第五讲 初等数论

5

本讲提要

- 二次剩余

1 二次剩余的基本概念

定义1 设$m>1$，若$x^2\equiv n(\bmod m),(n,m)=1$有解，则$n$叫做模$m$的二次剩余；若无解，则$n$叫做模$m$的二次非剩余。

考虑m为素数的情况，因为$m=2$时情况简单，我们仅考虑$m=p$为奇素数的情况，即

$$x^2\equiv n(\bmod p),\qquad (n,p)=1。\tag{1}$$

1 二次剩余的基本概念(续)

定理1 在模p的缩系$1,2,\cdots$，$p-1$中，有$\frac{p-1}{2}$个模p的二次剩余和$\frac{p-1}{2}$个模p的二次非剩余，且

$$1, <2^2>_p, \cdots, \left\langle \left(\frac{p-1}{2}\right)^2 \right\rangle_p \qquad (2)$$

就是模p缩系中的全部二次剩余。

1 二次剩余的基本概念(续)

定理1证明.

设$1 \le n \le p-1$ 是模p的任意一个二次剩余， 则(1)有解x_1。显然$p-x_1$也是一个解。而$x_1 \not\equiv p-x_1 \pmod p$，再由第三讲的定理12知(1)最多只有两个解。不失一般，可 设$1 \le x_1 \le \frac{p-1}{2}$，故由$1 \le n \le p-1$，

$< x_1^2 >_p \equiv x_1^2 \equiv n \pmod p$知$n$与(2)中之一相等。若(2)中有两个数同余，

设为$1 \le j < i \le \frac{p-1}{2}, < j^2 >_p = < i^2 >_p$，则$j^2 \equiv < j^2 >_p \equiv < i^2 >_p \equiv i^2 \pmod p$。

也就有$(i+j)(i-j) \equiv 0 \pmod p$。由于$1 < j+i < p$，故$p \mid i-j$，与所设

$1 \le j < i < \frac{p-1}{2}$矛盾。这就证明了(2)给出全部二次剩余。因 此，剩下

的二次非剩余也有 $\frac{p-1}{2}$个。

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。

1 二次剩余的基本概念(续)

定理2 如果n是模p的二次剩余，则

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{3}$$

而如果n是模p的二次非剩余，则

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}。 \tag{4}$$

1 二次剩余的基本概念(续)

定理2证明.

若n是模p的二次剩余，则(1)有解x_1, 且$(x_1, p)=1$，即

$x_1^2 \equiv n(\bmod p)$，而由第三讲的费马小定理知$1 \equiv x_1^{p-1} \equiv \left(x_1^2\right)^{\frac{p-1}{2}}$

$\equiv n^{\frac{p-1}{2}}(\bmod p)$，即(3)式成立，再由费马小定理：

$n^{p-1} \equiv 1(\bmod p) \Rightarrow n^{p-1}-1 \equiv 0(\bmod p) \Rightarrow$

$\left(n^{\frac{p-1}{2}}-1\right)\left(n^{\frac{p-1}{2}}+1\right) \equiv 0(\bmod p)$($p$为奇素数，因此，只有一个成立)。

n是模p的二次剩余，给出了$n^{\frac{p-1}{2}}-1 \equiv 0(\bmod p)$的$\dfrac{p-1}{2}$个解，且是

全部解。于是由定理1知模p的缩系中$\dfrac{p-1}{2}$个二次非剩余，只能给

$n^{\frac{p-1}{2}}+1 \equiv 0(\bmod p)$的全部解。

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。

1 二次剩余的基本概念(续)

推论1 n是模p的二次剩余的充分必要条件是

$n^{\frac{p-1}{2}} \equiv 1 \pmod p$；$n$是模$p$的二次非剩余的充分

必要条件是 $n^{\frac{p-1}{2}} \equiv -1 \pmod p$。

推论1证明.

$\Leftarrow \dfrac{p-1}{2}$个二次剩余给出$n^{\frac{p-1}{2}} \equiv 1 \pmod p$的全部

解。而$\dfrac{p-1}{2}$个二次非剩余恰恰给出$n^{\frac{p-1}{2}} \equiv -1 \pmod p$

的全部解。显然结论成立。

2 Legendre符号

定义2 设p为奇素数，$(p,n)=1$，令

$$\left(\frac{n}{p}\right)=\begin{cases}1，若n是模p的二次剩余；\\-1，若n是模p的二次非剩余。\end{cases}$$

函数$\left(\frac{n}{p}\right)$叫Legendre 符号。

#由定理2 知$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}\pmod{p}$。显然$\left(\frac{1}{p}\right)=1$。

若$n\equiv n'\pmod{p}$，$\left(\frac{n}{p}\right)=\left(\frac{n'}{p}\right)$。

2 Legendre符号(续)

当$n \equiv 0 (\bmod p)$，若定义$\left(\frac{n}{p}\right) = 0$，则有下面的定理：

定理3 对于给定的奇素数p，Legendre符号$\left(\frac{n}{p}\right)$是一个完全积性函数，即若$n = n_1 n_2$，则$\left(\frac{n}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$。

于是，当$n = \pm 2^m q_1^{l_1} q_2^{l_2} \cdots q_s^{l_s}$，其中$q_i$是素数，$m \geq 1$，$l_i \geq 1$，这里$i = 1,2,\cdots$，$s$，则有

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m \left(\frac{q_1}{p}\right)^{l_1} \left(\frac{q_2}{p}\right)^{l_2} \cdots \left(\frac{q_s}{p}\right)^{l_s}。$$

2 Legendre符号(续)

定理3证明.

如果$p \mid n_1 n_2$，则$p \mid n_1$或$p \mid n_2$，故$\left(\frac{n_1 n_2}{p}\right)=\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)=0$。

如果$p \nmid n_1 n_2$，则$p \nmid n_1$，$p \nmid n_2$，故

$$\left(\frac{n_1 n_2}{p}\right) \equiv \left(n_1 n_2\right)^{\frac{p-1}{2}} = n_1^{\frac{p-1}{2}} n_2^{\frac{p-1}{2}} \equiv \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right) (\mathrm{mod}\ p)。$$

因为$\left(\frac{n_1 n_2}{p}\right)-\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)=\pm 2,0,$

故上式给出$\left(\frac{n_1 n_2}{p}\right)=\left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)$。

2 Legendre符号(续)

定理4 对于每一个奇素数p，有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & 如果p\equiv 1(\bmod 4),\\ -1, & 如果p\equiv 3(\bmod 4)。\end{cases}$$

定理4证明.

因为$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}(\bmod p)$，所以$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$。

2 Legendre符号(续)

定理5 对于每一个奇素数p，有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1，如果p\equiv\pm1(\mathrm{mod}\,8)，\\-1，如果p\equiv\pm3(\mathrm{mod}\,8)。\end{cases}$$

定理5证明.

考虑以下$\frac{p-1}{2}$个同余式

$$p-1\equiv1(-1)(\mathrm{mod}\,p)$$

$$2\equiv2(-1)^2(\mathrm{mod}\,p)$$

$$p-3\equiv3(-1)^3(\mathrm{mod}\,p)$$

$$4\equiv4(-1)^4(\mathrm{mod}\,p)$$

$$\vdots$$

$$r\equiv\frac{p-1}{2}(-1)^{\frac{p-1}{2}}(\mathrm{mod}\,p)，\quad 其中r=\begin{cases}p-\frac{p-1}{2}，如果p\equiv3(\mathrm{mod}\,4)，\\\frac{p-1}{2}，如果p\equiv1(\mathrm{mod}\,4)。\end{cases}$$

2 Legendre符号(续)

定理5证明.（续）

将以上$\frac{p-1}{2}$个同余式相乘，左边都是偶数有：

$$2\cdot 4\cdot 6\cdot\cdots\cdot(p-3)(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}}\pmod p$$

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}\pmod p$$

因为$p\nmid\left(\frac{p-1}{2}\right)!$和$2^{\frac{p-1}{2}}\equiv\left(\frac{2}{p}\right)\pmod p$，故

$\left(\frac{2}{p}\right)\equiv(-1)^{\frac{p^2-1}{8}}\pmod p$，又因为$p$是奇素数，即得$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$。

3 高斯引理和二次互反律

定理6 (高斯引理) 设p是一个奇素数,$(p,n)=1$，且$\frac{p-1}{2}$个数

$$<n>_p,<2n>_p,\cdots,\left\langle\frac{(p-1)n}{2}\right\rangle_p \qquad (5)$$

中有m个大于$\frac{p}{2}$，则

$$\left(\frac{n}{p}\right)=(-1)^m。$$

3 高斯引理和二次互反律(续)

定理6证明.

以a_1，$a_2,\cdots$，a_l表示(5)中所有小于$\frac{p}{2}$的数，b_1，$b_2,\cdots$，b_m表示(5）中所有大于$\frac{p}{2}$的数，

有$l+m=\frac{p-1}{2}$，且$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv\prod_{k=1}^{(p-1)/2}kn=\left(\frac{p-1}{2}\right)!n^{\frac{p-1}{2}}(\bmod p)$。观察$p-b_t$也在1和$\frac{p-1}{2}$之间，故$a_s$，$p-b_t(s=1,2,\cdots$，$l$；$t=1,2,\cdots$，$m)$都是1和$\frac{p-1}{2}$之间的$\frac{p-1}{2}$个数。现证$\frac{p-1}{2}$个数各不相同，这只需证$a_s\neq p-b_t$。如果存在某个$a_s=p-b_t$，则有

$xn+yn\equiv 0(\bmod p),1\le x\le\frac{p-1}{2},1\le y\le\frac{p-1}{2}$，即$x+y\equiv 0(\bmod p)$。此不可能，故

$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}(p-b_t)=\left(\frac{p-1}{2}\right)!$。

所以$\left(\frac{p-1}{2}\right)!=\prod_{s=1}^{l}a_s\prod_{t=1}^{m}(p-b_t)\equiv(-1)^m\left(\frac{p-1}{2}\right)!n^{\frac{p-1}{2}}(\bmod p)$，故$n^{\frac{p-1}{2}}\equiv(-1)^m(\bmod p)$。

由于$n^{\frac{p-1}{2}}\equiv\left(\frac{n}{p}\right)(\bmod p)$，故$\left(\frac{n}{p}\right)\equiv(-1)^m(\bmod p)$，即得$\left(\frac{n}{p}\right)=(-1)^m$。

3 高斯引理和二次互反律(续)

定理7 (二次互反定律) 设$p>2$，$q>2$是两个素数，

$p\neq q$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}。$$

定理7证明.

当$1\le k\le\frac{p-1}{2}$，有$kq=q_k p+r_k$，$q_k=\left[\frac{kq}{p}\right],1\le r_k\le p-1,[]$为取整。

令$a=\sum_{s=1}^{l}a_s$，$b=\sum_{t=1}^{m}b_t$，此处，a_s，b_t与定理6中相同，得

$a+b=\sum_{k=1}^{(p-1)/2}r_k$，这里$n=q$。由定理6证明知$a_s$，$p-b_t$

$(s=1,2,\cdots,\ l,t=1,2,\cdots,\ m)$正好是$s=1,2,\cdots,\frac{p-1}{2}$的各个数。

3 高斯引理和二次互反律(续)

定理7证明.（续）

故有:$1+2+\cdots+\frac{p-1}{2}=a+mp-b=\frac{p^2-1}{8}$。

又$\sum_{k=1}^{(p-1)/2}kq=p\sum_{k=1}^{(p-1)/2}q_k+\sum_{k=1}^{(p-1)/2}r_k=p\sum_{k=1}^{(p-1)/2}q_k+a+b=\frac{p^2-1}{8}q$。

以上两式相减

$$\frac{p^2-1}{8}(q-1)=p\sum_{k=1}^{(p-1)/2}q_k-mp+2b,$$

取模2有$m\equiv\sum_{k=1}^{(p-1)/2}q_k \pmod 2$，得$\left(\frac{q}{p}\right)=(-1)^m=(-1)^{\sum_{k=1}^{(p-1)/2}q_k}=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]}$。

同理$\left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right]}$。

3 高斯引理和二次互反律(续)

定理7证明.（续）

剩下只需要证$\sum_{k=1}^{(p-1)/2}\left[\frac{kq}{p}\right]+\sum_{k=1}^{(q-1)/2}\left[\frac{kp}{q}\right]=\frac{p-1}{2}\frac{q-1}{2}$。

设$f(x,y)=qx-py$。当$x=1,2,\cdots,\frac{p-1}{2}$，$y=1,2,\cdots,\frac{q-1}{2}$时，$f(x,y)$

取$\frac{p-1}{2}\frac{q-1}{2}$个值。且$f(x,y)\neq 0$，否则$qx=py\Rightarrow q\mid y$，不可能。

可以看到每个固定的x，$f(x,y)>0$，当且仅当$y<\frac{qx}{p}$，即$y\leq\left[\frac{qx}{p}\right]$,

因此，全部正整数值$f(x,y)$的个数为$\sum_{x=1}^{(p-1)/2}\left[\frac{xq}{p}\right]$个。同理全部负整数值

$f(x,y)$的个数为$\sum_{y=1}^{(q-1)/2}\left[\frac{yp}{q}\right]$个。得证结论。

3 高斯引理和二次互反律(续)

例子1 设$p=593$，$n=438$，计算$\left(\dfrac{438}{593}\right)$。

因为$438=2\cdot 3\cdot 73$，故$\left(\dfrac{438}{593}\right)=\left(\dfrac{2}{593}\right)\left(\dfrac{3}{593}\right)\left(\dfrac{73}{593}\right)$。

因为$593\equiv 1 \pmod 8$，利用定理7和前面的有关性质，有

$\left(\dfrac{438}{593}\right)=\left(\dfrac{593}{3}\right)\left(\dfrac{593}{73}\right)=\left(\dfrac{2}{3}\right)\left(\dfrac{9}{73}\right)=-1$，所以438是模593

的二次非剩余。

4 二次同余式的解法

定理8 设n是模p的二次剩余，则有

当$p \equiv 3 \pmod 4$时， $\pm n^{\frac{p+1}{4}}$为式(1)的解；

当$p \equiv 5 \pmod 8$， $n^{\frac{p-1}{4}} \equiv 1 \pmod p$时，$\pm n^{\frac{p+3}{8}}$为式(1)的解；

当$p \equiv 5 \pmod 8$， $n^{\frac{p-1}{4}} \equiv -1 \pmod p$时，$\pm \left(\frac{p-1}{2}\right)! n^{\frac{p+3}{8}}$

为式(1)的解。

4 二次同余式的解法(续)

定理8证明.

当$p\equiv 3 \pmod 4$，且n为模p的二次剩余，由定理 2有$n^{\frac{p-1}{2}}\equiv 1 \pmod p$，则有

$$\left(\pm n^{\frac{p+1}{4}}\right)^2\equiv n^{\frac{p+1}{2}}\equiv n^{\frac{p-1}{2}+1}\equiv n \pmod p。$$

当$p\equiv 5 \pmod 8$，且n为模p的二次剩余，由定理 2有$n^{\frac{p-1}{2}}\equiv 1 \pmod p$，当

$n^{\frac{p-1}{4}}\equiv 1 \pmod p$时，$\left(\pm n^{\frac{p+3}{8}}\right)^2\equiv n^{\frac{p+3}{4}}\equiv n^{\frac{p-1}{4}}n\equiv n \pmod p$;

当$n^{\frac{p-1}{4}}\equiv -1 \pmod p$时，由Wilson定理$(p-1)!+1\equiv 0 \pmod p$，有

$$-1\equiv 1\cdot 2\cdots\cdots\left(\frac{p-1}{2}\right)\left(p-\frac{p-1}{2}\right)\cdots\cdots(p-2)(p-1)\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p,$$

因此，$\left(\pm\left(\frac{p-1}{2}\right)!n^{\frac{p+3}{8}}\right)^2\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2 n^{\frac{p+3}{4}}\equiv\left(\left(\frac{p-1}{2}\right)!\right)^2 n^{\frac{p-1}{4}}n\equiv n \pmod p$。

4 二次同余式的解法(续)

例子2 求$5 \pmod{11}$的平方根。

$\frac{p-1}{2}=\frac{10}{2}=5$，$x \equiv 5^5 \equiv 1 \pmod{11}$，所以$5 \pmod{11}$有平方根。

$\frac{p+1}{4}=\frac{12}{4}=3$，$x \equiv 5^3 \equiv 4 \pmod{11}$，所以$5 \pmod{11}$的平方根是 ± 4。

例子3 求$2 \pmod{11}$的平方根。

$\frac{p-1}{2}=\frac{10}{2}=5$，$x \equiv 2^5 \equiv -1 \pmod{11}$，所以$2 \pmod{11}$无平方根。

4 二次同余式的解法(续)

例子4 求$x^2 \equiv 71 \pmod{77}$的平方根。

由上一讲定理3，意味着求$x^2 \equiv 71 \equiv 1 \pmod{7}$和$x^2 \equiv 71 \equiv 5 \pmod{11}$，

因此，根据前面的定理8易求得两个方程的解分别为

$x \equiv \pm 1 \pmod{7}$，$x \equiv \pm 4 \pmod{11}$，所以

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases}, \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv -4 \pmod{11} \end{cases}, \begin{cases} x \equiv -1 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases}, \begin{cases} x \equiv -1 \pmod{7} \\ x \equiv -4 \pmod{11} \end{cases},$$

应用上一讲定理1中国剩余定理可得

$x \equiv 15, 29, -29, -15 \pmod{77}$。

1 中国剩余定理(CRT)

$$x \equiv 23 \pmod{105} \Rightarrow \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

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

$x \equiv b_1 \pmod{m_1}$，$x \equiv b_2 \pmod{m_2}, \cdots$，$x \equiv b_k \pmod{m_k}$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod m,$$

其中

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

1 中国剩余定理(CRT) (续)

例子1 解$x \equiv 3 \pmod 7$，$x \equiv 5 \pmod{15}$。

由于$80 \pmod 7 \equiv 3 \pmod 7, 80 \pmod{15} \equiv 5 \pmod{15}$,

所以解为$x \equiv 80 \pmod{105}$。

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

$$f(x) \equiv 0 \pmod m \tag{2}$$

有解的充分必要条件是每一个同余式

$$f(x) \equiv 0 \pmod{m_i} (i = 1, 2, \cdots, k) \tag{3}$$

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

谢谢！