View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 26, 185–201 (1973)

Structural Constants. I*

ADILSON GONÇALVES

Department of Mathematics, University of Brasilia, Brasil

Communicated by W. Feit

Received February 15, 1972

INTRODUCTION

Let G be a finite group, P a Sylow p-subgroup of G for an odd prime p, and $|G| = g = p \cdot g_0$, $(p, g_0) = 1$.

Fix an element $\pi \in G$ such that $P = \langle \pi \rangle$, and assume $C_G(P) = P$, $q = [N_G(P): P] = p - 1/t \neq p - 1$, where $C_G(P)$, $N_G(P)$ denote the centralizer of P in G and the normalizer of P in G, respectively.

Let $\pi = \pi_1, \pi_2, ..., \pi_t$ be the representatives of conjugacy classes of elements of order p, where $\pi_i \in P$, $1 \leqslant i \leqslant t$. For $1 \leqslant i, j, k \leqslant t$, denote by s_{ijk} the number of times a product of a conjugate of π_i, in $N_G(P)$, by a conjugate of π_j, in $N_G(P)$, equals π_k.

Denote by C_{ijk} the number of times a product of a conjugate of π_i, in G, by a conjugate of π_j, in G, equals π_k.

In this paper we study the relation between these numbers s_{ijk} and C_{ijk}, $1 \leqslant i, j, k \leqslant t$.

We denote $\pi_i^* \in P$ for the representative of π_i^{-1}. Herzog, in his paper "A characterization of the simple group PSL(2, p), $p > 3$" (see [13]), by assuming the situation we are considering here and also the condition $c_{ijk} = s_{ijk}$ for all $(i, j, k) \neq (i, i, i^*)$, $1 \leqslant i, j, k \leqslant t$, was able to show that: "If G is a simple group, then G is isomorphic to PSL(2, p), $p > 3$."

Considering some relations between c_{i11} and s_{i11}, $1 \leqslant i \leqslant t$, we are successful in proving, among other things, some similar results to that of Herzog.

We shall prove in this paper the following results:

THEOREM 1. *If G is a simple group and $s_{i11} = c_{i11}$, for all $i \in \{1, ..., t\}$, then G is isomorphic with* PSL $(2, p)$, $q = (p - 1)/2$ *odd*, $p \geqslant 7$.

* This research is part of the author's Ph.D. Thesis at the University of Chicago, 1971; it was supported by C.N.Pq, Brasil.

Copyright © 1973 by Academic Press, Inc.
All rights of reproduction in any form reserved.

For the other results we assume G satisfying the condition (*) $C_{i11} = 0$ whenever $s_{i11} = 0$ and $1 \leqslant i \leqslant t$.

We also define the rational number $r = r(G, p)$ by

$$r(G, p) = \max \left\{ \frac{c_{i11}}{s_{i11}} \,\middle|\, \begin{matrix} 1 \leqslant i \leqslant t \\ s_{i11} \neq 0 \end{matrix} \right\}.$$

P.S. 1. This number r has some interesting properties as, e.g.,

(i) $r \equiv 1 \pmod p$ as a rational number;

(ii) $\lim_{p\to\infty} r(A_p, p) = \infty$ where A_p is the alternating group on p letters.

THEOREM 2. *If G is a simple group and $r(G, p) \leqslant 2(p+2)/3$, then G is isomorphic with* PSL $(2, p)$, $p \geqslant 7$.

We denote through this paper $\Sigma s_{i11}/t$ by $a(p, t) = a$ (average of s_{i11}'s), and $r(G, p)$ by r.

THEOREM 3. *If G is a simple group with $a = 2$ and $r^2 < 28p$, then G is isomorphic with one of the following groups*:

(i) PSL(2, 11)($p = 11, r = 1$);

(ii) M_{11}, *the Mathieu group on* 11 *letters* ($p = 11, r = 35/2$).

THEOREM 4. *If G is a simple group with $a = 1$ and $r^2 < 1760p$, then G is isomorphic with one of the following groups*:

(i) PSL (2, 7)($p = 7, r = 1$);

(ii) A_7, *the alternating group on* 7 *letters* ($p = 7, r = 36$);

(iii) $U_3(3)$, *unitary group of dimension* 3 *over* GF(3)($p = 7, r = 106$).

P.S. 2. To reduce the length of this paper we will prove Theorem 4 in the particular case $s_{111} = \cdots = s_{t11} = 1$.

P.S. 3. There is a conjecture involving this number r and A_7, the alternating group on 7 letters.

Let x be the degree of the exceptional character in the principal p-block of G. Assume G satisfies our initial conditions.

If G is a simple group and $|G| = g = rpx$, is G isomorphic with A_7?

PRELIMINARIES

Here we present some results and notations (see Brauer [2] and W. Feit [6]) concerning the irreducible characters of $N_G(P)$ and those of G.

The irreducible characters of $N_G(P)$ are in two categories. The first one consists of t characters $\zeta_1, \zeta_2, \ldots, \zeta_t$ of degree $q = [N_G(P) : P]$, vanishing outside P. The second one consists of q linear characters which contain P in their kernel, and the following holds:

$$\sum_{s=1}^{t} \zeta_s(\pi_i) \cdot \zeta_s(\pi_j^{-1}) = \gamma_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases} \qquad \qquad (1)$$

$$\sum_{s=1}^{t} \zeta_s(\pi_i) = -1$$

The exceptional characters of G associated with the ζ_i's will be denoted by ψ_i, $i = 1, 2, \ldots, t$.

We also have

$$\begin{aligned} &\psi_i(1) = x \equiv \gamma/t (\mathrm{mod}\, p), \qquad \text{where} \quad \gamma = \text{sign} = \pm 1, \ 1 \leqslant i \leqslant t; \\ &\psi_i(\pi_j) = \epsilon\zeta_i(\pi_j) + c, \qquad \text{where} \quad \epsilon = \text{sign} = \pm 1, \ 1 \leqslant i, j \leqslant t, \end{aligned} \qquad (2)$$

and c is a rational integer neither depending on i nor on j.

The nonexceptional irreducible characters of G, nonvanishing on $P^* = P - \{1\}$(i.e., in $B_0(p)$, the principal p-block of G) will be denoted by η_i, $i = 1, \ldots, q$, where $\eta_1 = 1_G$, the principal character of G.

We know that each of theses characters η_i is constant on $P^* = P - \{1\}$ and also, if $\eta_i(1) = n_i$ and $\eta_i(\pi_j) = \epsilon_i$, $1 \leqslant j \leqslant t$, $1 \leqslant i \leqslant q$, then the following is true: $\epsilon_i = \text{sign} = \pm 1$, $\epsilon_1 = 1$, and $n_i \equiv \epsilon_i \pmod p$, $1 \leqslant i \leqslant q$.

Let $l = \sum_{i=1}^{q} \epsilon_i/n_i$. Since $\epsilon_1 = 1$ it is easily seen that

$$l \geqslant 1 - \frac{q-1}{p-1} = \frac{p-q}{p-1} \qquad \text{or} \qquad (p-1)l \geqslant p - q. \qquad (3)$$

It is also well known that

$$s_{ijk} = \frac{pq}{p^2}(q + B_{ijk}) = \frac{q}{p}(q + B_{ijk}), \qquad (4)$$

where

$$qB_{ijk} = \sum_{s=1}^{t} \zeta_s(\pi_i) \cdot \zeta_s(\pi_j) \cdot \zeta_s(\pi_k^{-1}), \qquad 1 \leqslant i, j, k \leqslant t;$$

$$C_{ijk} = \frac{g}{p^2}(l + A_{ijk}), \qquad (5)$$

where $|G| = g$,

$$xA_{ijk} = \sum_{s=1}^{t} \psi_s(\pi_i) \cdot \psi_s(\pi_j) \cdot \psi_s(\pi_k^{-1}), \qquad 1 \leqslant i, j, k \leqslant t$$

and x is the degree of the exceptional character in $B_0(p)$. Then

$$tc^2 = 2\epsilon c, \tag{6}$$

where ϵ is the same sign used in (2).

As a corollary we have, c the same rational integer used in (2),

$$t \geqslant 3 \Rightarrow c = 0. \tag{7}$$

Also, if $c = 0$, we get

$$xA_{ijk} = \epsilon q B_{ijk}. \tag{8}$$

1. Theorems 1 and 2

Before we prove Theorems 1 and 2 we will prove some lemmas.

Lemma 1.1.

(a) $$\sum_{i=1}^{t} s_{i11} = q - 1;$$

(b) $$\sum_{i=1}^{t} qB_{i11} = q - p.$$

Proof.

(a) It is quite clear since the orbit of $\pi = \pi_1$ has q elements and there is no i, $1 \leqslant i \leqslant t$, such that $\pi_i \cdot \pi = \pi$.

(b) $$s_{i11} = \frac{q}{p}(q + B_{i11}), \qquad ps_{i11} = q^2 + qB_{i11}.$$

By (a), $p(q-1) = q^2 t + \sum_{i=1}^{t} qB_{i11}$.
Now, since $qt = p - 1$ we have (b).

Proposition 1.2. $r(G, p) \equiv 1 \pmod{p}$ *as a rational number.*

Proof. Since $\sum_{i=1}^{t} s_{i11} = q - 1 \neq 0 \Rightarrow$ some $s_{i11} \neq 0$.
Thus it is enough for us to show that

$$C_{i11} \equiv s_{i11} \pmod{p}.$$

But for this, look at P acting on the set $\Omega = \{(x_i, x_1) \in G \times G \mid x_i \cdot x_1 = \pi_1\}$, by the rule $(x_i, x_1)^c = (x_i^c, x_1^c) = (c^{-1} \cdot x_i \cdot c, c^{-1} x_1 c)$.
Since P is self-centralized, then

$$(x_i, x_1) \notin N_G(P) \times N_G(P) \Rightarrow (x_i, x_1)^c = (x_i^c, x_1^c) \notin N_G(P) \times N_G(P)$$

and also $(x_i, x_1)^c \neq (x_i, x_1)$.

Thus P acts $f.p.f$ on set

$$\Omega^* = \left\{(x_i, x_1) \in G \times G \,\middle|\, \begin{array}{l} x_i \cdot x_1 = \pi_1, \\ (x_i, x_1) \notin N_G(P) \times N_G(P) \end{array}\right\}.$$

Then, $|\Omega^*| \equiv 0 \pmod p$ and $c_{i11} = s_{i11} + |\Omega^*|$.

LEMMA 1.3. *If $t = 2$, we have* (8′)

$$xA_{ijk} = \epsilon' \cdot q \cdot B_{ijk}, \tag{8'}$$

where $\epsilon' = \pm\epsilon$ is a sign.

Proof. Assume $t = 2$.

If $c = 0$, there is nothing to prove by (8).

Let c be different from zero. From (6) we have $c = \epsilon = \pm 1$.

We have two exceptional characters ψ_1, ψ_2 and since $\zeta_1(\pi_j) + \zeta_2(\pi_j) = -1$, $1 \leqslant j \leqslant 2$, we obtain

$$\Psi_1(\pi_j) = \epsilon\zeta_1(\pi_j) + c = \epsilon(\zeta_1(\pi_j) + 1) = -\epsilon\zeta_2(\pi_j), \quad \Psi_2(\pi_j) = -\epsilon \cdot \zeta_1(\pi_j).$$

Thus,

$$x \cdot A_{ijk} = \sum_{s=1} \Psi_s(\pi_i) \cdot \Psi_s(\pi_j)\, \Psi_s(\pi_k^{-1}) = -\epsilon q B_{ijk} \quad \text{for } 1 \leqslant i, j, k \leqslant 2.$$

Remark. Thus we can use

$$xA_{i11} = \epsilon' \cdot qB_{i11} \tag{9}$$

with $\epsilon' = \text{sign} = \pm 1$ for any $t \geqslant 2$.

LEMMA 1.4. *Assume G is a simple group neither of type* (A) $G \approx \mathrm{PSL}(2, p)$ *nor of type* (B) $G \approx \mathrm{SL}(2, p-1)$, *where $p - 1 = 2^a$, $a \geqslant 2$. Then*

$$|G\colon N_G(P)| = g/pq \leqslant r \cdot v,$$

where $v = (q - 1) \cdot (p + q)/p - q$.

Proof. Let x be the degree of exceptional character in $B_0(p)$, the principal p-block of G.

By a Theorem of Feit (see [7]), we have $x \geqslant p + q$.

Now, $C_{i11} \leqslant rs_{i11}$ for all $i \in \{1,\ldots, t\}$.

By (9), $xA_{i11} = \epsilon' qB_{i11}$, where $\epsilon' = \pm 1$.

Thus we obtain

$$\frac{g}{p^2}\left(\frac{\epsilon' q B_{i11}}{x}+l\right) \leqslant \frac{rq^2}{p}+\frac{rq^2}{p}\frac{rqB_{i11}}{p}, \qquad \text{all } i \in \{1,\ldots, t\}$$

and from this we obtain

$$\left(\frac{g\epsilon'}{px}-r\right) qB_{i11} \leqslant rq^2 - \frac{gl}{p}. \tag{10}$$

Applying Lemma 1.1, we have

$$\left(\frac{g\epsilon'}{px}-r\right)(q-p) \leqslant rq(p-1) - \frac{glt}{p}.$$

Therefore

$$\frac{g}{p}\left[\frac{\epsilon'(q-p)}{x}+lt\right] \leqslant rq(p-1) + r(q-p) = r\cdot p(q-1).$$

So

$$g\left[\frac{\epsilon'(q-p)}{x}+lt\right] \leqslant rp^2(q-1).$$

Multiplying both sides by q, we have

$$g\left[\frac{\epsilon' q(q-p)}{x}+l(p-1)\right] \leqslant rp^2q(q-1).$$

Now, we prove that $D = \epsilon' q(q-p)/x + l(p-1) > 0$. Indeed, by (3) we have

$$D = \frac{\epsilon' q(q-p)+l(p-1)x}{x} \geqslant \frac{\epsilon' q(q-p)+(p-q)x}{x}.$$

Since $x \geqslant p+q$, we obtain

$$D \geqslant \frac{\epsilon' q(q-p)+(p-q)(p+q)}{x} = \frac{p-q}{x}[(p+q)-\epsilon' q] > 0.$$

Thus we get

$$g \leqslant \frac{rp^2q(q-1)}{D} = \frac{rp^2q(q-1)}{\dfrac{\epsilon' q(q-p)}{x}+l(p-1)}.$$

By (3) we have

$$g \leqslant \frac{rp^2q(q-1)}{(p-q)\left[1-\dfrac{\epsilon' q}{x}\right]}. \tag{11}$$

Case 1. $\epsilon' = -1$.

Here we obtain

$$g \leqslant \frac{rp^2q(q-1)}{p-q}.$$

Therefore

$$g/pq \leqslant \frac{rp(q-1)}{p-q} \leqslant r(q-1)\,\frac{p+q}{p-q} = r \cdot v.$$

Case 2. $\epsilon' = +1$.

Here,

$$g/pq \leqslant \frac{rp(q-1)}{(p-q)\left[1-\frac{q}{x}\right]}.$$

But

$$x \geqslant p+q \Rightarrow g/pq \leqslant \frac{rp(q-1)}{(p-q)\left(1-\frac{q}{p+q}\right)} = \frac{rp(q-1)(p+q)}{(p-q)p} = r \cdot v$$

and this proves Lemma 1.4.

LEMMA 1.5. *Let G be a simple group. If* $C_{111} = 0$, *then* $p < q^2$.

Proof. Let us assume $C_{111} = 0$ and $p > q^2$.

From $C_{111} = 0 = s_{111}$, we obtain (using (4), (5), (9)) $B_{111} = -q$ and $l + \epsilon' q B_{111}/x = 0$.

Now, from (3) we have $l \geqslant (p-q)/(p-1) > 0$ and we have

$$l = \frac{\epsilon' q^2}{x} > 0 \Rightarrow \epsilon' = +1.$$

Let $x = ap + q$. Thus $ap + q = q^2/l$, and

$$(ap+q) = \frac{(p-1)\,q^2}{(p-1)l} \leqslant \frac{(p-1)\,q^2}{p-q},$$

$$(ap+q)(p-q) \leqslant (p-1)\,q^2.$$

If $a \geqslant 1$, we have

$$(p+q)(p-q) \leqslant (ap+q)(p-q) \leqslant (p-1)\,q^2, \quad p^2 - q^2 \leqslant pq^2 - q^2,$$

and then $p^2 \leqslant pq^2$, i.e., $p \leqslant q^2$, a contradiction and thus $a = 0$ and $x = q < (p-1)$.

By a theorem of Feit we must have G is either of type (A) $G \approx \mathrm{PSL}(2, p)$ or of type (B) $G \approx \mathrm{SL}(q, p-1)$, $p - 1 = 2^a$.

But in type (A), $q = (p-1)/2$ and

$$p > q^2 \Rightarrow 4p > (p-1)^2 \Rightarrow p^2 - 6p + 1 < 0 \Rightarrow p \leqslant 5.$$

By our hypothesis, $p = 5$, $q = t = 2$, and $G \approx \mathrm{PSL}(2,5) \approx A_5$. But here $s_{111} = 0 \neq C_{111}$, a contradiction.

Now, in type (B) we have $s_{111} = 0 \neq C_{111}$, a contradiction.

This proves Lemma 1.5.

Proof of Theorem 1. Assume G simple and $s_{i11} = c_{i11}$ for all $i \in \{1,..., t\}$. From (4), (5), and (9) we have

$$\left(\frac{g\epsilon' q}{px} - q\right) B_{i11} = q^2 - \frac{gl}{p}. \tag{12}$$

Now since $(g\epsilon' q)/(px) - q = 0 \Rightarrow g = px \Rightarrow g < x^2$, a contradiction.

We must have $(g\epsilon' q)/(px) - q \neq 0$ and (12) determines the B_{i11}'s and, moreover, $B_{111} = B_{211} = \cdots = B_{t11}$.

But this implies,

$$s_{111} = s_{211} = \cdots = s_{t11} = c_{t11} = \cdots = c_{111}, \quad A_{111} = A_{211} = \cdots = A_{t11}.$$

From $s_{111} = s_{211} = \cdots = s_{t11}$, we have that G cannot be of type (B) since in this type we have $q = 2$ and this gives $\sum_{i=1}^{t} s_{i11} = q - 1 = 1 \Rightarrow ts_{111} = 1 \Rightarrow t = 1$, a contradiction.

If G is of type (A), we are done since the group $\mathrm{PSL}(2, p)$, with $q = p - 1/2$ even, does not satisfy $s_{i11} = c_{i11}$ for all $i \in \{1,..., t\}$.

Thus we have, by Lemma 1.3, that

$$g/pq \leqslant r \cdot v = 1 \cdot v = v = (q-1)\frac{p+q}{p-q}.$$

Now,

$$\left.\begin{aligned} p + q &= p + \frac{p-1}{t} = \frac{(t+1)p - 1}{t} \\ p - q &= p - \frac{p-1}{t} = \frac{(t-1)p + 1}{t} \end{aligned}\right\} \Rightarrow \frac{p+q}{p-q} < \frac{t+1}{t-1}.$$

Since $(t+1)/(t-1) = 1 + 2/(t-1)$ is a decreasing function of t and $q - 1 = (p - 1/t) - 1 = p - (t+1)/t$, we have for $t \geqslant 2$,

$$v \leqslant 3 \cdot \frac{p-3}{2} \qquad \text{and} \qquad g/pq = mp + 1 \leqslant \frac{3(p-3)}{2}.$$

Then,

$$m < \frac{3(p-3)}{2p} \leqslant \frac{p+3}{2}.$$

By a Theorem of Brauer (see [3]), we have G is of type (A) or (B), and this proves Theorem 1.

Proof of Theorem 2. Assume G is simple and a counter example for Theorem 2.

We first claim that G is not of type (A) or (B). For, G cannot be of type (A) since there either $r = 1$ or $r = 5(p-1)/(p-5)$ (depending if q is odd or even, respectively) and in both situations we do not have G, a counterexample for Theorem 2.

Now, G cannot be of type (B) since for $\mathrm{SL}(2, p-1)$ $p - 1 = 2^a$, we have $s_{111} = 0$ and $c_{111} \neq 0$.

As in the proof of Theorem 1, $v \leqslant (p - 3/2) \times 3$. Hence

$$g/pq \leqslant r \cdot v = \frac{2(p+2)}{3} \times \frac{(p-3)3}{2} = (p+2)(p-3).$$

Thus, $g/pq = mp + 1 \leqslant (p+2)(p-3) \Rightarrow m < p + 2$.

Now, by theorems of Brauer and Nagai ([8]) we must have one of the possibilities for G:

(i) M_{11};

(ii) PSL(3, 3);

(iii) type (A);

(iv) type (B);

(v) $\mathrm{SL}(2, p+1)$, $p + 1 = 2^a$.

The possibility (i) is out since there $m = p + 2$.

The possibilities (iii) and (iv) are out as we saw previously.

The possibility (ii) is out since there we have $s_{111} = 0 \neq c_{111}$, by Lemma 1.5.

Finally, the possibility (v) is also out because there we have $q = 2$ and this implies $s_{111} = 0$.

But, by Lemma 1.5, it is not difficult to see that $C_{111} \neq 0$, and this proves Theorem 2.

2. Theorems 3 and 4

Proof of Theorem 3. Let G be a counterexample for Theorem 3.

We claim that G is not of type (A) nor of type (B). Indeed, if G is of type (A), PSL $(2, p)$ implies that $p = at^2 + t + 1 = 2t^2 + t + 1 = 11$ and $G \approx$ PSL $(2, 11)$ and G is not a counterexample.

If G is of type (B), $\mathrm{SL}(2, p-1)$, $p - 1 = 2^a$ implies that $q = 2 = at + 1 = 2t + 1$, a contradiction.

Thus by Lemma 1.4 $g/pq \leqslant r \cdot v$.

Assume $t > 2$, $p = 2t^2 + t + 1$, and p prime number $\Rightarrow t \geqslant 4 \Rightarrow p > 37$ and $t + 1/t(t-1) \leqslant 5/12$.

But

$$g/pq = mp + 1 \leqslant r \cdot v \leqslant \sqrt{28p} \cdot \frac{p-(t+1)}{t} \cdot \frac{t+1}{t-1}.$$

Thus

$$g/pq = mp + 1 \leqslant (p-5) \cdot \frac{5}{12} \cdot \sqrt{28p}.$$

Therefore $mp < \sqrt{28p}\,(p-5)5/12$. But $p \geqslant 37 \Rightarrow \sqrt{28p} < p$.

So $m < 5/12\,(p-5) < p - 5/2 < p + 3/2$ and by a theorem of Brauer (see [3]) we have a contradiction.

Thus $t = 2$, $p = 2t^2 + t + 1 = 11$, $q = 5$.

We also have $\sqrt{28p} = \sqrt{28 \times 11} < 18$, hence

$$v = (q-1)\frac{p+q}{p-q} = 4 \cdot \frac{16}{6} = \frac{32}{3}.$$

Then, $g/pq = m \times 11 + 1 \leqslant rv < 18 \cdot 32/3 = 192$.

Therefore $11m < 191$. So $m \leqslant 17$.

Also by the theorems of Brauer and Nagai (see [8]), we may assume $m > p + 2 = 13$.

Thus we have $15 \leqslant m \leqslant 17$, $g = 55 \cdot (11m + 1)$.

Since G is simple, we may consider only m odd.

(i) For $m = 15$, $g = 2 \cdot g'$, g' odd, so G is not simple by Burnside (see [11]).

(ii) For $m = 17$, $g = 4 \times 5 \times 11 \times 47$. Again G is not simple by Burnside (see [11]). And this proves Theorem 3.

Proof of Theorem 4. Assume G is a counterexample for Theorem 4. As before G cannot be of type (A) or (B). Thus, by Lemma 1.3, $g/pq \leqslant r \cdot v$.

We also have $q - 1 = \sum_{i=1}^{t} s_{i11} = at = t$, and this gives $p = t^2 + t + 1$, $q = t + 1$.

We also may assume by the theorems of Brauer and Nagai (see [8]) that

$$\frac{g}{pq} = mp + 1,$$

where $m > p + 2$. Thus we have

$$(p+2)p + 1 < g/pq \leqslant r \cdot v < \sqrt{1760}\,\sqrt{p} \cdot \frac{p-(t+1)}{t} \cdot \frac{t+1}{t-1}.$$

We claim that $t < 8$.
For, assume $t \geqslant 8$. Then $p \geqslant 8^2 + 8 + 1 = 73$, and

$$p \cdot (p+2) < \sqrt{1760}\,\sqrt{p}\,(p-7)\,\frac{9}{56}.$$

Therefore

$$(p+2) < \sqrt{1760}\,\sqrt{p} \cdot \frac{9}{56} < \sqrt{1760} \cdot \sqrt{p+2} \cdot \frac{9}{56}.$$

So

$$\sqrt{p+2} < \sqrt{1760} \cdot \frac{9}{56} \quad \text{and} \quad p+2 < \frac{1760 \times 81}{(56)^2}.$$

Then

$$75 \leqslant p+2 < \frac{1760 \times 81}{56 \times 56}.$$

Finally,

$$75 < \frac{142560}{3136} < 46,$$

a contradiction.

Considering also that for $t = 4$, $p = 21$ not prime; for $t = 7$, $p = 49 + 7 + 1 = 57$ not prime, we have the following possibilities for p:

$$\begin{array}{lll} t = 2, & p = 7, & q = 3; \\ t = 3, & p = 13, & q = 4; \\ t = 5, & p = 31, & q = 6; \\ t = 6, & p = 43, & q = 7. \end{array}$$

Now we will assume, as we mention in the introduction, $s_{111} = \cdots = s_{t11} = 1$ (instead of $a = 1$) to shorten this proof.

LEMMA 2.1. Let $|N_G(P)| = p \cdot q$ and let $n < p$ be a solution for $n^q \equiv 1 \pmod p$ and such that $n^s \not\equiv 1 \pmod p$ for $s < q$.

Define the sets $\Omega_1, \Omega_2, \ldots, \Omega_t$ as follows:

$$\Omega_1 = \{1, n, n^2 (\mathrm{mod}\ p), n^3 (\mathrm{mod}\ p), \ldots, n^{q-1} (\mathrm{mod}\ p)\};$$
$$\Omega_2 = \{\alpha_2, \alpha_2 n (\mathrm{mod}\ p), \alpha_2 n^2 (\mathrm{mod}\ p), \ldots, \alpha_2 n^{q-1} (\mathrm{mod}\ p)\},$$

where α_2 is the first integer $\in \{1, 2, \ldots, p-1\} - \Omega_1 = \{x \in \{1, \ldots, p-1\} \mid x \notin \Omega_1\}$. Then

$$\Omega_3 = \{\alpha_3, \alpha_3 n (\mathrm{mod}\ p), \alpha_3 n^2 (\mathrm{mod}\ p), \ldots, \alpha_3 n^{q-1} (\mathrm{mod}\ p)\},$$

where α_3 is the first integer $\in \{1, 2, \ldots, p-1\} - (\Omega_1 \cup \Omega_2)$.

Recursively, define $\Omega_3, \ldots, \Omega_t$ (note: $p - 1 = q \cdot t$).

Let π_{i_k} be a representative of the class containing π^{α_k}, for $k = 1, \ldots, t$, and $\alpha_1 = 1$. (Note: $\pi_{i_1} = \pi_1$.) Then

$$s_{111} = |\{(x, y) \in \Omega_1 \times \Omega_1 \mid x + y = 1 (\text{mod } p)\}|,$$

$$s_{i_2 11} = |\{(x, y) \in \Omega_2 \times \Omega_1 \mid x + y = 1 (\text{mod } p)\}|$$

$$\vdots$$

$$s_{i_t 11} = |\{(x, y) \in \Omega_t \times \Omega_1 \mid x + y = 1 (\text{mod } p)\}|.$$

Proof. First, q divides $p - 1$ and $q \neq 1, p - 1$. Let $U = \{Z/pZ - \{0\}; x\}$ be the multiplicative group of the field Z/pZ. U is cyclic of order $p - 1$. Since $q \mid p - 1$, there exists $W \subseteq U$ such that W is a subgroup of order q and the unique one of such order. Let $W = \langle \bar{n} \rangle$, $n < p$, $\bar{n} = n + pZ \in U$. Then, $\bar{n}^q = \bar{1}$ in $U \Rightarrow n^q = 1$ (mod p) and $n^s \not\equiv 1$ (mod p) for $s < q$, since $|W| = q$.

Thus, the q elements of W are $1, \bar{n}, \bar{n}^2, \ldots, \bar{n}^{q-1}$. This also says that the set $\Omega_1 = \{1; n, n^2 \text{ (mod } p), \ldots, n^{q-1} \text{ (mod } p)\}$ is uniquely determined by any solution n, of $n^q = 1$ (mod p) and $n^s \not\equiv$ (mod p) for $s < q$.

Now we can choose $\alpha_1 = 1, \alpha_2, \alpha_3, \ldots, \alpha_t$ integers as we wish such that

$$U = W \cup W \cdot \bar{\alpha}_2 \cup \cdots \cup W \cdot \bar{\alpha}_t, \text{ where } \bar{\alpha}_i = \alpha_i + pZ, \ 1 \leqslant i \leqslant t.$$

Then, the sets Ω_i, $1 \leqslant i \leqslant t$, are uniquely determined by the cosets $W \cdot \bar{\alpha}_i$, $1 \leqslant i \leqslant t$, and, moreover, the sets Ω_i's are pairwise disjoint and $|\Omega_i| = q$, $1 \leqslant i \leqslant t$.

Now, let $N(P)/C(P) = \langle \sigma \rangle$, σ an automorphism of P, $|\sigma| = q$.

$$\pi = \pi_1, \qquad \pi^\sigma = \pi^{a_\sigma},$$

a_σ an integer > 1.

Also,

$$(\pi^\sigma)^\sigma = (\pi^{a_\sigma})^\sigma = (\pi^\sigma)^{a_\sigma} = \pi^{a_\sigma^2}.$$

Hence, the elements conjugate to π in $N_G(P)$ are

$$\pi^{N(P)} = \{\pi, \pi^{a_\sigma}, \pi^{a_\sigma^2}, \ldots, \pi^{a_\sigma^{q-1}}\}.$$

Since $\sigma^q = 1$, we have a_σ as a solution of equation $n^q = 1$ (mod p), $n^s \not\equiv 1$ (mod p) if $s < q$. Hence,

$$\Omega_1 = \{1, a_\sigma, a_\sigma^2 (\text{mod } p), \ldots, a_\sigma^{q-1} (\text{mod } p)\}.$$

Now $s_{111} = n^0$ of times $\pi^{a_\sigma^i} \cdot \pi^{a_\sigma^j} = \pi = n^0$ of times $\pi^k \cdot \pi^l = \pi$ with $k, l \in \Omega_1 = n^0$ of pairs $(k, l) \in \Omega_1 \times \Omega_1$ such that $k + l = 1$ (mod p).

Now, look at α_2 and choose i_2 such that π_{i_2} is a representative for π^{α_2}. Then

$$\pi_{i_2}^{N(P)} = \{\pi_{i_2} = \pi^{\alpha_2}, \pi_{i_2}^{a_\sigma} = \pi^{\alpha_2 a_\sigma}, \ldots, \pi^{\alpha_2 a_\sigma^{q-1}}\}.$$

Let $\Omega_2 = \{\alpha_2, \alpha_2 a_\sigma \ (\mathrm{mod}\ p), \ldots, \alpha_2 a_\sigma^{q-1} \ (\mathrm{mod}\ p)\}$.
$s_{i_2 11} = n^0$ of times $\pi^{\alpha_2 a_\sigma^i} \cdot \pi^{a_\sigma^j} = \pi = n^0$ of times $\pi^k \cdot \pi^l = \pi$.
$k \in \Omega_2, l \in \Omega_1 = n^0$ of pairs $(k, l) \in \Omega_2 \times \Omega_1$ such that $k + l = 1 \ (\mathrm{mod}\ p)$.
Recursively, we finally obtain

$$\Omega_t = \{\alpha_t, \alpha_t a_\sigma (\mathrm{mod}\ p), \ldots, \alpha_t a_\sigma^{q-1} (\mathrm{mod}\ p)\}$$

and $s_{i_t 11} = n^0$ of pairs $(k, l) \in \Omega_t \times \Omega_1$ such that $k + l = 1 \ (\mathrm{mod}\ p)$. Hence, Lemma 4.4 follows.

Now, we claim the following.

The cases $t = 3, 5, 6$ cannot happen.

For $t = 3, p = 13, q = 4$. Here, following Lemma 2.1, $\Omega_1 = \{1, 5, 12, 8\}$. Now, since $p + 1/2 = 7 \notin \Omega_1 \Rightarrow s_{111}$ is even; hence this case is out.

By the same reasons the cases $t = 5$ and 6 are out.

LEMMA 2.2. *Let $g = pq(mp + 1)$. Then, we have*

(i) $t = 2, p = 7, q = 3$;

(ii) $g = 21(7m + 1)$, where $13 \leqslant m \leqslant 77$, $m = 13 + 4k$, $k = 0, 1, \ldots, 16$.

Proof. (i) We have just proved it.

(ii) Now, $v = (q - 1)(p + q)/p - q = 2 \cdot 10/4 = 5$,

$$r \leqslant \sqrt{1760 \times 7} < 112.$$

Thus, $g/pq = 7m + 1 \leqslant r \cdot v < 5 \times 112 = 560 \Rightarrow m \leqslant 79$. Now, $g = 21 \cdot (7m + 1)$ and G simple implies m odd.

Also $m > p + 2 = 9 \Rightarrow m \geqslant 11$.

But if $m = 11 + 4k$, we have $g = 21 \cdot [7(11 + 4k) + 1]$.

Therefore $g = 21 \cdot (78 + 28k) = 2 \times 21(14k + 39)$ and by a theorem of Burnside (see [11]), we cannot have G simple.

Thus we have $m = 13 + 4k$, $k = 0, 1, \ldots, 16$, and this proves Lemma 2.2.

LEMMA 2.3. *The only simple groups appearing are* (a) A_7; (b) $U_3(3)$, *and this finishes the proof of Theorem* 4, *since they are not counterexamples.*

Proof. By Lemma 2.2, we have $t = 2$, $p = 7$, $q = 3$, $g = 21(7m + 1)$, $13 \leqslant m \leqslant 77$, $m = 13 + 4k$, $k = 0, \ldots, 16$.

(i) $m = 13, g = 2^2 \cdot 3 \cdot 7 \cdot 23$.

Let S be the Sylow 23-subgroups of G. Let $n = [G: N_G(S)]$ and assume $n \neq 1$. Since $[N_G(S): C_G(S)]$ divides 22 and 11 does not divide g, by Burnside ([11]) we may assume $[N_G(S): C_G(S)] = 2$.

Now $n \neq 1$ implies 7 divides n and by calculation we found no such $n \equiv 1 \pmod{23}$ and so this case is out.

(ii) $m = 17, g = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = |A_7|$.

Here A_7 satisfies our hypothesis for $p = 7$ with value $r = 36$, and A_7 is the only simple group with its order.

(iii) $m = 21, g = 2^2 \cdot 3 \cdot 7 \cdot 37$.

Let S be the Sylow 37-subgroup of G. Let $n = [G: N_G(S)]$, $n \equiv 1 \pmod{37}$. By calculation we see that $n = 1$ is the only possibility. Hence, this case is out.

(iv) $m = 25, g = 2^4 \cdot 3 \cdot 7 \cdot 11$.

Let S = Sylow 11 subgroup of G. Let $n = |G: N(S)|$ and assume $n \neq 1$. Hence, $|N(S)/C(S)|$ divides 10 and, by Burnside [7], we may assume $|N(S)/C(S)| = 2$.

As before, $7/n$, and by calculation we see that the only possibility for n is $n = 7 \times 8 = 56$.

Let f_0 = degree of irreducible exceptional character in $B_0(11)$ = principal 11-block, and let f_1 = degree of irreducible, nonidentity, nonexceptional character in $B_0(11)$.

As before, $f_0, f_1/qn = 16 \times 7$, $(f_0, f_1) = 1$, and $f_0 \equiv \pm 2 \pmod{11}$, $f_1 \equiv \pm 1 \pmod{11}$, and this implies that one of $f_i < 21 = 2 \times 11 - 1$ and, by "Stanton condition," $C(S) = S$, a contradiction since $|C(S)| = 11 \times 3$.

(v) $M = 29, g = 2^2 \cdot 3^2 \cdot 7 \cdot 17$.

Let S = Sylow 17-subgroup of G. Let $n = [G: N(S)]$. We know that $N(S)/C(S)$ is cyclic and $|N(S)/C(S)|$ divides 16 and, by Burnside [7], $|N(S)/C(S)| = 2$.

Assuming $n \neq 1$, $7/n$. By calculation we found no number $n \equiv 1 \pmod{17}$ having $7/n$. Hence, this case is out.

(vi) $m = 33, g = 2^3 \cdot 3 \cdot 7 \cdot 29$.

Let S = Sylow 29-subgroup of G. Let $n = [G: N(S)]$. First, if $7/|N(S)|$, then $n/24 \Rightarrow n = 1$, out.

Thus, w.m.a., $7/n$. Also, by Burnside [7], $|N(S)/C(S)| = 2$ or 4.

By calculation we found no number n, $7/n$ such that $n \equiv 1 \pmod{29}$. Hence, this case is out.

(vii) $m = 37, g = 2^2 \cdot 3 \cdot 5 \cdot 13$.

Let S = Sylow 13-subgroup of G. Let $n = [G: N(S)]$ and assume $n \neq 1$. Hence, $|N(S)/C(S)|$ divides 12. By Burnside, $|N(S)/C(S)| = 2, 3$, or 6.

Possibilities for n: After calculation the only possibility for n is

$$n = 14, \quad |N(S)| = 2 \times 3 \times 5 \times 13 \Rightarrow 5/|C(S)|.$$

Now, if $3/|C(S)| \Rightarrow |N(S)/C(S)| = 2$ and $C(S) = S \times V, |V| = 15$. Let $W, V, |W| = 5$. W is the characteristic in $V \lhd N(S) \Rightarrow W \lhd N(S) \Rightarrow [G: N(W)]$ divides 14 and W a S_5-subgroup of $G \Rightarrow |G: N(W)| = 1$, a contradiction. Thus, $3 \nmid |C(S)|$ and $|N(S)/C(S)| = q_0 = 3$ or 6, and also $|C(S)| = 13 \times 5 \times 2$ or 13×5.

Again $W \leqslant C(S), |W| = 5 \Rightarrow W \lhd^{\text{char}} \cdot C(S) \lhd N(S) \Rightarrow N(W) \supseteq N(S) \Rightarrow [G: N(W)]$ divides $14 \Rightarrow [G: N(W)] = 1$, a contradiction. Hence, this case is out.

(viii) $m = 41, g = 2^5 \cdot 3^3 \cdot 7 = |U_3(3)|$.

Here $r = 106$ and, by Wales (see [16]), $U_3(3)$ is the only simple group with its order.

(ix) $m = 45, g = 2^3 \cdot 3 \cdot 7 \cdot 79$.

By calculation the Sylow 79-subgroup S of G is normal in G.

(x) $m = 49, g = 2^3 \cdot 3 \cdot 7 \cdot 43$.

By calculation, the Sylow 43-subgroup of G is normal in G, hence G is not simple.

(xi) $m = 53, g = 2^2 \cdot 3^2 \cdot 7 \cdot 31$.

Let $S =$ Sylow 31-subgroup of G. Let $n = [G: N(S)]$. Assume $n \neq 1$. As before, $7/n$.

By calculation the only possibility for n is $n = 7 \times 9 = 63$.

Now, $|N(S)/C(S)|$ divides 30. By Burnside ([11]), since $5 \nmid g$, we may assume (since $9/n$) $|N(S)/C(S)| = 2$, and we also have $|C(S)| \neq |S|$.

Let f_0 be the degree of exceptional character in $B_0(31) =$ principal 31-block, and let f_1 be the degree of nonidentity, nonexceptional, irreducible character in $B_0(31)$.

By Brauer ([2]), $f_0, f_1/2n = 2 \times 9 \times 7$, $(f_0, f_1) = 1$, and this implies that one of $f_i < (2 \times 31 - 1) = 61$ and this contradicts the "Stanton Condition" ([15]).

(xii) $m = 57, \quad g = 2^4 \cdot 3 \cdot 5$ [illegible] $\cdot 7.$ (12)

We eliminate this case using the following theorems:

Fong [9], Walter [17], Gorenstein–Walter [10], Alperin–Brauer–Gorenstein [1].

(xiii) $m = 61, g = 2^2 \cdot 3 \cdot 7 \cdot 107$.

Here the Sylow 107 is a normal subgroup of G and G is not simple.

(xiv) $m = 65, g = 2^3 \cdot 3^2 \cdot 7 \cdot 19$.

By calculation we see that the Sylow 19-subgroup of G is normal in G. Hence, G is not simple.

(xv) $m = 69, g = 2^3 \cdot 3 \cdot 7 \cdot (11)^2$.

We eliminate this case using the following theorems:

Brauer–Suzuki [5], Walter [17], Gorenstein–Walter [10].

(xvi) $m = 73, 2^9 \cdot 3 \cdot 7$.

We eliminate this case by Wales [16].

(xvii) $m = 77, g = 2^2 \cdot 3^4 \cdot 5 \cdot 7$.

We eliminate this case by Gorenstein–Walter [10]. Thus we found there is no counterexample for Theorem 4.

Acknowledgment

The author wishes to thank Professor G. Glauberman, of the University of Chicago, under whom his doctoral dissertation was written.

References

1. J. L. Alperin, R. Brauer, and D. Gorenstein, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups. I, *Trans. Amer. Soc.* **151** (1970).
2. R. Brauer, On groups whose order contains a prime to the first power, I, II, *Amer. J. Math.* **63** (1942).
3. R. Brauer, On permutation groups of prime degree and related classes of groups, *Ann. Math.* **44** (1943).
4. R. Brauer, On simple groups of order $5 \cdot 3^a \cdot 2^b$, Dept. of Math., Harvard Univ., Cambridge, 1967.
5. R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow subgroups are a quaternion group, *Proc. Nat. Acad. Sci.* **45** (1959).
6. W. Feit, On a class of doubly transitive permutation groups, *Illinois J. Math.* **4** (1960).
7. W. Feit, On finite linear groups, *J. Alg.* **5** (1967).
8. W. Feit, The Current Situation in the Theory of Finite Simple Groups, Dedicated to Richard Brauer on the occasion of his 70th Birthday.
9. P. Fong, Sylow 2-subgroups of small order. I, unpublished.
10. D. Gorenstein and J. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups, I, II, III, *J. Alg.* **2** (1965).
11. M. Hall, "The Theory of Groups," Macmillan, New York, 1959.
12. M. Hall, A search for simple groups of order less than a million, *in* "Computational Problems in Abstract Algebra," edited by J. Leech, Pergamon Press, New York, 1968.
13. M. Herzog, A characterization of the simple groups PSL(2, p), $p > 3$, *Israel J. Math.* **5** (1967).
14. D. Parrot, On the Mathieu groups M_{22} and M_{21}, *J. Austral. Math. Soc.* **XI**, Part 1 (1970).

15. R. Stanton, The Mathieu groups, *Canad. J. Math.* **3** (1951).
16. D. B. Wales, Simple groups of order $7 \cdot 3^a \cdot 2^b$, *J. Algebra* **4** (1970).
17. J. Walter, The characterization of finite simple groups with Abelian Sylow 2-subgroups, *Ann. Math.* **189** (1969), 3.