A LOWER BOUND ON THE NUMBER OF FINITE SIMPLE GROUPS

MICHAEL E. MAYS
Department of Mathematics
West Virginia University
Morgantown, West Virginia 26506
U.S.A.

(Received March 5, 1980)

ABSTRACT. Let S(n) = |{m < n: there is a (non-cyclic) simple group of order m}|. Investigation of known families of simple groups provides the lower bound S(n) >> n^{1/4}/log n.

KEY WORDS AND PHRASES. Simple group, asymptotic formula.

1980 MATHEMATICAL SUBJECT CLASSIFICATION. Primary 20 D 06.

The non-specialist reader should refer first to Hurley and Rudvalis (4).

Write S(n) = |{m < n: there is a simple group of order m}| and S'(n) = |{G: G is a simple group and |G| < n}|. Dornhoff (1), Dornhoff and Spitznagel (2), and Erdős (3) got successively better upper bounds for S(n) by refining an argument which uses the Sylow theorems to generate a necessary criterion for a simple group of order m to exist. From the observation that S(n) ≤ |{m < n: for any prime p|m there is a d|m such that d > 1 and d ≡ 1 (mod p)}| Dornhoff found that
S(n) = o(n) and Erdős derived a complicated bound better than that of Dornhoff but not as good as $o(n^{1-\varepsilon})$. It should be noted that in general $S(n) < S'(n)$ because it occasionally (in fact infinitely often) happens that non-isomorphic simple groups of the same order exist.

We offer the following lower bound for $S(n)$, hence for $S'(n)$

**THEOREM.** $S(n) \gg n^{1/4}/\log n$.

**PROOF.** We estimate the number of integers $m < n$ which can be the order of a simple group in one of the known families and note that in all but finitely many cases the orders of the groups in that family are distinct.

From a list of known families of simple groups (4, p. 708) we see that one family dominates in the sense that for $F_i(n) = \{m < n: m is the order of a simple group in family i\}$, $F_i(n) = O(F_1(n))$ for any $i$. $F_1(n)$ is the number of simple projective special linear groups of order less than $n$.

Thus to estimate $S(n)$ from below, we count tripletons $(k, p, a)$ such that

1) $k$ is an integer greater than 1,
2) $a$ is an integer $\geq 1$, and if $p = 2$ or $p = 3$ and $k = 2$ then $a > 1$, and
3) $p$ is a prime, and writing $q = p^a$ we have

$$f(k, p, a) = \frac{k(k-1)/2}{\prod_{i} (q^i - 1)/(k, p-1)} = |\text{PSL}_k(q)| < n.$$  

$\text{Artin (5)}$ showed that in exactly two cases distinct tripletons give rise to isomorphic groups, and in one case there are non-isomorphic groups of the same order in that family. Since $f(k, p, a) < \frac{k(k-1)/2}{q^{k(k+1)/2}-1} < q^2$, $S(n) \gg \{m < n: \text{there exists } (k, p, a) \text{ satisfying 1), 2), and 3)} \text{ such that } m = p^{ak^2}\}$. Such tripletons may be counted by a triple sum, and we have

$$S(n) \gg \sum_{a = 1}^{\infty} \sum_{k = 2}^{\infty} \sum_{p < n} \frac{1}{ak^2} \geq 1. \text{ Constraining } a \text{ and } k \text{ so that } n^{1/ak^2} \geq 2,$$
\[ S(n) \gg \sum_{a=1}^{\log n} \sum_{k=2}^{\log 2} \pi(n^{1/ak^2}), \]

and the Prime Number Theorem using \( a = 1 \) and \( k = 2 \) yields \( S(n) \gg n^{1/4}/\log n \).

This theorem is of interest because it has been conjectured (3) that \( S'(n) = o(n^{1-\varepsilon}) \), or even \( S'(n) = o(n^{1/3}) \). We have that \( 1/4 - \varepsilon \) is a lower bound on the exponent of \( n \), and if when all simple groups are classified no new family denser than the projective special linear groups appears, analyzing a perhaps more complicated triple sum carefully should yield the best exponent \( b \) in the estimate \( S'(n) = o(n^b) \).

ACKNOWLEDGMENT: I wish to thank Professor Raymond Ayoub of the Pennsylvania State University for his advice and help.

REFERENCES
