第三章 同余式

2024年12月11日 星期三 21:44

定义 3.1.1

设 $f(x)=a_nx^n+\cdots+a_1x+a_0$

$f(x)\equiv 0 \pmod m$ 叫做模 m 同余式

n 叫做 f(x) 的次数，记为 deg f. f(x) 又叫模 m 的 n 次同余式

如果整数 $x=a$ 使 $f(a)\equiv 0 \pmod m$，则 a 叫作同余式的解

$C_a=\{c \mid c\in\mathbb{Z},\ c\equiv a \pmod m\}$ 都使 $f\equiv 0$ 成立

$\therefore$ a 通常写成 $x\equiv a \pmod m$

定理 3.1.1

设 $m\in\mathbb{N}_+$，a 满足 $m\nmid a$，则一次同余式

$$ax\equiv 1 \pmod m$$

有解的充要条件是 $(a,m)=1$

且解是唯一的

证明：存在：$\because (a,m)=1$

$\therefore \exists s,t$ 使 $sa+tm=1$

$\therefore x=s \pmod m$ 是同余式的解

唯一：若还有解 x'，即 $ax'\equiv 1 \pmod m$

则 $a(x-x')\equiv 0 \pmod m$

$\because (a,m)=1 \quad \therefore x\equiv x'$ 唯一

定义 3.1.2

设 $m\in\mathbb{N}_+$，$a\in\mathbb{Z}$，若 $\exists a'$ 使 $a\cdot a'\equiv a'\cdot a\equiv 1 \pmod m$ 成立，

则 a 叫做模 m 可逆元

定理 3.1.2

设 $m\in\mathbb{N}_+$，则 $a\in\mathbb{Z}$ 是模 m 简化剩余 $\Leftrightarrow$ a 是模 m 逆元

证：$\Rightarrow$：$\because$ a 是模 m 简化剩余 $\therefore (a,m)=1$

由 3.1.1，$\exists a'$ 使 $a\cdot a'\equiv a'\cdot a\equiv 1 \pmod m$

$\Leftarrow$：若 a 是模 m 逆元，则 $\exists a'$ 使

$aa'\equiv 1 \pmod m$

即 $ax\equiv 1 \pmod m$ 有解 $x\equiv a'$

$\therefore (a,m)=1$

定理 3.1.3

设 $m\in\mathbb{N}_+$，$a\in\mathbb{Z}$ 满足 $m\nmid a$，则一次同余式 $ax\equiv b \pmod m$

有解 $\Leftrightarrow (a,m)\mid b$

且其解为 $x\equiv \frac{b}{(a,m)}\cdot\left(\left(\frac{a}{(a,m)}\right)^{-1} \left(\bmod \frac{m}{(a,m)}\right)\right)+t\frac{m}{(a,m)} \pmod m$

例：求解一次同余式 $33x\equiv 22 \pmod{77}$

$(33,77)=11 \mid 22 \quad \therefore$ 有解

$3x\equiv 1 \pmod 7$

$x_0'\equiv 5 \pmod 7$

$3x\equiv 2 \pmod 7$

$x_0\equiv 2\cdot x_0'\equiv 2\cdot 5\equiv 3 \pmod 7$

$\therefore x\equiv 3+t\cdot\frac{77}{(33,77)}\equiv 3+t\cdot 7 \pmod{77}$

定理 3.2.1 (中国剩余定理)

例：求解同余式组

$$\begin{cases} x\equiv b_1 \pmod 5\\ x\equiv b_2 \pmod 6\\ x\equiv b_3 \pmod 7\\ x\equiv b_4 \pmod{11}\end{cases}$$

解：令 $m=5\cdot 6\cdot 7\cdot 11=2310$

$M_1=6\cdot 7\cdot 11=462 \qquad M_2=5\cdot 7\cdot 11=385$

$M_3=5\cdot 6\cdot 11=330 \qquad M_4=5\cdot 6\cdot 7=210$

分别求解同余式 $M_i'\cdot M_i\equiv 1 \pmod{m_i}$

解得 $M_1'=3 \quad M_2'=1 \quad M_3'=1 \quad M_4'=1$

$\therefore x\equiv b_1\cdot 3\cdot 462+b_2\cdot 1\cdot 385+b_3\cdot 1\cdot 330+b_4\cdot 1\cdot 210 \pmod{2310}$

定理 3.4.5

设 p 是素数，n 是正整数，$n\le p$，则

$f(x)=x^n+\cdots+a_1x+a_0\equiv 0 \pmod p$

有 n 个解的充要条件是 x^p-x 被 f(x) 除所得余式的所有系数都是 p 的倍数