第5卷 第4期
1985年10月

数学研究与评论
JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION

Vol.5 No.4
Oct. 1985

一种具有Goldbach性质的可换环上的二次同余*

沈复兴

（北师大数学系）

[1]—[3] 用模型论与数论方法讨论了整数环的某些扩环的数论性质，说明一些数论命题间的和谐性与相对独立性。[4]进一步研究了一种具有Goldbach性质的可换环R，分析了R与整数环I的异同。[4]证明了R上有与I极不相同的二次同余性质。如R上存在$8k\pm3$形素元以2为平方剩余，也存在$8k\pm1$形素元不以2为平方剩余，等等。一个自然的问题是对任意非平方数$a\in I$，任意b，$c\in I$，若$(b, c)=1$，是否总存在$bk+c$形素元以a为平方剩余，且也存在$bk+c$形素元不以a为平方剩余？本文对此作出肯定回答，进一步揭示了R的二次同余性质。

可换环R的定义如下[4]：令N是正整数集，F是N上Frēchet滤集，$\mathbf{F}=\{X: X\subseteq N, N\setminus X$有限$\}$；$D$是由$\mathbf{F}$扩充而得的$\mathbf{N}$上超滤。$p_i$，$i\in N$，是第$i$个正有理素数。$k_n$，$n\in N$，是整数环$I$对其理想子环$(p_1^{s}\cdots p_n^{s})$的剩余类环，$R=\prod_D k_n$。即$R$是$k_n$，$n\in N$，模$D$的超积。

引理1. 设$a\in I$，a不是平方数，则存在无穷多个有理素数p，使$\left(\frac{a}{p}\right)=1$；也存在无穷多个有理素数$q$，$\left(\frac{a}{q}\right)=-1$。

引理2. 设a，$b\in I$，$(a, b)=1$，p_i是第i个正有理素数。则对任意$n\in N$，存在u，$v\in I$，使$au+bv=1$，且对任意$i\leqslant n$，有$p_i\nmid u$。

引理3 设$a, b, c\in I$，a不是平方数，$(b, c)=1$。则存在$m\in N$，对任意$n\in N$，$n>m$，K_n中存在$bx+c$形元以a为平方剩余；且K_n也存在$bx+c$形元不以a为平方剩余。

证明 因为a不是平方数，由引理1，知存在无限多个素数p，使$\left(\frac{a}{p}\right)=1$，取一个这样的$p$，使$p>b$。令$m=p$，对任意$n>m$，由$(p, b)=1$，用引理2，可找到$u$，$v\in I$，使$pu+bv=1$，且对任意$i\leqslant n$，$p_i\nmid u$。再由$(b, c)=1$，用Dirichlet定理知$\mathbf{N}$中存在无限多个素元$q$，使$q$为$bx+c$形。任取一个这样的素数$q=bx+c>p_n$，则$(q, p_1^{s}\cdots p_n^{s})=1$。因此也有$(qu, p_1^{s}\cdots p_n^{s})$

1984年9月5日收到。

$=1$。于是存在y，$z\in I$，使$quy+p_1^{a_1}\cdots p_n^{a_n}z=1$。

因为$\left(\frac{a}{p}\right)=1$，存在$k$，$l\in I$，使$a=l^2+kp$，这样

$$a=l^2+kp(quy+p_1^{a_1}\cdots p_n^{a_n}z)=l^2+kpquy+kpzp_1^{a_1}\cdots p_n^{a_n}。$$

在K_n中即为$a=l^2+kpquy$，或$a\equiv l^2\pmod{pqu}$。

由$(qu,\ p_1^{a_1}\cdots p_n^{a_n})=1$，知$pqu$是$K_n$中素元。而由$pqu$的取法可看出是$bx+c$形元。

另一个结论同样可证。

定理 设a，b，$c\in I$，a不是平方数，$(b,\ c)=1$，则R中存在$bx+c$形素元以a为平方剩余。R中也存在$bx+c$形素元不以a为平方剩余。

证明 用引理3，及模型论中超积基本定理即可证。只要注意："存在$bx+c$形素元以a为平方剩余"，及"不以a为平方剩余"可以在一阶语言中形式化表示出来。

参 考 文 献

[1]王世强，北京师范大学学报，1(1982)，17—22.
[2]王世强，武涛，同 上，3(1982)，21—25.
[3]王世强，中国科学A辑，1984 Ⅰ，16—23.
[4] 同 上，1984 Ⅲ，210—216.