ON ORDERS SOLELY OF ABELIAN GROUPS

by S. SRINIVASAN

(Received 6 November, 1985)

1. Introduction. Let $n = \prod_{i=1}^{r} p_i^{a_i}$ be the factorization of an integer $n(>1)$ into prime powers, and set $\Phi(n) := \prod_{i=1}^{r} (p_i^{a_i} - 1)$. In particular, for squarefree n, $\Phi(n) = \phi(n)$. Consider the set

$$A := \{n : 1 \leqslant a_i \leqslant 2,\ 1 \leqslant i \leqslant r;\ (n, \Phi(n)) = 1\}.$$

It is known (from [**5**]) that A consists precisely of those integers n for which there is no non-abelian group of order n. It is also known (from [**7**]) that the set

$$C := \{n : n \in A,\ n \text{ squarefree}\}$$

consists solely of integers n with the property that every group of order n is cyclic. We set $C' = A - C$.

For a sequence B of integers, let $B(x)$ denote the number of $m \in B$ with $m \leqslant x$. In [**1**], Erdös proved that

$$C(x) \sim e^{-\gamma} x L_3^{-1}, \qquad (x \to \infty) \tag{1}$$

in the notation $L_1 := \log x$, $L_{r+1} := \log L_r$ $(r \geqslant 1)$, where γ is Euler's constant. Recently, in [**8**], Warlimont considered $C'(x)$ and showed that

$$x L_2^{-1} L_3^{-2} \ll C'(x) \ll_\varepsilon x L_2^{-1} L_3^{\varepsilon - 1/2}, \qquad (x \to \infty) \tag{2}$$

for every $\varepsilon > 0$. In the present paper we show that here one can also have the lower estimate as the upper bound. Thus we obtain the following theorem.

Theorem. *We have*

$$C'(x) \asymp x L_2^{-1} L_3^{-2}, \tag{3}$$

as $x \to \infty$.

Remark. The proof here uses a result from the large sieve instead of the result from [**2**] which was employed in [**8**] in obtaining the upper bound in (2).

2. Some lemmas. The following lemma, derived from the large sieve, is basic in the proof.

Lemma 1. *Let $q(m)$ denote the least prime divisor of m and write*

$$S(x, y, p) := \sum_{\substack{m \leqslant x \\ (p, \phi(m)) = 1 \\ q(m) \geqslant y}} 1.$$

https://doi.org/10.1017/S0017089500006728 Published online by Cambridge University Press

Then, for $(2\leqslant)\ y \leqslant p \leqslant (\log x)^{1/4}$, *we have*

$$S(x, y, p) \leqslant c_0 \frac{x}{\log y} \exp\left(-\frac{\log\log x}{10p}\right), \qquad x \to \infty$$

where c_0 *is an absolute constant.*

Proof. In Theorem 7.1 of [**6**] (which is practically the Corollary in [**4**]), take $N = x$, $z = x^{1/2}$ (say) and, for primes q, $\omega(q) = 1$ if either $q \leqslant y$ or $q \equiv 1 \pmod p$ and $\omega(q) = 0$ otherwise. This gives

$$S(x, y, p) \leqslant \frac{2x}{L(z)},$$

where

$$L(z) := \sum_{m \leqslant z} \mu^2(m) \prod_{q | m} \frac{\omega(q)}{q - \omega(q)}.$$

Now from (9.38) of [**6**], since $\omega(q) = 0$ or 1, it follows that

$$L(z) \geqslant \prod_{\substack{q \leqslant z \\ \omega(q)=0}} \left(1 - \frac{1}{q}\right) \log z.$$

On using $\log z \geqslant \frac{2}{3} \prod_{q \leqslant z} \left(1 - \frac{1}{q}\right)^{-1}$ (say, for large z), we obtain, from the above estimates,

$$S(x, y, p) \leqslant 3x \prod_{q \leqslant x^{1/2}} \left(1 - \frac{\omega(q)}{q}\right).$$

This bound yields the result of Lemma 1, in view of the definition of $\omega(q)$ and the prime number theorem for the arithmetic progression of integers congruent to 1 mod p.

REMARK. Here the condition $p \leqslant (\log x)^{1/4}$ is imposed only for making c_0 effective.

For convenience of reference we state the next simple lemma. However, for our present purpose, we only need the upper bound given by this lemma.

LEMMA 2. *We have*

$$\sum_{p > Y} \frac{\log p}{p^2} \exp(-X/p) \sim X^{-1}$$

as $X/Y \to \infty$.

Proof. Writing $\theta(u) := \sum_{p \leqslant u} \log p$ and $b(u) = u^{-2} \exp(-X/u)$, we have

$$\sum_{p > Y} \frac{\log p}{p^2} \exp(-X/p) = \sum_{m > Y} \theta(m)(b(m) - b(m+1)) + O(\theta(Y+1) b(Y+1)).$$

Using $\theta(u) \sim u$, $u \to \infty$ (cf. for example [**3**, Theorem 434, p. 362]) we see that the above

https://doi.org/10.1017/S0017089500006728 Published online by Cambridge University Press

quantity equals

$$\sum_{m>Y} m(b(m)-b(m+1))+O(Y^{-1}\exp(-X/Y))+o(X^{-1}),$$

since $b(u)$ is monotonic in $(Y, \frac{1}{2}X)$ and $(\frac{1}{2}X, \infty)$. Now, as $X/Y \to \infty$, the last expression equals $\sum_{m>Y} b(m)+o(X^{-1}) \sim X^{-1}$. This proves the lemma.

3. Proof of the theorem. To start with, we have

$$C'(x) \leq \sum_{1<k\leq x} \sum_{\substack{m\leq xk^{-2} \\ mk\in C}} 1 \leq \sum_{1<k\leq Z} \sum_{\substack{m\leq xk^{-2} \\ mk\in C}} 1+O(xZ^{-1}) \tag{4}$$

for *any* $Z \leq x$. Now let $Y \leq Z$ be another parameter to be chosen later. In the last double summation of (4) we consider those mk having a prime divisor $q \leq Y$. For each prime $q \leq Y$, the number of such mk ($\leq x$) having q for the least prime divisor does not exceed, by Lemma 1 (with $p=q$, $y=2$, say),

$$c_0(\log 2)^{-1}x\exp(-L_2/10q),$$

since $mk \in C$. Hence the number of mk^2 under consideration in (4) is

$$O\Big(xZ\sum_{q\leq Y}\exp(-L_2/10q)\Big)=O(xZ^2\exp(-L_2/10Y)).$$

Choosing here $Y=L_2^{3/4}=Z^{1/2}$, say, it follows from (4) that

$$C'(x) \leq \sum_{Y<k\leq Y^2} \sum_m{}^* 1+O(xL_2^{-3/2}) \tag{4'}$$

with * signifying the restrictions (i) $m \leq xk^{-2}$, (ii) $mk \in C$ and (iii) the least prime divisor of mk exceeds Y. Now, these conditions imply that k is a *prime* (p, say). Again, by Lemma 1 (with $y=Y$ and xp^{-2} for x) we obtain

$$\begin{aligned}\sum_{Y<p\leq Y^2} \sum_m{}^* 1 &= \sum_{Y<p\leq Y^2} S(x/p^2, Y, p) \\ &\ll \sum_{Y<p\leq Y^2} \frac{x\log p}{p^2(\log Y)^2}\exp\Big(-\frac{\log\log x}{10p}\Big) \\ &\ll \frac{x}{(\log Y)^2}\sum_{p>Y}\frac{\log p}{p^2}\exp\Big(-\frac{\log\log x}{10p}\Big).\end{aligned}$$

Therefore, by our choice of Y and Lemma 2 (with $X=L_2/10$, noting that $X/Y\to\infty$), we conclude from (4') that

$$C'(x)=O(xL_3^{-2}L_2^{-1}+xL_2^{-3/2}). \tag{5}$$

Combining the lower estimate in (2) with (5) completes the proof of the theorem.

ACKNOWLEDGEMENT. The author wishes to thank the referee for some helpful suggestions.

REFERENCES

1. P. Erdös, Some asymptotic formulas in number theory, *J. Indian Math. Soc.* (*N.S.*) **12** (1948), 75–78.

2. R. R. Hall, Halving an estimate obtained from Selberg's upper bound method, *Acta Arith.* **25** (1973/4), 347–351.

3. G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers,* 4th edn. (Oxford University Press, 1964).

4. H. L. Montgomery, A note on the large sieve, *J. London Math. Soc.* **43** (1968), 93–98.

5. L. Rédei, Das "schiefe Produkt" in der Gruppen theorie, *Comment. Math. Helv.* **20** (1947), 225–264.

6. H.-E. Richert, *Sieve methods* (Tata Institute Lecture Notes, Bombay, 1976).

7. T. Szele, Uber die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört, *Comment. Math. Helv.* **20** (1947), 265–267.

8. R. Warlimont, On the set of natural numbers which only yield orders of abelian groups, *J. Number Theory* **20** (1985), 354–362.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400 005
INDIA

https://doi.org/10.1017/S0017089500006728 Published online by Cambridge University Press