PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 1, January 1995

ARITHMETICAL CONDITIONS ON ELEMENT ORDERS AND GROUP STRUCTURE

JIPING ZHANG

(Communicated by Ronald M. Solomon)

ABSTRACT. General results are provided on bounding the number of different prime factors of the order of finite groups in terms of the number for the order of elements.

This paper is concerned mainly with the following general question:

What can be said about the structure of a finite group G if some information is known about the arithmetical structure of the orders of elements of G?

1

To formulate our results, we first introduce some natural notation.

Let n be a positive integer and

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad (a_i \geq 1, p_i \neq p_j \text{ for } i \neq j)$$

the prime-factor-decomposition of n. We now put

$$\alpha(n) = k, \qquad \omega(n) = \max\{a_i : i = 1, 2, \ldots, k\}.$$

We also define

$$\alpha(1) = \omega(1) = 0.$$

If G is a finite group, we write

$$\rho(G) = \alpha(|G|),$$
$$\alpha(G) = \max\{\alpha(o(x)) : x \in G\},$$
$$\omega(G) = \max\{\omega(o(x)) : x \in G\}.$$

We know from Higman [8] that if G is a finite solvable group with $\alpha(G) = 1$, then $\rho(G) \leq 2$. M. Suzuki [13] and R. Brandl [1] determined the finite nonsolvable groups with $\alpha(G) = 1$. In this paper we will give some upper bounds on $\rho(G)$ in terms of $\alpha(G)$ and pose some unsolved problems.

Received by the editors November 1, 1992 and, in revised form, April 15, 1993.
1991 *Mathematics Subject Classification.* Primary 20D60.
Supported in part by the Commission of the European Communities and NSF of China.

0002-9939/94 $1.00 + $.25 per page

2

We now state our main results.

Theorem 1. *If G is a finite solvable group, then*

$$\rho(G) \leq \alpha(G)(\alpha(G)+3)/2.$$

Remark. Comparing this result with the famous conjecture of Huppert on character degrees, the reader may ask whether or not $\rho(G)$ is bounded by $2\alpha(G)$. This is not true, since we have an example G (see the example at the end of this paper) for which the bound is realized. However, it is plausible that a linear bound may also work.

Theorem 2. *Let G be an arbitrary finite group; then*

$$\rho(G) \leq 16\alpha(G)^3(\alpha(G)+3)\exp(\alpha(G)).$$

Remark. Theorem 2 offers an affirmative answer to a problem posed in [12].

Theorem 1 together with Hall-Higman's results on p-length [7] yields the following

Corollary 3. *If G is a finite solvable group, then the nilpotent length $F_l(G) \leq 4(n+1)^{m(m+3)/2} - 1$, where $n = \omega(G)$ and $m = \alpha(G)$.*

We note here that $F_l(G)$ cannot be bounded by any function of $\alpha(G)$ since for any n there is a finite group G of order $2^a 3^b$ with $F_l(G) \geq n$.

Now we are going to prove Theorem 1.

3

Proof of Theorem 1. Let $f(n)$ be a function defined over the set of all positive integers such that $f(n) = n(n+3)/2$. It is easy to see that $\alpha(G) \geq \alpha(G/N)$ and $\alpha(G) \geq \alpha(M)$ for any subgroup M and any normal subgroup N of G. If the theorem is not true, let G be a counterexample of minimal possible order. So $\alpha(G)$ is at least 2 by [8].

We claim that any chief-factor of G is isomorphic to a Sylow subgroup of G. Suppose that $1 = N_0 \leq N_1 \leq \cdots \leq N_m = G$ is a chain of normal subgroups of G such that N_i/N_{i-1} is a minimal normal subgroup of G/N_{i-1} for $i = 1, 2, \ldots, m$. Then N_i/N_{i-1} is a p_i-subgroup for some prime p_i. We need only to prove that $p_i \neq p_j$ for any $i \neq j$. If this is not the case, let i be the largest integer such that $p_i = p_j$ for some $j < i$. If $i = m$, then p_m is a prime divisor of the order of N_{m-1} and therefore $\rho(G) = \rho(N_{m-1})$. The minimality of G implies that $\rho(N_{m-1}) \leq f(\alpha(N_{m-1}))$. Since $\alpha(N_{m-1}) \leq \alpha(G)$, $\rho(G) = \rho(N_{m-1}) \leq f(\alpha(N_{m-1})) \leq f(\alpha(G))$, which is a contradiction. Therefore, i is less than m. Let H be a Hall π_1-subgroup of G, where π_1 is the set of p_k's with $k > i$. Then we have $G = HN_i$ with $(|H|, |N_i|) = 1$. By the choice of i, p_i is a divisor of the order of N_{i-1} and thus $\rho(G) = \rho(HN_{i-1})$. Now a contradiction as in the case $i = m$ can be obtained. Hence $p_i \neq p_j$ for $i \neq j$, as claimed.

Let P_i be a Sylow p_i-subgroup of G for each i such that $\{P_1, P_2, \ldots, P_m\}$ is a Sylow system of G. Thus $P_iP_j = P_jP_i$ for any i, j. Clearly P_m is of order p_m. Let π be the set of those primes p_j such that p_j does not divide the order of $C_G(P_m)$, and let K be a P_m-invariant Hall π-subgroup of G. Then $C_K(P_m) = 1$. Now by the well-known theorem of J. G. Thompson, K is

nilpotent and thus $\rho(K) = \alpha(K) \leq \alpha(G)$. The minimality of G implies that $\rho(C_G(P_m)/P_m) \leq f(\alpha(C_G(P_m)/P_m))$. Since $\alpha(C_G(P_m)/P_m) \leq \alpha(C_G(P_m)) - 1 \leq \alpha(G) - 1$, it follows that $\rho(G) = \rho(K) + 1 + \rho(C_G(P_m)/P_m) \leq 1 + \alpha(G) + f(\alpha(G)-1) = 1+\alpha(G)+(\alpha(G)-1)(\alpha(G)+2)/2 = \alpha(G)(\alpha(G)+3)/2 = f(\alpha(G))$, which is contradictory to the assumption on G. The contradiction proves the theorem.

4

In order to prove Theorem 2 we need to prove several lemmas.

Lemma 4. *Let A_n $(n \geq 5)$ be the alternating group of degree n; then $\rho(A_n) \leq 12\exp(\alpha(A_n))$.*

Proof. Let p_i be the ith prime number. By Betrand's postulate, p_i is less than 2^i for $i \geq 2$. Let m be the integer such that $2^m \leq n+1 < 2^{m+1}$. Since $p_1^2+p_2+\cdots+p_{m-1} = 2^2+3+p_3+\cdots+p_{m-1} \leq 1+2+2^2+\cdots+2^{m-1} = 2^m-1 \leq n$, A_n has an element of order $p_1^2p_2\cdots p_{m-1}$. Thus $\alpha(A_n) \geq m-1$. By a well-known theorem in number theory, $n/(8\log n) \leq \rho(A_n) \leq 12n/\log n$. Now

$$\alpha(A_n) \geq m-1 \geq \log_2(n+1) - 2 \geq \log n - 2, \quad \rho(A_n) \leq 12n/\log n \leq 12\exp(\alpha(A_n)+2)/(\alpha(A_n)+2).$$

It is easy to verify that $\rho(A_n) \leq 12\exp(\alpha(A_n))$ for $n \leq 124$ (In fact, $\rho(A_n) \leq 30$ if $n \leq 124$.) If $n > 124$, then $m \geq 7$ and $\alpha(A_n) \geq 6$. Since $e^2 \leq 8 \leq \alpha(A_n)+2$, $12\exp(\alpha(A_n)+2)/(\alpha(A_n)+2) \leq 12\exp(\alpha(A_n))$ and the lemma follows.

Lemma 5. *If G is a finite simple group of Lie type, then*

$$\rho(G) \leq 32\alpha(G)\exp(\alpha(G)).$$

Proof. Suppose that $G = G_m(q)$, where m is the Lie rank of G and q is a power of the characteristic r of G. Let $\Phi_i(x)$ be the cyclotomic polynomial whose roots are the ith primitive roots of unity. Then there exist nonnegative integers $f(m)$, $g(m)$, and $k(m,i)$ depending on m and/or i such that $|G| = q^{f(m)}\prod_{i\leq g(m)}\Phi_i(q)^{k(m,i)}/d$, where d is an integer with $d|m$. If $k(m,i) \neq 0$, then we know from Broué [2] that G has an abelian subgroup of order $\Phi_i(q)/d'$ $(d' = (d, \Phi_i(q)))$ except for $G = {}^2G_2(q)$, ${}^2F_4(q)$, or ${}^2B_2(q)$. For the exceptions, $r = 2$ or 3, $q = r^{2n+1}$, and only for the integer i which is divisible by $2r$ we have $\Phi_i(q) = \Phi_{2i}(\sqrt{q}) = n_1n_2$, where n_1 and n_2 are both integers and polynomials of $\sqrt{q}$ with coefficients in $Z[\sqrt{r}]$, and G also has abelian subgroups of order n_1 and n_2 respectively. Thus we have in any case that $\alpha(\Phi_i(q)) \leq 2\alpha(G)$. Accordingly, $\rho(G) \leq 1 + 2g(m)\alpha(G)$. Therefore, $\rho(G) \leq 1 + 60\alpha(G)$ if $g(m) \leq 30$. If $g(m) > 30$, then $G = A_m(q)$, ${}^2A_m(q)$, $B_m(q)$, $C_m(q)$, $D_m(q)$, or ${}^2D_m(q)$. Now the Weyl group of G contains as a section the symmetric group S_h of degree h with $h = [(m+1)/2]$, the integer part of $(m+1)/2$. Then we see that $g(m) \leq 2m+2$ and $h \geq m/2$. By the proof of Lemma 4 we have that $1 + h \leq 4\exp(\alpha(S_h)) \leq 4\exp(\alpha(G))$. Thus $\rho(G) \leq 1 + 2g(m)\alpha(G) \leq 1 + 4(m+1)\alpha(G) \leq 1 + 4(2h+1)\alpha(G) \leq 8(h+1)\alpha(G) \leq 32\alpha(G)\exp(\alpha(G))$ and the lemma follows.

Lemma 6. *If G is a sporadic simple group, then $\rho(G) \leq 15$.*

Proof. This is easily seen to be true by checking the orders of sporadic simple groups [4].

Now we are ready to prove Theorem 2.

Proof of Theorem 2. Suppose, toward a contradiction, that the theorem is not true and let G be a counterexample of minimal possible order. We set $S_0(G) = 1$ and define $S_1(G)$ to be the subgroup generated by the Fitting subgroup $F(G)$ and all minimal normal subgroups of G. Define $S_k(G)$ inductively by $S_k(G)/S_{k-1}(G) = S_1(G/S_{k-1}(G))$ for $k \geq 2$. Thus $S_1(G) = N_1 \times N_2 \times \cdots \times N_t \times F(G)$, where N_i's are nonabelian simple subgroups. Let m be the smallest number such that $S_m(G) = G$; then $S_{m-1}(G)$ is a proper subgroup of G. We see now that $S_k(G)/S_{k-1}(G) = B_k \times F_k$, where F_k is nilpotent and B_k is a direct product of nonabelian simple groups.

If B_k is nontrivial, then we claim that there is a prime factor p_k such that p_k divides the order of B_k and is prime to $|S_{k-1}(G)||G/S_k(G)|$. Set $\overline{G} = G/S_{k-1}(G)$. If the claim is not true, then for any prime divisor q of the order of B_k either $q \mid |S_{k-1}(G)|$ or $q \mid |G/S_k(G)|$. Let R be a Sylow 2-subgroup of $S_k(G)$; then $N_G(R)S_k(G) = G$ by the Frattini argument. Set $T = N_G(R)S_{k-1}(G)$. Clearly, F_k is contained in $\overline{T}$ while B_k is not. Thus T is a proper subgroup of G with $\rho(G) = \rho(T)$. By the minimality of G, $\rho(G) = \rho(T) \leq 16\alpha(T)^3(\alpha(T)+3)\exp(\alpha(T)) \leq 16\alpha(G)^3(\alpha(G)+3)\exp(\alpha(G))$, which is a contradiction. The contradiction proves that the claim holds.

Let Q_k be a Sylow subgroup of F_k then $\overline{Q_k}$ is normal in $\overline{G}$ by the nilpotence of F_k. If $\overline{Q_k}$ is not contained in the Frattini subgroup $\Phi(\overline{G})$ of $\overline{G}$, then we claim that $\overline{Q_k}$ is a minimal normal subgroup of $\overline{G}$ and is isomorphic to a Sylow subgroup of G. Let A be a maximal subgroup of G such that $S_{k-1}(G)$ is contained in A and Q_k is not contained in A then $G = AQ_k$. Hence $\overline{AQ_k} = \overline{G}$. If $(|\overline{Q_k}|, |A|) \neq 1$, then $\rho(G) = \rho(A)$, which is impossible by our assumption on G. Thus $(|\overline{Q_k}|, |A|) = 1$ and it follows at once from the maximality of A that $\overline{Q_k}$ is minimal normal in $\overline{G}$ and the claim holds.

Now from the claim we see that $F_k = \overline{H_k} \times \Phi_k$, where $\Phi_k = \Phi(\overline{G})$ and H_k is a Hall subgroup of G such that $|H_k| = |\overline{H_k}|$ and $\overline{H_k}$ is the product of some minimal normal subgroups of $\overline{G}$ which are also Sylow subgroups of $\overline{G}$. Since any prime divisors of $|\Phi_k|$ divide also the order of $\overline{G}/\Phi_k$, $\rho(G) \leq \sum_{k \leq m}(\rho(B_k) + \rho(\overline{H_k}))$. If B_k is nontrivial, then it is a direct product of nonabelian simple groups, so $B_k = M_1 \times M_2 \times \cdots \times M_s \times D$, where D is a normal subgroup making no contributions to $\rho(B_k)$, i.e., $\rho(B_k) = \rho(B_k/D)$ and M_i's are nonabelian simple groups such that there exists a prime divisor q_i of $|M_i|$ for each i with $(q_i, |M_j|) = 1$ for $j \neq i$. It is then obvious that $s \leq \alpha(B_k)$. Thus by Lemmas 4, 5, and 6, $\rho(B_k) \leq 32\alpha(B_k)^2\exp(\alpha(B_k))$. It follows that $\rho(B_k) + \rho(\overline{H_k}) \leq 32\alpha(B_k)^2\exp(\alpha(B_k)) + \alpha(\overline{H_k}) \leq 32(\alpha(B_k)^2 + \alpha(\overline{H_k})^2)\exp(\alpha(G)) \leq 32\alpha(G)^2\exp(\alpha(G))$ and thus $\rho(G) \leq 32m\alpha(G)^2\exp(\alpha(G))$. If B_k is nontrivial, then, as shown in the second paragraph of this proof, there is a prime divisor p_k of $|B_k|$ such that $(p_k, |S_{k-1}(G)||G/S_k(G)|) = 1$. So $(p_k, |\Phi(\overline{G})|) = 1$. By the property of H_k we see that p_k is prime to $|F_k|$. Let P_k be a Sylow p_k-subgroup of G if B_k is nontrivial and be trivial if B_k is trivial. Then $P_k \cong \overline{P_k}$. Set $N = P_kH_kS_{k-1}(G)$ then, noticing that $(|H_k|, |S_{k-1}(G)|) = 1$, we have $N/S_{k-1}(G) = C_{N/S_{k-1}(G)}(H_k) = C_N(H_k)S_{k-1}(G)/S_{k-1}(G)$. Hence we may

assume without loss of generality that $P_kH_k = P_k \times H_k$ for any k. Since $\overline{H_k}$ is normal in $\overline{G}$ for any k, by Frattini argument for G/H_1 and P_1H_1/H_1 we may assume that P_1H_1 is P_kH_k-invariant for any k. Apply our argument to $N_G(P_1H_1)$ and repeat the same procedure, we may also assume that P_iH_i is P_jH_j-invariant for any $i \leq j \leq m$. We set now $E = \langle P_i, H_i : i = 1, 2, \ldots, m\rangle$ and by Theorem 1, $\rho(E) \leq \alpha(E)(\alpha(E) + 3)/2 \leq \alpha(G)(\alpha(G) + 3)/2$. Since clearly $m \leq \rho(E)$, we have $\rho(G) \leq 16\alpha(G)^3(\alpha(G) + 3)\exp(\alpha(G))$, which is again contradictory to the assumption on G. We are done.

5

Example. Let $\mathrm{GF}(13^4)$ be as usual the Galois field of 13^4 elements. Let V be the additive group of $\mathrm{GF}(13^4)$ and N a subgroup of the multiplicative group of $\mathrm{GF}(13^4)$. Then N acts on V naturally and the extension $V : N$ is a Frobenius group with kernel V. Suppose that N is of order 35, and let a be an involution of the Galois group of $\mathrm{GF}(13^4)$. Now $N = \langle x\rangle \times \langle y\rangle$ and $x^a = x^{-1}$ and $y^a = y$, where x is of order 5 and y is of order 7. Of course $\langle a\rangle$ also acts on V in the usual way. Let W be a cyclic subgroup of order 29; then $N : \langle a\rangle$ acts on W in the following way: $w^x = w$, $w^a = w^{-1}$, and $w^y = w^{16}$, where $\langle w\rangle = W$. Finally we set $G = (V \times W) : (N : \langle a\rangle)$ then $\rho(G) = 5$ and $\alpha(G) = 2$. So $\rho(G) = \alpha(G)(\alpha(G) + 3)/2$.

6

We conclude by making two remarks.

(a) We see that for arbitrary finite groups G, $\rho(G) \geq \alpha(G)$. What can we say about G if $\rho(G) = \alpha(G)$? Evidently, if G is finite nilpotent, then $\rho(G) = \alpha(G)$. But it is easy to see that any finite group can be embedded into a finite group G with $\rho(G) = \alpha(G)$. So the condition $\rho(G) = \alpha(G)$ does little to restrict the structure of G. But one can prove by [14] without any difficulties that the finite nonabelian group G with $\rho(G) = \alpha(G)$ is not simple.

(b) Let G be a finite group with trivial center. We define

$$\beta(G) = \max\{\alpha(|G/C_G(x)|) : x \in G\}.$$

It is also an interesting question to find a function $g(n)$ of integers n such that $\rho(G) \leq g(\beta(G))$. B. Huppert conjectured that $\rho(G) \leq 2\beta(G)$ for any finite solvable groups G. Recently, Ferguson [5] proved that $\rho(G) \leq 4\beta(G) + 6$ if G is finite solvable.

Acknowledgments

The author thanks Professor M. Broué for comments and the referee for suggestions.

References

1. R. Brandl, *Finite groups all of whose elements are of prime power order*, Boll. Un. Mat. Ital. A (5) **18** (1981), 491–493.
2. M. Broué and G. Malle, *Théorèmes de Sylow génériques pour les groupes réductifs sur les corp finis*, Math. Ann. **292** (1992), 241–262.
3. R. W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters*, Wiley, New York, 1985.

4. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.
5. P. A. Ferguson, *Lengths of conjugacy classes of finite solvable groups.* II, J. Algebra **154** (1993), 223–227.
6. D. Gluck, *Primes dividing character degrees and character orbit sizes*, Proc. Sympos. Pure Math., vol. 47, Part 2, Amer. Math. Soc., Providence, RI, 1987, pp. 45–46.
7. P. Hall and G. Higman, *The p-length of a solvable group, and reduction theorems for Burnside's problem*, Proc. London Math. Soc. (3) **6** (1956), 1–42.
8. G. Higman, *Finite groups in which every element has prime power order*, J. London Math. Soc. **32** (1957), 335–342.
9. B. Huppert, *Inequalities for character degrees of solvable groups*, Arch. Math. (Basel) **46** (1986), 387–392.
10. L. K. Hua, *Introduction to number theory*, Sciences Press, Beijing, 1957.
11. O. Manz, *Arithmetical conditions on character degrees and group structure*, Proc. Sympos. Pure Math., vol. 47, Part 2, Amer. Math. Soc., Providence, RI, 1987, pp. 65–69.
12. W. J. Shi, *Characterization of finite simple groups and related topics*, Adv. in Math. (China) **20** (1991), 135–141.
13. M. Suzuki, *Finite groups with nilpotent centralizers*, Trans. Amer. Math. Soc. **99** (1961), 425–470.
14. J. S. Williams, *Prime graph components of finite groups*, J. Algebra **69** (1981), 487–513.
15. J. P. Zhang, *Finite groups with many conjugate elements*, J. Algebra (to appear).

DMI, École Normale Supérieure, Paris, France

Mathematical Institute, Beijing University, Beijing, China