Canad. Math. Bull. Vol. 30 (4), 1987

ON THE NUMBER OF GROUPS OF SQUAREFREE ORDER

BY
M. RAM MURTY AND S. SRINIVASAN

ABSTRACT. Let $G(n)$ denote the number of non-isomorphic groups of order n. We prove that for squarefree integers n, there is a constant A such that

$$G(n) = 0(\emptyset(n)/(\log n)^{A \log\log\log n}),$$

where $\emptyset$ denotes the Euler function. This upper bound is essentially best possible, apart from the constant A.

1. **Introduction.** With the recent classification of finite simple groups, the number of non-isomorphic groups of order n affords a good estimate. Indeed, letting $G(n)$ denote this number, it is known that [6],

$$\log G(n) = O(\log^3 n). \tag{1}$$

For squarefree integers n, the upper bound in (1) can be reduced, rather drastically. In [4], it was shown that

$$\mu^2(n)G(n) \leqq \varphi(n), \tag{2}$$

where φ denotes the Euler φ-function. In [2], the authors asked whether

$$G(n) = o(\varphi(n)), \tag{3}$$

as n ranges over squarefree numbers.

More generally, denote by $C(n)$ the number of groups of order n, all of whose Sylow subgroups are cyclic. Then, is it true that

$$C(n) = o(\varphi(n)), \tag{4}$$

as n tends to infinity? The purpose of this paper is to establish (4). In fact, we derive an upper bound for $C(n)$ and show that it is apart from constants, best possible.

THEOREM 1. *There is a constant $A > 0$ such that*

$$C(n) = 0(\varphi(n)/(\log n)^{A \log\log\log n}).$$

Received by the editors April 11, 1986.
AMS Subject Classification: 10H26.

COROLLARY. *For squarefree integers n,*

$$G(n) = 0(\varphi(n)/(\log n)^{A \log\log\log n}).$$

REMARK. This corollary establishes (3).

THEOREM 2. *There is a constant $B > 0$ such that for infinitely many squarefree n,*

$$G(n) > \varphi(n)/(\log n)^{B \log\log\log n}.$$

COROLLARY.

$$C(n) = \Omega(\varphi(n)/(\log n)^{B \log\log\log n}).$$

REMARK. Theorem 2 improves upon the Ω-result established in [2] and together with Theorem 1, shows that this is the best possible estimate, apart from values of A and B.

NOTATION. For the sake of convenience in the proofs, we shall denote $L_2 = \log\log n$, and $L_3 = \log\log\log n$.

2. **Preliminaries.** The function $C(n)$ was first introduced in [5]. There, an explicit formula was derived, which we utilise in our derivation of the upper bound. Define $v(p^j, m)$ by the following formula:

$$p^{v(p^j,m)} = \prod_{q|m} (p^j, q - 1),$$

where p and q denote prime numbers (here and elsewhere in the paper).

LEMMA 1.

$$C(n) = \sum_{\substack{d|n \\ (d,n/d)=1}} \prod_{p^\alpha \| d} \left(\sum_{j=1}^{\alpha} \frac{p^{v(p^j,n/d)} - p^{v(p^{j-1},n/d)}}{p^{j-1}(p-1)} \right).$$

REMARK. The notation $p^\alpha \| d$ means that $p^\alpha | d$ and $p^{\alpha+1} \nmid d$. When n is squarefree, we find an explicit formula for $G(n)$, a classical result of Hölder [3].

PROOF. The proof is given in [5].

Define $f(n)$ as follows:

$$f(n) = \prod_{p|n} (n, p - 1). \tag{5}$$

The function $f(n)$ was introduced earlier in [4], in the context of enumerating finite groups, but is a function of interest in its own right.

LEMMA 2.

$$\frac{C(n)}{f(n)} \leqq \prod_{\substack{p|n \\ \nu(p,n)>0}} \frac{2}{p-1}.$$

PROOF. We first note that

$$f(n) = \prod_{p|n} (n, p-1) = \prod_{p|n} \prod_{q^\alpha \| n} (q^\alpha, p-1) = \prod_{q^\alpha \| n} q^{\nu(q^\alpha, n)},$$

by virtue of the definition of $\nu(q^\alpha, n)$. By lemma 1, we deduce

$$C(n) \leqq \prod_{p^\alpha \| n} \left(1 + \sum_{j=1}^{\alpha} \frac{p^{\nu(p^j, n)} - p^{\nu(p^{j-1}, n)}}{p^{j-1}(p-1)}\right)$$

as each summand in the resulting expansion of the product dominates the corresponding summand appearing in the formula for $C(n)$. Dropping the p^{j-1} in the denominator, we find that the telescoping sum in the product yields,

$$C(n) \leqq \prod_{\substack{p^\alpha \| n \\ \nu(p,n)>0}} \left(1 + \frac{p^{\nu(p^\alpha, n)} - 1}{p-1}\right).$$

In view of our initial observation concerning $f(n)$, the inequality stated in the Lemma follows.

LEMMA 3. *There is a constant $C > 0$ and a squarefree $M \leqq x^2$ such that*

$$\sum_{\substack{p-1|M \\ p \text{ prime}}} 1 > \exp(C \log x / \log\log x),$$

where C is independent of x.

REMARK. Prachar proved this result with M not necessarily squarefree, but subject to the generalised Riemann hypothesis. By utilising results from the large sieve theory, this restriction was removed in Adleman, Pomerance and Rumely [1]. The proof can be found in [1].

LEMMA 4. *Let n be a positive integer and denote by M_2 the set of prime divisors p of n such that $(p-1)|n$. Let $\nu_2(n)$ denote the cardinality of M_2 and set*

$$\nu_3(n) = \nu\left(\prod_{p \in M_2} (p-1)\right)$$

where $\nu(n)$ denotes the number of distinct prime factors of n. Let $n = n_1 n_2$ where n_1 is the product of the prime divisors of n. Then

$$2^{\nu_3(n)} d(n_2) \geqq \nu_2(n),$$

where $d(n)$ denotes the number of divisors of n.

PROOF. For each $p \in M_2$, $p - 1 = Q_1Q_2$ where $Q_1|n_1$ and $Q_2|n_2$, and $\nu(Q_1) = \nu(p - 1)$ in the factorisation. As $\nu_3(n)$ denotes the number of distinct prime factors appearing in the factorizations, then $2^{\nu_3(n)}$ is the total number of possibilities for Q_1 and $d(n_2)$ is an upper bound for the possibilities for Q_2. Hence,

$$2^{\nu_3(n)}d(n_2) \geqq \nu_2(n),$$

as desired.

3. **The upper bound.** In this section, we shall prove Theorem 1. Let us denote by V, the product:

$$V = \prod_{\substack{p|n \\ \nu(p,n)>0}} p.$$

Then, lemma 2 implies that

$$C(n) \leqq \varphi(n)/V^{1/2} \tag{6}$$

in view of the fact that $f(n) \leqq \varphi(n)$. Let us write $n = n_1n_2$ where n_1 is the product of the primes dividing n. Then, for $p|n$, $(n, p - 1) \leqq Vn_2$, as primes not dividing V do not contribute to $(n, p - 1)$. Therefore,

$$C(n) \leqq (Vn_2)^{\nu(n)}. \tag{7}$$

We first note the trivial estimate

$$C(n) \leqq \varphi(n)/n_2,$$

so that if $n_2 \geqq Y = \exp(\epsilon L_2L_3)$, for some $\epsilon > 0$, (to be chosen later), the desired estimate follows. We therefore suppose that

$$n_2 \leqq \exp(\epsilon L_2L_3).$$

We consider two cases:

CASE 1. $\nu(n) \leqq (\log n)^{1/2}$.

In this case, we find that if $V > \exp(L_2L_3)$, then the desired result follows immediately from (6). If $V < \exp(L_2L_3)$, then from (7) we find that

$$C(n) = 0(n^{\epsilon}),$$

in this case.

CASE 2. $\nu(n) > (\log n)^{1/2}$.

Let $\nu_1(n)$ denote the number of prime divisors p of n such that $(p - 1)\,|n$. Then

(8) $$f(n) = \prod_{p|n} (n, p - 1) \leqq 2^{-\nu_1(n)}\varphi(n),$$

because each prime p enumerated by $\nu_1(n)$ can contribute at most $(p - 1)/2$ to the product for $f(n)$. Therefore, in the notation of lemma 4,

$$\nu_1(n) + \nu_2(n) = \nu(n).$$

Thus, if $\nu_1(n) > \frac{1}{2}(\log n)^{1/2}$, then from (8), we deduce that, in this case,

$$G(n) = 0(\varphi(n) \exp(-C_1(\log n)^{1/2}))$$

for some $C_1 > 0$. We may therefore suppose that $\nu_2(n) \geqq \frac{1}{2}(\log n)^{1/2}$, because $\nu(n) > (\log n)^{1/2}$. By lemma 4, (with the same notation for $\nu_3(n)$),

$$2^{\nu_3(n)}d(n_2) \geqq \nu_2(n) \geqq \frac{1}{2}(\log n)^{1/2}.$$

At the outset of our proof, we stated that

$$n_2 \leqq Y = \exp(\epsilon L_2 L_3).$$

Now by an elementary estimate, due to Ramanujan, (see Prachar [8]),

$$d(n_2) \leqq \exp(C \log Y/\log \log Y)$$

for some constant $C > 0$. Hence,

$$d(n_2) \leqq \exp(\epsilon L_2),$$

so that

(9) $$\nu_3(n) \geqq \delta \log \log n$$

for some $\delta > 0$ and a suitable choice of $\epsilon > 0$.
Hence, for at least $\nu_3(n)$ primes $q|n$, we have $\nu(q, n) > 0$. If p_i denotes the i-th prime, setting

$$D = \prod_{i \leqq \nu_3(n)} \frac{1}{2}(p_i - 1),$$

we find, utilising elementary estimates, that for some constant $C_0 > 0$,

$$D \geqq \exp(C_0 L_2 L_3),$$

in view of (9). From the inequality in lemma 2, we deduce that

$$C(n) \leqq \varphi(n) \exp(-C_1 L_2 L_3)$$

for some constant $C_1 > 0$, as desired. This completes the proof of the theorem.

4. **The Ω-estimate.** We now prove Theorem 2. By lemma 3, there is a squarefree integer $M \leqq x^2$ such that

$$M = q_1 \ldots q_r$$

and the set

$$E = \{p{:}p - 1|M\}$$

has size at least

$$\exp(C \log x/\log\log x)$$

for some $C > 0$. If for some $q_i|M$, there is no $p \in E$ such that $q_i|(p - 1)$, then we may remove it from M, without any loss. Therefore we may suppose that for every $q|M$, there is a $p \in E$ such that $q|p - 1$. Choose a subset E^* of E such that

$$\operatorname*{lcm}_{p \in E^*} (p - 1) = M,$$

and set $n = M(\prod_{p \in E} p)$. We first note that $p - 1|n$ for all $p \in E$. Clearly,

$$|E^*| \leqq r,$$

as M has r prime factors. Also,

$$|E| \leqq \{p|n{:}p - 1|n\} \leqq |E| + r.$$

For this particular choice of n, we find

$$G(n) \geqq \prod_{p|M} \left(\frac{p^{\nu(p,n/M)} - 1}{p - 1}\right). \tag{10}$$

We utilise the inequality $(p^\nu - 1)/(p - 1) \geqq p^{\nu-1}$ for $\nu \geqq 1$ to deduce from (10) that

$$G(n) \geqq M^{-1} \prod_{p|M} p^{\nu(p,n/M)}.$$

Since,

$$p^{\nu(p,m)} = \prod_{q|m} (p, q - 1),$$

we obtain

$$G(n) \geqq M^{-1} \prod_{p|M} \prod_{q|n/M} (p, q - 1)$$

$$= M^{-1} \prod_{q|n/M} (M, q - 1).$$

We note that every $q|n/M$ satisfies $q - 1|M$. Hence,

$$G(n) \geqq M^{-1}\varphi(n/M) = \varphi(n)M^{-1}/\varphi(M)$$
$$\geqq \varphi(n)/M^2.$$

As $M \leqq x^2$, we deduce

$$G(n) \geqq \varphi(n)/x^4.$$

We now need an upper bound for x. As E has size at least $\exp(C \log x/\log \log x) = T$ (say), n is at least the product of the first T primes, so that $\log n \geqq C_3 T \log T$ for an appropriate constant $C_3 > 0$. Hence,

$$C \log x/\log \log x \leqq \log \log n,$$

which implies that for some constant $C_4 > 0$,

$$\log x \leqq C_4 L_2 L_3.$$

Hence, the Ω-estimate follows from this.

5. **Concluding remarks.** Our result shows that

$$\sum_{n \leqq x} C(n) = o(x^2). \tag{11}$$

Of independent interest is the behaviour of the function

$$f(n) = \prod_{p|n} (n, p - 1).$$

Is it true that $f(n) = o(\varphi(n))$? We cannot answer this at present though we can show that for odd values of n, $f(n) = o(\varphi(n))$.

In this connection, let

$$A(n) = \text{card}(p|n : p - 1 \nmid n).$$

Then, it is easy to see that

$$f(n) \leqq 2^{-A(n)}\varphi(n).$$

Is it true that $A(n) \to \infty$ as $\nu(n) \to \infty$? If so, this would establish that $f(n) = o(\varphi(n))$.

It is not difficult to show that

$$\sum_{n \leqq x}{}' f(n) = O((x \log \log x/\log x)^2), \tag{12}$$

where the dash on the summation indicates that n is squarefree. Indeed, in [4], it was proved that

$$\sum_{n \leqq x} \mu^2(n) \log^2 f(n) = O(x(\log \log x)^2)$$

so that

$$\mathrm{card}(n \leqq x : f(n) > x^{1/2}) = O(x(\log \log x/\log x)^2).$$

From this, (12) is easily deduced.

Of course, the behaviour of $f(n)$ now has no relevance to $G(n)$ or $C(n)$ in view of Theorems 1 and 2. But we record our remarks here as the function $f(n)$ is of interest in its own right.

Recently Pomerance proved that the question concerning the order of magnitude of the sum appearing in (11) is intimately connected with the Halberstam-Elliott conjecture concerning the distribution of the primes in arithmetic progressions. More precisely, he showed in [9] that

$$\sum_{n \leqq x} \mu^2(n) G(n) > x^{1.68} \tag{13}$$

by utilizing a key theorem of Balog-Fouvry-Rousselet asserting the existence of at least $x/\log^2 x$ primes $p < x$ such that all the prime factors of $p - 1$ are $<x^{.32}$. If a corresponding result could be established for an arbitrary exponent $c > 0$, rather than .32 appearing in the above cited result, we would obtain

$$\sum_{n \leqq x} \mu^2(n) G(n) > x^{2-c}. \tag{14}$$

Similar results naturally hold for the summatory function involving $C(n)$. Pomerance conjectures that

$$\sum_{n \leqq x} \mu^2(n) G(n) = \cdot x^2/\exp[\,(1 + o(1))\,\log x \log_3 x/\log_2 x] \tag{15}$$

where $\log_2 x$ denotes $\log \log x$ and $\log_3 x = \log(\log_2 x)$. The upper bound in (15), with $C(n)$ replacing $\mu^2(n)G(n)$, has been shown by Pomerance in [9].

References

1. L. M. Adleman, C. Pomerance, R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Annals of Mathematics, **117** (1983), pp. 173-206.

2. P. Erdös, M. Ram Murty, V. Kumar Murty, *On the enumeration of finite groups*, Journal of Number Theory, **25** (1987), pp. 360-378.

3. O. Hölder, *Die gruppen mit quadratfreier ordnungszahl*, Nachr. Konigl. Ges. Wiss. Gottingen Math.-Phys. Kl (1895), pp. 211-229.

4. M. Ram Murty, V. Kumar Murty, *On the number of groups of a given order*, Journal of Number Theory, **18** (1984), pp. 178-191.

5. ———, *On groups of squarefree order*, Math. Annalen, **267** (1984), pp. 299-309.

6. P. Neumann, *An enumeration theorem for finite groups*, Quart. J. Math. Oxford Ser. (2) **20** (1969), pp. 395-401.

7. K. Prachar, *Uber die anzahl der Teiler einer naturlichen zahl welche die form p − 1 haben*, Monatsh. Math. **59** (1955), pp. 91-97.

8. ———, *Primzahlverteilung, Die grundlehren der Math. Wiss*, in *Einzeldarst*, Vol. 91, Berlin, Springer, 1957.

9. C. Pomerance, *On the average number of groups of squarefree order*, (to appear in the Proceedings of the A.M.S.).

M. Ram Murty
Department of Mathematics
McGill University
Montreal, Canada H3A 2K6

S. Srinivasan
School of Mathematics
Tata Institute of Fundamental Research
Bombay 400 005
India