现代密码学理论与实践

第 4 章　有限域

苗付友　黄文超

October 10, 2019

课件地址

http://staff.ustc.edu.cn/∼huangwc/crypto.html

Motivation

- DES 的问题
- AES 加密与椭圆曲线加密

- 域是一些元素的集合，其上定义了两个算术运算 (加法和乘法)，具有常规算术性质，如封闭性、结合律、交换律、分配律、加法逆和乘法逆等。
- 模算术是一种整数算术，它将所有整数约减为一个固定的集合 $[0, 1, ..., n-1]$，n 为某个整数。任何这个集合外的整数通过除以 n 取余的方式约减到这个范围内。
- 两个整数的最大公因子是可以整除这两个整数的最大正整数。
- 一个有限域就是有有限个元素的域。可以证明有限域的阶 (元素个数) 一定可以写作素数的幂形式 p^n，n 为一个整数，p 为素数。
- 阶为 p 的有限域可以由模 p 的算术来定义。
- 阶为 p^n，$n > 1$ 的有限域可由多项式算术来定义。

Outline

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

Outline

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

群 Groups

定义: 群 $\{G, \cdot\}$

定义一个二元运算 $\cdot$ 的集合，G 中每一个序偶 (a, b) 通过运算生成 G 中元素 $(a \cdot b)$, 满足下列公理:

A1 封闭性 Closure: 如果 a 和 b 都属于 G, 则 $a \cdot b$ 也属于 G.

A2 结合律 Associative: 对于 G 中任意元素 a, b, c，都有 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ 成立

A3 单位元 Identity element: G 中存在一个元素 e，对于 G 中任意元素 a，都有 $a \cdot e = e \cdot a = a$ 成立

A4 逆元 Inverse element: 对于 G 中任意元素 a, G 中都存在一个元素 a'，使得 $a \cdot a' = a' \cdot a = e$ 成立

例子：群

用 N_n 表示 n 个不同符号的集合，$N_n = \{1, 2, ..., n\}$。
n 个不同符号的一个置换是一个 N_n 到 N_n 的一一映射。
定义 S_n 为 n 个不同符号的所有置换组成的集合。
S_n 中的每一个元素都代表集合 $\{1, 2, ..., n\}$ 的一个置换，
容易验证，S_n 是一个群：

- A1 如果 $\pi, \rho \in S_n$，则合成映射 $\pi \cdot \rho$ 根据置换 π 来改变 ρ 中元素的次序而形成，如，$\{3, 2, 1\} \bullet \{1, 3, 2\} = \{2, 3, 1\}$，显然 $\pi \cdot \rho \in S_n$
- A2 映射的合成显而易见满足结合律
- A3 恒等映射就是不改变 n 个元素位置的置换，对于 S_n，单位元是 $\{1, 2, ..., n\}$
- A4 对于任意 $\pi \in S_n$，抵消由 π 定义置换的映射就是 π 的逆元，这个逆元总是存在，例如：$\{2, 3, 1\} \bullet \{3, 1, 2\} = \{1, 2, 3\}$

群 Groups

定义：有限群 Finite Group 和无限群 Infinite Group

- 如果一个群的元素是有限的，则该群称为有限群
- 群的阶等于群中元素的个数
- 反之，如果一个群的元素是无限的，则该群称为无限群

定义：交换群 Abelian Group （阿贝尔群）

A5 交换律 Commutative: 对于 G 中任意的元素 a, b，都有 $a \cdot b = b \cdot a$ 成立

定义：循环群 Cyclic Group

- 如果群中的每一个元素都是一个固定的元素 $a(a \in G)$ 的幂 $a^k(k$ 为整数)，则称群 G 为循环群
- 元素 a 生成了群 G，或者说 a 是群 G 的生成元。

环 Rings

定义：环 $\{R, +, \times\}$

具有加法和乘法两个二元运算的元素的集合，对于环中的所有 $a, b, c,$ 都服从以下公理：

- [A1-A5] 关于加法是一个交换群。单位元是 0，a 的逆是 -a.

M1 **乘法封闭性** 如果 a 和 b 属于 R, 则 ab 也属于 R

M2 **乘法结合律** 对于 R 中任意 a, b, c 有 $a(bc) = (ab)c$.

M3 **乘法分配律** $a(b + c) = ab + ac$ 或者 $(a + b)c = ac + bc$

定义：交换环

M4 **乘法交换律** $ab = ba$，交换环

定义：整环

M5 **乘法单位元** R 中存在元素 1 使得所有 a 有 $a1 = 1a$.

M6 **无零因子** 如果 R 中有 a, b 且 $ab = 0$, 则 $a = 0$ or $b = 0$.

域 Fields

定义：域 $\{F, +\times\}$

具有加法和乘法的两个二元运算的元素的集合，对于 F 中的任意元素 a, b, c, 满足以下公理：

- [A1-M6] F 是一个整环

M7 乘法逆元 对于 F 中的任意元素 a(除 0 以外), F 中都存在一个元素 a^{-1}, 使得 $aa^{-1} = (a^{-1})a = 1$.

性质

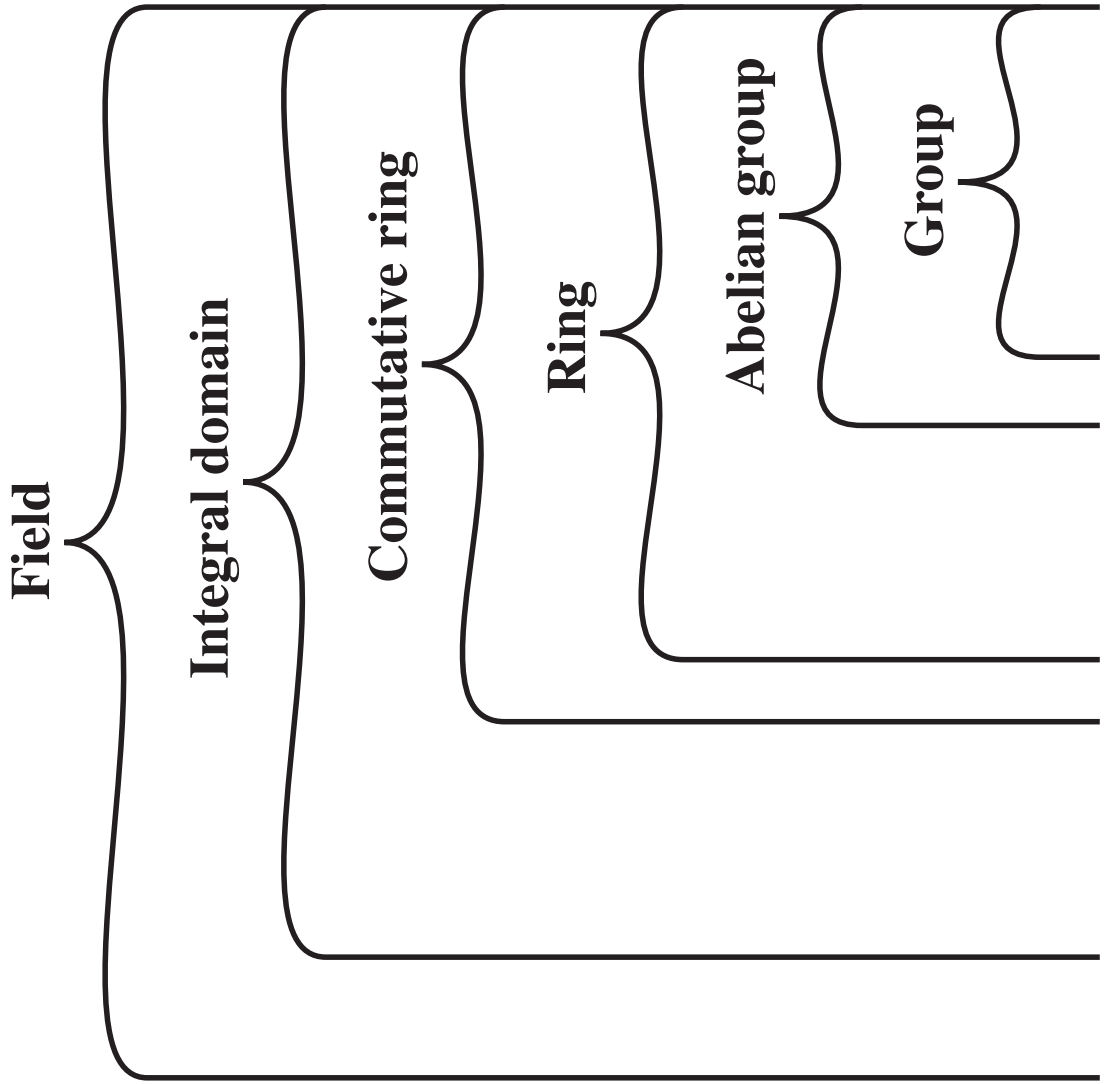
域就是一个集合，在其上进行加减乘除而不脱离该集合

- 除法：$a/b = a(b^{-1})$

例子

- 有理数集合, 实数集合和复数集合都是域
- 整数集合不是域，因为只有 1 和-1 有乘法逆元

群、环、域的关系



(A1) Closure under addition:
(A2) Associativity of addition:
(A3) Additive identity:

(A4) Additive inverse:

(A5) Commutativity of addition:
(M1) Closure under multiplication:
(M2) Associativity of multiplication:
(M3) Distributive laws:

(M4) Commutativity of multiplication:
(M5) Multiplicative identity:

(M6) No zero divisors:

(M7) Multiplicative inverse:

Outline

1. 群、环、域
2. **模运算**
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

模运算

定义

给定任意正整数 n 和 a，如果用 a 除以 n，得到的商q 和余数r 满足如下关系:

$$a = qn + r$$

其中 $0 \leq r < n; q = \lfloor a/n \rfloor$。$\lfloor x \rfloor$ 表示小于等于 x 的最大整数。

性质

给定 a 和 n 时，q 和 r 即唯一确定，即

$$a = \lfloor a/n \rfloor \times n + (a \mod n)$$

因子 Divisors

定义: 因子

如果 $a = mb$, 其中 a, b, m 为整数，则当 $b \neq 0$ 时，即 b 能整除a, 或 a 除以 b 余数为 0, $b \mid a$, 则 b 是 a 的一个因子。

例子

24 的正因子有 1, 2, 3, 4, 6, 8, 12 和 24。

性质

- 如果 $a \mid 1$, 则 $a = \pm 1$
- 如果 $a \mid b$，且 $b \mid a$, 则 $a = \pm b$
- 任何 $b \neq 0$ 能整除 0
- 如果 $b \mid g$，且 $b \mid h$, 则对任何整数 m 和 n 有 $b \mid (mg + nh)$

同余 Congruence

定义：同余

如果 $(a \mod n) = (b \mod n)$，则称整数 a 和 b 是模 n 同余。

性质

- 如果 $n \mid (a - b)$，则 $a = b \mod n$ （= 代表模 n 同余）
- 如果 $a = b \mod n$，则 $b = a \mod n$
- 如果 $a = b \mod n$ 且 $b = c \mod n$，则 $a = c \mod n$

模算术运算

定义：模算术

运算 ($\bmod n$) 将所有整数映射到集合 $\{0, 1, \ldots, (n-1)\}$。因此，限制在这个集合的技术称为模算术。

性质

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

模算术运算

$+$	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

Table: 模 8 加法

$\times$	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

Table: 模 8 乘法

模算术运算

定义：加法逆元 $-w$

若存在 z，使得

$$w + z = 0 \mod n$$

则，z 即为加法逆元 $-w$

定义：乘法逆元 w^{-1}

若存在 z，使得

$$w \times z = 1 \mod n$$

则，z 即为乘法逆元 w^{-1}

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

Table: 模 8 的加法逆元和乘法逆元

模运算的性质

定义：剩余类集 剩余集 Residues

定义比 n 小的非负整数集合为 Z_n：

$$Z_n = \{0, 1, ..., (n-1)\}$$

定义：剩余类

模 n 的剩余类表示为 $[0], [1], [2], \ldots, [n-1]$，其中：

$$[r] = \{a \mid a \in Z \wedge (a \equiv r \mod n)\}$$

例：模 4 的剩余类

$$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots,\}, \quad [1] = \{\ldots, -7, -3, 1, 5, 9, \ldots,\}$$

$$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots,\}, \quad [3] = \{\ldots, -5, -1, 3, 7, 11, \ldots,\}$$

模运算的性质

Table: Z_n 中整数模运算的性质

性质	表达式
交换律	$(w+x) \mod n = (x+w) \mod n$ $(w \times x) \mod n = (x \times w) \mod n$
结合律	$[(w+x)+y] \mod n = [w+(x+y)] \mod n$ $[(w \times x) \times y] \mod n = [w \times (x \times y)] \mod n$
分配律	$[w \times (x+y)] \mod n = [(w \times x)+(w \times y)] \mod n$
单位元	$(0+w) \mod n = w \mod n$ $(1 \times w) \mod n = w \mod n$
加法逆元 $(-w)$	$\forall w \in Z_n$，存在一个 z 使得 $w+z=0 \mod n$

Outline

1. 群、环、域
2. 模运算
3. **欧几里得算法**
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

欧几里得算法 Euclid Algorithm

(回顾) 定义: 因子

如果 $a = mb$, 其中 a, b, m 为整数，则当 $b \neq 0$ 时，即 b 能整除a, 或 a 除以 b 余数为 0, $b \mid a$, 则 b 是 a 的一个因子。

定义: 最大公因子

正整数 c 称为 a 和 b 的最大公因子，如果

1. c 是 a 和 b 的因子
2. a 和 b 的任何公因子都是 c 的因子

等价定义为:

$$\gcd(a, b) = \max\left[k, \text{满足} k \mid a \wedge k \mid b\right]$$

性质

对任意非负整数 a 和任意正整数 b:

$$\gcd(a, b) = gcd(b, a \mod b)$$

欧几里得算法 Euclid Algorithm

EUCLID(a, b)

1. $A \leftarrow a; B \leftarrow b$
2. if $B = 0$ return $A = \gcd(a, b)$
3. $R = A \mod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. goto 2

例：求 $\gcd(1970, 1066)$

$$
\begin{aligned}
1970 &= 1 \times 1066 + 904 && \gcd(1066, 904)\\
1066 &= 1 \times 904 + 162 && \gcd(904, 162)\\
904 &= 5 \times 162 + 94 && \gcd(162, 94)\\
162 &= 1 \times 94 + 68 && \gcd(94, 68)\\
94 &= 1 \times 68 + 26 && \gcd(68, 26)\\
68 &= 2 \times 26 + 16 && \gcd(26, 16)\\
26 &= 1 \times 16 + 10 && \gcd(16, 10)\\
16 &= 1 \times 10 + 6 && \gcd(10, 6)\\
10 &= 1 \times 6 + 4 && \gcd(6, 4)\\
6 &= 1 \times 4 + 2 && \gcd(4, 2)\\
4 &= 2 \times 2 + 0 && \gcd(2, 0)
\end{aligned}
$$

Outline

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

有限域 GF(p) Galois Fields

定义: GF(p)

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p-1\}$ 的集合

$$Z_p$$

其中，运算为模 p 的算术运算。

定义: GF(p^n) ????

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p^n-1\}$ 的集合

$$Z_{p^n}$$

其中，运算为????

有限域 GF(p) Galois Fields

定义: GF(p)

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p-1\}$ 的集合

$$Z_p$$

其中，运算为模 p 的算术运算。

性质: 乘法逆元 (w^{-1})

任意 $w \in Z_p$, 如果 $w \neq 0$, 则存在 $z \in Z_p$, 使得

$$w \times z \equiv 1 \mod p$$

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

Table: 模 8 的乘法逆元

w	0	1	2	3	4	5	6
w^{-1}	–	1	4	5	2	3	6

Table: 模 7 的乘法逆元

在 GF(p) 中求乘法逆元

扩展的 EUCLID(m,b)

1. $(A_1, A_2, A_3) \leftarrow (1, 0, m); (B_1, B_2, B_3) \leftarrow (0, 1, b)$
2. if $B_3 = 0$ return 不存在乘法逆元
3. if $B_3 = 1$ return $B_2 = b^{-1} \mod m$
4. $Q = \lfloor \frac{A_3}{B_3} \rfloor$
5. $(T_1, T_2, T_3) \leftarrow (A_1 - QB_1, A_2 - QB_2, A_3 - QB_3)$
6. $(A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$
7. $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$
8. goto 2

性质：不变式 — 最终 $bB_2 \equiv 1 \mod m$

在每一步计算之后，始终满足

$$mT_1 + bT_2 = T_3, mA_1 + bA_2 = A_3, mB_1 + bB_2 = B_3$$

在 GF(p) 中求乘法逆元

例：在域 GF(1759) 里求元素 550 的乘法逆元

Q	A_1	A_2	A_3	B_1	B_2	B_3
–	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

Outline

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. **多项式运算**
6. 有限域 GF(2^n)

多项式运算

三种多项式运算

1. 使用代数基本规则的普通多项式运算
2. 系数运算是模 p 运算的多项式运算，即系数在 GF(p) 中
3. 系数在 GF(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

运算 1: 普通多项式运算

一个 n 次多项式 $(n \geq 0)$ 的表达形式如下

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

其中 a_i 是某个指定数集 S 中的元素，该数集称为系数集，且 $a \neq 0, f(x)$ 是定义在系数集 S 上的多项式

多项式运算

运算 1: 运算法则

如果 $f(x)=\sum_{i=0}^{n} a_i x^i, g(x)=\sum_{i=0}^{m} b_i x^i, n \geq m$, 则**加法运算**定义为:

$$f(x)+g(x)=\sum_{i=0}^{m}(a_i+b_i)x^i+\sum_{i=m+1}^{n} a_i x^i$$

乘法运算定义为:

$$f(x)\times g(x)=\sum_{i=0}^{n+m} c_i x^i, \quad c_k=a_0 b_k+a_1 b_{k-1}+\cdots+a_{k-1}b_1+a_k b_0$$

多项式运算

运算 1：例子

如果 $f(x) = x^3 + x^2 + 2, g(x) = x^2 - x + 1$ 则：

$$\begin{aligned} f(x) + g(x) &= x^3 + 2x^2 - x + 3 \\ f(x) - g(x) &= x^3 + x + 1 \\ f(x) \times g(x) &= x^5 + 3x^2 - 2x + 2 \\ f(x) \ / \ g(x) &= ?? \end{aligned}$$

运算 2: 系数在 Z_p 中的多项式运算

运算 2: 系数在 Z_p 中的多项式运算

在计算每个系数的值时需要做模运算

例:$p = 2$ 时，系数为 0 或 1

令 $f(x) = x^3 + x^2, g(x) = x^2 + x + 1$，则

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

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

令 $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$, $g(x) = x^3 + x + 1$, 则

$$f(x) + g(x) = f(x) - g(x) = x^7 + x^5 + x^4$$

$$f(x) \times g(x) = x^{10} + x^4 + x^2 + 1$$

$$f(x)/g(x) = x^4 + 1$$

运算 2: 系数在 Z_p 中的多项式运算

定义：最大公因式 $c(x) = \gcd(a(x), b(x))$

- $c(x)$ 是可以整除 $a(x)$ 和 $b(x)$
- $a(x)$ 和 $b(x)$ 的任何公因式都是 $c(x)$ 的因式

性质

$$\gcd[a(x), b(x)] = \gcd[b(x), a(x) \mod b(x)]$$

运算 2: 系数在 Z_p 中的多项式运算

EUCLID(a, b) (最大公因子)

1. $A \leftarrow a; B \leftarrow b$
2. if $B = 0$ return $A = \gcd(a, b)$
3. $R = A \mod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. goto 2

EUCLID$(a(x), b(x))$ (最大公因式)

1. $A(x) \leftarrow a(x); B(x) \leftarrow b(x)$
2. if $B(x) = 0$ return $A(x) = \gcd[a(x), b(x)]$
3. $R(x) = A(x) \mod B(x)$
4. $A(x) \leftarrow B(x)$
5. $B(x) \leftarrow R(x)$
6. goto 2

最大公因式

例：求 $\gcd[a(x), b(x)]$

其中，$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $b(x) = x^4 + x^2 + x + 1$

1. $A(x) = a(x), B(x) = b(x), R(x) = x^3 + x^2 + 1$
2. $A(x) = x^4 + x^2 + x + 1, B(x) = x^3 + x^2 + 1, R(x) = 0$
3. $\gcd[a(x), b(x)] = x^3 + x^2 + 1$

Outline

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. **有限域 GF(2^n)**

有限域 GF(2^n)

回顾定义: GF(p)

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p-1\}$ 的集合

$$Z_p$$

其中，运算为模 p 的算术运算。

定义: GF(p^n) ????

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p^n-1\}$ 的集合

$$Z_{p^n}$$

其中，运算为????

有限域 GF(2^n)

回顾定义: GF(p)

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p-1\}$ 的集合

$$Z_p$$

其中，运算为模 p 的算术运算。

定义: GF(p^n) ????

给定一个素数 p, 元素个数为 p 的有限域被定义为: 整数 $\{0, 1, \ldots, p^n-1\}$ 的集合

$$Z_{p^n}$$

其中，运算为????

动机: 加密算法

- 域
- 有限域
- 乘法逆元
- 2 进制表达

有限域 GF(2^n)

回顾：三种多项式运算

1. 使用代数基本规则的普通多项式运算
2. 系数运算是模 p 运算的多项式运算，即系数在 GF(p) 中
3. GF(p^n):系数在 GF(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

有限域 GF(2^n)

运算 3: 多项式模运算

设集合 S 由域 Z_p 上次数小于 n的所有多项式组成，每个多项式具有如下形式：

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

其中，$a_i \in \{0, 1, \ldots, p-1\}$。S 共有 p^n 个不同的多项式

- 该运算遵循基本代数规则中的普通多项式运算规则
- 系数运算以 p 为模，即遵循有限域 Z_p 上的运算规则
- 如果乘法运算的结果是次数大于 $n-1$ 的多项式，那么必须将其除以某个次数为 n 的既约多项式 $m(x)$ 并取余式。对于多项式 $f(x)$，这个余数可表示为 $r(x) = f(x) \mod m(x)$

有限域 GF(2^n)

在 GF(2^n) 求乘法逆元

类似于在 $GF(p)$ 中求乘法逆元: 扩展 EUCLID 算法

有限域的另一种表示: 生成元

定义: 生成元 g

对于阶为 q 的有限域，其生成元是一个元素，记为 g，该元素的前 $q-1$ 个幂构成了 F 的所有非零元素，即域 F 的元素为

$$0, g^0, g^1, \ldots, g^{q-2}$$

性质

考虑有多项式 $f(x)$ 定义的域 F，如果 F 内的一个元素 b 满足 $f(b)=0$，则称 b 为多项式 $f(x)$ 的根，可以证明:
可以证明一个不可约的多项式的根 g是这个不可约多项式定义的有限域的生成元

有限域的另一种表示: 生成元

例: 生成元

考虑有多项式 x^3+x+1 定义的有限域 $\mathrm{GF}(2^3)$。设生成元为 g, 则 $g^3+g+1=0$。因此:

$$
\begin{array}{rcll}
0 & = & & 0 \\
g^0 & = & & 1 \\
g^1 & = & & g \\
g^2 & = & & g^2 \\
g^3 & = & & g+1 \\
g^4 & = & g(g^3)=g(g+1)= & g^2+g \\
g^5 & = & g(g^4)=g(g^2+g)= & g^2+g+1 \\
g^6 & = & g(g^5)=g(g^2+g+1)= & g^2+1 \\
g^7 & = & g(g^6)=g(g^2+1)= & 1
\end{array}
$$

总结

1. 群、环、域
2. 模运算
3. 欧几里得算法
4. 有限域 GF(p)
5. 多项式运算
6. 有限域 GF(2^n)

作业

- Chapter 4 第五版
  - 6, 7, 9, 11, 12, 13, 19, 23, 24, 27