

On the number of conjugacy classes in a finite p -group

Antonio VERA-LÓPEZ
(Received February 23, 1988)

Abstract

Let G be a finite p -group of order $p^m = p^{2n+e}$, with n a non-negative integer, p a prime number and $e=0$ or 1 , and let $r(G)$ be the number of conjugacy classes of elements of G . Then the following equality, due to P. Hall, holds ([4], p. 549):

$$r(G) = (p^2 - 1)n + p^e + k(p^2 - 1)(p - 1),$$

For some non-negative integer k . In this paper, we obtain new properties relative to $r(G)$ by the analysis of the number $r_c(gN)$ of conjugacy classes of elements of G that intersect the coset gN , where N is a normal subgroup of G and g any element of G . It contains a number of equations and congruences relating $r(G)$ to other invariants of G . In particular, our results improve the above equality of P. Hall, when G has maximal nilpotent class or $n \leq p+1$. Examples are given, which make our improvements evident.

Introduction

The standard notation of the theory of groups is used in this paper. In the following, G will denote a finite non-abelian p -group of order $p^m = p^{2n+e}$, with n a positive integer, p a prime number, and $e=0$ or 1 , and $r(G)$ denotes the number of conjugacy classes of elements of G . If S is a non-empty subset of G , $r_c(S)$ denotes the number of conjugacy classes of elements of G that intersect S . The lower central series of G is the series $G > Y_2 > \dots > Y_c = 1$ of normal subgroups Y_i of G in which $Y_2 = G' = [G, G]$ is the derived subgroup of G and Y_i is the subgroup generated by the set $\{[x, y] = x^{-1}y^{-1}xy \mid x \in G, y \in Y_{i-1}\}$ for each $i=3, \dots, c$; the number $c-1$ is called the nilpotent class of G . G is said to have maximum degree of commutativity $d = d(G)$ if $[Y_i, Y_j] \leq Y_{i+j+d}$ for all $i, j=1, 2, 3, \dots$ and d is the maximum such integer; obviously $d \geq 0$. It is well-known (cf. [4])

(*) This work has been supported by the University of the Basque Country

that G has nilpotent class at most $m-1$. In case $c=m-1$, and $m \geq 4$, we consider the subgroup $Y_1 \ni Y_4$ of G defined by: Y_1/Y_4 is the centralizer of Y_2/Y_4 in G/Y_4 . Then $|G:Y_1|=p$ and $|Y_1:Y_2|=p$. If Y_1 is an abelian group, then we have $r(G)=p^2-1+p^{m-2}$. Therefore we can suppose that Y_1 is non-abelian.

Specifically we prove the following results:

- A) There exist non-negative integer numbers k_1 and k_2 such that
 - i) $p \cdot r(G) = (p^2-1)(|Z(G)| + n + e + p - 2) + p^{1-e} + k_1 \cdot (p^2-1)(p-1)$
 - ii) $p \cdot r(G) = (p^2-1)(|G/G'|/p + n + e + p - 2) + p^{1-e} + k_2 \cdot (p^2-1)(p-1)$.

In particular if $n \leq p+1$, A) yields

- B) There exist non-negative integer numbers k_3 and k_4 such that
 - i) $r(G) = (p^2-1)(|Z(G)|/p + n - 1) + p^e + k_3 \cdot (p^2-1)(p-1)$.
 - ii) $r(G) = (p^2-1)(|G/G'|/p^2 + n - 1) + p^e + k_4 \cdot (p^2-1)(p-1)$.

Since $|Z(G)| \geq p$ and $|G/G'| \geq p^2$, it is evident that B) improves P. Hall's equality. On the other hand, if p divides $n-2$, then A) also yields

- C) There exist non-negative integer numbers k_5 and k_6 such that
 - i) $r(G) = (p^2-1)(|Z(G)|/p + 1 + (n-2)/p) + p^e + k_5 \cdot (p^2-1)(p-1)$.
 - ii) $r(G) = (p^2-1)(|G/G'|/p^2 + 1 + (n-2)/p) + p^e + k_6 \cdot (p^2-1)(p-1)$.

In case $p=2$, A) ii) yields the best bound possible in the case $|G| \leq 2^7$ for fixed values of $|G/G'|$ greater than 4.

For each real number x , $[x]$ denotes the integral part of x . Then $Y_{[(c-d+1)/2]}$ is an abelian group and for each natural number $j \leq (c-d+1)/2$ such that Y_j is abelian, there exists a non-negative integer k such that

$$|G|r(G) = (k+1) \sum_{i=3}^j |Y_i||Y_{c-(i-1)-d}|(|Y_{i-1}/Y_i|-1) + p^{2m_j} + p^{m_2}(p^{2(m-m_2)}-1) + k \cdot p^{\min(m_2, m_j)} \cdot (p^2-1)(p-1),$$

in which $c-1$ is the nilpotent class of G , d the degree of commutativity of G and p^{m_i} the order of the i th term Y_i of the lower central series of G .

In particular, if G has maximum nilpotent class $(m-1)$ and $j \leq n$ is a natural number such that Y_j is abelian, then the following equalities hold:

- D) i) $p \cdot r(G) = (p^2-1)(j+p-1) + p^{m-2j+1} + k \cdot (p^2-1)(p-1)$ for some $k \geq 0$.

ii) If $d \geq 1$ or $j \leq p$, then we have

$$r(G) = (p^2 - 1)j + p^{m-2j} + k' \cdot (p^2 - 1)(p - 1)$$

for some $k' \geq 0$

(notice that $d \geq 1$, whenever m is odd or $m \geq p + 2$ (cf. [1])).

In general, if $d \geq 1$, there exists $k'' \geq 0$ such that

iii) $r(G) = (p^2 - 1)(p^{d-1}(j - 2) + 2) + p^{m-2j} + k'' \cdot (p^2 - 1)(p - 1).$

(putting $j = n$ in D) ii) we get P. Hall's equality). In addition, by using results of N. Blackburn, C. R. Leedham-Green and Susan MoKay, and R. Shepherd (cf. [1], [5], [8]), we get :

iv) 1) If $p = 3$ and $m \geq 5$, then we have $r(G) = 16 + 3^{m-4} + k_1 \cdot 16$ for some $k_1 \geq 0$.

2) If $p = 5$ and $m \geq 6$, then D) iii) is satisfied substituting d for $[(m - 5)/2]$ and putting $j = [(m - [(m - 5)/2])/2]$.

3) If $p = 7$ and $m \geq 9$, then D) iii) is satisfied substituting d for $[(m - 8)/2]$ and putting $j = [(m - [(m - 8)/2])/2]$.

4) If $p \geq 11$ and $m > 3p - 7$, then D) iii) is satisfied substituting d for $[(m - 3p + 7)/2]$ and putting $j = [(m - [(m - 3p + 7)/2])/2]$.

Theorems and Proofs

THEOREM 1. Suppose that G is a non-abelian p -group of order $p^m = p^{2n+e}$ with n a positive integer, p a prime number and $e = 0$ or 1 . Then there exist non-negative integer numbers k_1 and k_2 such that

- i) $p \cdot r(G) = (p^2 - 1)(|Z(G)| + n + e + p - 2) + p^{1-e} + k_1 \cdot (p^2 - 1)(p - 1).$
- ii) $p \cdot r(G) = (p^2 - 1)(|G/G'|/p + n + e + p - 2) + p^{1-e} + k_2 \cdot (p^2 - 1)(p - 1),$

where $r(G)$ denotes the number of conjugacy classes of elements of G .

PROOF. We claim that there exists $M \trianglelefteq G$ satisfying the following conditions: $G/M \simeq C_p$, $Z(G) \leq M$, and $|Z(M)| \geq p^2$. In fact, we consider $N \trianglelefteq G$ such that $|N| = p^2$. Then $\text{Aut}(N) \simeq C_{p(p-1)}$ or $GL(2, p)$ and consequently $G/C_G(N) \leq C_p$. If N is contained in $Z(G)$ and M is a maximal subgroup of G such that $Z(G) \leq M$ then the above conditions are satisfied. Otherwise, we have $G/C_G(N) \simeq C_p$ and we take $M = C_G(N)$. Thus, in the following we can assume the existence of M . Set $G/M = \langle \bar{g} \rangle \simeq C_p$. Then arguing as in Note E of [2] we have $p \cdot r(G) = (p^2 - 1)s_g + r(M)$, where s_g is the number of conjugacy M -classes of M fixed by the conjugation-automorphism induced by g . Evidently, we have $s_g = |Z(G)| + k'_1 \cdot (p - 1)$ for some $k'_1 \geq 0$, since M contains $Z(G)$, and also by using a result of J.

Poland (cf. [6] Th. (4.2)) we have

$$r(M) = (n+e-1)(p^2-1) + p^{1-e} + (p^2-1)(p-1) + k'_2(p^2-1)(p-1) \text{ for some } k'_2 \geq 0,$$

because $|M| = p^{2(n+e-1)+1-e}$ and M is not of maximal class (for example, $Z(M) \neq C_p$). Now we conclude

$$p \cdot r(G) = (p^2-1)(|Z(G)| + n+e+p-2) + p^{1-e} + k_1 \cdot (p^2-1)(p-1) \text{ for some } k_1 \geq 0.$$

On the other hand, we have $s_g = r_G(gM) \geq r_{G/G'}(gM/G') = |M/G'| = |G/G'|/p$, hence $s_g = |G/G'|/p + k'_3(p-1)$ for some $k'_3 \geq 0$, and arguing as above we get the second equality.

COROLLARY 2. *Suppose that $n \leq p+1$. Then there exist non-negative integers k_3 and k_4 such that*

- i) $r(G) = (p^2-1)(|Z(G)|/p + n-1) + p^e + k_3 \cdot (p^2-1)(p-1)$.
- ii) $r(G) = (p^2-1)(|G/G'|/p^2 + n-1) + p^e + k_4 \cdot (p^2-1)(p-1)$.

PROOF. From Theorem 1 we get $k_i \equiv n-2 \pmod{p}$ and the conditions $k_i \geq 0$ and $n-2 < p$ imply $k_i = n-2 + k_{i+2} \cdot p$ for some $k_{i+2} \geq 0$. Now substituting these values into the equalities of Theorem 1 we get

$$\begin{aligned} r(G) &= (p^2-1)(|Z(G)|/p + n-1) \\ &\quad + ((p^2-1)e + p^{1-e})/p + k_3(p^2-1)(p-1) \\ &= (p^2-1)(|G/G'|/p^2 + n-1) \\ &\quad + ((p^2-1)e + p^{1-e})/p + k_4(p^2-1)(p-1). \end{aligned}$$

Finally we notice that $((p^2-1)e + p^{1-e})/p = p^e$ and therefore we obtain the desired equalities.

Evidently, the equalities given in Corollary 2 improve the following congruence of P. Hall

$$r(G) = (p^2-1)n + p^e + k \cdot (p^2-1)(p-1) \text{ for some } k \geq 0 \text{ (cf. [4]V. 15.2),}$$

whenever $m \leq 2(p+1) + e$.

For example, let us suppose that $p=2$. A theorem of O. Taussky (cf. [4] III. 11.9. a)) asserts that the only non-abelian 2-groups for which $|G:G'|=4$ are the dihedral, semidihedral and generalized quaternion groups. In each of these groups, the number of conjugacy classes is $r(G) = 3 + 2^{m-2}$. Thus we can assume that $|G/G'| \geq 8$ and Corollary 2 yields $r(G) = 3(n+1) + 2^e + k \cdot 3$, for some $k \geq 0$, improving the information given in the above equality of P. Hall. Furthermore, in case $|G| \leq 2^6$ and by using Hall-

Senior's notation (cf. [3]) we obtain best possible bounds. Indeed,

For $|G|=32$ and $|G'|=2$, Corollary 2 yields $r(G)=17+3.k$ and the lower bound $r(G)=17$ is attained for the stem groups of the family Γ_5 .

For $|G|=32$ and $|G'|=4$, Corollary 2 yields $r(G)=11+3.k$ and the lower bound $r(G)=11$ is attained for the stem groups of the family Γ_6, Γ_7 .

For $|G|=64$ and $|G'|=4$, Corollary 2 yields $r(G)=19+3.k$ and the lower bound $r(G)=19$ is attained for the stem groups of the family Γ_{13} .

For $|G|=64$ and $|G'|=8$, Corollary 2 yields $r(G)=13+3.k$ and the lower bound $r(G)=13$ is attained for the stem groups of the family Γ_{22} and Γ_{23} .

Thus our results are best possible, in case $n \leq p+1$. Suppose now that $|G|=2^7$ (and $|G/G'| \geq 8$), then Theorem 1 yields 2. $r(G)=3(|G/G'|/2+3+1)+1+k.3$, with $k \geq 0$; necessarily k is an odd number, that is, $k=1+2k'$ with $k' \geq 0$ and consequently $r(G)=3(|G/G'|/4+2)+2+3.k'$. For $|G/G'|=8$ we have $r(G)=14+3.k'$ and the lower bound $r(G)=14$ is attained for the stem groups of the family Γ_{106} (cf. [7]). In general, if $|G|=2^{4t+3}$ for some $t \geq 0$, then Theorem 1 yields

$$r(G)=3.(|G/G'|/4+t+1)+2+3.k \text{ for some } k \geq 0.$$

COROLLARY 3. *Suppose that p divides $n-2$. Then there exist non-negative integers k_5 and k_6 such that*

- i) $r(G)=(p^2-1)(|Z(G)|/p+1+(n-2)/p)+p^e+k_5 \cdot (p^2-1)(p-1).$
- ii) $r(G)=(p^2-1)(|G/G'|/p^2+1+(n-2)/p)+p^e+k_6 \cdot (p^2-1)(p-1).$

PROOF. This result follows immediately from Theorem 1, arguing as in Corollary 2.

In the following, let d be the degree of commutativity of G and let $c-1$ be the nilpotent class of G . If $(c-d)/2$ is an integer, we have

$$[Y_{(c-d)/2}, Y_{(c-d)/2}] \leq Y_{2(c-d)/2+d} = Y_c = 1,$$

On the other hand, if $(c-d+1)/2$ is an integer, then we have

$$[Y_{(c-d+1)/2}, Y_{(c-d+1)/2}] \leq Y_{c-d+1+d} = Y_{c+1} = 1,$$

Thus, Y_j is an abelian group, in case $j=[(c-d+1)/2]$ (and evidently, Y_v is abelian for each $v \geq (c-d+1)/2$).

In the following we assume that j is any natural number satisfying $j \leq (c-d+1)/2$ and Y_j is abelian. For each $i \leq j$ we have $i \leq (c-d+1)/2$, hence $c-(i-1)-d \geq i$ and consequently $Y_{c-(i-1)-d} \leq Y_i$. Moreover

$$[Y_{c-(i-1)-d}, Y_{i-1}] \leq Y_{c-(i-1)+i-1+d-d} = Y_c = 1$$

whence

$$Y_{c-(i-1)-d} \leq Z(Y_{i-1}) \cap Y_i \text{ for each } i \leq j \tag{1}$$

Next, let us consider a series

$$1 = N_m < N_{m-1} < \dots < N_1 < N_0 = G$$

of normal subgroups N_i of G such that $N_{i-1}/N_i = \langle \bar{x}_i \rangle \simeq C_p$ and $Y_t = N_{m-t}$ for each $t = 2, \dots, c$. Then we have

$$r(G) = s_1(p^2 - 1)/p + s_2(p^2 - 1)/p^2 + \dots + s_m(p^2 - 1)/p^m + 1/|G|$$

where $s_i = r_{N_{i-1}}(x_i N_i)$ is the number of conjugacy N_i -classes of N_i fixed by the automorphism $f_i: N_i \rightarrow N_i$ defined by $f_i(z) = z^{x_i}$ for all $z \in N_i$ (cf. Note E of [2]). We have $N_i \leq Y_j$ if and only if $|N_i| = p^{m-i} \leq |Y_j| = p^{m_j}$, i.e., $m-i \leq m_j$, and N_i is abelian in this case. Furthermore, $s_i = r_{N_{i-1}}(x_i N_i) = |N_i|$ if N_{i-1} is abelian, that is, in case $i \geq m - m_j + 1$. Therefore we have $s_i = p^{m-i}$ for each $i = m - m_j + 1, \dots, m$ and consequently

$$\sum_{i=m-m_j+1}^m s_i/p^i = \sum_{i=m-m_j+1}^m p^{m-i}/p^i = (p^{2m_j} - 1)/(p^m(p^2 - 1)) \tag{2}$$

Thus we have the following decomposition of the number $|G|r(G)$:

$$|G|r(G) = \sum_{i=1}^m s_i p^{m-i}(p^2 - 1) + 1 = \sum_{i=1}^{m-m_j} s_i p^{m-i}(p^2 - 1) + p^{2m_j} \tag{3}$$

Consider the abelian group $G/G' = G/Y_2$ of order p^{m-m_2} . For each i such that $1 \leq i \leq m - m_2$ it is $N_{m-m_2} = Y_2 \leq N_i < N_{i-1}$ and

$$s_i = r_{N_{i-1}}(x_i N_i) \geq r_{N_{i-1}G'}(\tilde{x}_i N_i/G') = |N_i/G'| = p^{m-i}/p^{m_2} = p^{m-m_2-i},$$

hence $s_i = p^{m-m_2-i} + k_i \cdot (p - 1)$ for some $k_i \geq 0$ and consequently

$$\begin{aligned} \sum_{i=1}^{m-m_2} s_i p^{m-i}(p^2 - 1) &= p^{m_2}(p^{2(m-m_2)} - 1) \\ &+ k' p^{m_2}(p^2 - 1)(p - 1) \text{ for some } k' \geq 0 \end{aligned} \tag{4}$$

We now analyse the numbers s_i for $i = m - m_2 + 1, \dots, m - m_j$, these corresponding to groups $N_i < N_{i-1}$ situated into the following chain

$$N_{m-m_j} = Y_j < Y_{j-1} < \dots < Y_3 < Y_2 = N_{m-m_2}.$$

We define $I_i = \{u \mid Y_i \leq N_u < N_{u-1} \leq Y_{i-1}\}$ for each $i = 2, \dots, j$. From (1) we get $s_u = |Y_{c-(i-1)-d}| + k_{iu}(p - 1)$ for some $k_{iu} \geq 0$ and for all $u \in I_i$, consequently

$$\sum_{u \in I_i} s_u p^{m-u}(p^2 - 1) = |Y_{c-(i-1)-d}| \sum_{u=m-m_{i-1}+1}^{m-m_i} p^{m-u}(p^2 - 1)$$

$$+ k_i p^{m_i} (p^2 - 1) (p - 1)$$

for some $k_i \geq 0$ (since $|Y_{i-1}/Y_i| = p^{m_{i-1}-m_i}$ implies $|I_i| = m_{i-1} - m_i$).

Finally, inasmuch as

$$\{m - m_2 + 1, \dots, m - m_j\} = \bigcup_{i=3}^j I_i$$

and

$$\begin{aligned} \sum_{u=m-m_{i-1}+1}^{m-m_i} p^{m-u} &= p^{m_i} ((p^{m_{i-1}-m_i} - 1) / (p - 1)) \\ &= |Y_i| ((|Y_{i-1}/Y_i| - 1) / (p - 1)) \end{aligned}$$

the following theorem holds :

THEOREM 4. *Let j be a natural number such that $j \leq (c - d + 1) / 2$ and Y_j is an abelian group. Then there exists a non-negative integer number k such that*

$$\begin{aligned} |G|r(G) &= \sum_{i=3}^j |Y_i| |Y_{c-(i-1)-d}| (p^2 - 1) ((|Y_{i-1}/Y_i| - 1) / (p - 1)) \\ &\quad + p^{2m_j} + p^{m_2} (p^{2(m-m_2)} - 1) + k \cdot p^{\min\{m_2, m_j\}} (p^2 - 1) (p - 1), \end{aligned}$$

in which, $c - 1$ is the nilpotent class of G , d is the degree of commutativity of G and p^{m_u} is the order of u -th term Y_u of the lower central series of G .

Next, we analyse the case $c = m$, i.e., G has maximal class $m - 1$. In this case, we have $G/Y_2 \simeq C_p \times C_p$ and $Y_{i-1}/Y_i \simeq C_p$ for each $i = 1, \dots, c$. Therefore $m_i = m - i$ and we have

$$\sum_{i=3}^j |Y_i| |Y_{m-(i-1)-d}| ((p - 1) / (p - 1)) = \sum_{i=3}^j p^{m-i} p^{i-1+d} = p^{m-1+d} (j - 2),$$

and Theorem 4 yields $|G|r(G) = (p^2 - 1) p^{m-1+d} (j - 2) + p^{2(m-j)} + p^{m-2} (p^4 - 1) + k \cdot p^{m-j} (p^2 - 1) (p - 1)$ for some $k \geq 0$ and we have

$$\begin{aligned} p^2 r(G) &= (p^2 - 1) p^{1+d} (j - 2) + p^{m-2j+2} \\ &\quad + p^4 - 1 + k' (p^2 - 1) (p - 1) \text{ for some } k' \geq 0 \end{aligned} \tag{5}$$

From the above equality we deduce that p divides $-1 + k' (p^2 - 1) (p - 1)$, hence $k' = 1 + k'' p$ for some $k'' \geq 0$ and $-1 + k' (p^2 - 1) (p - 1) = p^3 - p^2 - p + k'' (p^2 - 1) (p - 1)$. By substituting this latter number in (5) we get

$$\begin{aligned} p \cdot r(G) &= (p^2 - 1) p^d (j - 2) + p^{m-2j+1} + p^3 + p^2 - p - 1 \\ &\quad + k'' (p^2 - 1) (p - 1) \\ &= (p^2 - 1) (p^d (j - 2) + p + 1) + p^{m-2j+1} \end{aligned}$$

$$+ k''(p^2-1)(p-1) \quad (6)$$

Suppose that $d=0$. In this case, (6) implies that p divides $-(j-1)+k''$, so, if $j-1 \not\equiv p$, necessarily we have $k''=j-1+k'''(p^2-1)(p-1)$ for some $k''' \geq 0$ and (6) yields

$$r(G) = (p^2-1)j + p^{m-2j} + k'''(p^2-1)(p-1).$$

Suppose that $d \geq 1$. In this case, $k''=1+k_1''p$ for some $k_1'' \geq 0$ and (6) yields

$$r(G) = (p^2-1)(p^{d-1}(j-2)+2) + p^{m-2j} + k_1''(p^2-1)(p-1)$$

for some $k_1'' \geq 0$.

Thus we have showed

COROLLARY 5. *Let G be a p -group of maximal class $m-1$ and let j be a natural number smaller than or equal to $(m-d)/2$ such that Y_j is an abelian group. Then there exists a non-negative integer k such that*

$$p \cdot r(G) = (p^2-1)(p^d(j-2)+p+1) + p^{m-2j+1} + k \cdot (p^2-1)(p-1).$$

In particular, if $d \geq 1$ or $j \leq p$ then there exists $k' \geq 0$ such that

$$r(G) = (p^2-1)j + p^{m-2j} + k'(p^2-1)(p-1). \quad (7)$$

Furthermore, in case $d \geq 1$ we have

$$r(G) = (p^2-1)(p^{d-1}(j-2)+2) + p^{m-2j} + k''(p^2-1)(p-1) \\ \text{for some } k'' \geq 0.$$

It is well-known that $d \geq 1$ whenever m is an odd number or $m \geq p+2$ (cf. [1]), thus (7) improves P. Hall's result (obtained putting $j=n$ in (7)), indeed if j is smaller than n , then (7) can be written in the following way

$$r(G) = (p^2-1)(j + p^e(p^{n-j-1} + p^{n-j-2} + \dots + p + 1)) \\ + p^e + k'(p^2-1)(p-1).$$

In addition, we have

COROLLARY 6. *Let G be a finite p -group of maximal class $m-1$. Then the following equalities hold :*

- 1) *If $p=3$ and $m \geq 5$, then $r(G) = 16 + 3^{m-4} + k_1 \cdot 16$ for some $k_1 \geq 0$.*
- 2) *If $p=5$ and $m \geq 6$, then we have*

$$r(G) = (5^2-1)(5^{(m-5)/2-1}([(m - [(m-5)/2]) / 2] - 2) + 2) + 5^{m-2[(m-5)/2]} + \\ k_2(5^2-1)(5-1) \\ \text{for some } k_2 \geq 0.$$

3) If $p=7$ and $m \geq 9$, then we have

$$r(G) = (7^2 - 1)(7^{\lfloor (m-8)/2 \rfloor - 1} (\lfloor (m - \lfloor (m-8)/2 \rfloor)/2 \rfloor - 2) + 2) + 7^{m-2\lfloor (m-8)/2 \rfloor} + k_3(7^2 - 1)(7 - 1)$$

for some $k_3 \geq 0$.

4) If $p \geq 11$ and $m \geq 3p - 6$ we have

$$r(G) = (p^2 - 1)(p^{\lfloor (m-3p+7)/2 \rfloor - 1} (\lfloor (m - \lfloor (m-3p+7)/2 \rfloor) - 2) + 2) + p^{m-2\lfloor (m-3p+7)/2 \rfloor} + k_4(p^2 - 1) \cdot (p - 1)$$

for some $k_4 \geq 0$.

PROOF. This result follows directly from the following inequalities (cf. [1], [5], [8]) $d \geq m - 4$ if $p = 3$; $d \geq \lfloor (m - 5)/2 \rfloor$ if $p = 5$; $d \geq \lfloor (m - 8)/2 \rfloor$ if $p = 7$ and $d \geq \lfloor (m - 3p + 7)/2 \rfloor$ for any prime number p .

References

- [1] N. BLACKBURN, On a special class of p -groups, Acta Math. 100, (1958), 45-92.
- [2] W. BURNSIDE, Theory of Groups of Finite Order, 2nd edn., Dover, 1955.
- [3] M. HALL and J. SENIOR, The groups of order 2^m , $m \leq 6$, MacMillan Co., New York, 1964.
- [4] B. HUPPERT, Endliche Gruppen I, Springer-Verlag, Berlin, 1967.
- [5] C. R. LEEDHAM-GREEN and S. MCKAY, On p -groups of maximal class I, Quart. J. Math. Oxford (2), 27 (1976), 297-311.
- [6] J. POLAND, Two problems of finite groups with k conjugate classes, J. Austral. Math. Soc. 8 (1968), 49-55.
- [7] E. RODEMICH, The groups of order 128, J. Algebra, 67 (1980), 129-142.
- [8] R. SHEPHERD, Ph D. Thesis, University of Chicago, 1971.
- [9] A. VERA-LOPEZ, The number of conjugacy classes in a finite nilpotent group, Rend. Sem. Mat. Univ. Padova 73 (1985), 209-216.

Departamento de Matemáticas
Facultad de Ciencias
Universidad del País Vasco