ISRAEL JOURNAL OF MATHEMATICS, Vol. 47, Nos. 2-3, 1984

CONJUGACY CLASSES IN FINITE SOLVABLE GROUPS

BY
ANTONIO VERA LÓPEZ

ABSTRACT

In this note, we obtain the number of conjugacy classes in a finite solvable group as a function of any tuple of the composition factors of G. Using this relation, we give a new elementary proof of one of Mann's results for solvable groups, without using character theory, and we improve this result for some classes of groups.

1. Let G be a finite group of order $|G| = q_1^{e_1} \cdots q_t^{e_t}$, with q_i prime and $q_i \neq q_j$ for every $i \neq j$. We define the numbers

$$d_{|G|} = \text{g.c.d.}(q_1 - 1, \cdots, q_t - 1),$$

$$\delta_{|G|} = \text{g.c.d.}(q_1^2 - 1, \cdots, q_t^2 - 1),$$

$$\mu_{|G|} = \text{g.c.d.}((q_1^2 - 1)(q_1 - 1), \cdots, (q_t^2 - 1)(q_t - 1)),$$

where g.c.d.$(m_i \mid i \in I)$ denote the greatest common divisor of the family of numbers $(m_i \mid i \in I)$. Let $r(G)$ be the number of conjugacy classes of G.

P. Hall (cf. [4] V. 15.2) shows that, if G is a p-group, p prime, then $|G| \equiv r(G)$ $(\text{mod}(p^2 - 1)(p - 1))$.

In 1950 Hirsch proved that $|G| \equiv r(G) \pmod{\delta_{|G|}}$ (cf. [2]) and also that $|G| \equiv r(G) \pmod{2\delta_{|G|}}$ when $|G|$ is odd. A different proof was given by van der Waall in [7].

In 1968 J. Poland (cf. [6]) shows that

$$|G| \equiv r(G) \ (\text{mod g.c.d.}((q_i - 1)^2 \mid i = 1, \cdots, t)).$$

In 1978, A. Mann (cf. [5]) using Brauer's lemma (e.g. [2], (12.1)) shows that

$$(1) \qquad |G| \equiv r(G) \pmod{d_{|G|} \cdot \delta_{|G|}}$$

for each finite group G, generalizing all the above-mentioned results. Moreover,

Received July 10, 1983

it has been pointed out in [7] that one cannot generalize further $|G| \equiv r(G)$ (mod $\mu_{|G|}$).

In this work, we obtain the number of conjugacy classes in a finite solvable group as a function of any tuple of the composition factors of G. Using this relation, we obtain a new proof of Mann's result (1) for solvable groups without using character theory and we investigate some special cases.

In the following, G will denote a finite group. We use the standard notation: $x^y = y^{-1}xy$, $\mathrm{Cl}_G(x) = \{x^g \mid g \in G\}$, $[x, y] = x^{-1}y^{-1}xy$, $G' = \langle [x, y] \mid x, y \in G \rangle$ and if $S \neq \emptyset$ is a subset of G, $S^g = \{z^g \mid z \in S\}$.

LEMMA. *Let $N \trianglelefteq G$ be such that $G/N \simeq C_p$, p prime, and $g \in G - N$. Consider the isomorphism $\psi : N \to N$, $n \mapsto n^g$ and suppose that ψ leaves exactly s conjugacy classes of N unchanged: $\mathrm{Cl}_N(n_1), \cdots, \mathrm{Cl}_N(n_s)$. Then*

(a) $r(G) = ps + (r(N) - s)/p$ (cf. [1] p. 472),

(b) $s \equiv 1$ (mod $d_{|N|}$).

PROOF. The relation $r(G) = ps + (r(N) - s)/p$ is shown by considering the action of G on each $\Omega_x = xN$, $x \in G - N$, given by: $(xn) \cdot y = y^{-1}(xn)y$ $\forall (n, y) \in N \times G$, and using the equation $u_x \cdot |N| = \Sigma_{m \in N} \theta_x(m) = |S_x|$ where $S_x = \{(w, n) \in \Omega_x \times N \mid w^n = w\}$, u_x is the number of orbits of (Ω_x, N) and $\theta_x(m) = |\{w \in \Omega_x \mid w^m = w\}|$.

On the other hand, arguing as in [5] p. 83, there exists a natural number k such that k has exactly order $d_{|N|}$ module any divisor ($\neq 1$) of $|N|$. Now, we consider the permutation $\alpha : n \mapsto n^k$ for each $n \in N$ and let $T = \mathrm{Cl}_N(n_1) \cup \cdots \cup \mathrm{Cl}_N(n_s)$. If $n \in T$, then there is $m \in N$ such that $n^g = n^m$, hence $(n^k)^g = (n^k)^m$ and $n^k \in T$. Thus $T - \{1\}$ is a union of some orbits of this permutation, but the length of each orbit ($\neq \{1\}$) of this permutation is $d_{|N|}$, hence $|T| \equiv 1$ (mod $d_{|N|}$). Finally, as $|\mathrm{Cl}_N(n_i)|$ is a divisor of the order of N, we have $|\mathrm{Cl}_N(n_i)| \equiv 1$ (mod $d_{|N|}$), hence

$$|T| = \sum_{i=1}^{s} |\mathrm{Cl}_N(n_i)| \equiv s \pmod{d_{|N|}},$$

and therefore $s \equiv 1$ (mod $d_{|N|}$).

THEOREM. *Let G be a solvable group, $1 = N_e \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N_0 = G$ a composition series of G such that $N_{i-1}/N_i \simeq C_{p_i}$ $i = 1, \cdots, e$ and $g_{i-1} \in N_{i-1} - N_i$. Then*

$$r(G) = \sum_{i=1}^{e} s_i((p_i^2 - 1)/(p_1 \cdots p_i)) + (1/|G|)$$

where s_i is the number of conjugacy classes of N_i unchanged by the automorphism $\psi_i : N_i \to N_i$, $x \mapsto x^{g_{i-1}}$, $i = 1, \cdots, e$. Moreover $s_i \equiv 1$ (mod $d_{|N_i|}$), $i = 1, \cdots, e$.

PROOF. We have $G/N_1 \simeq C_{p_1}$, hence $r(G) = p_1 s_1 + (r(N_1) - s_1)/p_1$ and $s_1 \equiv 1$ (mod $d_{|N_1|}$) by the lemma. Therefore

(2) $$p_1 r(G) = s_1(p_1^2 - 1) + r(N_1).$$

Similarly, $N_1/N_2 \simeq C_{p_2}$ implies

(3) $$p_2 r(N_1) = s_2(p_2^2 - 1) + r(N_2)$$

with $s_2 \equiv 1 \pmod{d_{|N_2|}}$. Now (2) and (3) imply

$$p_1 p_2 r(G) = s_1(p_1^2 - 1)p_2 + s_2(p_2^2 - 1) + r(N_2).$$

Thus, repeating this argument all times as the length of the composition series of G, we obtain the desirable relation:

(4) $$|G|\, r(G) = p_1 \cdots p_e r(G) = s_1(p_1^2 - 1)p_2 \cdots p_e + \cdots + s_e(p_e^2 - 1) + r(N_e)$$

where $r(N_e) = 1 = s_e$ and $s_i \equiv 1 \pmod{d_{|N_i|}}$ for each $i = 1, \cdots, e$.

REMARK. Let $i \leqq e - 2$. Clearly $s_i = 1$ if and only if N_{i-1} is a Frobenius group of nilpotent kernel N_i and complement $\langle g_{i-1} \rangle$ isomorphic to C_{p_i}. In this case we have $s_e = 1$, $s_{e-1} = p_{e-1}$ and $s_j \neq 1$ for each $j = i + 1, \cdots, e - 2$.

COROLLARY 1. *Let $q_1, \cdots, q_t$ be the primes dividing the order $|G|$ of the solvable group G. Then $|G| \equiv r(G) \pmod{d_{|G|}\delta_{|G|}}$.*

PROOF. Let $1 = N_e \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N_0 = G$ be a composition series of G such that $N_{i-1}/N_i \simeq C_{p_i}$, p_i prime, $i = 1, \cdots, e$. Then $|G| = p_1 \cdots p_e$, $\{p_1, \cdots, p_e\} = \{q_1, \cdots, q_t\}$ and we have the relation (4). Moreover $s_i \equiv 1 \pmod{d_{|N_i|}}$ and $d_{|G|} \mid d_{|N_i|}$ for each $i \neq e$, imply $s_i \equiv 1 \pmod{d_{|G|}}$. So $s_i(p_{i+1} \cdots p_e) \equiv 1 \pmod{d_{|G|}}$ and

$$s_i(p_i^2 - 1) \cdot (p_{i+1} \cdots p_e) \equiv p_i^2 - 1 \pmod{d_{|G|}\delta_{|G|}}.$$

Thus

(5) $$|G|\, r(G) - 1 \equiv \sum_{i=1}^{e} (p_i^2 - 1) \pmod{d_{|G|}\delta_{|G|}}.$$

On the other hand, it can be verified easily, by induction on the number e, that

(6) $$\sum_{i=1}^{e} (p_i^2 - 1) \equiv (p_1 \cdots p_e)^2 - 1 \pmod{d_{|G|}\delta_{|G|}}$$

hence (5) and (6) imply $|G|\, r(G) \equiv |G|^2 \pmod{d_{|G|}\delta_{|G|}}$, so $r(G) \equiv |G| \pmod{d_{|G|}\delta_{|G|}}$, because $\text{g.c.d.}(|G|, d_{|G|}\delta_{|G|}) = 1$.

REMARK. This proof is different from Mann's proof (cf. [5]) and we only use some elementary results of finite group theory. Notice also that the congruence $|G| \equiv r(G) \pmod{\delta_{|G|}}$ is deduced directly from (4), because

$$\text{g.c.d.}((p_1^2 - 1)p_2 \cdots p_e, (p_2^2 - 1)p_3 \cdots p_e, \cdots, p_e^2 - 1) = \text{g.c.d.}(p_1^2 - 1, \cdots, p_e^2 - 1).$$

COROLLARY 2. *Let G be a solvable group of order $q_1^{e_1}\cdots q_t^{e_t}p$, where $\{q_1,\cdots,q_t,p\}$ is the set of different divisor primes of the order of G. If there exists $N \trianglelefteq G$ such that $G/N \simeq C_p$, then*

$$(7)\qquad r(G)\equiv\left(p^2+\sum_{i=1}^{t}e_i(q_i^2-1)\right)(|G|^{-1})\ (\mathrm{mod}\ \delta_{|G|}d_{|N|}).$$

PROOF. Let $N_1 = N$ and $p_1 = p$, with the notation of the theorem. Then we have $|G|r(G)-1=\sum_{i=1}^{e-1}s_i(p_i^2-1)p_{i+1}\cdots p_e+s_e(p_e^2-1)$, with $s_e=1$ and $s_i\equiv 1$ (mod $d_{|N_i|}$) $i=1,\cdots,e-1$. Clearly $d_{|N|}$ is a divisor of $d_{|N_i|}$ for each $i=1,\cdots,e-1$, hence $s_i\equiv 1$ (mod $d_{|N|}$) and arguing as in the theorem, we obtain

$$|G|r(G)-1\equiv\sum_{i=1}^{e}(p_i^2-1)=(p^2-1)+\sum_{i=1}^{t}e_i(q_i^2-1)\ (\mathrm{mod}\ \delta_{|G|}d_{|N|}).$$

EXAMPLES. Let G be a solvable group of order $q_1^{e_1}\cdots q_t^{e_t}\cdot p$ with p the smallest divisor prime of the order of G. Then we can apply Corollary 2 to obtain

$$r(G)\equiv\left(p^2+\sum_{i=1}^{t}e_i(q_i^2-1)(|G|^{-1})\ (\mathrm{mod}\ \delta_{|G|}\cdot \mathrm{g.c.d.}(q_1-1,\cdots,q_t-1)\right).$$

For example, if $|G|=2q_1^{e_1}q_2^{e_2}$ with the q_i odd and primes different from 3, then Mann's result shows that $|G|\equiv r(G)$ (mod 3) and Corollary 2 determine $r(G)$ module $3\cdot$ g.c.d.(q_1-1,q_2-1). If $|G|=11.13^{e_1}\cdot 37^{e_2}$, then (1) determines $r(G)$ module $2^4{\cdot}3$ and (7) determines $r(G)$ module $2^5{\cdot}3^2$.

COROLLARY 3. *Let p and q be two primes such that $p \nmid (q-1)$ and let G a group of order p^nq. Then*

$$(8)\qquad r(G)\equiv((q^2-1)p^n+(p+1)(p^n-1)+1)((p^nq)^{-1})\ (\mathrm{mod}(p-1)\cdot\delta_{|G|}).$$

PROOF. Since $p\nmid(q-1)$, G has a unique Sylow p-subgroup, hence $(q,p,\overset{n}{\cdots},p)$ is a tuple of composition factors of G and with the notation of the theorem, we have

$$|G|r(G)-1=s_1(q^2-1)p^n+s_2(p^2-1)p^{n-1}+\cdots+s_{n+1}(p^2-1)$$

with $s_i\equiv 1$ (mod$(p-1)$). Therefore

$$|G|r(G)-1\equiv(q^2-1)p^n+(p^2-1)((p^n-1)/(p-1))\ (\mathrm{mod}\ z)$$

with $z=$ g.c.d.$((q^2-1)(p-1),(p^2-1)(p-1))=(p-1)\cdot\delta_{|G|}$.

EXAMPLE. Set $|G|=5^n\cdot 7$, then (1) determines $r(G)$ module $2^4{\cdot}3$ and (8) determines $r(G)$ module $2^5{\cdot}3$.

COROLLARY 4. *Let G be a metabelian group. Then*

$$(9)\qquad r(G)\equiv(|G'|-1)\cdot(|G/G'|^{-1})+|G/G'|\ (\mathrm{mod}\ d_{|G|}\cdot\delta_{|G/G'|}).$$

PROOF. We can refine the series $1 \trianglelefteq G' \trianglelefteq G$ to obtain a composition series of $G: 1 = N_e \trianglelefteq N_{e-1} \trianglelefteq \cdots \trianglelefteq N_v = G' \trianglelefteq \cdots \trianglelefteq N_0 = G$ such that $N_{i-1}/N_i \simeq C_{p_i}$ for $i = 1, \cdots, e$. Arguing as in the theorem, we have

$$|G/G'| \cdot r(G) = (p_1 \cdots p_v) \cdot r(G)$$
$$= s_1(p_1^2 - 1)p_2 \cdots p_v + s_2(p_2^2 - 1)p_3 \cdots p_v + \cdots + s_v(p_v^2 - 1) + r(G').$$

But, $r(G') = |G'|$ and $s_i p_{i+1} \cdots p_v \equiv 1 \pmod{d_{|G|}}$, hence

$$|G/G'| r(G) - |G'| \equiv \sum_{i=1}^{v} (p_i^2 - 1) \equiv (p_1 \cdots p_v)^2 - 1 \pmod{d_{|G|}\delta_{|G/G'|}}.$$

Thus we obtain the relation (9).

EXAMPLE. If $|G| = p^2 q$ and $|G'| = p^2$, (9) determines $r(G)$ module $(q^2 - 1) \cdot \text{g.c.d.}(p-1, q-1)$. For example, if $G = A_4$ is the alternating group of degree 4, then $|G/G'| = 3$ and (9) implies $r(G) \equiv 4 \pmod 8$, whereas (1) does not give any information in this easy case.

REMARK. In general, if there exists $N \trianglelefteq G$ such that $|G/N|$ and $r(N)$ are known and G/N is a solvable group, then arguing as in Corollary 4, we obtain the relation

$$r(G) \equiv (r(N) - 1) \cdot (|G/N|^{-1}) + |G/N| \pmod{d_{|G|} \cdot \delta_{|G/N|}}.$$

REFERENCES

1. W. Burnside, *Theory of Groups of Finite Order*, 2nd edn., Dover, 1955.
2. W. Feit, *Characters of Finite Groups*, Academic Press, New York, 1967.
3. K. A. Hirsch, *On a theorem of Burnside*, Q. J. Math. **1** (2) (1950), 97–99.
4. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
5. A. Mann, *Conjugacy classes in finite groups*, Isr. J. Math. **31** (1978), 78–84.
6. J. Poland, *Two problems of finite groups with k conjugate classes*, J. Austral. Math. Soc. **8** (1968), 49–55.
7. R. W. van der Waall, *On a theorem of Burnside*, Elem. Math. **25** (1970), 136–137.

DEPARTAMENTO DE ALGEBRA Y FUNDAMENTOS
FACULTAD DE CIENCIAS MATEMÁTICAS
C/DOCTOR MOLINER S/N BURJASOT, VALENCIA, SPAIN