现代密码学理论与实践

第4章 有限域

本章要点

- 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。

4.1群, 环和域Groups, Rings, and Fields

- 群G, 记作{G, •}, 定义一个二元运算•的集合，G中每一个序偶(a, b)通过运算生成G中元素(a•b)，满足下列公理：
  - (A1) 封闭性Closure: 如果a和b都属于G, 则a•b也属于G.
  - (A2) 结合律Associative: 对于G中任意元素a, b, c，都有a•(b•c)=(a•b)•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•e=e•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•a’=a’•a=e成立

群、有限群和无限群

- 用N_n表示n个不同符号的集合，{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$\pi \bullet \rho$根据置换π来改变ρ中元素的次序而形成，如，{3,2,1}•{1,3,2}={2,3,1},显然$\pi \bullet \rho \in S_n$
  - 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}•{3,1,2}={1,2,3},
- 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，且群的阶等于群中元素的个数；否则称为无限群

交换群和循环群

- 交换群Abelian Group：还满足以下条件的群称为交换群(又称阿贝尔群)
  - (A5) 交换律Commutative：对于G中任意的元素a, b，都有a•b=b•a成立
- 当群中的运算符是加法时，其单位元是0；a的逆元是-a, 并且减法用以下的规则定义：

$$a - b = a + (-b)$$

- 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 ∈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)

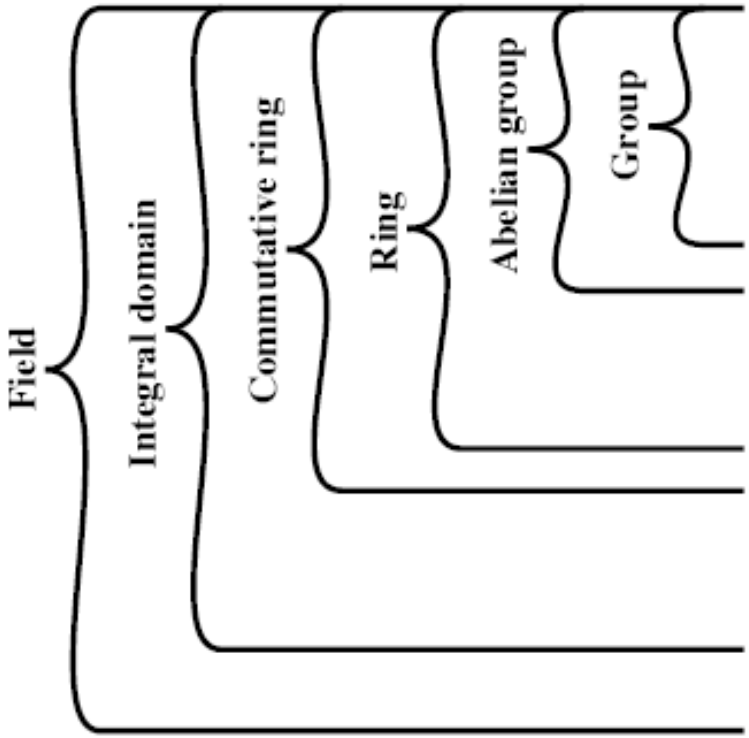
- 环R, 由{R, +, x}表示, 是具有加法和乘法两个二元运算的元素的集合，对于环中的所有a, b, c, 都服从以下公理：
  - (A1-A5), 单位元是0，a的逆是 -a.
  - (M1), 乘法封闭性, 如果a和b属于R, 则ab也属于R
  - (M2), 乘法结合律,对于R中任意a, b, c有a(bc)=(ab)c.
  - (M3), 乘法分配律, a(b+c)=ab+ac or (a+b)c=ac+bc
  - (M4), 乘法交换律, ab=ba，交换环
  - (M5), 乘法单位元, R中存在元素1使得所有a有 a1=1a.
  - (M6), 无零因子, 如果R中有a, b且ab=0, 则 a=0 or b=0.

  满足M4的是交换环；满足M5和M6的交换环是整环

域 (Fields)

- 域F, 可以记为{F, +, x}, 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$aa^{-1}=(a^{-1})a=1$.
  - 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: $a/b=a(b^{-1})$.
- 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 $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 4.1 Group, Ring, and Field

4.2 Modular Arithmetic

- 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 0≤r＜n；q=⌊a/n⌋⌊x⌋表示小于等于x的最大整数

  Eg: 11=1x7 + 4, r=4; -11=(-2)x7 + 3, r=3

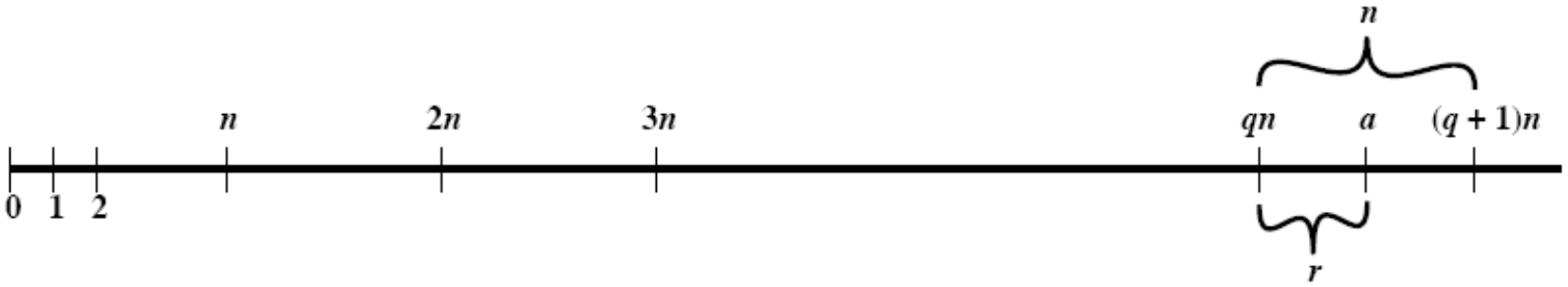


Figure 4.2 The Relationship $a = qn + r;\ 0 \le r < n$

因子 Divisors

- 如果a=mb, 其中a, b, m为整数，则当b≠0时，即b能整除a, 或a除以b余数为0, b|a. b是a的一个因子。24的正因子有1, 2, 3, 4, 6, 8, 12和24。
- 以下关系成立
  - 如果a|1, 则a=±1
  - 如果a|b，且b|a, 则a=±b
  - 任何b≠0能整除0
  - 如果b|g，且b|h, 则对任何整数m和n有b|(mg+nh)
- Eg: b=7, g=14, h=63, m=3, n=2, 7|14 and 7|63
  求证：7|(3x14 + 2x63)
  证明：(3x14 + 2x63)=7(3x2 + 2x9)
  显然, 7|(7(3x2 + 2x9))
- 如果a ≡ 0 mod n，则n|a

同余 (congruence)

- 给定整数a, b及n≠0, 当且仅当a-b=kn时，a与b 在模n时同余，记为 $a \equiv b \bmod n$ 或 $a \equiv_n b$

  Ex: $17 \equiv_5 7$ ∵17-7=2*5;

  $53 \equiv_7 11$ ∵53-11=6*7

  $a \equiv_n b$ 当且仅当 a mod n = b mod n
- 如果a是整数，n是正整数，定义a除以n所得之余数为a模n。对于任意整数a，我们总可写出： $a = \lfloor a/n \rfloor \times n + (a \bmod n)$
  - 11 mod 7 = 4; -11 mod 7 = 3
- 如果(a mod n)=(b mod n), 则称整数a和b是模n同余，表示为$a \equiv b \bmod n$ 或 $a \equiv_n b$
  - $73 \equiv 4 \bmod 23$； $21 \equiv -9 \bmod 10$

同余的性质

- 如果n|(a-b), 则a≡b mod n
  证明: 如果n|(a-b), 则有(a-b)=kn, k为某些整数，
  所以a=b+kn。
  故a mod n = (b + kn)除以n的余数
  = b 除以n的余数
  = b mod n
- a≡b mod n 隐含b≡a mod n
- a≡b mod n 和b≡c mod n 隐含a≡c mod n
  Ex: 23≡8(mod 5)，因为23-8=15=5x3
  -11≡5(mod 8)，因为-11-5=-16=8x(-2)
  81≡0(mod 27)，因为81-0=81=27x3

模算术运算

$(a_1 \text{ op } a_2) \bmod n = [(a_1 \bmod n) \text{ op } (a_2 \bmod n)] \bmod n$

①反身性：$a = a \bmod n$

②对称性：若$a = b \bmod n$，则$b = a \bmod n$

③传递性: 若$a = b \bmod n$ 且$b = c \bmod n$，则$a = c \bmod n$

④如果 $a = b \bmod n$且 $c = d \bmod n$，则

$a+c = (b+d) \bmod n$

$a-c = (b-d) \bmod n$

$a \cdot c = (b \cdot d) \bmod n$

⑤ $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$(a-b) \bmod n = (a \bmod n - b \bmod n) \bmod n$

$(a \cdot b) \bmod n = (a \bmod n \cdot b \bmod n) \bmod n$

⑥如果$ac = bd \bmod n$ 且 $c = d \bmod n$, $\gcd(c,n)=1$,

则 $a = b \bmod n$　证明：留给学生

例： $3*2 = 1*2 \bmod 4$ 且 $2 = 2 \bmod 4$， 但$3 \neq 1 \bmod 4$，

∵ $\gcd(2,4) \neq 1$

Table 4.1 Arithmetic Modulo 8

+	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

(a) Addition modulo 8

×	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

(b) Multiplication modulo 8

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

(c) Additive and multiplicative inverses modulo 8

加法逆元和乘法逆元

- 加法逆元(-w)
  - 对每一个$w \in Z_n$，存在一个z，使得
    $w+z \equiv 0 \bmod n$，则z即为加法逆元-w
- 乘法逆元(w^{-1})
  - 对每一个$w \in Z_p$，存在一个z，使得$wxz \equiv 1 \bmod p$，
    p为素数， w与p互素，则z即为乘法逆元w^{-1}
  - 因为w与p互素，如果用w乘以Z_p中的所有数模p，得到的余数将以不同次序涵盖Z_p中的所有数，那么至少有一个余数的值为1。因此，在Z_p中的某个数与w相乘模p的余数为1, 这个数就是w的乘法逆元, w^{-1}
  - 某些但非全部整数存在一个乘法逆元就将使模数不再是素数。如果gcd(a, n)=1, 则能在Z_n中找到b，使得
    $axb \equiv 1 \bmod n$，则b即为乘法逆元a^{-1}, 因为a与n互素。

模算术的性质

- 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)}

b是a mod n 的剩余，如果 a=b mod n 或

a是b mod n的剩余，如果 b=a mod n

(1)模n的完全剩余集 Complete Set of Residues mod n

如果对每个整数a，在集合{r_1,r_2,…,r_n}中恰有一个余数r_i,使得 a=r_i mod n ,则称{r_1,r_2,…,r_n}为模n的完全剩余集，{0,1,…,n-1}形成模n 的完全剩余集。

与同余不同之处：a≡$_n$b,当且仅当 a mod n=b mod n

a≡$_n$r，即a=r mod n, 不是说 a mod n = r

比如 20≡$_3$14，得20=14 mod 3, r=2，但20 mod 3 ≠14，而是20 mod 3=14 mod 3

模算术的性质

(2)模n的缩剩余集(Reduced set of Residues mod n)

完全剩余集的一个子集，指的是集合中的元素都和n互素

例:n=10，模n的完全剩余集是{0, 1, 2,…,9}，缩剩余集是 {1, 3, 7, 9}

Table 4.2 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive laws	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

4.3 欧几里得算法Euclid Algorithm

- 数论的一个最基本的技巧是Euclid算法，求两个正整数的最大公约数 gcd(a, n), greatest common divisor
  对于任何非负的整数a和n，gcd(a, n)=gcd(n mod a, a)
  原理是计算$g_{i+1}=g_{i-1}$ mod g_i 直到 $g_i=0$为止。

Algorithm gcd(a, n)
begin
    g_0:=n, g_1:=a, i:=1
    while $g_i \neq 0$ do
        begin
            $g_{i+1}=g_{i-1}$ mod g_i
            i:=i+1
        end n
    gcd:= g_{i-1}
end

例如：gcd(22, 55)=gcd(55 mod 22, 22)=gcd(11, 22)=11

Euclid's GCD Algorithm

- **Euclid's Algorithm** to compute GCD(a,b):
  1. A ← a, B ← b
  2. 若 B=0，则返回 A=gcd(a, b)
  3. R = A mod B
  4. A ← B, B ← R
  5. 转到2
  6. Int gcd(int x,int y){
     Return (!y) ? x: gcd(y,x%y);
     }
- 如果a和b只有唯一的正公因子1，则称整数a和b是互素的，即gcd(a, b)=1

Example: 求gcd(1970, 1066)

1970 = 1 x 1066 + 904	gcd(1066, 904)
1066 = 1 x 904 + 162	gcd(904, 162)
904 = 5 x 162 + 94	gcd(162, 94)
162 = 1 x 94 + 68	gcd(94, 68)
94 = 1 x 68 + 26	gcd(68, 26)
68 = 2 x 26 + 16	gcd(26, 16)
26 = 1 x 16 + 10	gcd(16, 10)
16 = 1 x 10 + 6	gcd(10, 6)
10 = 1 x 6 + 4	gcd(6, 4)
6 = 1 x 4 + 2	gcd(4, 2)
4 = 2 x 2 + 0	gcd(2, 0)

Gcd(1970,1066)=2

4.4 有限域GF(p) Galois Fields

- 有限域在密码学中扮演重要角色
- 有限域的阶(元素个数)必须是一个素数的幂p^n, n 为正整数。元素个数是p^n的有限域一般记为GF(p^n)，即Galois fields, 模p^n.
- 关注两种特殊情形，n=1时的有限域和p为2时的有限域，即GF(p)和GF(2^n)
- 最简单的有限域是GF(2)，它的代数运算简述如下：

+	0	1
0	0	1
1	1	0

加

x	0	1
0	0	0
1	0	1

乘

w	-w	w^{-1}
0	0	
1	1	1

求逆

Galois Fields GF(p)

- 阶为p的有限域GF(p)
  - 给定一个素数p，元素个数为p的有限域GF(p)被定义为整数{0,1, … , p-1}的集合Z_p，其运算为模p的算术运算
  - Z_n中的任一整数有乘法逆元当且仅当该整数与n互素，若n为素数， Z_n中的所有非零整数都与n互素，因此Z_n中所有非零整数都有乘法逆元
  - 对每一个$w \in Z_p$，存在一个z，使得$w \times z \equiv 1 \bmod p$，则z即为乘法逆元$w^{-1}$
  - 因为w与p互素，如果用w乘以Z_p中的所有数模p，得到的余数将以不同次序涵盖Z_p中的所有数，即余数集合是{0,1, … , p-1}的置换形，那么至少有一个余数的值为1。因此，在Z_p中的某个数与w相乘模p的余数为1, 这个数就是w的乘法逆元，w^{-1}。 所以，Z_p是一个有限域。

Table 4.3 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	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

(b) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 7

在GF(p)中求乘法逆元

- 如果gcd(m, b)=1，那么b有模m的乘法逆元，欧几里得算法可被扩展如下：求出gcd(m, b)后，当gcd为1时，算法返回b的乘法逆元

EXTENDED EUCLID(*m*, *b*)

1.(A1, A2, A3)=(1, 0, *m*);
(B1, B2, B3)=(0, 1, *b*)
2. if B3 = 0
return A3 = gcd(*m*, *b*); no inverse
3. if B3 = 1
return B3 = gcd(*m*, *b*); B2 = b^{-1} mod *m*
4. Q = A3 div B3
5. (T1, T2, T3)=(A1−QB1, A2−QB2, A3−QB3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2

在域GF(1759)中求550的乘法逆元

Table 4.4 Finding the Multiplicative Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	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

计算乘法逆元素$ax \bmod n = 1$, $x=a^{-1}=?$

- 计算乘法逆元素 Computing multiplicative inverses

  给定$a \in [0, n-1]$, $\gcd(a, n)=1$，若能找到唯一整数$x \in [0,n-1]$，满足：$ax \bmod n=1$, 则称a和x互逆

  如 $n=10$, $a=3$, $x=7$, $ax \bmod n=1 = 3x7 \bmod 10$

  $n=17$, $a=5$, $x=7$, $ax \bmod n=1 = 5x7 \bmod 17$

  引理4.1: 如果$\gcd(a, n)=1$, 则对于每个i, j, $0 \le i < j < n$,

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

  证明：(略) 可以用反证法证明

  此性质意味着每一个$ai \bmod n$ $(i=0,\ldots,n-1)$都是不同的模n剩余，而$\{ ai \bmod n \}_{i=0,1,\ldots,n-1}$是完全剩余集$\{0,1,\ldots,n-1\}$的置换形式

计算乘法逆元素

例如: n=5, a=3, gcd(3,5)=1, {0,1,…,n-1}={0,1,2,3,4}

3*0 mod 5=0

3*1 mod 5=3

3*2 mod 5=1

3*3 mod 5=4

3*4 mod 5=2

$\{ai \bmod n\}_{i=0,1,\ldots,n-1}=\{0,3,1,4,2\}$

引理4.1说明, 当gcd(a, n)=1时, a一定有一个唯一的逆元素。

定理4.1 如果gcd(a, n)=1, 一定存在整数x, 0<x<n,

满足ax mod n=1

可以用Euclid’s计算最大公约数算法的扩展来求逆。

用扩展的Euclid算法求逆

Algorithm inv(a, n)
begin
    g_0:=n; g_1:=a; u_0:=1; v_0:=0; u_1:=0; v_1:=1; i:=1
    while $g_i \neq 0$ do "$g_i = u_i n + v_i a$"
        begin
            y:=g_{i-1} div g_i;
            g_{i+1}:= g_{i-1} –y*g_i;
            u_{i+1}:= u_{i-1} –y*u_i;
            v_{i+1}:= v_{i-1} –y*v_i;
            i:=i+1
        end
    x:= v_{i-1}
    if x>=0, then inv:= x, else inv:= x+n
end

$g_i = u_i n + v_i a$ 是循环变量，当g_i=0时 g_{i-1}=gcd(a, n)。如果gcd(a, n)=1, 则g_{i-1}=1，并且 $v_{i-1}a - 1 = u_{i-1}n$ 。

因此，$v_{i-1}a \bmod n = 1$, v_{i-1} ＝x，就是a的逆元素。

扩展的Euclid算法求逆

例：3x mod 7=1，　　g_0:=n; g_1:=a; u_0:=1; v_0:=0; u_1:=0; v_1:=1

i	g_i	u_i	v_i	y
0	7	1	0	
1	3	0	1	2
2	1	1	-2	3
3	0			

$y:=g_{i-1}$ div g_i;　$g_{i+1}:= g_{i-1}–y*g_i$

$u_{i+1}:= u_{i-1}–y*u_i$; $v_{i+1}:= v_{i-1}–y*v_i$

因此得到v_{i-1} = -2，x = -2 + 7 = 5。

例：5x mod 49=1，x=10

i	g_i	u_i	v_i	y
0	49	1	0	
1	5	0	1	9
2	4	1	-9	1
3	1	-1	10	4
4	0			

因此得到v_{i-1} =10=x 。

4.5 多项式运算

- 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GF(p)中
  - 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
- 普通多项式运算
  - 一个n次多项式(n>=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_n=0，f(x)是定义在系数集S上的多项式
  - 零次多项式称为常数多项式，是系数集里的一个元素，如果a_n=1，对应的n次多项式就称为首1多项式

普通多项式运算

- 加或减就是相应系数的加减，乘则要用到所有系数
- 例如

let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 – x + 1$

$f(x) + g(x) = x^3 + 2x^2 – x + 3$

$f(x) – g(x) = x^3 + x + 1$

$f(x)$ x $g(x) = x^5 + 3x^2 – 2x + 2$

$f(x) / g(x) = x + 2$, ……x

$$
\begin{array}{l}
x^3 + x^2 \quad + 2 \\
+ \quad (x^2 - x + 1) \\
\hline
x^3 + 2x^2 - x + 3
\end{array}
$$

(a) Addition

$$
\begin{array}{l}
x^3 + x^2 \quad + 2 \\
- \quad (x^2 - x + 1) \\
\hline
x^3 \quad + x + 1
\end{array}
$$

(b) Subtraction

$$
\begin{array}{l}
x^3 + x^2 \quad + 2 \\
\times \quad (x^2 - x + 1) \\
\hline
x^3 + x^2 \quad + 2 \\
- x^4 - x^3 \quad - 2x \\
x^5 + x^4 \quad + 2x^2 \\
\hline
x^5 \quad + 3x^2 - 2x + 2
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|l}
 & x + 2 \\
\cline{2-2}
x^2 - x + 1 & x^3 + x^2 \quad + 2 \\
 & x^3 - x^2 + x \\
\cline{2-2}
 & 2x^2 - x + 2 \\
 & 2x^2 - 2x + 2 \\
\cline{2-2}
 & x
\end{array}
$$

(d) Division

Figure 4.3 Examples of Polynomial Arithmetic

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
- 可以模任何素数p，但是我们更感兴趣的是模2的运算
  - 也就是说所有的系数不是0就是1
  - 比如，令 $f(x) = x^3 + x^2$ ， $g(x) = x^2 + x + 1$

    则 $f(x) + g(x) = x^3 + x + 1$

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

$$
\begin{array}{llll}
x^7 & +x^5+x^4+x^3 & +x+1 & \\
 & +(x^3 & +x+1) & \\
\hline
x^7 & +x^5+x^4 & &
\end{array}
$$

(a) Addition

$$
\begin{array}{llll}
x^7 & +x^5+x^4+x^3 & +x+1 & \\
 & -(x^3 & +x+1) & \\
\hline
x^7 & +x^5+x^4 & &
\end{array}
$$

(b) Subtraction

$$
\begin{array}{llll}
 & x^7 & +x^5+x^4+x^3 & +x+1 \\
 & & \times (x^3 & +x+1) \\
\hline
 & x^7 & +x^5+x^4+x^3 & +x+1 \\
 & x^8 & +x^6+x^5+x^4 & +x^2+x \\
x^{10} & +x^8+x^7+x^6 & +x^4+x^3 & \\
\hline
x^{10} & & +x^4 & +x^2+1
\end{array}
$$

(c) Multiplication

$$
\begin{array}{r|l}
 & x^4+1 \\
\cline{2-2}
x^3+x+1 & x^7+x^5+x^4+x^3+x+1 \\
 & x^7+x^5+x^4 \\
\cline{2-2}
 & x^3+x+1 \\
 & x^3+x+1 \\
\cline{2-2}
\end{array}
$$

(d) Division

Figure 4.4 Examples of Polynomial Arithmetic over GF(2)

多项式的模运算

- 多项式可以写成如下形式:
  - $f(x) = q(x)\ g(x) + r(x)$
  - 其中，$r(x)$就可被看作是余数
  - $r(x) = f(x) \bmod g(x)$
- 如果没有余数，就称g(x)可以整除f(x)
- 如果g(x)除了1和它自身以外没有其他公因式，就称它是不可约多项式或素多项式irreducible or prime
- 算术模运算模一个不可再分的多项式，结果形成一个域

求多项式的最大公因式

- 可以为多项式求解最大公因式
  - 如果$c(x)$是可以整除$a(x)$和$b(x)$最大公因式，则$c(x) = \text{GCD}(a(x), b(x))$
  - 可以用Euclid's Algorithm 求解多项式最大公因式:

EUCLID[$a(x)$, $b(x)$]

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

4.6 有限域GF(2^n)

- 所有加密算法都涉及到整数集上的算术运算，如果用到除法，必须使用定义在域上的运算。
- 整数集里的数与给定的二进制位数所能表达的信息一一对应，即整数集的范围从0到2^n-1，正好对应一个n位的字。
- 将一个整数集不平均地映射到自身的算法用于加密时可能要弱于一个提供一一映射的算法，因此，有限域GF(2^n)对加密算法是很有吸引力的。所以要寻找一个包含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，用多项式算术来构造所需的域。
- 可以使用扩展的欧几里德算法来为集合中的元素找到逆元。

Table 4.5 Arithmetic in GF(2^3)

	+	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

	×	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

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

(c) Additive and multiplicative inverses

多项式模运算

- 设集合S由域Z_p上次数小于等于n-1的所有多项式组成，每个多项式具有如下形式：

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

  - 其中，a_i在集合{0,1,…,p-1}上取值，S共有p^n个不同的多项式
  - 当p=3, n=2时，集合中共有3^2=9个多项式，分别是

    0　　x　　2x

    1　　x+1　　2x+1

    2　　x+2　　2x+2
  - 当p=2, n=3时，集合中共有2^3=8个多项式，分别是

    0　　x+1　　x^2+x

    1　　x^2　　x^2+x+1

    x　　x^2+1

多项式模运算

- 如果定义了合适的运算，那么每个这样的集合S都是一个有限域，定义由如下几条组成：
  - 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)
- 和简单模运算类似，多项式模运算也有剩余类集合的概念。设m(x)为n次多项式，则模m(x)剩余类集合有p^n个元素，每个元素都可以表示成一个p^n次多项式(m<n)
- 以n次既约多项式m(x)为模的所有多项式组成的集合满足图4.1的所有公理，于是可以形成一个有限域。
- 为构造有限域$GF(2^3)$,需要选择一个3次既约多项式：x^3+x^2+1和x^3+x+1，选择后者则结果如表4.6所示。

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

求乘法逆元

- 扩展的欧几里德算法可以用来求一个多项式的乘法逆元。如果多项式b(x)的次数小于m(x)且gcd[m(x),b(x)]=1，那么可以求出b(x)以m(x)为模的乘法逆元。

  扩展的EUCLID[$m(x)$, $b(x)$]

  1. [A1(x), A2(x), A3(x)] ←[1,0,$m(x)$]; [B1(x), B2(x), B3(x)] ←[1,0,$b(x)$]
  2. **if** B3(x) = 0 **return** A3(x) = gcd[$m(x)$, $b(x)$]; no inverse
  3. **if** B3(x) = 1 **return** B3(x) = gcd[$m(x)$, $b(x)$]; B2(x)=$b(x)^{-1}$ mod m(x)
  4. Q(x) = quotient of A3(x)/B3(x)
  5. [T1(x), T2(x), T3(x)] ←[A1(x), A2(x)-Q(x)B1(x), A2(x)-Q(x)B2(x), A3(x)-Q(x)B3(x)]
  6. [A1(x), A2(x), A3(x)] ←[B1(x), B2(x), B3(x)]
  7. [B1(x), B2(x), B3(x)] ←[T1(x), T2(x), T3(x)]
  8. **goto** 2

Extended Euclid

Table 4.7 Extended Euclid $[(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)]$

Initialization	$A1(x) = 1; A2(x) = 0; A3(x) = x^8 + x^4 + x^3 + x + 1$ $B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$
Iteration 1	$Q(x) = x$ $A1(x) = 0; A2(x) = 1; A3(x) = x^7 + x + 1$ $B1(x) = 1; B2(x) = x; B3(x) = x^4 + x^3 + x^2 + 1$
Iteration 2	$Q(x) = x^3 + x^2 + 1$ $A1(x) = 1; A2(x) = x; A3(x) = x^4 + x^3 + x^2 + 1$ $B1(x) = x^3 + x^2 + 1; B2(x) = x^4 + x^3 + x + 1; B3(x) = x$
Iteration 3	$Q(x) = x^3 + x^2 + x$ $A1(x) = x^3 + x^2 + 1; A2(x) = x^4 + x^3 + x + 1; A3(x) = x$ $B1(x) = x^6 + x^2 + x + 1; B2(x) = x^7; B3(x) = 1$
Iteration 4	$B3(x) = \gcd[(x^7 + x + 1), (x^8 + x^4 + x^3 + x + 1)] = 1$ $B2(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

计算上的考虑

- 因为系数不是0就是1, 因此GF(2^n)中的每个多项式都可以表示成一个n位的二进制整数
- 加法其实就是异或运算XOR, 两个多项式加法等同于按位异或运算
- 乘法通过左移一位后按位异或来实现
- 模运算也是通过左移和异或来实现

在伽罗瓦域中的计算

Computing in Galois Fields 在伽罗瓦域中的计算

（1）伽罗瓦域 GF(p)

当模数是素数p，每个整数a∈[1,p-1]与p互素，因而都有唯一的模p的逆。这一组模p的整数，加上算术运算，被称为有限域－伽罗瓦域Galois Fields。

（2）伽罗瓦域 GF(2^n)

多项式系数是二进制0和1，一个元素a可被表示成一个位矢量，长度为n, (a_{n-1},…a_1,a_0)，每一个长度为n的可能的2^n位的矢量都对应着GF(2^n)中的不同元素。例如二进制数11001在GF(2^5)中可以记作x^4+x^3+1。

Computing in Galois Fields

- 在GF(2^n)中的运算(模2运算是基础)

  加、减运算是异或，加无进位，减无借位，乘法运算是“与”，除法运算只要位数够长即可进行。

例：计算d=a^2，p(x) =x^3＋x＋1，在GF(2^3)中，a=101

a×a=101×101=10001

模p(x)：a^2/p(x) =10001/1011=111, 即d。

例：a=111, b=100, p(x) =1011, 计算d=a×b, in GF(2^3).

a×b=111×100=11100

a×b模p(x)：11100/1011=001

即111×100 mod 1011=001,在模1011时a与b互逆。

- 在GF(2^n)中求逆，$f(x)^{-1}=f(x)^{2^n-2}$ mod p(x)

使用生成元

- 定义有限域的另一种等价方式有时更方便，它使用相同的不可约多项式。
- 阶为q的有限域F的生成元是一个元素，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$0,g^0,g^1,\ldots,g^{q-2}$.
- 考虑由多项式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。

使用生成元

Table 4.8 Generator for GF(2^3) using $x^3 + x + 1$

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

Table 4.9 GF(2^3) Arithmetic Using Generator for the Polynomial ($x^3 + x + 1$)

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

(a) Addition

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

(b) Multiplication

Summary

- We have considered:
  - concept of groups, rings, fields
  - modular arithmetic with integers
  - Euclid's algorithm for GCD
  - finite fields GF(p)
  - polynomial arithmetic in general and in GF(2^n)

谢 谢！