PACIFIC JOURNAL OF MATHEMATICS
Vol. 104, No. 2, 1983

SIMPLE GROUPS AND A DIOPHANTINE EQUATION

LEO J. ALEX

Let G be a finite simple group whose order is of the form pm where p is a prime, $(p, m) = 1$, and the index of a Sylow p-subgroup in its normalizer is three in G. Suppose the degree equation for the principal p-block, $B_0(p)$, has the form $1 + 2^a = 3^b5^c + 2^d3^e5^f$ where a, b, c, d, e and f are non-negative integers. In this paper it is shown that under these conditions G must be isomorphic to one of the groups $L(2,7)$, $U(3,3)$, $L(3,4)$ and A_8. This is accomplished by solving the exponential Diophantine degree equation for $B_0(p)$.

1. Introduction. 1.1. In this paper finite simple groups, G, with a Sylow p-subgroup whose normalizer has order $3p$ such that the degree equation for the principal p-block, $B_0(p)$, has the form $1 + 2^a = 3^b5^c + 2^d3^e5^f$ are studied.

In §2 several preliminary results dealing primarily with the values of the characters in $B_0(p)$ are obtained. In particular, inequalities relating the degrees of these characters are derived, so that the task of solving the degree equation for $B_0(p)$ is simplified.

In §3 the degree equation, $1 + 2^a = 3^b5^c + 2^d3^e5^f$, for $B_0(p)$ is solved. This is accomplished, with computer assistance, by considering the equation modulo a sequence of prime power moduli and applying the group theoretic results from §2. The inequalities relating the characer degrees are especially useful here in bounding the size of these degrees.

In §4 the possible degree equations left after the analysis in §3 are studied, and it is shown that the only finite simple groups with a Sylow p-normalizer of order $3p$ and degree equation for $B_0(p)$ of the form $1 + 2^a = 3^b5^c + 2^d3^e5^f$ are the groups $L(2,7)$, $U(3,3)$, $L(3,4)$ and A_8.

1.2. NOTATION. In general upper-case letters denote groups, and Sp is used to denote a Sylow p-subgroup. If A is a subgroup of G, then $N(A)$, $C(A)$, $|G:A|$, $|A|$, $Z(A)$ denote the normalizer of A in G, the centralizer of A in G, the index of A in G, the order of A, and the center of A in G, respectively. Upper-case Greek letters are used to denote ordinary characters of G.

2. Preliminary results. Let G be a finite simple group satisfying the hypothesis

(2.1) $\quad |N(\mathrm{Sp})| = 3p$, for a Sylow p-subgroup Sp.

Brauer's work [3] yields the following information concerning $B_0(p)$, the principal p-block of G.

The characters in $B_0(p)$ are the principal character 1, two other nonexceptional characters Λ, Γ, and $(p-1)/3$ exceptional characters $\chi^{(m)}$, $m = 1, 2, \cdots, (p-1)/3$. There are signs δ_1, δ_2, $\delta' = \pm 1$ such that $\Lambda(1) \equiv \delta_1 \pmod{p}$, $\Gamma(1) \equiv \delta_2 \pmod{p}$, $\chi^{(m)}(1) \equiv -3\delta' \pmod{p}$, $m = 1, 2, \cdots, (p-1)/3$ and

$$1 + \delta_1\Lambda(1) + \delta_2\Gamma(1) + \delta'\chi^{(m)}(1) = 0. \tag{2.2}$$

In the sequel we make the additional hypothesis that the degree equation (2.2) for $B_0(p)$ has the form

$$1 + 2^a = 3^b5^c + 2^d3^e5^f, \tag{2.3}$$

where a, b, c, d, e, f are non-negative integers.

We next list several results which are effective in obtaining information about the structure of G from the degree equation for $B_0(p)$. The first two lemmas appear in the work of Brauer and Tuan [4].

LEMMA 2.1. *Let G be a simple group of order pq^br, where p and q are primes, $(pq, r) = 1$. Suppose G has no elements of order pq. Then for any q-block, $B(q)$, $\Sigma \delta_i\chi_i(1) \equiv o \pmod{q^b}$, where the summation is taken over all characters in $B_0(p) \cap B(q)$.*

It has become traditional to refer to Lemma 2.1 as the principle of "block separation".

LEMMA 2.2. *If G is a simple group, χ is an irreducible character of G of degree q^s, q a prime, $s > 0$, then χ cannot be in $B_0(q)$.*

The following lemma is extremely productive in eliminating possible degree equations. It is due to Keller [5]. A proof appears in [1].

LEMMA 2.3. *Let G be a simple group satisfying hypothesis* (2.1) *with degrees equation $1 + x = y + z$ for $B_0(p)$ then xyz is a positive integral square.*

The next two lemmas give inequalities between the degrees of the characters in $B_0(p)$. The proof of the first lemma appears in [1].

LEMMA 2.4. *Let G be a simple group satisfying hypothesis* (2.1) *with degree equation $1 + x = y + z$ in $B_0(p)$.*

(1) *If $z \equiv 3 \pmod{p}$, then*

(a) *$x < z^2$ when $p = 7$ and*

(b) *$x < \frac{1}{2}(z^2 - 2z)$ when $p > 7$.*

(2) *If* $z \equiv -1 \pmod{p}$, *then*
(a) $x \leq \frac{1}{2}(z^3 - 3z)$ *when* $x \equiv 1 \pmod{p}$ *and*
(b) $x \leq [3/(2p-2)](z^3 - 3z)$ *when* $x \equiv -3 \pmod{p}$.

LEMMA 2.5. *Let G be a simple group satisfying hypothesis* (2.1) *where the degree equation for $B_0(p)$ has the form* $1 + 2^a = r^b + 2^c r^d$, *where* $r = 3$ *or* 5, *then*
(1) $a > c, b \geq d$,
(2) *when* $r = 3$, $a \leq 40$, *and*
(3) *when* $r = 5$, $a \leq 41$.

Proof. Let χ, θ be characters of degree 2^a and r^b, respectively. Then by Lemma 2.2, χ is not in $B_0(2)$, and θ is not in $B_0(r)$. Then $a \geq c$, $b \geq d$ from Lemma 2.1 applied respectively to $B_0(p) \cap B_0(2)$ and $B_0(p) \cap B_0(r)$. Also if $a = c$ then $b = 0$ which is not possible since G is simple. This proves (1).

When $r = 3$, consideration of the degree equation modulo 2^c and 3^d yields $3^b \equiv 1 \pmod{2^c}$ and $2^a \equiv 1 \pmod{3^d}$, whence 2^{c-2} divides b and 3^{d-1} divides a. Now Lemma 2.4 implies that $2^a \leq 2^{3c}3^{3d}$. Thus $a \leq 3c + 3d(\log 3)/(\log 2)$. Clearly $b \leq a$. Thus we may conclude that

$$2^{c-2} + 3^{d-1} \leq 2a \leq 6c + 6d(\log 3)/(\log 2). \tag{2.4}$$

A short calculation involving inequalities (2.4) yields $d \leq 4$ and $c \leq 8$. Also when $d = 4$ it must be the case that $c \leq 7$, and when $c = 8$ necessarily $d \leq 3$. Then further consideration of inequalities (2.4) yields $a \leq 40$. This proves (2).

Similarly when $r = 5$, consideration of the degree equation modulo 2^c and 5^d yields $5^b \equiv 1 \pmod{2^c}$ and $2^a \equiv -1 \pmod{5^d}$, whence 2^{c-2} divides b and 5^{d-1} divides a. In this case consideration of Lemma 2.4 yields

$$2^{c-2} + 5^{d-1} \leq 2a \leq 6c + 6d(\log 5)/(\log 2). \tag{2.5}$$

Then consideration of (2.5) yields $d \leq 3$ and $c \leq 8$. Also when $d = 3$, then $c \leq 7$; and when $c = 8$, then $d \leq 2$. Thus $a \leq 41$. This completes the proof of Lemma 2.5.

3. Solution of the degree equation. Next we apply the results of §2 to solve the degree equation (2.3) for the principal p-block of G.

The first step in the solution process is to test the equation modulo a sequence of primes and prime powers in order to determine information regarding the exponents a, b, c, d, e, and f. The equation is tested by computer modulo 7, 13, 19, 37 and 73 in that order. The computer used for this purpose was the CDC 6600 at the University of Minnesota Computer Center. These tests yield sets of congruences on the exponents a, b, d, and e modulo 36 and on the exponents c and f the congruences are

modulo 72. This is due to the fact that the exponents of 2, 3, and 5 modulo $7 \cdot 13 \cdot 19 \cdot 37 \cdot 73$ are 36, 36, and 72 respectively. Next the equation is tested modulo 5, 3, 9, 27, 4, 8, and 16. Then the sets of congruences are checked to see that Lemma 2.3 is satisfied and that none of the terms 2^a, 3^b5^c, or $2^d3^e5^f$ is necessarily equal to 1. At this point there are the following 19 sets of congruences on the exponents to consider:

	$a \pmod{36}$	$b \pmod{36}$	$c \pmod{72}$	$d \pmod{36}$	$e \pmod{36}$	$f \pmod{72}$
(1)	9	0	0	9	0	0
(2)	27	0	0	27	0	0
(3)	2	0	0	2	0	0
(4)	6	0	0	6	0	0
(5)	10	0	0	10	0	0
(6)	14	0	0	14	0	0
(7)	18	0	0	18	0	0
(8)	22	0	0	22	0	0
(9)	26	0	0	26	0	0
(10)	30	0	0	30	0	0
(11)	34	0	0	34	0	0
(12)	3	1	0	1	1	0
(13)	9	3	0	1	5	0
(14)	10	0	4	4	0	2
(15)	5	0	2	3	0	0
(16)	5	3	0	1	1	0
(17)	6	2	1	2	0	1
(18)	7	1	2	1	3	0
(19)	9	2	2	5	2	0

Now we test these 19 remaining cases by hand to determine the possible solutions to equation (2.3). In this regard, Lemma 2.5 is especially productive.

First of all in cases (1) and (2), consideration of equation (2.3) modulo 5 yields that $c = 0$ and $f = 0$. Then Lemma 2.5, (2) *gives* $a \leq 40$, *whence* $a = 9$ in case (1), and $a = 27$ in case (2). But then the equations are $1 + 2^9 = 1 + 2^9$ and $1 + 2^{27} = 1 + 2^{27}$, respectively. These are not possible degree equations for a simple group. This contradiction eliminates cases (1) and (2). Similarly in cases (3)–(11), consideration of equation (2.3) modulo 3 yields that $b = e = 0$. Then Lemma 2.5, (3) gives $a \leq 41$ whence $a = 6, 10, 14, 18, 22, 26, 30, 34$ in cases (4)–(11) respectively; and in case (3), $a = 2$ or 38. In each of these cases it is then easy to see that the equation must have the form $1 + 2^a = 1 + 2^a$, a contradiction to the simplicity of G.

Next in cases (12), (13) and (16), consideration of equation (2.3) modulo 5 gives $c = f = 0$. Then Lemma 2.5, (2) yields $a \leq 40$. Thus cases

(12), (13) and (16) give the possible degree equations $1 + 8 = 3 + 6$, $1 + 512 = 27 + 486$, and $1 + 31 = 27 + 6$, respectively for $B_0(p)$. Similarly in cases (14) and (15), consideration of equation (2.3) modulo 3 and Lemma 2.5, (3) give the possible degree equations $1 + 1024 = 625 + 400$ and $1 + 32 = 25 + 8$, respectively.

In case (17), consideration of equation (2.3) modulo 3 yields that $e = 0$. Then consideration modulo 27 gives $b = 2$. Next consideration modulo 8 yields $b = 2$. Finally consideration modulo 31 and 25 gives $f = 1$, whence $a = 6$. Thus the possible degree equation $1 + 64 = 45 + 20$ is determined.

In case (18), considerations modulo 5, 9 and 4 yield $f = 0$, $b = 1$, and $d = 1$, respectively. Then consideration modulo 109 gives $c \equiv 2 \pmod{54}$ and $e \equiv 3 \pmod{54}$. Then if $e > 3$, consideration modulo 81 yields $a \equiv 43 \pmod{54}$. But then consideration modulo 163 gives a contradiction. Thus $e = 3$. Next considerations modulo 25, 11 and 101 yield $a \equiv 7 \pmod{20}$, $c \equiv 2 \pmod{20}$, and $a \equiv 7 \pmod{100}$, respectively. Then consideration modulo 125 yields $c = 2$, whence $a = 7$. Hence the possible degree equation $1 + 128 = 75 + 54$ has been determined.

In the final case (19), consideration modulo 5 yields $f = 0$. Then consideration modulo 32, 17, and 64 gives $d = 5$. Next consideration modulo 27, 81, 243, 109, and 163 yield that $b = 2$ and $e = 2$. Then consideration modulo 128, 97, 257 and 1024 give $a = 9$. Thus $c = 2$, and the possible degree equation $1 + 512 = 225 + 288$ is obtained.

Next we summarize our work in the form of a lemma.

LEMMA 3.1. *Let G be a simple group satisfying hypothesis* (2.1) *with degree equation* (2.3) *for $B_0(p)$. Then the degree equation is one of the following*: $1 + 8 = 3 + 6$, $1 + 512 = 27 + 486$, $1 + 32 = 27 + 6$, $1 + 1024 = 625 + 400$, $1 + 32 = 25 + 8$, $1 + 64 = 45 + 20$, $1 + 128 = 75 + 54$, *and* $1 + 512 = 225 + 288$.

4. Proof of the main theorem. Now let G be a simple group satisfying hypothesis (2.1) with degree equation (2.3) for $B_0(p)$. We will next consider the possible choices for the degree equation given by Lemma 3.1 and determine the groups involved.

In the case of the equation $1 + 8 = 6 + 3$, the Brauer relatins listed above equation (2.2) imply that $p = 7$. Then the work [**2**] of Blichfeldt yields that G is isomorphic to $L(2, 7)$. It is an easy matter to verify that $L(2, 7)$ satisfies hypothesis (2.1) with degree equation $1 + 8 = 6 + 3$ for $B_0(7)$.

For the equation $1 + 512 = 27 + 486$, the Brauer relations also give $p = 7$. But in this case the block separation Lemma 2.1 applied to $B_0(3) \cap B_0(7)$ gives a contradiction. Thus there is no group corresponding to this equation.

In the case of the equation $1 + 32 = 27 + 6$, the Brauer relations give $p = 7$. Then the work [6] of Lindsey yields that G is isomorphic to $U(3, 3)$. It is an easy matter to verify that $U(3, 3)$ satisfies hypothesis (2.1) with degree equatin $1 + 32 = 27 + 6$ for $B_0(7)$.

For the equations $1 + 1024 = 625 + 400$, $1 + 32 = 25 + 8$, $1 + 128 = 75 + 54$, and $1 + 512 = 225 + 288$, there is no choice for the prime p which is consistent with the Brauer relations.

Finally in the case of the equation $1 + 64 = 20 + 45$, the Brauer relations yield $p = 7$. Then the work [1] of Alex and Morrow shows that G is isomorphic to $L(3, 4)$ or A_8. It is an easy matter to verify that each of these groups satisfies hypothesis (2.1) with degree equation $1 + 64 = 20 + 45$ for $B_0(7)$.

We are now in a position to state the main result of this paper.

THEOREM 4.1. *Let G be a finite simple group such that $|N(\mathrm{Sp})| = 3p$, for a Sylow p-subgroup* Sp. *Suppose the degree equation for $B_0(p)$ has the form $1 + 2^a = 3^b5^c + 2^d3^e5^f$, where a, b, c, d, e, and f are non-negative integers. Then G is isomorphic to one of the groups $L(2, 7)$, $U(3, 3)$, $L(3, 4)$, or A_8.*

REFERENCES

1. Leo J. Alex and Dean C. Morrow, *Simple groups with a Sylow normalizer of order $3p$*, J. Algebra, **61**, No. 2 (1979), 311–327.
2. H. L. Blichfeldt, *Finite Collineation Groups*, University of Chicago Press, Chicago, 1917.
3. Richard Brauer, *On groups whose order contains a prime number to the first power*. I, II, Amer. J. Math., **64** (1942), 401–440.
4. Richard Brauer and H. F. Tuan, *On simple groups of finite order*, Bull. Amer. Math. Soc., **51** (1945), 756–766.
5. Gordon E. Keller, Private communication.
6. J. H. Lindsey II, *On a projective representation of the Hall-Janko group*, Bull. Amer. Math. Soc., **74** (1968), 1094.

Received September 9, 1980.

STATE UNIVERSITY COLLEGE
ONEONTA, NY 13820