关于华罗庚和段学复的一个猜想

张勤海, 曲海鹏 *

山西师范大学数学与计算机科学学院, 临汾 041004

* E-mail: zhangqh@dns.sxnu.edu.cn, orcawhale@163.com

收稿日期: 2008-06-23; 接受日期: 2008-11-17

国家自然科学基金 (批准号: 10671114)、山西省自然科学基金 (批准号: 2008012001) 和山西省回国留学人员 (批准号: [2007]13-56) 资助项目

摘要 设 G 是有限 p -群, $|G| = p^n$. 对于 $0 \leq m \leq n$, G 的 p^m 阶子群的个数记为 $s_m(G)$. 华罗庚和段学复曾经猜想: 对于任意的有限 p -群 G , 只要 $p > 2$, $s_m(G)$ 模 p^3 只可能同余于 $1, 1+p, 1+p+p^2$ 或 $1+p+2p^2$ 等四种情形. 本文对此猜想进行研究, 给出了此猜想成立的一些群类及此猜想不成立的一些群类.

关键词 华段猜想 亚循环 p -群 交换 p -群 内交换 p -群 超特殊 p -群

MSC(2000) 主题分类 20D15

1 引言

设 G 是有限 p -群, $|G| = p^n$. 对于 $0 \leq m \leq n$, G 的 p^m 阶子群的个数记为 $s_m(G)$. Kulakoff 的一个经典结果^[1]断言: 对于素数 $p > 2$, $s_m(G) \equiv 1$ 或 $1+p \pmod{p^2}$. 在这个结果的鼓舞下, 1930 年, 华罗庚和段学复在清华大学组织了有限 p -群讨论班, 研究 p -群 G 的子群个数 $s_m(G) \pmod{p^3}$ 的可能情形. 他们的主要结果见文献 [2, 3]. 特别是段学复证明了下列定理:

定理 1^[2] 设 G 是有限 p -群, $p > 2$, $|G| = p^n$. 令 $\exp(G) = p^{n-\alpha}$. 如果 $2\alpha+1 \leq m \leq n$, 则有

$$s_m(G) \equiv 1, 1+p, 1+p+p^2 \text{ 或 } 1+p+2p^2 \pmod{p^3}.$$

段学复曾在 1983 年对徐明曜说, 当年他和华罗庚猜想: 对于任意的有限 p -群 G , 只要 $p > 2$, $s_m(G) \pmod{p^3}$ 只可能同余于 $1, 1+p, 1+p+p^2$ 或 $1+p+2p^2$ 等 4 种情形. 徐明曜把这个猜想写在文献 [4] 中, 见该文第 211 页中的“问题 1”. 为方便记, 以下简称为华段猜想.

在华罗庚和段学复之后, 继续研究这个问题的文章不多, 值得提出的有文献 [5, 6]. 值得提出的有以下结果.

定理 2^[6] 设 G 是有限 p -群, $p > 2$, $|G| = p^n$. 若 $\exp(G) = p$, 则对满足 $2 \leq m \leq n-2$, 有

$$s_m(G) \equiv 1+p+2p^2 \pmod{p^3}.$$

引用格式: 张勤海, 曲海鹏. 关于华罗庚和段学复的一个猜想. 中国科学 A, 2009, 39(3): 294-298
Zhang Q H, Qu H P. On Hua-Tuans conjecture. Sci China Ser A, 2009, 52(2): 389-393, DOI:
10.1007/s11425-009-0020-z

这说明, 对于方次数为 p 的群, 华段猜想是成立的.

本文继续对华段猜想进行研究. 首先在第 2 节四个定理中给出若干关于华段猜想成立的正面结果, 并在最后的例子中说明, 在一般情形下, 华段猜想是不成立的.

设 G 为有限 p 群, 我们用 $c_m(G)$ 表示 G 的 p^m 阶循环子群的个数, $\Omega_m(G)$ 表示所有阶数不大于 p^m 的元素生成的子群, $\mathcal{U}_m(G)$ 表示 G 中所有形如 a^{p^m} 的元素生成的子群, $e(G)$ 表示 G 的幂指数, $H * K$ 表示 G 的子群 H 与 K 的中心积.

为证明下面的结果, 需要 Rédei 关于内交换 p -群分类 (非交换 p -群被称为内交换的, 如果它的所有真子群皆交换).

引理 3^[7] 设 $p > 2$ 是素数, G 是有限内交换 p -群. 则 G 是下列诸群之一:

(1) 亚循环情形: $M_{(n,m)} = \langle a, b \mid a^{p^n} = b^{p^m} = 1, a^b = a^{1+p^{n-1}} \rangle$, 其中 $n \geq 2, m \geq 1$;

(2) 非亚循环情形: $M_{(n,m,1)} = \langle a, b, c \mid a^{p^n} = b^{p^m} = c^p = 1, [a, b] = c, [c, a] = [c, b] = 1 \rangle$, 其中 n, m 是任意正整数.

2 华段猜想的某些正面结果和反例

首先看华段猜想的正面结果.

我们注意到当 G 为 p^n 阶群时, $s_{n-1}(G) = \frac{p^d-1}{p-1} \equiv 1, 1+p$ 或 $1+p+p^2 \pmod{p^3}$. 即华段猜想总成立. 以下设 $m \leq n-2$.

定理 4 设 $p > 2$ 是素数, 则有限内交换 p -群满足华段猜想.

证明 设 $G = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_s \rangle$, $|G| = p^n$ 且 $e(G) = e$, 其中 $o(a_1) \geq o(a_2) \geq \cdots \geq o(a_s)$. 再设 $M = \langle a_1^p \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_s \rangle$, $K = \langle a_2 \rangle \times \cdots \times \langle a_s \rangle$. 由于当 M 为循环群时, G 为循环群或 p^2 阶初等交换群, 定理显然成立, 故以下假设 M 为非循环群.

设 $1 \leq m \leq n-2$. 下面通过考虑 m 的不同取值来计算 $s_m(G)$ 的值.

情形 1: $m < e$. 此时 $s_m(G) = s_m(M)$. 对 $|G|$ 进行归纳可得结论.

情形 2: $m \geq e$.

设 H 为不含于 M 的 G 的 p^m 阶子群, 则存在 $x \in H \setminus M$, 使得 $H = \langle x \rangle (H \cap M)$. 容易看出 $\langle x \rangle \cap (H \cap M) = \langle x^p \rangle$. 反之, 在 $G \setminus M$ 中任取一元素 x , 再从 M 中取一包含 x^p 的 p^{m-1} 阶子群 L , 就可以得到一个 p^m 阶子群 $\langle x \rangle L$. 注意到 L 与 $L/\langle x^p \rangle$ 的选取是一一对应的, 而 $M = \langle x^p \rangle \times K$, 进而 $L/\langle x^p \rangle \leq K$. 从而 L 有 $s_{m-e}(K)$ 种取法. 又显然 x 有 $p^n - p^{n-1}$ 种取法, 故在不去重数的前提下, 我们得到了 $(p^n - p^{n-1})s_{m-e}(K)$ 个群. 而当我们取定一个 p^m 阶群 H 时, $L = H \cap M$ 是确定的, 但由于 $H \setminus M$ 中有 $p^m - p^{m-1}$ 个元素, 相应地, x 也有 $p^m - p^{m-1}$ 种取法. 去掉重数即知

$$s_m(G) - s_m(M) = p^{n-m} s_{m-e}(K). \quad (1)$$

当 $m = n-2$ 时, $s_{n-2}(M) \equiv 1+p$ 或 $1+p+p^2 \pmod{p^3}$ 且 $s_{n-2-e}(K) \equiv 1 \pmod{p}$. 由等式 (1) 可得 $s_m(G) \equiv 1+p+p^2$ 或 $1+p+2p^2 \pmod{p^3}$.

当 $m < n-2$ 时, 由等式 (1) 可得 $s_m(G) \equiv s_m(M) \pmod{p^3}$. 对 $|G|$ 进行归纳可得结论.

引理 5 设 G 为亚循环 p 群, $p > 2$. 若 $N \trianglelefteq G$ 且 $|N| = p$. 则对于 $1 \leq m \leq e(G)$, 包含 N 的 G 的 p^m 阶循环子群个数为 $\frac{|\Omega_{m-1}(G)|}{p^{m-1}}$.

证明 设 $\langle x \rangle \geq N$, $\langle y \rangle \geq N$ 且 $o(x) = o(y) = p^m$. 则 $N = \langle x^{p^{m-1}} \rangle = \langle y^{p^{m-1}} \rangle$. 由于

$p > 2$, 故亚循环群为正则 p -群. 易知存在整数 i 使得 $(xy^i)^{p^{m-1}} = 1$, 从而 $x \in \langle y \rangle \Omega_{m-1}(G)$. 于是对于任意的包含 N 的 G 的 p^m 阶循环子群 H , 有 $H \leq \langle y \rangle \Omega_{m-1}(G)$. 由于 $\langle y \rangle \Omega_{m-1}(G)$ 中含有 $(p-1)|\Omega_{m-1}(G)|$ 个 p^m 阶元, 从而包含 N 的 G 的 p^m 阶循环子群个数为

$$\frac{(p-1)|\Omega_{m-1}(G)|}{p^{m-1}(p-1)} = \frac{|\Omega_{m-1}(G)|}{p^{m-1}}.$$

定理 6 设 $p > 2$ 是素数, G 为有限亚循环 p -群, $|G| = p^n$, $1 \leq m \leq n$, 则 $s_m(G) \equiv 1, 1+p$ 或 $1+p+p^2 \pmod{p^3}$, 特别地, G 满足华段猜想.

证明 任取 $N \trianglelefteq G$, $|N| = p$. 令 $\overline{G} = G/N$, 若 $m > e(G)$, 易见 $s_m(G) = s_{m-1}(\overline{G})$, 对 $|G|$ 进行归纳可得结论.

下设 $m \leq e(G)$, 由于不包含 N 的 G 的 p^k 阶子群均循环及引理 5 可得

$$s_m(G) = s_{m-1}(\overline{G}) + c_m(G) - \frac{|\Omega_{m-1}(G)|}{p^{m-1}}. \quad (2)$$

由于 $|\Omega_m(G)|/|\Omega_{m-1}(G)| \leq p^2$, 分以下情形讨论:

情形 1 $|\Omega_m(G)|/|\Omega_{m-1}(G)| = p$.

由 $c_m(G) = \frac{|\Omega_m(G)| - |\Omega_{m-1}(G)|}{p^m - p^{m-1}}$, 可得 $c_m(G) = \frac{|\Omega_{m-1}(G)|}{p^{m-1}}$. 再由等式 (2) 可得 $s_m(G) = s_{m-1}(\overline{G})$. 对 $|G|$ 进行归纳可得结论.

情形 2 $|\Omega_m(G)|/|\Omega_{m-1}(G)| = p^2$.

此时 $|\Omega_m(G)| = p^{2m}$, 而 $|\Omega_{m-1}(G)| = p^{2m-2}$. 从而

$$c_m(G) - \frac{|\Omega_{m-1}(G)|}{p^{m-1}} = \frac{|\Omega_m(G)| - |\Omega_{m-1}(G)|}{p^m - p^{m-1}} - \frac{|\Omega_{m-1}(G)|}{p^{m-1}} = p^m.$$

当 $m \geq 3$ 时, 由等式 (2) 可得 $s_m(G) \equiv s_{m-1}(\overline{G}) \pmod{p^3}$, 对 $|G|$ 进行归纳可得结论. 当 $m = 2$ 时, $s_2(G) = 1 + \frac{|\Omega_2(G)| - |\Omega_1(G)|}{p^2 - p} = 1 + p$ 或 $1 + p + p^2$, 当 $m = 1$ 时, $s_1(G) = 1 + p$, 定理仍然成立.

定理 7 设 $p > 2$ 是素数, 则有限超特殊 p -群满足华段猜想.

证明 由文献 [8, 定理 5.2] 及定理 2 可知, 只需设 $G = N * N * \cdots * N * M$, 其中 $N \cong M_{(1,1,1)}$, $M \cong M_{(2,1)}$. 设 $|G| = p^n$, $K = \Omega_1(G)/G'$ 且 $L = G/G'$, 则 $|L| = |\Omega_1(G)| = p^{n-1}$, $|K| = p^{n-2}$. 由于对 p^3 阶群定理显然成立, 故假设 $n \geq 5$. 注意 $\Omega_1(G) = G'$, 于是对任何不含在 $\Omega_1(G)$ 中的子群 H , 均有 $G' \leq H$. 从而对于任意 $1 \leq m \leq n$, 有

$$s_m(G) = s_m(\Omega_1(G)) + s_{m-1}(L) - s_{m-1}(K). \quad (3)$$

下面计算 $s_m(G)$ 的值.

当 $m = n - 2$ 时, 由于 $n \geq 5$, 知 $\Omega_1(G)' = G'$, 从而 $s_{n-2}(\Omega_1(G)) = s_{n-3}(K)$. 由公式 (3) 可得 $s_{n-2}(G) = s_{n-3}(L)$. 而 L 为初等交换群, 易得 $s_{n-2}(G) \equiv 1 + p + 2p^2 \pmod{p^3}$.

当 $1 \leq m \leq n - 3$ 时, 由 L 和 K 均为初等交换群, 易知 $s_{m-1}(L) \equiv s_{m-1}(K) \pmod{p^3}$. 再由公式 (3) 可得 $s_m(G) \equiv s_m(\Omega_1(G)) \pmod{p^3}$. 依定理 2 可得结论.

定理 8 设 $p > 2$ 是素数, 则有限内交换 p -群满足华段猜想.

证明 由引理 3 和定理 6, 可以假设 $G \cong M_{(n,m,1)}$, 且不妨设 $n \geq m$. 设 $M = \langle a^p \rangle \times \langle b \rangle \times \langle c \rangle$, $K = \langle b \rangle \times \langle c \rangle$, 完全仿照定理 4 的证明方法即得.

最后, 我们给出一个华段猜想不成立的例子.

例 9 设 $p \geq 5$ 是素数, G 是具下列定义关系的 p^5 阶群:

$$G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = 1, [b, a] = c, [c, a] = b^p, [c, b] = a^p \rangle,$$

则 $s_3(G) = 1 + p + 3p^2$, 从而 G 不满足华段猜想.

证明 首先由 $d(G) = 2$, $\Phi(G) = \langle a^p, c, b^p \rangle$ 可知, G 的 $p+1$ 个极大子群分别为:

$$H_1 = \langle b, \Phi(G) \rangle = \langle b, a^p, c \rangle \cong M_{(2,1,1)},$$

$$H_2 = \langle a, \Phi(G) \rangle = \langle a, b^p, c \rangle \cong M_{(2,1,1)},$$

$$H_{i+2} = \langle ab^i, \Phi(G) \rangle = \langle ab^i, a^p, c, b^p \rangle, \quad 1 \leq i \leq p-1.$$

下面分析 G 的 p^3 阶子群的个数. 由于它们是 G 的 2-极大子群, 就一定是上述 $p+1$ 个极大子群中某个的极大子群. 注意到这 $p+1$ 个极大子群中任意两个的交都是 $\Phi(G)$, 于是它们的极大子群中, 除 $\Phi(G)$ 外, 任意两个均不相同. 又由于二元生成群有 $1+p$ 个极大子群, 三元生成群有 $1+p+p^2$ 个极大子群. 因此, 为计算 $s_3(G)$, 只要看诸 H_j 中有几个是二元生成的即可. 显然, $H_1 \cong H_2$ 是二元生成的. 下面考虑群 H_{i+2} , $1 \leq i \leq p-1$. 由 $|G| = p^5 \leq p^p$, 根据定理 [9, III, Satz 10.2], G 是正则的. 又由于 $\exp(G') = p$, 于是 G 是 p -交换的, 即成立

$$(xy)^p = x^p y^p, \quad \forall x, y \in G.$$

再注意到 G' 是交换群, 简单的计算可得, 当 $i = \pm 1$ 时, $H \cong M_{(2,1)} \times C_p$ 是三元生成的; 而当 $i^2 \not\equiv 1 \pmod{p}$ 时, $H \cong M_{(2,1,1)}$ 是二元生成的.

这样, 有

$$s_3(G) = \sum_{j=1}^{p+1} s_3(H_j) - p = 2(1+p+p^2) + (p-1)(1+p) - p = 1+p+3p^2.$$

事实上, 我们应用 Magma 搜索了所有的 p^5 阶群 ($5 \leq p \leq 13$), 找出了使华段猜想不成立的群. 它们在 “the SmallGroup database” 中的编号是:

$p = 5$: 4, 7, 11, 22, 23, 43, 44, 47, 49, 51, 55;

$p = 7$: 4, 11, 12, 13, 24, 25, 44, 45, 51, 56, 57, 58, 59;

$p = 11$: 4, 11, 12, 13, 14, 15, 28, 29, 44, 45, 51, 56, 57, 58, 59; 60, 61;

$p = 13$: 4, 11, 12, 13, 14, 15, 16, 30, 31, 52, 53, 59, 64, 65, 66, 67, 68, 69, 70.

并且, 对于所有上述情形都有 $s_3(G) = 1 + p + 3p^2$.

最后, 我们提出下列可供进一步研究的问题.

问题 10 是否存在一个正整数 k , 使得对于 $p > k$ 以及任意的有限 p 群 G 和任意的 i , 都有 $s_i(G) \not\equiv 1 + p + kp^2 \pmod{p^3}$?

致谢 感谢徐明曜教授告知我们这个问题, 并与我们做了有益的讨论. 感谢审稿人有价值的建议, 他(她)的建议帮助我们改进了定理 6 的结论.

参考文献

- 1 Kulakoff A. Über die Anzahl der eigentlichen Untergruppen und der Elemente von gegebener Ordnung in p -Gruppen. *Math Ann*, **104**: 778–793 (1931)
- 2 Tuan H F. An Anzahl theorem of Kulakoff's type for p -groups. *Sci Rep Nat Tsing Hua Univ Ser A*, **5**: 182–189 (1948)
- 3 Hua L K. Some “Anzahl” theorems for groups of prime power orders. *Sci Rep Nat Tsing Hua Univ*, **4**: 313–327 (1947)

- 4 徐明曜. 关于有限 p -群的若干问题. *数学进展*, **14**: 205–226 (1985)
- 5 Dyubyuk P E. On the number of subgroups of certain categories of finite p -groups (in Russian). *Mat Sbornik N S*, **30**(72): 575–580 (1952)
- 6 Berkovich Y. On the number of subgroups of given order in a finite p -group of exponent p . *Proc Amer Math Soc*, **109**: 875–879 (1990)
- 7 Rédei L. Das schiefe Product in der Gruppentheorie. *Comment Math Helvet*, **20**: 225–267 (1947)
- 8 Gorenstein D. Finite Groups. New York: Chelesa Publishing Company, 1980
- 9 Huppert B. Endliche Gruppen I. New York: Springer-Verlag, 1967