

第三章 同余

3.1 同余的概念及性质

3.2 剩余类与剩余系

3.3 简化剩余类与简化剩余系

3.4 Euler函数

3.5 Euler定理，Fermat定理及Wilson定理

3.6 求余运算与模运算

3.1 同余的概念及性质

3.1 同余的概念及性质函数

定义1.1 设 $m \neq 0$, $a, b \in \mathbb{Z}$, 若 $m \mid a - b$, 就称 a 与 b 模 m 同余, 记为 $a \equiv b \pmod{m}$ 。称 b 是 a 对模 m 的剩余。否则称 a 与 b 模 m 不同余, 记为 $a \not\equiv b \pmod{m}$ 。

因为 $m \mid a - b$ 等价于 $-m \mid a - b$, 所以以后总假定模数 $m > 0$ 。

定义中如果 $0 \leq b < m$, 则称 b 是 a 对 m 的最小非负剩余。

若 $1 \leq b \leq m$ 则称 b 是 a 对模 m 的最小正剩余; 若 $-\frac{m}{2} < b \leq \frac{m}{2}$ 或 $-\frac{m}{2} \leq b < \frac{m}{2}$, 则称 b 是 a 对模 m 的绝对最小剩余。

定义中 $m \mid a - b$ 等价于存在 $q \in N$ ，使得 $a = b + qm$ ，可得如下等价定义。

定义1.1' 对 $m \in N$ ， $a, b \in Z$ ，若存在 $q \in Z$ ，使得 $a = b + qm$ ，则 $a \equiv b \pmod{m}$ 。

在很多计算中，经常用 **b** (较小) 代替 **a** (较大)。特别地，取 **b** 为 **a** 对模 **m** 的绝对最小剩余，可使计算大为减化。

定理1.1 $a \equiv b \pmod{m}$ 的充要条件是 a 和 b 被 m 除后所得的最小非负余数相等, 即若

$$a = q_1m + r_1, 0 \leq r_1 < m;$$

$$b = q_2m + r_2, 0 \leq r_2 < m;$$

则 $r_1 = r_2$ 。

证明 $a - b = (q_1 - q_2)m + (r_1 - r_2)$, 由 $m \mid a - b$ 得 $m \mid r_1 - r_2$ 。

但 $0 \leq |r_1 - r_2| < m$, 所以必有 $r_1 = r_2$ 。

证毕。

定理1.1的余数相同，正是“同余”的意义所在。下面是同余的性质。

定理1.2 同余是等价关系，即

(1) 自反性: $a \equiv a \pmod{m}$;

(2) 对称性: $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$;

(3) 传递性: $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$;

证明 由 $m \mid a - a$, $m \mid a - b \Leftrightarrow m \mid b - a$, $m \mid a - b$,

$m \mid b - c \Rightarrow m \mid (a - b) + (b - c) = a - c$, 即得。证毕。

定理1.3 同余式可以相加、相乘，即如果 $a \equiv b \pmod{m}$ ，
 $c \equiv d \pmod{m}$ ，则 $a + c \equiv (b + d) \pmod{m}$ ， $ac \equiv (bd) \pmod{m}$ 。

证明 由 $a = b + q_1m$ ， $c = d + q_2m$ 得 $a + c = (b + d) + (q_1 + q_2)m$ ，
 $ac = bd + (bq_2 + cq_1 + q_1q_2m)m$ ，所以 $a + c \equiv (b + d) \pmod{m}$
 $ac \equiv (bd) \pmod{m}$ 。证毕。

定理1.4 设 $f(x) = a_nx^n + \cdots + a_1x + a_0$ ， $g(x) = b_nx^n + \cdots + b_1x + b_0$ ，
满足 $a_i \equiv b_i \pmod{m}$ ($1 \leq i \leq n$)。若 $x_1 \equiv x_2 \pmod{m}$ ，则
 $f(x_1) \equiv g(x_2) \pmod{m}$ 。此时称2个多项式模 m 同余。

证明 反复利用定理1.3即得。证毕。

定理1.5 设 $a \equiv b \pmod{m}$, $d \mid m$, 其中 $d \in N$, 则 $a \equiv b \pmod{d}$

证明 由 $d \mid m, m \mid a - b \Rightarrow d \mid a - b$ 。 证毕。

定理1.6 设 $a \equiv b \pmod{m}$, $d > 0$, 则 $ad \equiv (bd) \pmod{md}$ 。

证明 由 $m \mid a - b, md \mid ad - bd$ 即得。 证毕。

一般地, 由 $ac \equiv bc \pmod{m}$ 不能推出 $a \equiv b \pmod{m}$, 例如 $3 \cdot 6 \equiv 8 \cdot 6 \pmod{10}$, 但 $3 \not\equiv 8 \pmod{10}$ 。但有如下性质。

定理1.7 设 $ca \equiv cb \pmod{m}$, $(c, m) = 1$, 则有 $a \equiv b \pmod{m}$ 。

证明 由 $m \mid ca - cb = c(a - b)$, $(c, m) = 1$ 得 $m \mid a - b$ 。 证毕。

定理1.8 若 $(a, m) = 1$, 则存在 c 使得 $ca \equiv 1 \pmod{m}$ 。称 c 是 a 对模 m 的逆, 记作 $a^{-1} \pmod{m}$ 或 a^{-1} 。

证明 由第1章定理2.4及 $(a, m) = 1$, 存在 $x, y \in N$, 使得 $ax + my = 1$ 。取 $c = x$ 即得。 证毕。

可见由广义Euclid算法, 不仅可以求出 (a, m) , 且当 $(a, m) = 1$ 时, 可求出 $a^{-1} \pmod{m}$ 。

定理 1.8 (补充) 设 m 是一个正整数, a 是满足 $(a, m) = 1$ 的整数, 则存在唯一的整数 a' , $1 \leq a' < m$, 使得, $a \cdot a' \equiv 1 \pmod{m}$.

证一 (存在性证明) 因为 $(a, m) = 1$, 根据定理 2.3.4, k 遍历模 m 的一个最小简化剩余系时, $a \cdot k$ 也遍历模 m 的一个简化剩余系. 因此, 存在整数 $k = a'$, $1 \leq a' < m$ 使得 $a \cdot a'$ 属于 1 的剩余类, 即式 (2.31) 成立.

(唯一性证明) 若有整数 a', a'' $1 \leq a', a'' < m$ 使得

$$a \cdot a' \equiv 1, \quad a \cdot a'' \equiv 1 \pmod{m},$$

则 $a(a' - a'') \equiv 0 \pmod{m}$, 从而, $a' - a'' \equiv 0 \pmod{m}$. 故 $a' = a''$. 证毕.

因为在实际运用中, 常常需要具体地求出整数, 所以运用广义欧几里得除法给出定理 2.3.5 的构造性证明.

证二 (构造性证明) 因为 $(a, m) = 1$, 根据定理 1.3.7, 运用广义欧几里得除法, 可找到整数 s, t 使得

$$s \cdot a + t \cdot m = (a, m) = 1.$$

因此, 整数 $a' = s \pmod{m}$ 满足式 (2.31). 证毕.

定理1.9 设 $a \equiv b \pmod{m_i}$, 其中 $m_i \in N (i=1, \dots, k)$, 当且仅当 $a \equiv b \pmod{[m_1 \cdots m_k]}$ 。

证明 由 $a \equiv b \pmod{m_i}$, 得 $m_i \mid a - b (i=1, \dots, k)$, 所以 $[m_1 \cdots m_k] \mid a - b$, $a \equiv b \pmod{[m_1 \cdots m_k]}$ 。

反之, 由 $m_i \mid [m_1 \cdots m_k] (1 \leq i \leq k)$ 即得。证毕。

例1.1 2019年2月4日是星期一，问第 2^{2019} 天是星期几？

解 因为 $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$, 即2在 mod 7 下求幂时，得到的结果以 2^3 为周期。因 $2019 = 3 \cdot 672 + 3$, 所以 $2^{2019} = (2^3)^{672} \cdot 2^3 \equiv 1 \pmod{7}$, 即第 2^{2019} 天是星期二。

例1.2 求 3^{406} 的个位数。

解 $3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \equiv -1 \pmod{10}$, $3^4 \equiv 1 \pmod{10}$ 。而 $406 = 4 \cdot 101 + 2$, 所以 $3^{406} = (3^4)^{101} \cdot 3^2 \equiv 9 \pmod{10}$
即个位数是 9。

3.2 剩余类与剩余系

3.2 剩余类与剩余系

由定理1.2知，同余是一种等价关系，因此全体整数可按照给定的模 m 是否同余，划分为若干个两两不相交的集合，使得在同一集合中的任意2个数模 m 同余，不同集合中的任意2个数模 m 不同余，这样得到的集合就是模 m 的同余类。

设 $m \in N$ ，对 $\forall a \in Z$ ，定义集合 $[a]_m = \{c \mid c \in Z, c \equiv a \pmod{m}\}$ 。

如果模 m 是清晰的，可将它简记为 $[a]$ 。

$[a]$ 有以下性质。

定理2.1 (1) $[a] = [b] \Leftrightarrow a \equiv b \pmod{m}$ 。

(2) 对 $\forall a, b \in \mathbb{Z}$ ，或者 $[a] = [b]$ ，或者 $[a] \cap [b] = \Phi$ 。

证明 (1) “ \Rightarrow ” $a \in [a] = [b]$ ， $\therefore a \equiv b \pmod{m}$ 。

“ \Leftarrow ” 对 $\forall c \in [a]$ ，得 $c \equiv a \pmod{m}$ 。由 $a \equiv b \pmod{m}$ ，得 $c \equiv b \pmod{m}$ ， $\therefore c \in [b]$ ，即 $[a] \subseteq [b]$ 。同理 $[b] \subseteq [a]$ ，所以 $[a] = [b]$ 。

(2) 若 $[a] \neq [b]$ ，则必有 $[a] \cap [b] = \Phi$ ，否则 $[a] \cap [b] \neq \Phi$ 存在 $c \in [a] \cap [b]$ 。 $c \in [a]$ 且 $c \in [b]$ ，所以 $c \equiv a \pmod{m}$ ， $c \equiv b \pmod{m}$ ，可得 $a \equiv b \pmod{m}$ 。由(1)， $[a] = [b]$ ，矛盾。

证毕。

定义2.1 $[a]$ 称为模 m 下 a 的剩余类。

定理2.2 对 $m \in N$ ，有且仅有 m 个模 m 的剩余类 $[0], [1], \dots, [m-1]$

证明 由定理2.1的(2)， $[0], [1], \dots, [m-1]$ 互不相交。对 $\forall c \in Z$ ，由第1章定理2.1，存在 q, r ，使得 $c = qm + r$ ，其中 $0 \leq r < m$ ，因此 $c \in [r]$ 。证毕。

由定理2.1和2.2知， $[0], [1], \dots, [m-1]$ 形成 Z 的一个划分。

定义2.2 在模 m 的 m 个剩余类 $[0], [1], \dots, [m-1]$ 的每一个中任取一个代表元素，形成一系列数 y_0, y_1, \dots, y_{m-1} ，称为模 m 的一个完全剩余系。

显然，完全剩余系中任2个数模 m 不同余。

因为 $a \equiv b \pmod{m} \Leftrightarrow a = qm + b$ ，即 b 是 a 被 m 除所得的余数，由第1章定理2.1的推论知，余数有各种取法，因此可得以下不同形式的完全剩余系。

(1) $0, 1, \dots, m-1$ 称为模 m 的最小非负完全剩余系。

(2) $1, 2, \dots, m$ 称为模 m 的最小正完全剩余系。

(3) $-(m-1), \dots, -1, 0$ 称为模 m 的最大非正完全剩余系。

(4) $-m, -(m-1), \dots, -1$ 称为模 m 的最大负完全剩余系。

(5) $-\left\lfloor \frac{m}{2} \right\rfloor, \dots, -1, 0, 1, \dots, \left\lfloor \frac{m+1}{2} \right\rfloor - 1$ 称为绝对最小完全剩余系。

在求模指数运算或多项式求模运算时，用绝对最小完全剩余系将使问题简化。

3.3 简化剩余类与简化剩余系

3.3 简化剩余类与简化剩余系

为了引入简化剩余类与简化剩余系，先证明如下定理。

定理3.1 设 $r \in \mathbb{Z}$, $a \in [r]_m$ ，则 $(a, m) = (r, m)$ 。

证明 $a \in [r]_m$, $a \equiv r \pmod{m}$ ，存在 $q \in \mathbb{N}$ ，使得 $a = r + qm$ 。

由第1章定理3.1得 $(a, m) = (r + qm, m) = (r, m)$ 。证毕。

定义3.1 如果 $(r, m) = 1$ ，则 $[r]_m$ 称为模 m 的简化剩余类。

由定理3.1知，简化剩余类 $[r]_m$ 中的每一元素都与 m 互素。

定义3.2 已知模 m 的所有简化剩余类，从每个类中任取一元素构成的一系列数称为模 m 的简化剩余系。

类似于完全剩余系，也有最小非负简化剩余系、最小正简化剩余系、最大非正简化剩余系、最大负简化剩余系、绝对最小简化剩余系等概念。

在定义3.2中取元素时，在模 m 的最小非负完全剩余系 $\{0, 1, \dots, m-1\}$ 中取，可有 $\varphi(m)$ 个取值，因此模 m 的简化剩余系中元素的个数为 $\varphi(m)$ 。

显然，任意给定 $\varphi(m)$ 个与 m 互素的数，只要他们模 m 两两不同余，就一定是模 m 的简化剩余系。在实际应用中常用这个方法判断给定的一系列数是否为简化剩余系。

定理3.2 设 $(a, m) = 1$ ，若 x 遍历模 m 的完全(简化)剩余系，则 ax 也遍历模 m 的完全(简化)剩余系。

证明 设 x_1, \dots, x_s 是模 m 的完全(简化)剩余系(当为完全剩余系时 $s = m$ ，当为简化剩余系时 $s = \varphi(m)$)。当 $(a, m) = 1$ ， ax_1, \dots, ax_s 必定模 m 两两不同余，否则设 $ax_i \equiv ax_j \pmod{m}$ ，其中 $i \neq j$ 。由定理1.7得 $x_i \equiv x_j \pmod{m}$ ，矛盾。因此 ax_1, \dots, ax_s 也是模 m 的完全(简化)剩余系。证毕。

定理3.3 设 $(m_1, m_2) = 1$ ，若 x, y 分别遍历模 m_1 和模 m_2 的完全（简化）剩余系，则 $m_2x + m_1y$ 遍历模 m_1m_2 的完全（简化）剩余系。

证明 先证明完全剩余系的情况。

若 x, y 分别遍历模 m_1 、模 m_2 的完全剩余系, x, y 分别有 m_1, m_2 个取值, 那么 $m_2x + m_1y$ 有 m_1m_2 个取值。下面证明这 m_1m_2 个取值模 m_1m_2 两两不同余, 否则存在 $(x, y) \neq (x', y')$, 但 $m_2x + m_1y \equiv (m_2x' + m_1y') \pmod{m_1m_2}$ 。由定理1.5得 $m_2x + m_1y \equiv (m_2x' + m_1y') \pmod{m_1}$, $m_2x \equiv m_2x' \pmod{m_1}$ 。由 $(m_1, m_2) = 1$ 及定理1.7得 $x \equiv x' \pmod{m_1}$, 类似地 $y \equiv y' \pmod{m_2}$ 。与 $(x, y) \neq (x', y')$ 矛盾。

注： $(x, y) \not\equiv (x', y')$ 意指 $x \not\equiv x' \pmod{m_1}$ ，或 $y \not\equiv y' \pmod{m_2}$ ，或 $x \not\equiv x' \pmod{m_1}$ 且 $y \not\equiv y' \pmod{m_2}$ 。

对于简化剩余系需要证明两点：

(1) 对于满足 $(x, m_1) = 1$ 及 $(y, m_2) = 1$ 的任意 x, y ，有 $(m_2x + m_1y, m_1m_2) = 1$ 。

(2) 对于满足 $(c, m_1m_2) = 1$ 的任意 c ，存在 x, y ，满足 $(x, m_1) = 1$ 及 $(y, m_2) = 1$ ，使得 $c = m_2x + m_1y$ 。

(1) 因为 $(m_2x + m_1y, m_1) = (m_2x, m_1) = (x, m_1) = 1$,
 $(m_2x + m_1y, m_2) = (m_1y, m_2) = (y, m_2) = 1$ 。
所以 $(m_2x + m_1y, m_1m_2) = 1$ 。

(2) 对于模 m_1m_2 简化剩余系中的任一元素 c ，它也是模 m_1m_2 完全剩余系中的元素，由上知，存在 x, y ，使得 $c = m_2x + m_1y$ 。由 $(c, m_1m_2) = 1$ 得 $(c, m_1) = 1$ ， $(c, m_2) = 1$ 。
所以 $1 = (c, m_1) = (m_2x + m_1y, m_1) = (m_2x, m_1) = (x, m_1)$ 。
同理 $(y, m_2) = 1$ 。证毕。

于是

$$nx_j \equiv nx_{j'} \pmod{m},$$

$$my_i \equiv my_{i'} \pmod{n}.$$

注意到 $(m, n) = 1$, 由定理 20 第 (1) 条即得 $x_j \equiv x_{j'} \pmod{m}$, $y_i \equiv y_{i'} \pmod{n}$. 于是 $x_j = x_{j'}$, $y_i = y_{i'}$. 因此定理获证.

3.4 Euler函数

3.4 Euler函数

下面从简化剩余系的角度重新考虑Euler函数的性质。为完整起见，这里重复一下第2章定理4.2。

定理4.1 设 $n \in N$ ，

(1) $\varphi(n)$ 是积性的。

(2) 如果 n 为素数，则 $\varphi(n) = n - 1$ 。如果 $n = p^\alpha$
(p 为素数)，则 $\varphi(n) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$ 。

(3) 如果 $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ ， $\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})$ 。

证明：

(1) $\varphi(1) = 1$ 由定义即得。由定理3.3, 当 x, y 分别遍历模 m_1 和模 m_2 的简化剩余系时, x 有 $\varphi(m_1)$ 个取值, y 有 $\varphi(m_2)$ 个取值, $\varphi(m_1)\varphi(m_2)$ 有 $m_2x + m_1y$ 个取值, 而模 m_1m_2 的简化剩余系有 $\varphi(m_1m_2)$ 个元素。由 $m_2x + m_1y$ 遍历模 m_1m_2 的简化剩余系, 即得 $\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$ 。

(2) 由定义知, $\varphi(p^\alpha)$ 等于满足 $1 \leq r \leq p^\alpha$ 且 $(r, p^\alpha) = 1$ 的 r 的个数。由于 p 是素数, 由 $(r, p^\alpha) = 1$, 必有 $(r, p) = 1$ 。否则若 $(r, p) \neq 1$, 则由第1章例2.3知 $p \mid r$, 从而 r 和 p^α 有公因子 p , 与 $(r, p^\alpha) = 1$ 矛盾。而 $(r, p) = 1$ 当且仅当 $p \nmid r$, 所以由 $(r, p^\alpha) = 1$ 得 $p \nmid r$, 所以 $\varphi(p^\alpha)$ 等于 $1, 2, \dots, p^\alpha$ 中不能被 p 整除的数的个数。由于 $1, 2, \dots, p^\alpha$ 中能被 p 整除的数是 $p, 2p, \dots, (p^{\alpha-1})p$, 有 $p^{\alpha-1}$ 个, 所以 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$

(3) 证明同第2章定理4.1。

例4.1 设 $n = pq$ ，其中 p, q 是2个不同的大素数，求 $\varphi(n)$ 。

解 由于 p, q 是不同的素数，所以 $(p, q) = 1$ ，

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

$$= pq - (p + q) + 1 = n - (p + q) + 1。$$

例4.2 已知 n, p, q 如上，证明分解 n （即由 n 求出 p, q ）与求 $\varphi(n)$ 是等价的。

证明 由例4.1， $p + q = n + 1 - \varphi(n)$ ，又知 $pq = n$ ，由一元二次方程根与系数的关系得 p, q 是方程 $x^2 - (n + 1 - \varphi(n))x + n = 0$ 的解。因此已知 $\varphi(n)$ ，就可得该方程的2个解 p, q ，反之已知 p, q ，由例4.1可得 $\varphi(n)$ 。

3.5 Euler定理, Fermat定理及Wilson定理

3.5 Euler定理, Fermat定理及Wilson定理

在实际应用中, 常常需要考虑 $a^k \bmod m$ 形式的计算, 称之为模指数运算。在 k 不断增大时, 若该运算呈周期, 就可由一个周期内的运算得到所有的结果。下面的Euler定理给出运算的一个周期。

定理5.1 (Euler小定理) 设 $m \in N$, $a \in Z$, 满足 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。

证明 取 $r_1, \dots, r_{\varphi(m)}$ 是模 m 的一组简化剩余系, 由定理3.2, 当 $(a, m) = 1$ 时, $ar_1, \dots, ar_{\varphi(m)}$ 也是模 m 的一组简化剩余系, 即 $ar_1, \dots, ar_{\varphi(m)}$ 是 $r_1, \dots, r_{\varphi(m)}$ 的某个排列, 所以 $(ar_1) \cdots (ar_{\varphi(m)}) \equiv r_1 \cdots r_{\varphi(m)} \pmod{m}$ 由于 $(1 \leq i \leq \varphi(m))$, $r_i^{-1} \pmod{m}$ 存在, 因此两边可约去 r_i , 得 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。

证毕。

例5.1 $m=9$, $a=2$ 有 $(2,9)=1$, $\varphi(9)=6$, $2^6 \equiv 1 \pmod{9}$ 。

定理5.2 (Fermat定理) 设 p 为素数, 则对 $\forall a \in \mathbb{Z}$, 有 $a^p \equiv a \pmod{p}$

证明 分两种情形讨论。

(1) 当 $p \mid a$ 时, $a \pmod{p} = 0$, $a^p \equiv 0 \pmod{p}$, 结论成立。

(2) 当 $p \nmid a$ 时, 此时 $(a, p)=1$, 由定理5.1, $a^{\varphi(p)} \equiv 1 \pmod{p}$,
即 $a^{p-1} \equiv 1 \pmod{p}$, 两边同乘 a , 即得。 证毕。

推论 设 m 是奇整数, 如果 $(a, m)=1$ 且 $a^{m-1} \not\equiv 1 \pmod{m}$, 则
 m 是合数。

证明 此推论为定理5.2的逆否命题。 证毕。

3.6 求余运算与模运算

3.6 求余运算与模运算

在实际应用中，已知模数 m 时，常将剩余系或简化剩余系（如果 m 为素数）取为最小非负完全（简化）剩余系 $0, 1, \dots, m-1$ ，将使得讨论的问题变得简单。

在带余数除法 $a = qm + r$ 中，将 r 记为 $a \bmod m$ 。由 a, m 求 $a \bmod m$ 的运算称为求余运算，它将整数 a 映射到最小非负完全（简化）剩余系 $0, 1, \dots, m-1$ 。求余运算在最小非负完全（简化）剩余系中的运算称为模运算，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: $[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$,

$$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n \text{ 。}$$

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

记 $Z_m = \{0, 1, \dots, m-1\}$ 。

例6.1 $Z_8 = \{0, 1, 2, \dots, 7\}$ ，考虑 Z_8 上的模加法和模乘法，结果如表4-1所示。

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	6	4	2
7	0	7	6	5	4	3	2	1

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

记 $Z_m^* = \{a \mid 0 < a < m, (a, m) = 1\}$ 。由定理1.8知， Z_m^* 中每一元素都有乘法逆元。

例6.1 RSA算法是1978年由R. Rivest, A. Shamir和 L. Adleman提出的一种用数论构造的、也是迄今为止理论上最为成熟完善的公钥密码体制，该体制已得到广泛的应用。算法如下：

1. 密钥的产生:

- (1) 选两个保密的大素数 p 和 q ;
- (2) 计算 $n = p \times q$, $\varphi(n) = (p-1)(q-1)$, 其中 $\varphi(n)$ 是 n 的 Euler 函数值;
- (3) 选一整数 e , 满足 $1 < e < \varphi(n)$, 且 $(\varphi(n), e) = 1$;
- (4) 计算 d , 满足 $d \cdot e \equiv 1 \pmod{\varphi(n)}$, 即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元。因 e 与 $\varphi(n)$ 互素, 由模运算可知, 它的乘法逆元一定存在;
- (5) 以 $\{e, n\}$ 为公开钥, $\{d, n\}$ 为秘密钥。

2. 加密: 设明文 a 是不大于 n 的整数, 以 $c \equiv a^e \pmod{n}$ 作为加密后的密文。

3. 解密: 计算 $c^d \pmod{n}$ 。

证明:

如果 $p \nmid m$, 根据费马小定理, 则 $m^{p-1} = 1 \pmod p$, 又因为

$$p-1 \mid \Phi(n)$$

$$\text{有 } m^{k\Phi(n)+1} = m \pmod p;$$

如果 $p \mid m$, 则 $m = 0 \pmod p$ 且 $m^{k\Phi(n)+1} = m \pmod p$,

综上 $m^{k\Phi(n)+1} = m \pmod p$ 。

同理可得 $m^{k\Phi(n)+1} = m \pmod q$ 。

因为 p, q 互素, 由定理3.1.9及定理1.2.9得,

$$m^{k\Phi(n)+1} = m \pmod n。$$

下面证明 $c^d \equiv a \pmod{n}$ ，即解密的确恢复出明文 a 。

证明 由 $ed \equiv 1 \pmod{\varphi(n)}$ ，存在 $k \in \mathbb{N}$ ，使得 $ed = k\varphi(n) + 1$ 。

当 $c \equiv a^e \pmod{n}$ 时， $c^d \equiv a^{ed} \pmod{n} \equiv a^{k\varphi(n)+1}$ 。

下面分两种情况讨论：

(1) $(a, n) = 1$, 由Euler定理 $a^{\varphi(n)} \equiv 1 \pmod n$, 所以
 $a^{k\varphi(n)+1} \pmod n \equiv (a^{\varphi(n)})^k a \pmod n \equiv a$ 。

(2) $(a, n) \neq 1$, 先看 $(a, n) = 1$ 的含义, 由 $n = pq$, 知
 $(a, p) = 1$ 且 $(a, q) = 1$, 即 $p \nmid a$ 且 $q \nmid a$, 所以 $(a, n) \neq 1$ 意味着 $p \mid a$ 或 $q \mid a$ 。不妨设 $p \mid a$, 即存在 $t \in N$, 使得 $a = tp$ 。

此时必有 $(q, a) = 1$ ，否则 a 也是 q 的倍数，因而是 $n = pq$ 的倍数，与 $a < n$ 矛盾。由 $(q, a) = 1$ 及 Fermat 定理得 $a^{\varphi(q)} \equiv 1 \pmod{q}$ 两边做 $k \frac{\varphi(n)}{\varphi(q)}$ 次幂得 $a^{k\varphi(n)} \equiv 1 \pmod{q}$ ， $a^{k\varphi(n)+1} \equiv a \pmod{q}$ 。

同理， $a^{k\varphi(n)+1} \equiv a \pmod{p}$ 。由定理 1.9 及第 1 章定理 2.9 得 $a^{k\varphi(n)+1} \equiv a \pmod{n}$ ，即 $c^d \equiv a \pmod{n}$ 。证毕。

定理6.1 设 $(a, m) = 1$, 则 $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$ 。

证明 由Euler定理 $a^{\varphi(m)} \equiv 1 \pmod{m}$, 所以 $a \cdot a^{\varphi(m)-1} \equiv a^{\varphi(m)} \equiv 1 \pmod{m}$,
即 $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$ 。 证毕。

推论 设 $(a, m) = 1$, 则方程 $ax \equiv b \pmod{m}$ 的解为
$$x \equiv ba^{-1} \pmod{m} \equiv ba^{\varphi(m)-1} \pmod{m} 。$$

当 m 很大且不知道其分解式时, $\varphi(m)$ 不易求出, 此时求 a^{-1} 还是用广义Euclid算法。

3.7 模指数运算

3.7 模指数运算

模指数运算是指已知 $a, n, m \in N$ ，求 $a^n \bmod m$ ，如果按其含义直接计算，则中间结果非常大，有可能超出计算机所允许的整数取值范围。如上例中解密运算 $66^{77} \bmod 119$ ，先求 66^{77} 再取模，则中间结果就已远远超出了计算机允许的整数取值范围。而用模运算的性质：

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

就可减小中间结果。

再者，考虑如何提高加、解密运算中指数运算的有效性。例如求 x^{16} ，直接计算的话需做15次乘法。然而如果重复对每个部分结果做平方运算即求 x, x^2, x^4, x^8, x^{16} ，则只需4次乘法。

下面的快速算法首先将 n 写成二进制形式

$$n = b_k 2^k + b_{k-1} 2^{k-1} + \cdots + b_1 2 + b_0, \text{ 其中 } b_i \in \{0, 1\}, i = 0, 1, \cdots, k。$$

$$\text{那么 } a^n = \left(\left(\cdots \left(\left(a^{b_k} \right)^2 a^{b_{k-1}} \right)^2 \cdots \right) a^{b_1} \right)^2 a^{b_0}。$$

$$\text{例如 } 100 = 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0，$$

$$a^{100} = ((((((a)^2 a)^2)^2)^2 a)^2)^2。$$

所以计算的中间结果为 $a, a^3, a^6, a^{12}, a^{24}, a^{25}, a^{50}, a^{100}$ 。

取中间结果的初值为 $c = 1$ ，它的值的变化如表7.1所示。

表7.1 快速指数算法中间结果示例

i	b_i	c	运算
6	1	$c = c^2 a$	平方，乘法
5	1	$c = c^2 a$	平方，乘法
4	0	$c = c^2$	平方
3	0	$c = c^2$	平方
2	1	$c = c^2 a$	平方，乘法
1	0	$c = c^2$	平方
0	0	$c = c^2$	平方

从表7.1可见，对每一 $i = 6, 5, 4, 3, 2, 1, 0$ ，如果 $b_i = 1$ ，则对中间结果做平方，再乘以 a 。如果 $b_i = 0$ ，则仅对中间结果做平方。

因此得算法如下：

(1) 将 n 表示成二进制形式 $n = b_k b_{k-1} \cdots b_1 b_0$ ；

(2) 初值 $c = 1$ ；

(3) For $i = k$ downto 0 do

$$c = c^2 \bmod m$$

$$\text{if } b_i = 1 \text{ then } c = (ca) \bmod n$$

(4) 返回 c 。

例7.1 求 $7^{560} \bmod 561$

解 560的二进制为1000110000中间结果如表7.2所示

表7.2 快速指数算法示例

<i>i</i>	初值	9	8	7	6	5	4	3	2	1	0
<i>b_i</i>		1	0	0	0	1	1	0	0	0	0
<i>c</i>	1	7	49	157	526	160	241	298	166	67	1

所以 $7^{560} \bmod 561 = 1$ 。