PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, April 1976

ON LARGE CYCLIC SUBGROUPS OF FINITE GROUPS

EDWARD A. BERTRAM[1]

ABSTRACT. It is known that for each (composite) n every group of order n contains a proper subgroup of order greater than $n^{1/3}$. We prove that given $0 < \delta < 1$, for almost all $n \leqslant x$, as $x \to \infty$, every group G of order n contains a characteristic cyclic subgroup of square-free order $> n^{1-1/(\log n)^{1-\delta}}$, and provide an upper bound to the number of exceptional n. This leads immediately to a like density result for a lower bound to the number of conjugacy classes in G.

From the deep theorem by Feit and Thompson [6] that all groups of odd order are solvable, it immediately follows that for every odd (composite) integer n, if G is a group of order n then G contains a proper subgroup of order $\geqslant n^{1/2}$. On the other hand, Brauer and Fowler [2] showed that every group G of even order $n > 2$ contains a proper subgroup of order $> n^{1/3}$.

Denoting by $k(G)$ the number of conjugacy classes in the finite group G, we know that for every n, $k(G) > \log_2 \log_2 n$ if G has order n (see, e.g., [5] or [8]). Recently [1] the author showed that given any $c < \log 2$, for almost all integers $n \leqslant x$, as $x \to \infty$, $k(G) > (\log n)^c$ for each G of order n. Here we give a proof of the following

THEOREM. *Given $0 < \delta < 1$, almost all integers $n \leqslant x$, as $x \to \infty$, have the property that every group of order n contains a characteristic cyclic subgroup of square-free order $> n^{1-1/(\log n)^{1-\delta}}$, where the number of exceptional integers is $< x(2 \log \log x)/(\log x)^{\delta}$ for all large x.*

As an immediate corollary we considerably improve the above density result on the lower bound for $k(G)$, now obtaining $k(G) > n^{1-\varepsilon}$.

Finally, we note that Erdös [4], sharpening the results of Dornhoff and Spitznagel [3] on the scarcity of simple group orders, proved that for almost all $n \leqslant x$, every group of order n has a normal Sylow p-subgroup, where p is the largest prime factor of n, and the number of exceptional integers is

$$< x/\exp[(1/\sqrt{2} + O(1))(\log x \log \log x)^{1/2}].$$

In the course of the proof of our theorem we find that if $\{\varepsilon_n\}$ is a sequence tending to 0 (however slowly) then for almost all $n \leqslant x$, as $x \to \infty$, every group of order n has a normal Sylow p-subgroup of prime order $p > n^{\varepsilon_n}$,

Received by the editors February 19, 1975.

AMS (MOS) subject classifications (1970). Primary 20D10; Secondary 20D99.

[1] The author would like to thank P. Erdös and E. Straus for their important contributions to the preparation of this paper.

where of course the number of exceptional integers has an upper bound depending on $\{\varepsilon_n\}$.

LEMMA 1. *The number of positive integers $n \leqslant x$, such that $p^2 | n$ for some prime $p > f(x)$, is less than $x/f(x)$.*

PROOF. Since, for fixed p, the number of integers $\leqslant x$ which are divisible by p^2 is $[x/p^2]$, the number sought in the lemma is certainly no more than

$$\sum_{p>f(x)} \left[\frac{x}{p^2}\right] \leqslant x \sum_{p>f(x)} \frac{1}{p^2} < x \sum_{m>f(x)} \frac{1}{m^2} < x \int_{f(x)}^{\infty} \frac{dt}{t^2} = \frac{x}{f(x)}.$$

LEMMA 2. *The number of positive integers $\leqslant x$ with a prime factor $p > f(x)$, and simultaneously a divisor $d > 1$ satisfying $d \equiv 1 \pmod p$, is less than $x(\log x + 1)/f(x)$.*

PROOF. For fixed p, the number of positive integers $\leqslant x$, which are simultaneously divisible by p and some divisor $d > 1$ satisfying $d \equiv 1 \pmod p$, is at most $\sum_{l=1}^{[x/p^2]} [x/p(lp+1)]$. Thus, the number sought in the lemma is no more than

$$\sum_{p>f(x)} \sum_{l=1}^{[x/p^2]} \left[\frac{x}{p(lp+1)}\right] < x \sum_{p>f(x)} \left(\frac{1}{p^2} \sum_{l=1}^{[x/p^2]} \frac{1}{l}\right)$$
$$< x\left(\sum_{l=1}^{x} \frac{1}{l}\right)\left(\sum_{m>f(x)} \frac{1}{m^2}\right) < \frac{x(\log x + 1)}{f(x)}.$$

LEMMA 3. *The number of integers $\leqslant x$ which have a divisor $d \geqslant h(x)$, such that each prime factor of d is $\leqslant g(x)$, is less than $x(\log(g(x)) + c_1)/\log(h(x))$.*

PROOF. If $m_1, m_2, m_3, \ldots, m_N$ denote these integers, then in $\prod_{i=1}^{N} m_i$ the contribution of the primes $\leqslant g(x)$ is at least $h^N(x)$. On the other hand, the primes $\leqslant g(x)$ certainly contribute no more to $\prod_{i=1}^{N} m_i$ than their contribution to $[x]!$ Hence

$$h^N(x) \leqslant \prod_{p \leqslant g(x)} p^{(\sum_{i\geqslant 1}[x/p^i])} < \prod_{p \leqslant g(x)} p^{(x/(p-1))}$$

or

$$\frac{N \log(h(x))}{x} < \sum_{p \leqslant g(x)} \frac{\log p}{p-1} = \sum_{p \leqslant g(x)} \frac{\log p}{p} + \sum_{p \leqslant g(x)} \frac{\log p}{p(p-1)}$$
$$< \sum_{p \leqslant g(x)} \frac{\log p}{p} + \sum_{j=2}^{\infty} \frac{\log j}{j(j-1)} < \log(g(x)) + c_1$$

since we know [7, 22.6] that

$$\sum_{p \leqslant g(x)} \frac{\log p}{p} = \log(g(x)) + O(1),$$

and the infinite sum converges.

LEMMA 4. *Given* $0 < \delta < 1$, *almost all integers* $n \leqslant x$, *as* $x \to \infty$, *have a square-free divisor* n_0 *with the properties*:

(i) *if a prime p divides* n_0, *then* $p > (\log x)^{1+\delta}$;

(ii) *for each prime p which divides* n_0, *if* $d > 1$ *divides* n, *then* $d \not\equiv 1 (\mathrm{mod}\ p)$;

(iii) $(n_0, n/n_0) = 1$;

(iv) $n_0 > n^{1-1/(\log n)^{1-\delta}}$.

PROOF. Given $0 < \delta < 1$, almost all $n \leqslant x$ satisfy $n > x^\delta$; for such n and all large x,

$$\frac{n}{\exp((\log x)^\delta)} > n^{1-1/\delta(\log x)^{1-\delta}} > n^{1-1/(\log n)^{1-\delta}}.$$

Lemma 3, with $g(x) = (\log x)^{1+\delta}$ and $h(x) = \exp((\log x)^\delta)$, implies that the number of integers $n \leqslant x$, with prime decomposition

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l} p_{l+1}^{\alpha_{l+1}} \cdots p_{\nu(n)}^{\alpha_{\nu(n)}} \quad (p_i < p_{i+1})$$

satisfying

$$p_l \leqslant (\log x)^{1+\delta} < p_{l+1} \quad \text{and} \quad \prod_{i=1}^{l} p_i^{\alpha_i} \geqslant \exp((\log x)^\delta)$$

for some l, is less than $x((1+\delta)\log\log x + c_1)/(\log x)^\delta$ (showing, since we may assume $x^\delta < n$, that almost all integers $n \leqslant x$, as $x \to \infty$, have a prime factor $> (\log x)^{1+\delta}$). Lemmas 1 and 2 (with $f(x) = (\log x)^{1+\delta}$) now show that except for at most $x/(\log x)^{1+\delta} + x(\log x + 1)/(\log x)^{1+\delta}$ of those integers $n \leqslant x$, $n = \prod_{i=1}^{l} p_i^{\alpha_i} \prod_{j=l+1}^{\nu(n)} p_j^{\alpha_j}$, $p_l \leqslant (\log x)^{1+\delta} < p_{l+1}$ and $\prod_{i=1}^{l} p_i^{\alpha_i} \leqslant \exp((\log x)^\delta)$, we have for $l + 1 \leqslant j \leqslant \nu(n)$: (a) $\alpha_j = 0$ and (b) $d|n$ and $d > 1 \Rightarrow d \not\equiv 1 \pmod{p_j}$. For such n, put $n_0 = \prod_{j=l+1}^{\nu(n)} p_j$. Then n_0 is square-free and satisfies (i) through (iv). Finally, the number of integers $n \leqslant x$ which do not have such a square-free divisor n_0 is less than

$$x^\delta + \frac{x((1+\delta)\log\log x + c_1)}{(\log x)^\delta} + \frac{x}{(\log x)^{1+\delta}} + \frac{x(\log x + 1)}{(\log x)^{1+\delta}}$$
$$< 2x\frac{\log\log x}{(\log x)^\delta} \quad \text{for all large } x.$$

THEOREM. *Given* $0 < \delta < 1$, *almost all integers* $n \leqslant x$, *as* $x \to \infty$, *have the property that every group of order n has a characteristic cyclic subgroup of square-free order* $n_0 > n^{1-1/(\log n)^{1-\delta}}$, *where* $(n_0, n/n_0) = 1$.

PROOF.[2] We prove that each $n \leqslant x$, which has a square-free divisor n_0 satisfying (i) through (iv) of Lemma 4, has the property stated in the theorem.

Assume that n has such a divisor $n_0 = p_1 p_2 \cdots p_k (n_0, n/n_0) = 1$. Then each Sylow p_i-subgroup of G, $S_{p_i}(G)$, $1 \leqslant i \leqslant k$, is a normal subgroup (cyclic, of order p_i) of G, by property (ii) of Lemma 4, applied to the total number d_i of Sylow p_i-subgroups of G. Moreover, since the image, under any automorphism

[2] We thank the referee for simplifying the original proof (by induction) and also showing that the subgroup is characteristic.

of G, of an element of order p_i is another element of order p_i, each $S_{p_i}(G)$ is characteristic in G. Also, $S_{p_i} \cap S_{p_j}$ is the identity subgroup, for each pair $i \neq j$, $1 \leqslant i, j \leqslant k$. Thus $g_i g_j = g_j g_i$ for each such i, j, since $g_i g_j g_i^{-1} g_j^{-1} \in S_{p_i} \cap S_{p_j}$, by normality. If g_i generates $S_{p_i}(G)$, the product $g_1 g_2 \cdots g_k$ is therefore an element of order $p_1 p_2 \cdots p_k = n_0$, and so generates a (cyclic) subgroup H of order n_0. Since H is generated by the characteristic subgroups $S_{p_i}(G)$, it is also a characteristic subgroup of G.

REMARK. Let ε_x be a (positive) function tending to 0 arbitrarily slowly as $x \to \infty$. From Lemma 3, with $g(x) = x^{\varepsilon_x}$ and $h(x) = \sqrt{x}$, almost every $n \leqslant x$ has a prime factor $p > x^{\varepsilon_x}$; and almost none of these integers has a nontrivial divisor $\equiv 1 \pmod{p}$, by Lemma 2. Thus for almost all n every group of order n has a normal Sylow p-subgroup of order $p > n^{\varepsilon_n}$.

COROLLARY. *Given $\varepsilon > 0$, almost all $n \leqslant x$ have the property that $k(G) > n^{1-\varepsilon}$ for each group G of order n.*

PROOF. Suppose G is a group of order n, and H a cyclic subgroup of G, of order $n_0 > n^{1-\varepsilon/2}$. Let the (complete) conjugacy class (in G) of $h \in H$ be denoted by $[h]$, and the centralizer (in G) of h by $C(h)$.

Summing over the $k_G(H)$ distinct classes (of G) in H we have

$$n_0 = |H| = \sum |[h] \cap H| \leqslant \max_{h \in H} |[h]| \cdot k_G(H)$$

$$\leqslant \frac{n \cdot k(G)}{\min_{h \in H} |C(h)|} \leqslant \frac{n}{n_0} \cdot k(G),$$

or $k(G) \geqslant n_0^2/n > n^{1-\varepsilon}$.

REMARK. *Erdös comments that by more complicated number theoretic methods one can prove that as $f(n) \to \infty$ arbitrarily slowly almost every n has a square-free divisor $d > n/(\log n)^{f(n)}$ so that $(d, n/d) = 1$ and, for every $p | d, n$ has no nontrivial divisor $\equiv 1 (\operatorname{mod} p)$. This is best possible and leads to an improvement of the main theorem, replacing $n^{1-1/(\log n)^{1-\delta}}$ by $n^{1-(f(n)\log\log n)/\log n}$.*

REFERENCES

1. E. A. Bertram, *A density theorem on the number of conjugacy classes in finite groups*, Pacific J. Math. **55** (1974), 329–333.
2. R. Brauer and K. A. Fowler, *On groups of even order*, Ann. of Math. (2) **62** (1955), 565–583. MR **17**, 580.
3. L. Dornhoff and E. L. Spitznagel, Jr., *Density of finite simple group orders*, Math. Z. **106** (1968), 175–177. MR **38** #1162.
4. P. Erdös, *On the scarcity of simple groups*, Science and Human Progress, Professor D. D. Kosambi Commemoration Volume, 1974.
5. P. Erdös and P. Turán, *On some problems of a statistical group-theory*. IV, Acta. Math. Acad. Sci. Hungar. **19** (1968), 413–435. MR **38** #1156.
6. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR **29** #3538.
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford Univ. Press, London, 1960.
8. M. Newman, *A bound for the number of conjugacy classes in a group*, J. London Math. Soc. **43** (1968), 108–110. MR **37** #1461.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024