JOURNAL OF NUMBER THEORY 28, 363–368 (1988)

On Nilpotent but Not Abelian Groups and Abelian but Not Cyclic Groups

PAUL ERDÖS

Mathematical Institute, Hungarian Academy of Sciences, Budapest H-1364, Hungary

AND

MICHAEL E. MAYS

Department of Mathematics, West Virginia University, Morgantown, West Virginia 26506

Received June 19, 1987

We derive asymptotic formulas for $A(n)-C(n)=|\{m<n$: every group of order m is abelian but not every group of order m is cyclic$\}|$, $N(n)-A(n)=|\{m<n$: every group of order m is nilpotent but not every group of order m is abelian$\}|$, and related counting functions from group theory.

There is only one group of order p, p a prime, up to isomorphism. This is equivalent to saying that every group of prime order is cyclic. A necessary and sufficient condition that there be only one group of order n is that $(n, \phi(n))=1$, where $\phi(n)$ is the totient function of Euler. $(n, \phi(n))=1$ iff n is squarefree and no two prime factors p and q of n have $p \equiv 1 \pmod{q}$.

Erdös [1] found an asymptotic formula for the counting function

$$\begin{aligned} C(n) &= |\{m \leqslant n\text{: there is only one group of order } m\}| \\ &= |\{m \leqslant n\text{: every group of order } m \text{ is cyclic}\}| \\ &= |\{m \leqslant n\text{: } (m, \phi(m))=1\}|, \end{aligned}$$

given by

$$C(n)=(1+o(1))\frac{ne^{-\gamma}}{\log\log\log n}, \tag{1}$$

where γ is Euler's constant.

Pazderski [8] studied the function $\psi(n)$ defined by extending mul-

641/28/3-9

0022-314X/88 $3.00

tiplicatively the recursion for prime powers $\psi(p^s) = (p^s - 1)\psi(p^{s-1})$, $\psi(1) = 1$. He gave several theorems of the form

> Every group of order n has property P if and only if n has property P' and $\psi(n)$ has property P''.

For example, since $\psi(n) = \phi(n)$ iff n is squarefree, we have that every group of order n is cyclic iff $(n, \psi(n)) = 1$ and n is squarefree. Two analogous results from [8] are that every group of order n is abelian iff $(n, \psi(n)) = 1$ and n is cubefree, and every group of order n is nilpotent iff $(n, \psi(n)) = 1$.

Mays [4] used these results to find asymptotic formulas for $A(n) = |\{m \leqslant n$: every group of order m is abelian$\}|$ and $N(n) = |\{m \leqslant n$: every group of order m is nilpotent$\}|$. It happens that the "same" formula

$$(1 + o(1))\frac{ne^{-\gamma}}{\log\log\log n}$$

is an appropriate measure of the rate of growth for all three counting functions $C(n)$, $A(n)$, and $N(n)$. This turns out to be a special case of a result of Scourfield [11], who established that an asymptotic formula similar to this is valid if any function which is "polynomial like" is used in place of $\psi(n)$.

On the other hand, $C(n) \leqslant A(n) \leqslant N(n)$ from first principles, so it is reasonable to expect that some finer information has gotten lost in the $o(1)$ term. This paper estimates the differences $A(n) - C(n)$ and $N(n) - A(n)$.

Throughout we will use some standard estimates for functions of prime numbers. It will be convenient to use a generic constant c in our series of estimates rather than to keep track of new constants introduced in every step. In all cases the constant c is independent of n.

If p and q are primes, it follows from Remark 1 in [9] that

$$\sum_{\substack{p < n \\ p \equiv 1 \pmod q}} 1/p = (\log\log n)/(q-1) + O(\log q/q).$$

In particular, if $q \leqslant (\log n)^{o(1)}$, then

$$\sum_{\substack{p < n \\ p \equiv 1 \pmod q}} 1/p = (1 + o(1))(\log\log n)/(q-1). \tag{2}$$

We will also need the following well-known lemma from sieve theory: Let $q_1 < q_2 < \cdots < x$ be a sequence of primes such that $\sum_{x^\varepsilon < q_i < x} 1/q_i \to 0$

for every $\varepsilon > 0$. Then the number of integers $n < x$ for which $n \not\equiv 0 \pmod{q_i}$ is

$$(1 + o(1)) \times \prod_{q_i < x} (1 - 1/q_i). \tag{3}$$

Note that the hypothesis is satisfied for the primes $r \equiv 1 \pmod{p}$, if $p \to \infty$.

Two useful sums over primes are

$$\sum_{p > t} 1/p^2 = (1 + o(1))\, 1/(t \log t), \tag{4}$$

and

$$\sum_{p > t} 1/p^3 = (\tfrac{1}{2} + o(1))\, 1/(t^2 \log t). \tag{5}$$

These follows from the prime number theorem using summation by parts or a formula relating the density of primes in the neighborhood of y to $1/\log y$.

A useful bound for a special product of the form (3) is

$$\prod_{p < n} (1 - 1/p) = (1 + o(1))\, e^{-\gamma}/\log n. \tag{6}$$

To sieve by primes in an arithmetic progression we can use (2) to write

$$\prod_{\substack{p \equiv 1 \pmod{q} \\ p < n}} (1 - 1/p) = (1 + O(\log q/q))/(\log n)^{1/(q-1)}. \tag{7}$$

A good reference for sieving argument results is Halberstam and Richert [3], and for the other estimates involving prime numbers Prachar [10], Estermann [2], or Norton [7].

THEOREM 1. *There exists a constant c such that*

$$A(n) - C(n) = (1 + o(1)) \frac{cn}{\log \log n (\log \log \log n)^2}.$$

Proof. The most general $m < n$ counted by $A(n) - C(n)$ has the prime factorization $p_1^2 p_2^2 \cdots p_r^2 q_1 q_2 \cdots q_s$, where no p_i is a q_j, $r \geqslant 1$, $p_1 < p_2 < \cdots p_r$, $q_1 < q_2 < \cdots < q_s$, and no unitary congruences $p_i \equiv \pm 1 \pmod{p_j}$, $p_i \equiv \pm 1 \pmod{q_j}$, $q_i \equiv 1 \pmod{p_j}$, or $q_i \equiv 1 \pmod{q_j}$ hold among the prime divisors of m.

However, we may without loss of generality assume that the form of m is more restricted. Suppose first that m has a prime factor $p < \log\log n/(\log\log\log n)^2$. Then all other prime factors q of m must satisfy $q \not\equiv 1 \pmod p$, and so of the numbers less than n at most $n\prod_{r\equiv 1 \pmod p,\, r<n}(1-1/r)$ are eligible. But by (7) this product is no bigger than

$$(1+O(\log p/p))/(\log n)^{1/(p-1)} < ce^{(\log\log n)^2}.$$

which is small enough to be ignored as n becomes large. Thus we may assume that all prime factors or m are bigger than $\log\log n/(\log\log\log n)^2$. Furthermore, if there are two or more prime factors occurring in the square-full part of m, say p_1 and p_2, then the total number of multiples of m eligible is no more than $n/(p_1^2 p_2^2)$, and the set of all such numbers is no larger than

$$n\sum_{p_1,p_2} 1/p_1^2 p_2^2 \leqslant n\sum_{p_1} 1/p_1^2 \sum_{p_2} 1/p_2^2,$$

where the sum over p_1 is for $p_1 > (\log\log n)/(\log\log\log n)^2$ and the sum over p_2 is $p_1 > p_2 > (\log\log n)/(\log\log\log n)^2$. By (4) this is of smaller order of magnitude than the bound claimed in the theorem. Thus m has a unique squared prime factor p. Also inconsequential by (4) are square prime factors larger than $(\log\log n)(\log\log\log n)^2$ because there are not enough multiples of such numbers less than n.

Now fix p and consider how many eligible $m < n$ are counted with square factor p^2. Write $t = n/p^2$. By (1), of the t multiples up^2 of p^2 less than n, $(1+o(1))\,e^{-\gamma}t/\log\log\log n$ have $(u, \phi(u)) = 1$ and hence have no unitary congruences among the q_i. To ensure that $q_i \not\equiv 1 \pmod p$ we rule these primes out with the sieving factor

$$\prod_{\substack{r\equiv 1 \pmod p \\ r<n}} (1-1/r) = (1+O(\log p/p))/(\log n)^{1/(p-1)}.$$

Now we sum over p and use the lemma to get

$$(1+o(1))\,e^{-\gamma}n/\log\log\log n \sum_p 1/p^2(\log n)^{1/(p-1)},$$

where the summation extends over all primes p between $(\log\log n)/(\log\log\log n)^2$ and $(\log\log n)(\log\log\log n)^2$. The proof is complete upon noting that by a partial summation formula similar to (4) the summation is

$$(1+o(1))\,c/(\log\log n\log\log\log n).$$

THEOREM 2. *There exists a constant c such that*

$$N(n) - A(n) = (1 + o(1)) \frac{cn}{(\log \log n)^2 (\log \log \log n)^2}.$$

Proof. We use the same technique here as was used in the proof of Theorem 1. We need to estimate

$$|\{m < n: m \text{ is not square-free and } (m, \psi(m)) = 1\}|.$$

The most general such m have prime factors with arbitrary exponents, with at least one prime factor occurring to at least the third power. However, we can successively restrict m to guarantee

(i) all prime factors of m are $> \log \log n/(\log \log \log n)^2$,

(ii) no prime factor occurs to a power higher than the third,

(iii) exactly one prime factor p occurs with exponent three,

(iv) $p < (\log \log n)(\log \log \log n)^2$, and

(v) m/p^3 is square-free.

This is done by noting in each case that the asymptotic size of the set of $m < n$ discarded as failing to meet the condition is smaller than the asymptotic value claimed for $N(n) - A(n)$ in the theorem.

Now fix the prime p occurring with exponent three and write $t = n/p^3$. There are t multiples up^3 of p^3 less than n, and the relevant multiples for our theorem satisfy $(u, \phi(u)) = 1$ and $q \not\equiv 1 \pmod{p}$ for any $q|u$. When factors for these conditions are included and we sum over p, the expression to evaluate is the same as in Theorem 1 except for a factor of p^3 replacing p^2 in the denominator.

With Carl Pomerance, we observe that several other results of [8] can be used to establish asymptotic limits for counting functions associated with finite groups. In particular, the method of this paper applied to the characterization of supersolvable groups in Pazderski's Satz 3 gives that there exists a constant c with $1 > c > 6/\pi^2$ such that

$$\begin{aligned} U(n) &= |\{m < n: \text{every group of order } m \text{ is supersolvable}\}| \\ &= (1 + o(1))\, cn. \end{aligned}$$

Murty and Murty [6] use a result of Hughes to draw the same conclusion about the existence of a "constant of supersolvability."

Satz 4 and Satz 5 of [8] similarly can be used to establish the existence of constants c, $1 > c > 6/\pi^2$, for groups with cyclic commutator subgroups and metacyclic groups. The characterization of integers n for which every

group of order n is p-nilpotent implies the existence of a constant c greater than $(p-1)/p$ but less than 1 for which

$$N_p(n) = |\{m < n: \text{every group of order } m \text{ is } p\text{-nilpotent}\}|$$

satisfies

$$N_p(n) = (1 + o(1))\, cn.$$

This statement of the p-nilpotence density result corrects a result of Mays [5], the error of which was pointed out by Pomerance. In all of these cases, the technique is to start with a set of integers of positive density for which the number theoretic condition is vacuously satisfied (square-free numbers for $U(n)$ and the two generalized commutativity conditions, and numbers not divisible by p for p-nilpotent groups), and augment that set with sets built by sieving to ensure that forbidden congruences among the prime factors of the remaining number do not occur.

REFERENCES

1. P. ERDÖS, Some asymptotic formulas in number theory, *J. Indian Math. Soc.* **12** (1948), 75–78.
2. T. ESTERMANN, "Introduction to Modern Prime Number Theory," Cambridge Tracts in Math. and Math. Physics, Vol. 41 (1952).
3. H. HALBERSTAM AND H.-E. RICHERT, "Sieve Methods," Academic Press, London/New York, 1974.
4. M. E. MAYS, Counting Abelian, nilpotent, and supersolvable group orders, *Arch. Math.* **31** (1978), 536–538.
5. M. E. MAYS, Counting p-nilpotent group orders, *Proc. West Virginia Acad. Sci.* **50** (1978), 92–94.
6. M. RAM MURTY AND V. KUMAR MURTY, On the density of various classes of groups, *J. Number Theory* **17** (1983), 29–36.
7. K. K. NORTON, On the number of restricted prime factors of an integer, I, *Illinois J. Math.* **20** (1976), 681–705.
8. G. PAZDERSKI, Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören, *Arch. Math.* **10** (1959), 331–343.
9. C. POMERANCE, On the distribution of amicable numbers, *J. Reine Angew. Math.* **293/294** (1977), 217–222.
10. K. PRACHAR, "Primzahlverteilung," Springer, Berlin/Gottingen/Heidelberg, 1957.
11. E. J. SCOURFIELD, An asymptotic formula for the property $(n, f(n)) = 1$ for a class of multiplicative functions, *Acta Arithmetica* **29** (1976), 401–423.