第四讲 初等数论
4

本讲提要

- 同余(续)

1 中国剩余定理(CRT)

$$x \equiv 23(\mathrm{mod}\,105) \Rightarrow \begin{cases} x \equiv 2(\mathrm{mod}\,3) \\ x \equiv 3(\mathrm{mod}\,5) \\ x \equiv 2(\mathrm{mod}\,7) \end{cases}$$

中国剩余定理揭示这一过程是可逆的。

定理1 设m_1，$m_2,\cdots$，m_k是k个两两互素的正整数，$m = m_1 m_2 \cdots m_k$，$m = m_i M_i (i = 1,2,\cdots,\ k)$则同余式组

$$x \equiv b_1(\mathrm{mod}\,m_1),\ x \equiv b_2(\mathrm{mod}\,m_2),\cdots,\ x \equiv b_k(\mathrm{mod}\,m_k)$$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k (\mathrm{mod}\,m),$$

其中

$$M_i' M_i \equiv 1(\mathrm{mod}\,m_i)(i = 1,2,\cdots,\ k)。$$

1 中国剩余定理(CRT) (续)

定理1证明.

由$m = m_i M_i$，有$(M_i, m_i) = 1$，且

$$x \equiv \sum_{j=1}^{k} M_j' M_j b_j \equiv M_i' M_i b_i \equiv b_i \pmod{m_i} \ (i = 1,2,\cdots, \ k),$$

因此，x为同余组的解。

若x_1，x_2同为同余组的解，则

$x_1 \equiv x_2 \pmod{m_i} \ (i = 1,2,\cdots, \ k)$。

因为当$i \neq j$，有$(m_i, m_j) = 1$,

所以$x_1 \equiv x_2 \pmod{m}$ (第二讲定理9)。

2.1 同余定义与概念(续)

定理9 若$a \equiv b(\mathrm{mod}\ m_i)$，$i = 1,2,\cdots,$ n，则

$a \equiv b(\mathrm{mod}\ [m_1, m_2, \cdots, m_n])$。

定理9证明.

可知$m_i \mid a-b$，$i = 1,2,...,$ n。

$a-b$，m_i按标准分解式展开可知 $[m_1, m_2, \cdots, m_n] \mid a-b$。

$\therefore\ a \equiv b(\mathrm{mod}\ [m_1, m_2, \cdots, m_n])$。

1 中国剩余定理(CRT) (续)

定理2 一次同余式组

$$x \equiv b_1 (\mathrm{mod}\, m_1),\ \ x \equiv b_2 (\mathrm{mod}\, m_2), \qquad (1)$$

可解的充分必要条件是$(m_1, m_2) \mid b_1 - b_2$，且当式(1)可解时对模$[m_1, m_2]$有唯一解。

定理2证明.

$\rightarrow$ 如果(1)有公解x_0。令$(m_1, m_2) = d$，显然有 $x_0 \equiv b_1 (\mathrm{mod}\, d)$，$x_0 \equiv b_2 (\mathrm{mod}\, d)$，

因此，$d \mid b_1 - b_2$。

$\leftarrow$ 因为 $x \equiv b_1 (\mathrm{mod}\, m_1)$的解可写为$x = b_1 + m_1 y$，其中$y$为任意整数，代入

$x \equiv b_2 (\mathrm{mod}\, m_2)$，有$m_1 y \equiv b_2 - b_1 (\mathrm{mod}\, m_2)$。因为$(m_1, m_2) = d$，$d \mid b_2 - b_1$，

所以根据上一讲定理11知$m_1 y \equiv b_2 - b_1 (\mathrm{mod}\, m_2)$有解，

且对模$\frac{m_2}{d}$有唯一解$y \equiv y_0 \left(\mathrm{mod} \frac{m_2}{d} \right)$，即$y = y_0 + \frac{m_2}{d} t \ \ (t = 0, \pm 1, \pm 2, \cdots)$。

所以(1)的全部解为：

$$x = b_1 + m_1 \left(y_0 + \frac{m_2}{d} t \right) = b_1 + m_1 y_0 + \frac{m_1 m_2}{d} t (t = 0, \pm 1, \pm 2, \cdots)。$$

这些解对模$[m_1, m_2]$都同余，故对模$[m_1, m_2]$唯一。

3 一次同余式(续)

定理11 设$(a,m)=d$，$m>0$，$d\mid b$，则同余式

$$ax\equiv b(\mathrm{mod}\ m)$$

有d个解。

定理11 证明.

如果某整数是 $\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$的解，则同样为 $ax\equiv b(\mathrm{mod}\ m)$的解，反之亦然。

$\frac{a}{d}x\equiv\frac{b}{d}x\left(\mathrm{mod}\ \frac{m}{d}\right)$有唯一解，假定是 t。则全体整数 $t+k\frac{m}{d}$，$k=0,\pm1,\pm2,\cdots$

是$ax\equiv b(\mathrm{mod}\ m)$的解。对模 m而言，恰有 t，$t+\frac{m}{d}$，$t+2\frac{m}{d}$,...，$t+(d-1)\frac{m}{d}$个互

不同余的整数解。这是 因为对于 $t+k\frac{m}{d}$，设$k=qd+r,0\le r<d$，代入得

$t+k\frac{m}{d}\equiv t+qm+r\frac{m}{d}\equiv t+r\frac{m}{d}(\mathrm{mod}\ m)$。又若$0\le e<d,0\le f<d$，则

$t+e\frac{m}{d}\equiv t+f\frac{m}{d}(\mathrm{mod}\ m)$，有$f=e$，说明$t$，$t+\frac{m}{d}$，$t+2\frac{m}{d}$,...，$t+(d-1)\frac{m}{d}$模

m互不同余。

1 中国剩余定理(CRT) (续)

例子1 解$x \equiv 3(\mathrm{mod}\,7)$，$x \equiv 5(\mathrm{mod}\,15)$。

由于$80(\mathrm{mod}\,7) \equiv 3(\mathrm{mod}\,7), 80(\mathrm{mod}\,15) \equiv 5(\mathrm{mod}\,15)$，

所以解为$x \equiv 80(\mathrm{mod}\,105)$。

定理3 若m_1，$m_2, \cdots$，m_k是k个两两互素的正整数，

$m = m_1 m_2 \cdots m_k$，则同余式

$$f(x) \equiv 0(\mathrm{mod}\,m) \qquad (2)$$

有解的充分必要条件是每一个同余式

$$f(x) \equiv 0(\mathrm{mod}\,m_i)(i = 1,2,\cdots, k) \qquad (3)$$

有解。并且，若用 T_i表示式(3)的解数，T表示式(2)的解数，则$T = T_1 T_2 \cdots T_k$。

1 中国剩余定理(CRT) (续)

定理3证明.

$\rightarrow$ 设x_0是适合(2)的整数，则由$f(x_0)\equiv 0(\mathrm{mod}\, m)$，可得$f(x_0)\equiv 0(\mathrm{mod}\, m_i)$ $(i=1,2,\cdots, k)$。

$\leftarrow$ 反之，若x_i适合$f(x_i)\equiv 0(\mathrm{mod}\, m_i)(i=1,2,\cdots, k)$，因为$1\le i<j\le k$时，$(x_i, x_j)=1$，由定理1，有唯一的$x_0, 0\le x_0<m$，适合$x_0\equiv x_i(\mathrm{mod}\, m_i)$ $(i=1,2,\cdots, k)$，且$f(x_0)\equiv f(x_i)\equiv 0(\mathrm{mod}\, m_i)(i=1,2,\cdots, k)$，故$f(x_0)\equiv 0(\mathrm{mod}\, m)$。这就证明了充要条件。

现设$f(x)\equiv 0(\mathrm{mod}\, m_i)$的$T_i$个不同解是

$x\equiv u_{i,e_i}(\mathrm{mod}\, m_i), 0\le u_{i,e_i}\le m_i (e_i=1,2,\cdots, T_i;\ i=1,2,\cdots, k)$,

对其中任一组$(u_{1,e_1}, u_{2,e_2},\cdots, u_{k,e_k})$，应用定理1可得唯一的$x, 0\le x<m$是(2)的解。不同组，得到的解$x$也不同，故$T_1T_2\cdots T_k\le T$。反之，令$x_1, x_2,\cdots, x_T$，$0\le x_i<m(i=1,2,\cdots, T)$是(2)的$T$个解，则对某个$j(0\le j\le T)$，$(x_j(\mathrm{mod}\, m_1), x_j(\mathrm{mod}\, m_2),\cdots, x_j(\mathrm{mod}\, m_k))$应是某个一组$(u_{1,e_1}, u_{2,e_2},..., u_{k,e_k})$，故$T\le T_1T_2\cdots T_k$。这就证明了$T=T_1T_2\cdots T_k$。

1 中国剩余定理(CRT) (续)

例子2 解同余式$6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}30)$。由定理3解同余式可先分别解以下两个同余式：

$$6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}5)$$

和

$$6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}6)。$$

第一个同余式有解

$$x\equiv 0,1,2(\mathrm{mod}5)$$

第二个同余式有解

$$x\equiv 2,5(\mathrm{mod}6)。$$

由定理1，当(b_1,b_2)取$(0,2),(0,5),(1,2),(1,5),(2,2),(2,5)$时，得$6x^3+27x^2+17x+20\equiv 0(\mathrm{mod}30)$的6个解

$$x\equiv 6b_1+25b_2\equiv 2,5,11,17,20,26(\mathrm{mod}30)。$$

2 模是素数幂的同余式

模是素数幂的同余式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\,p^\alpha),\qquad (4)$$

$n>0, p^\alpha\nmid a_n$，其中p是素数，$\alpha\geq 1$。

适合(4)式的每个整数都适合同余式

$$f(x)\equiv 0(\mathrm{mod}\,p)。\qquad (5)$$

如果(5)式无解，自然(4)式也无解。

2 模是素数幂的同余式(续)

定理4 设$x \equiv x_1 (\mathrm{mod}\ p)$即

$$x \equiv x_1 + pt_1 \quad (t_1 = 0, \pm 1, \pm 2, \cdots) \tag{6}$$

是(5)式的一个解，且$p \nmid f'(x_1)$，这里$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$表示$f(x)$的导数，则(6)式恰好给出(4)式的一个解$x \equiv x_\alpha (\mathrm{mod}\ p^\alpha)$，即

$$x \equiv x_\alpha + p^\alpha t_\alpha \qquad (t_\alpha = 0, \pm 1, \pm 2, \cdots),$$

其中$x_\alpha \equiv x_1 (\mathrm{mod}\ p)$。

推论1 设$f(x) \equiv 0 (\mathrm{mod}\ p)$和$f'(x) \equiv 0 (\mathrm{mod}\ p)$无公解，则同余式$f(x) \equiv 0 (\mathrm{mod}\ p^\alpha)$和$f(x) \equiv 0 (\mathrm{mod}\ p)$的解数相同。

2 模是素数幂的同余式(续)

定理4证明.

归纳法。

当$\alpha=1$时，定理显然成立。现假定定理对$\alpha-1(\alpha\geq 2)$成立，即(6)

恰好给出$f(x)\equiv 0(\mathrm{mod}\ p^{\alpha-1})$的一个解$x\equiv x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1}(t_{\alpha-1}=0,\pm1,\pm2,\cdots)$,

其中$x_{\alpha-1}\equiv x_1(\mathrm{mod}\ p)$。把$x\equiv x_{\alpha-1}+p^{\alpha-1}t_{\alpha-1}$代入(4)，由$2\alpha-2\geq\alpha$可得

$f(x_{\alpha-1})+p^{\alpha-1}t_{\alpha-1}f'(x_{\alpha-1})\equiv 0(\mathrm{mod}\ p^{\alpha})$，但$f(x_{\alpha-1})\equiv 0(\mathrm{mod}\ p^{\alpha-1})$,

因此，由第二讲定理8知$t_{\alpha-1}f'(x_{\alpha-1})\equiv-\dfrac{f(x_{\alpha-1})}{p^{\alpha-1}}(\mathrm{mod}\ p)$。由$x_{\alpha-1}\equiv x_1(\mathrm{mod}\ p)$,

即得$t_{\alpha-1}f'(x_1)\equiv-\dfrac{f(x_{\alpha-1})}{p^{\alpha-1}}(\mathrm{mod}\ p)$。由于$(f'(x_1),p)=1$，故上式恰有一个解

$t_{\alpha-1}\equiv t'_{\alpha-1}+pt_{\alpha}\ \ (t_{\alpha}=0,\pm1,\pm2,\cdots)$。这样就得到了(4)的解

$x=x_{\alpha-1}+p^{\alpha-1}(t'_{\alpha-1}+pt_{\alpha})=x_{\alpha-1}+p^{\alpha-1}t'_{\alpha-1}+p^{\alpha}t_{\alpha}(t_{\alpha}=0,\pm1,\pm2,\cdots)$。

令$x_{\alpha}=x_{\alpha-1}+p^{\alpha-1}t'_{\alpha-1}$，即$x\equiv x_{\alpha}(\mathrm{mod}\ p^{\alpha})$是(4)的一个解且$x\equiv x_1(\mathrm{mod}\ p)$。

2.1 同余定义与概念(续)

定理8 如果$ac \equiv bc(\bmod m)$，且若$(m,c)=d$，则

$$a \equiv b\left(\bmod \frac{m}{d}\right)。$$

定理8证明.

由定理6知$m \mid ac-bc=c(a-b) \Rightarrow \frac{m}{d}\left|\frac{c}{d}(a-b),\right.$

又$\because \left(\frac{m}{d},\frac{c}{d}\right)=1 \Rightarrow \frac{m}{d}\left|a-b。\right.$

$\therefore a \equiv b\left(\bmod \frac{m}{d}\right)。$

3 整数的剩余表示

定义1 设$m_1 > 0$，$m_2 > 0, \cdots$，$m_k > 0, (m_i, m_j) = 1, 0 < i < j \le k$，$< a >_b$ 表示b模a的非负最小剩余，一个整数x对于模m_1，$m_2, \cdots$，m_k的剩余表示是指序列$(< x >_{m_1}, < x >_{m_2}, \cdots, < x >_{m_k})$，记作$x \leftrightarrow (< x >_{m_1}, < x >_{m_2}, \cdots, < x >_{m_k})$。

定理5 设$m_1 > 0$，$m_2 > 0, \cdots$，$m_k > 0, (m_i, m_j) = 1, 0 < i < j \le k$，两个整数$x$，$x'$对模$m_1$，$m_2, \cdots$，$m_k$的剩余表示相同的充分必要条件是$x \equiv x' (\mathrm{mod}\, M)$，这里 $M = m_1 m_2 \cdots m_k$。

3 整数的剩余表示(续)

定理5 证明.

$\rightarrow$ 设x和x'对于模m_1，m_2,…，m_k的剩余表示分别为

$(< x >_{m_1}, < x >_{m_2}, \cdots, < x >_{m_k})$和$(< x' >_{m_1}, < x' >_{m_2}, \cdots, < x' >_{m_k})$,

其中$< x >_{m_i} = x - q_i m_i, 0 \leq < x >_{m_i} < m_i, < x' >_{m_i} = x' - q_i' m_i$,

$0 \leq < x' >_{m_i} < m_i$，$i = 1,2,\cdots$，$k$。如果$< x >_{m_i} =< x' >_{m_i}$，

$i = 1,2,\cdots$，k，则$m_i \mid x - x'$，故$M \mid x - x'$。

$\leftarrow$ 因为$M \mid x - x'$，又因为$x - x' =< x >_{m_i} + q_i m_i - < x' >_{m_i} - q_i' m_i$,

$i = 1,2,\cdots$，k，故$m_i \mid < x >_{m_i} - < x' >_{m_i}$，$i = 1,2,\cdots$，$k$。

由此推出$< x >_{m_i} =< x' >_{m_i}$，$i = 1,2,\cdots$，$k$。

3 整数的剩余表示(续)

定义2 设$m_1 > 0$，$m_2 > 0,\cdots$，$m_k > 0,(m_i, m_j) = 1, 0 < i < j \le k$，$M = m_1 m_2 \cdots m_k, 0 \le x < M$，此时整数$x$对于模$m_1$，$m_2,\cdots$，$m_k$的剩余表示$(< x >_{m_1}, < x >_{m_2}, \cdots, < x >_{m_k})$也叫$x$的模系数记数法。

定理6 设Z表示整数集，$Z_l = \{0,1,\cdots,l-1\}$表示最小非负剩余组成的集，设$m_1 > 0$，$m_2 > 0,\cdots$，$m_k > 0,(m_i, m_j) = 1, 0 < i < j \le k$，$0 \le x < m_1 m_2 \cdots m_k$，则集

$$S = \{x \mid 0 \le x < m_1 m_2 \cdots m_k\}$$

与集

$$S_1 = \{(a_1, a_2, \cdots, a_k) \mid a_j \in Z_{m_j}, j = 1,2,\cdots,k\}$$

之间存在一一对应关系。

3 整数的剩余表示(续)

定理7 设x和y的剩余表示分别为 $(< x >_{m_1}, < x >_{m_2}, \cdots, < x >_{m_k})$和 $(< y >_{m_1}, < y >_{m_2}, \cdots, < y >_{m_k})$，则有

(1) $< x \pm y >_M$ 的剩余表示为 $(<< x >_{m_1} \pm < y >_{m_1} >_{m_1}, << x >_{m_2} \pm < y >_{m_2} >_{m_2}, \cdots, << x >_{m_k} \pm < y >_{m_k} >_{m_k})$。

(2) $< xy >_M$ 的剩余表示为 $(<< x >_{m_1} < y >_{m_1} >_{m_1}, << x >_{m_2} < y >_{m_2} >_{m_2}, \cdots, << x >_{m_k} < y >_{m_k} >_{m_k})$。

定理7 证明.

对于任意 $1 \le i \le k$，$x = m_i q_1 + < x >_{m_i}$，$y = m_i q_2 + < y >_{m_i}$，

$< x >_{m_i} + < y >_{m_i} = m_i q_3 + << x >_{m_i} + < y >_{m_i} >_{m_i}$，

故 $x + y = m_i q_1 + m_i q_2 + < x >_{m_i} + < y >_{m_i}$

$= m_i (q_1 + q_2 + q_3) + << x >_{m_i} + < y >_{m_i} >_{m_i}$，故

$< x + y >_{m_i} = << x >_{m_i} + < y >_{m_i} >_{m_i}$。类似可证明

$< x - y >_{m_i} = << x >_{m_i} - < y >_{m_i} >_{m_i}$，$< xy >_{m_i} = << x >_{m_i} < y >_{m_i} >_{m_i}$。

因此，定理 7成立。

3 整数的剩余表示(续)

例子3　对于模 4,3,5,11。

$x = 102 \leftrightarrow (2,0,2,3)$

$y = 211 \leftrightarrow (3,1,1,2)$

则

$$\begin{array}{r} 102 \\ +\,211 \\ \hline \end{array} \qquad \begin{array}{r} (2,0,2,3) \\ (3,1,1,2) \\ \hline \end{array}$$

$$\langle 313 \rangle_{660} = 313 \leftrightarrow \quad (1,1,3,5)$$

谢谢！