西 南 师 范 大 学 学 报
1987年1月 JOURNAL OF SOUTHWEST TEACHERS UNIVERSITY 第1期

关于覆盖同余式的若干结果

孙智伟 孙智宏
（南京大学数学系）

【摘 要】

本文给出了k阶同余覆盖系的某些性质．利用这些性质，我们证明并改进了一个由J. L. Selfridge观察到的结果，还得出对任意自然数k，k阶同余覆盖系只有有限个．

如果每个整数x都至少满足下面同余式组

$$x\equiv a_1 \pmod{n_1},\ x\equiv a_2 \pmod{n_2},\ \cdots,\ x\equiv a_k \pmod{n_k} \tag{1}$$

中的一个，则称(1)为一组覆盖同余式，并称

$$a_1(n_1),\ a_2(n_2),\ \cdots,\ a_k(n_k) \tag{2}$$

为一个覆盖系(不要求诸n_i互异)．我们说$a_i(n_i)$是多余的，如果覆盖系(2)中去掉$a_i(n_i)$后仍是覆盖系．(2)被称为一个k阶覆盖系，如果对任何$i(1\leqslant i\leqslant k)$，$a_i(n_i)$对于覆盖系(2)都不多余．(2)为$k$阶覆盖系时(2)也记为$\left\{\left(a_i,\ n_i\right\}\right)_{i=1}^{k}$．显然任何一个覆盖系经删除“多余的”后成为一确定阶覆盖系．对于$1<c=n_1<n_2<\cdots<n_k$情形，Erdös, P.[1]征解c任意大时覆盖系的存在性问题，并问各模互异且全为奇数的覆盖系是否存在．Selfridge, J. L.[1]观察到模最多有两个不同素因子时，至少有一个模有平方因子．孙琦、万大庆、旷京华[2]曾用逐步淘汰法则证明有不同的两对数n_i，n_j和n_s，n_t存在，使得$(n_i,\ n_j)>1$，$(n_s,\ n_t)>1$．其中记号$(a,\ b)$表示整数a和b的最大公因数．

本文主要证明以下结果

定理1 设$\left\{\left(a_i,\ n_i\right)\right\}_{i=1}^{k}$为一个$k$阶覆盖系，$1$，$n_1$，$n_2$，$\cdots$，$n_k$中$d(>1)$所整除的模为$n_{i_1}$，$\cdots$，$n_{i_{t(d)}}$，共$t(d)$ $(\geqslant 1)$个，d所不整除的模为$n_{i_{t(d)+1}}$，$\cdots$，n_{i_k}，$n_{i_{k+1}}=1$．则有

(i) a_{i_1}，$\cdots$，$a_{i_{t(d)}}$中至少有$d/(d,[n_{i_{t(d)+1}},\ \cdots,\ n_{i_{k+1}}])$个数mod d互不同余；

(ii) $t(d)\geqslant d/(d,[n_{i_{t(d)+1}},\ \cdots,\ n_{i_{k+1}}])$．

其中记号$[m_1,\ \cdots,\ m_s]$表示m_1，$\cdots$，m_s的最小公倍数．

本文1985年9月28日收到．

定理 2　设$\{(a_i, n_i)\}_{i=1}^{k}$，$\{(b_j, m_j)\}_{j=1}^{l}$分别为 k 阶、l 阶覆盖系。则

(i) $a_1(n_1),\cdots,a_{s-1}(n_{s-1}), a_{s+1}(n_{s+1}), \cdots, a_k(n_k), a_s+b_1n_s(m_1n_s), a_s+b_2n_s(m_2n_s), \cdots, a_s+b_ln_s(m_ln_s)$为一个覆盖系 $(1\leqslant s\leqslant k)$。

(ii) 当$[n_1, \cdots, n_{k-1}]=n_k$时，$a_1(n_1),\cdots, a_{k-1}(n_{k-1}); a_k+b_1n_k(m_1n_k), \cdots, a_k+b_ln_k(m_ln_k)$ 为一个 $k+l-1$ 阶覆盖系。

定理 3　对任意自然数 k，k 阶覆盖系只有有限个。

利用定理 1 我们证明并改进了 Selfridge, J. L. 的命题（估计 Selfridge 没有证明），还改善了文[2]中的结果. 利用定理 2 我们证明了：最小模为 C 的不同模覆盖系如果存在，则有无穷多个无多余的这样的覆盖系. 除此外，定理 1 和定理 2 还有好多重要推论.

定理 1 的证明　我们分两步来证明定理 1：

(1) $t(d)=k>1$ 的情形　设自然数 q 满足的同余式是

$$q\equiv a_{s(q)} \pmod{n_{s(q)}}, \qquad 1\leqslant s(q)\leqslant k$$

于是　$q\equiv q_{s(q)} \pmod d$

故有　$a_{s(1)}, a_{s(2)}, \cdots, a_{s(d)}$

mod d 互不同余，从而 $s(1), s(2), \cdots, s(d)$两两不等，又它们都在 1 与 k 之间，故

$$t(d)=k\geqslant d=d/(d,1)=d/(d, n_{i_{k+1}})$$

可见 $t(d)=k$ 时定理为真。

(2) $1\leqslant t(d)<k$ 的情形　由于$\{(a_i, n_i)\}_{i=1}^{k}$为 k 阶覆盖系，故存在整数 x_0 使得

$$x_0 \not\equiv a_{i_j} \pmod{n_{i_j}} \qquad j=t(d)+1, \cdots, k$$

令 $x_q=x_0+q[n_{i_{t(d)+1}}, \cdots, n_{i_k}]$（$q$ 为任一自然数），则显然也有

$$x_q \not\equiv a_{i_j} \pmod{n_{i_j}} \quad j=t(d)+1, \cdots, k$$

由覆盖系定义可知存在 $s(q)$使得 $1\leqslant s(q)\leqslant t(d)$，且

$$\begin{aligned} x_q &\equiv a_{i_{s(q)}} \pmod{n_{i_{s(q)}}} \\ &\equiv a_{i_{s(q)}} \pmod d \end{aligned}$$

又　$x_l\equiv x_r \pmod d \Longleftrightarrow d\mid (l-r)[n_{i_{t(d)+1}}, \cdots, n_{i_k}]$

$$\Longleftrightarrow \frac{d}{(d_1, [n_{i_{t(d)+1}}, \cdots, n_{i_k}])} \mid \frac{(l-r)[n_{i_{t(d)+1}}, \cdots, n_{i_k}]}{(d, [n_{i_{t(d)+1}}, \cdots, n_{i_k}])}$$

$$\Longleftrightarrow \frac{d}{(d, [n_{i_{t(d)+1}}, \cdots, n_{i_k}])} \mid (l-r)$$

因此　$x_1, x_2, \cdots, x_{d/(d,[n_{i_{t(d)+1}}, \cdots, n_{i_k}])}$

mod d 互不同余，从而

$$a_{i_{s(1)}}, a_{i_{s(2)}}, \cdots, a_{i_{s(d/(d, [n_{i_{t(d)+1}}, \cdots, n_{i_k}]))}}$$

mod d 互不同余．由此得

$$s(1),\ s(2),\ \cdots,\ s(d/(d,\ [n_{i_{t(d)+1}},\ \cdots,\ n_{i_k}]))$$

任意两两不等，但对任何自然数 q，$1\leqslant s(q)\leqslant t(d)$，故

$$t(d)\geqslant d/(d,\ [n_{i_{t(d)+1}},\ \cdots,\ n_{i_k}])=d/(d,\ [n_{i_{t(d)+1}},\ \cdots,\ n_{i_k},\ n_{i_{k+1}}])$$

综合（1）、（2），定理 1 获证．

令 $d=p^\alpha$ 为某模因子，p 为素数，$\alpha\geqslant 1$．设 $p^{\alpha-\delta\alpha}$ 为 1，n_1，n_2，$\cdots$，n_k 中不为 p^α 所整除的模中可能含有的 p 的最高幂次，由定理 1 得

$$t(p^\alpha)\geqslant p^\alpha/(p^\alpha,\ [n_{i_{t(p^\alpha)+1}},\ \cdots,\ n_{i_{k+1}}])=p^\alpha/(p^\alpha,\ p^{\alpha-\delta\alpha})=p^{\delta_\alpha}\qquad(1\leqslant\delta_\alpha\leqslant\alpha)$$

又 $t(p^\alpha)\leqslant k$，故我们有

$$k\geqslant t(p^\alpha)\geqslant p^{\delta_\alpha}\geqslant p\qquad(*)$$

这是定理 1 最有用的特例，由此可得若干重要推论．

推论1.1（改进的 Selfridge 命题）设 $\{(a_i,\ n_i)\}_{i=1}^k$ 为一个 k 阶覆盖系，$1<n_1<n_2<\cdots<n_k$，不同素因子个数多于两个的模不超过两个，则至少有一个模有平方因子．

证 设模 n_1，$\cdots$，n_k 都不含平方因子，令 $[n_1,\ n_2,\ \cdots,\ n_k]=p_1p_2\cdots p_r$ 为标准分解式，这儿 $p_1<p_2<\cdots<p_r$．显然 p_r 所整除的素因子个数不超过两个的模仅可能为下面的 r 个之一：

$$p_r\times 1,\ p_r\times p_1,\ p_r\times p_2,\ \cdots,\ p_r\times p_{r-1}$$

对于 $r=1,2,3$，分别有 $p_r\leqslant t(p_r)\leqslant r+0, r+0, r+1$（$r=3$ 时 $p_1p_2p_3$ 为唯一可能的素因子个数多于两个的模）．这与 p_r 前有 $r-1$ 个不同素数矛盾，故 $r\geqslant 4$，从而 $p_r\geqslant 7$．由条件可知 $p_r\leqslant t(p_r)\leqslant r+2$，而这与 $p_r\geqslant 7$ 矛盾．故原假设不真，明所欲证．

推论1.2 设 $\{(a_i,\ n_i)\}_{i=1}^k$ 为一个 k 阶覆盖系，p 为 $[n_1,\ \cdots,\ n_k]$ 的最小素因子，则对于 $1,2,\cdots,\ k$ 的任一排列 i_1，i_2，$\cdots$，i_k 有

$$[n_{i_1},\ \cdots,\ n_{i_{p-1}}]\mid[n_{i_p},\ \cdots,\ n_{i_k}]$$

证 设 $[n_{i_1},\ \cdots,\ n_{i_{p-1}}]=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ 为标准分解式，由（*）有

$$t(p_i^{e_i})\geqslant p_i>p-1,\ i=1,\ \cdots,\ s$$

但 n_{i_1}，$\cdots$，$n_{i_{p-1}}$ 只是 $p-1$ 个模，故 $p_i^{e_i}$ 至少整除 n_{i_p}，$\cdots$，n_{i_k} 中一个，因此

$$p_i^{e_i}\mid[n_{i_p},\ \cdots,\ n_{i_k}]$$

从而

$$[n_{i_1},\ \cdots,\ n_{i_{p-1}}]=\prod_{i=1}^{s}p_i^{e_i}\mid[n_{i_p},\ \cdots,\ n_{i_k}]$$

由推论 1.2，显然可得

(1) $n_i \mid [n_1, \cdots, n_{i-1}, n_{i+1}, \cdots, n_k]$, $i=1, 2, \cdots, k$.

(2) 所有模都不含平方因子的充要条件是有 $k-p+1$ 个模不含平方因子.

(3) 若模全为奇数，则

$$[n_{i_1}, n_{i_2}] \mid [n_{i_3}, \cdots, n_{i_k}] .$$

推论1.3 对于不同模覆盖系，最大模不为素数幂.

证 若不然，则与 $t(p^\alpha) \geqslant p > 1$ 矛盾.

最后提一下，(*) 式改善了文[2]的结果.

定理 2 的证明 (i) 若对于整数 x，有 $x \not\equiv a_i \pmod{n_i}$, $j=1, \cdots, s-1, s+1, \cdots, k$, 则因 $\left\{(a_i, n_i)\right\}_{i=1}^{k}$ 为 k 阶覆盖系而有 $x \equiv a_s \pmod{n_s}$. 设 $x=a_s+qn_s$，由于 $\left\{\left(b_j, m_j\right)\right\}_{j=1}^{l}$ 为 l 阶覆盖系，故存在 j 使得

$$q \equiv b_j \pmod{m_j} \qquad 1 \leqslant j \leqslant l$$

于是 $\quad x=a_s+qn_s \equiv a_s+b_jn_s \pmod{m_jn_s} \quad (1 \leqslant j \leqslant l)$

因此 (i) 为真.

(ii) 由 (i) 可知

$$a_1(n_1), \cdots, a_{k-1}(n_{k-1}), a_k+b_1n_k(m_1n_k), \cdots, a_k+b_ln_k(m_ln_k)$$

为一个覆盖系，下面来证它的阶数就是 $k+l-1$，为此只需说明其中无多余.

我们先说明 $a_1(n_1), \cdots, a_{k-1}(n_{k-1})$ 都不多余.

设 $1 \leqslant u \leqslant k-1$. 由于 $a_u(n_u)$ 在 $\left\{\left(a_i, n_i\right)\right\}_{i=1}^{k}$ 中不多余，故有整数 x 使得

$$x \not\equiv a_i \pmod{n_i} \qquad i=1, 2, \cdots, k \qquad i \neq u.$$

注意到 $u \neq k$，即得 $x \not\equiv a_k \pmod{n_k}$ 且有

$$x \not\equiv a_i \pmod{n_i} \qquad i=1, 2, \cdots, k-1 \qquad i \neq u \tag{3}$$

由 $x \not\equiv a_k \pmod{n_k}$ 又可得

$$x \not\equiv a_k+b_jn_k \pmod{m_jn_k} \qquad j=1, 2, \cdots, l \tag{4}$$

(3)、(4) 两式表明 $a_u(n_u)$ 不多余.

现在再来说明 $a_k+b_1n_k(m_1n_k), \cdots, a_k+b_ln_k(m_ln_k)$ 都不多余.

设 $1 \leqslant v \leqslant l$. 由于 $b_v(m_v)$ 在 $\left\{\left(b_j, m_j\right)\right\}_{j=1}^{l}$ 中不多余，故有整数 q 使得

$$q \not\equiv b_j \pmod{m_j} \quad j=1, 2, \cdots, l. \quad j \neq v$$

令 $y=a_k+qn_k$，则

$$y \not\equiv a_k+b_jn_k \pmod{m_jn_k} \quad j=1, \cdots, v-1, v+1, \cdots, l \tag{5}$$

如果有 $i(1 \leqslant i \leqslant k-1)$ 使得 $y \equiv a_i \pmod{n_i}$，则因 $n_i \mid [n_1, \cdots, n_{k-1}]$, $[n_1, \cdots, n_{k-1}] \mid n_k$ 而有

$$x \equiv a_k \pmod{n_k} \Rightarrow x \equiv y \pmod{n_k}$$
$$\Rightarrow x \equiv y \pmod{n_i} \Rightarrow x \equiv a_i \pmod{n_i}$$

这与 $a_k(n_k)$ 在 $\left\{\left(a_i, n_i\right)\right\}_{i=1}^{k}$ 中不多余相矛盾. 因此

$$y \not\equiv a_i \pmod{n_i} \qquad i=1, 2, \cdots, k-1 \tag{6}$$

(5)、(6)两式表明 $a_k+b_v n_k(m_v n_k)$不多余.

综上，定理2得证.

推论2.1 如果存在以 $n_1=c>1$ 为最小模（各模皆为大于1的奇数）的不同模覆盖系，则有无穷多个无多余的这样的覆盖系.

证 (i) 设以 $c(>1)$为最小模的不同模覆盖系存在，其中模个数最少的一个必无多余. 假设无多余的以 c 为最小模的不同模覆盖系只有有限个，令$\{(a_i, n_i)\}_{i=1}^{k}$为其中最大模最大的一个，这儿 $c=n_1<n_2<\cdots<n_k$. 由定理2 (i) 知

$$a_1(n_1),\ \cdots,\ a_{k-1}(n_{k-1}),\ a_k+a_1n_k(n_1n_k),\ \cdots,\ a_k+a_kn_k\left(n_k^2\right)$$

为一个覆盖系. 由定理2 (ii) 证明过程的前一半知 $a_1(n_1),\cdots,a_{k-1}(n_{k-1})$均不多余. 在上覆盖系中去掉多余的以后所得的新覆盖系不但各模互异及最小模又为 $n_1=c$，而且其最大模比 n_k还大，这与 $\{(a_i, n_i)\}_{i=1}^{k}$的选择矛盾. 因此若存在以 $c(>1)$ 为最小模的不同模覆盖系，则有无穷多个无多余的这样的覆盖系.

(ii) 类似于 (i) 可证：如果存在诸模全为大于1的奇数的不同模覆盖系，则有无穷多个无多余的这样的覆盖系.

由 (i)、(ii) 推论2.1获证.

推论2.2 设$\{(a_i, n_i)\}_{i=1}^{k}$为一个 k 阶不同模覆盖系，则$\{(0, 2),\ (1, 2)\}\cup\{(1+2a_i, 2n_i)\}_{i=1}^{k}$恰是一个 $k+1$ 阶不同模覆盖系.

证 覆盖系 0(2), 1(2)符合定理2 (ii) 中条件，故$\{(0, 2\}\cup\{(1+2a_i, 2n_i)\}_{i=1}^{k}$为一个 $2+k-1=k+1$ 阶不同模覆盖系，推论2.2证毕.

由推论2.2及

$$0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)$$

是一个5阶不同模覆盖系可知：对于任何不小于5的自然数 k，k 阶不同模覆盖系存在.

定理3的证明 设$n_1,\ n_2,\ \cdots,\ n_k$为一个 k 阶覆盖系诸模，p 为某模素因子，又设 $1, n_1, n_2, \cdots, n_k$中不同的 p 成分（m 的 p 成分为 p^α，意指 $p^\alpha\mid m$ 但 $p^{\alpha+1}\nmid m$）共有 s 个，将它们由小到大排列如下：

$$p^{\alpha_0},\ p^{\alpha_1},\ \cdots,\ p^{\alpha_s}\qquad 0=\alpha_0<\alpha_1<\alpha_2<\cdots<\alpha_s,\ s>1$$

记

$$\delta=\max_{0\leqslant i<s}\{\alpha_{i+1}-\alpha_i\}=\alpha_{j+1}-\alpha_j,\qquad (0\leqslant j<s)$$

由 (*) 式得 $k\geqslant t(p^{\alpha_{j+1}})\geqslant p^{\alpha_{j+1}-\alpha_j}=p^\delta$

而 $$\alpha_s=\alpha_s-\alpha_0=\sum_{i=0}^{s-1}(\alpha_{i+1}-\alpha_i)\leqslant\sum_{i=0}^{s-1}\delta=s\delta$$

故有 $$p^{\alpha_s}\leqslant p^{s\delta}=(p^\delta)^s\leqslant k^s$$

由于模共 k 个，且有不同 p 成分的模不同，又 $t(p^{a_s})\geqslant p$，所以 $(s-1)+p\leqslant k$，即 $s\leqslant k-p+1$。因而

$$p^{a_s}\leqslant k^s\leqslant k^{k-p+1}\leqslant k^{k-1}$$

因为 $k\geqslant t(p)\geqslant p$，故有

$$[n_1,\ \cdots,\ n_k]\leqslant\prod_p k^{k-1}\leqslant\prod_{p<k}k^{k-1}=k^{(k-1)\pi(k)}$$

式中 $\prod_p k^{k-1}$ 的 p 跑过 $[n_1,\ \cdots,\ n_k]$ 的不同素因子；$\pi(k)$ 表示不超过 k 的素数个数。

由上式可见 k 阶覆盖系只有有限个，因此定理 3 成立。

参 考 文 献

[1] Guy, Richard K.: Unsolved Problems in Number Theory, Spring-Verlag, Berlin-Heidelberg, New York, 1981, 140—141.

[2] 孙琦、万大庆、旷京华：并于覆盖同余式组的一个注记，《数学研究与评论》，1984年，第2期，1—3。

SOME RESULTS ON COVERING SYSTEMS OF CONGRUENCES

SUN ZHIWEI　　SUN ZHIHONG

ABSTRACT

$a_i\pmod{n_i}$, $1\leqslant i\leqslant k$ is said to be a k th order covering system if it is a covering system, but none of its subsystems is. In this paper, we give some useful properties of k th order covering systems. Using these properties, we prove and improve a proposition observed by J. L. Selfridge, and obtain that the number of kth order covering systems is finite for any positive integer k.