Math. Ann. 267, 299–309 (1984)

Mathematische Annalen
© Springer-Verlag 1984

On Groups of Squarefree Order

M. Ram Murty[1,*] and V. Kumar Murty[2]

1 Department of Mathematics, McGill University, Montreal, Quebec, Canada H3A 2K6
2 School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA

1. Introduction

Let $G(n)$ denote the number of non-isomorphic groups of order n. Various estimates for $G(n)$ have been given by several authors. With the recent classification of all finite simple groups, it is known that [4],

$$\log G(n) \ll (\log n)^3 . \tag{1.1}$$

It therefore follows from (1.1) that

$$\sum_{n \leq x} \log G(n) = O(x(\log x)^3) . \tag{1.2}$$

The purpose of this paper is twofold. Firstly, let us call a group a *C-group* if all its Sylow subgroups are cyclic. Denote by $C(n)$ the number of non-isomorphic C-groups of order n. We give an explicit formula for $C(n)$. Define $v(p^j, m)$ by

$$p^{v(p^j,m)} = \prod_{q|m} (p^j, q-1) , \tag{1.3}$$

where p and q denote primes and j is a positive integer. We have:

Theorem 1.1.

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

When n is squarefree, we get an explicit formula for $G(n)$.

Corollary (Hölder [2]). *For n squarefree,*

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

By means of these formulas, we prove the following asymptotic formulas.

[*] This research was supported by NSERC grant No. U0237

Theorem 1.2. *As* $x\to\infty$,

$$\sum_{n\leq x}\log C(n)=\left(\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n\varphi(n)}+\underline{o}(1)\right)x\log\log x,$$

where Λ *is the von Mangoldt function and* φ *is the Euler function.*

Theorem 1.3. *As* $x\to\infty$,

$$\sum_{n\leq x}\mu^2(n)\log G(n)=(C+\underline{o}(1))x\log\log x,$$

where

$$C=\frac{6}{\pi^2}\left(\sum_p\frac{\log p}{p^2-1}\right)$$

and the summation is over prime numbers.

The paper is essentially divided into two parts. The first part is group theoretic, where we give presentations for all C-groups. This will enable us to enumerate them thereby obtaining Theorem 1.1. The second part consists of an arithmetical analysis of $G(n)$ when n is squarefree. We isolate those integers n for which $G(n)$ becomes large.

2. Notation

Throughout the paper, p, q, r denote primes. From the above definition, we find

$$v(p,n)=\sum_{\substack{q\mid n\\ q\equiv 1\,(\mathrm{mod}\,p)}}1.$$

If G is a group and H is a subgroup, $C_G(H)$ denotes the centralizer of H in G. Finally, we define the "squarefree core" function: $\gamma(n)=\prod_{p\mid n}p$.

3. C-Groups

In this section, we give a presentation for any C-group. Let G be a C-group of order n and let

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r},\qquad p_1<p_2<\dots<p_r$$

be the prime factorization of n. We fix this notation throughout this section. We recall that G is supersolvable [1, Theorem 9.4.3].

Lemma 3.1. *There are elements* $X_1,\dots,X_n\in G$ *of order* $p_1^{\alpha_1},p_2^{\alpha_2},\dots,p_r^{\alpha_r}$ *(respectively), such that*

$$X_i^{-1}X_jX_i=X_j^{a(i,j)},\qquad 1\leqq i<j\leqq r.$$

Here, the $a(i,j)$ *are integers satisfying* $1\leqq a(i,j)<p_j^{\alpha_j}$, $(a(i,j),p_j)=1$. *The* $\{X_i\}$ *generate* G.

Proof. Since G is generated by its Sylow subgroups, the second statement is obvious. As G is supersolvable, there is a unique (i.e. normal) p_r-Sylow subgroup S (say). Let X_r be a generator of S, and let M be a complement of S. Then M is again a C-group. We may assume $r>1$ as there is nothing to prove if $r=1$. By induction, there are elements $X_1, \ldots, X_{r-1}$ of the above type. The result follows.

We make one choice of elements $\{X_i\}$ as in Lemma 3.1 and fix them for the rest of this section. The following result is the essential ingredient which enables us to obtain an explicit formula for $C(n)$.

Lemma 3.2. *Let $i<j<k$. If $a(i,j)\neq 1$ then $a(j,k)=1$.*

Proof. Let $a(i,j)=a\neq 1$ and $a(j,k)=b$. Suppose $b\neq 1$. Set $a(i,k)=d$, and $e=b^a$. Then,

$$\begin{aligned} X_k^e &= X_j^{-a}X_kX_j^a=(X_i^{-1}X_j^{-1}X_i)X_k(X_i^{-1}X_jX_i) \\ &= X_i^{-1}X_j^{-1}X_k^{d'}X_jX_i=X_i^{-1}X_k^{bd'}X_i=X_k^b, \end{aligned}$$

where $dd'\equiv 1(\operatorname{mod} p_k^{\alpha_k})$. Therefore $b^a\equiv b(\operatorname{mod} p_k^{\alpha_k})$. But we know from $a(j,k)=b$ that

$$b_j^{p^{\alpha_j}}\equiv 1(\operatorname{mod} p_k^{\alpha_k})$$

and as $b\neq 1$, we must have $(a-1, p_j^{\alpha_j})>1$. Hence, $a\equiv 1(\operatorname{mod} p_j)$. It follows that

$$\frac{a^{p_i\alpha_i}-1}{a-1}\equiv p_i^{\alpha_i}(\operatorname{mod} p_j)\,.$$

We also know from $a(i,j)=a$ that

$$a^{p_i\alpha_i}\equiv 1(\operatorname{mod} p_j^{\alpha_j})\,.$$

Therefore, as $i\neq j$, we deduce

$$a\equiv 1(\operatorname{mod} p_j^{\alpha_j})\,.$$

But this contradicts our assumption that $a\neq 1$.

Lemma 3.3. *Let A denote the set*

$$\left\{p_i \ni \textit{there is a } p_i\textit{-Sylow subgroup } S_i \ni |C_G(S_i)|\equiv 0\left(\operatorname{mod} \prod_{j\geqq i} p_j^{\alpha_j}\right)\right\}.$$

Then

(i) *$p_i\notin A$ if and only if $a(i,j)\neq 1$ for some $j>i$.*
(ii) *If $p_i\in A$, there is a unique p_i-Sylow subgroup.*

Proof. Suppose that $p_i\notin A$. Let S_i denote the subgroup generated by X_i. Then

$$|C_G(S_i)|\not\equiv 0\left(\operatorname{mod} \prod_{j\geqq i} p_j^{\alpha_j}\right)$$

and in particular, X_i does not commute with some $X_j (j>i)$, i.e. $a(i,j)\neq 1$ for some $j>i$. Conversely, suppose $a(i,j)\neq 1$ for some $j>i$. Again, let S_i denote the subgroup generated by X_i. By Lemma 3.2, $a(k,i)=1$ for all $k<i$. Thus X_i commutes with all $X_k, k<i$. If

$$|C_G(S_i)|\equiv 0\left(\operatorname{mod} \prod_{j\geqq i} p_j^{\alpha_j}\right),$$

this would imply that S_i is contained in the center of G, contradicting $a(i,j) \neq 1$. Since $|C_G(S_i)|$ is the same for all p_i-Sylow subgroups, it follows that $p_i \notin A$. This proves (i).

If $p_i \in A$, then by (i), $a(i,j) = 1$ for all $j > i$. Since X_i is normalized by all $X_j, j < i$, it follows that X_i generates a normal p_i-Sylow subgroup. This proves (ii).

We can now make the following definitions. The *active divisor* d_G of G is

$$d = d_G = \prod_{p_i \notin A} p_i^{\alpha_i}.$$

We also call n/d_G the *inactive divisor* of G.

Lemma 3.4. *Let G be a C-group of order n, with active divisor d, and put $de = n$. Then there is a unique normal, cyclic subgroup K of order e.*

Proof. As the Hall subgroups of a solvable group are conjugate, and as $(d, e) = 1$, any normal subgroup of order e must be unique. Let K be the subgroup generated by $\{X_i \ni p_i \ni A\} = \{X_i \ni p_i | e\}$. From Lemma 3.3 (i), we see that if $p_i, p_j \in A$, then X_i and X_j commute. Therefore, K is abelian, and as all its Sylow subgroups are cyclic, K is in fact cyclic. That K is normal follows from Lemma 3.3 (ii).

Let d be a divisor of n such that $(d, e) = 1$, $e = n/d$. Let r be an integer such that $1 \leqq r < e$, and the order of $r(\operatorname{mod} e)$ divides d, and is divisible by $\gamma(d)$. Then

$$G(d, r) = \langle x, y : x^d = y^e = 1, x^{-1}yx = y^r \rangle$$

is a C-group of order n with active divisor d.

Lemma 3.5. *Let G be a C-group of order n. Then there is a divisor d of n with $(d, e) = 1$, $e = n/d$, and an integer $1 \leqq r < e$ whose order* $(\operatorname{mod} e)$ *divides d, and is divisible by $\gamma(d)$, such that $G \cong G(d, r)$.*

Proof. Let Q be the subgroup of G generated by $\{X_i | p_i \notin A\}$. If $p_i, p_j \notin A$, $p_i < p_j$, then $a(i,j) = 1$. This follows from Lemmas 3.2 and 3.3 (i). Thus these X_i commute, and so Q is cyclic of order d_G. Let K be the subgroup of G described in Lemma 3.4. As G is supersolvable, K has a complement, which must be a conjugate of Q. Hence G has a presentation

$$\langle x, y : x^{d_G} = y^{n/d_G} = 1, x^{-1}yx = y^r \rangle$$

with r an integer such that $1 \leqq r < e$, and $r(\operatorname{mod} e)$ has order dividing d and divisible by $\gamma(d)$. Thus $G \cong G(d_G, r)$.

Remark. This result should be compared with another presentation given in Hall [1, Theorem 9.4.3]. That presentation, however, does not lead to an easy enumeration of C-groups.

Lemma 3.6. *$G(d, r) \cong G(d', r')$ if and only if $d = d'$ and $r^\alpha \equiv r'(\operatorname{mod} e)$ for some α coprime to d.*

Proof. We write $e = n/d$ and $e' = n/d'$ and

$$G = G(d, r) = \langle x, y : x^d = y^e = 1, x^{-1}yx = y^r \rangle$$

$$G' = G(d', r') = \langle X, Y : X^{d'} = Y^{e'} = 1, X^{-1}YX = Y^{r'} \rangle .$$

Let $\varphi: G(d,r) \to G(d',r')$ be an isomorphism. We show that if $p|d$ then $p|d'$. By symmetry, this will show that $d=d'$. If G or G' is abelian, this is obvious. So we may suppose that they are both non-abelian.

Choose a prime divisor p (respectively q) of d (respectively e) and a generator x_p (respectively x_q) of a p- (respectively q) Sylow subgroup of G, such that $x_p^{-1}x_q x_p = x_q^\alpha$, $\alpha \neq 1$. If $p \nmid d'$, $\varphi(x_p)$ generates a normal p-Sylow subgroup S_p' in G'. Since x_q generates a normal subgroup in G, $\varphi(x_q)$ generates a normal q-Sylow subgroup S_q' in G'. Since

$$\varphi(x_p)^{-1}\varphi(x_q)\varphi(x_p)\varphi(x_q)^{-1} = \varphi(x_q)^{\alpha-1} \in S_p' \cap S_q' = \{1\},$$

we see that $\alpha = 1$, contradicting our choice. Thus $p|d'$. As remarked above, this shows that $d=d'$.

Since Hall subgroups are conjugate, there is a $g \in G'$ and integers α, and β such that

$$\varphi(x) = g^{-1}X^\alpha g, \qquad \varphi(y) = Y^\beta.$$

Note that α is coprime to d.

Then $x^{-1}yx = y^r$ implies that

$$(g^{-1}X^{-\alpha}g)Y^\beta(g^{-1}X^\alpha g) = Y^{\beta r}.$$

As $\langle Y \rangle$ is normal, it follows that $X^{-\alpha}Y^\gamma X^\alpha = Y^{\gamma r}$ where $gY^\beta g^{-1} = Y^\gamma$. Thus $(r')^\alpha \gamma \equiv r\gamma \bmod e)$. As $(\beta, e) = 1$, so also $(\gamma, e) = 1$. Thus $(r')^\alpha \equiv r(\bmod e)$.

Conversely, if r and r' satisfy $(r')^\alpha \equiv r(\bmod e)$, with α coprime to d, we can define an isomorphism

$$\varphi: G(d,r) \to G(d,r')$$

by sending $\varphi(x) = X^\alpha$ and $\varphi(y) = Y$.

4. Proof of Theorem 1.1

Let $C_{d,m}(n)$ denote the member of C-groups G of order n such that $G \cong G(d,r)$ with some $r(\bmod e)$ of order m. Then, using Lemma 3.6,

$$C(n) = \sum_{\substack{d|n \\ (d,e)=1}} \sum_{\gamma(d)|m|d} C_{d,m}(n). \tag{4.1}$$

(Here, $e = n/d$.) Since $G(d,r) \cong G(d,r')$ if r and r' generate the same subgroup $(\bmod e)$, we see that

$$\begin{aligned} C_{d,m}(n) &= \#\{r(\bmod e) \text{ of order } m\}/\varphi(m) \\ &= \prod_{p^j \| m} \left(\frac{\#\{r_p(\bmod e) \text{ of order } p^j\}}{\varphi(p^j)} \right). \end{aligned} \tag{4.2}$$

Now, the number of $r_p(\bmod e) \ni r_p^{p^j} \equiv 1 \ (\bmod e)$ is

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

Hence, the number of $r_p(\bmod e)$ of order p^j is

$$p^{v(p^j,e)} - p^{v(p^{j-1},e)}. \tag{4.3}$$

Now, putting (4.1)–(4.3) together, we find that

$$C(n)=\sum_{\substack{d|n\\(d,e)=1}}\ \sum_{\gamma(d)|m|d}\ \prod_{p^j\|m}\left(\frac{p^{v(p^j,e)}-p^{v(p^{j-1},e)}}{\varphi(p^j)}\right)$$

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

as desired. This completes the proof.

In case n is squarefree, the inner sum is

$$\frac{p^{v(p,e)}-1}{p-1},$$

where $v(p,e)$ is the number of prime factors of e which are $\equiv 1(\bmod p)$. The corollary now follows immediately.

To conclude this section, we show that

$$C(n)<\prod_{p|n}(n,p-1)\,. \tag{4.4}$$

This bound will be utilized in the proof of Theorem 1.2.

In any C-group G of order n, the p_r-Sylow subgroup (p_r is the largest prime factor of n) S_r is normal in G. As S_r has a complement in G, G is then a semidirect product of S_r and a C-group H of order $m=n/p_r^{\alpha_r}$. To bound $C(n)$, therefore, we need to count the number of homomorphisms

$$\theta: H\to\operatorname{Aut}(S_r)\,.$$

Hence, the number of possible θ's is

$$\prod_{q^\beta\|m}(q^\beta, p_r^{\alpha_r-1}(p_r-1))=\prod_{q^\beta\|m}(q^\beta,p_r-1)=(n,p_r-1)\,.$$

Therefore

$$C(n)\leqq C(n/p_r^{\alpha_r})\cdot(n,p_r-1)\,,$$

and an easy induction argument completes the proof of (4.4).

We further remark that $C(n)\leqq\varphi(n)$ and so, by the methods of [3], C-groups are scarce. But this bound is insufficient for us to deduce Theorem 1.2.

5. Arithmetical Lemmas

We record in this section all the results which are of an arithmetical nature that will be used in the proofs of Theorems 1.2 and 1.3.

Lemma 5.1.

$$\sum_{\substack{q\leqq x\\ q\equiv 1(d)}}\frac{1}{q}\ll\frac{\log\log x+\log d}{\varphi(d)}\,.$$

Proof. We split the sum into Σ_1 and Σ_2 where in Σ_1, $q<d^2$, and in Σ_2, $q\geqq d^2$. Clearly,

$$\Sigma_1 \ll \frac{\log d}{d} \leqq \frac{\log d}{\varphi(d)}.$$

As for Σ_2, we have by partial summation and the Brun-Titchmarsh theorem

$$\Sigma_2 \ll \frac{\log\log x}{\varphi(d)}.$$

This proves the result.

Lemma 5.2. *Let p be a prime. Then*

$$\sum_{\substack{q<z\\ q\equiv 1(p)}} \frac{1}{q} = \frac{\log\log z}{p-1} + O(1),$$

where the constant implied is absolute. If furthermore, $p<(\log z)^c$ (where c is an arbitrary constant) then

$$\sum_{\substack{q<z\\ q\equiv 1(p)}} \frac{1}{q} = \frac{\log\log z}{p-1} + O\left(\frac{\log p}{p}\right).$$

Proof. The result follows easily from the Siegel-Walfisz theorem, partial summation and the Brun-Titchmarsh theorem.

Lemma 5.3. *Let a be a squarefree number and denote by $Q(x,a)$ the number of squarefree numbers $n\leqq x$ such that $a|n$. Then*

$$Q(x,a) = \frac{6}{\pi^2} f(a)x + O\left(d(a)\sqrt{\frac{x}{a}}\right),$$

where

$$f(a) = \prod_{p|a} (p+1)^{-1}$$

and $d(a)$ denotes the number of divisors of a.

Proof. We have by familiar properties of the Möbius function,

$$Q(x,a) = \sum_{\substack{n\leqq x/a\\ (n,a)=1}} \sum_{d^2|n} \mu(d) = \sum_{d^2\leqq x/a} \mu(d) \sum_{\substack{n\leqq x/a\\ d^2|n}} \sum_{\substack{\delta|a\\ \delta|n}} \mu(\delta)$$

The inner sums become

$$\sum_{\delta|a} \mu(\delta) \frac{x/a}{[d^2,\delta]} + O(d(a)),$$

where the symbol $[a,b]$ denotes the least common multiple of a and b. We therefore get

$$Q(x,a)=\sum_{\substack{d^2\leqq x/a\\(d,a)=1}}\mu(d)\frac{\phi(a)x}{d^2a^2}+O\left(d(a)\sqrt{\frac{x}{a}}\right)$$

since

$$\sum_{\delta|a}\frac{\mu(\delta)}{[d^2,\delta]}$$

is zero unless $(a,d)=1$ in which case it is $\phi(a)/d^2a$. Finally, we deduce

$$Q(x,a)=\frac{6x}{\pi^2}\frac{\phi(a)}{a^2}\prod_{p|a}\left(1-\frac{1}{p^2}\right)^{-1}+O\left(d(a)\sqrt{\frac{x}{a}}\right)$$

which gives us the desired result.

Lemma 5.4. *Uniformly for $p<\log x$,*

$$\sum_{\substack{n\leqq x\\p|n}}v^2(p,n)\ll\frac{x(\log\log x)^2}{p^3}.$$

Proof. We have

$$\sum_{\substack{n\leqq x\\p|n}}v(p,n)^2=\sum_{\substack{n\leqq x\\p|n}}\sum_{\substack{q|n\\q\equiv 1(p)}}\sum_{\substack{r|n\\r\equiv 1(p)}}1\leqq\sum_{\substack{q\equiv 1(p)\\q\leqq x}}\sum_{\substack{r\equiv 1(p)\\r\leqq x}}\frac{x}{pqr}\ll\frac{x(\log\log x)^2}{p^3}$$

by Lemma 5.1.

Lemma 5.5. *The number of $n\leqq x$ such that $p|n$ and having no prime divisor $\equiv 1(\bmod p)$, is*

$$\ll\frac{x}{p}(\log\log x)^{-A}$$

for any fixed $A>0$, uniformly for $p<(\log\log x)^{1/2}$.

Proof. The number of integers in question is, by Brun's sieve

$$\ll\frac{x}{p}\prod_{\substack{q\equiv 1(p)\\q<z}}\left(1-\frac{1}{q}\right)$$

for $z=x^{1/2}$. By Lemma 5.2, this is

$$\ll\frac{x}{p}\exp\left(-\frac{\log\log z}{p-1}\right)$$

$$\ll\frac{x}{p}\exp(-(\log\log x)^{1/2})$$

as $p<(\log\log x)^{1/2}$. The lemma clearly follows from this.

6. The Upper Bound Asymptotic Formulas

Let

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

We have seen that $C(n)\leqq g(n)$ and so we begin by finding asymptotic formulas for

$$\sum_{n\leqq x}\log g(n)$$

and

$$\sum_{n\leqq x}\mu^2(n)\log g(n).$$

Clearly

$$\sum_{n\leqq x}\log g(n)=\sum_{n\leqq x}\sum_{p|n}\sum_{\substack{d|n\\ d|(p-1)}}\wedge(d).$$

On interchanging summation, the above sum becomes

$$\sum_{d\leqq x}\wedge(d)\sum_{\substack{p\leqq x\\ p\equiv 1(d)}}\left[\frac{x}{pd}\right]=\Sigma_1+\Sigma_2,$$

where in Σ_1, $d<\log\log x$ and in Σ_2, $d>\log\log x$. Then, by Lemma 5.1,

$$\Sigma_2\ll\sum_d{}'\frac{\wedge(d)}{d\varphi(d)}(\log\log x+\log d)$$

where in the summation, $d>\log\log x$. It is now easy to see that

$$\Sigma_2=\underline{o}(x\log\log x),$$

as $x\to\infty$.

In Σ_1, we apply Lemma 5.2 and the Brun-Titchmarsh inequality to deduce

$$\Sigma_1=\left(\sum_d\frac{\wedge(d)}{d\varphi(d)}+\underline{o}(1)\right)x\log\log x.$$

This proves the upper bound asymptotic formula in Theorem 1.2. Similarly, to handle the squarefree case, we utilise Lemma 5.3 to deduce

$$\sum_{n\leqq x}\mu^2(n)\log g(n)=\sum_{d\leqq x}\wedge(d)\sum_{\substack{p\leqq x\\ p\equiv 1(d)}}Q(x,pd)=\left(\frac{6}{\pi^2}\sum_p\frac{\log p}{p^2-1}+\underline{o}(1)\right)x\log\log x.$$

as $x\to\infty$.

7. Lower Bound Asymptotic Formulas

It is in the lower bound asymptotic formula, that the explicit formula for $C(n)$ becomes important.

Let S denote the set of natural numbers n for which $v(p,n) \geqq 1$ for every $p|n$ satisfying the inequality $p < (\log\log n)^{1/2}$. Put

$$d_n = \prod_{\substack{p^\alpha \| n \\ p^\alpha < (\log\log n)^{1/2}}} p_\alpha \,.$$

Then, for $n \in S$, it is easy to see that

$$\begin{aligned} C(n) &\geqq \prod_{p^\alpha \| d_n} \left(\sum_{j=1}^{\alpha} \frac{p^{v(p^j, n/d_n)} - p^{v(p^{j-1}, n/d_n)}}{p^{j-1}(p-1)} \right) \\ &\geqq 2^{-v(d_n)} \varphi(d_n)^{-1} \prod_{p^\alpha \| d_n} p^{v(p^\alpha, n/d_n)}, \end{aligned}$$

where $v(n)$ denotes the number of prime factors of n. Hence

$$\sum_{n \leqq x} \log C(n) \geqq \sum_{\substack{n \leqq x \\ n \in S}} \sum_{p^\alpha \| d_n} v(p^\alpha, n/d_n) \log p - \sum_{n \leqq x} \log(2^{v(d_n)} \varphi(d_n)) \,.$$

Clearly, the last sum on the right is

$$\begin{aligned} &\ll \sum_{n \leqq x} \log d_n = \sum_{n \leqq x} \sum_{e | d_n} \Lambda(e) \\ &\ll \sum_{e < (\log\log x)^{1/2}} \Lambda(e) x/e \end{aligned}$$

which is easily seen to be $\underline{o}(x \log\log x)$ as $x \to \infty$.

Now, since $v(p^\alpha, n/d_n) \leqq v(p^\alpha, n) \leqq \alpha v(p,n)$, we have

$$\sum_{\substack{n \leqq x \\ n \notin S}} \sum_{p^\alpha \| d_n} v(p^\alpha, n/d_n) \log p \leqq (\log\log\log x)^2 \sum_{\substack{n \leqq x \\ n \in S}} \sum_{\substack{p | n \\ p < (\log\log n)^{1/2}}} v(p,n) \,.$$

This last sum is $\underline{o}(x \log\log x)$ by a straightforward application of the Cauchy-Schwarz inequality and Lemmas 5.4 and 5.5. Therefore

$$\sum_{n \leqq x} \log C(n) \geqq \sum_{n \leqq x} \sum_{p^\alpha \| d_n} v(p^\alpha, n/d_n) \log p + \underline{o}(x \log\log x) \,.$$

The sum on the right hand side of the inequality is evidently

$$\begin{aligned} &\geqq \sum_{n \leqq x} \sum_{p^\alpha \| d_n} \sum_{\substack{q | n \\ q > (\log\log x)^{1/2}}} \sum_{\substack{d | p^\alpha \\ d | (q-1)}} \Lambda(d) \\ &= \sum_{d < (\log\log x)^{1/2}} \Lambda(d) \sum_{\substack{q \equiv 1 (d) \\ (\log\log x)^{1/2} < q \leqq x}} \left[\frac{x}{qd} \right] \\ &= \sum_{d < (\log\log x)^{1/2}} \frac{\Lambda(d)}{d} \frac{x \log\log x}{\varphi(d)} + \underline{o}(x \log\log x) \end{aligned}$$

after an application of Brun-Titchmarsh theorem and Lemma 5.2. Thus,

$$\sum_{n \leqq x} \log C(n) \geqq \left\{ \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n \varphi(n)} + \underline{o}(1) \right\} x \log\log x$$

as $x \to \infty$.

The corresponding formula for squarefree numbers can be proved by utilising Lemma 5.3 in the penultimate step of the above proof and is entirely analogous. This completes the proofs of Theorems 1.2 and 1.3.

8. Concluding Remarks

Further results of a similar nature can be proved. We only give one example.

Let $G^*(n)$ be the number of non-isomorphic groups of order n which are nilpotent. Then $G^*(n)$ is a multiplicative function. Therefore

$$\sum_{n \leqq x} \log G^*(n) = \sum_{\substack{p^\alpha \leqq x \\ \alpha \geqq 2}} \left[\frac{x}{p^\alpha}\right] \log G(p^\alpha).$$

Utilising (1.1) we deduce easily:

Theorem 8.1. *There exists a constant $c>0$ such that*

$$\sum_{n \leqq x} \log G^*(n) = (1 + \underline{o}(1))cx$$

as $x \to \infty$.

With regard to improving (1.2), we conclude by asking:

Question. Does there exist a constant $c>0$ such that

$$\sum_{n \leqq x} \log G(n) \geqq cx \log x$$

as $x \to \infty$?

References

1. Hall, M.: Theory of groups. New York: Macmillan 1959
2. Hölder, O.: Die Gruppen mit quadratfreier Ordnungszahl. Nachr. Königl. Ges. Wiss. Göttingen Math.-Phys. K**1**, 211–229 (1895)
3. Murty, M.R., Murty, V.: The number of groups of a given order (to appear in *J. Number Theory*)
4. Neumann, P.: An enumeration theorem for finite groups. Quart. J. Math. Oxford Ser. (2) **20**, 395–401 (1969)

Received June 20, 1983