# 第三讲 初等数论

**3**

# 本讲提要

- 同余(续)

# 1 剩余类和完全剩余系(续)

定理1 (威尔逊定理)设$p$是一个素数，

则$(p-1)!+1\equiv 0(\bmod p)$。

定理1证明.

$p=2,3$时，同余式成立。

设$p>3$是奇素数，$S=\{2,3,\ldots,p-2\}$，$a\in S$。

因为$(a,p)=1$所以有$ma+np=1\Rightarrow am\equiv 1(\bmod p)$,

设$b\equiv m(\bmod p),0<b<p$，知$b\neq 1$，$b\neq p-1$,故$b\in S$,

且$ab\equiv 1(\bmod p)$，这里$a\neq b$，否则$b^2\equiv 1(\bmod p)\Rightarrow$

$(b-1)(b+1)\equiv 0(\bmod p)$，而$b\neq 1$，$b\neq p-1$，故不成立。

# 1 剩余类和完全剩余系(续)

定理1证明.（续）

现取$a' \in S$，$a' \neq a$，$a' \neq b$,则类似有$b' \in S$使$a'b' \equiv 1 \pmod p$，且

$b' \neq a'$，$b' \neq a$，这是因为若$b' = a$，则

$$\left.\begin{array}{r} a'b' \equiv a'a \equiv 1 \pmod p \\ ab \equiv 1 \pmod p \end{array}\right\} \Rightarrow a(a'-b) \equiv 0 \pmod p \Rightarrow a' \equiv b \pmod p,$$

故不可能。

同理$b' \neq b$。

如此下去知$S$中数可成为$\frac{p-3}{2}$对，且每对$a$，$b$满足$ab \equiv 1 \pmod p$，

故$2 \cdot 3 \cdots \cdots (p-2) \equiv 1 \pmod p$，即得$(p-1)!+1 \equiv 0 \pmod p$。

## 2 缩系

定义 1如果一个模$m$的剩余类里的数与$m$互素(显然一个互素全部互素)，就把它叫做一个与模$m$互素的剩余类，在其中各取一个数组成的集叫模$m$的一组缩系。

定义 2欧拉函数$\varphi(n)$是一个定义在整数上的函数，$\varphi(n)$的值为序列$0,1,\cdots$，$n-1$中与$n$互素的数的个数。显然$p$是素数时$\varphi(p)=p-1$。

定理 2 模$m$的一组缩系含有$\varphi(m)$个数。

显然。

定理 3 若$a_1,\cdots$，$a_{\varphi(m)}$是$\varphi(m)$个与$m$互素的整数，则$a_1,\cdots$，$a_{\varphi(m)}$为缩系的充要条件为它们两两模$m$不同余。

显然。

# 2 缩系(续)

定理 4 若$(a,m)=1$，$x$是通过模$m$的缩系则$ax$也是模$m$的缩系。

定理4证明.

显然$ax$有$\varphi(m)$个整数。

因为$(a,m)=1,(x,m)=1,$

所以$(ax,m)=1$。

若$x$中存在$x_1$，$x_2$有$ax_1\equiv ax_2 \pmod m$，由于$(a,m)=1,$

可得$x_1\equiv x_2 \pmod m$，这与$x$是通过模$m$的缩系矛盾。

故$ax$也为通过模$m$的缩系。

# 2 缩系(续)

定理5（欧拉定理）设$m>1,(a,m)=1$，则

$$a^{\varphi(m)}\equiv 1(\bmod m)。$$

定理5证明.

设$r_1$，$r_2,\cdots$，$r_{\varphi(m)}$为模$m$的一组缩系，由 定理4知

$ar_1$，$ar_2,\cdots$，$ar_{\varphi(m)}$亦是模$m$的缩系。

因此,$(ar_1)(ar_2)\cdots(ar_{\varphi(m)})\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m)$,

即$a^{\varphi(m)}r_1r_2\cdots r_{\varphi(m)}\equiv r_1r_2\cdots r_{\varphi(m)}(\bmod m)$。

因为$r_1$，$r_2,\cdots$，$r_{\varphi(m)}$为模$m$的一组缩系，所以$(r_1r_2\cdots r_{\varphi(m)},m)=1$。

由上讲定理8知$a^{\varphi(m)}\equiv 1(\bmod m)$。

## 2.1 同余定义与概念(续)

定理8 如果$ac \equiv bc \pmod{m}$，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$\because \left(\frac{m}{d},\frac{c}{d}\right)=1 \Rightarrow \frac{m}{d} \left| a-b \right.$。

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

## 2 缩系(续)

由定理5立刻可得：

定理6（费马小定理）若$p$是素数，则

$$a^p \equiv a \pmod p$$。

定理 7 设$m_1 > 0$，$m_2 > 0, (m_1, m_2) = 1$，而$x_1$，$x_2$分别通过模$m_1$，$m_2$的缩系，则$m_2 x_1 + m_1 x_2$通过模$m_1 m_2$的缩系。

# 2 缩系(续)

定理 7证明.

首先，由上一讲定理13知$m_2x_1+m_1x_2$两两不同余。

其次，证明$(m_2x_1+m_1x_2, m_2m_1)=1$，否则存在素数$p\mid m_2x_1+m_1x_2$，$p\mid m_1m_2$。如果$p\mid m_1$，则$p\mid m_2x_1$，又$p\nmid x_1$，故$p\mid m_2$，这与$(m_1,m_2)=1$矛盾。如果$p\mid m_2$，可证同样矛盾。这样两个缩系通过$m_2x_1+m_1x_2$形成与$m_1m_2$互素的$\varphi(m_1)\varphi(m_2)$个数。

最后，证明凡与$m_1m_2$互素的$a$有：$a\equiv m_2x_1+m_1x_2 \pmod{m_1m_2}$，且$(x_1,m_1)=(x_2,m_2)=1$。由上一讲定理13知有上式的表示形式，只需要证当$(a,m_1m_2)=1$时有$(x_1,m_1)=(x_2,m_2)=1$。如果$(x_1,m_1)>1$，有素数$q$，$q\mid x_1$，$q\mid m_1$，由此$q\mid a$，这与$(a,m_1m_2)=1$矛盾，故$(x_1,m_1)=1$。同理$(x_2,m_2)=1$。

## 2 剩余类和完全剩余系(续)

定理13 设$m_1>0$，$m_2>0,(m_1,m_2)=1$，而$x_1$，$x_2$分别通过模$m_1$，$m_2$的完系，则$m_2x_1+m_1x_2$通过模$m_1m_2$的完系。

定理13证明.

$x_1$，$x_2$分别有$m_1$，$m_2$个整数，因此，$m_2x_1+m_1x_2$有$m_1m_2$个整数。剩下只需要证明它们对模$m_1m_2$两两不同余即可。

假定：$m_2x_1'+m_1x_2'\equiv m_2x_1''+m_1x_2''(\mathrm{mod}\, m_1m_2)$，　　(5)

则$m_2x_1'\equiv m_2x_1''(\mathrm{mod}\, m_1)$，$m_1x_2'\equiv m_1x_2''(\mathrm{mod}\, m_2)$。

由于$(m_1,m_2)=1, \therefore x_1'\equiv x_1''(\mathrm{mod}\, m_1)$，$x_2'\equiv x_2''(\mathrm{mod}\, m_2)$。

又由于$x_1'$，$x_1''$同取自模$m_1$的完全剩余系，由此可得：

$x_1'=x_1''$。同理$x_2'=x_2''$。因此，若$(x_1',x_2')$与$(x_1'',x_2'')$不同，则(5)式不能成立。

## 2 缩系(续)

由定理7立得：

推论1　若$(m_1, m_2) = 1$，则$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$。

定理8　设$n$的标准分解$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)。$$

定理8证明.

$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$。而由$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$知，

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)。$$

## 3 一次同余式

定义3 设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，其中$n>0$，$a_i(i=0,1,\cdots,n)$是整数，又设$m>0$，则

$$f(x)\equiv 0(\bmod m)$$

叫模$m$的同余式。若$a_n\not\equiv 0(\bmod m)$，则$n$叫次数。如果$x_0$满足$f(x_0)\equiv 0(\bmod m)$，则$x\equiv x_0(\bmod m)$叫同余式的解。不同的解是指互不同余的解。

例子1 用验算的方法知同余式

$$x^5+2x^4+x^3+2x^2-2x+3\equiv 0(\bmod 7)$$

仅有解$x\equiv 1,5,6(\bmod 7)$。

## 3 一次同余式(续)

例子 2 用同余式

$$x^4 - 1 \equiv 0 \pmod{16}$$

有8个解$x \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$。

例子 3 用同余式

$$x^2 + 3 \equiv 0 \pmod{5}$$

无解。

# 3 一次同余式(续)

定理 9 设$(a,m)=1$，$m>0$，则同余式

$$ax\equiv b(\bmod m)$$

恰有一个解，这个解就是$x\equiv ba^{\varphi(m)-1}(\bmod m)$。特别地，我们将$ax\equiv 1(\bmod m)$的解$a^{\varphi(m)-1}$称为$a$的逆元，记为$a^{-1}$。

定理 9证明.

1,2,. . .，$m$为模$m$的完系。因为$(a,m)=1$，所以$a$，$a2$,. . .，$am$，由上一讲定理12知$am$也是完系，故有且仅有一个$aj\equiv b(\bmod m)$，因此，$x\equiv j(\bmod m)$为一次同余唯一解。

由定理5可得解为$x\equiv ba^{\varphi(m)-1}(\bmod m)$。

## 2 剩余类和完全剩余系(续)

定理12 设$(k,m)=1$，而$a_0$，$a_1,\cdots$，$a_{m-1}$是模$m$的一组完系则$ka_0$，$ka_1,\cdots$，$ka_{m-1}$也是模$m$的一组完系。

定理12证明.

如果不是完系，则由定 理11存在

$$ka_i \equiv ka_j \pmod{m}，\quad 0 \le i < j \le m-1。$$

则$m \mid k(a_i - a_j)$。又$(k,m)=1$，由上一讲定理 5，知$m \mid a_i - a_j$。矛盾。

# 3 一次同余式(续)

定理10 设$(a,m)=d$，$m>0$，则同余式

$$ax\equiv b(\bmod m)$$

有解的充分必要条件是 $d\mid b$。

定理10证明.

$\rightarrow\because m\mid ax-b,\therefore d\mid ax-b$，由$d\mid a,\therefore d\mid b$。

$\leftarrow\because\left(\frac{a}{d},\frac{m}{d}\right)=1$且$d\mid b$，

$\therefore$同余式$\frac{a}{d}x\equiv\frac{b}{d}\left(\bmod\frac{m}{d}\right)$有解(定理9)。即$ax\equiv b(\bmod m)$有解。

# 3 一次同余式(续)

定理11　设$(a,m)=d$，$m>0$，$d\mid b$，则同余式

$$ax \equiv b(\bmod m)$$

有$d$个解。

定理11 证明.

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

$\frac{a}{d}x \equiv \frac{b}{d}\left(\bmod \frac{m}{d}\right)$有唯一解，假定是 $t$。则全体整数 $t+k\frac{m}{d}$，$k=0,\pm 1,\pm 2,\cdots$

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

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

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

$m$互不同余。

# 4 模是素数的同余式

定理12（拉格朗日定理）设$p$是素数，$f(x)=a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$，$n>0$，$a_n \not\equiv 0 \pmod p$，是一个整系数多项式，则同余式

$$f(x) \equiv 0 \pmod p$$

最多有$n$个解。

定理12证明.

归纳法。

当$n=1$时，$a_1 x + a_0 \equiv 0 \pmod p$，$p \nmid a_1$，恰有一解。

假定$n-1$时为真，即最多有$n-1$个解，需证明$n$时最多只有$n$个解。如果$n \geq p$结论立即成立。

# 4 模是素数的同余式(续)

定理12 证明.（续）

否则（反证法），即在 $n \le p-1$至少有$n+1$个解为：

$x_0$，$x_1, \cdots$，$x_n$，$x_i \not\equiv x_j \pmod p, 0 \le i < j \le n$。

做$f(x)-f(x_0)=\sum_{k=1}^{n} a_k(x^k - x_0^k)=(x-x_0)g(x)$，这里

$g(x)$是首项系数为 $a_n$的$n-1$次整系数多项式。由于 当

$k>0$时$x_k - x_0 \not\equiv 0 \pmod p$，而$f(x_k)-f(x_0)\equiv(x_k-x_0)g(x_k)$

$\equiv 0 \pmod p$，说明$g(x)$有$n$个解。这与其有 $n-1$个解矛盾。

# 4 模是素数的同余式(续)

定理13 设同余式

$$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0\equiv 0 \pmod p$$

的解的个数大于 $n$，这里$p$是素数，$a_i$是整数 $(i=0,1,\cdots, n)$，则$p|a_i (i=0,1,\cdots, n)$。

定理13证明.

如果某些系数不能被$p$整除，设这些系数的脚标最大为$k$。$k$次同余式

$$a_k x^k+a_{k-1}x^{k-1}+\cdots+a_1 x+a_0\equiv 0 \pmod p),\ p\nmid a_k$$

的解的个数大于$k$，这与定理12矛盾。

# 4 模是素数的同余式(续)

定理14 对于任意给的素数$p$，多项式

$$f(x)=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1$$

的所有系数被$p$整除。

定理14证明.

令$g(x)=(x-1)(x-2)\cdots(x-p+1)$，则$1,2,\cdots$，$p-1$是$g(x)\equiv 0(\mathrm{mod}\ p)$的$p-1$个解。由费马小定理,$1,2,\cdots$，$p-1$也是$h(x)\equiv x^{p-1}-1\equiv 0(\mathrm{mod}\ p)$的$p-1$个解，故同余式$f(x)\equiv g(x)-h(x)(\mathrm{mod}\ p)$有$p-1$个解，而考察$f(x)$为$p-2$次多项式。由定理13知其系数均能被$p$整除。

这里常数项是$(-1)^{p-1}(p-1)!+1$，为定理1(威尔逊定理)的结论。

谢谢！