Counting Supersolvable and Solvable Group Orders

Edward Bertram* and Guanhong Li

Abstract. For more than 100 years, group and number theorists have been interested in quesitons such as: (a) If a group G has order $|G| = \prod p_i^{\alpha_i}$ (p_i distinct primes), what conditions on the primes p_i and their exponents α_i ensure that G is cyclic, or G is abelian, or G is nilpotent, or supersolvable, or solvable? (b) How fast does $g(n) = |\{m \leq n \mid$ *every* group G of order m has one of these properties$\}|$ grow as a function of n? Questions (a) and (b) have been answered when the property is either cyclic, abelian, or nilpotent. But when the property is supersolvable or solvable, only question (a) has been fully answered. We greatly increase the current lower bounds for $g(n)$ when the property is supersolvable or solvable. In the latter case our lower bound is just below the best upper bound known.

1 Introduction

All groups here are finite. A group G is *cyclic* if there is an element $g \in G$ such that every element of G may be expressed as a power g^m of g (where m is an integer). A group G is *abelian* if for every pair $a, b \in G$, $ab = ba$. A sequence $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ of normal subgroups of G is a *central series* for G if for $1 \leq i \leq r$ we have $N_i/N_{i-1} \leq Z(G/N_{i-1})$, the center of G/N_{i-1}. A group is *nilpotent* if it has a central series. G is nilpotent if and only if every maximal subgroup of G is normal. G is *supersolvable* if there exist normal subgroups N_i of G with $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ where each factor N_i/N_{i-1} is cyclic. G is supersolvable if and only if every maximal subgroup $M \leq G$ has prime index $[G : M]$ [Huppert, 1954]. G is *solvable* if there exist normal subgroups N_i of G with $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ where each N_i/N_{i-1} is abelian.

There is exactly one isomorphism class of groups of order n if and only if every group of order n is cyclic. [Miller, Collected Works I] was the first to discover that there is exactly one isomorphism class of groups of order n if and only if $(n, \varphi(n)) = 1$, where $\varphi(n)$ (Euler's totient function) $= |\{m \leq n \mid (m, n) = 1\}| = n \prod_{\text{primes } p \mid n} \left(1 - \frac{1}{p}\right)$. Thus for example every group of order 15 is cyclic. If we set

$$C(n) = |\{m \leq n \mid \text{every group of order } m \text{ is cyclic}\}|$$

then $C(n) = |\{m \leq n \mid m \text{ is square free and no two prime factors } p, q \text{ of } m \text{ satisfy } p \equiv 1 \pmod{q}\}|$.

Similarly, [Dickson, 1905] a group of order $n = \prod p_i^{\alpha_i}$ (p_i distinct primes) is abelian if and only if (i) each $\alpha_i \leq 2$ and (ii) $(p_i, p_j^{\alpha_j} - 1) = 1$ for every i, j. Thus for example, every group of order 45 is abelian. If we set

$$A(n) = |\{m \leq n \mid \text{every group of order } m \text{ is abelian}\}|$$

then $A(n) = |\{m \leq n \mid m = \prod p_i^{\alpha_i} \text{ where each } \alpha_i \leq 2 \text{ and } (p_i, p_j^{\alpha_j} - 1) = 1 \text{ for every } i, j\}|$.

Also [Bachman, 1960] proved that a group of order $n = \prod p_i^{\alpha_i}$ is nilpotent if and only if for every i, j, $(p_i, \prod_{\lambda=1}^{\alpha_j}(p_j^{\lambda} - 1)) = 1$. Thus for example every group of order $135 = 3^3 \cdot 5$ is nilpotent. If we set

$$N(n) = |\{m \leq n \mid \text{every group of order } m \text{ is nilpotent}\}|$$

then $N(n) = |\{m \leq n \mid m = \prod p_i^{\alpha_i} \text{ and for every } i, j, (p_i, \prod_{\lambda=1}^{\alpha_j}(p_j^{\lambda} - 1)) = 1\}|$.

Finally, let $\psi(p^k)$ be the *multiplicative* function defined on prime powers by $\psi(p^k) = (p^k - 1)(p^{k-1} - 1) \ldots (p - 1)$. Then in [Pazderski, 1959, pg. 335] we find a proof that a group of order $n = \prod_{i=1}^{t} p_i^{\alpha_i}$ $(p_1 < p_2 < \cdots < p_t)$ is supersolvable if and only if:

(1) For all $1 \leq i \leq t$, the distinct prime factors of $(n, \psi(p_i^{\alpha_i}))$ are the same as those of $(n, p_i - 1)$.

(2) If there exists $i \neq k$ such that $p_i \leq \alpha_k$ (i.e. some prime factor of n is less than or equal to the multiplicity of another prime factor of n) then

   (a) There does not exist a prime p_j such that $p_i \mid (p_j - 1)$ and $p_j \mid (p_k - 1)$, and

   (b) $\alpha_i \leq 2$, and if $\alpha_i = 2$ then $p_i^2 \mid (p_k - 1)$. Thus for example every group of order 54 is supersolvable. If we set

$$U(n) = |\{m \leq n \mid \text{every group of order } m \text{ is supersolvable}\}|$$

then $U(n) = |\{m \leq n \mid m = \prod_{i=1}^{t} p_i^{\alpha_i}$ $(p_1 < p_2 < \cdots < p_t)$ and m (replacing n) satisfies (1) and (2)(a),(b) above$\}|$. Finally, set

$$S(n) = |\{m \leq n \mid \text{every group of order } m \text{ is solvable}\}|$$

and note that $C(n) \leq A(n) \leq N(n) \leq U(n) \leq S(n)$.

In [Pakianathan and Shankar, 2000], we find criteria based on J. Thompson's deep result [Thompson, 1968] on minimal simple groups, for the positive integer m to be a *solvable group order*, that is every group of order m is solvable: m is a solvable group order if and only if m is not a multiple of any of (i) $2^p(2^p-1)$, p a prime (ii) $3^p(3^{2p}-1)/2$, p an odd prime (iii) $p(p^2-1)/2$, p a prime > 3 and $p \equiv 2$ or $3 \pmod 5$ (iv) $2^4 3^3 13$ (v) $2^{2p}(2^{2p}+1)(2^{2p}-1)$, p an odd prime. The On-line Encyclopedia of Integer Sequences (OEIS) has a list of many such m (A056866).

[Erdös, 1948] found the asymptotic behavior of $C(n) = \sum_{\substack{m \le n \\ (m,\varphi(m))=1}} 1$, proving that $C(n) = (1+o(1))\frac{ne^{-\gamma}}{\log\log\log n}$ where $\gamma = 0.57721\ldots$ is Euler's constant. [Mays, 1978] proved that $A(n)$ and $N(n)$ also $= (1+o(1))\frac{ne^{-\gamma}}{\log\log\log n}$, so $C(n)$, $A(n)$ and $N(n)$ each grow more slowly than n. Using an old result of Burnside, and the Feit-Thompson Theorem that every non-abelian finite simple group has even order, [Mays, 1978] proved that $S(n) > 0.869n$ for $n > N_0$.

Using Pazderski's criteria, we check that every group of square-free order $n = \prod p_i$ (distinct primes) is supersolvable. ζ is the Riemann Zeta function and $\zeta(2) = \sum_{k=1}^{\infty} 1/k^2 = \pi^2/6$. Since [Montgomery, 1981] the number of square-free integers $\le n$ is equal to $\frac{n}{\zeta(2)} + O(\sqrt{n}) > \left(\frac{6}{\pi^2}\right) n > 0.6079n$, we know that $U(n) > 0.6079n$.

[Y. D. Zhang and Fan Young, 1981] reformulated Pazderski's criteria and gave a different proof that their criteria characterize those integers n for which every group of order n is supersolvable: A group of order n is supersolvable if and only if $n = \prod_{i=1}^{r} p_i^{\lambda_i}$ $(p_1 < p_2 < \cdots < p_r)$ and

(i) For any i, j, $\left(p_i, \prod_{s=1}^{\lambda_j}(p_j^s - 1)\right) = (p_i, p_j - 1)$

(ii) When $p_i \le \lambda_j$ $(1 \le i < j \le r)$, we must have $1 \le \lambda_i \le 2$ and $p_i^{\lambda_i} \mid (p_j - 1)$, and moreover no p_k exists $(i < k < j)$ such that $p_i \mid (p_k - 1)$ and $p_k \mid (p_j - 1)$.

Finally, [A. Hughes, 1980] stated that n is a supersolvable order if and only if three criteria are satisfied:
Suppose $n = \prod_{i=1}^{s} p_i^{a_i}$, $p_1 < p_2 < \cdots < p_s$ (primes). Then n is an supersolvable order if and only if there exist p, q, r (distinct) prime divisors of n, such that

(1) If $p^d \mid (q^t - 1)$ $(t \le a_q, d \le a_p)$ then $p^d \mid (q-1)$.

(2) If $p^3 \mid n$ and $p^3 \mid (q-1)$ then $a_q < p$.

(3) If $p < q < r$, $p \mid (q-1)$ and $pq \mid (r-1)$ then $a_r < p$.

Hughes stated that his proof is "to appear", but the proof has never appeared. We decided to count the number of supersolvable orders between 2 and 10^k when $1 \le k \le 13$, using each author's criteria. As expected, the authors' counts agree and are displayed as $U(10^k)$ in the Table below for $1 \le k \le 13$. The average time it took the 3 counts for each k, is also displayed.

k	$U(10^k)$	Average Time (Rounded)
1	9	0.00064 (seconds)
2	88	0.00187 (seconds)
3	871	0.00269 (seconds)
4	8,682	0.00494 (seconds)
5	86,772	0.01354 (seconds)
6	867,683	0.08478 (seconds)
7	8,676,833	1.0221 (seconds)
8	86,768,040	17.3962 (seconds)
9	867,679,854	323.582 (seconds)
10	8,676,796,466	0.0620 (days)
11	86,767,961,313	0.8528 (days)
*12	867,679,598,773	10.061 (days)*
*13	8,676,795,952,899	133.475 (days)*

*When $k = 12$ (or 13), these are the times it would take one computer to run the program. The HPC is a cluster of computers, and 10 computers were run concurrently. For example, when $k = 12$, each computer counts in an interval of length 10". To get a closer estimate of the HPC runtime (not including queue times), divide the time by 10.

Here is the public repository for the project:

`https://github.com/guanhongl/supersolubility`

The files `ss.c`, `ss_pazderski.c`, and `ss_h.c` correspond to the three criteria.
Below these, readers will find the directions for running the program locally.

Our table of $U(n)$ reveals that $U(n) > 0.8676n$ without using the results of Burnside and Feit-Thompson.

In order to find $S(n)$, we found $NS(n) = n - S(n)$, the number of integers $m \leq n$ such that some group of order m is not solvable. For example, since some group of order 60 (namely Alt(5)) is not solvable, and $m = 60$ is the only $m \leq 10^2$ for which some group of order m is not solvable, we have $NS(10^2) = 1$. Using the criteria based on J. Thompson's result on minimal simple groups, we know that some group of order m is not solvable if and only if m is a multiple of at least one of (i), (ii), (iii), (iv) or (v) (listed earlier). For example, some group of order $1344 = 2^6 \cdot 3 \cdot 7$ is not solvable since $1344 = (24) \cdot 2^p(2^p - 1)$ where $p = 3$. Using a (2017) Lenovo Y520-151KBM desktop computer and source code written in Mathematica (modified slightly from that at OEIS AO56866), we found for $3 \leq k \leq 8$, keeping track of the time taken in seconds:

k	$NS(10^k)$	Time (Rounded)
3	20	
4	224	0.66
5	2240	7.29
6	22416	110.35
7	224132	1,872.89
8	2241423	32,924.33

Since there are $86,400$ seconds/day, it took approximately 0.38 days to find the number of $m \leq 10^8$ for which some group of order m is not solvable. We stopped at 10^8, since we estimate that it will take at least a week to find $NS(10^9)$ with not much information gained. Since $S(n) = n - NS(n)$, we have the following:

k	$S(10^k)$	$S(10^k)/10^k$
3	980	0.980
4	9776	0.9776
5	97760	0.9776
6	977584	0.977584
7	9775868	0.97758680
8	97758577	0.97758577

As noted earlier [Mays, Thm. 5, 1978] proved that for n large enough: $0.869n < S(n) < 0.978n$. We see from the above table how close to his upper bound $S(n)$ is.

References

[1] G. Bachman, On finite nilpotent groups. Canad. J. Math., 12, 68-72 (1960).

[2] L. E. Dickson, Definitions of a group and a field by independent postulates. Trans. Amer. Math. Soc., 6, 193-204 (1905).

[3] P. Erdös, Some asymptotic formulas in number theory. J. Indian Math. Soc. 12, 75-78 (1948).

[4] A. Hughes, Automorphisms of nilpotent groups and supersolvable orders. Amer. Math. Soc. Proc. Symp. Pure Math, 37, 205-207 (1980).

[5] B. Huppert, Normalteiler und maximale Untergruppen endlicher Gruppen, Math. Zeit. 60, 409-434 (1954).

[6] B. Huppert, Endliche Gruppen 1, Hauptsatz 9.5, Kapitel VI, Springer Verlag, Berlin (1967).

[7] M. E. Mays, Counting abelian, nilpotent, solvable, and supersolvable group orders. Archiv der Mathematik, 31, 536-538 (1978).

[8] G. A. Miller, Collected Works I, pg. 332. Univ. of Illinois, Urbana Ill (1935).

[9] H. L. Montgomery, R.C. Vaughan, The distribution of square-free numbers, in H. Halberstam, C. Hooley (Eds.), Recent Progress in Analytic Number Theory, Vol. 1, Academic Press, London, 1981, pp. 247-256.

[10] J. Pakianathan, K. Shankar, Nilpotent Numbers, Amer. Math. Monthly, 107, 631-634 (2000).

[11] G. Pazderski, Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören. Archiv der Mathematik, 10, 331-343 (1959).

[12] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. 74, 383-437 (1968).

[13] Y. D. Zhang, Fan Young, On supersolvablility of groups of order n. Journal of Mathematics, Vol. 1, No. 1, 86-95 (1981).

Author Information

Corresponding Author:
Edward Bertram, University of Hawaii at Manoa, Honolulu, Hawaii
Email: ed@math.hawaii.edu

Guanhong Li
B.S. Computer Science
University of Hawaii at Manoa