4.1 密码学中的一些常用数学知识

4.1.1 群、环、域

群、环、域都是**代数系统**（也称代数结构）

代数系统是对要研究的现象或过程建立起的一种数学模型，模型中包括要处理的数学对象的集合以及集合上的关系或运算，运算可以是一元的也可以是多元的，可以有一个也可以有多个。

设 $*$是集合 S 上的运算，若对 $\forall a,b \in S$，有 $a*b \in S$，则称 S 对运算 $*$ 是封闭的。若是一元运算，对 $\forall a \in S$，有 $*a \in S$，则称 S 对运算 $*$ 是**封闭**的。

若对 $\forall a,b,c \in S$，有 $(a*b)*c=a*(b*c)$，则称**满足结合律**。

定义4-1　设$\langle G,*\rangle$是一个代数系统，$*$ 满足：

（1）封闭性。

（2）结合律。

则称$\langle G,*\rangle$ 是半群。

定义4-2　设$\langle G,*\rangle$是一个代数系统，$*$ 满足：

（1）封闭性。

（2）结合律。

（3）存在元素 e，对 $\forall a\in G$，有 $a*e=e*a=a$ 称 e 为$\langle G,*\rangle$的单位元。

（4）对 $\forall a\in G$，存在元素 a^{-1}，使得 $a*a^{-1}=a^{-1}*a=e$；称 a^{-1}为元素 a 的逆元。则称$\langle G,*\rangle$ 是群。若其中的运算$*$ 已明确，有时将$\langle G,*\rangle$ 简记为G 。

如果G是有限集合，则称$\langle G,*\rangle$是**有限群**，否则是无限群。

有限群中，G的元素个数称为**群的阶数**。

如果群$\langle G,*\rangle$中的运算$*$还满足交换律，即对$\forall a,b\in G$，有$a*b=b*a$，则称$\langle G,*\rangle$为**交换群**或**Abel群**。

群中运算$*$一般称为乘法，称该群为**乘法群**。若运算$*$改为$+$，则称为**加法群**，此时逆元a^{-1}写成$-a$。

【例4-1】

1. $\langle I,+\rangle$是Abel群，其中 I 是整数集合。

2. $\langle Q,\cdot\rangle$是Abel群，其中 Q 是有理数集合。

3. 设 A是任一集合，P表示 A 上的双射函数集合，$\langle P,\circ\rangle$是群，这里 $\circ$ 表示函数的合成，通常这个群不是Abel群。

4. $\langle Z_n,+_n\rangle$ 是Abel群，其中 $Z_n=\{0,1,\cdots,n-1\}$，$+_n$ 是模加，$a+_n b$ 等于 $(a+b)\bmod n$，$x^{-1}=n-x$。$\langle Z_n,\times_n\rangle$ 不是群，因为0没有逆元，这里 $\times_n$ 是模乘，$a\times_n b$ 等于 $(a\times b)\bmod n$。

定义4-3　设$\langle G,*\rangle$是一个群，I是整数集合。如果存在一个元素$g\in G$，对于每一个元素$a\in G$，都有一个相应的$i\in I$，能把a表示成g^i，则称$\langle G,*\rangle$是**循环群**，g称为循环群的**生成元**，记$G=\langle g\rangle=\{g^i|i\in I\}$。称满足方程$a^m=e$的最小正整数$m$为$a$的**阶**，记为$|a|$。

密码学中使用的群大多为循环群。

定义4-4 若代数系统$\langle R,+,\bullet\rangle$的二元运算+和$\bullet$满足：

（1）$\langle R,+\rangle$是Abel群；

（2）$\langle R,\bullet\rangle$是半群；

（3）乘法$\bullet$在加法+上可分配，即对$\forall a,b,c\in R$，有

$$a\cdot(b+c)=a\cdot b+a\cdot c \text{ 和 } (b+c)\cdot a=b\cdot a+c\cdot a$$

则称$\langle R,+,\bullet\rangle$是**环**。

【例4-2】

（1）$\langle I, +, \bullet \rangle$是环，因为$\langle I, + \rangle$是Abel群，$\langle I, \bullet \rangle$是半群，乘法$\bullet$在加法$+$上可分配。

（2）$\langle Z_n, +_n, \times_n \rangle$是环，因为$\langle Z_n, +_n \rangle$是Abel群，$\langle Z_n \times_n \rangle$是半群，$\times_n$对$+_n$可分配。

（3）$\langle M_n, +, \bullet \rangle$是环，这里$M_n$是$I$上$n \times n$方阵集合，$+$是矩阵加法，$\bullet$是矩阵乘法。

（4）$\langle R(x), +, \bullet \rangle$是环，这里$R(x)$是所有实系数的多项式集合，$+$和$\bullet$分别是多项式加法和乘法。

定义4-5 若代数系统$\langle \mathrm{F}, +, \bullet \rangle$的二元运算$+$和$\bullet$满足：

(1)$\langle \mathrm{F}, + \rangle$是Abel群；

(2)$\langle \mathrm{F}-\{0\}, \bullet \rangle$是Abel群，其中0是+的单位元；

(3) 乘法$\bullet$在加法$+$上可分配，即对$\forall a,b,c \in \mathrm{F}$，有

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{和} \quad (b+c) \cdot a = b \cdot a + c \cdot a$$

则称$\langle \mathrm{F}, +, \bullet \rangle$是**域**。

$\langle Q, +, \bullet \rangle$、$\langle R, +, \bullet \rangle$、$\langle C, +, \bullet \rangle$都是域，其中$Q$、$R$、$C$分别是有理数集合、实数集合和复数集合。

有限域是指域中元素个数有限的域，元素个数称为**域的阶**。若 q 是素数的幂，即 $q = p^r$，其中 p 是素数，r 是自然数，则阶为 q 的域称为Galois域，记为 $GF(q)$ 或 F_q。

已知所有实系数的多项式集合 $R(x)$ 在多项式加法和乘法运算下构成环。类似地，任意域 F 上的多项式（即系数取自 F）集合 $F(x)$ 在多项式的加法和乘法运算下也构成环。

$F(x)$ 中**不可约多项式**的概念与整数中的素数概念类似，是指在 F 上仅能被非0常数或自身的常数倍除尽，但不能被其它多项式除尽的多项式。

两个多项式的最高公因式为1时，称它们**互素**。

多项式的系数取自以素数 p 为模的域 F 时，这样的多项式集合记为 $F_p[x]$。

若 $m(x)$ 是 $F_p[x]$ 上的 n 次不可约多项式，$F_p[x]$ 上多项式加法和乘法改为以 $m(x)$ 为模的加法和乘法，此时的多项式集合记为 $F_p[x]/m(x)$，集合中元素个数为 p^n，$F_p[x]/m(x)$ 是一个有限域 $GF(p^n)$。

4.1.2 素数和互素数

1.因子

设 $a,b(b\neq 0)$ 是两个整数，如果存在另一整数 m，使得 $a=mb$，则称 b **整除** a，记为 $b|a$，且称 b 是 a 的**因子**。否则称 b 不整除 a，记为 $b\nmid a$。

整除的性质：

(1) $a|1$，那么 $a=\pm 1$；

(2) $a|b$ 且 $b|a$，则 $a=\pm b$；

(3) 对任一 $b(b\neq 0)$，$b|0$；

(4) $b|g,b|h$，则对任意整数 m,n，有 $b|(mg+nh)$。

这里只给出(4)的证明，其它三个性质的证明都很简单，

证(4)：

由 $b|g, b|h$ 知，存在整数 g_1、h_1，使得

$$g = bg_1 \quad , \quad h = bh_1$$

所以

$$mg + nh = mbg_1 + nbh_1 = b(mg_1 + nh_1)$$

因此 $b|(mg+nh)$。

2. 素数

称整数 $p(p>1)$ 是素数，如果 的因子只有 ± 1 和 $\pm p$ 。

若 p 不是素数，则称为**合数**。

任一整数 $a(a>1)$ 都能唯一地分解为以下形式：

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

其中，$p_1 < p_2 < \cdots < p_t$ 是素数，$a_i > 0\ (i = 1, \cdots, t)$。例如

$$91 = 7 \times 13 \quad , \quad 11011 = 7 \times 11^2 \times 13$$

这一性质称为整数分解的**唯一性**，也可如下陈述：

设 P 是所有素数集合，则任意整数 $a(a>1)$ 都能唯一地写成以下形式：

$$a = \prod_{p \in P} p^{a_p}$$

其中 $a_p \geq 0$ 。

等号右边的乘积项取所有的素数，然而大多指数项 a_p为0。

相应地，任一正整数也可由非0指数列表表示。如：11011可表示为 $\{a_7=1, a_{11}=2, a_{13}=1\}$。

两数相乘等价于对应的指数相加，即：由 $k=mn$ 可得：对每一素数 p，$k_p=m_p+n_p$　。

而由 $a|b$ 可得：对每一素数 $p, a_p \le b_p$。这是因为p^k只能被 $p^j (j \le k)$ 整除。

3.互素数

称 c 是两个整数 a,b 的最大公因子，如果

(1) c 是 a 的因子也是 b 的因子，即 c 是 a,b 的公因子；

(2) a 和 b 的任一公因子，也是 c 的因子。

表示为 $c=\gcd\{a,b\}$ 。

由于我们要求最大公因子为正，所以

$$\gcd\{a,b\}=\gcd\{a,-b\}=\gcd\{-a,b\}=\gcd\{-a,-b\}$$ 。

一般 $\gcd\{a,b\}=\gcd\{|a|,|b|\}$ 。

由任一非0整数能整除0，可得 $\gcd\{a,0\}=a$ 。如果将 a,b 都表示为素数的乘积，则 $\gcd\{a,b\}$ 极易确定。

【例4-3】

$$300 = 2^2 \times 3^1 \times 5^2$$

$$18 = 2^1 \times 3^2$$

$$(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$$

一般由 $c = \gcd\{a,b\}$ 可得：对每一素数 p，$c_p = \min\{a_p, b_p\}$ 。

如果 $\gcd\{a,b\} = 1$，则称 a 和 b 互素。

称 d 是两个整数 a,b 的最小公倍数，如果

(1) d 是 a 的倍数也是 b 的倍数，即 d 是 a,b 的公倍数；

(2) a 和 b 的任一公倍数，也是 d 的倍数。

表示为 $c = \mathrm{lcm}\{a,b\}$ 。

若 a,b 是两个互素的正整数，则 $\mathrm{lcm}\{a,b\} = ab$ 。

4.1.3 模运算

设 n 是一正整数，a 是整数，如果用 n 除 a，得商为 q，余数为 r，则

$$a = qn + r, 0 \le r < n, q = \left\lfloor \frac{a}{n} \right\rfloor$$

其中 $\lfloor x \rfloor$ 为小于或等于 x 的最大整数。

用 $a \bmod n$ 表示余数 r，则 $a = \left\lfloor \frac{a}{n} \right\rfloor n + a \bmod n$ 。

如果 $(a \bmod n) = (b \bmod n)$，则称两整数 a 和 b **模** n **同余**，记为 $a \equiv b \bmod n$。称与 a 模 n 同余的数的全体为 a 的**同余类**，记为 $[a]$，称 a 为这个同余类的表示元素。

注意： 如果$a \equiv 0 \pmod{n}$，则$n \mid a$。

同余有以下性质：

(1) $n \mid (a-b)$ 与 $a \equiv b \bmod n$ 等价。

(2) $(a \bmod n) = (b \bmod n)$，则$a \equiv b \bmod n$。

(3) $a \equiv b \bmod n$，则 $b \equiv a \bmod n$。

(4) $a \equiv b \bmod n$，$b \equiv c \bmod n$，则 $a \equiv c \bmod n$。

(5) 如果 $a \equiv b \bmod n$，$d \mid n$，则 $a \equiv b \bmod d$。

(6) 如果 $a \equiv b \bmod n_i \ (i = 1, \cdots, k)$, $d = [n_1, \cdots, n_k]$，则 $a \equiv b \bmod d$。

证明：

(5)由 $a \equiv b \bmod n$ 及 $d \mid n$，得 $n \mid (a-b)$，$d \mid (a-b)$。

(6) 由 $a \equiv b \bmod n_i$ 得 $n_i \mid (a-b)$，即 $a-b$ 是 n_1, L, n_k 的公倍数，所以 $d \mid (a-b)$。

从以上性质易知，同余类中的每一元素都可作为这个同余类的表示元素。

求余数运算（简称求余运算）$a \bmod n$ 将整数 a 映射到集合 $\{0,1,\cdots,n-1\}$，称求余运算在这个集合上的算术运算为**模运算**，模运算有以下性质：

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

(2) $[(a \bmod n)-(b \bmod n)] \bmod n = (a-b) \bmod n$ 。

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

证(1)：

设 $(a \bmod n) = r_a$ ，$(b \bmod n) = r_b$ ，则存在整数 j, k 使得

$$a = jn + r_a，\ b = kn + r_b。$$

因此

$$(a+b) \bmod n = [(j+k)n + r_a + r_b] \bmod n = (r_a + r_b) \bmod n$$

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

(2)、(3)的证明类似。

【例4-4】设 $Z_8 = \{0,1,\cdots,7\}$ ，考虑 Z_8 上的模加法和模乘法，结果如下：

表4-1 模8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

×	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	3	4	2
7	0	7	6	5	4	6	2	1

从加法结果可见，对每一 x，都有一 y，使得 $x+y\equiv 0 \bmod 8$。如对2，有6，使得 $2+6\equiv 0 \bmod 8$，称 y 为 x 的负数，也称为**加法逆元**。

对 x，若有 y，使得 $x\times y\equiv 1 \bmod 8$，如 $3\times 3\equiv 1 \bmod 8$，则称 y 为 x 的倒数，也称为**乘法逆元**。本例可见并非每一 x 都有乘法逆元。

一般，定义 Z_n 为小于 n 的所有非负整数集合，即：

$$Z_n=\{0,1,\cdots,n-1\}$$

称 Z_n 为模 n 的**同余类集合**。

其上的模运算有以下性质：

(1) **交换律**：$(w+x) \bmod n = (x+w) \bmod n$

$(w \times x) \bmod n = (x \times w) \bmod n$

(2) **结合律**：$[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$

$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$

(3) **分配律**：$[w \times (x+y)] \bmod n = [(w \times x)+(w \times y)] \bmod n$

(4) **单位元**：$(0+w) \bmod n = w \bmod n$　　$(1 \times w) \bmod n = w \bmod n$

(5) **加法逆元**：对$w \in Z_n$，存在 $z \in Z_n$，使得 $w+z \equiv 0 \bmod n$，记 $z=-w$。此外还有以下性质：

如果$(a+b) \equiv (a+c) \bmod n$，则 $b \equiv c \bmod n$，称为**加法的可约律**。

该性质可由 $(a+b)\equiv(a+c)\bmod n$ 的两边同加上 a 的加法逆元得到。

然而类似性质对乘法却不一定成立。

例如，$6\times3\equiv6\times7\equiv2\bmod8$，但 $3\not\equiv7\bmod8$。

原因是6乘0到7得到的8个数仅为 Z_8 的一部分，看上例。

如果将对 Z_8 作6的乘法 $6\times Z_8$（即用6乘 Z_8 中每一数）看作 Z_8 到 Z_8 的映射的话，Z_8 中至少有两个数映射到同一数，因此该映射为多到一的，所以对6来说，没有唯一的乘法逆元。

但对5来说，$5\times5\equiv1\bmod8$，因此5有乘法逆元5。

仔细观察可见，与8互素的几个数1，3，5，7都有乘法逆元。

记 $Z_n^*=\{a\mid0<a<n,\gcd\{a,\ n\}=1\}$。

定理4-1 Z_n^* 中每一元素有乘法逆元。

证明

首先证明Z_n^*中任一元素a与Z_n^*中任意两个不同元素b,c（不妨设$c<b$）相乘，其结果必然不同。

否则设$a\times b\equiv a\times c \bmod n$，则存在两个整数 k_1,k_2，使得 $ab=k_1n+r$，$ac=k_2n+r$，可得 $a(b-c)=(k_1-k_2)n$，所以 a是$(k_1-k_2)n$的一个因子。又由 $\gcd\{a,\ n\}=1$，得 a是 k_1-k_2的一个因子，设 $k_1-k_2=k_3a$，所以 $a(b-c)=k_3an$，即 $b-c=k_3n$，与 $0<c<b<n$ 矛盾。所以 $|a\times Z_n^*|=|Z_n^*|$。

对 $a\times Z_n^*$ 中任一元素ac，由 $\gcd\{a,\ n\}=1,\gcd\{c,\ n\}=1$，得 $\gcd\{ac,n\}=1$，$ac\in Z_n^*$，所以 $a\times Z_n^*\subseteq Z_n^*$。

由以上两条得 $a \times Z_n^* = Z_n^*$。因此对 $1 \in Z_n^*$，存在 $x \in Z_n^*$，使得 $a \times x \equiv 1 \bmod n$，即 x 是 a 的乘法逆元。记为 $x = a^{-1}$。

（定理4-1证毕）

证明中用到如下结论：设 A, B 是2个集合，满足 $A \subseteq B$ 且 $|A| = |B|$，则 $A = B$。

设 p 为一素数，则 Z_p 中每一非0元素都与 p 互素，因此有乘法逆元。类似于加法可约律，可有以下乘法可约律：

如果 $(a \times b) \equiv (a \times c) \bmod n$ 且 a 有乘法逆元，那么对 $(a \times b) \equiv (a \times c) \bmod n$ 两边同乘以 a^{-1}，即得 $b \equiv c \bmod n$。

4.1.4 模指数运算

模指数运算是指对给定的正整数 m,n，计算 $a^m \bmod n$。

【例4-5】

$a=7,n=19$，则易求出 $7^1 \equiv 7 \bmod 19, 7^2 \equiv 11 \bmod 19, 7^3 \equiv 1 \bmod 19$。

由于 $7^{3+j} = 7^3 \cdot 7^j \equiv 7^j \bmod 19$，所以 $7^4 \equiv 7 \bmod 19$，$7^5 \equiv 7^2 \bmod 19$，…，即从 $7^4 \bmod 19$ 开始所求的幂出现循环，循环周期为3。

可见在模指数运算中，若能找出循环周期，则会使得计算简单。

称满足方程 $a^m \equiv 1 \bmod n$ 的最小正整数 m 为模 n 下 a 的阶，记为 $\mathrm{ord}_n(a)$。

定理4-2

设 $\mathrm{ord}_n(a)=m$，则 $a^k \equiv 1 \bmod n$ 的充要条件是 k 为 m 的倍数。

证明

设存在整数 q，使得 $k=qm$，则 $a^k \equiv (a^m)^q \equiv 1 \bmod n$。

反之，假定 $a^k \equiv 1 \bmod n$，令 $k=qm+r$ 其中 $0<r\le m-1$，那么

$$a^k \equiv (a^m)^q a^r \equiv a^r \equiv 1 (\bmod n)$$

与 m 是阶矛盾。

（定理4-2证毕）

4.1.5 费尔马定理、欧拉定理、卡米歇尔定理

这三个定理在公钥密码体制中起着重要作用。

1.费尔马(Fermat) 定理

定理4-3(费尔马定理)

若 p 是素数，a 是正整数且 $\gcd\{a,p\}=1$，则 $a^{p-1}\equiv 1 \bmod p$ 。

证明 在定理1-1的证明中知，当 $\gcd\{a,p\}=1$ 时，$a\times Z_p = Z_p$，其中 $a\times Z_p$ 表示 a 与 Z_p 中每一元素做模 p 乘法。

又知 $a\times 0\equiv 0 \bmod p$，所以 $a\times Z_p-\{0\}=Z_p-\{0\}$，$a\times(Z_p-\{0\})=Z_p-\{0\}$。即

$$\{a \bmod p, 2a \bmod p, \cdots, (p-1)a \bmod p\} = \{1,2,\cdots,p-1\}$$

分别将两个集合中的元素连乘，得：

$$a \times 2a \times \cdots (p-1)a \equiv [(a \bmod p) \times (2a \bmod p) \times \cdots \times ((p-1)a \bmod p)] \bmod p$$
$$\equiv (p-1)! \bmod p$$

另一方面，

$$a \times 2a \times \cdots (p-1)a = (p-1)! a^{p-1}$$

因此

$$(p-1)! a^{p-1} \equiv (p-1)! \bmod p$$

由于$(p-1)!$与p互素，因此$(p-1)!$有乘法逆元，由乘法可约律得 $a^{p-1} \equiv 1 \bmod p$。

（定理4-3证毕）

Fermat定理也可写成如下形式：

设p是素数，a是任一正整数，则 $a^p \equiv a \bmod p$ 。

2.欧拉函数

设 n 是一正整数，小于 n 且与 n 互素的正整数的个数称为 n 的**欧拉函数**，记为 $\varphi(n)$ 。

【例4-6】 $\varphi(6)=2$，$\varphi(7)=6$，$\varphi(8)=4$ 。

定理4-4

(1) 若 n 是素数，则 $\varphi(n)=n-1$；

(2) 若 n 是两个素数 p 和 q 的乘积，则

$$\varphi(n)=\varphi(p)\times\varphi(q)=(p-1)\times(q-1)$$；

(3) 若 n 有标准分解式 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_t}\right)$$ 。

证明

（1）显然；

（2）考虑 $Z_n=\{0,1,\cdots,pq-1\}$，其中不与 n 互素的数有三类：$A=\{p,2p,\cdots,(q-1)p\}$，$B=\{q,2q,\cdots,(p-1)q\}$，$C=\{0\}$，且 $A\cap B=\Phi$，否则如果 $ip=jq$，其中 $1\le i\le q-1,\ 1\le j\le p-1$ 则 p 是 jq 的因子，因此是 j 的因子，设 $j=kp,k\ge 1$。

则 $ip=kpq$，$i=kq$，与 $1\le i\le q-1$ 矛盾。所以

$$\varphi(n)=|Z_n|-[|A|+|B|+|C|]=pq-[(q-1)+(p-1)+1]$$
$$=(p-1)\times(q-1)=\varphi(p)\times\varphi(q).$$

(3) 当 $n=p^{\alpha}$ 时，1□ n 之间与 n 不互素的数有 $1\cdot p,2\cdot p,\cdots,p^{\alpha-1}\cdot p$ ，共 $p^{\alpha-1}$ 个，所以 $\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$。

当 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ ，由(2)得，

$$\varphi(n)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_t^{\alpha_t})=\left(p_1^{\alpha_1}-p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2}-p_2^{\alpha_2-1}\right)\cdots\left(p_t^{\alpha_t}-p_t^{\alpha_t-1}\right)$$

$$=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_t}\right).$$

（定理4-4证毕）

【例4-7】

$$\varphi(21)=\varphi(3\times7)=\varphi(3)\times\varphi(7)=2\times6=12$$

$$\varphi(72)=\varphi(2^3 3^2)=72\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=24$$

3. 欧拉定理

定理4-5（Euler定理）

若 a 和 n 互素，则 $a^{\varphi(n)} \equiv 1 \bmod n$ 。

证明

设 $R=\{x_1, x_2, \cdots, x_{\varphi(n)}\}$ 是由小于 n 且与 n 互素的全体数构成的集合，$a \times R=\{ax_1 \bmod n, ax_2 \bmod n, \cdots, ax_{\varphi(n)} \bmod n\}$，考虑 $a \times R$ 中任一元素 $ax_i \bmod n$，因 a 与 n 互素，x_i 与 n 互素，所以 ax_i 与 n 互素，且 $ax_i \bmod n < n$，因此 $ax_i \bmod n \in R$，所以 $a \times R \subseteq R$ 。

又因$a\times R$中任意两个元素都不相同，否则$ax_i \bmod n = ax_j \bmod n$，由$a$与$n$互素知$a$在$\bmod n$下有乘法逆元，得$x_i = x_j$。

所以$|a\times R| = |R|$，得$a\times R = R$，所以$\prod_{i=1}^{\varphi(n)}(ax_i \bmod n) = \prod_{i=1}^{\varphi(n)} x_i$，$\prod_{i=1}^{\varphi(n)} ax_i \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod n$，$a^{\varphi(n)}\cdot\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} x_i \pmod n$，由每一$x_i$与$n$互素，知$\prod_{i=1}^{\varphi(n)} x_i$与$n$互素，$\prod_{i=1}^{\varphi(n)} x_i$在$\bmod n$下有乘法逆元。所以$a^{\varphi(n)} \equiv 1 \bmod n$。

（定理4-5证毕）

推论： $\mathrm{ord}_n(a) \mid \varphi(n)$ 。

推论说明，$\mathrm{ord}_n(a)$ 一定是 $\varphi(n)$ 的因子。如果 $\mathrm{ord}_n(a)=\varphi(n)$，则称 a 为 n 的**本原根**。

如果 a 是 n 的本原根，则

$$a, a^2, \cdots, a^{\varphi(n)}$$

在 $\bmod n$ 下互不相同且都与 n 互素。

特别地，如果 a 是素数 p 的本原根，则

$$a, a^2, \cdots, a^{p-1}$$

在 $\bmod p$ 下都不相同。

【例4-8】 $n=9$，则 $\varphi(n)=6$，考虑2在 $\bmod 9$ 下的幂 $2^1 \bmod 9 \equiv 2, 2^2 \bmod 9 \equiv 4$，$2^3 \bmod 9 \equiv 8$，$2^4 \bmod 9 \equiv 7$，$2^5 \bmod 9 \equiv 5$，$2^6 \bmod 9 \equiv 1$。即 $\mathrm{ord}_9(2)=\varphi(9)$，所以2为9的本原根。

【例4-9】 $n=19$，$a=3$ 在mod 19下的幂分别为

3，9，8，5，15，7，2，6，18，16，10，11，

14，4，12，17，13，1

即 $\mathrm{ord}_{19}(3)=18=\varphi(19)$，所以3为19的本原根。

本原根不唯一。

可验证除3外，19的本原根还有2，10，13，14，15。

注意

并非所有的整数都有本原根，只有以下形式的整数才有本原根：

$$2,\ 4,\ p^{\alpha},\ 2p^{\alpha}$$

其中 p 为奇素数。

4. 卡米歇尔定理

对满足 $\gcd\{a,n\}=1$ 的所有 a ，使得 $a^m \equiv 1 \bmod n$ 同时成立的最小正整数 m，称为 n 的卡米歇尔（Carmichael）函数，记为 $\lambda(n)$。

【例4-10】

n=8，与8互素的数有1,3,5,7，即 $\varphi(8)=4$ 。

$$1^2 \equiv 1 \bmod 8,\ 3^2 \equiv 1 \bmod 8,\ 5^2 \equiv 1 \bmod 8,\ 7^2 \equiv 1 \bmod 8,$$

所以 $\lambda(8)=2$ 。

从该例看出，$\lambda(n) \le \varphi(n)$ 。

定理4-6

(1) 如果 $a|b$，则 $\lambda(a)|\lambda(b)$；

(2) 对任意互素的正整数 a,b，有 $\lambda(ab)=[\lambda(a),\lambda(b)]$；

(3)
$$\lambda(n)=\begin{cases}\varphi(n)=1, & n=1\\ \varphi(n)=1, & n=2\\ \varphi(n)=2, & n=4\\ \frac{1}{2}\varphi(n)=2^{\alpha-2}, & n=2^{\alpha},\alpha>2\\ \varphi(n)=p-1, & n=p\text{奇素数}\\ \varphi(n)=p^{\alpha}-p^{\alpha-1}, & n=p^{\alpha},p\text{奇素数，}\alpha>1\\ \left[\lambda\left(p_1^{\alpha_1}\right),\cdots,\lambda\left(p_t^{\alpha_t}\right)\right], & n=\prod_{i=1}^{t}p_i^{\alpha_i}\end{cases}$$

证明

(1) 对满足 $\gcd\{x,b\}=1$ 的所有 x，$x^{\lambda(b)}\equiv 1 \bmod b$，由 $a|b$ 得，$x^{\lambda(b)}\equiv 1 \bmod a$。设 $\lambda(b)=k\lambda(a)+r$，其中 $0\le r<\lambda(a)$，则 $x^{\lambda(b)}\equiv\left(x^{\lambda(a)}\right)^k x^r\equiv x^r\equiv 1 \bmod a$，所以 $r=0$，即 $\lambda(a)|\lambda(b)$。

(2) 由(1)得，$\lambda(a)|\lambda(ab),\lambda(b)|\lambda(ab)$，即$\lambda(ab)$是 $\lambda(a)$ 和 $\lambda(b)$ 的公倍数。又设 d 是$\lambda(a)$ 和 $\lambda(b)$ 的任一公倍数，由 $\lambda(a)|d,\lambda(b)|d$ 得 $x^d\equiv 1 \bmod a, x^d\equiv 1 \bmod b$，其中 $\gcd\{x,a\}=1,\gcd\{x,b\}=1$，所以 $x^d\equiv 1 \bmod ab$，其中 $\gcd\{x,ab\}=1$，$\lambda(ab)|d$。所以$\lambda(ab)$是$\lambda(a)$和 $\lambda(b)$ 的最小公倍数。

(3) 可由(2)得到。

（定理4-6证毕）

定理4-7（卡米歇尔定理）

若 a 和 n 互素，则 $a^{\lambda(n)} \equiv 1 \bmod n$ 。

证明

设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ ，下面证明 $a^{\lambda(n)} \equiv 1 \bmod p_i^{\alpha_i} \left(i = 1, \cdots, t\right)$ 。

如果 $p_i^{\alpha_i} = 2, 4$ 或奇素数的幂，由定理1-6(3)，$\lambda\left(p_i^{\alpha_i}\right) = \varphi\left(p_i^{\alpha_i}\right)$ ，所以 $a^{\lambda\left(p_i^{\alpha_i}\right)} = a^{\varphi\left(p_i^{\alpha_i}\right)} \equiv 1 \bmod p_i^{\alpha_i}$ 。

又因 $\lambda\left(p_i^{\alpha_i}\right) \mid \lambda(n)$，所以 $a^{\lambda(n)} \equiv 1 \bmod p_i^{\alpha_i}$ 。

当 $p_i^{\alpha_i} = 2^{\alpha_i} \left(\alpha_i > 2\right)$ 时，$\lambda\left(p_i^{\alpha_i}\right) = \frac{1}{2}\varphi\left(2^{\alpha_i}\right) = 2^{\alpha_i - 2}$ ，我们需要证明 $a^{2^{\alpha_i - 2}} \equiv 1 \bmod 2^{\alpha_i}$ ，对 α_i 用归纳法。

当 $\alpha_i = 3$ 时，$a^2 \equiv 1 \bmod 8$ 对每一奇整数 a 成立。设 $a^{2^{\alpha_i - 2}} \equiv 1 \bmod 2^{\alpha_i}$ 对 α_i 成立，即 $a^{2^{\alpha_i - 2}} = 1 + t2^{\alpha_i}$，$t$ 是一正整数。则当 $\alpha_i + 1$ 时，

$$a^{2^{\alpha_i - 1}} = \left(1 + t2^{\alpha_i}\right)^2 = 1 + t2^{\alpha_i + 1} + t^2 2^{2\alpha_i} \equiv 1 \bmod 2^{\alpha_i + 1}$$

由归纳法，$a^{2^{\alpha_i - 2}} \equiv 1 \bmod 2^{\alpha_i}$ 对任意 $\alpha_i \left(\alpha_i > 2\right)$ 成立。

由 $a^{\lambda(n)} \equiv 1 \bmod p_i^{\alpha_i} \left(i = 1, \cdots, t\right)$，得 $a^{\lambda(n)} \equiv 1 \bmod d$，其中 $d = \left[p_1^{\alpha_1}, \cdots, p_t^{\alpha_t}\right] = p_1^{\alpha_1} \cdots p_t^{\alpha_t} = n$，所以 $a^{\lambda(n)} \equiv 1 \bmod n$ 。

（定理4-7证毕）

4.1.6 素性检验

素性检验是指对给定的数检验其是否为**素数**。

1.爱拉托斯散(Eratosthenes)筛法

定理4-8 设 n 是一正整数，如果对所有满足 $p \le \sqrt{n}$ 的素数 p，都有 $p \nmid n$，那么 n 一定是素数。

基于这个定理，有一个寻找素数的算法，称为**爱拉托斯散(Eratosthenes)筛法**。

要找不大于 n 的所有素数，先将2到 n 之间的整数都列出，从中删除小于等于 $\sqrt{n}$ 的所有素数 $2,3,5,7,\cdots,p_k$（设满足 $p \le \sqrt{n}$ 的素数有 k 个）的倍数，余下的整数就是所要求的所有素数

【例4-11】求不超过 $n=100$ 的所有素数。

解：因为$\sqrt{100}=10$，小于10的素数有2、3、5、7，删去2□100之间的整数中2的倍数（保留2）得：

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

删去3的倍数（保留3）得：

1	2	3	5	7	~~9~~
11		13	~~15~~	17	19
~~21~~		23	25	~~27~~	29
31		~~33~~	35	37	~~39~~
41		43	~~45~~	47	49
~~51~~		53	55	~~57~~	59
61		~~63~~	65	67	~~69~~
71		73	~~75~~	77	79
~~81~~		83	85	~~87~~	89
91		~~93~~	95	97	~~99~~

删去5的倍数（保留5）得：

1	2	3	5	7	
11		13		17	19
		23	~~25~~		29
31			~~35~~	37	
41		43		47	49
		53	~~55~~		59
61			~~65~~	67	
71		73		77	79
		83	~~75~~		89
91			~~85~~	97	

删去7的倍数（保留7）得：

1	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	~~49~~
		53			59
61				67	
71		73		77	79
		83			89
~~91~~				97	

此时，余下的数就是不超过100的所有素数。

爱拉托斯散筛法在判断是否为素数时，要除以小于等于 的所有素数，当 很大时，实际上是不可行的。

2.Miller-Rabin概率检测法

引理4-1 如果 p 为大于2的素数，则方程 $x^2 \equiv 1 \pmod{p}$ 的解只有 $x \equiv 1$ 和 $x \equiv -1$。

证明 由 $x^2 \equiv 1 \pmod{p}$，有 $x^2 - 1 \equiv 0 \bmod p$，$(x+1)(x-1) \equiv 0 \bmod p$，因此 $p \mid (x+1)$ 或 $p \mid (x-1)$ 或 $p \mid (x+1)$ 且 $p \mid (x-1)$。

若 $p \mid (x+1)$ 且 $p \mid (x-1)$，则存在两个整数 k 和 j，使得 $x+1 = kp$，$x-1 = jp$ 两式相减得 $2 = (k-j)p$，为不可能结果。所以有 $p \mid (x+1)$ 或 $p \mid (x-1)$。

设 $p \mid (x+1)$，则 $x+1 = kp$，因此 $x \equiv -1 \pmod{p}$。

类似地可得 $x \equiv 1 \pmod{p}$。

（引理4-1证毕）

引理4-1的逆否命题为：

如果方程 $x^2 \equiv 1 \bmod p$ 有一解 $x_0 \notin \{-1,1\}$，那么 p 不为素数。

【例4-12】

考虑方程 $x^2 \equiv 1 \pmod 8$ 由4.1.3节 $\mathbf{Z}_8$ 上模乘法的结果得

$1^2 \equiv 1 \bmod 8$，$3^2 \equiv 1 \bmod 8$，$5^2 \equiv 1 \bmod 8$，$7^2 \equiv 1 \bmod 8$

又 $5 \equiv -3 \bmod 8$，$7 \equiv -1 \bmod 8$，

所以方程的解为1，-1，3，-3，可见8不是素数。

下面介绍Miller-Rabin的素性概率检测法。

其核心部分如下：

WITNESS(a，n)

1. 将n-1表示为二进制形式 $b_k b_{k-1} \cdots b_0$ ；
2. $d \leftarrow 1$

for $i = k$ downto 0 do {

$x \leftarrow d$ ；

$d \leftarrow (d \times d) \bmod n$ ；

if $d = 1$ and $(x \neq 1)$ and $(x \neq n-1)$ then return *FALSE* ；

if $b_i = 1$ then $d \leftarrow (d \times a) \bmod n$ } ；

if $d \neq 1$ then return *FALSE* ；

return *TRUE* .

算法有两个输入，n 是待检验的数，a 是小于n 的整数。如果算法的返回值为 *FALSE* ，则 n 肯定不是素数，如果返回值为 *TRUE*，则 n 有可能是素数。

for 循环结束后，有 $d \equiv a^{n-1} \bmod n$，由 Fermat 定理知，若 n 为素数，则 d 为1。因此若 $d \neq 1$，则 n 不为素数，所以返回 *FALSE*。

因为 $n-1 \equiv -1 \bmod n$，所以 $(x \neq 1)\ and\ (x \neq n-1)$ 意指 $x^2 \equiv 1 (\bmod n)$ 有不在 $\{-1, 1\}$ 中的根，因此 n 不为素数，返回*FALSE*。

该算法有以下性质：对 s 个不同的 a，重复调用这一算法，只要有一次算法返回为 *FALSE*，就可肯定 n 不是素数。如果算法每次返回都为 *TRUE*，则 n 是素数的概率至少为 $1-2^{-s}$，因此对于足够大的 s，就可以非常肯定地相信 n 为素数。

3. AKS算法

2002年，印度数学家 Manindra Agrawal，Neeraj Kayal，Nitin Saxena 给出了一个确定性的素数判别算法，简称**AKS算法**。

设 N 和 I 分别是自然数集合和整数集合，且 $n \in N, a \in I, \gcd\{a,n\}=1$，满足

$$a^k \equiv 1 \bmod n$$

的最小正整数 k 称为模 n 下 a 的阶，记为 $\mathrm{ord}_n(a)$。

算法基于以下引理：

引理4-2

设 $n \geq 2$ 是一自然数，$a \in I, \gcd\{a,n\}=1$，则 n 是素数的充要条件是：

$$(X+a)^n \equiv X^n + a \pmod{n}$$

证明

对 $0<i<n$，$(X+a)^n-(X^n+a)$ 中 X^i 的系数为 $\binom{n}{i}a^{n-i}$。

如果 n 是素数，则 $\binom{n}{i}=0$，所以 $x^i(0<i<n)$ 的系数都为0。

如果 n 是合数，可设 q 是它的一个素数因子且 $q^k \mid n$，则 q^k 不能除尽 $\binom{n}{q}$，而且 q^k 和 a^{n-q} 互素，所以在模 n 下，的 X^q 系数不为 0，$(X+a)^n-(X^n+a) \not\equiv 0 \bmod n$ 。

（引理4-2证毕）

引理4-2给出了一个素数检验的简单方法，然而要验证等式$(X+a)^n \equiv X^n + a \pmod{n}$是否成立，需计算 n 个系数。

为了减少系数的计算，可在等式的两边同时对一个形如 $X^r - 1$ 的多项式取模（其中 r 是一个适当选择的小整数），即将判断等式 $(X+a)^n \equiv X^n + a \pmod{n}$ 是否成立，改为判断

$$(X+a)^n \equiv X^n + a \left(\bmod X^r - 1, n\right)$$

是否成立。

$(X+a)^n \equiv X^n + a \left(\bmod X^r - 1, n\right)$ 表示在环 $Z_n[X]/(X^r - 1)$ 上，$(X+a)^n = X^n + a$。

算法如下：

输入整数 n，

1. 如果 $n=a^b, a\in N, b>1$，输出“合数”；
2. 求满足 $\mathrm{ord}_r(n)>\log^2 n$ 的最小的 r；
3. 如果存在 a，满足 $a\le r$ 且
   $1<\gcd\{a,n\}<n$，输出“合数”；
4. 如果 $n\le r$，输出“素数”；
5. for $a=1$ to $\left\lfloor\sqrt{\varphi(r)}\log n\right\rfloor$ do
   如果 $(X+a)^n\not\equiv X^n+a\left(\mathrm{mod}\, X^r-1, n\right)$，输出“合数”；
6. 输出“素数”。

4.1.7 欧几里得算法

欧几里得（Euclid）算法是数论中的一个基本技术，是求两个正整数的最大公因子的简化过程。

而推广的Euclid算法不仅可求两个正整数的最大公因子，而且当两个正整数互素时，还可求出其中一个数关于另一个数的乘法逆元。

1. 求最大公因子

Euclid算法是基于下面一个基本结论：

设 a,b 是任意两个正整数，将它们的最大公因子 $\gcd\{a,b\}$ 简记为 (a,b) 。有以下重要结论

$$(a,b)=(b,a \bmod b)$$

证明：

b 是正整数，因此可将 a 表示为 $a=kb+r,\ a \bmod b=r,$ 其中 k 为一整数，所以 $a \bmod b=a-kb$ 。

设 d 是 a,b 的公因子，即 $d|a, d|b$ ，所以 $d|kb$ 。由 $d|a$ 和 $d|kb$ 得 $d|(a \bmod b)$ ，因此 d 是 b 和 $a \bmod b$ 的公因子。

所以得出 a,b 的公因子集合与 $b, a \bmod b$ 的公因子集合相等，两个集合的最大值也相等，得证。

在求两个数的最大公因子时，可重复使用以上结论。

【例4-13】

(55, 22)= (22, 55 mod 22)= (22, 11)= (11, 0)=11。

【例4-14】

(18,12)=(12,6)=(6,0)=6,

(11,10)= (10,1) =1。

Euclid算法如下：设 a,b 是任意两个正整数, 记 $r_0=a, r_1=b$, 反复用上述除法（称为辗转相除法），有:

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2, & 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3, & 0 \le r_3 < r_2 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_n + r_{n+1}, & r_{n+1} = 0
\end{aligned}
$$

由于 $r_1=b>r_2>\cdots>r_n>r_{n+1}\geq 0$，经过有限步后，必然存在 n 使得 $r_{n+1}=0$。可得 $(a,b)=r_n$，即辗转相除法中最后一个非0余数就是 a 和 b 的最大公因子。这是因为

$$(a,b)=(b,r_2)=(r_2,r_3)=\cdots=(r_{n-1},r_n)=(r_n,0)=r_n \quad 。$$

因 $(a,b)=(|a|,|b|)$，因此可假定算法的输入是两个正整数，并设 $a>b$。

EUCLID (a,b)

1. $X\leftarrow a$; $Y\leftarrow b$;
2. if $Y=0$ then return $X=(a, b)$;
3. if $Y=1$ then return $Y=(a, b)$;
4. $R=X$ mod Y;
5. $X=Y$;
6. $Y=R$;
7. goto 2.

【例4-15】 求 (1970, 1066)。

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

因此 (1970, 1066)=2。

在辗转相除法中，有

$$r_n = r_{n-2} - r_{n-1}q_{n-1};$$
$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2};$$
$$\cdots$$
$$r_3 = r_1 - r_2 q_2;$$
$$r_2 = r_0 - r_1 q_1.$$

依次将后一项带入前一项，可得 r_n 由 $r_0 = a, r_1 = b$ 的线性组合表示。

因此有如下结论：

存在整数 s,t，使得 $sa + tb = (a,b)$，即两个数的最大公因子能由这两个数的线性组合表示。

2. 求乘法逆元

如果$(a,b)=1$，则 b 在 $\bmod a$ 下有乘法逆元（不妨设$b<a$），即存在一 $x(x<a)$，使得 $bx\equiv 1 \bmod a$ 。推广的Euclid算法先求出(a,b)，当$(a,b)=1$时，则返回 b的逆元。

EXTENDED EUCLID (a,b)（设 $b<a$ ）

1. $(X_1,X_2,X_3)\leftarrow(1,0,a)$；$(Y_1,Y_2,Y_3)\leftarrow(0,1,b)$ ；
2. if $Y_3=0$ then return $X_3=(a,b)$； no inverse;
3. if $Y_3=1$ then return $Y_3=(a,b)$ ； $Y_2=b^{-1} \bmod f$ ；
4. $Q=\left\lfloor \frac{X_3}{Y_3} \right\rfloor$
5. $(T_1,T_2,T_3)\leftarrow(X_1-QY_1,X_2-QY_2,X_3-QY_3)$；
6. $(X_1,X_2,X_3)\leftarrow (Y_1,Y_2,Y_3)$ ；
7. $(Y_1,Y_2,Y_3)\leftarrow(T_1,T_2,T_3)$；
8. goto 2

算法中的变量有以下关系：

$$aT_1+bT_2=T_3;\quad aX_1+bX_2=X_3;\quad aY_1+bY_2=Y_3$$

这一关系可用**归纳法**证明：设前一轮的变量为 (T_1',T_2',T_3')、(X_1',X_2',X_3')、(Y_1',Y_2',Y_3') 满足

$$aT_1'+bT_2'=T_3';\quad aX_1'+bX_2'=X_3';\quad aY_1'+bY_2'=Y_3'$$

则这一轮的变量 (T_1,T_2,T_3)、(X_1,X_2,X_3)、(Y_1,Y_2,Y_3) 和前一轮的变量有如下关系：

$$(T_1,T_2,T_3)=(X_1'-Q'Y_1',X_2'-Q'Y_2',X_3'-Q'Y_3')$$
$$(X_1,X_2,X_3)=(Y_1',Y_2',Y_3')$$
$$(Y_1,Y_2,Y_3)=(T_1,T_2,T_3)$$

所以

$$aT_1+bT_2=a\left(X_1'-Q'Y_1'\right)+b\left(X_2'-Q'Y_2'\right)$$
$$=aX_1'+bX_2'-Q'\left(aY_1'+bY_2'\right)=X_3'-Q'Y_3'=T_3$$

$$aX_1 + bX_2 = aY_1' + bY_2' = Y_3' = X_3$$

$$aY_1 + bY_2 = aT_1 + bT_2 = T_3 = Y_3$$

在算法EUCLID (a,b) 中，等于前一轮循环中的 Y，Y 等于前一轮循环中的 $X \bmod Y$。

而在算法EXTENDED EUCLID(a,b)中，X_3 等于前一轮循环中的 Y_3，Y_3 等于前一轮循环中的 $X_3 - QY_3$，由于 Q是Y_3 除 X_3的商，因此Y_3 是前一轮循环中的Y_3 除 X_3 的余数，即 $X_3 \bmod Y_3$，可见EXTENDED EUCLID (a,b) 中的 X_3、Y_3 与EUCLID(a,b)中的 X、Y 作用相同，因此可正确产生(a,b)。

如果$(a,b)=1$，则在倒数第二轮循环中 $Y_3 = 1$。由 $Y_3 = 1$可得 $aY_1 + bY_2 = Y_3$，$aY_1 + bY_2 = 1$，$bY_2 = 1 + (-Y_1) \times a$，$bY_2 \equiv 1 \bmod a$，所以 $Y_2 \equiv b^{-1} \bmod a$。

【例4-16】 求 (1769, 550)，

算法的运行结果及各变量的变化情况如表4-2所示：

表4-2 求 (1769,550) 时推广Euclid算法的运行结果

循环次数	Q	X_1	X_2	X_3	Y_1	Y_2	Y_3
初值	-	1	0	1769	0	1	550
1	3	0	1	550	1	-3	119
2	4	1	-3	119	-4	13	74
3	1	-4	13	74	5	-16	45
4	1	5	-16	45	-9	29	29
5	1	-9	29	29	14	-45	16
6	1	14	-45	16	-23	74	13
7	1	-23	74	13	37	-119	3
8	4	37	-119	3	-171	550	1

所以$(1769，550)=1，550^{-1} \bmod 1769 = 550$ 。

4.1.8 中国剩余定理

中国剩余定理是数论中最有用的一个工具，它有两个用途:

一是如果已知某个数关于一些两两互素的数的同余类集，　就可重构这个数。

二是可将大数用小数表示、大数的运算通过小数实现。

【例4-17】

Z_{10}中每个数都可从这个数关于2和5（10的两个互素的因子）的同余类重构。

比如已知 x 关于2和5的同余类分别是[0]和[3]，即 $x \bmod 2 \equiv 0, x \bmod 5 \equiv 3$。可知 x 是偶数且被5除后余数是3，所以可得8是满足这一关系的唯一的 x 。

【例4-18】

假设只能处理5以内的数，则要考虑15以内的数，可将15分解为两个小素数的乘积，$15=3\times5$，将1到15之间的数列表表示，表的行号为 0~2，列号为 0~4，将1到15的数填入表中，使得其所在行号为该数除3得到的余数,列号为该数除5得到的余数。

如 $12 \bmod 3=0, 12 \bmod 5=2$ ，所以12应填在第0行，第2列。

表4-3 1到15之间的数

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

现在就可处理15以内的数了。

例如求 $12\times13(\mathrm{mod}15)$，因12和13所在的行号分别是0和1，12和13所在的列号分别是2和3，由 $0\times1\equiv0\,\mathrm{mod}\,3;\ 2\times3\equiv1\mathrm{mod}\,5$ 得 $12\times13(\mathrm{mod}15)$ 所在的列号和行号分别为0和1，这个位置上的数是6，所以得 $12\times13(\mathrm{mod}15)\equiv6$ 。

又因 $0+1\equiv1\mathrm{mod}\,3;\ 2+3\equiv0\,\mathrm{mod}\,5$ ，第1行、第0列为10，所以 $12+13\equiv10\,\mathrm{mod}\,15$ 。

以上两例是中国剩余定理的直观应用,下面具体介绍定理的内容。

中国剩余定理最早见于《孙子算经》的“物不知数”问题：今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？

这一问题用方程组表示为：

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

下面给出解的构造过程。首先将三个余数写成和式的形式

$$2+3+2$$

为满足第一个方程，即模3后，后2项消失，给后2项各乘以3，得：

$$2+3\cdot 3+2\cdot 3$$

为满足第二个方程，即模5后，第一、三项消失，给第一、三项各乘以5，得：

$$2\cdot5+3\cdot3+2\cdot3\cdot5$$

同理给前2项各乘以7，得：

$$2\cdot5\cdot7+3\cdot3\cdot7+2\cdot3\cdot5$$

然而，将结果带入第一方程，得到$2\cdot5\cdot7$，为消去$5\cdot7$，将结果的第一项再乘以$(5\cdot7)^{-1}\bmod3$，得$2\cdot5\cdot7\cdot(5\cdot7)^{-1}\bmod3+3\cdot3\cdot7+2\cdot3\cdot5$。类似地，将第二项乘以$(3\cdot7)^{-1}\bmod5$，第三项乘以$(3\cdot5)^{-1}\bmod7$，得结果为

$$2\cdot5\cdot7\cdot(5\cdot7)^{-1}\bmod3+3\cdot3\cdot7\cdot(3\cdot7)^{-1}\bmod5+2\cdot3\cdot5\cdot(3\cdot5)^{-1}\bmod7=233$$

又因为$233+k\cdot 3\cdot 5\cdot 7=233+105k$（$k$为任一整数）都满足方程组，可取$k=-2$，得到小于$105(=3\cdot 5\cdot 7)$的唯一解23，所以方程组的唯一解构造如下：

$$\left[2\cdot 5\cdot 7\cdot (5\cdot 7)^{-1} \bmod 3+3\cdot 3\cdot 7\cdot (3\cdot 7)^{-1} \bmod 5+2\cdot 3\cdot 5\cdot (3\cdot 5)^{-1} \bmod 7\right] \bmod (3\cdot 5\cdot 7)$$

把这种构造法推广到一般形式，就是如下的中国剩余定理。

定理4-9（中国剩余定理）

设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，$M = \prod_{i=1}^{k} m_i$ ，则一次同余方程组

$$\begin{cases} a_1 \pmod{m_1} \equiv x \\ a_2 \pmod{m_2} \equiv x \\ \cdots \\ a_k \pmod{m_k} \equiv x \end{cases}$$

对模 M 有唯一解:

$$x \equiv \left(\frac{M}{m_1} e_1 a_1 + \frac{M}{m_2} e_2 a_2 + \cdots + \frac{M}{m_k} e_k a_k \right) \pmod{M}$$

其中 e_i 满足

$$\frac{M}{m_i} e_i \equiv 1 \pmod{m_i} (i = 1, 2, \cdots, k)$$

证明

设 $M_i = M/m_i = \prod_{\substack{\lambda=1 \\ \lambda\neq i}}^{k} m_\lambda$，$i = 1,2,\cdots,k$，由 M_i 的定义得 M_i 与 m_i 是互素的，可知 M_i 在模 m_i 下有唯一的乘法逆元，即满足 $\frac{M}{m_i} e_i \equiv 1 (\mathrm{mod}\, m_i)$ 的 e_i 是唯一的。

下面证明对 $\forall i \in \{1,2,\cdots,k\}$，上述满足 $a_i (\mathrm{mod}\, m_i) \equiv x$ 。注意到当 $j \neq i$ 时，$m_i \mid M_j$，即 $M_j \equiv 0 (\mathrm{mod}\, m_i)$ 。所以

$$\begin{aligned} &\left(M_j \times e_j \bmod m_j\right) \bmod m_i \\ &\equiv \left(\left(M_j \bmod m_i\right) \times \left(\left(e_j \bmod m_j\right) \bmod m_i\right)\right) \bmod m_i \equiv 0 \end{aligned}$$

而　　$\left(M_i \times \left(e_i \bmod m_i\right)\right) \bmod m_i \equiv \left(M_i \times e_i\right) \bmod m_i \equiv 1$

所以 $x (\mathrm{mod}\, m_i) \equiv a_i$，即 $a_i (\mathrm{mod}\, m_i) \equiv x$ 。

下面证明方程组的解是唯一的。

设 x' 是方程组的另一解，即

$$x' \equiv a_i \pmod{m_i}, (i = 1, 2, \cdots, k)$$

由 $x \equiv a_i \pmod{m_i}$ 得 $x' - x \equiv 0 \pmod{m_i}$，即 $m_i \mid (x' - x)$。再根据 m_i 两两互素，有 $M \mid (x' - x)$，即 $x' - x \equiv 0 \pmod{M}$，所以 $x' \pmod{M} = x \pmod{M}$。

（定理4-9证毕）

中国剩余定理提供了一个非常有用的特性，即在模 M（$M = \prod_{i=1}^{k} m_i$）下可将大数 由一组小数$(a_1, a_2, \cdots, a_k)$ 表达，且大数的运算可通过小数实现。表示为：

$$A \leftrightarrow (a_1, a_2, \cdots, a_k)$$

其中 $a_i = A \bmod m_i \ (i = 1, \cdots, k)$，则有以下推论：

推论：

如果 $A \leftrightarrow (a_1, a_2, \cdots, a_k)$，　$B \leftrightarrow (b_1, b_2, \cdots, b_k)$

那么

$$(A+B) \bmod M \leftrightarrow ((a_1+b_1) \bmod m_1, \cdots, (a_k+b_k) \bmod m_k)$$

$$(A-B) \bmod M \leftrightarrow ((a_1-b_1) \bmod m_1, \cdots, (a_k-b_k) \bmod m_k)$$

$$(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, \cdots, (a_k \times b_k) \bmod m_k)$$

证明 可由模运算的性质直接得出。

【例4-18续】表4-3的构造：

设 $1 \leqslant x \leqslant 15$，求 $a \equiv x \bmod 3, b \equiv x \bmod 5$，将 x 填入表的 a 行、b 列。表建立完成后，数 x 可由它的行号 a 和列号 b ，按中国剩余定理如下恢复：

$$x \equiv \left[a \cdot 5 \cdot \left(5^{-1} \bmod 3\right) + b \cdot 3 \cdot \left(3^{-1} \bmod 5\right)\right] \bmod 15 \equiv \left[a \cdot 5 \cdot 2 + b \cdot 3 \cdot 2\right] \bmod 15$$
$$\equiv \left[10a + 6b\right] \bmod 15$$

例如，$12 \bmod 3 \equiv 0, 12 \bmod 5 \equiv 2$；$13 \bmod 3 \equiv 1, 13 \bmod 5 \equiv 3$。所以12位于表中第0行、第2列，13位于表中第1行、第3列。反之若求表中第0行、第2列的数，将$a = 0, b = 2$带入$x \equiv \left[10a + 6b\right] \bmod 15$，得$x = 12$。

已知数x的行号a和列号b，可将x表示为(a, b)。x的运算用(a, b)实现。设$x_1 = (a_1, b_1), x_2 = (a_2, b_2)$，则$x_1 + x_2 = (a_1 + a_2, b_1 + b_2), x_1 \cdot x_2 = (a_1 \cdot a_2, b_1 \cdot b_2)$。

例如12=(0, 2),13=(1, 3), 12+13=(0, 2)+(1, 3)=(1, 0), 12·13=(0, 2)·(1, 3)=(0, 1), 所以12+13为10，12·13为6。

【例4-19】 由以下方程组求 x

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 7 \end{cases}$$

解：

$M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$，$M_1 = 105$，$M_2 = 70$，$M_3 = 42$，$M_4 = 30$，

易求 $e_1 \equiv M_1^{-1} \bmod 2 \equiv 1$，$e_2 \equiv M_2^{-1} \bmod 3 \equiv 1$，$e_3 \equiv M_3^{-1} \bmod 5 \equiv 3$，

$e_4 \equiv M_4^{-1} \bmod 7 \equiv 4$，

所以 $x \bmod 210 \equiv (105 \times 1 \times 1 + 70 \times 1 \times 2 + 42 \times 3 \times 3 + 30 \times 4 \times 5) \bmod 210 \equiv 173$

或写成 $x \equiv 173 \bmod 210$ 。

【例4-20】

为将973mod1813由模数分别为37和49的两个数表示，

可取　　$x=973,\quad M=1813, m_1=37, m_2=49$

由 $a_1 \equiv 973 \bmod m_1 \equiv 11,\ a_2 \equiv 973 \bmod m_2 \equiv 42$ 得，x 在模37和模49下的表达为（11，42）。

若要求 $973 \bmod 1813 + 678 \bmod 1813$，可先求出

$$678 \leftrightarrow (678 \bmod 37,\ 678 \bmod 49) = (12,\ 41)$$

从而可将以上加法表达为

$$((11+12) \bmod 37, (42+41) \bmod 49) = (23, 34)$$

4.1.9 离散对数

1. 指标

首先回忆一下一般对数的概念，指数函数 $y=a^x\ (a>0, a\neq 1)$ 的逆函数称为以 a 为底 x 的对数，记为 $y=\log_a(x)$。

对数函数有以下性质：

$$\log_a(1)=0,$$

$$\log_a(a)=1,$$

$$\log_a(xy)=\log_a(x)+\log_a(y),\ \log_a(x^y)=y\log_a(x)$$

在模运算中也有类似的函数。设 p 是一素数，a 是 p 的本原根，则 产生出1到 p-1之间的所有值，且每一值只出现一次。

因此对任意 $b \in \{1, \cdots, p-1\}$，都存在唯一的 $i(1 \le i \le p-1)$，使得 $b \equiv a^i \bmod p$。

称 i 为模 p 下以 a 为底 b 的指标，记为 $i = \mathrm{ind}_{a,p}(b)$。

指标有以下性质：

(1) $\mathrm{ind}_{a,p}(1) = 0;$

(2) $\mathrm{ind}_{a,p}(a) = 1;$

这两个性质分别由以下关系可得：

$$a^0 \bmod p = 1 \bmod p = 1, a^1 \bmod p = a \quad 。$$

以上假定模数 p 是素数，对于非素数也有类似结论，看下例。

【例4-21】

设 $p=9$，则 $\varphi(p)=6$，$a=2$ 是 p 的一个本原根，a 的不同的幂为（模9下）：

$$2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1$$

由此可得 的指数表如表4-4（a）所示。

表4-4(a) 模9下2的指数表

指标	0	1	2	3	4	5
指数	1	2	4	8	7	5

重新排列表4-4（a），可求每一与9互素的数的指标如表4-4（b）所示。

表4-4(b) 与9互素的数的指标

数	1	2	4	5	7	8
指标	0	1	2	5	4	3

在讨论指标的另两个性质时，需要如下定理：

定理4-10

若 $a^z \equiv a^q \bmod p$，其中 p 为素数，a 是 p 的本原根，则有 $z \equiv q \bmod \varphi(p)$ 。

证明

因 a 和 p 互素，所以 a 在模 p 下存在逆元 a^{-1} ，在 $a^z \equiv a^q \bmod p$ 两边同乘以 $\left(a^{-1}\right)^q$ ，得 $a^{z-q} \equiv 1 \bmod p$ 。

因 a 是 p 的本原根，a 的阶为 $\varphi(p)$ ，所以存在一整数 k，使得 $z-q \equiv k\varphi(p)$ ，所以 。

（定理4-10证毕）

由定理4-10可得指标的以下两个性质：

(3) $\mathrm{ind}_{a,p}(xy)=[\mathrm{ind}_{a,p}(x)+\mathrm{ind}_{a,p}(y)]\bmod\varphi(p)$；

(4) $\mathrm{ind}_{a,p}(y^r)=[r\times\mathrm{ind}_{a,p}(y)]\bmod\varphi(p)$。

证明

(3)设 $x\equiv a^{\mathrm{ind}_{a,p}(x)} \bmod p$, $y\equiv a^{\mathrm{ind}_{a,p}(y)} \bmod p$, $xy\equiv a^{\mathrm{ind}_{a,p}(xy)} \bmod p$,

由模运算的性质得：

$$a^{\mathrm{ind}_{a,p}(xy)} \bmod p=(a^{\mathrm{ind}_{a,p}(x)} \bmod p)(a^{\mathrm{ind}_{a,p}(y)} \bmod p)=(a^{\mathrm{ind}_{a,p}(x)+\mathrm{ind}_{a,p}(y)}) \bmod p$$

所以

$$\mathrm{ind}_{a,p}(xy)=[\mathrm{ind}_{a,p}(x)+\mathrm{ind}_{a,p}(y)]\bmod\varphi(p)$$

性质(4)是性质(3)的推广。

从指标的以上性质可见，指标与对数的概念极为相似，将指标称为**离散对数**，如下所述。

2.离散对数

设 p 是素数，a 是 p 的本原根，即 $a^1, a^2, \cdots, a^{p-1}$ 在 $\bmod p$ 下产生 $1 \sim p-1$ 的所有值，所以对 $\forall b \in \{1, \cdots, p-1\}$，有唯一的 $i \in \{1, \cdots, p-1\}$ 使得 $b \equiv a^i \bmod p$。称 i 为模 p 下以 a 为底 b 的离散对数，记为 $i \equiv \log_a(b) (\bmod p)$ 。

当a，p，i 已知时，用快速指数算法可比较容易地求出 b，但如果已知 a，b 和 p，求 i 则非常困难。目前已知的最快的求离散对数算法其时间复杂度为：

$$O\left(\exp\left((\ln p)^{1/3} \ln(\ln p)\right)^{2/3}\right)$$

所以当 p 很大时，该算法也是不可行的。

4.1.10 二次剩余

设 n 是正整数，a 是整数，满足 $\gcd\{a,n\}=1$，称 a 是模 n 的**二次剩余**，如果方程

$$x^2 \equiv a \pmod{n}$$

有解。否则称为**二次非剩余**。

【例4-22】

$x^2 \equiv 1 \bmod 7$ 有解：x=1，x=6；

$x^2 \equiv 2 \bmod 7$ 有解：x=3，x=4；

$x^2 \equiv 3 \bmod 7$ 无解；

$x^2 \equiv 4 \bmod 7$ 有解：x=2，x=5；

$x^2 \equiv 5 \bmod 7$ 无解；

$x^2 \equiv 6 \bmod 7$ 无解；

可见共有3个数（1、2、4）是模7的二次剩余，且每个二次剩余都有两个平方根（即例中的 x）。

容易证明，若 p 是素数，则模 p 的二次剩余的个数为 $(p-1)/2$，且与模 p 的二次非剩余的个数相等。

如果 a 是模 p 的一个二次剩余，那么 a 恰有两个平方根，一个在 $0\sim(p-1)/2$ 之间，另一个在 $(p-1)/2\sim p-1$ 之间，且这两个平方根中的一个也是一个模 p 二次剩余。

定义4-6

设 p 是素数，a 是一整数，符号 $\left(\frac{a}{p}\right)$ 的定义如下：

$$\left(\frac{a}{p}\right)=\begin{cases}0 & \text{如果 } a \text{ 被 } p \text{ 整除}\\ 1 & \text{如果 } a \text{ 是模 } p \text{ 的平方剩余}\\ -1 & \text{如果 } a \text{ 是模 } p \text{ 的非平方剩余}\end{cases}$$

称符号 $\left(\frac{a}{p}\right)$ 为Legendre符号。

【例4-23】

$$\left(\frac{1}{7}\right)=\left(\frac{2}{7}\right)=\left(\frac{4}{7}\right)=1\text{，}\quad\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=\left(\frac{6}{7}\right)=-1\text{。}$$

计算 $\left(\frac{a}{p}\right)$ 有一个简单公式：$\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \bmod p$

【例4-24】

$p=23, a=5, a^{(p-1)/2} \bmod p = 5^{11} \bmod p = -1$，所以 5 不是模23的二次剩余。

Legendre符号有以下性质：

定理4-11 设 p 是奇素数，a 和 b 都不能被 p 除尽，则

(1) 若 $a \equiv b \bmod p$，则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$；

(2) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$；

(3) $\left(\frac{a^2}{p}\right)=1$；

(4) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$。

以下定义的Jacobi符号是Legendre符号的推广。

定义4-7

设 n 是正整数，且 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，定义Jacobi符号为

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{a_1}\left(\frac{a}{p_2}\right)^{a_2}\cdots\left(\frac{a}{p_k}\right)^{a_k}$$

其中右端的符号是Legendre符号。

当 n 为素数时，Jacobi符号就是Legendre符号。

Jacobi符号有以下性质：

定理4-12

设 n 是正合数，a 和 b 是与 n 互素的整数，则

(1) 若 $a \equiv b \bmod n$ ，则 $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$ ；

(2) $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ ；

(3) $\left(\frac{ab^2}{n}\right)=\left(\frac{a}{n}\right)$ ；

(4) $\left(\frac{a+n}{n}\right)=\left(\frac{a}{n}\right)$ 。

对一些特殊的，Jacobi符号可如下计算：

$$\left(\frac{1}{n}\right)=1,\quad \left(\frac{-1}{n}\right)=(-1)^{(n-1)/2},\quad \left(\frac{2}{n}\right)=(-1)^{(n^2-1)/8}$$

定理4-13（Jacobi符号的互反律）

设 m、n 均为大于 2 的奇数，则

$$\left(\frac{m}{n}\right)=(-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

若 $m\equiv n\equiv 3 \bmod 4$，则 $\left(\frac{m}{n}\right)=-\left(\frac{n}{m}\right)$；否则 $\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)$。

以上性质表明：

为了计算Jacobi符号（包括Legendre符号作为它的特殊情形），我们并不需要求素因子分解式。

例如105虽然不是素数，在计算Legendre符号 $\left(\frac{105}{317}\right)$ 时，可以先把它看作Jacobi符号来计算，由上述两个定理得：

$$\left(\frac{105}{317}\right)=\left(\frac{317}{105}\right)=\left(\frac{2}{105}\right)=1$$

一般在计算$\left(\frac{m}{n}\right)$时，如果有必要，可用$m \bmod n$ 代替m，而互反律用以减小 $\left(\frac{m}{n}\right)$中的 n 。

可见，引入Jacobi符号对计算Legendre符号是十分方便的，但应强调指出Jacobi符号和Legendre符号的本质差别是： Jacobi符号$\left(\frac{a}{n}\right)$不表示方程 $x^2 \equiv a \bmod n$ 是否有解。

例如 $n = p_1 p_2$ ，a 关于 p_1 和 p_2 都不是二次剩余，即 $x^2 \equiv a \bmod p_1$ 和 $x^2 \equiv a \bmod p_2$ 都无解，由中国剩余定理知 $x^2 \equiv a \bmod n$也无解。

但是由于 $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = -1$ ，所以 $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) = 1$ 。

即 $x^2 \equiv a \bmod n$ 虽无解，但Jacobi符号 $\left(\frac{a}{n}\right)$ 却为1。

【例4-25】

考虑方程 $x^2 \equiv 2 \bmod 3599$，由于 $3599 = 59 \times 61$，所以方程等价于方程组

$$\begin{cases} x^2 \equiv 2 \bmod 59 \\ x^2 \equiv 2 \bmod 61 \end{cases}$$

由于 $\left(\frac{2}{59}\right) = -1$，所以方程组无解，但Jacobi符号

$$\left(\frac{2}{3599}\right) = (-1)^{\left(3599^2-1\right)/8} = 1$$

下面考虑公钥密码体制中一个非常重要的问题。

设 n 是两个大素数 p 和 q 的乘积。由上述结论，$1\sim p-1$ 之间有一半数是模 p 的平方剩余（记这些数的集合为 Q_p）另一半是模 p 的非平方剩余（记这些数的集合为 NQ_p），对 q 也有类似结论（分别记两个集合为 Q_p 和 NQ_p）。

另一方面，a 是模 n 的平方剩余，当且仅当 a 既是模 p 的平方剩余也是模 q 的平方剩余，即 $a\in Q_p\cap Q_q$ 。

所以对满足 $0<a<n,\gcd\{a,n\}=1$ 的 a ，有一半满足 $\left(\frac{a}{n}\right)=1$（$a\in Q_p\cap Q_q$ 或 $a\in NQ_p\cap NQ_q$），另一半满足 $\left(\frac{a}{n}\right)=-1$（$a\in Q_p\cap NQ_q$ 或 $a\in NQ_p\cap Q_q$）。

而在满足$\left(\frac{a}{n}\right)=1$的$a$中，有一半满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$（$a\in Q_p\cap Q_q$），这些$a$就是模$n$的**平方剩余**；

另一半满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$（$a\in NQ_p\cap Q_q$），这些$a$是模$n$的**非平方剩余**。

设a是模n的平方剩余，即存在x使得$x^2\equiv a \bmod n$成立，因a既是模p的平方剩余，又是模q的平方剩余，所以存在y、z，使得$(\pm y)^2\equiv a \bmod p, (\pm z)^2\equiv a \bmod q$，当$p\equiv q\equiv 3 \bmod 4$时，$y$和$z$可容易地求出（看4.5节）。因此

$$x\equiv \pm y \bmod p,\ x\equiv \pm z \bmod q$$

由中国剩余定理可求得x，即为$a \bmod n$的四个平方根。

以上结果表明，已知 n 的分解 $n=pq$，且 a 是模 n 的平方剩余，就可求得 $a \bmod n$ 的四个平方根。

下面考虑相反的问题，即已知 $a \bmod n$ 的两个不同的平方根（ $u \bmod n$ 和 $w \bmod n$ ，且 $u \not\equiv \pm w \bmod n$ ），就可分解 n 。

事实上由 $u^2 \equiv w^2 \bmod n$ 得 $(u+w)(u-w) \equiv 0 \bmod n$ ，但 n 既不能整除 $u+w$ 也不能整除 $u-w$ ，否则由 $n \mid (u+w)$ 或 $n \mid (u-w)$ 得 $u \equiv -w \bmod n$ 或 $u \equiv w \bmod n$。

由 $(u+w)(u-w) \equiv 0 \bmod n$ 得 $p \mid (u+w)(u-w)$ 及 $q \mid (u+w)(u-w)$，所以必有 $p \mid (u+w)$ 或 $p \mid (u-w)$ 及 $p \mid (u+w)$ 或 $p \mid (u-w)$ 。

当 $p|(u+w)$ 时，必有 $q\nmid(u+w)$ ，否则 $n=pq|(u+w)$ 。所以当 $p|(u+w)$ 时，必有 $q|(u-w)$ 。

同理当 $p|(u-w)$ 时，必有 $q|(u+w)$ 。

在第一种情况下　$\gcd\{n,u+w\}=p,\quad \gcd\{n,u-w\}=q$

在第二种情况下　$\gcd\{n,u-w\}=p,\quad \gcd\{n,u+w\}=q$

因此得到了 n 的两个因子。

将以上讨论总结为：

定理4-14

当 $p\equiv q\equiv 3 \bmod 4$ 时，求解方程 $x^2\equiv a \bmod n$ 与分解 n 是等价的。

当 $p\equiv q\equiv 3 \bmod 4$ 时，$a \bmod n$ 的两个不同的平方根 u 和 w 的Jacobi符号有如下关系：$\left(\frac{u}{n}\right)=-\left(\frac{w}{n}\right)$

证明

由以上讨论知，u 、w 满足

$$p|(u+w),\quad q|(u-w)\quad 或\quad p|(u-w),\quad q|(u+w)$$

即 $u \equiv -w \bmod p,\ u \equiv w \bmod q$

或 $u \equiv w \bmod p,\ u \equiv -w \bmod q$ 。

若为第一种情况，

$$\left(\frac{u}{n}\right)=\left(\frac{u}{p}\right)\left(\frac{u}{q}\right)=\left(\frac{-w}{p}\right)\left(\frac{w}{q}\right)=\left(\frac{-1}{p}\right)\left(\frac{w}{p}\right)\left(\frac{w}{q}\right)$$

设 $p=4k+3$ ，则 $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2} \bmod p=(-1)^{2k+1} \bmod p=-1$ 所以上式等于 $-\left(\frac{w}{p}\right)\left(\frac{w}{q}\right)=-\left(\frac{w}{n}\right)$ 同理可证 第二种情况。

（定理4-14证毕）

4.1.11 循环群

定理4-15（Lagarange定理）

有限群 G 的任意子群 H 的阶整除群的阶，即 $|H|\|G|$。

定理4-16 循环群的子群是循环群。

证明

设 H 是循环群 $G=\{g^i|i=1,\cdots\}$ 的子群，k 是使得 $g^k\in H$ 的最小正整数。对任一 $a=g^i\in H$，令 $i=qk+r\ (0\le r<k)$，则 $g^i=(g^k)^q g^r$，$g^r=g^i(g^{qk})^{-1}\in H$。

所以 $r=0$，否则与 k 的最小性矛盾。

所以 $g^i=(g^k)^q$，是由 g^k 生成的循环子群。

（定理4-16证毕）

定理4-17 设G是n阶有限群，a是G中任一元素，有$a^n=e$。

证明 设$\mathrm{H}=\{e,a,a^2,\cdots,a^{r-1}\}$，其中$r$是$a$的阶，易证$\langle \mathrm{H},\bullet\rangle$是$\langle \mathrm{G},\bullet\rangle$的子群，由Lagarange定理，$|\mathrm{H}|\,|\,|\mathrm{G}|$，$r|n$，存在正整数$t$，使得$n=rt$。所以$a^n=(a^r)^t=e$。

（定理4-17证毕）

定理4-18 素数阶的群是循环群，且任一与单位元不同的元素是生成元。

证明 设$\langle \mathrm{G},\bullet\rangle$是群，且$|\mathrm{G}|=p$（$p$为素数）。任取$a\in\mathrm{G}$，$a\neq e$，构造$\mathrm{H}=\{e,a,a^2,\cdots\}$，易知H是G的子群（同定理4-16）。设$|\mathrm{H}|=n$，则$n\neq 1$。由Lagarange定理，$n|p$，所以$n=p$，$\mathrm{H}=\mathrm{G}$。所以G是循环群，$n$是生成元。

（定理4-18证毕）

定理4-19

设 a^r 是 n 阶循环群 $\Gamma=\langle a\rangle$ 中任一元素，$d=\gcd\{n,r\}$。那么 $\mathrm{ord}_n(a^r)=\frac{n}{d}$。

证明 由 $d=\gcd\{n,r\}$，$d\mid n$ 且 $d\mid r$。

设 $n=dq_1, r=dq_2$，其中 $q_1=\frac{n}{d}, q_2=\frac{r}{d}$，且 $\gcd\{q_1,q_2\}=1$。

首先 $(a^r)^{\frac{n}{d}}=(a^{dq_2})^{\frac{n}{d}}=a^{q_2 n}=(a^n)^{q_2}=e^{q_2}=e$。设 $\mathrm{ord}_n(a^r)=k$，则 $k\mid\frac{n}{d}$。其次，由 $(a^r)^k=e$，可得 $n\mid rk$，两边同除以 d，得 $\frac{n}{d}\mid\frac{r}{d}k$，但 $(\frac{n}{d},\frac{r}{d})=1$，所以 $\frac{n}{d}\mid k$。

所以 $k=\frac{n}{d}$，$\mathrm{ord}_n(a^r)=\frac{n}{d}$。

（定理4-19证毕）

定理4-20

在 n 阶循环群 $\Gamma=\langle a\rangle$ 中，a^r 是生成元当且仅当 $(r,n)=1$。

证明

设 $\gcd\{n,r\}=d$。若 a^r 是生成元，则有 $\mathrm{ord}_n(a^r)=n$。

但由定理4-19，$\mathrm{ord}_n(a^r)=\frac{n}{d}$，所以有 $\frac{n}{d}=n, d=1$，即 $\gcd\{n,r\}=1$。

反之若 $d=\gcd\{n,r\}=1$，则 $\mathrm{ord}_n(a^r)=\frac{n}{d}=n$，$a^r$ 是生成元。

（定理4-20证毕）

4.1.12循环群的选取

在实际应用中经常需要使用群生成算法产生一系列循环群，群的描述包括一个有限的循环群 $\hat{G}$ 以及 $\hat{G}$ 的素数阶的子群 G 、G 的生成元 g、G 的阶 q ，用 $\Gamma[\hat{G},G,g,q]$ 表示群的描述，其上的运算有：

- 乘法运算—为确定性的多项式时间算法，输入$\Gamma[\hat{G},G,g,q]$及 $h_1,h_2 \in \hat{G}$,输出 $h_1 \bullet h_2 \in \hat{G}$ 。
- 求逆运算—为确定性的多项式时间算法，输入$\Gamma[\hat{G},G,g,q]$及 $h \in \hat{G}$,输出 $h^{-1} \in \hat{G}$。
- 子群判定运算—为确定性的多项式时间算法，输入$\Gamma[\hat{G},G,g,q]$及 $h \in \hat{G}$,输出 $h \in \hat{G}$。

- 求生成元及子群的阶—为确定性的多项式时间算法，输入 $\Gamma[\hat{G},G,g,q]$，输出 g 和 q 。

有些群不存在求子群的阶的多项式时间算法，比如对合数 n，群 Z_n^*。

实际应用中，经常使用的循环群有以下几类

(1)设 $l_1(\kappa),l_2(\kappa)$ 是安全参数 κ 的多项式有界的整数函数，满足 $1<l_1(\kappa)<l_2(\kappa)$，$\Gamma[\hat{G},G,g,q]$ 由三元组 (q,p,g) 表示，其中

- q 是一个 $l_1(\kappa)$ 比特长的随机素数。
- q 是一个 $l_2(\kappa)$ 比特长的随机素数，满足 $p\equiv 1 \bmod q$。
- g 是 G 的随机生成元。

其含义为循环群 $\hat{G} \equiv Z_p^*$，G是 $\hat{G}$ 的阶为 q 的唯一子群。

Z_p^* 中的元素能用 $l_2(\kappa)$ 长的比特串表示，其上的元素乘法运算可用模 p 乘法运算，求逆运算可使用推广的欧几里得算法，判断元素 $\alpha \bmod p \in Z_p^*$ 是否属于子群G 可通过判断 $\alpha^q \equiv 1 \bmod p$ 是否成立。

G的随机生成元 g 可如下产生：产生 Z_p^* 的随机元素，求它的 $\frac{p-1}{q}$ 次幂，如果求幂后得到 $1 \bmod p$，则重新选取 Z_p^* 的另一随机元素，重复上述过程。

(2)除了 $p = 2q+1$，其余参数与1的群相同，此时关于 Z_p^* 的 q 阶子群 G 有以下结论。

定理4-21　当 $p=2q+1$ 时，Z_p^* 的 q 阶子群 G 是二次剩余类子群（即其所有元素都是二次剩余）

证明

若 g 是 Z_p^* 的生成元，对任一 $a\in G$，存在整数 i，使得 $a\equiv g^i \bmod p$。又知 $a^q=1$，所以 $g^{iq}=g^{i\frac{p-1}{2}}=1$，所以 $p-1\mid i\frac{p-1}{2}$，i 一定是偶数，即 a 是二次剩余。

（定理4-21证毕）

因为计算Legendre符号 $\left(\frac{a}{p}\right)$ 比求模指数运算 $\alpha^q\equiv 1 \bmod p$ 容易，所以判断元素 $\alpha \bmod p\in Z_p^*$ 是否属于子群G，可通过判断 $\left(\frac{a}{p}\right)$ 是否等于1。

4.1.13双线性映射

设 q 是一大素数，G_1 和 G_2 是两个阶为 q 的群，其上的运算分别称为加法和乘法。

G_1 到 G_2 的双线性映射 $\hat{e}: G_1 \times G_1 \to G_2$，
满足下面的性质：

(1)双线性：

如果对任意 $P,Q,R \in G_1$ 和 $a,b \in Z$ ，有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ 或 $\hat{e}(P+Q,R)=\hat{e}(P,R)\cdot\hat{e}(Q,R)$ 和 $\hat{e}(P,Q+R)=\hat{e}(P,Q)\cdot\hat{e}(P,R)$ 那么就称该映射为双线性映射。

(2)非退化性：

映射不把 $G_1 \times G_1$ 中的所有元素对（即序偶）映射到 G_2 中的单位元。

由于 G_1, G_2 都是阶为素数的群，这意味着：如果 p 是 G_1 的生成元，那么 $\hat{e}(P,P)$ 就是 G_2 的生成元。

(3)可计算性：

对任意的 $P, Q \in G_1$，存在一个有效算法计算 $\hat{e}(P,Q)$ 。

Weil配对和Tate配对是满足上述三条性质的双线性映射。

第二类双线性映射形如：$\hat{e}:G_1\times G_2\to G_T$，其中$G_1$、$G_2$和$G_T$都是阶为$q$的群，$G_2$到$G_1$有一个同态映射$\psi$：$G_2\to G_1$满足$\psi(g_2)=g_1$，其中$g_1$和$g_2$分别是$G_1$和$G_2$上的固定生成元。

G_1中的元素可用较短的形式表达，因此在构造签名方案时，把签名取为G_1中的元素，可得短的签名。

在构造加密方案时，把密文取为G_1中的元素，可得短的密文。

4.1.14 计算复杂性

对一个密码系统来说，应要求在密钥已知的情况下，加密算法和解密算法是“容易的”，而在未知密钥的情况下，推导出密钥和明文是“困难的”。那么如何描述一个计算问题是“容易的”还是“困难的”？

可用解决这个问题的算法的计算时间和存储空间来描述。

算法的计算时间和存储空间（分别称为算法的时间复杂度和空间复杂度）定义为算法输入数据的长度 n 的函数 $f(n)$。

当 n 很大时，通常只关心 $f(n)$ 随着 n 的无限增大是如何变化的，即**算法的渐近效率**。

渐近效率通常使用以下几种：

1. O 记号

O 记号给出的是 $f(n)$ 的渐近上界。如果存在常数 C 和 N，当 $n>N$ 时，$f(n)\le Cg(n)$，则记 $f(n)=O(g(n))$。所以 O 记号给出的是 $f(n)$ 在一个常数因子内的上界。

例如，$f(n)=8n+10$，则当 $n>N=10$ 时，$f(n)\le 9n$，所以 $f(n)=O(n)$。

一般，若 $f(n)=a_0+a_1n+\cdots+a_kn^k$，则 $f(n)=O(n^k)$。

若算法的时间复杂度为 $T=O(n^k)$，则称该算法是多项式时间的；

若 $T=O(k^{f(n)})$，其中 k 是常数，$f(n)$ 是多项式，就称该算法是指数时间的。

2. O记号

O记号给出的渐近上界可能是渐近紧确的，也可能不是。比如 $2n^2=O(n^2)$ 是渐近紧确的，但$2n=O(n^2)$却不是。

o记号给出的是 $f(n)$ 的非渐近紧确的上界。如果对任意常数C，存在常数N，当 $n>N$ 时，$0\le f(n)\le Cg(n)$，则记 $f(n)=o(g(n))$。

例如$2n=o(n^2), 2n^2\ne o(n^2)$。

直观上看，在 o表示中，当 n 趋于无穷时，$f(n)$ 相对于 $g(n)$ 来说就不重要了，即 $\lim\limits_{n\to\infty}\dfrac{f(n)}{g(n)}=0$

定义4-8

字母表 Σ是一个有限的符号集合，Σ 上的语言 L 是Σ上的符号构成的符号串的集合。

一个图灵机 M 接受一个语言 L 表示为$x \in L \Leftrightarrow M(x)=1$, 这里简单地用 来表示接受。

有两种类型的计算性问题是比较重要的。

第一种是可以在多项式时间内判定的语言集合，表示为 P 。

正式地说，$x \in L$，当且仅当存在图灵机在最多 $p(|x|)$（p 为某个多项式，x 是图灵机的输入串，$|x|$ 表示 x 的长度）步内接受一个输入 x，我们就说语言 L 在 P 中。

第二种是NP类语言，NP问题是指可在多项式时间内验证它的一个解的问题。

即对语言中的元素存在多项式时间的图灵机可验证该元素是否属于该语言。

正式地说，如果存在一个多项式图灵机 M 使得$x \in L$ 当且仅当存在一个串 w_x 使得 $M\left(x, w_x\right)=1$。我们就说语言L 在NP中。w_x 称为 x 的证据，用于证明$x \in L$ 。

因为可在多项式时间内求解就一定可在多项式时间内验证。但反过来不成立，因为求解比验证解更为困难。

用 P 表示所有 P 问题的集合，NP表示所有NP问题的集合，则有 $P \subset NP$ 。

在NP类中，有一部分可以证明比其他问题困难，这一部分问题称为NPC问题。也就是说，NPC问题是NP类中“最难”的问题。

定义4-9

一个函数 $\grave{o}:\mathrm{R}\to[0,1]$ 是可忽略的当且仅当对于 $\forall c>0$，存在一个 $N_c>0$ 使得对于 $\forall N>N_c$,有 $\grave{o}(N)<1/N^c$ 。

直观地，$\grave{o}(\cdot)$ 是可忽略的当且仅当它的增长速度比任何多项式的逆更慢。

一个常见的例子是逆指数 $\grave{o}(k)=2^{-k}$。

对于任意的 c，$2^{-k}=O(1/k^c)$ 。

称一个机器是概率多项式时间的，如果它的运行步数是安全参数的多项式函数，简记为PPT。

定义4-10

设$\mathrm{X}=\{X_k\}$和 $\mathrm{Y}=\{Y_k\}$是两个分布总体，其中 X_k 和 Y_k 是同一空间上的分布（对于所有的 k ）。

X 和 Y 是计算上不可区分的（记为 $\mathrm{X} \overset{c}{\equiv} \mathrm{Y}$ ），如果对于所有PPT敌手，下式是可忽略的：

$$\left|\Pr\left[x \leftarrow_R X_k; \mathrm{A}(x)=1\right]-\Pr\left[y \leftarrow_R Y_k; \mathrm{A}(y)=1\right]\right|$$

一些符号使用说明：如果 S 是集合，则 $x \leftarrow_R S$ 表示从 S 中均匀随机地选取元素 。

如果 $A(\cdot)$ 是随机化算法，则 $x \leftarrow A(\cdot)$ 表示运行 $A(\cdot)$（输入是均匀随机的）得到输出 x 。

$x=f(\cdot)$ 表示将 $f(\cdot)$ 的值赋值给 x 。

概率表达式中 $\mathrm{A}(x)=1$ 表示判断 $\mathrm{A}(x)$ 是否为1。