JOURNAL OF NUMBER THEORY 17, 29–36 (1983)

On the Density of Various Classes of Groups

M. RAM MURTY

Department of Mathematics, M.I.T., Cambridge, Massachusetts 02139

AND

V. KUMAR MURTY

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138

Communicated by H. Zassenhaus

Received April 14, 1981; revised August 15, 1981

Let $\mathscr{E}$ be a subset of the set of all isomorphism classes of finite groups. We consider the number $F_{\mathscr{E}}(x)$ of positive integers $n \leqslant x$ such that all groups of order n lie in $\mathscr{E}$. When $\mathscr{E}$ consists of the isomorphism classes of all finite groups of any of the following types, we obtain an asymptotic formula for $F_{\mathscr{E}}(x)$: cyclic groups, abelian groups, nilpotent groups, supersolvable groups, and solvable groups. In the course of the arguments, we also obtain, for almost all n, a lower bound for the number of groups of a given order n.

1. INTRODUCTION

Let $\mathscr{G}$ be the set of all isomorphism classes of finite groups and $\mathscr{E}$ a certain subset. If $T(x)$ (resp. $G(x)$) denotes the number of groups $H \in \mathscr{E}$ (resp. $H \in \mathscr{G}$) whose orders are $\leqslant x$, we define the density of $\mathscr{E}$, denoted $\delta(\mathscr{E})$, as

$$\delta(\mathscr{E}) = \lim_{x \to \infty} T(x)/G(x), \tag{1.1}$$

provided this limit exists. Then (1.1) represents, in a natural way, the probability that a randomly selected finite group lies in $\mathscr{E}$. For example, if $\mathscr{E}$ consists of all isomorphism classes of finite abelian groups, then we shall see in a simple way that $\delta(\mathscr{E}) = 0$. If $\mathscr{E}$ consists of isomorphism classes of groups of squarefree order, then Mays [8] showed that $\delta(\mathscr{E}) = 0$. The calculation of δ requires good upper and lower bounds for $T(x)$ and $G(x)$ and this makes computations in a given specific case difficult. It seems reasonable to conjecture that if $\mathscr{E}$ consists of all isomorphism classes of finite simple groups then $\delta(\mathscr{E}) = 0$.

0022-314X/83 $3.00

If we confine our attention to the distribution of orders of groups in $\mathscr{F}$, we are led to consider the number $F_{\mathscr{F}}(x)$ of $n \leqslant x$ such that all groups of order n lie in $\mathscr{F}$. If we set $g(n)$ to be the number of non-isomorphic groups of order n and for fixed positive integer k,

$$\mathscr{F} = \mathscr{E}_k = \{H: \text{card}(H) = n \text{ and } g(n) = k\}$$

then $F_{\mathscr{F}}(x)/k$ is just the number of $n \leqslant x$ such that $g(n) = k$. For $k = 1$, Erdös [3] showed that

$$F_{\mathscr{F}}(x) = (1 + o(1))\, xe^{-\gamma}/\log_3 x,$$

where γ is Euler's constant and we write $\log_1 x = \log x$, $\log_a x = \log(\log_{a-1} x)$. If k is any positive integer, we shall show below that for $\mathscr{F} = \mathscr{E}_k$,

$$F_{\mathscr{F}}(x) \ll x/\log_4 x.$$

Hence $\delta(\mathscr{E}_k) = 0$.

Let $\mathscr{F}$ be any one of the following subsets of $\mathscr{G}$: the isomorphism classes of all finite cyclic groups (C), abelian groups (A), nilpotent groups (N), supersolvable groups (SS), and solvable groups (S). Then, we shall derive an asymptotic formula for $F_{\mathscr{F}}(x)$. In case that $\mathscr{F}$ is C, the result was obtained by Erdös. If $\mathscr{F}$ is A or N, this result was also obtained by Mays [9], who used a general result of Scourfield. One can derive this result in a simple way without recourse to any general result. In the case $\mathscr{F}$ is SS or S, Mays [9] obtained upper and lower bounds for $F_{\mathscr{F}}(x)$. By using a lemma of Erdös on primitive sequences, we are able to give an asymptotic formula in these cases also.

Unless otherwise specified, all groups in this paper are assumed to be finite. Also, we shall refer to a group and its isomorphism class interchangeably.

2. Scarcity of Abelian Groups

If $\mathscr{A}$ is the set of all isomorphism classes of abelian groups then we shall show $\delta(\mathscr{A}) = 0$. This is easily deduced from the following.

THEOREM 2.1. *For each fixed* $\varepsilon > 0$,

$$g(n) \geqslant (1 - \varepsilon) \log_4 n, \tag{2.1}$$

with the possible exception of at most $o(x)$ *of the* $n \leqslant x$.

Remark. It is highly unlikely that (2.2) reflects the true order of $g(n)$. It is expected that $\log g(n) \ll (\log n)^3$, but this has not been proved. (See also the concluding remarks.)

Our proof of the theorem will require the following lemmas, which seem to be of some independent interest.

LEMMA 2.3. *Let $r(n)$ denote the number of prime pairs (p, q) such that $pq \mid n$ and $q \equiv 1 \pmod{p}$. Then $g(n) \geqslant r(n)$.*

Proof. For any pair (p, q) enumerated by $r(n)$, we can form the group $H(pq) \oplus C(n/pq)$, where $C(a)$ is the cyclic group of order a and $H(pq) = \langle x, y: x^p = y^q = 1, x^{-1}yx = y^s \rangle$ with $s^p \equiv 1 \pmod{q}$, $s \neq 1$, is a non-abelian group of order pq. As it is clear that these groups are non-isomorphic for distinct pairs (p, q), the lemma is proved.

LEMMA 2.4. *Let $f(x)$ be any function satisfying $1 < f(x) \leqslant x$, f increasing and unbounded as $x \to \infty$. Define $v_t(n)$ to be the number of distinct prime factors of n that are less than t and let $\varepsilon > 0$. Then, with the possible exception of $x/(\varepsilon^2 \log_2 f(x))$ of the $n \leqslant x$, we have*

$$(1 - \varepsilon) \log_2 f(x) \leqslant v_{f(x)}(n) \leqslant (1 + \varepsilon) \log_2 f(x).$$

Proof. We shall follow the method of Turán [13]. Using well-known estimates, and writing f for $f(x)$ we have

$$\sum_{n \leqslant x} v_f(n) = \sum_{p < f} \left[\frac{x}{p} \right] = x \log_2 f(x) + O(x)$$

and

$$\begin{aligned} \sum_{n \leqslant x} v_f^2(n) &= \sum_{}{}' \left[\frac{x}{pq} \right] + \sum_{p < f} \left[\frac{x}{p} \right] \\ &= x(\log_2 f(x))^2 + O(x \log_2 f(x)), \end{aligned}$$

where square brackets denote the greatest integer function, p, q denote primes and the sum $\sum'$ is over $p, q < f$, $p \neq q$. Hence we find

$$\sum_{n \leqslant x} (v_f(n) - \log_2 f(x))^2 \ll x \log_2 f(x).$$

Thus the number of $n \leqslant x$ for which

$$|v_f(n) - \log_2 f(x)| > \varepsilon \log_2 f(x)$$

is $\ll x/(\varepsilon^2 \log_2 f(x))$, as desired.

LEMMA 2.5. *Let* $p < (\log_2 x)^a$ *for some fixed* $0 < a < 1$. *Then, the number of* $n \leqslant x$, $n \equiv 0(p)$ *and having no prime divisor* $\equiv 1 (\mathrm{mod}\, p)$ *is* $O(x/(\log_2 x)^A)$ *for any* $A > 0$. *Here, the implied constant depends only on* A.

This is essentially what Erdös proves in [3, p. 77].

We can now prove our theorem.

Proof of Theorem 2.1. We shall show that

$$r(n) \geqslant (1 - \varepsilon) \log_4 n \tag{2.2}$$

with at most $\ll x/\log_4 x$ exceptional $n \leqslant x$. This will, by Lemma 2.3, give the desired result.

Fix $0 < a < 1$, and for each x, consider the primes $p \leqslant (\log_2 x)^{1-a}$. By Lemma 2.5, we see that for each of these primes, the number of integers $n \leqslant x$, $n \equiv 0(p)$ and which have no prime factor $\equiv 1 (\mathrm{mod}\, p)$ is $o(x/(\log_2 x)^2)$. Hence, with the exception of $o(x/(\log_2 x)^2)(\log_2 x)^{1-a} = o(x/\log_2 x)$ values of $n \leqslant x$, $\phi(n)$ is divisible by each of the prime divisors p of n, $p \leqslant (\log_2 x)^{1-a}$. Here, $\phi(n)$ denotes Euler's totient function. Taking $f(x)$ to be $(\log_2 x)^{1-a}$ in Lemma 2.4, we conclude that

$$r(n) \geqslant v_f(n) \geqslant (1 - \varepsilon) \log_4 x$$

with at most $O(x/\log_4 x)$ exceptional $n \leqslant x$. This proves the theorem.

COROLLARY. $\delta(\mathscr{A}) = 0$.

Proof. Let $A(x)$ denote the number of abelian groups of orders $\leqslant x$. By a result of Erdös and Szekeres [6], we have $A(x) \ll x$, so that by an easy calculation

$$A(x)/G(x) \ll 1/\log_4 x = o(1)$$

as desired.

3. SOME ASMPTOTIC FORMULAE

We begin with the following theorems.

THEOREM 3.1. *As* $x \to \infty$,

$$F_C(x) \sim F_A(x) \sim F_N(x) \sim xe^{-\gamma}/\log_3 x.$$

Proof. For $F_C(x)$, the result was proved by Erdös [3], since a classical result of Burnside implies that a necessary and sufficient condition for an n

to be included is that $(n, \phi(n)) = 1$. As $C \subseteq A \subseteq N$, it is enough now to prove that $F_N(x)$ is asymptotically majorized by $xe^{-\gamma}/\log_3 x$. Our argument closely follows that of Erdös. Fix $\varepsilon > 0$, and let $y = (\log_2 x)^{1-\varepsilon}$. We split the set $S(x)$ of the $n \leqslant x$ under consideration into two classes $S_1(x)$ and $S_2(x)$ depending on the size of their least prime divisor p. Specifically, $n \in S_1(x)$ if $p < y$ and $n \in S_2(x)$ if $p \geqslant y$. An upper bound for the cardinality of $S_2(x)$ is the number of $n \leqslant x$ having no prime divisor less than y. By the sieve of Eratosthenes and Merten's theorem, this number is equal to

$$x \prod_{p \leqslant y} \left(1 - \frac{1}{p}\right) + O(2^y) = (1 + o(1))\, xe^{-\gamma}/(1 - \varepsilon) \log_3 x.$$

Now consider those n in $S_1(x)$. If all groups of order n are nilpotent, and m is the squarefree core of n, it is clear that $(m, \phi(m)) = 1$. Hence, an upper bound for the number of such n is the number of $n \leqslant x$ which are divisible by p and have no prime factor $\equiv 1 \pmod p$. By Lemma 2.5, this is $o(x/(\log_2 x)^2) \cdot (y) = o(x/\log_3 x)$. Now we let ε tend to 0 to complete the proof.

THEOREM 3.2. *There is a constant $c_1 \geqslant 6/\pi^2$ such that*

$$F_{SS}(x) \sim c_1 x.$$

Our proof will depend on the following arithmetical lemmas.

LEMMA 3.3. *Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ with $p_1 < p_2 < p_3 \ldots$. All groups of order n are supersolvable iff for p, q, r distinct prime divisors of n,*

(1) $p^d \mid (q^t - 1)$, $t \leqslant \alpha_q$, $d \leqslant \alpha_p$ *implies* $p^d \mid (q - 1)$;

(2) $p^3 \mid (q - 1)$ *implies* $\alpha_q < p$;

(3) $p < q < r$, $p \mid (q - 1)$, $pq \mid (r - 1)$ *implies* $\alpha_r < p$.

See Hughes [7].

Remark. The analogues of this condition for abelian groups and nilpotent groups were found by Dickson and Bachman (see [1]), respectively, and for solvable groups it was discovered by Thompson [12].

The next lemma is a special case of a well-known result of Erdös [4] which gives a criterion for a sequence of integers to have a density. A sequence of integers is called primitive if no element divides any other.

LEMMA 3.4. *Let $m_1 < m_2 < \cdots$ be any primitive sequence of integers and let $b_1 < b_2 < \cdots$ be the sequence composed of those integers which are divisible by at least one m_i. If the number of $m_i \leqslant x$ is $O(x/\log x)$ then the sequence of b's has a density.*

Proof of Theorem 3.2. If we show that the sequence of integers n such that all groups of order n are supersolvable, has a density c_1, it will follow that $c_1 \geqslant 6/\pi^2$ as it is easily seen from Lemma 3.3 that the groups of squarefree order are supersolvable. Actually, we will show that the complementary sequence has a density. To do this, we begin by extracting a maximal primitive subsequence, say $m_1 < m_2 < \cdots$ of the complementary sequence. Clearly, the sequence $b_1 < b_2 < \cdots$ composed of integers divisible by an m_i is precisely the complementary sequence. For by maximality, every element of the complement is divisible by an m_i and Lemma 3.3 shows that any multiple of an m_i must be in the complement as m_i itself is. Let $h(x)$ be the number of $m_i \leqslant x$. If we can show $h(x) = O(x/\log x)$, then Lemma 3.4 will give the desired result.

Suppose m is one of the m_i and q is the largest prime divisor of m. Then, all groups of order m/q are supersolvable. Indeed, if this were not the case, m/q would be in the complementary sequence. Then for some j, we would have $m_j \mid m/q$ and so also $m_j \mid m$, which is a contradiction.

We claim that this implies:

$$\text{either } q^2 \mid m \text{ or } q \mid (p-1)(p^2-1)\cdots(p^a-1) \text{ for some } p^a \mid m. \qquad (*)$$

Suppose $q^2 \nmid m$. By the above remark, m/q satisfies conditions (1), (2), (3) of Lemma 3.3, but m fails to do so. But $\alpha_q = 1$ implies that it satisfies both (2) and (3), and the only way (1) can fail to hold is if $q \mid (p^s - 1)$ for some $s \leqslant \alpha_p$. This proves $(*)$.

Denote by $j(x)$ the number of integers $m \leqslant x$ having property $(*)$, where q is the largest prime divisor of m. Then $h(x) \leqslant j(x)$. Write $j(x) = j_1(x) + j_2(x)$, where $j_1(x)$ is the number of integers $m \leqslant x$ satisfying $(*)$ and having $q > (\log x)^2$.

We can estimate $j_1(x)$ directly as follows:

$$\begin{aligned} j_1(x) &\ll \sum_{q > (\log x)^2} \sum_{t \leqslant x} \frac{x}{q(tq+1)} \\ &\ll x \log x \sum_{q > (\log x)^2} q^{-2} \ll x/\log x. \end{aligned}$$

To estimate $j_2(x)$, we use a method of Rankin [11]. A prime in the summation indicates that the range is only over those n all of whose prime factors are $\leqslant y = (\log x)^2$. Then,

$$\begin{aligned} j_2(x) &\leqslant \sum_{n \leqslant x}{}' 1 \leqslant \sum_{n \leqslant x}{}' \left(\frac{x}{n}\right)^{1/2} \leqslant x^{1/2} \prod_{p \leqslant y} (1 - p^{-1/2})^{-1} \\ &= x^{1/2} \prod_{p \leqslant y} \left(1 + \frac{1}{p^{1/2} - 1}\right) \end{aligned}$$

$$\leqslant \exp\left(\tfrac{1}{2}\log x + \sum_{p\leqslant y}\frac{1}{p^{1/2}-1}\right)$$

$$\ll \exp(\tfrac{1}{2}\log x + 2y^{1/2}/\log y) \leqslant x^{1/2+\delta},$$

where $\delta = (\log\log x)^{-1}$. In the penultimate step, we used the prime number theorem. Hence $h(x) \leqslant j(x) = j_1(x) + j_2(x) \ll (x/\log x)$.

Our final result in this section concerns solvable groups.

THEOREM 3.5. *There is a constant c_2 such that $F_S(x) \sim c_2 x$.*

Proof. Thompson [12] has shown the deep result that every minimal simple group is isomorphic to one of the following:

(a) $L_2(2^p)$, p any prime,

(b) $L_2(3^p)$, p any prime,

(c) $L_2(p)$, p any prime >3, such that $p^2 + 1 \equiv 0 \pmod 5$,

(d) $Sz(2^p)$, p any odd prime,

(e) $L_3(3)$

(see [12] for notation). Let Z be the ascending sequence of orders of the above types of groups. Then, all groups of order m are solvable if and only if no $s \in Z$ divides m. Necessity is trivial to see and conversely, if G is a group of order m where no $s \in Z$ divides m, then G is not simple, say $H \lhd G$. By induction, H and G/H are solvable so it follows that G is solvable.

The number of $s \leqslant x$, $s \in Z$ is obviously $O(x/\log x)$ as each order corresponds to a prime and each prime gives rise to at most four orders. But now, the method of the previous theorem and Lemma 3.4 complete the proof.

The value of c_2 above is, in fact, quite close to 1, though it is clear that it must be less than 1. The above reasoning shows that

$$c_2 \geqslant \prod_{s\in Z'}\left(1-\frac{1}{s}\right),$$

where Z' is a maximal primitive subsequence of Z.

4. CONCLUSION

If $\mathscr{F}$ consists of all isomorphism classes of finite simple groups, we have already conjectured that $\delta(\mathscr{F}) = 0$. Erdös [5] has shown that the number of $n \leqslant x$ such that there is a non-abelian simple group of order n is $o(x/\log x)$. (See also Dornhoff [2].) Hence, if we let $s(n)$ be the number of simple groups of order n, and conjecture $s(n) = O(\log n)$, then it follows that

$\delta(\mathcal{F}) = 0$. But Neuman [10] has pointed out that even a much weaker form of such a conjecture already implies that $\log g(n) = O(\log n)^3$. Of course, the recent (presumed) classification of finite simple groups settles all these conjectures. In fact, it implies that $s(n) = O(1)$.

ACKNOWLEDGMENTS

The results of this paper were presented at the 6th British Combinatorics Conference at Royal Holloway College in June 1977. We would like to thank Professors J. D. Dixon, F. Fiala and L. D. Nel for their support, which made it possible to attend that conference. We also thank Professor Dixon for his comments on a preliminary version of this paper.

REFERENCES

1. G. BACHMAN, On finite nilpotent groups, *Canad. J. Math.* **12** (1960), 68–72. See also L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905), 198–204.
2. L. DORNHOFF, Simple groups are scarce, *Proc. Amer. Math. Soc.* **19** (1968), 692–696.
3. P. ERDÖS, Some asymptotic formulas in number theory, *J. Indian Math. Soc.* **12** (1948), 75–78.
4. P. ERDÖS, On the density of some sequences of integers, *Bull. Amer. Math. Soc.* **54** (1948), 685–692.
5. P. ERDÖS, The scarcity of simple groups, to appear.
6. P. ERDÖS AND G. SZEKERES, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandte zahlentheoretisches Problem, *Acta Litt. Sci. Reg. Univ. Hungar. Fr. Jos. Sect. Sci. Math.* **7** (1934), 94–103.
7. A. HUGHES, On supersolvable orders, to appear.
8. M. E. MAYS, Groups of squarefree order are scarce, *Pacific J. Math.* **91** (1980), 373–375.
9. M. E. MAYS, Counting abelian, nilpotent, solvable, and supersolvable groups, *Arch. Math.* **31** (1978), 536–538.
10. P. NEUMAN, An enumeration theorem for finite groups, *Quart. J. Math. Oxford* **20** (1969), 395 – 401.
11. R. A. RANKIN, The difference between consecutive prime numbers, *J. London Math. Soc.* **13** (1938), 242–247.
12. J. THOMPSON, Non-solvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
13. P. TURÁN, On a theorem of Hardy–Ramanujan, *J. London Math. Soc.* **9** (1934), 284–286.