乘法满足结合律和交换律, 有单位元 $1$ , 不一定有逆元
  - $\mathbb{Z}_n$ 中的数什么时候才有乘法逆元呢?
  - 引理: 整数 $a$ 在模 $n$ 乘法下有逆元, 当且仅当 $a$ 与 $n$ 互素。
  - 所有与 $n$ 互素的元素在模 $n$ 乘法下构成乘法交换群
  - $1 \dots n-1$ 都与 $n$ 互素, 则 $n$ 为素数
  - 对于任一素数 $p$ ,  $\mathbb{Z}_p$ 为域, 其元素个数为 $p$ 个
-

## 域的例子（续）

- $F[x]/(f(x)) = \{r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1x + r_0 \mid r_i \in F, 0 \leq i \leq n-1\}$ , 加法和乘法都是模 $f(x)$ 的运算, 运算封闭
- 加法满足结合律和交换律, 有零元 $0$ , 有负元
- 乘法满足结合律和交换律, 有单位元 $1$ , 不一定有逆元
- $F[x]/(f(x))$ 中的多项式什么时候才有乘法逆元呢?

## 域的例子（续）

- 引理： $r(x)$ 在模 $f(x)$ 乘法下有逆元，当且仅当 $r(x)$ 与 $f(x)$ 互素。
- 所有与 $f(x)$ 互素的元素在模 $f(x)$ 乘法下构成乘法交换群
- 次数比 $f(x)$ 的次数低的多项式都与 $f(x)$ 互素，则 $f(x)$ 为不可约多项式
- 对于任一首项系数为1的不可约多项式， $F[x]/(f(x))$ 为域
- 若 $F=Z_p$ ，则 $F[x]/(f(x))$ 中元素个数为 $p^n$ 个
- $p^n$ 域的构造方法是首先选取 $Z_p$ 中的一个 $n$ 次不可约多项式，然后构造集合

$$F[x]/(f(x)) = \{r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1x + r_0 \mid r_i \in F, 0 \leq i \leq n-1\}$$

集合中的加法和乘法运算为模多项式 $f(x)$ 的运算



## 第二十六讲 有限域基础

---

A vertical line with two white circles. The top circle is connected to a blue horizontal bar containing the text '有限域的基本概念'. The bottom circle is connected to a blue horizontal bar containing the text 'GF(2^8) 域'.

有限域的基本概念

$\text{GF}(2^8)$  域

---

## AES中的处理单元

- AES加密标准算法中是以字节为处理单元
- 可以将每一字节看作是有限域 $GF(2^8)$ 上的一个元素，分别对应于一个次数不超过7的多项式。如 $b_7b_6b_5b_4b_3b_2b_1b_0$ 可表示为多项式

$$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0$$

- 还可以将每个字节表示为一个十六进制数，即每4比特表示为一个十六进制数，代表较高位的4比特的符号仍在左边。例如，**01101011**可表示为**6B**
- 它们之间的运算为 $GF(2^8)$ 中的运算





# GF(2<sup>8</sup>) 中的运算

**定义：** 在GF(2<sup>8</sup>) 上的加法定义为二进制多项式的加法，且其系数模2。

例如： ‘57’ + ‘83’ = ‘D4’，用多项式表示为

$$(x^6+x^4+x^2+x+1)+(x^7+x+1)=x^7+x^6+x^4+x^2 \pmod{m(x)}$$

用二进制表示为

$$01010111+10000011=11010100$$

**定义：** 在GF(2<sup>8</sup>)上的乘法（用符号 · 表示）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

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

它的十六进制表示为 ‘11B’。

例如： ‘57’ · ‘83’ = ‘C1’可表示为以下的多项式乘法：

$$(x^6+x^4+x^2+x+1)(x^7+x+1)=x^7+x^6+1 \pmod{m(x)}$$

A decorative blue horizontal bar with a series of white horizontal lines is positioned to the left of the title.

## GF(2<sup>8</sup>) 中的逆元和x乘法

---

**定义：**对任何次数小于8的多项式**b(x)**，可用推广的欧几里得算法得

$$b(x)a(x)+m(x)c(x)=1$$

即**a(x) b(x)=1 mod m(x)**。因此**a(x)**是**b(x)**的乘法逆元。

**定义：**函数**xtime(x)**定义为GF(2)上的**x b(x)**。其运算如下：若**b<sub>7</sub>=0**，则**x b(x)**的结果就是把字节**b**左移一位，且在最右边补上上0；若**b<sub>7</sub>=1**，则先对**b(x)**在字节内左移一位（最后一位补0），则再与‘1B’（00011011）做逐比特异或。

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the section header.

## xtime(x)的例子

---

- 例如, '57'·'13'可按如下方式实现:
- '57'·'02'=xtime(57)='AE';
- '57'·'04'=xtime(AE)='47';
- '57'·'08'=xtime(47)='8E';
- '57'·'10'=xtime(8E)='07';
- '57'·'13'='57'·('01'  $\oplus$  '02'  $\oplus$  '10')
- ='57'  $\oplus$  'AE'  $\oplus$  '07'='FE'

## GF(2<sup>8</sup>)上的模多项式运算

- 4个字节构成的向量可以表示为系数在GF(2<sup>8</sup>)上的次数小于4的多项式
- 多项式的加法就是对应系数相加；换句话说，多项式的加法就是4字节向量的逐比特异或。
- 规定多项式的乘法运算必须要取模 $M(x)=x^4+1$ ，这样使得次数小于4的多项式的乘积仍然是一个次数小于4的多项式，将多项式的模乘运算记为 $\otimes$ ，设 $a(x)=a_3x^3+a_2x^2+a_1x+a_0$ ， $b(x)=b_3x^3+b_2x^2+b_1x+b_0$ ， $c(x)=a(x)\otimes b(x)=c_3x^3+c_2x^2+c_1x+c_0$ 。由于 $x^j \bmod (x^4+1)=x^{j \bmod 4}$ ，所以

$$c_0=a_0b_0\oplus a_3b_1\oplus a_2b_2\oplus a_1b_3;$$

$$c_1=a_1b_0\oplus a_0b_1\oplus a_3b_2\oplus a_2b_3;$$

$$c_2=a_2b_0\oplus a_1b_1\oplus a_0b_2\oplus a_3b_3;$$

$$c_3=a_3b_0\oplus a_2b_1\oplus a_1b_2\oplus a_0b_3。$$

# 多项式乘法的矩阵表示

可将上述计算表示为

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

其中元素的加法和乘法为  $\mathbf{GF}(2^8)$  域上的运算

## 模 $x^4+1$ 逆元

**定理：**系数在 $\mathbf{GF}(2^8)$ 上的多项式 $a_3x^3+a_2x^2+a_1x+a_0$ 是模 $x^4+1$ 可逆的，当且仅当矩阵

$$\begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$$

在 $\mathbf{GF}(2^8)$ 上可逆。

# 证明

**证明：**  $a_3x^3+a_2x^2+a_1x+a_0$  是模  $x^4+1$  可逆的，当且仅当存在多项式  $h_3x^3+h_2x^2+h_1x+h_0$  满足

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_3x^3+h_2x^2+h_1x+h_0)=1 \bmod (x^4+1)$$

因此有

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_2x^3+h_1x^2+h_0x+h_3)=x \bmod (x^4+1)$$

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_1x^3+h_0x^2+h_3x+h_2)=x^2 \bmod (x^4+1)$$

$$(a_3x^3+a_2x^2+a_1x+a_0)(h_0x^3+h_3x^2+h_2x+h_1)=x^3 \bmod (x^4+1)$$

## 证明（续）

将以上关系写成矩阵形式即得

$$\begin{pmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} h_0 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_3 \\ h_3 & h_2 & h_1 & h_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

（证毕）





---

感谢聆听!

[xynie@uestc.edu.cn](mailto:xynie@uestc.edu.cn)

---