ACTA ARITHMETICA
LXI.1 (1992)

When the group-counting function assumes a prescribed integer value at squarefree integers frequently, but not extremely frequently

by

Claudia A. Spiro-Silverman (Boston, Mass.)

1. Introduction. Throughout the sequel, k, m, and n denote positive integers, p, q, and r signify primes, and x and y represent sufficiently large positive real numbers unless otherwise indicated. We denote the natural logarithm of x by $\log x$, and recursively define the functions $L_k(x)$ by

$$L_2 x = \log\log x\,, \qquad L_{k+1} = L_k \log x \quad \text{for } k \ge 2\,.$$

Write $\phi(n)$ for the number of $m \le n$ with m and n relatively prime.

Put $g(n)$ for the number of (isomorphism classes of) groups of order n. In studying the local distribution of this function, one examines the quantities

$$F_k(x) = \#\{n \le x : g(n) = k\},$$
$$Q_k(x) = \#\{n \le x : n \text{ squarefree}, \ g(n) = k\}$$

as x tends to infinity with k fixed. Clearly, $F_k(x) \ge Q_k(x)$.

If $h(x)$ and $l(x)$ are complex-valued functions, we write $h(x) \sim l(x)$ to signify that

$$\lim_{x\to\infty} \frac{h(x)}{l(x)} = 1,$$

and we put $h(x) = o(l(x))$ to indicate that

$$\lim_{x\to\infty} \frac{h(x)}{l(x)} = 0.$$

The expressions $h(x) = O(l(x))$ and $h(x) \ll l(x)$ both mean that there is a positive constant C for which $|h(x)| \le Cl(x)$, if x is sufficiently large. We will write $l(x) \gg h(x)$ to connote that $0 < h(x) \ll l(x)$ for all sufficiently large x.

1991 *Mathematics Subject Classification*: 11Q15, 11N.
Key words and phrases: group-counting, squarefree order, lower bound.

In 1948, Erdős [1] demonstrated that

$$F_1(x) = Q_1(x) \sim \frac{e^{-\gamma} x}{L_3 x}, \tag{1}$$

where $\gamma = .577\ldots$ denotes Euler's constant. He used the criterion that $\phi(n)$ is coprime to n if and only if $g(n) = 1$ [1, 11, 12]. Later, M. K. Murty and V. K. Murty [8] showed that

$$Q_2(x) \sim F_2(x) \ll \frac{x L_4 x}{(L_3 x)^2},$$

and stated the conjecture that

$$F_2(x) \sim \frac{e^{-\gamma} x}{(L_3 x)^2}. \tag{2}$$

Subsequently, Erdős, M. R. Murty and V. K. Murty established the following two theorems (see Theorem 3, the remark immediately after the theorem, and the proof of this theorem, in [2]).

(i) If $k = 2^l$, with l a nonnegative integer, then we have

$$F_k(x) \sim Q_k(x) \sim \frac{e^{-\gamma} x}{l!(L_3 x)^{l+1}};$$

(ii) If k is not an integer power of 2, we have

$$0 \le Q_k(x) \le F_k(x) = o\left(\frac{x}{L_2 x}\right).$$

Result (i) contains both (1) and (2) as special cases. Independently, M.-G. Lu [7] showed the more precise estimate

$$F_2(x) = \frac{e^{-\gamma} x}{(L_2 x)^2} + O\left(\frac{x (L_4 x)^2}{(L_3 x)^3}\right).$$

For a somewhat more detailed account of the history of this type of problem, we refer the reader to [10]. In this paper, we showed that

$$Q_k(x) \sim \frac{\mathcal{K}(k) x (L_2 x)^2}{(\log x)^{1/(k-1)} (L_3 x)^{(k-4)/(k-3)}} \tag{3}$$

for some positive constant $\mathcal{K}(k)$, whenever $k - 2$ is prime, and k fails to belong to a certain set $\mathcal{S}$ [10, Theorem 1]. In particular, (3) holds when k is contained in

$$\{7, 19, 31, 49, 73, 91, 103\}$$

(see the remark following Theorem 1 of [10]).

By contrast, in the present paper, we will show that if k belongs to the set $\mathcal{S}$, then we have

$$Q_k(x) = \frac{x}{(L_2 x)^{O(1)}} \tag{4}$$

(see Theorem 1, below). To state the main theorem of this paper, we require the definition of $\mathcal{S}$, which we state here for completeness.

Definition. For each positive integer n and for each prime p, let $\psi(n,p)$ signify the number of primes q dividing n for which $q \equiv 1 \pmod{p}$. Put

$$\mathcal{S} = \{g(n) : n \text{ odd, squarefree; } \psi(n,p) \le 1 \text{ for all } p \mid n\}.$$

Theorem 1. *For every element k of $\mathcal{S}$, there is a computable constant $c(k)$ for which*

$$F_k(x) \ge Q_k(x) \gg x(L_2 x)^{-c(k)}.$$

Combining this estimate with (i) and (ii) yields the immediate corollary that (4) holds whenever $k \in \mathcal{S}$. Here, the implied constant depends upon k. Similarly, $F_k(x) = x/(L_2 x)^{O(1)}$. In a forthcoming paper, we will show that if k is not in $\mathcal{S}$, then we have

$$Q_k(x) = \frac{x}{(\log x)^{\lambda(k)}} (L_2 x)^{O(1)}$$

for some positive constant $\lambda(k)$ not exceeding 1, provided that there exists a squarefree positive integer n satisfying $g(n) = k$. The sentence containing (3) gives a special case of that result. Thus, if k and m are fixed, with $k \in \mathcal{S}$ but with $m \notin \mathcal{S}$, then $g(n)$ assumes the value k more frequently than the value m. So, the values of $\mathcal{S}$ are assumed—in this sense—more frequently than the other integers. Thus, in view of (i) and (ii) above, the title of this paper refers to elements of $\mathcal{S}$ which are not integer powers of 2.

We remark that all positive integers not exceeding 100 are contained in $\mathcal{S}$, except for

$$7, 11, 19, 29, 31, 47, 49, 53, 67, 71, 73, 79, 87, 91,$$

which are not. This fact can be verified computationally by the methods of [10] (see the discussion at the end of the introduction of that paper). We will give superior methods in a forthcoming paper, where we will show that $\mathcal{S}$ is closed under multiplication. Thus, $\mathcal{S}$ contains all integers of the form $2^\alpha 3^\beta 5^\delta 13^\eta$.

2. Preliminary results.

The foundation upon which the proof of Theorem 1 is built is the following result of O. Hölder from the end of the last century [5].

Lemma 1. *For every squarefree positive integer n, we have*

$$g(n) = \sum_{d \mid n} \prod_{p \mid d} \frac{p^{\psi(n/d,p)} - 1}{p - 1},$$

where the sum extends over the positive integers d dividing n, and the product runs over the primes p which divide d.

We note that the factor

$$\frac{p^{\psi(n/d,p)}-1}{p-1}$$

vanishes whenever $\psi(n/d,p)=0$, and equals 1 when $\psi(n/d,p)=1$. Thus, we have the following corollary.

Corollary 1. *If n is an odd, squarefree positive integer satisfying $\psi(n,p)\le 1$ for every prime divisor p of n, then $g(n)$ does not exceed the number $d(n)$ of positive integers dividing n. Furthermore, let m be an odd, squarefree positive integer, and assume that there exists a bijective mapping f from the prime divisors of n to the primes dividing m, such that*

$$p \mid q-1 \quad \textit{if and only if} \quad f(p)\mid f(q)-1\,. \tag{5}$$

(Here, p and q are required to divide n.) Then $g(n)=g(m)$.

Proof. Since $\psi(n,p)$ can never exceed 1 for any prime p dividing n, we deduce that each exponent $\psi(n/d,p)$ must be 0 or 1. Accordingly, Lemma 1 implies that

$$g(n)\le \sum_{d|n}\prod_{p|d}1\le \sum_{d|n}1\,.$$

This is the first statement of the corollary. For the remainder of the result, let m and n, and the map f, satisfy the hypotheses of the corollary. Then, extend f to a map f^* from the set of positive integer divisors of n to the set of positive divisors of m, by defining

$$f^*(d)=\prod_{p|d}f(p)$$

for every divisor d of n. Since m and n are squarefree, and f is a bijection, we can conclude from the Fundamental Theorem of Arithmetic that f^* bijectively maps the set $\{d : d\,|\,n\}$ to the set $\{d : d\,|\,m\}$. In addition, (5) implies that

$$\psi(n/d,p)=\psi(m/f^*(d),f(p)) \quad \text{if } d\mid n \text{ and } p\mid n\,.$$

The rest of the corollary is now a consequence of Lemma 1. ∎

One way to indicate what the corollary means is to say that if $\psi(n,p)\le 1$ for every prime $p\mid n$, then $g(n)$ depends only upon relationships of the form $q\equiv 1 \pmod p$ (where $p\mid n$ and $q\mid n$), and not upon the prime divisors of n themselves. This result does not hold if $\psi(n,q)\ge 2$ for some prime q dividing n. Indeed, Lemma 1 implies that

$$g(n)\ge \frac{q^{\psi(n/q,q)}-1}{q-1}\,,$$

where the right-hand side just corresponds to the divisor $d = q$ of n. Since $q \not\equiv 1 \,(\operatorname{mod} q)$, we can conclude from the definition of $\psi(n,p)$ that $\psi(n/q,q) = \psi(n,q)$. Hence,

$$g(n) \geq \frac{q^{\psi(n,q)} - 1}{q-1} \,.$$

By assumption, the exponent is at least 2, so that $g(n) \geq q+1$. In particular, $g(n)$ will depend upon q, and the second statement of Corollary 1 cannot be made to hold for such n. (The first statement is also false, in general—for example, $g(7 \cdot 29 \cdot 43) = 9$, while $d(7 \cdot 29 \cdot 43) = 8$.)

So far, we have considered odd, squarefree n. If n is even and squarefree, and $\psi(n,2) \leq 1$, then either $n = 2$, or $n = 2p$ for some prime $p > 2$. In the first case we have $g(n) = 1$, and in the second we have $g(n) = 2$. We noted earlier that both 1 and 2 are in $\mathcal{S}$. In view of this remark, the last paragraph, and Corollary 1, it follows from the definition of $\mathcal{S}$ that $\mathcal{S}$ is the set of values of $g(n)$, for n such that $g(n)$ depends only upon relations of the form $q \equiv 1 \,(\operatorname{mod} p)$ (where $p \mid n$ and $q \mid n$), and not upon the actual primes dividing n.

The proof of Theorem 1 will lead us to construct a set of primes satisfying appropriate relations of the type $q \equiv 1 \,(\operatorname{mod} p)$, and failing to fulfill other relations of this form. To bound the size of the product of these primes from above, if we put constraints on how small they can be, we will require the following theorem of Linnik on the least prime in an arithmetic progression [6].

LEMMA 2. *There is a positive, absolute constant* c_1 *such that if* h *and* m *are any coprime integers with* $m > 0$, *then the minimal prime* $p \equiv h \,(\operatorname{mod} m)$ *satisfies* $p = O(m^{c_1})$.

One of the main components of the proof of Theorem 1 is the construction of an integer n, all of whose prime divisors are near $L_2 x$, satisfying $g(n) = k$. We state the (apparently more general) form of this construction as our next lemma.

LEMMA 3. *Let* $k \in \mathcal{S}$, *and assume that* y *is a sufficiently large positive real number* (*where the sufficiently large constraint depends upon* k). *Then there are constants* c_2, c_3, *and* ω, *depending only on* k, *such that there exists a positive integer* n *fulfilling the following three conditions.*

(i) $g(n) = k$;
(ii) *n is squarefree, and has exactly ω prime divisors*;
(iii) *if the prime p divides n, then we have* $y < p < c_2 y^{c_3}$.

Proof. Assume that y is at least 3. By the last lemma, there is a constant $c_4 > 0$ such that if h and m are any coprime integers with $m > 0$, then there is a prime q congruent to h modulo m for which $q < c_4 m^{c_1}$. Now since $k \in \mathcal{S}$, there must be an odd, squarefree integer l such that

$$g(l) = k, \tag{6}$$

and

$$\psi(l,p) \le 1 \quad \text{for every prime } p \mid l. \tag{7}$$

Suppose that $q_1, \dots, q_\omega$ are the distinct prime divisors of l, and that $q_1 < \dots < q_\omega$. Recursively select primes $p_1, \dots, p_\omega$ to satisfy the following criteria:

$$y \le p_1 \le 2y\,; \tag{8}$$

if $p_1, \dots, p_{i-1}$ are selected $(i \le \omega)$, choose p_i so that

$$p_i \equiv 1 \pmod{p_j} \qquad \text{if } j < i \text{ and if } q_i \equiv 1 \pmod{q_j}\,, \tag{9}$$

$$p_i \equiv -1 \pmod{p_j} \qquad \text{if } j < i \text{ and if } q_i \not\equiv 1 \pmod{q_j}\,. \tag{10}$$

Bertrand's Postulate guarantees that the inequality (8) has a solution, and we choose p_1 accordingly. To show that we can select p_i so that (9) and (10) hold (for $p_1, \dots, p_{i-1}$ chosen), we observe that the Chinese Remainder Theorem allows us to rewrite the resulting system of congruences as a single congruence of the form

$$p_i \equiv h_i \pmod{p_1 \dots p_{i-1}}\,,$$

with $(h_i, p_1 \dots p_{i-1}) = 1$. Hence, the minimal solution p_i must fulfill the condition

$$p_i < c_4 (p_1 \dots p_{i-1})^{c_1}\,. \tag{11}$$

We further observe from (9) and (10) that

$$p_i \equiv 1 \pmod{p_j} \quad \text{if and only if} \quad q_i \equiv 1 \pmod{q_j}\,, \tag{12}$$

for $j < i$. Furthermore, since $p_i \equiv \pm 1 \pmod{p_{i-1}}$, we have

$$p_i > p_{i-1}, \tag{13}$$

unless $p_{i-1} = 2$. Now, by construction, p_1 is odd, and hence, the recursive selection of the primes p_j gives (13) for all i. Consequently, (12) holds for all i and j. It follows from (6), (7), (12), and Corollary 1 that

$$g(p_1 \dots p_\omega) = k\,. \tag{14}$$

Furthermore, (13) implies that

$$p_1 \dots p_{i-1} < p_{i-1} \dots p_{i-1} = p_{i-1}^{i-1}\,.$$

Thus, (11) yields

$$p_i < c_4 p_{i-1}^{(i-1)c_1} \le c_4 p_{i-1}^{(\omega-1)c_1}\,,$$

since $i \le \omega$. We can argue by induction on i to get

$$p_i \le c_4 p_1^{((\omega-1)c_1)^{i-1}}\,. \tag{15}$$

Let

$$n = p_1 \dots p_\omega \tag{16}$$

be the product of the primes p_i. Then Condition (i) follows from (14), Condition (ii) is an immediate consequence of (13) and 16), and Condition (iii) can be deduced from (8) and (15). ■

From the integer n given in our third lemma, it is possible to get a large number of positive integers $m \le x$ for which $g(m) = k$. Here, "large", in practice, will be $x/(L_2x)^{c_5}$ for some appropriate power c_5 (depending on k), when we choose y appropriately. We delay the details until the proof of our main theorem. The construction begins with the next lemma.

LEMMA 4. *If m and n are odd, squarefree, positive integers such that*

$$(\phi(m), m) = (\phi(m), n) = (\phi(n), m) = (m, n) = 1,$$

then mn is an odd, squarefree, positive integer with $g(mn) = g(n)$.

Proof. Recall that

$$\phi(l) = \prod_{p \mid l} p^{\nu_p(l)-1}(p-1) \tag{17}$$

for every positive integer l, where $\nu_p(l)$ denotes the exponent to which the prime p occurs in the canonical decomposition of l. Hence, if p is any prime divisor of l, then $p-1$ divides $\phi(l)$. Thus, the condition $(m, \phi(n)) = 1$ yields the relation $(m, p-1) = 1$. So, if q is a prime divisor of m, and p is any prime dividing n, then q does not divide $p-1$. That is,

$$\psi(n, q) = 0 \quad \text{for all } q \mid m\,. \tag{18}$$

Similarly, the equation $(m, \phi(m)) = 1$ implies that

$$\psi(m, q) = 0 \quad \text{for all } q \mid m\,; \tag{19}$$

and the relation $(\phi(m), n) = 1$ gives

$$\psi(m, p) = 0 \quad \text{for all } p \mid n\,. \tag{20}$$

Since $(m, n) = 1$, the product mn is squarefree. Moreover, mn is odd, because m and n are odd. We use Lemma 1 to compute $g(mn)$. It follows from (18) and (19) that

$$\psi(l, q) = 0 \quad \text{whenever } l \mid mn \text{ and } q \mid m\,. \tag{21}$$

Since

$$\frac{p^{\psi(mn/d,p)} - 1}{p-1} = 0$$

whenever $\psi(mn/d,p)=0$, we conclude from (21) and Lemma 1 that

$$g(mn)=\sum_{d\mid mn}\prod_{p\mid d}\frac{p^{\psi(mn/d,p)}-1}{p-1}=\sum_{d\mid n}\prod_{p\mid d}\frac{p^{\psi(mn/d,p)}-1}{p-1}\,. \tag{22}$$

If the prime p contributes to the last product, then p is a divisor of n. By (20) and the definition of $\psi(l,p)$, we have

$$\psi(mn/d,p)=\psi\left(\frac{n}{d}\cdot m,p\right)=\sum_{q\mid n/d\,\text{or}\,q\mid m;q\equiv 1\ (\bmod\ p)}1$$
$$=\psi(n/d,p)+\psi(m,p)=\psi(n/d,p)\,.$$

Here, we have utilized the fact that $(m,n)=1$, and $d\mid n$. Thus, (22) gives

$$g(mn)=\sum_{d\mid n}\prod_{p\mid d}\frac{p^{\psi(n/d,p)}-1}{p-1}\,,$$

and the lemma is now an immediate consequence of Lemma 1. ∎

Before we prove Theorem 1, we state two more lemmas.

LEMMA 5. *If m is any positive integer, then we have*

$$\sum_{p\le x;p\equiv 1\ (\bmod\ m)}\frac{1}{p}=\frac{L_2x}{\phi(m)}+O\left(\frac{\log(2m)}{\phi(m)}\right)$$

as x tends to ∞, where the implied constant does not depend on m.

Proof. This result is a special case of Lemma (6.3) of Norton [9]. ∎

LEMMA 6. *If y tends to ∞ with x, and $y\le\log x$, then the number $N(x,y)$ of positive integers $n\le x$ which have no prime divisors less than y satisfies*

$$N(x,y)=\frac{e^{-\gamma}x}{\log y}(1+o(1)).$$

Proof. This result is discussed in Halberstam and Roth's book [4] (cf. equation (3.2)). For a proof, see the first two paragraphs on that page. ∎

More general results are known. For an example, we refer the reader to Theorem 1.1 on p. 30 of Halberstam and Richert's book [3], and indeed, this entire book is related to this subject, at least in some sense.

3. The proof of the main theorem. Let k be in $\mathcal{S}$. Let x be sufficiently large, and put $y=(L_2x)^2$. By Lemma 3, there are positive constants c_2 and c_3, and a positive integer ω, such that there is a positive integer n satisfying conditions (i)–(iii) of that lemma. Write

$$n=p_1p_2\ldots p_\omega,\qquad y<p_1<p_2<\ldots<p_\omega<c_2y^{c_3}\,. \tag{23}$$

Since $g(n)=k$, we can deduce from Lemma 4 that

$$Q_k(x) \geq \sum_{m\in A(x,n)} 1, \tag{24}$$

where

$$A(x,n)=\{\text{squarefree } m : mn\leq x,\ (\phi(m),m)=(\phi(m),n) \\ =(m,\phi(n))=(m,n)=1\}\,.$$

If $P(m)$ denotes the smallest prime divisor of m, then (24) implies that

$$Q_k(x) \geq \sum_{m\in A(x,n),\, P(m)>z} 1\,, \tag{25}$$

where

$$z=(L_2x)^{3c_3} > c_2 y^{c_3}\,. \tag{26}$$

Now (17) and (23) imply that $\phi(n)=\prod_{i=1}^{\omega}(p_i-1)$ has no prime divisor exceeding z. And, clearly n does not have a prime factor greater than z. Accordingly, (25) implies that

$$Q_k(x) \geq \sum_{m\in B(x,n),\, P(m)>z} 1\,, \tag{27}$$

where

$$B(x,n)=\{\text{squarefree } m\leq x/n : (\phi(m),m)=(\phi(m),n)=1\}.$$

If we replace the condition $(\phi(m),m)=(\phi(m),n)=1$ by the weaker constraint $(\phi(m),m)=1$, the resulting error we incur in the sum on the right-hand side of (27) is

$$O\Big(\sum_{m\leq x/n,\, (\phi(m),n)>1} 1\Big)\,.$$

Since m is squarefree, it follows from (17) that if $(\phi(m),n)>1$, then there must be a prime divisor q of m with $(q-1,n)>1$. So, (23) implies that we have $q\equiv 1 \,(\operatorname{mod} p_i)$ for some i. Consequently, our error is

$$O\Big(\sum_{i=1}^{\omega}\ \sum_{q\equiv 1\,(\bmod\ p_i)}\ \sum_{m\leq x/n,\, q|m} 1\Big)\,.$$

Clearly, if q exceeds x then the inner sum is void. Thus, our error is

$$O\Big(\sum_{i=1}^{\omega}\ \sum_{q\equiv 1\,(\bmod\ p_i),\, q\leq x} \frac{x}{qn}\Big)\,.$$

We can deduce from Lemma 5 and equation (23) that this error is

$$O\Big(\frac{x}{n}\sum_{i=1}^{\omega}\Big(\frac{L_2x}{p_i}+\frac{\log p_i}{p_i}\Big)\Big)=O\Big(\frac{xL_2x}{ny}+\frac{x\log y}{ny}\Big)\,.$$

Since $y = (L_2 x)^2$, the error is

$$O\Big(\frac{x}{nL_2 x}\Big).$$

Hence, (27) yields

$$Q_k(x) \geq \sum_{m\leq x/n,\, (\phi(m),m)=1,\, m \text{ squarefree},\, P(m)>z} 1 + O\Big(\frac{x}{nL_2 x}\Big). \tag{28}$$

By (17) we must have m squarefree whenever $(\phi(m), m) = 1$, so that the condition that m be squarefree can be deleted from beneath the last sum. If we also delete the constraint $(\phi(m), m) = 1$, the error we make is

$$O\Big(\sum_{m\leq x/n,\, P(m)>z,\, (29) \text{ and/or } (30) \text{ hold}} 1\Big),$$

where conditions (29) and (30) respectively state that

$$m \text{ contains two prime divisors } q \text{ and } r \text{ with } r \equiv 1 \,(\mathrm{mod}\, q); \tag{29}$$

$$\text{there is a prime } q \text{ with } q^2 \mid m. \tag{30}$$

If $q \mid m$, and $P(m) > z$, then $q > z$. So, the last error is

$$O\Big(\sum_{q>z} \sum_{r\equiv 1 \,(\bmod\, q)} \sum_{m\leq x/n,\, q|m,\, r|m} 1 + \sum_{q>z} \sum_{m\leq x/n,\, q^2|m} 1\Big).$$

First, we observe that the penultimate sum over m is void if $r > x$. Then we estimate the last two sums on m trivially, to get the bound

$$O\Big(\frac{x}{n}\sum_{q>z}\frac{1}{q}\sum_{r\leq x,\, r\equiv 1 \,(\bmod\, q)}\frac{1}{r} + \frac{x}{n}\sum_{q>z}\frac{1}{q^2}\Big)$$

for this error. We can conclude from Lemma 5 that this error is

$$O\Big(\frac{x}{n}\sum_{q>z}\Big(\frac{L_2 x}{q^2} + \frac{\log q}{q^2}\Big) + \frac{x}{n}\sum_{q>z}\frac{1}{q^2}\Big).$$

Next, we ignore the primality of q and recall that

$$\sum_{q>z}\frac{1}{q^2} \ll \int_z^\infty \frac{1}{u^2}\,du = \frac{1}{z};$$

$$\sum_{q>z}\frac{\log q}{q^2} \ll \int_z^\infty \frac{\log u}{u^2}\,du \leq \int_z^\infty \frac{\log z}{\sqrt{z}}\,\frac{1}{u^{3/2}}\,du = \frac{2\log z}{\sqrt{z}}\,\frac{1}{\sqrt{z}}.$$

(In the last integral we have written $(\log u)/u^2$ as the product of $(\log u)/\sqrt{u}$ and $1/u^{3/2}$, and majorized the first factor.)

We obtain the estimate

$$O\left(\frac{x}{n}\left(\frac{L_2x}{z}+\frac{\log z}{z}\right)+\frac{x}{n}\frac{1}{z}\right)$$

for our error, in this manner. According to (26), this error is

$$O\left(\frac{x}{n(L_2x)^{3c_3-1}}\right).$$

Hence, (28) becomes

$$Q_k(x)\geq\sum_{m\leq x/n,\,P(m)>z}1+O\left(\frac{x}{nL_2x}\right).$$

An application of Lemma 6 yields

$$\begin{aligned}Q_k(x)&\geq\frac{e^{-\gamma}x}{3c_3nL_3x}(1+o(1))+O\left(\frac{x}{nL_2x}\right)\\&=\frac{e^{-\gamma}}{3c_3}\frac{x}{nL_3x}(1+o(1)),\end{aligned}$$

in view of (26).

The theorem is now a consequence of (24). ■

References

[1] P. Erdős, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. 12 (1948), 75–78.

[2] P. Erdős, M. R. Murty, and V. K. Murty, *On the enumeration of finite groups*, J. Number Theory 25 (1987), 360–378.

[3] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Math. Soc. Monographs 4, Academic Press, London 1974.

[4] H. Halberstam and K. F. Roth, *Sequences*, Springer, New York 1983.

[5] O. Hölder, *Die Gruppen mit quadratfreier Ordnungszahl*, Nach. Königl. Gessell. der Wiss. Göttingen Math.-Phys. Kl. 1895, 211–229.

[6] Yu. V. Linnik, *On the least prime in an arithmetic progression. II. The Deuring–Heilbronn phenomenon*, Mat. Sb. (N.S.) 15 (57) (1944), 347–368.

[7] M.-G. Lu, *The asymptotic formula for* $F_2(x)$, Sci. Sinica Ser. A 30 (1987), 262–278.

[8] M. R. Murty and V. K. Murty, *On the number of groups of a given order*, J. Number Theory 18 (1984), 178–191.

[9] K. K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. 20 (1976), 681–705.

[10] C. A. Spiro, *The probability that the number of groups of squarefree order is two more than a fixed prime*, Proc. London Math. Soc. 60 (1990), 444–470.

[11] T. Szele, *Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört*, Comment. Math. Helv. 20 (1947), 265–267.

[12] J. Szép, *On finite groups which are necessarily commutative*, ibid., 223–224.

MATHEMATICS DEPARTMENT
BOSTON COLLEGE
BOSTON, MASSACHUSETTS 02167
U.S.A.

Received on 29.3.1990 (2024)