第20卷第2期 数学研究与评论 Vol. 20 No. 2
2000年5月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION May 2000

关于素幂模的组合同余律*

王 瑞
(云南大学信息学院计算机科学系，昆明 650091)

摘 要：本文将经典的 Wilson 同余关系、Wolstenholme 同余关系等系统地推广到模 p 缩系的各子系上，获得关于模 p，p^2 等一系列基本而重要的组合同余关系，深刻揭示了模 p 各子系及其之间的内在联系，极大丰富了人们对整数的认识.

关键词：k 次剩余系；k 次剩余解系；对称性；限制非剩余系；组合同余关系.
分类号：AMS(1991) 11A05/CLC O156,O157
文献标识码：A **文章编号**：1000-341X(2000)02-0277-06

1 预备知识

设 p 为奇素数，A_p 表示模 p 的最小正缩系.

若 $p=kq+1$，k,q 均为大于等于 1 的整数，则集合

$$R_p(k)=\{r\in A_p : x^k\equiv r(\mathrm{mod}\,p)\text{有解}\} \tag{1}$$

称为模 p 的 k 次剩余系，$\overline{R}_p(k)=A_p\backslash R_p(k)$ 为 k 次非剩余系. 令集合

$$S_p(q)=\{r\in A_p : r^q\equiv 1(\mathrm{mod}\,p), q\text{ 为 }r\text{ 的阶数}\} \tag{2}$$

为模 p 的 q 阶系，则集合

$$Pr(q)=\{r\in A_p : r^q\equiv 1(\mathrm{mod}\,p)\} \tag{3}$$

称为 q 阶系 $S_p(q)$ 的延伸系或扩张系. 易知，

$$R_p(k)=\bigcup_{d|q} S_p(d)=Pr(q) \tag{4}$$

且 $o(R_p(k))=o(Pr(q))=q$，$o(S_p(q))=\varphi(q)$. 这里 $o(X)$ 表示集合 X 的元素个数，$\varphi(\cdot)$ 为 Euler 函数. 令集合

$$T_p^k(r)=\{\tau\in A_p : \tau^k\equiv r(\mathrm{mod}\,p), r\in R_p(k)\} \tag{5}$$

为 k 次剩余 r 解系，简称 k 次 r 解系. 不难看出：集族

$$W_p(k)=\{T_p^k(r_i) : r_i\in R_p(k), i=1,\cdots,q\} \tag{6}$$

是 A_p 的一个分类. 称 $W_p(k)$ 为关于 $R_p(k)$ 的一个划分或 k 次解分类，简记为 $A_p/(k)$. 易知：$o(T_p^k(r_i))=k$，$i=1,\cdots,q$，$o(A_p/(k))=q$.

若 $\forall\, r\in R_p(k)$，均有 $p-r\in R_p(k)$，则称 $R_p(k)$ 为 k 次对称系.

* 收稿日期：1997-09-23；修订日期：1999-07-22
作者简介：王瑞(1960-)，男，北京通县人，云南大学副教授.

若$\forall\ \tau\in T_p^k(r)$，均有 $p-\tau\in T_p^k(r)$，则称 $T_p^k(r)$为 k 次对称解系.

显然，$R_p(k)$为对称系的充分必要条件是 q 为偶数；$T_p^k(r)$为对称系的充分必要条件是 k 为偶数.

若 $p=2kq+1, k, q\geqslant 1$ 为整数，令

$$\overline{R}_p(2k)_k=R_p(k)\backslash R_p(2k)=\{\sigma\in A_p:\sigma^q\equiv -1(\mathrm{mod}\,p)\} \tag{7}$$

为模 p 的限制 $2k$ 次非剩余系. 显然 $o(\overline{R}_p(2k)_k)=q$. 当 q 为奇数时，集合

$$T_p^{2k}(\sigma)_-=\{\tau\in A_p:\tau^{2k}\equiv -\sigma(\mathrm{mod}\,p),\sigma\in\overline{R}_p(2k)_k\} \tag{8}$$

称为模 p 的限制 $2k$ 次非剩余 σ 解系，简称限制 $2k$ 次 σ 解系. 显然，$o(T_p^{2k}(\sigma)_-)=2k$. 事实上，$T_p^{2k}(\sigma)_-=T_p^{2k}(p-\sigma)$. 同样，可构造集合

$$T_p^k(\sigma)_-=\{\tau\in A_p:\tau^k\equiv -\sigma(\mathrm{mod}\,p),\sigma\in\overline{R}_p(2k)_k\}, \tag{9}$$

显然，$T_p^k(\sigma)_-=T_p^k(p-\sigma)$，$o(T_p^k(\sigma)_-)=k$.

2 模 p 组合同余关系

首先给出上述各子系对模 p 的组合同余关系.

定理 2.1 设 $p=kq+1$ 为奇素数，$R_p(k)=\{r_1,r_2,\cdots,r_q\}$，$T_p^k(r_i)=\{\tau_{i1},\tau_{i2},\cdots,\tau_{ik}\}$，$r_i\in R_p(k)$，$i=1,\cdots,q$，则下列多项式组

$$f_i(x)=(x-\tau_{i1})(x-\tau_{i2})\cdots(x-\tau_{ik})-x^k+r_i\quad(i=1,2,\cdots,q) \tag{10}$$

的各项系数均被 p 整除. 即：

$$\sum_{j=1}^{k}\tau_{ij},\cdots,\sum_{j=1}^{k}\frac{\tau_{i1}\tau_{i2}\cdots\tau_{ik}}{\tau_{ij}},(-1)^k\tau_{i1}\tau_{i2}\cdots\tau_{ik}+r_i\equiv 0(\mathrm{mod}\,p),i=1,2,\cdots,q. \tag{11}$$

证明 对任意 $1\leqslant i\leqslant q$，设 $g_i(x)=(x-\tau_{i1})(x-\tau_{i2})\cdots(x-\tau_{ik})$，则 $\tau_{i1},\tau_{i2},\cdots,\tau_{ik}$是同余式

$$g_i(x)\equiv 0(\mathrm{mod}\,p)\quad(i=1,2,\cdots,q) \tag{12}$$

的 k 个解，由定理所设知，$\tau_{i1},\tau_{i2},\cdots,\tau_{ik}$也是同余式

$$h_i(x)=x^k-r_i\equiv 0(\mathrm{mod}\,p)\quad(i=1,2,\cdots,q) \tag{13}$$

的 k 个解. 故同余式

$$f_i(x)=g_i(x)-h_i(x)\equiv 0(\mathrm{mod}\,p)\quad(i=1,2,\cdots,q) \tag{14}$$

有 k 个解，而 $f_i(x)$均是 $k-1$ 次的多项式. 由素模同余式解数的 Lagrange 定理之推论[1,2]知，$f_i(x)$的所有系数被 p 整除.

注意到 $f_i(x)$的首次项 x^{k-1}、一次项 x^1 等项系数以及常数项，便得(11)中等各组合同余关系. □

对于 k 次剩余系 $R_p(k)$，类似地，可得如下结果：

定理 2.2 设 $p=kq+1$，$R_p(k)=\{r_1,r_2,\cdots,r_q\}$，则多项式

$$f(x)=(x-r_1)\cdots(x-r_q)-x^q+1 \tag{15}$$

的所有系数含因数 p，从而，有组合同余关系：

$$\sum_{i=1}^{q}r_i,\cdots,\sum_{i=1}^{q}\frac{r_1r_2\cdots r_q}{r_i},r_1r_2\cdots r_q+(-1)^q\equiv 0(\mathrm{mod}\,p). \tag{16}$$

仿照定理 2.1 或参见文[5]可证明.

对于限制 $2k$ 次非剩余系 $\overline{R}_p(2k)_k$，也有类似的结果：

定理 2.3 设 $p=2kq+1$ 为奇素数，$\overline{R}_p(2k)_k=\{\sigma_1,\sigma_2,\cdots,\sigma_q\}$，则多项式

$$f(x)=(x-\sigma_1)(x-\sigma_2)\cdots(x-\sigma_q)-x^q-1 \tag{17}$$

的所有系均含素因数 p，从而，有

$$\sum_{i=1}^{q}\sigma_i,\ \cdots,\ \sum_{i=1}^{q}\frac{\sigma_1\sigma_2\cdots\sigma_q}{\sigma_i},\ (-1)^q\sigma_1\cdot\sigma_2\cdots\sigma_q-1\equiv 0(\mathrm{mod}p). \tag{18}$$

对于限制 $2k$ 次非剩余解系 $T_q^{2k}(\sigma_i)_-$，有

定理 2.4 设 $p=2kq+1$ 为奇素数，q 为奇数，$T_p^{2k}(\sigma_i)_-=\{\tau_{i1},\tau_{i2},\cdots\tau_{i2k}\}$，$\sigma_i\in\overline{R}_p(2k)_k$，$i=1,2,\cdots,q$，则如下多项式列

$$f_i(x)=(x-\tau_{i1})(x-\tau_{i2})\cdots(x-\tau_{i2k})-x^{2k}-\sigma_i\quad(i=1,2,\cdots,q) \tag{19}$$

的所有系数均含素因子 p.

对于 $T_p^k(\sigma)_-$，也有结果：

定理 2.5 设 $p=2kq+1$ 为奇素数，$T_p^k(\sigma)_-=\{\tau_1,\tau_2,\cdots,\tau_k\}$，$\sigma\in\overline{R}_p(2k)_k$，则多项式

$$f(x)=(x-\tau_1)(x-\tau_2)\cdots(x-\tau_k)-x^k-\sigma \tag{20}$$

的各项系数均能被 p 整除.

定理 2.6 设 $p=kq+1$ 为素数，$S_p(q)=\{\pi_1,\pi_2,\cdots,\pi_{\varphi(q)}\}$，则多项式

$$G_q(x)=(x-\pi_1)\cdots(x-\pi_{\varphi(q)})-F_q(x) \tag{21}$$

的各项系数均含素因子 p. 这里 $F_q(x)$ 为有理数域 Q 上 q 阶分圆多项式.

证明 利用 Möbius 反演公式[2,3] $F_q(x)=\prod_{d|q}(x^d-1)^{\mu(q/d)}$，类似可证(略). 这里 $\mu(\cdot)$ 是 Möbius 函数.

事实上，定理 2.3，2.4，2.5 均可视为定理 2.1 的某些基本推论或重要特例. 这些结论包含象 Wilson 定理那样的同余关系，以及各子系上过去未揭示的各类组合型同余性质.

3 模 p^2 的组合同余关系

在上节讨论及所得结论的基础上，进一步导出关于模 p^2 等组合型同余关系，展示模 p 各子系及其之间深层次性质和规律.

定理 3.1 设 $p=kq+1$ 为奇素数，$r\in R_p(k)$，其 k 次剩余 r 解系 $T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\}$ 为对称的，则当 k 充分大时，多项式

$$g(x)=(x-\tau_1)(x-\tau_2)\cdots(x-\tau_k)=x^k-b_1x^{k-1}+\cdots-b_{k-1}x+\tau_1\tau_2\cdots\tau_k \tag{22}$$

中次数小于 $k-1$ 的所有奇数次项系数均含 p^2 因子，即

$$b_{k-1},b_{k-3},\cdots,b_3\equiv 0(\mathrm{mod}p^2). \tag{23}$$

为此给出如下命题：

命题 3.2 若 $T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\}$，则对(22)式，有

$$g^{(t)}(x)=A_k^tx^{k-t}-A_{k-1}^tb_1x^{k-1-t}+\cdots+(-1)^{k-t}A_t^tb_{k-t},\quad 0\leqslant t<k, \tag{24}$$

其中 $g^{(t)}(x)$ 表示 $g(x)=(x-\tau_1)(x-\tau_2)\cdots(x-\tau_k)$ 的 t 阶导数，$A_m^t=m(m-1)\cdots(m-t+1)$，$m$

$=t,t+1,\cdots,k$；$(-1)^{k-t}b_{k-t}$是 $g(x)$中 x^t 项的系数. 特别地，若 $T_p^k(r)$是对称的，则

$$g^{(t)}(x)|_{x=p}=t!\ \cdot b_{k-t}. \tag{25}$$

证明 首先，将 $g(x)$展开为 k 次多项式，然后对其求 t 阶导数便得(24)；其次，由分析中 Taylor 公式知，

$$(-1)^{k-t}b_{k-t}=g^{(t)}(0)/t!,\quad 0\leqslant t<k. \tag{26}$$

再由 $T_p^k(r)$的对称性，得

$$g^{(t)}(0)=(-1)^{k-t}g^{(t)}(p),\quad 0\leqslant t<k. \tag{27}$$

结合(26)和(27)即知(25)成立.

定理 3.1 的证明 对(22)的多项式 $g(x)$求奇数阶导数 $g^{(t)}(x)$，$(t=1,3,\cdots,k-3)$，在 $x=p$ 处的表述. 一方面，由命题 3.2 的(24)得

$$g^{(t)}(x)|_{x=p}=A_k^t p^{k-t}-A_{k-1}^t b_1 p^{k-1-t}+\cdots+A_{t+1}^t b_{k-1-t}p-t!\ \cdot b_{k-t}, \tag{28}$$

其中 $A_m^t=m(m-1)\cdots(m-t+1)$，$m=k,k-1,\cdots,t+1,t$. 另一方面，再由命题 3.2 的(25)，即 $g^{(t)}(p)=t!\ \cdot b_{k-t}$，有

$$A_k^t p^{k-t}-A_{k-1}^t b_1 p^{k-1-t}+\cdots+A_{t+1}^t b_{k-1-t}p=2t!\ \cdot b_{k-t}. \tag{29}$$

于是，由定理 2.1 知，$p|b_j(j=1,2,\cdots k-1)$. 又因为 k 充分大，且 $k-t\geqslant 3$. 因此，对(29)取模 p^2 得

$$2t!\ b_{k-t}\equiv 0(\mathrm{mod}\,p^2), \tag{30}$$

而 $1\leqslant t\leqslant k-3<p$，故 $b_{k-t}\equiv 0(\mathrm{mod}\,p^2)$. 分别取 $t=1,3,\cdots,k-3$ 便得(23)各同余关系. □

此结果，当 $k=p-1>2,r=1$ 时，即包含经典的 J. Wolstenholme 同余律：[1,2]

$$\sum_{\tau=1}^{p-1}\frac{(p-1)!}{\tau}\equiv 0(\mathrm{mod}\,p^2). \tag{31}$$

还有 $b_3,\cdots,b_{p-2}\equiv 0(\mathrm{mod}\,p^2)$，因此，我们得到了模 p 缩系上较 J. Wolstenholme 定理更深入的组合型同余律，并且系统地推广到了它的对称子系上. 例如(11)中除首项外，其余各奇次组合积和式在对称性条件下知它们是对模 p^2 同余的.

一般地，有如下同余性质：

定理 3.3 设 $T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\}$，$T_p^k(r)^*=\{p-\tau_1,p-\tau_2,\cdots,p-\tau_k\}$称为 $T_p^k(r)$的伴随系，则 $t=0,1,\cdots,k-2$，有

$$(-1)^{k-t}b_{k-t}\equiv b_{k-t}^*(\mathrm{mod}\,p^2), \tag{32}$$

其中 $(-1)^{k-t}b_{k-t}$是 $g(x)=(x-\tau_1)\cdots(x-\tau_k)$展开式中 x^t 项的系数；$(-1)^{k-t}b_{k-t}^*$是 $g_*(x)=(x-p+\tau_1)(x-p+\tau_2)\cdots(x-p+\tau_k)$展开式中 x^t 项的系数，且 $t!b_{k-t}^*=g^{(t)}(p)$，$t!b_{k-t}=g_*^{(t)}(p)$，特别地，若 $T_p^k(r)=T_p^k(r)^*$，即 $T_p^k(r)$具有对称性，$b_{k-t}=b_{k-t}^*$，该定理就是定理 3.1.

由命题 3.2 及定理 3.1 的证法不难证明(略).

4 几个推论

据 §2，§3 的论证和结论，可推得一些有趣的组合同余律，陈述如下：

推论 4.1 设 $p=kq+1$ 是奇素数，

$$R_p(k)=\{r_1,r_2,\cdots,r_q\},T_p^k(r_i)=\{\tau_{i1},\tau_{i2},\cdots,\tau_{ik}\},r_i\in R_p(k),i=1,\cdots,q,$$

则

$$\sum_{i=1}^{q}\tau_{i1}\tau_{i2}\cdots\tau_{ik}\equiv 0(\mathrm{mod}p),\tag{33}$$

若 q 为偶数，即 $R_p(k)$具有对称性，设 $T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\},T_p^k(p-r)=\{\tau_1^*,\tau_2^*,\cdots,\tau_k^*\}$，则

$$\tau_1\tau_2\cdots\tau_k+\tau_1^*\tau_2^*\cdots\tau_k^*\equiv 0(\mathrm{mod}p)\tag{34}$$

证明 据定理 2.1 的(11)和定理 2.2(16)，立即得(33)和(34).

推论 4.2 设 $p=kq+1$ 为奇素数，$T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\}$，则对任何整数 n，有

$$g^{(t)}(n)\equiv A_k^t n^{k-t}(\mathrm{mod}p),t=1,2,\cdots,k-1\tag{35}$$

这里 $g^{(t)}(n)$是多项式 $g(x)=(x-\tau_1)\cdots(x-\tau_k)$的 t 阶导数在 $x=n$ 处的值，亦即为多项式

$$G(x)=(x+n-\tau_1)(x+n-\tau_2)\cdots(x+n-\tau_k)$$

的 x^t 的项系数 $B_{k-t}(n)$的 $t!$ 倍：$t!\ B_{k-t}(n)=G^{(t)}(0)=g^{(t)}(n)$. 故(35)又可写成

$$B_{k-t}(n)\equiv\binom{k}{t}n^{k-t}(\mathrm{mod}p).\tag{36}$$

若 $T_p^k(r)$具有对称性，则

(i) 当 t 为奇数时，且 $k-t>2$，有

$$\frac{g^{(t)}(n)}{t!}=B_{k-t}(n)\equiv\binom{k}{t}n^{k-t}-\binom{k-1}{t}b_1n^{k-1-t}+\sum_{i=1}^{\frac{k-1-t}{2}}\binom{k-2i}{t}b_{2i}n^{k-2i-t}(\mathrm{mod}p^2).\tag{37}$$

(ii) 当 t 为偶数时，且 $k-t>3,t\neq 0$，有

$$\frac{g^{(t)}(n)}{t!}=B_{k-t}(n)\equiv\binom{k}{t}n^{k-t}-\binom{k-1}{t}b_1n^{k-1-t}+\sum_{i=1}^{\frac{k-t}{2}}\binom{k-2i}{t}b_{2i}n^{k-2i-t}(\mathrm{mod}p^2).\tag{38}$$

(iii) 当 $t=0,\tau\in T_p^k(r)$，有

$$\sum_{i=0}^{k/2}b_{2i}\tau^{k-2i}\equiv b_1\tau^{k-1}(\mathrm{mod}p^2).\tag{39}$$

特别地，取 $r=1,\tau=1$，有

$$\sum_{i=0}^{k/2}b_{2i}\equiv b_1(\mathrm{mod}p^2).\tag{40}$$

这里 $(-1)^jb_j$ 为 $g(x)$的 x^{k-j}项系数，$j=0,\cdots,k,b_0=1,b_k=\tau_1\tau_2\cdots\tau_k$.

利用命题 3.2 和定理 2.1，3.1 便证得此推论的各结果. □

推论 4.3 设 $T_p^k(r)=\{\tau_1,\tau_2,\cdots,\tau_k\}$是对称的，则若 t 为奇数，当 $k-t\geqslant 5$ 时，有

$$p(t+1)b_{k-(1+t)}\equiv 2b_{k-t}(\mathrm{mod}p^4).\tag{41}$$

当 $k-t=3$ 时，

$$p(k-2)b_2\equiv 2b_3(\mathrm{mod}p^3).\tag{42}$$

只须注意定理 3.1 的证明过程及结论，便可得证.

5 结束语

关于模 p 子系上的组合同余律问题的研究是十分基础的课题，本文将 k 次剩余理论、素模同余式理论及数学分析工具成功地结合起来创立了研究组合同余律问题的新方法，取得了突破性进展. 获得了系统性的结论. 所建立的一系列基本而重要的组合同余关系，不仅深化了人们对模 p 缩系及其各子系的认识，也为研究数论、组合数学等其它问题提供了重要理论. 同时，为抽象代数建立了大量的事实依据.

参考文献：

[1] 华罗庚. 数论导引 [M]. 北京：科学出版社，1979.

[2] 柯召，孙琦. 数论讲义(上、下册) [M]. 北京：高等教育出版社，1986.

[3] IRELAND K, ROSON M. *A Classical Introdution to Modern Number Theory* [M], New York: Spring-Verlag, 1982.

[4] WANG Rui. *A criterion for irreducible ploynomials over a unique factorization domain R* [J]. Bulletin. Math. Sinica, 1995, **11**: 42-44.

[5] WANG Rui. *Congruence relations for its subsystem of residue with mod p* [J]. Acta Math. Sinica, 1997, **40**(6): 947—950.

[6] WANG Rui. *Some structures of irreducible polynomials over a unique factorization domain R* [J]. J. Math. Res & Exp., 1999, **19**(2): 367—373.

Combin-Congruence Law with Power Modules of Prime

WANG Rui

(Dept. of Comp. Sci., Information College, Yunnan University, Kunming 650091)

Abstract: Results in this paper generalize further to k-residue solution subsystem with mod p Wang Rui's congruence theorem in [5].

Key words: k-residue subsystem; k-residue solution subsystem; symmetric subsystem; combin-congruence law.