第 2 章：分组密码体制

2.4 数论基础

赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 3 月 4 日

目录

目录

群（Groups）

定义 (群，Groups)

记作 $\{G, \cdot\}$, 定义了一个二元运算 $\cdot$ 的集合 G，G 中每一个序偶 (a, b) 通过运算 $\cdot$ 生成 G 中的元素 $a \cdot b$，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。

注：当群中的运算符是加法时，习惯上记它的单位元为 0，a 的逆元是 $-a$, 并且减法用以下的规则定义：$a - b = a + (-b)$.

有限群、无限群、阶、交换群和循环群

定义 (有限群，无限群，阶)

如果群的元素是有限个，则该群称为**有限群**；否则，称为**无限群**。有限群中元素的个数称为有限群的**阶**。

定义 (交换群，阿贝尔群，Abelian Groups)

还满足以下条件的群称为**交换群**：

(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 Groups)

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

环（Rings）

定义 (环，Rings)

环 R, 记为 $\{R, +, \times\}$，是具有加法和乘法两个二元运算的元素的集合，对于环中的任意元素 a, b, c 满足以下公理：

(A1-A5) R 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) **分配律**：$a(b + c) = ab + ac$ 或 $(a + b)c = ac + bc$。

例 (环)

定义在整数集 $\mathbb{Z}$ 上的加法和乘法运算，都满足上述公理，所以 $\{\mathbb{Z}, +, \times\}$ 构成一个环。

交换环和整环

定义 (交换环)

环如果还满足以下条件，则被称为**交换环**：

(M4) **乘法交换律**：$ab = ba$。

定义 (整环)

交换环如果还满足以下条件，则被称为**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 $a = 0$ 或 $b = 0$。

注：无零因子指没有非平凡零因子。

例 (整环)

定义在整数集上的环 $\{\mathbb{Z}, +, \times\}$ 是交换环，也是整环。

域（Fields）

定义 (域，Fields)

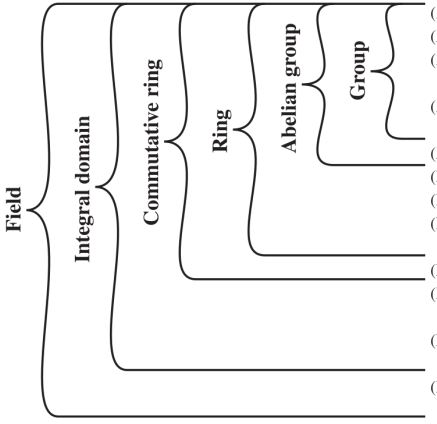
记为 $\{F, +, \times\}$, 是有加法和乘法的两个二元运算的元素的集合，对于 F 中的任意元素 a, b, c, 满足以下公理：

(A1-M6) F 是一个整环；

(M7) 乘法逆元：对于 F 中的任意非零元素 a，F 中都存在一个元素 a^{-1}，使得 $aa^{-1} = a^{-1}a = 1$。

- 域就是一个集合，在其上进行加减乘除而不脱离该集合，除法按以下规则定义：$a/b = ab^{-1}$。
- 有理数集合、实数集合和复数集合都是域；
- 整数集合不是域，因为除了 1 和 -1 有乘法逆元，其他元素都无乘法逆元。

群、环和域的关系



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \quad 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

目录

模运算和同余

定义 (模运算)

如果 a 是整数，n 是正整数，定义 a 除以 n 所得余数为 a 模 n，记为 $a \bmod n$。对于任意整数 a，有

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

例如，$11 \bmod 7 = 4$，$-11 \bmod 7 = 3$.

定义 (同余)

如果 $a \bmod n = b \bmod n$，则称整数 a 和 b 是模 n 同余，表示为 $a \equiv b \pmod{n}$ 或 $a \equiv_n b$.

例如，$73 \equiv 4 \pmod{23}$，$21 \equiv -9 \pmod{10}$

同余的性质

性质

- $n|(a-b) \Leftrightarrow a \equiv b \pmod{n}$.
- **对称性**：$a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$.
- **传递性**：$a \equiv b \pmod{n}$ **且** $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

证明.

- $(\Rightarrow)$ **如果** $n|(a-b)$，**则有** $(a-b) = kn$，k **为某个整数，所以** $a = b + kn$。**故** $a \bmod n = (b + kn) \bmod n = b \bmod n$。
- $(\Leftarrow)$ **如果** $a \equiv b \pmod{n}$，**那么** $a = k_1 n + r, b = k_2 n + r$，**进而** $n|(a-b)$。

模算术运算

性质 (模运算的分配率)

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

性质 (模运算的加性和乘性)

如果 $a \equiv b \pmod{n}$ **且** $c \equiv d \pmod{n}$，**则**

$$(a+c) \equiv (b+d) \pmod{n}$$
$$(a \times c) \equiv (b \times d) \pmod{n}$$

- $n|(a-b) \wedge n|(c-d) \Rightarrow n|(a-b+c-d) \Rightarrow n|[(a+c)-(b+d)] \Rightarrow (a+c) \equiv (b+d) \pmod{n}$.
- $n|(a-b) \wedge n|(c-d) \Rightarrow n|[c(a-b)+b(c-d)] \Rightarrow n|(ac-bd) \Rightarrow ac \equiv bd \pmod{n}$.

模算术运算

性质

如果 $ac \equiv bd \pmod{n}$ **且** $c \equiv d \pmod{n}$，$\gcd(c, n) = 1$，**则** $a \equiv b \pmod{n}$。

例如：$3 \times 2 \equiv 1 \times 2 \pmod{4}$ **且** $2 \equiv 2 \pmod{4}$，**但** $3 \neq 1 \pmod{4}$，**因为** $\gcd(2, 4) \neq 1$。

证明.

$$ac \equiv bd \pmod{n} \Rightarrow n|(ac - bd) \tag{1}$$

$$c \equiv d \pmod{n} \Rightarrow n|(c - d) \Rightarrow c - d = kn \text{ for some } k. \tag{2}$$

So we have $d = c - kn$. Continuing the argument of Eq. (1), we have that

$$n|[ac - b(c - kn)] \Rightarrow n|(ac - bc - kbn) \Rightarrow n|(a - b)c$$

Because $\gcd(c, n) = 1$, then c does not contain divisor n. Hence $a - b$ must have divisor n, i.e., $n|(a - b)$. We thus obtain $a \equiv b \pmod{n}$. □

模算术运算

推论

如果 $ai \equiv aj \pmod{n}$ 且 $\gcd(a, n) = 1$，则 $i \equiv j \pmod{n}$。

令 $\mathbb{Z}_n \triangleq \{0, \ldots, n-1\}$ 为小于 n 的非负整数集合。

引理

如果 $\gcd(a, n) = 1$，则对于每个 $i, j \in \mathbb{Z}_n$ 且 $i \neq j$，那么

$$ai \bmod n \neq aj \bmod n$$

证明.

假设 $ai \bmod n = aj \bmod n$，即 $ai \equiv aj \pmod{n}$。由于 $\gcd(a, n) = 1$，所以 $i \equiv j \pmod{n}$。又因为 $i, j \in \mathbb{Z}_n$，所以只能 $i = j$，这与条件 $i \neq j$ 相矛盾，所以假设不成立。 □

加法逆元和乘法逆元

- **加法逆元**：对于给定的 $a \in \mathbb{Z}_n$，如果存在 $z \in \mathbb{Z}_n$，使得 $a + z \equiv 0 \pmod{n}$，则称 z 为 a 的加法逆元，即 $-a = z$。
- **乘法逆元**：对于给定的 $a \in \mathbb{Z}_n \backslash \{0\}$，如果存在 $z \in \mathbb{Z}_n \backslash \{0\}$，使得 $az \equiv 1 \pmod{n}$，则称 z 为 a 的乘法逆元，即 $a^{-1} = z$。
- $\mathbb{Z}_n \backslash \{0\}$ 中的所有元素都有加法逆元，但不一定都有乘法逆元

+	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

模 8 加法

×	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

模 8 乘法

乘法逆元存在的条件

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

模 7 乘法

定理 (乘法逆元存在的条件)

如果 $\gcd(a, n) = 1$，则 $\mathbb{Z}_n \backslash \{0\}$ 中存在 a 的模 n 乘法逆元 $z \in \mathbb{Z}_n \backslash \{0\}$，使得 $az \equiv 1 \pmod{n}$，即 $a^{-1} \bmod n = z$。

因为 a 与 n 互素，由前面的引理知，如果用 a 乘以 $\mathbb{Z}_n \backslash \{0\}$ 中的所有数 z 模 n，得到的余数将以不同次序涵盖 $\mathbb{Z}_n \backslash \{0\}$ 中的所有数，那么至少有一个余数为 1，这时的 z 即为 a 的乘法逆元。

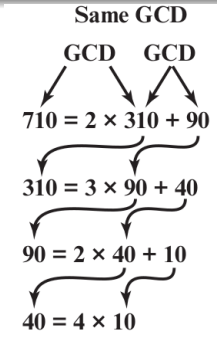
乘法逆元存在的条件

$i \in \mathbb{Z}_n$	$ai \bmod n \in \mathbb{Z}_n$
0	0
1	$a \bmod n$
2	$2a \bmod n$
$\vdots$	$\vdots$
$n-1$	$a(n-1) \bmod n$

- 由引理知，当 $\gcd(a, n) = 1$ 时，第二列的 n 个元素互不相等。
- 又这 n 个元素都取值于 $\mathbb{Z}_n$，因此它们构成的集合就是 $\mathbb{Z}_n$。
- 那么这个集合必然存在元素 1，记 $ax \bmod n = 1$，这个 x 就是 a 的乘法逆元。

目录

欧几里得算法（Euclidean Algorithm）



- 欧几里得算法是数论中的一个基本技巧，可以求两个正整数的最大公约数。
- 欧几里得算法的原理：对任意整数 a, b，且 $a \geq b > 0$，则 $\gcd(a, b) = \gcd(b, a \bmod b)$。
- 也就是说，求 a, b 的最大公约数可以转化为求 b 和 a 模 b 的最大公约数，即辗转相除法。

```
Euclid(a,b){
    if(b==0) then return a;
    else return Euclid(b, a mod b);
}
```

欧几里得算法的原理

- 假设要求整数 a 和 b 的最大公因子，不妨令 $a \geq b > 0$.
- b 除 a 可以表示为 $a = qb + r$，其中 $0 \leq r < b$ 为余数。
- 如果 $r = 0$，则 $\gcd(a, b) = b$；
- 如果 $r \neq 0$，考虑 $\gcd(a, b)$ 和 $\gcd(b, r)$ 之间的关系：
  - 令 $d = \gcd(a, b)$。因为 $d|a$ 且 $d|b$，所以 $d|(a - qb)$，即 $d|r$。也就是说，d 是 b, r 的公因子。那么，$d \leq \gcd(b, r)$.
  - 令 $c = \gcd(b, r)$。因为 $c|b$ 且 $c|r$，所以 $c|(qb + r)$，即 $c|a$。也就是说，c 是 a, b 的公因子。因为 a, b 的最大公因子是 d，所以 $c = \gcd(b, r) \leq d$.
- 所以 $\gcd(a, b) = \gcd(b, r)$，即求 a 和 b 的最大公因子可以转化为求 b 和 r 的最大公因子。

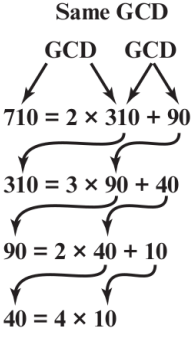
扩展欧几里得算法

- 给定两个整数 a 和 b，扩展欧几里得算法不仅可以求出最大公因子 d，而且可以得到两个整数 x 和 y，满足

$$ax + by = d = \gcd(a, b)$$

- 利用欧几里得算法，并且假设每步 i 都可得到 x_i 和 y_i 满足 $r_i = ax_i + by_i$。则有以下关系式：

$$\begin{aligned} a &= q_1 b + r_1 & r_1 &= ax_1 + by_1 \\ b &= q_2 r_1 + r_2 & r_2 &= ax_2 + by_2 \\ r_1 &= q_3 r_2 + r_3 & r_3 &= ax_3 + by_3 \\ &\vdots & &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n & r_n &= ax_n + by_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$



- 从而得到 $d = r_n = ax_n + by_n = ax + by$，即 $x = x_n, y = y_n$.

扩展欧几里得算法

$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
⋮	⋮	⋮	⋮
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_n \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

用扩展欧几里得算法求乘法逆元

- 如果 a 和 n 互素，那么 a 有模 n 的乘法逆元，即 a^{-1} 存在。
- 问题：如何确定 a 的乘法逆元 a^{-1}？
- 利用扩展欧几里得算法，存在整数 x 和 y，满足

$$ax + ny = \gcd(a, n) = 1$$

两边同时模 n，得到

$$(ax + ny) \bmod n = 1$$

进而得到

$$ax \bmod n = 1$$

所以 $a^{-1} = x$.

目录

有限域（Galois Fields）

- 有限域（也称伽罗瓦域）是包含有限个元素的域，用 $\mathrm{GF}(q)$ 或 $\mathbb{F}_q$ 表示包含 q 个元素的有限域。
- 有限域的阶（即元素个数）只能是素数 p 或素数的幂次 p^n。
- 包含 p 个元素的有限域称为素域，记为 $\mathrm{GF}(p)$。
- 包含 p^n 个元素的域称为扩域，记为 $\mathrm{GF}(p^n)$。
- 关注两种有限域：有限域 $\mathrm{GF}(p)$ 和有限域 $\mathrm{GF}(2^n)$。

有限域 $\mathrm{GF}(p)$

- 给定素数 p，有限域 $\mathrm{GF}(p)$ 的集合为 $\mathbb{Z}_p$，运算为模 p 算术运算。
- 由于 $\mathbb{Z}_p$ 中的所有非零整数都与 p 互素，因此 $\mathbb{Z}_p$ 中所有非零整数都有乘法逆元。
- 最简单的有限域是 $\mathrm{GF}(2)$，它的代数运算简述如下：

$+$	0	1
0	0	1
1	1	0

Addition

$\times$	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

有限域 $\mathrm{GF}(p)$ 的问题

- 所有加密算法都涉及整数集上的算术运算。
- 假如使用 8 比特来表示一个数，那么整数集为 $\mathbb{Z}_{256}$；
- 由于 256 不是一个素数，这个集合不是一个域；
- 小于 256 的最大素数为 251，所以可以在域 $\mathbb{Z}_{251}$ 上运算，但 $251 \sim 255$ 范围内的数就不能使用，造成存储空间浪费。
- 所以希望寻找一个包含 2^n 个元素的集合，其上定义了加法和乘法使之成为一个域，给集合的每个元素赋值为 0 到 $2^n - 1$ 之间的唯一整数。
- $\mathrm{GF}(2^n)$ 是一种含有 2^n 个元素的有限域。

有限域 $\mathrm{GF}(2^n)$ 的定义

- **集合**：所有次数小于 n 且系数为 0 或 1 的多项式，其中每个多项式有如下形式：

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

  其中 $a_i \in \{0, 1\}$。

- 多项式 $m(x)$ 是系数为 0 或 1 且次数为 n 的**不可约多项式**，也称为**素多项式**，扮演模数的角色。

- **加法**：多项式系数对应相加，按照 $\mathbb{Z}_2$ 上的模 2 加法，等价于异或。

- **乘法**：按照多项式乘法进行，如果运算结果的次数大于 $n-1$，需要除以不可约多项式 $m(x)$，得到的余式为乘法计算结果。

举例：有限域 $\mathrm{GF}(2^3)$

- 有限域 $\mathrm{GF}(2^3)$ 所在的集合包含 8 个多项式：
$$\{0, 1, x, x^2, x^2 + x, x + 1, x^2 + 1, x^2 + x + 1\}$$
- 需要选择次数为 3 的不可约多项式，仅有两个这样的多项式 $x^3 + x^2 + 1$ 和 $x^3 + x + 1$。
- 加法和乘法分别为多项式加法和多项式乘法，对应系数模 2。
- 考虑 $f(x) = x + 1, g(x) = x^2 + x + 1$，取不可约多项式 $m(x) = x^3 + x + 1$。
- $f(x) + g(x) = x^2$。
- $f(x)g(x) = x^3 + 1$，次数超过 3，需模不可约多项式。
- $f(x)g(x) \bmod m(x) = x$。

举例：有限域 $\mathrm{GF}(2^8)$

有限域 $\mathrm{GF}(2^8)$，$m(x) = x^8 + x^4 + x^3 + x + 1$，考虑两个多项式 $f(x) = x^6 + x^4 + x^2 + x + 1$ 和 $g(x) = x^7 + x + 1$。

$$
\begin{aligned}
f(x) + g(x) &= x^6 + x^4 + x^2 + x + 1 + x^7 + x + 1 \\
&= x^7 + x^6 + x^4 + x^2
\end{aligned}
$$

$$
\begin{aligned}
f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\
&\quad + x^7 + x^5 + x^3 + x^2 + x \\
&\quad + x^6 + x^4 + x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}
$$

$$
\begin{array}{r}
x^5 + x^3 \\
\hline
x^8 + x^4 + x^3 + x + 1 \;\big/\; x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
\underline{x^{13} + x^9 + x^8 + x^6 + x^5} \\
x^{11} + x^4 + x^3 \\
\underline{x^{11} + x^7 + x^6 + x^4 + x^3} \\
x^7 + x^6 + 1
\end{array}
$$

Therefore, $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$.

有限域 $\mathrm{GF}(2^n)$ 上乘法的另一种计算方式

- $\mathrm{GF}(2^n)$ 内的一个多项式可以由它的二元系数 $(a_{n-1} \cdots a_1 a_0)$ 唯一表示，因此 $\mathrm{GF}(2^n)$ 内的每个元素可以用 n 位数来表示。
- 加法等价于按位异或，乘法通过左移及按位异或计算。

- 考虑有限域 $\mathrm{GF}(2^8)$，使用不可约多项式 $m(x) = x^8 + x^4 + x^3 + x + 1$。
- 考虑两个元素 $A = (a_7 \ldots a_0)$ 和 $B = (b_7 \cdots b_0)$。
- 则 $A + B = (c_7 \cdots c_0)$ 其中 $c_i = a_i \oplus b_i$。
- 考虑乘法 $\{02\} \cdot A$，即用 x 乘 A 对应的多项式：
  - 当 $a_7 = 0$ 时，$\{02\} \cdot A = (a_6 \cdots a_0 0)$
  - 当 $a_7 = 1$ 时，$\{02\} \cdot A = (a_6 \cdots a_0 0) \oplus (00011011)$
- 这样可以通过反复运用上面的规则计算 $A \cdot B$。

举例：有限域 $\mathrm{GF}(2^8)$ 上的乘法

- 有限域 $\mathrm{GF}(2^8)$，$m(x) = x^8 + x^4 + x^3 + x + 1$，考虑两个多项式 $f(x) = x^6 + x^4 + x^2 + x + 1$ 和 $g(x) = x^7 + x + 1$。
- 计算 $f(x) \times g(x)$，即 $(01010111) \times (10000011)$：

Redoing this in binary arithmetic, we need to compute $(01010111) \times (10000011)$. First, we determine the results of multiplication by powers of x:

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

So,

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

which is equivalent to $x^7 + x^6 + 1$.

$\mathrm{GF}(2^3)$ 中的运算，$m(x) = x^3 + x + 1$

+	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+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

×	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	$x+1$

使用生成元定义 $GF(2^n)$

- 阶为 q 的有限域 $\mathbb{F}$ 的生成元是域的一个元素，记为 g，该元素的前 $q-1$ 个幂构成了 $\mathbb{F}$ 的所有非零元素，即域 $\mathbb{F}$ 的元素为 $\{0, g^0, g^1, \ldots, g^{q-2}\}$。
- 考虑由多项式 $m(x)$ 定义的域 $\mathbb{F}$，如果 $\mathbb{F}$ 内的一个元素 b 满足 $m(b) = 0$，则称 b 为多项式 $m(x)$ 的根。
- 可以证明一个不可约多项式的根 g 是这个不可约多项式定义的有限域的生成元。
- 通常，由不可约多项式 $m(x)$ 生成的域 $\mathrm{GF}(2^n)$，有 $g^n = m(g) - g^n$。计算 g^{n+1} 到 g^{2^n-2}。域的元素对应 g^0 到 g^{2^n-2}，外加 0。域元素的乘法用等式 $g^k = g^{k \bmod (2^n-1)}$ 计算。

由 $m(x) = x^3 + x + 1$ 生成的域 $\mathrm{GF}(2^3)$

- $m(g) = 0 \Rightarrow g^3 + g + 1 = 0$，所以 $g^3 = g + 1$。
- $g^4 = g \cdot g^3 = g^2 + g$。
- $g^5 = g \cdot g^4 = g^3 + g^2 = g^2 + g + 1$。
- $g^6 = g \cdot g^5 = g^3 + g^2 + g = g^2 + 1$。
- $g^7 = g^3 + g = 1 = g^0$，开始循环，一般地 $g^k = g^{k \bmod (2^n - 1)}$。

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

使用生成元的 $\mathrm{GF}(2^3)$ 算术

	+	000	001	010	100	011	110	111	101
		0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
001	1	1	0	$g+1$	g^2+1	g	g^2+g+1	g^2+g	g^2
010	g	g	$g+1$	0	g^2+g	1	g^2	g^2+1	g^2+g+1
100	g^2	g^2	g^2+1	g^2+g	0	g^2+g+1	g	$g+1$	1
011	g^3	$g+1$	g	1	g^2+g+1	0	g^2+1	g^2	g^2+g
110	g^4	g^2+g	g^2+g+1	g^2	g	g^2+1	0	1	$g+1$
111	g^5	g^2+g+1	g^2+g	g^2+1	$g+1$	g^2	1	0	g
101	g^6	g^2+1	g^2	g^2+g+1	1	g^2+g	$g+1$	g	0

	×	000	001	010	100	011	110	111	101
		0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1
010	g	0	g	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1
100	g^2	0	g^2	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g
011	g^3	0	$g+1$	g^2+g	g^2+g+1	g^2+1	1	g	g^2
110	g^4	0	g^2+g	g^2+g+1	g^2+1	1	g	g^2	$g+1$
111	g^5	0	g^2+g+1	g^2+1	1	g	g^2	$g+1$	g^2+g
101	g^6	0	g^2+1	1	g	g^2	$g+1$	g^2+g	g^2+g+1

多项式欧几里得算法

- 类似于计算两个整数最大公因子的欧几里得算法
  $\gcd(a, b) = \gcd(b, a \bmod b)$
- 计算两个多项式 $a(x)$ 和 $b(x)$ 最大公因式的欧几里得算法为
  $\gcd(a(x), b(x)) = \gcd(b(x), a(x) \bmod b(x))$

Euclidean Algorithm for Polynomials	
Calculate	**Which satisfies**
$r_1(x) = a(x) \bmod b(x)$	$a(x) = q_1(x)b(x) + r_1(x)$
$r_2(x) = b(x) \bmod r_1(x)$	$b(x) = q_2(x)r_1(x) + r_2(x)$
$r_3(x) = r_1(x) \bmod r_2(x)$	$r_1(x) = q_3(x)r_2(x) + r_3(x)$
$\bullet$ $\bullet$ $\bullet$	$\bullet$ $\bullet$ $\bullet$
$r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$	$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x)$
$r_{n+1}(x) = r_{n-1}(x) \bmod r_n(x) = 0$	$r_{n-1}(x) = q_{n+1}(x)r_n(x) + 0$ $d(x) = \gcd(a(x), b(x)) = r_n(x)$

多项式欧几里得算法

- $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $b(x) = x^4 + x^2 + x + 1$, **计算** $\gcd(a(x), b(x))$.
- **首先用** $a(x)$ **除以** $b(x)$, **得余式** $r_1(x) = x^3 + x^2 + 1$

$$
\begin{array}{r}
x^2 + x \\
x^4 + x^2 + x + 1 \overline{)\, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\underline{x^6 \quad + x^4 + x^3 + x^2} \\
x^5 \quad + x + 1 \\
\underline{x^5 \quad + x^3 + x^2 + x} \\
x^3 + x^2 \quad + 1
\end{array}
$$

- **再用** $b(x)$ **除以** $r_1(x)$, **整除**, **所以** $\gcd(a(x), b(x)) = r_1(x)$.

$$
\begin{array}{r}
x + 1 \\
x^3 + x^2 + 1 \overline{)\, x^4 \quad + x^2 + x + 1} \\
\underline{x^4 + x^3 \quad + x} \\
x^3 + x^2 \quad + 1 \\
\underline{x^3 + x^2 \quad + 1}
\end{array}
$$

多项式扩展欧几里得算法

- 类似的，扩展欧几里得算法在计算两个多项式 $a(x)$ 和 $b(x)$ 最大公因式的同时能够得到两个多项式 $v(x)$ 和 $w(x)$，满足

$$a(x)v(x) + b(x)w(x) = \gcd(a(x), b(x))$$

- 当 $\gcd(a(x), b(x)) = 1$ 时，存在 $a(x) \bmod b(x)$ 或 $b(x) \bmod a(x)$ 的乘法逆元，即为：

$$a(x)^{-1} \bmod b(x) = v(x)$$

或

$$b(x)^{-1} \bmod a(x) = w(x)$$

多项式扩展欧几里得算法

例

- 已知 $a(x) = x^8 + x^4 + x^3 + x + 1$, $b(x) = x^7 + x + 1$，计算 $b(x)^{-1} \bmod a(x) = ?$

Initialization	$a(x) = x^8 + x^4 + x^3 + x + 1; v_{-1}(x) = 1; w_{-1}(x) = 0$ $b(x) = x^7 + x + 1; v_0(x) = 0; w_0(x) = 1$
Iteration 1	$q_1(x) = x; r_1(x) = x^4 + x^3 + x^2 + 1$ $v_1(x) = 1; w_1(x) = x$
Iteration 2	$q_2(x) = x^3 + x^2 + 1; r_2(x) = x$ $v_2(x) = x^3 + x^2 + 1; w_2(x) = x^4 + x^3 + x + 1$
Iteration 3	$q_3(x) = x^3 + x^2 + x; r_3(x) = 1$ $v_3(x) = x^6 + x^2 + x + 1; w_3(x) = x^7$
Iteration 4	$q_4(x) = x; r_4(x) = 0$ $v_4(x) = x^7 + x + 1; w_4(x) = x^8 + x^4 + x^3 + x + 1$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

小结

1. 群、环和域
2. 模算术
3. 欧几里得算法
4. 有限域