第3章 同　余

3.1 同余的概念及性质

定义 3.1.1　设 $m\neq 0, a, b\in \mathbf{Z}$。若 $m\mid a-b$，就称 a 与 b 模 m 同余，记为 $a\equiv b \bmod m$，称 b 是 a 对模 m 的剩余；否则称 a 与 b 模 m 不同余，记为 $a\not\equiv b \bmod m$。

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

在定义 3.1.1 中，如果 $0\leqslant b<m$，则称 b 是 a 对模 m 的最小非负剩余；若 $1\leqslant b\leqslant m$，则称 b 是 a 对模 m 的最小正剩余；若 $-\frac{m}{2}<b\leqslant\frac{m}{2}$ 或 $-\frac{m}{2}\leqslant b<\frac{m}{2}$，则称 b 是 a 对模 m 的绝对最小剩余。

定义 3.1.1 中的 $m\mid a-b$ 等价于：存在 $q\in\mathbf{N}$，使得 $a=b+qm$。可得如下等价定义。

定义 3.1.1′　对 $m\in\mathbf{N}, a, b\in\mathbf{Z}$，若存在 $q\in\mathbf{Z}$，使得 $a=b+qm$，则 $a\equiv b \bmod m$。

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，可使计算大为简化。

定理 3.1.1　$a\equiv b \bmod m$ 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

$$a = q_1 m + r_1,\quad 0\leqslant r_1 < m$$
$$b = q_2 m + r_2,\quad 0\leqslant r_2 < m$$

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 $0\leqslant|r_1-r_2|<m$，所以必有 $r_1=r_2$。　证毕。

定理 3.1.1 的余数相同，正是“同余”的意义所在。下面是同余的性质。

定理 3.1.2　同余是等价关系，即同余具有以下 3 个性质。

(1) 自反性：$a\equiv a \bmod m$。

(2) 对称性：$a\equiv b \bmod m\Leftrightarrow b\equiv a \bmod m$。

(3) 传递性：$a\equiv b \bmod m, b\equiv c \bmod m\Rightarrow a\equiv c \bmod m$。

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

定理 3.1.3　同余式可以相加、相乘，即，如果 $a\equiv b \bmod m, c\equiv d \bmod m$，则 $a+c\equiv(b+d) \bmod m, ac\equiv(bd) \bmod m$。

证明　由 $a=b+q_1 m, c=d+q_2 m$ 得

$$a+c=(b+d)+(q_1+q_2)m$$
$$ac=bd+(bq_2+cq_1+q_1q_2m)m$$

所以

$$a+c\equiv(b+d)\bmod m,\quad ac\equiv(bd)\bmod m$$

证毕。

定理 3.1.4 设 $f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0$，$g(x)=b_nx^n+\cdots+b_2x^2+b_1x+b_0$，满足 $a_i\equiv b_i \bmod m(1\leqslant i\leqslant n)$。若 $x_1\equiv x_2 \bmod m$，则 $f(x_1)\equiv g(x_2) \bmod m$。此时称两个多项式模 m 同余。

证明 反复利用定理 3.1.3 即得。 证毕。

定理 3.1.5 设 $a\equiv b \bmod m$，$d|m$，其中 $d\in\mathbf{N}$，则 $a\equiv b \bmod d$。

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

定理 3.1.6 设 $a\equiv b \bmod m$，$d>0$，则 $ad\equiv(bd) \bmod (md)$。

证明 由 $m|a-b$，$md|ad-bd$ 即得。 证毕。

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

定理 3.1.7 设 $ca\equiv cb \bmod m$，$(c,m)=1$，则有 $a\equiv b \bmod m$。

证明 由 $m|ca-cb=c(a-b)$，$(c,m)=1$ 可得 $m|a-b$。 证毕。

定理 3.1.8 若 $(a,m)=1$，则存在 c 使得 $ca\equiv 1 \bmod m$。称 c 是 a 对模 m 的逆元，记作 $a^{-1} \bmod m$ 或 a^{-1}。

证明 由定理 1.2.4 及 $(a,m)=1$ 可知，存在 $x,y\in\mathbf{Z}$，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)，而且当 $(a,m)=1$ 时，还可以求出 $a^{-1} \bmod m$。

定理 3.1.9 $a\equiv b \bmod m_i$，其中 $m_i\in\mathbf{N}(i=1,2,\cdots,k)$，当且仅当 $a\equiv b \bmod [m_1m_2\cdots m_k]$。

证明

必要性：由 $a\equiv b \bmod m_i$，得 $m_i|a-b(i=1,2,\cdots,k)$，所以 $[m_1m_2\cdots m_k]|a-b$，$a\equiv b \bmod [m_1m_2\cdots m_k]$。

充分性：由 $m_i|[m_1m_2\cdots m_k](1\leqslant i\leqslant k)$ 即得。 证毕。

例 3.1.1 2019 年 2 月 4 日是星期一。从该天数起，第 2^{2018} 天是星期几？

解 因为 $2^1\equiv 2 \bmod 7$，$2^2\equiv 4 \bmod 7$，$2^3\equiv 1 \bmod 7$，即 2 在模 7 下求幂时，得到的结果以 2^3 为周期。因 $2018=3\cdot 672+2$，所以 $2^{2018}=(2^3)^{672}\cdot 2^2\equiv 4 \bmod 7$，即第 2^{2018} 天是星期五。

例 3.1.2 求 3^{406} 的个位数。

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

3.2　剩余类与剩余系

由定理 3.1.2 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两个数模 m 同余，不同集合中的任意两个数模 m 不同余，这样得到的集合就是模 m 的同余类。

设 $m\in\mathbf{N}$，对任意的 $a\in\mathbf{Z}$，定义集合 $[a]_m=\{c\mid c\in\mathbf{Z},c\equiv a \bmod m\}$。如果模 m 是清晰的，可将它简记为 $[a]$。

$[a]$ 有以下性质。

定理 3.2.1

(1) $[a]=[b]\Leftrightarrow a\equiv b \bmod m$。

(2) 对任意的 $a,b\in\mathbf{Z}$，或者 $[a]=[b]$，或者 $[a]\cap[b]=\varnothing$。

证明

(1) 先证明“⇒”。$a\in[a]=[b]$，所以 $a\equiv b \bmod m$。

再证明“⇐”。对 $\forall c\in[a]$，得 $c\equiv a \bmod m$。由 $a\equiv b \bmod m$，得 $c\equiv b \bmod m$，所以 $c\in[b]$，即 $[a]\subseteq[b]$。同理 $[b]\subseteq[a]$，所以 $[a]=[b]$。

(2) 若 $[a]\neq[b]$，则必有 $[a]\cap[b]=\varnothing$，否则存在 $c\in[a]\cap[b]$。$c\in[a]$ 且 $c\in[b]$，所以 $c\equiv a \bmod m$，$c\equiv b \bmod m$，可得 $a\equiv b \bmod m$。由(1)，$[a]=[b]$，矛盾。　　证毕。

定义 3.2.1　$[a]$ 称为模 m 下 a 的剩余类。

定理 3.2.2　对 $m\in\mathbf{N}$，有且仅有 m 个模 m 的剩余类 $[0],[1],[2],\cdots,[m-1]$。

证明　由定理 3.2.1 的(2)，$[0],[1],[2],\cdots,[m-1]$ 互不相交。对任意的 $c\in\mathbf{Z}$，由定理 1.2.1，存在 q、r，使得 $c=qm+r$，其中 $0\leqslant r<m-1$，因此 $c\in[r]$。　　证毕。

由定理 3.2.1 和定理 3.2.2 知，$[0],[1],[2],\cdots,[m-1]$ 形成 $\mathbf{Z}$ 的一个划分。

定义 3.2.2　在模 m 的 m 个剩余类 $[0],[1],[2],\cdots,[m-1]$ 的每一个中任取一个代表元素，形成一列数：$y_0,y_1,y_2,\cdots,y_{m-1}$，称为模 m 的一个完全剩余系。

显然，完全剩余系中任意两个数模 m 不同余。

因为 $a\equiv b \bmod m\Leftrightarrow a=qm+b$，即 b 是 a 被 m 除所得的余数，由定理 1.2.1 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) $0,1,2,\cdots,m-1$，称为模 m 的最小非负完全剩余系。

(2) $1,2,\cdots,m$，称为模 m 的最小正完全剩余系。

(3) $-(m-1),-(m-2),\cdots,-1,0$，称为模 m 的最大非正完全剩余系。

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

(5) $-\left\lfloor\frac{m}{2}\right\rfloor,\cdots,-1,0,1,\cdots,\left\lfloor\frac{m+1}{2}\right\rfloor-1$ 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，使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

为了引入简化剩余类与简化剩余系，先证明如下定理。

定理 3.3.1 设 $r\in\mathbf{Z}$，$a\in[r]_m$，则$(a,m)=(r,m)$。

证明 $a\in[r]_m$，$a\equiv r \bmod m$，存在 $q\in\mathbf{N}$，使得 $a=r+qm$。由定理 1.3.1 得$(a,m)=(r+qm,m)=(r,m)$。 证毕。

定义 3.3.1 如果$(r,m)=1$，则$[r]_m$ 称为模 m 的简化剩余类。

由定理 3.3.1 知，简化剩余类$[r]_m$ 中的每一个元素都与 m 互素。

定义 3.3.2 已知模 m 的所有简化剩余类，从每个类中任取一个元素构成的一列数称为模 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 3.3.2 中取元素时，在模 m 的最小非负完全剩余系$\{0,1,2,\cdots,m-1\}$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，只要它们两两模 m 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列数是否为简化剩余系。

定理 3.3.2 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 $x_1,x_2,\cdots,x_s$ 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$(a,m)=1$ 时，$ax_1,ax_2,\cdots,ax_s$ 必定两两模 m 不同余，否则设 $ax_i\equiv ax_j \bmod m$，其中 $i\neq j$。由定理 3.1.7 得 $x_i\equiv x_j \bmod m$，矛盾。因此 $ax_1,ax_2,\cdots,ax_s$ 也是模 m 的完全(简化)剩余系。 证毕。

定理 3.3.3 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，则 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 个取值两两模 m_1m_2 不同余，否则存在 $(x,y)\not\equiv(x',y')$，但 $m_2x+m_1y\equiv(m_2x'+m_1y') \bmod m_1m_2$ 的情况。由定理 3.1.5 得

$$m_2x+m_1y\equiv(m_2x'+m_1y') \bmod m_1,\quad m_2x\equiv m_2x' \bmod m_1$$

由$(m_1,m_2)=1$ 及定理 3.1.7 得 $x\equiv x' \bmod m_1$，类似地可得 $y\equiv y' \bmod m_2$。这与$(x,y)\not\equiv(x',y')$矛盾。

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

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

$c=m_2x+m_1y$。

证明

(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) 模 m_1m_2 简化剩余系中的任一元素 c 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，

$$1=(c,m_1)=(m_2x+m_1y,m_1)=(m_2x,m_1)=(x,m_1)$$

同理可得 $(y,m_2)=1$。　　证毕。

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，这里重新给出定理 2.4.2。

定理 3.4.1　设 $n\in\mathbf{N}$。

(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

$$\varphi(n)=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right)$$

(3) 如果 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则

$$\varphi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$$

证明

(1) $\varphi(1)=1$ 由定义 2.4.1 即得。由定理 3.3.3，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，m_2x+m_1y 有 $\varphi(m_1)\varphi(m_2)$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，即可得 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$。

(2) 由定义 2.4.1 知，$\varphi(p^\alpha)$等于满足 $1\leqslant r\leqslant p^\alpha$ 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 $(r,p)\neq1$，则由例 1.2.3 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 $1,2,\cdots,p^\alpha$ 中不能被 p 整除的数的个数。由于 $1,2,\cdots,p^\alpha$ 中能被 p 整除的数是 $p,2p,\cdots,(p^{\alpha-1})p$，有 $p^{\alpha-1}$个，所以

$$\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}=p^\alpha\left(1-\frac{1}{p}\right)$$

证毕。

(3) 证明同定理 2.4.1。

例 3.4.1 设 $n=pq$,其中 p、q 是两个不同的大素数,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 3.4.2 已知 n、p、q 如例 3.4.1,证明分解 n(即由 n 求出 p、q)与求 $\varphi(n)$是等价的。

证明 由例 3.4.1,$p+q=n+1-\varphi(n)$,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 $\varphi(n)$,就可得该方程的两个解 p、q;反之,已知 p、q,由例 3.4.1 可得 $\varphi(n)$。

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,若该运算呈现周期性,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 3.5.1(Euler 定理) 设 $m\in\mathbf{N}$,$a\in\mathbf{Z}$,满足$(a,m)=1$,则 $a^{\varphi(m)}\equiv 1 \bmod m$。

证明 取 $r_1,r_2,\cdots,r_{\varphi(m)}$ 是模 m 的一个简化剩余系,由定理 3.3.2,当$(a,m)=1$ 时,$ar_1,ar_2,\cdots,ar_{\varphi(m)}$ 也是模 m 的一个简化剩余系,即 $ar_1,ar_2,\cdots,ar_{\varphi(m)}$ 是 $r_1,r_2,\cdots,r_{\varphi(m)}$ 的某个排列,所以 $ar_1ar_2\cdots ar_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)} \bmod m$。由于$(r_i,m)=1(1\leqslant i\leqslant\varphi(m))$,$r_i^{-1} \bmod m$ 存在,因此两边可约去 r_i,得 $a^{\varphi(m)}\equiv 1 \bmod m$。 证毕。

例 3.5.1 $m=9$,$a=2$,有$(2,9)=1$,$\varphi(9)=8$,$2^8\equiv 1 \bmod 9$。

定理 3.5.2(Fermat 定理) 设 p 为素数,则对任意的 $a\in\mathbf{Z}$,有 $a^p\equiv a \bmod p$。

证明 分两种情形讨论。

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

(2) 当 $p\nmid a$ 时,此时$(a,p)=1$,由定理 3.5.1,$a^{\varphi(p)}\equiv 1 \bmod p$,即 $a^{p-1}\equiv 1 \bmod p$,两边同时乘以 a,即得。 证毕。

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

证明 此推论为定理 3.5.2 的逆否命题。 证毕。

定理 3.5.3(Wilson 定理) 设 p 是素数,则$(p-1)!\equiv -1 \bmod p$。

证明 $p=2$ 时,结论显然成立。

下面假设 $p\geqslant 3$。取模 p 的一个简化剩余系 $r_1,r_2,\cdots,r_{p-1}$,对每一个 $r_i(1\leqslant i\leqslant p-1)$,由定理 3.1.8,存在 $r_j(1\leqslant j\leqslant p-1)$,使得 $r_ir_j\equiv 1 \bmod p$。而 $r_i=r_j$ 的充要条件是 $r_i^2\equiv 1 \bmod p$,即$(r_i+1)(r_i-1)\equiv 0 \bmod p$。所以 $r_i\equiv 1 \bmod p$ 或 $r_i\equiv -1 \bmod p$。但两式不能同时成立,否则,$r_i=q_1p+1=q_2p-1$,其中 $q_1,q_2\in\mathbf{N}$,所以$(q_2-q_1)p=2$,与 $p\geqslant 3$ 矛盾。在 $r_1,r_2,\cdots,r_{p-1}$中不妨设 $r_1\equiv 1 \bmod p$,$r_{p-1}\equiv -1 \bmod p$,其余的 r_i 和其逆元两两

配对，即得

$$r_1 r_{p-1} \prod (r_i r_j) \equiv -1 \bmod p$$

证毕。

例 3.5.2　设 $p=13$，取 $r_j=j(1\leqslant j\leqslant 12)$，有

$$2\cdot 7 \equiv 3\cdot 9 \equiv 4\cdot 10 \equiv 5\cdot 8 \equiv 6\cdot 11 \equiv 1 \bmod 13$$

所以

$$\begin{aligned} &1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12 \\ =&1\cdot 12\cdot (2\cdot 7)\cdot (3\cdot 9)\cdot (4\cdot 10)\cdot (5\cdot 8)\cdot (6\cdot 11) \\ \equiv&-1 \bmod 13 \end{aligned}$$

例 3.5.3　设 p 为素数，证明

$$1^2\cdot 3^2\cdot \cdots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$$

证明

$$\begin{aligned} (p-1)!=&[1\cdot (p-1)][3\cdot (p-3)]\cdot \cdots \cdot [(p-2)\cdot (p-(p-2))] \\ =&(-1)^{\frac{p-1}{2}}\cdot 1^2\cdot 3^2\cdot \cdots \cdot (p-2)^2 \bmod p \end{aligned}$$

所以

$$1^2\cdot 3^2\cdot \cdots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$$

证毕。

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 $0,1,2,\cdots,m-1$，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 $0,1,2,\cdots,m-1$。在最小非负完全（简化）剩余系中的求余运算称为模运算，有以下性质。

（1）交换律：

$$(w+x) \bmod n = (x+w) \bmod n$$
$$(w\cdot x) \bmod n = (x\cdot w) \bmod n$$

（2）结合律：

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

（3）分配律：

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

记 $\mathbf{Z}_m=\{0,1,2,\cdots,m-1\}$。

例 3.6.1　$\mathbf{Z}_8=\{0,1,2,\cdots,7\}$，考虑 $\mathbf{Z}_8$ 上的模加法和模乘法，如表 3.6.1 所示。

表 3.6.1　$\mathbf{Z}_8$ 上的模 8 运算

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

从加法结果可见，对每一个 x，都有一个 y，使得 $x+y\equiv 0 \bmod 8$。例如，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。

记 $\mathbf{Z}_m^*=\{a\mid 0<a<m,(a,m)=1\}$。由定理 3.1.8 知，$\mathbf{Z}_m^*$ 中的每个元素都有乘法逆元。

例 3.6.2　RSA 算法是在 1978 年由 R. Rivest、A. Shamir 和 L. Adleman 提出的，它是用数论构造的、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。RSA 算法包括密钥的产生、加密和解密 3 部分。

(1) 密钥的产生。

① 选两个保密的大素数 p 和 q。

② 计算 $n=p\cdot q$，$\varphi(n)=(p-1)(q-1)$，其中 $\varphi(n)$ 是 n 的 Euler 函数值。

③ 选一个整数 e，满足 $1<e<\varphi(n)$，且 $(\varphi(n),e)=1$。

④ 计算 d，满足 $d\cdot e\equiv 1 \bmod \varphi(n)$，即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元。因 e 与 $\varphi(n)$ 互素，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 $c\equiv a^e \bmod n$ 作为加密后的密文。

(3) 解密。计算 $c^d \bmod n$。

下面证明 $c^d\equiv a \bmod n$，即解密的确能恢复出明文 a。

证明　由 $ed\equiv 1 \bmod \varphi(n)$，存在 $k\in\mathbf{N}$，使得 $ed=k\varphi(n)+1$。当 $c\equiv a^e \bmod n$ 时，$c^d\equiv a^{ed} \bmod n\equiv a^{k\varphi(n)+1} \bmod n$。

下面分两种情况讨论：

(1) $(a,n)=1$，由 Euler 定理得 $a^{\varphi(n)}\equiv 1 \bmod n$，所以

$$a^{k\varphi(n)+1}\equiv (a^{\varphi(n)})^k a \bmod n\equiv a \bmod n$$

(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 $t\in\mathbf{N}$，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 $a^{\varphi(q)}\equiv 1 \bmod q$，对两边求 $k\dfrac{\varphi(n)}{\varphi(q)}$ 次幂，得

$$a^{k\varphi(n)}\equiv 1 \bmod q,\quad a^{k\varphi(n)+1}\equiv a \bmod q$$

同理，$a^{k\varphi(n)+1}\equiv a \bmod p$。由定理 3.1.9 及定理 1.2.9 得 $a^{k\varphi(n)+1}\equiv a \bmod n$，即 $c^d\equiv a \bmod n$。　　证毕。

定理 3.6.1　设$(a,m)=1$，则 $a^{-1}\equiv a^{\varphi(m)-1} \bmod m$。

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

推论　设$(a,m)=1$，则方程 $ax\equiv b \bmod m$ 的解为

$$x \equiv ba^{-1} \bmod m \equiv ba^{\varphi(m)-1} \bmod m$$

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

3.7　模指数运算

已知 $a,n,m\in\mathbf{N}$，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。例如 RSA 算法中的解密运算 $66^{77} \bmod 119$，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：

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

就可减小中间结果。

另外，考虑如何提高加密、解密运算中指数运算的有效性。例如求 x^{16}，直接计算时需做 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}，则只需做 4 次乘法。

上面的快速运算方法就是模指数运算。

在应用模指数运算时，首先将 n 写成二进制形式：

$$n = b_k 2^k + b_{k-1}2^{k-1} + \cdots + b_1 2 + b_0$$

其中，$b_i\in\{0,1\}$，$i=0,1,2,\cdots,k$。那么，

$$a^n = ((\cdots((a^{b_k})^2 a^{b_{k-1}})^2\cdots)a^{b_1})^2 a^{b_0}$$

例如：

$$100 = 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0$$

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

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 $c=1$，它的中间结果如表 3.7.1 所示。

表 3.7.1　模指数运算的中间结果示例

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

从表 3.7.1 可见，对每一个($i=6,5,4,3,2,1,0$)，如果 $b_i=1$，则对中间结果做平方运算，再乘以 a；如果 $b_i=0$，则仅对中间结果做平方运算。

因此，模指数运算的算法如下：

(1) 将 n 表示成二进制形式：$n=b_kb_{k-1}\cdots b_1b_0$。

(2) 取初值：$c=1$。

(3) 执行以下循环：

```
for i=k downto 0 do
      c=c^2 mod m
      if b_i=1 then c=(ca) mod n
```

(4) 返回 c。

例 3.7.1 求 $7^{560} \bmod 561$。

解 560 的二进制形式为 1000110000，取中间结果的初值为 $c=1$。对它应用模指数运算的中间结果如表 3.7.2 所示。

表 3.7.2 例 3.7.1 模指数运算的中间结果

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

所以，$7^{560} \bmod 561=1$。

习 题

1. 设素数 $p\nmid a$，$k\geqslant 1$。证明：$n^2\equiv an \bmod p^k$ 成立的充要条件是 $n\equiv 0 \bmod p^k$ 或 $n\equiv a \bmod p^k$。

2. (1) 求 2^{400} 对模 10 的最小非负剩余。

(2) 求 2^{1000} 的十进制表示中的最后两位数字。

(3) 求 9^{9^9} 和 $9^{9^{9^9}}$ 的十进制表示中的最后两位数字。

(4) 求 $(13\ 481^{56}-77)^{28}$ 被 111 除后所得的最小非负余数。

(5) 设 $s=2^k$，$k\geqslant 2$。求 2^s 对模 10 的最小非负剩余。

3. 证明：当 $m>2$ 时，$0^2,1^2,2^2,\cdots,(m-1)^2$ 一定不是模 m 的完全剩余系。

4. 设 $r_1,r_2,\cdots,r_m$ 和 $r_1',r_2',\cdots,r_m'$ 分别是模 m 的两个完全剩余系。证明：当 m 是偶数时，$r_1+r_1',r_2+r_2',\cdots,r_m+r_m'$ 一定不是模 m 的完全剩余系。

5. 设 $m\geqslant 3, r_1, r_2, \cdots, r_s$ 是所有小于 $\frac{m}{2}$ 且和 m 互素的正整数。证明：$-r_s, \cdots, -r_2, -r_1, r_1, r_2, \cdots, r_s$ 及 $r_1, r_2, \cdots, r_s, (m-r_s), \cdots, (m-r_2), (m-r_1)$ 都是模 m 的简化剩余系。由此推出：当 $m\geqslant 3$ 时，$2\mid\varphi(m)$。

6. 设 $(m,n)=1$。证明：$m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \bmod mn$。

7. 设素数 $p>2, a>1$。证明：

(1) a^p+1 的素因子 q 必是 $a+1$ 的因子，或是 $q\equiv 1 \bmod 2p$。

(2) 形如 $2kp+1$ 的素数有无穷多个。

8. 设 p 是奇素数。证明：

(1) $2^2\cdot 4^2\cdots(p-1)^2\equiv(-1)^{\frac{p+1}{2}} \bmod p$。

(2) $\left(\frac{p-1}{2}!\right)^2\equiv(-1)^{\frac{p+1}{2}} \bmod p$。

(3) $(p-1)!!\equiv(-1)^{\frac{p-1}{2}}(p-2)!! \bmod p$。

第4章 同余方程

4.1 同余方程的基本概念

设 $m,n\in\mathbf{N}$,多项式 $f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0$,其中 $a_i\in\mathbf{Z}(i=0,1,2,\cdots,n)$,则

$$f(x)\equiv 0 \bmod m \tag{4.1.1}$$

称为模 m 的同余方程。若 $m\nmid a_n$,则称式(4.1.1)的次数为 n,记为 $\deg f=n$。

若 $x=c$ 使式(4.1.1)成立,则称之为式(4.1.1)的解。此时与 c 模 m 同余的任一整数也是它的解。不同的解的个数称为它的解数。

显然,式(4.1.1)的解及其解数只需要在模 m 的一个完全剩余系中考虑。

例 4.1.1 求方程 $4x^2+27x-12\equiv 0 \bmod 15$ 的解。

解 在多项式求值时,取完全剩余系为绝对最小完全剩余系时,将使计算简化。在模15的绝对最小完全剩余系 $-7,-6,\cdots,-1,0,1,\cdots,6,7$ 中直接演算,可知 $x=-6,3$ 是解,解数是2。

例 4.1.2 求 $4x^2+27x-9\equiv 0 \bmod 15$ 的解。

解 直接演算知该方程无解。

因为 $4x^2+27x-9\equiv x^2+3x-6 \bmod 15$,所以 $4x^2+27x-9\equiv 0 \bmod 15$ 与 $x^2+3x-6\equiv 0 \bmod 15$ 的解和解数相同,但因 x^2+3x-6 的系数小,直接演算更为简单。一般地有以下定理。

定理 4.1.1

(1) 若 $f(x)\equiv g(x) \bmod m$,则式(4.1.1)的解和解数与 $g(x)\equiv 0 \bmod m$ 相同,称这两个同余方程模 m 等价。

(2) 若 $(a,m)=1$,则式(4.1.1)的解和解数与方程 $af(x)\equiv 0 \bmod m$ 相同。特别地,当 $(a_n,m)=1$ 时,取 $a\equiv a_n^{-1} \bmod m$,可使式(4.1.1)的首项系数变为1。

证明 简单,略去。

类似地,有同余方程组的概念。

记 $m_1,m_2,\cdots,m_k\in\mathbf{N}$,$f_1(x),f_2(x),\cdots f_k(x)$ 都为整系数多项式,则

$$\begin{cases} f_1(x)\equiv 0 \bmod m_1 \\ f_2(x)\equiv 0 \bmod m_2 \\ \quad\vdots \\ f_k(x)\equiv 0 \bmod m_k \end{cases} \tag{4.1.2}$$

称为同余方程组。

若 $x=c$ 满足式(4.1.2)，则称之为式(4.1.2)的解，此时与 c 模 $m=[m_1m_2\cdots m_k]$同余的任意整数也是它的解。显然，式(4.1.2)的解及解数只需在模 m 的一个完全剩余系中考虑。

4.2　一次同余方程

若 $m\nmid a$，则方程

$$ax\equiv b \bmod m \tag{4.2.1}$$

称为一次同余方程。

若式(4.2.1)有解，设为 x_0，则存在 $q\in\mathbf{Z}$，使得 $ax_0=b+qm$。可得

$$(a,m)\mid b \tag{4.2.2}$$

即式(4.2.2)是式(4.2.1)有解的必要条件。

例如，在 $4x\equiv 2 \bmod 8$ 中，$(4,8)=4\nmid 2$，该方程一定无解。在 $3x\equiv 2 \bmod 8$ 中，$(3,8)=1\mid 2$，该方程可能有解，在模 8 的绝对最小剩余系 $-3,-2,-1,0,1,2,3,4$ 中逐一验证，知 $x=-2$ 是解，解数为 1。在 $6x\equiv 2 \bmod 8$ 中，$(6,8)=2\mid 2$，在模 8 的绝对最小剩余系中逐一验证，知 -1 和 3 是解，解数是 2。可见式(4.2.1)可能无解，也可能有解，有解时解数可能为 1，也可能大于 1。

定理 4.2.1 给出了式(4.2.2)(也是式(4.2.1))有解的充分条件。

定理 4.2.1　设 $m\nmid a$，$d=(a,m)$，同余方程(4.2.1)有解的充要条件是 $d\mid b$。在有解时，它的解数为 d。又设 x_0 是

$$\frac{a}{d}x\equiv\frac{b}{d} \bmod \frac{m}{d} \tag{4.2.3}$$

的一个解，则式(4.2.1)的 d 个解是 $x_0+\frac{m}{d}t(\bmod m)$，其中 t 为 $0,1,2,\cdots,d-1$。

证明　充分性由以下构造方法给出。

第 1 步：由 $d\mid b$，得 $\frac{b}{d}$ 是整数，构造方程(4.2.3)，显然 $\left(\frac{a}{d},\frac{m}{d}\right)=1$。由定理 3.6.1 的推论，式(4.2.3)有解：

$$x_0\equiv\frac{b}{d}\left(\frac{a}{d}\right)^{-1} \bmod \frac{m}{d}$$

第 2 步：方程 $ax\equiv b \bmod m$ 的全部解为 $x_0+t\frac{m}{d}$，其中 $t\in\mathbf{Z}$，这是因为

$$a\left(x_0+t\frac{m}{d}\right)=ax_0+tm\frac{a}{d}\equiv ax_0 \bmod m$$

又由于

$$\frac{a}{d}x_0\equiv\frac{b}{d} \bmod \frac{m}{d}$$

得 $ax_0\equiv b \bmod m$。所以

$$a\left(x_0+t\frac{m}{d}\right)\equiv b \bmod m$$

下面在全部解中求出模 m 不同余的解。

设

$$x_1=x_0+t_1\frac{m}{d},\quad x_2=x_0+t_2\frac{m}{d}$$

则

$$x_1-x_2=(t_1-t_2)\frac{m}{d}$$

所以 $m|x_1-x_2$ 当且仅当 $d|t_1-t_2$。即 $x_1\not\equiv x_2 \bmod m$ 当且仅当 $t_1\not\equiv t_2 \bmod d$。所以 t 遍历模 d 的一个完全剩余系(可取为最小非负完全剩余系 $0,1,2,\cdots,d-1$)就可得 $ax\equiv b \bmod m$ 的全部解,即全部解有 d 个。 证毕。

推论 设$(a,m)=1$,则方程 $ax\equiv b \bmod m$ 有唯一解 $x\equiv ba^{\varphi(m)-1} \bmod m$。

证明 由$(a,m)=1|b$ 及定理 3.6.1 的推论得解。解的唯一性由$(a,m)=1$ 得。

例 4.2.1 解方程 $20x\equiv 15 \bmod 135$。

解 $d=(20,135)=5,5|15$,所以方程有 5 个解。构造方程 $4x\equiv 3 \bmod 27$,得解为 $3\cdot 4^{\varphi(27)-1}\equiv 21 \bmod 27$。所以方程的 5 个解为 $21+t\cdot 27(t=0,1,2,3,4)$,即 21,48,75,102,129。

4.3 一次同余方程组和中国剩余定理

中国剩余定理有两个用途:

(1) 已知某个数关于一些两两互素的数的同余类,就可重构这个数。

(2) 可将大数用小数表示,大数的运算可通过小数实现。

例 4.3.1 $\mathbf{Z}_{10}$ 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。例如,已知 x 关于 2 和 5 的同余类分别是[0]和[3],即 $x \bmod 2=0$,$x \bmod 15=3$。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 4.3.2 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,$15=3\cdot 5$,将 1～15 的数列表表示,表的行号为 0～2,列号为 0～4,将 1～15 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,如表 4.3.1 所示。例如 $12 \bmod 3=0$,$12 \bmod 5=2$,所以 12 应填在第 0 行、第 2 列。

表 4.3.1 1～15 的数

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

用(0，2)表示 12。现在就可处理 15 以内的数了。

例如，求 12·13(mod 15)，13 在第 1 行、第 3 列，将 13 表示为(1，3)，由 0·1≡0 mod 3，2·3≡1 mod 5 得 12·13(mod 15)的小数表示是(0，1)，这个位置上的数是 6，所以 12·13(mod 15)≡6。又因 0+1≡1 mod 3，2+3≡0 mod 5，所以 12+13 的小数表示是(1，0)，这个位置上的数是 10，所以 12+13≡10 mod 15。

以上两例是中国剩余定理的直观应用。下面具体介绍该定理的内容。

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 3 个余数写成和的形式：2+3+2。为满足第一个方程，即模 3 后，后两项消失，将后两项各乘以 3，得 2+3·3+2·3。为满足第二个方程，即模 5 后，第一、三项消失，将第一、三项各乘以 5，得 2·5+3·3+2·3·5。同理，给前两项各乘以 7，得 2·5·7+3·3·7+2·3·5。

然而，将结果代入第一方程，得到 2·5·7，为消去 5·7，将结果的第一项再乘以$(5\cdot 7)^{-1} \bmod 3$，得 $2\cdot 5\cdot 7(5\cdot 7)^{-1} \bmod 3+3\cdot 3\cdot 7+2\cdot 3\cdot 5$。类似地，将第二项乘以$(3\cdot 7)^{-1} \bmod 5$，将第三项乘以$(3\cdot 5)^{-1} \bmod 7$，结果为

$$2\cdot 5\cdot 7\cdot (5\cdot 7)^{-1} \bmod 3+3\cdot 3\cdot 7\cdot (3\cdot 7)^{-1} \bmod 5$$
$$+2\cdot 3\cdot 5\cdot (3\cdot 5)^{-1} \bmod 7 = 233$$

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

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

把这种构造法推广到一般形式，就是中国剩余定理。

定理 4.3.1(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

$$\begin{cases} x \bmod m_1 \equiv a_1 \\ x \bmod m_2 \equiv a_2 \\ \vdots \\ x \bmod m_k \equiv a_k \end{cases} \tag{4.3.1}$$

对模 M 有唯一解：

$$x \equiv \left(\frac{M}{m_1}e_1a_1+\frac{M}{m_2}e_2a_2+\cdots\frac{M}{m_k}e_ka_k\right) \bmod M \tag{4.3.2}$$

其中，e_i 满足

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

证明 设

$$M_i = \frac{M}{m_i} = \prod_{\substack{l=1 \\ l \neq i}} m_l \quad (i = 1,2,\cdots,k)$$

由 M_i 的定义知 M_i 与 m_i 是互素的，因此 M_i 在模 m_i 下有唯一的乘法逆元，即满足 $\frac{M}{m_i}e_i \equiv 1 \bmod m_i$ 的 e_i 是唯一的。

下面证明对任意 $i \in \{1,2,\cdots,k\}$，上述 x 满足 $x \bmod m_i \equiv a_i$。注意到当 $j \neq i$ 时，$m_i \mid M_j$，即 $M_j \equiv 0 \bmod m_i$，所以

$$(M_j \times e_j \bmod m_j) \bmod m_i \equiv ((M_j \bmod m_j) \times (e_j \bmod m_j) \bmod m_i)) \bmod m_i \equiv 0$$

而

$$(M_i \times (e_i \bmod m_i)) \bmod m_i \equiv (M_i \times e_i) \bmod m_i \equiv 1$$

所以 $x \bmod m_i \equiv a_i$。

下面证明方程组的解是唯一的。

设 x' 是方程组的另一解，即 $x' \equiv a_i \bmod m_i (i = 1,2,\cdots,k)$。由 $x \equiv a_i \bmod m_i$ 得 $x' - x \equiv 0 \bmod m_i$，即 $m_i \mid (x' - x)$。再根据 m_i 两两互素，有 $M \mid (x' - x)$，即 $x' - x \equiv 0 \bmod M$，所以 $x' \bmod M = x \bmod M$。 证毕。

中国剩余定理提供了一个非常有用的特性，即在模 $M\left(M = \prod_{i=1}^{k} m_i\right)$ 下可将大数 A 用一组小数 $(a_1, a_2, \cdots, a_k)$ 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，$a_i = A \bmod m_i (i = 1,2,\cdots,k)$。

有以下推论。

推论 如果

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

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。 证毕。

定理 4.3.2 设 $m_1, m_2, \cdots, m_k, M, e_1, e_2, \cdots, e_k$ 与定理 4.3.1 相同。

$$x = \frac{M}{m_1}e_1x_1 + \frac{M}{m_2}e_2x_2 + \cdots \frac{M}{m_k}e_kx_k \tag{4.3.3}$$

则当 x_i 遍历模 $m_i (i = 1,2,\cdots,k)$ 的完全（简化）剩余系时，x 遍历模 M 的完全（简化）剩余系。

证明 先证明完全剩余系的情况。当 x_i 遍历模 m_i 的完全剩余系时，x_i 有 m_i 个取值 $(1 \leqslant i \leqslant k)$，因此 x 有 M 个取值。下面证明这 M 个取值模 M 两两不同余。设

$$x' = \frac{M}{m_1}e_1x'_1 + \frac{M}{m_2}e_2x'_2 + \cdots + \frac{M}{m_k}e_kx'_k$$

若 $x \equiv x' \bmod M$，则 $x \equiv x' \bmod m_i$，从而得 $x_i \equiv x'_i \bmod m_i (1 \leqslant i \leqslant k)$。

再证明简化剩余系的情况。

由于简化剩余系中的元素是由完全剩余系中与模数互素的元素构成的，所以只要证明$(x,M)=1$当且仅当$(x_i,m_i)=1(1\leqslant i\leqslant k)$。由$(x,M)=1$得$(x,m_i)=1(1\leqslant i\leqslant k)$。否则，若$d=(x,m_i)\neq 1$，则$d|x,d|m_i$得$d|M$。$d$是$x$、$M$的公因子，与$(x,M)=1$矛盾。

由$(x_i,m_i)=1$及式(4.3.3)得$x \bmod m_i\equiv x_i, x_i\in[x]_{m_i}$。由定理 3.3.1 得$(x_i,m_i)=(x,m_i)$，所以$(x_i,m_i)=1$。反之，若$(x_i,m_i)=1(1\leqslant i\leqslant k)$，则$x \bmod m_i\equiv x_i$，得$(x,m_i)=(x_i,m_i)=1,(x,M)=1$。　　证毕。

例 4.3.3　表 4.3.1 的构造。

设$1\leqslant x\leqslant 15$，求$x\equiv a \bmod 3, x\equiv b \bmod 5$，将$x$填入表的$a$行、$b$列。表建立完成后，数$x$由它的行号$a$和列号$b$表示为$(a,b)$。由$(a,b)$及中国剩余定理可按如下的方法恢复$x$：

$$\begin{aligned} x &\equiv (a\cdot 5\cdot (5^{-1} \bmod 3)+(b\cdot 3\cdot (3^{-1} \bmod 5)) \bmod 15\\ &=(a\cdot 5\cdot 2+b\cdot 3\cdot 2) \bmod 15\\ &\equiv [10a+6b] \bmod 15 \end{aligned}$$

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$a=0$，$b=2$代入$x\equiv(10a+6b) \bmod 15$，得$x=12$。

已知x表示为(a,b)，x的运算可用(a,b)实现。设$x_1=(a_1,b_1), x_2=(a_2,b_2)$，则

$$x_1+x_2=(a_1+a_2,b_1+b_2),\quad x_1\cdot x_2=(a_1\cdot a_2,b_1\cdot b_2)$$

例如：

$$12=(0,2),\quad 13=(1,3)$$

$$12+13=(0,2)+(1,3)=(1,0),\quad 12\cdot 13=(0,2)\cdot(1,3)=(0,1)$$

所以 12+13 为 10，12·13 为 6。

例 4.3.4　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　$M=2\cdot 3\cdot 5\cdot 7=210, M_1=105, M_2=70, M_3=42, M_4=30$。

易得

$$\begin{aligned} e_1 &\equiv M_1^{-1} \bmod 2 = 1\\ e_2 &\equiv M_2^{-1} \bmod 3 = 1\\ e_3 &\equiv M_3^{-1} \bmod 5 = 3\\ e_4 &\equiv M_4^{-1} \bmod 7 = 4 \end{aligned}$$

所以，

$$\begin{aligned} x &\equiv (105\times 1\times 1+70\times 1\times 2+42\times 3\times 3+30\times 4\times 5) \bmod 210\\ &\equiv 173 \bmod 210 \end{aligned}$$

例 4.3.5　为将 973 mod 1813 由模数分别为 37 和 49 的两个数表示，可取

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

由$a_1\equiv 973 \bmod m_1=11, a_2\equiv 973 \bmod m_2=42$，得$x$在模 37 和模 49 下的表达式为

(11,42)。若要求 973 mod 1813+678 mod 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

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

例 4.3.6 解方程 $19x\equiv 556 \bmod 1155$。

解 这是一次同余式,可按 4.2 节的方法求解。但因模数 1155 较大,可按中国剩余定理将方程变成模数较小的同余方程组。由 $1155=3\cdot 5\cdot 7\cdot 11$ 及定理 1.1.9,该方程与以下方程组等价:

$$\begin{cases}19x\equiv 556 \bmod 3\\19x\equiv 556 \bmod 5\\19x\equiv 556 \bmod 7\\19x\equiv 556 \bmod 11\end{cases}\overset{(1)}{\Leftrightarrow}\begin{cases}x\equiv 1 \bmod 3\\x\equiv 4 \bmod 5\\5x\equiv 3 \bmod 7\\8x\equiv 6 \bmod 11\end{cases}\overset{(2)}{\Leftrightarrow}\begin{cases}x\equiv 1 \bmod 3\\x\equiv 4 \bmod 5\\x\equiv 2 \bmod 7\\x\equiv 9 \bmod 11\end{cases}$$

由定理 4.3.1 即得 $x\equiv 394 \bmod 1155$。其中第(1)步由定理 4.1.1 的(2)得出,第(2)步由一元同余式解出 $5x\equiv 3 \bmod 7$ 及 $8x\equiv 6 \bmod 11$ 得出。注意,第(1)步中得出的方程组不是定理 4.3.1 中的形式,不能直接应用定理 4.3.1。

例 4.3.7 解同余方程组

$$\begin{cases}x\equiv 3 \bmod 7\\6x\equiv 10 \bmod 8\end{cases}$$

解 解出一次同余式 $6x\equiv 10 \bmod 8$ 的解为 $x\equiv 3,7 \pmod 8$,方程组等价于以下两个方程组:

$$\begin{cases}x\equiv 3 \bmod 7\\x\equiv 3 \bmod 8\end{cases}\quad 及\quad\begin{cases}x\equiv 3 \bmod 7\\x\equiv 7 \bmod 8\end{cases}$$

由定理 4.3.1 得 $x\equiv 3,31 \pmod{56}$。

注: $x\equiv 3,7 \pmod 8$ 表示 $x\equiv 3 \bmod 8$,$x\equiv 7 \bmod 8$。以后常用这种简单记法。

例 4.3.8 在例 3.6.1 的 RSA 加密算法中,按照中国剩余定理,可将解密过程简化如下:解密者已知 p、q,计算

$$d_p\equiv d \bmod (p-1),\quad d_q\equiv d \bmod (q-1)$$

$$a_p\equiv c^{d_p} \bmod p,\quad a_q\equiv c^d \bmod q$$

然后建立以下方程组:

$$\begin{cases}x\equiv a_p \bmod p\\x\equiv a_q \bmod q\end{cases}$$

由中国剩余定理求出 $x \bmod (pq)$ 即为明文 a。这是因为 $d_p=d+k\varphi(p)$,其中 $k\in\mathbf{N}$。

$$a_p\equiv c^{d_p} \bmod p\equiv c^d(a^{\varphi(p)})^k \bmod p\equiv c^d \bmod p$$

$$\equiv(a \bmod n)\bmod p\equiv a \bmod p$$

同理,$a_q\equiv a \bmod q$,因此方程组

$$\begin{cases}x\equiv a_p \bmod p\\x\equiv a_q \bmod q\end{cases}$$

中的 x 即为 a。

$c_d \bmod n$ 的运行时间是 $O(\log d\cdot\log^2 n)$,若 d 与 n 同阶,运行时间为 $O(\log^3 n)$。改

进后算法的加速比是

$$\frac{\log^3 n}{2(\log n/2)^3}=4$$

中国剩余定理也用于解高次同余方程(即 $\deg f\geqslant 2$),解法和解数由定理 4.3.3 给出。

定理 4.3.3　设 $m=m_1m_2\cdots m_k$,其中 $m_i(1\leqslant i\leqslant k)$是两两互素的正整数,则同余方程

$$f(x)\equiv 0 \bmod m \tag{4.3.4}$$

与同余方程组

$$\begin{cases} f(x)\equiv 0 \bmod m_1\\ f(x)\equiv 0 \bmod m_2\\ \quad\vdots\\ f(x)\equiv 0 \bmod m_k \end{cases} \tag{4.3.5}$$

等价。设 T 是式(4.3.4)的解数,T_i 是 $f(x)\equiv 0 \bmod m_i(1\leqslant i\leqslant k)$的解数,则 $T=T_1T_2\cdots T_k$。

证明　设 x_0 是式(4.3.4)的解,即 $f(x_0)=0 \bmod m$,由定理 3.1.5 得 $f(x)\equiv 0 \bmod m_i(1\leqslant i\leqslant k)$,即 x_0 也是式(4.3.5)的解。

反之,设 x_0 是式(4.3.5)的解,即 $f(x)\equiv 0 \bmod m_i(1\leqslant i\leqslant k)$,由定理 3.1.9 得 $f(x_0)\equiv 0 \bmod [m_1,m_2,\cdots,m_k]\equiv 0 \bmod m$,即 x_0 也是式(4.3.4)的解。

设 $f(x)\equiv 0 \bmod m_i$ 的解是 $b_i(1\leqslant i\leqslant k)$,建立以下方程组:

$$\begin{cases} x\equiv b_1 \bmod m_1\\ x\equiv b_2 \bmod m_2\\ \quad\vdots\\ x\equiv b_k \bmod m_k \end{cases} \tag{4.3.6}$$

由中国剩余定理得

$$x_0\equiv\left(\frac{m}{m_1}e_1b_1+\frac{m}{m_2}e_2b_2+\cdots+\frac{m}{m_k}e_kb_k\right)\bmod m \tag{4.3.7}$$

由 $x_0\equiv b_i \bmod m_i$ 得 $f(x_0)\equiv f(b_i)\equiv 0 \bmod m_i$,即 x_0 是式(4.3.5)的解,因此也是式(4.3.4)的解。

若 $b_i(1\leqslant i\leqslant k)$遍历 $f(x)\equiv 0 \bmod m_i$ 的所有解,则 x_0 遍历 $f(x)\equiv 0 \bmod m$ 的所有解,因此 $T=T_1T_2\cdots T_k$。　证毕。

定理 4.3.3 的证明过程也给出了解高次同余方程(4.3.4)的过程:将 m 分解成两两互素的数的乘积,建立方程组(4.3.5),解出该方程组,得一次同余方程组(4.3.6),由中国剩余定理求出的式(4.3.7)即为原方程(4.3.4)的解。通常,可先将 m 分解成标准分解式:$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$,取 $m_i=p_i^{\alpha_i}(1\leqslant i\leqslant k)$,因此一般的高次同余方程的求解就归结为模为素数幂的同余方程的求解。

4.4　模为素数的高次同余方程

本节考虑以下同余方程:

$$f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0=0 \bmod p \tag{4.4.1}$$

其中，p 为素数，$a_0 \in \mathbf{Z}(i=1,2,\cdots,n)$，$p \nmid a_n$。

首先考虑多项式的 Euclid 除法，有以下结论。

定理 4.4.1 设 $f(x)=a_n x^n+\cdots+a_2 x^2+a_1 x+a_0$，$g(x)=x^m+\cdots+b_2 x^2+b_1 x+b_0$，其中 $a_i(1\leqslant i\leqslant n)$，$b_j(1\leqslant j\leqslant m-1)\in\mathbf{Z}$，则存在唯一的整系数多项式 $q(x)$ 和 $r(x)$，使得 $f(x)=q(x)g(x)+r(x)$，满足 $\deg r<\deg g$。

证明 分两种情况讨论：

(1) $n<m$ 时，取 $q(x)=0$，$r(x)=f(x)$。

(2) $n\geqslant m$ 时，对 n 采用数学归纳法证明。

当 $n=m$ 时，因为

$$f(x)-a_n g(x)=(a_{n-1}-a_n b_{n-1})x^{n-1}+\cdots+(a_2-a_n b_2)x^2+(a_1-a_n b_1)x+(a_0-a_n b_0)$$

取 $q(x)=a_n$，$r(x)=f(x)-a_n g(x)$，即得。

假设 $n-1(n-1\geqslant m)$ 时结论成立。则在 n 时，由于

$$f(x)-a_n x^{n-m}g(x)=(a_{n-1}-a_n b_{m-1})x^{n-1}+\cdots+(a_{n-m}-a_n b_0)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_2 x^2+a_1 x+a_0$$

即 $f(x)-a_n x^{n-m}g(x)$ 是 $n-1$ 次多项式。由归纳假设，存在唯一的整系数多项式 $q_1(x)$ 和 $r_1(x)$，使得

$$f(x)-a_n x^{n-m}g(x)=q_1(x)g(x)+r_1(x)$$

其中 $\deg r_1<\deg g$，取 $q(x)=a_n x^{n-m}+q_1(x)$，$r(x)=r_1(x)$ 即得证。唯一性的证明与整数的带余除法类似。 证毕。

定理 4.4.2 同余方程(4.4.1)与一个次数不超过 $p-1$ 的同余式模 p 等价。

证明 由多项式 Euclid 除法，存在唯一的一对 $q(x)$、$r(x)$，使得

$$f(x)\equiv q(x)(x^p-x)+r(x)$$

其中 $\deg r\leqslant p-1$。由 Fermat 定理，对任意 x 有 $x^p-x\equiv 0 \bmod p$，所以 $f(x)\equiv r(x) \bmod p$。 证毕。

以下几个定理的证明过程给出了求式(4.4.1)的等价式的方法。

定理 4.4.3 若同余方程(4.4.1)有 k 个不同的解 $x\equiv c_i \bmod p(1\leqslant i\leqslant k)$，则存在唯一的整系数多项式 $g_k(x)$，使得 $f(x)\equiv(x-c_1)(x-c_2)\cdots(x-c_k)g_k(x) \bmod p$，其中 $g_k(x)$ 的首项系数为 a_n，$\deg g_k=n-k$。

证明 对 $f(x)$ 和 $x-c_1$ 用 Euclid 除法，存在唯一的一对 $g_1(x)$、$r_1(x)$，使得

$$f(x)=(x-c_1)g_1(x)+r_1(x)$$

其中 $\deg r_1=0$，即 $r_1(x)$ 为常数。由 $f(c_1)\equiv r_1(c_1) \bmod p\equiv 0 \bmod p$ 得 $r_1(x)\equiv 0 \bmod p$，所以 $f(x)\equiv(x-c_1)g_1(x) \bmod p$。再由 $f(c_2)\equiv(c_2-c_1)g_1(c_2)\equiv 0 \bmod p$ 得 $g_1(c_2)\equiv 0 \bmod p$，对 $g_1(x)$ 与 $(x-c_2)$ 用 Euclid 除法，得到唯一的 $g_2(x)$，满足 $g_1(x)\equiv(x-c_2)g_2(x) \bmod p$。如此下去，得到 $g_{k-1}(x)=(x-c_k)g_k(x) \bmod p$。所以

$$f(x)\equiv(x-c_1)(x-c_2)\cdots(x-c_k)g_k(x) \bmod p$$

显然 $g_k(x)$ 的首项系数为 a_k，$\deg g_k=n-k$。 证毕。

定理 4.4.4 同余方程(4.4.1)的解数不超过它的次数。