ON FINITE GROUPS WITH CYCLIC SYLOW SUBGROUPS FOR ALL ODD PRIMES

BY
MARCEL HERZOG

ABSTRACT
Finite simple groups of order divisible by three primes only and the odd Sylow subgroups of which are cyclic are classified.

1. **Introduction.** The purpose of this paper is to classify certain finite groups in which all Sylow subgroups of odd order are cyclic. Although this assumption on Sylow subgroups simplifies the structure of the groups considerably, the problem of their classification is far from being solved. The partial results which are known were obtained under additional assumptions concerning either the structure of a Sylow 2-subgroup P of the group G, or the number of prime divisors of the order of G. To the first type belong results by Zassenhaus [9] for a cyclic P, those of Suzuki [7] dealing with dihedral and generalized quaternion P and the recent paper by Gagen [5] dealing with an Abelian P. To the second type belongs the $p^\alpha q^\beta$-theorem of Burnside, according to which any group whose order is divisible by at most two distinct primes is solvable.

The main result of this paper is the following

THEOREM 1. *Let G be a non-cyclic simple finite group and suppose that all Sylow subgroups of G of odd order are cyclic. Assume also that:*

$$o(G) = p^a u^b w^c$$

where p, u and w are primes. Then G is isomorphic to one of the following groups: $PSL(2,5)$, $PSL(2,7)$, $PSL(2,8)$ and $PSL(2,17)$.

Theorem 1 follows from the following more general result:

THEOREM 2. *Let G be a non-cyclic finite simple group, and suppose that*

$$o(G) = p^a r^b s$$

where p and r are distinct primes and

$$s < p^a - 1, \qquad (pr, s) = 1.$$

Assume also that the Sylow p-subgroup P of G is cyclic and that if $a \geqq 2$ then

Received April 22, 1968.

G has at least two conjugate classes of elements of order p. Then one of the following statements holds.

(I) $a = 1$, $r = 2$ *and G is isomorphic either to* $PSL(2, p)$ *with* $p = 2^m \pm 1$, $p > 3$ *or to* $PSL(2, 2^m)$ *with* $p = 2^m + 1 > 3$.

(II) $a = 2$, $p = 3$, $r = 2$ *and* $G \cong PSL(2, 8)$.

Conversely, these groups satisfy the assumptions of the theorem.

As an immediate corollary from Theorem 2 we get the following

COROLLARY. *Suppose that the group G satisfies the assumptions of Theorem 2, with the exception of the assumption about conjugate classes of elements of order p. Suppose, however, that one of the following conditions holds:*

(a) *either* $p = 3$ *or* $[N_G(P): C_G(P)] \neq p - 1$;

(b) $p - 1$ *does not divide s*;

(c) *s is an odd integer*;

(d) *G contains a cyclic subgroup of order s*;

(e) *r does not divide* $p - 2$.

Then the conclusion of Theorem 2 holds.

The above mentioned results generalize those of [2]. Their proof depends heavily upon properties of characters of groups with a cyclic Sylow subgroup, which are obtained in Section 2. These properties are of independent interest and they are also needed in a forthcoming paper.

In order to deduce Theorem 1 from Theorem 2, the following well-known result is used, for which no reference could be found.

THEOREM 3. *Let* $G \cong PSL(2, q)$, *where* $q = p^m > 3$ *and p is a prime. Assume that* $o(G)$ *is divisible by three primes only. Then G is isomorphic to one of the following groups*:

(A) $p = 2$, $PSL(2,4)$ *and* $PSL(2,8)$;

(B) $p > 2$, $PSL(2,5)$, $PSL(2,7)$, $PSL(2,9)$ *and* $PSL(2,17)$.

We use the standard notation $C_G(T)$, $N_G(T)$, $o(T)$ and $T^{\#}$, where T is a subset of the group G, to denote respectively: the centralizer, normalizer, number of elements and the non-unit elements of T. The commutator subgroup of G will be denoted by G', and if $\sigma \in G$ then $\langle \sigma \rangle$ is the group generated by σ. An element σ of G is called a *p-element* or p'-element, where p is a prime number, according to whether p divides the order of σ or not. If A and B are subgroups of G and A is a normal subgroup of B, then B/A is called a *section* of G. If A/B and C/D are sections of G, and if each coset of B in A has a non-empty intersection with precisely one coset of D in C and each coset of D in C has a non-empty intersection with precisely one coset of B in A, then A/B and C/D are called *incident sections*. We will say that $N_G(A)/C_G(A)$ *acts frobeniusly* on the subgroup A of G if $\alpha^\eta = \alpha$ for $\alpha \in A^{\#}$ and $\eta \in N_G(A)$ implies that $\eta \in C_G(A)$. Finally, if a and b are integers, then (a, b) denotes their greatest common divisor.

2. **Groups with a cyclic Sylow p-subgroup.** In his recent work [3], E. C. Dade extended the results of R. Brauer [1] about blocks of defect 1 to blocks with cyclic defect groups, exploiting a new technique of J. Thompson [8]. Our aim in this section is to show that in the specific case of groups G mentioned in the title, the theory of blocks with cyclic defect groups renders a very detailed information about characters belonging to the principal p-block, provided that the commutator subgroup G' is large enough. These results generalize Brauer's theory of characters of groups which are divisible by the prime p to the first power only.

Before stating the main proposition, two well-known lemmas will be stated and proved. These lemmas express important properties of groups with a cyclic Sylow p-subgroup, for most of which no reference could be found.

LEMMA 2.1. *Let G be a finite group with a cyclic Sylow p-subgroup $P = \langle \sigma \rangle$. of order p^a. Let P_0 be a non-trivial subgroup of P. Then*:

(a) $[N_G(P_0): C_G(P_0)]$ *divides* $p - 1$;

(b) $C_G(P_0) \cap N_G(P) = C_G(P)$;

(c) $[N_G(P_0): C_G(P_0)] = [N_G(P): C_G(P)]$ *and the sections* $N_G(P_0)/C_G(P_0)$ *and* $N_G(P)/C_G(P)$ *of* G *are incident*;

(d) $N_G(P_0)/C_G(P_0)$ *acts frobeniusly on* P_0.

LEMMA 2.2. *Let G be a finite group with a cyclic Sylow p-subgroup P of order p^a. Then the $p^a - 1$ non-trivial ordinary irreducible characters of P are divided under conjugation by elements of $N_G(P)$ into $(p^a - 1)/q$ transitivity classes of q characters each, where $q = [N_G(P): C_G(P)]$.*

Proof of the Lemmas. Lemma 2.2 follows immediately from (d) and the properties of Frobenius groups.

Since $[N_G(P_0): C_G(P_0)]$ is not divisible by p, the N/C theorem implies (a).

To prove (b), let $\tau \in C_G(P_0) \cap N_G(P) = D$. As $C_G(P) \subset D$, it suffices to show that $\tau \in C_G(P)$. Since τ acts trivially on P_0, it also acts trivially on $\Omega_1(P) = \langle \sigma^{p^{a-1}} \rangle$ and it follows by [6, Theorem 5.2.4] that $\tau = \rho\eta$, where ρ is a p-element of D and η is a p'-element of D which belongs to $C_G(P)$. As ρ is a p-element of $N_G(P)$, ρ belongs to P and consequently $\tau = \rho\eta \in C_G(P)$, as required.

In order to prove (*c*), it suffices to show that

$$N_G(P_0) = N_G(P) \cdot C_G(P_0). \tag{1}$$

Indeed, if (1) holds, then by (b)

$$[N_G(P_0): C_G(P_0)] = [N_G(P): C_G(P)].$$

If $\{\sigma_i \mid i = 1, \cdots, q\}$ are coset representatives of $C_G(P)$ in $N_G(P)$, then by (b) $\sigma_i\sigma_j^{-1} \in C_G(P_0)$ would imply $\sigma_i\sigma_j^{-1} \in C_G(P)$, a contradiction. Hence $\{\sigma_i \mid i = 1, \cdots, q\}$ are also coset representatives of $C_G(P_0)$ in $N_G(P_0)$. It is clear that a coset of $C_G(P_0)$

in $N_G(P_0)$ has a non-empty intersection with a unique coset of $C_G(P)$ in $N_G(P)$ and vice versa.

Now let $\tau \in N_G(P_0)$; in order to prove (1) it suffices to show that $\tau \in N_G(P)C_G(P_0)$, as P_0 is a characteristic subgroup of P. Let $P_0 = \langle \mu \rangle$; then there exists $\eta \in N_G(P)$ such that $\mu^\tau = \mu^\eta$. But then $\tau\eta^{-1} \in C_G(\mu) = C_G(P_0)$, $\tau \in C_G(P_0)N_G(P)$, as required in order to prove (c).

Finally, suppose that $\rho \in P_0^{\#}$, $\eta \in N_G(P_0)$ and $\rho^\eta = \rho$. Then by (c) $\eta = \eta_1\gamma$, where $\eta_1 \in N_G(P)$ and $\gamma \in C_G(P_0)$. Obviously also $\rho^{\eta_1} = \rho$ and consequently, by (b), $\eta_1 \in C_G(\langle \rho \rangle) \cap N_G(P) = C_G(P) \subset C_G(P_0)$. Thus η belongs to $C_G(P_0)$, which proves (d).

We proceed with the main:

Proposition 2.1. *Let G be a finite group with a cyclic Sylow p-subgroup P of order p^a, and assume that $[G:G'] < (p^a - 1)/q$, where $q = [N_G(P):C_G(P)]$. Let B be the principal p-block of G and let P be a defect of B. Then:*

(a) *B contains q modular irreducible characters.*

(b) *B contains $q + (p^a - 1)/q$ ordinary irreducible characters divided into two families: $\{X_\lambda \mid \lambda \in \Lambda\}$ and $\{X_i \mid i = 1, \cdots, q\}$, where Λ is a set of representatives of the classes of non-trivial ordinary characters of P which are conjugate by elements of $N_G(P)$. The $\{X_\lambda\}$ are called "exceptional characters".*

(c) *If $\sigma \in P^{\#}$ and π is a p'-element of $C_G(\sigma)$, then:*

$$X_\lambda(\sigma\pi) = \varepsilon \sum_{\tau \in R} \lambda^\tau(\sigma) \quad \text{for } \lambda \in \Lambda \tag{2}$$

where τ runs over a set R of coset representatives of $C_G(P)$ in $N_G(P)$, and $\varepsilon = \pm 1$. Also:

$$X_j(\sigma\pi) = \varepsilon_j \quad \text{for } j = 1, \cdots, q \tag{3}$$

where $\varepsilon_j = \pm 1$.

(d) *The exceptional characters take the same values on p'-elements of G.*

(e) *The degrees of the ordinary characters of B are given by:*

$$x = X_\lambda(1) = bp^a + \varepsilon q \quad \text{for } \lambda \in \Lambda \tag{4}$$

$$x_j = X_j(1) = b_j p^a + \varepsilon_j \quad \text{for } j = 1, \cdots, q \tag{5}$$

where b and b_j are non-negative integers.

Proof. By [3, Theorem 1, Part 1], (a) and (b) hold for some e, a divisor of q, instead of q. By [3, Theorem 1, Part 2], (d) holds. Since the exceptional characters are of the same degree and since $[G:G'] < (p^a - 1)/e$, the principal character 1_G is non-exceptional, say $1_G = X_1$. Let $\sigma \in P^{\#}$ and let π be a p'-element of $C_G(\sigma)$. Then it follows from [3, Corollary 1.9 and Lemma 1.4] and Lemma 2.1. (c) that:

$$1 = X_1(\sigma\pi) = \frac{\varepsilon_1\gamma_i}{e} \sum_{\tau \in R} \phi_i^\tau(\pi)$$

where $p^i = [P: \langle\sigma\rangle]$, $\gamma_i = \pm 1$ and ϕ_i is a modular irreducible character of $C_G(\sigma)$. As $o(R) = q$ it follows immediately from the above equation with respect to $\pi = 1$ that

$$q = e, \qquad \varepsilon_1\gamma_i = 1, \qquad \phi_i(1) = 1$$

for all i. Consequently, (a) and (b) hold, and γ_i are of the same sign. Hence it may be assumed that $\gamma_i = 1$ for all i. The above equation, together with the fact that $|\phi_i^\tau(\pi)| = 1$, also yields $\phi_i(\pi) = 1$ for all i and for all p'-elements π of $C_G(\sigma)$. These remarks, together with Corollary 1.9 of [3] and Lemma 2.1.(c) yield:

$$X_\lambda(\sigma\pi) = \varepsilon \sum_{\tau \in R} \lambda^\tau(\sigma) \qquad \text{for } \lambda \in \Lambda$$

$$X_j(\sigma\pi) = \varepsilon_j \qquad \text{for } j = 1, \cdots, e$$

where ε, $\varepsilon_j = \pm 1$ and R is a set of coset representatives of $C_G(P)$ in $N_G(P)$, which is also a set of coset representatives of $C_G(\langle\sigma\rangle)$ in $N_G(\langle\sigma\rangle)$.

It remains only to prove (e). By (3)

$$(b_j + \varepsilon_j)p^a = \sum_{\sigma \in P^\#} X_j(\sigma) + x_j = (p^a - 1)\varepsilon_j + x_j$$

for all j and some non-negative integers b_j and (5) follows. Also by (2)

$$bp^a = \sum_{\sigma \in P^\#} X_\lambda(\sigma) + x = \varepsilon(-q) + x$$

for some non-negative integer b implying formula (4). The proof of the Proposition is complete.

As an immediate corollary from Proposition 2.1 we get the following

COROLLARY 2.1. *Under the assumptions of Proposition* 2.1 *and denoting* x *by* x_0, $-\varepsilon$ *by* ε_0 *and* $(p^a - 1)/q$ *by* t *we have:*

$$x_i \equiv \varepsilon_i \ (\mathrm{mod}\ p^a) \qquad \text{for } i = 1, \cdots, q$$

$$tx_0 \equiv \varepsilon_0 \ (\mathrm{mod}\ p^a)$$

(6) $$\sum_{j=0}^{q} \varepsilon_i x_i = 0.$$

Proof. The congruences follow immediately from part (e) of Proposition 2.1. To prove (6), let $\sum_X$ denote summation over all characters of the block B, and let $\sigma \in P^\#$. It is well-known that

$$\sum_X X(\sigma)X(1) = 0.$$

On the other hand, Proposition 2.1 implies that:

$$\sum_X X(\sigma)X(1) = x_0 \sum_\Lambda X_\lambda(\sigma) + \sum_{i=1}^{q} \varepsilon_i x_i$$

where $\sum_\Lambda$ denotes summation over all $\lambda \in \Lambda$. Since by (2)

$$\sum_\Lambda X_\lambda(\sigma) = -\varepsilon_0 \sum_{\tau \in R} \left(\sum_\Lambda \lambda^\tau(\sigma) \right) = -\varepsilon_0(-1) = \varepsilon_0$$

it follows from the above equations that $\sum_{i=0}^{q} \varepsilon_i x_i = 0$.

3. Proof of Theorem 2 and the Corollary. We begin with the proof of Theorem 2. If $a = 1$, then (I) holds by Theorem 1 in [2]. It is easy to check that the groups mentioned in (I) and (II) satisfy the assumptions of the theorem. Therefore from now on it will be assumed that $a \geqq 2$. The theorem will be proved once we show that $a = 2$ and $G \cong PSL(2,8)$.

We will need the following well-known number theoretical result:

LEMMA 3.1.(a) *Let p be a prime and suppose that*

$$p^a - 1 = 2^b.$$

Then either $a = 1$ or $a = 2$, $p = 3$ and $b = 3$.

(b) *The equation*

$$3^x - 2^y = \varepsilon, \qquad \varepsilon = \pm 1$$

has only the following solution in natural integers: (1) $\varepsilon = 1$, $x = 1$, $y = 1$; (2) $\varepsilon = 1$, $x = 2$, $y = 3$; (3) $\varepsilon = -1$, $x = 1$ $y = 2$.

Proof. (a) First assume that a is odd. Since $p - 1 = 2^c$ for some c, we have

$$2^b = p^a - 1 = (2^c + 1)^a - 1 = 2^c(2k + a)$$

for some non-negative integer k. Therefore $2k + a = 1$, $a = 1$.

Assume now that $a = 2d$, d a positive integer. Then

$$2^b = p^{2d} - 1 = (p^d - 1)(p^d + 1)$$

and 2 divides $(p^d + 1)/(p^d - 1)$. Consequently

$$p^d + 1 \geqq 2(p^d - 1)$$

which implies $p^d = 3$, $p = 3$, $a = 2d = 2$ and $b = 3$.

(b) If $x = 1$, then clearly either $y = 1$, $\varepsilon = 1$ or $y = 2$, $\varepsilon = -1$. If $x \geqq 2$ and $\varepsilon = 1$, then by part (a) $x = 2$ and $y = 3$. Thus it remains to show that the equation

$$3^x = 2^y - 1$$

has no solution in natural integer for $x > 1$. Indeed, suppose that y is even. Then

$$3^x = (2^{y/2} - 1)(2^{y/2} + 1)$$

which implies: $2^{y/2} - 1 = 1$, $y = 2$ and $x = 1$, in contradiction to the assumption $x > 1$. If y is odd, then:

$$3^x = 2^y - 1 = (3-1)^y - 1 \equiv -2 \pmod 3)$$

a contradiction. The proof of Lemma 3.1 is complete.

We will proceed now with the proof of Theorem 2. Let B be the principal p-block of G. The characters of B are described in Proposition 2.1 and Corollary 2.1, and we will adopt the notation introduced there. It follows from (6) that at least one $x_i \neq 1$ is not divisible by r; denote that x_i by y. As $q = [N_G(P): C_G(P)]$ divides $p-1$, it follows from (4) and (5) that y is not divisible by p either. Thus y divides s and

$$y < p^a - 1.$$

Equations (4) and (5) then again imply that $y = x$ is a degree of an exceptional character of B and that

$$\text{either } x = q \text{ or } x = p^a - q.$$

Each case will be considered separately.

Case I. Assume that $x = q$. Since G has at least two conjugate classes of elements of order p, it follows that $q < p - 1$. But then the result of [4] applies, forcing the existence of a normal subgroup of G of order at least p^{a-1}, in contradiction to the simplicity of G.

Case II. Assume that $x = p^a - q$. Since x divides s, $a > 1$ and $q < p - 1$, it follows that

$$s = p^a - q. \tag{7}$$

This implies that $(q, s) = 1$ and $q = r^c$ for some non-negative integer c. As G is simple, $N_G(P) \neq C_G(P)$ and hence $q \neq 1$, $c > 0$. As $x = x_0 = p^a - q$ and $\varepsilon_0 = 1$, it follows that

$$1 + \varepsilon_0 x_0 = 2 + (p^a - 1) - r^c = 2 + r^c(t-1) \tag{8}$$

where $t = (p^a - 1)/q > 1$. Suppose that $r \neq 2$. Then (6) and (8) imply that at least one $x_i \neq 1, x$ is not divisible by r, hence divides $s = p^a - q$, in contradiction to (5). Therefore $r = 2$ and $q = 2^c$. Now suppose that $c \geqq 2$. Then again by (6) and (8) there exists $x_i \neq 1, x$, say x_j, which is not divisible by 4. It follows from (5) that x_j divides $2s < 2(p^a - 1)$ and consequently $x_j = p^a + \varepsilon_j$. But then $(p^a + \varepsilon_j)/2$ divides s, in contradiction to (7). Thus we have shown that

$$r = q = 2.$$

Let $x_2 = up^a + \varepsilon_2$ be the degree of the unique non-principal non-exceptional character of B. Then it follows from (6) that

$$1 + \varepsilon_0 x_0 + \varepsilon_2 x_2 = p^a - 1 + (up^a + \varepsilon_2)\varepsilon_2 = 0$$

Thus $u\varepsilon_2 = -1$, hence $u = 1$, $\varepsilon_2 = -1$ and $x_2 = p^a - 1$. Consequently $p^a - 1$ divides $o(G)$, and since $(p^a - 1, p^a) = (p^a - 1, p^a - 2) = 1$, it follows that

$$p^a - 1 = 2^d, \qquad a \geqq 2$$

where d is a non-negative integer. Lemma 3.1 then yields:

$$p = 3, \quad a = 2 \text{ and } d = 3$$

and

$$o(G) = 9 \cdot 2^b \cdot 7.$$

Let Q be a Sylow 7-subgroup of G and let $e = [N_G(Q): C_G(Q)]$. Denote the principal 7-block by B_1. Then by (6) B_1 contains a non-principal ordinary character of odd order z. Consequently z divides 9 and therefore z is a degree of an exceptional character of B_1. By Lemma 2 of [2] $z \neq 3$ and consequently $z = 9 = 7+2$, $e = 2$ and the ε which multiplies z in (6) is -1. Since $e = 2$, B_1 contains only one non-principal non-exceptional character W of degree $w = 7u + \rho$, where $\rho = \pm 1$ and u is a positive integer. Now it follows from (6) that:

$$1 + 9(-1) + (7u + \rho)\rho = 0$$

yielding $u\rho = 1$, $u = \rho = 1$ and $w = 8$. By Lemma 1 of [2], the existence in B_1 of the character W of degree $8 < 14$ implies that G contains no elements of order 14. Lemma 3 of [2] then yields:

$$\sum Z(1)Z(\tau) \equiv 0 \pmod{2^b} \tag{9}$$

where $\tau \in Q^{\#}$ and the summation ranges over characters Z which belong simultaneously to B_1 and B_2, where B_2 is the 2-block of G containing W. By Lemma 2 of [2] B_2 is a block of defect $b-1$ at most and consequently it contains characters of even orders only. Thus it follows from (9) and from the fact that W is the only character of B_1 of even order that

$$8 \cdot 1 \equiv 0 \pmod{2^b}.$$

As 8 divides $o(G)$, this congruence yields:

$$2^b = 8, \qquad o(G) = 7 \cdot 8 \cdot 9 = 504.$$

Let R be a Sylow 2-subgroup of G. It is well-known that R cannot be be quaternion. If R is dihedral, then Suzuki [7] ghas shown that $G \cong PSL(2,u)$ for some prime u, which is not the case. Finally, if R is Abelian, then it follows from Gagen's result [5] that G contains a subgroup which is isomorphic either to $PSL(2,2^n)$, $n > 1$ or to $PSL(2,u)$ for some prime $u \equiv \pm 3 \pmod 8$, $u > 3$. Since $o(G) = 504$, it follows that

$$G \cong PSL(2,8)$$

and the proof of Theorem 2 is complete.

We will proceed with the proof of the Corollary. It is easy to check that the groups mentioned in the conclusion of Theorem 2 all satisfy assumptions (a)–(e). Thus it suffices to show that in each of the cases (a)–(e), G is either of Type (I) or of Type (II) mentioned in Theorem 2.

In the proof of Theorem 2, the assumption about the existence of at least two conjugate classes of elements of order p was applied only for the elimination of the possibility that:

$$a \geqq 2, \; x = q = p - 1 \text{ and } q \text{ divides } s. \tag{10}$$

In cases (a) for $p \neq 3$, (b), and (c) this cannot happen. In case (d) the simplicity of G implies that s is an odd integer, again eliminating (10). Finally suppose that $x = x_0 = q = p - 1$ and r does not divide $p - 2$. Then $\varepsilon_0 = -1$ and

$$1 + \varepsilon_0 x_0 = 1 - (p-1) = -(p-2) \tag{11}$$

and it follows from (6) that at least one $x_i \neq 1, x$, say x_j, is prime to r. But then x_j divides $s < p^a - 1$, in contradiction to (5). Thus also in cases (e) and (a) with $p = 3$, (10) cannot happen and the proof of the corollary is complete.

4. Proof of Theorems 1 and 3. First we will prove Theorem 3. It follows immediately from the formula

$$o(PSL(2,p^m)) = \gamma_p(p^m - 1)p^m(p^m + 1)$$

where $\gamma_p = 1$ if $p = 2$ and $\gamma_p = \frac{1}{2}$ if $p \neq 2$, that 6 divides $o(PSL(2,p^m))$ for all p^m. Thus, in view of our assumptions

$$o(G) = p^a \cdot 2^b \cdot 3^c, \qquad b \geqq 2.$$

Case (A). Assume that $q = 2^m$, $m \geqq 2$. Then $m = b$ and

$$o(G) = (2^m - 1)2^m(2^m + 1) = p^a \cdot 2^m \cdot 3^c.$$

As $(2^m - 1, 2^m + 1) = 1$, it follows that

$$3^c = 2^m + \varepsilon, \qquad \varepsilon = \pm 1, \qquad m \geqq 2.$$

In view of Lemma 3.1.(b), only the cases $m = 2$ and $m = 3$ could occur. Since $PSL(2,4)$ and $PSL(2,8)$ satisfy the assumptions of Theorem 3, the proof of Case (A) is complete.

Case (B). Assume that $q = r^m > 3$ and r is an-odd prime. Then

$$o(G) = (r^m - 1)r^m(r^m + 1)/2 = p^a \cdot 2^b \cdot 3^c.$$

Suppose that neither $r^m - 1$ nor $r^m + 1$ is a power of 2. Then each such expression is divisible by an odd prime, and since $(r^m - 1, r^m + 1) = 2$, these primes are distinct and obviously not equal to r. But then $o(G)$ is divisible by at least four primes, in contradiction to our assumptions. Thus

$$2^x = r^m + \varepsilon, \qquad \varepsilon = \pm 1, \qquad r^m > 3.$$

Consequently $r^m - \varepsilon \equiv 2 \pmod 4$ and $x = b \geqq 2$.

Suppose first that $r = 3$. Then by Lemma 3.1.(b) only the case $m = 2$, $G \cong PSL(2,9)$ could occur. This group satisfies the assumptions of Theorem 3.

Suppose next that $r > 3$. Then $r = p$, $m = a$ and

$$(p^a - \varepsilon)/2 = 3^c.$$

Since $p^a + \varepsilon = 2^b$, it follows that

$$2^{b-1} - 3^c = \varepsilon, \qquad b - 1 \geqq 1.$$

Lemma 3.1.(b) now implies that only one of the following cases could occur:

$$c = 1, \qquad b = 2, \qquad \varepsilon = -1 \quad \text{and} \quad G = PSL(2,5)$$

$$c = 1, \qquad b = 3, \qquad \varepsilon = 1 \quad \text{and} \quad G = PSL(2,7)$$

$$c = 2, \qquad b = 4, \qquad \varepsilon = -1 \quad \text{and} \quad G = PSL(2,17).$$

Each of the above groups satisfies the assumptions of Theorem 3. The proof is complete in all cases.

We proceed with the proof of Theorem 1. Since G is a non-cyclic simple group, $u \neq p \neq w$ and without loss of generality we may assume that

$$p^a > u^b > w^c.$$

Let p_1 and p_2 be distinct odd primes among p, u and w. Let $p_i^{a_i}$, $i = 1,2$ be the highest powers of p_i dividing $o(G)$. We may assume without loss of generality that

$$p_1^{a_1} < p_2^{a_2}.$$

Since p_i, $i = 1,2$ are odd primes

$$p_1^{a_1} < p_2^{a_2} - 1$$

and it follows from the Corollary, part (c), that G has to be isomorphic to some $PSL(2,q)$, $q > 3$. Consequently, by Theorem 3, G is isomorphic to one of the following groups: $PSL(2,5)$, $PSL(2,7)$, $PSL(2,8)$ and $PSL(2,17)$. The proof of Theorem 1 is complete.

References

1. R. Brauer, *Investigations on group characters*, Ann. of Math. **42** (1941), 936–958.

2. R. Brauer, and H. F. Tuan, *On simple groups of finite order*, I, Bull. Amer. Math. Soc. **51** (1945), 756–766.

3. E. C. Dade, *Blocks with cyclic defect groups*, Ann. of Math. **84** (1966), 20–48.

4. W. Feit, *Groups which have a faithful representation of degree less than* $p-1$, Trans. Amer. Math. Soc. **112** (1964), 287–303.

5. T. M. Gagen, *On groups with abelian Sylow 2-groups*, Math. Z. **90** (1965), 268–272.

6. D. Gorenstein, *Finite Groups*, Harper and Row, 1968.

7. M. Suzuki, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math. **77** (1955), 657–691.

8. J. G. Thompson, *Vertices and sources*, J. of Algebra **6** (1967), 1–6.

9. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Volume I, 1937.

University of California,
Santa Barbara