ACTA ARITHMETICA
LXXI.3 (1995)

Groups of cubefree order

by

Claudia Spiro-Silverman (Babson Park, Mass.)

1. Introduction. Statement of the main theorem. Let k, m, n, p, q, and r denote positive integers with p, q, and r signifying primes, and take x to be a positive real number. We call the number n *cubefree* if n is not divisible by the cube of a prime. Denote the Euler phi-function of n by $\phi(n)$, and the natural logarithm of x by $\log x$. Put $L_2x = \log\log x$, $L_3x = \log L_2x$, and $L_4x = \log L_3x$. If $h(x)$ and $j(x)$ are complex-valued functions, we write $h(x) \sim j(x)$ to mean

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

and we put $h(x) = o(j(x))$ to show that

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

The expression $h(x) \ll j(x)$ signifies that there is a positive constant K for which $|h(x)| \le Kj(x)$, if x is sufficiently large. We will write $j(x) \gg h(x)$ to mean that $0 < h(x) \ll j(x)$ for all sufficiently large x.

Earlier authors have studied the functions

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

and

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

(e.g., see [3], [8]–[11]). We examine the function

$$C_k(x) = \#\{n \le x : n \text{ cubefree},\ g(n) = k\}.$$

We immediately have

$$x \ge F_k(x) \ge C_k(x) \ge Q_k(x). \tag{1}$$

In 1948, Erdős [2] showed that

$$F_1(x) \sim e^{-\gamma}x/L_3x,$$

where $\gamma = .5772\ldots$ is Euler's constant. His proof shows that we have

$$F_1(x) \sim C_1(x) \sim Q_1(x). \tag{2}$$

Subsequently, M. R. Murty and V. K. Murty [9] showed that

$$Q_2(x) \sim C_2(x) \sim F_2(x) \ll \frac{xL_4x}{(L_3x)^2},$$

and stated the conjecture that

$$F_2(x) \sim \frac{e^{-\gamma}x}{(L_3x)^2}. \tag{3}$$

Later, Erdős, M. R. Murty, and V. K. Murty established that when $k = 2^l$ for some nonnegative integer l, then we have

$$Q_k(x) \sim C_k(x) \sim F_k(x) \sim \frac{e^{-\gamma}x}{l!(L_3x)^{l+1}}$$

(see Theorem 3 of [3], and its proof). Note that the case $k = 2$ implies the conjecture (3). They also showed that if k is not an integer power of 2, then we have $F_k(x) = o(x/L_2x)$. For a more detailed account of the history of the work done on these types of questions, we refer the reader to the introduction to [10]. In that paper, we showed that for positive integers k not belonging to the set $\mathcal{S} \doteq \{g(n) : n \text{ odd, squarefree}\}$, and such that $k-2$ is prime, there exist positive computable constants $\kappa = \kappa(k)$ for which the formula

$$Q_k(x) \sim \frac{\kappa x(L_2x)^2}{(\log x)^{1/(k-3)}(L_3x)^{(k-4)/(k-3)}} \tag{4}$$

holds. The positive integers k not exceeding 103 to which this result applies, are 7, 19, 31, 49, 73, 91, and 103 (see the main theorem of [10], and the remark following that theorem). By contrast, if k is contained in the aforementioned set $\mathcal{S}$, then we have

$$Q_k(x) \gg_k x(L_2x)^{-\lambda(k)} \tag{5}$$

for some positive computable constant $\lambda = \lambda(k)$ (see the main theorem of [11]). The first positive integer failing to be in $\mathcal{S}$ is 7 (see the discussion following the statement of Theorem 1 of [10]). These results show that the functions $Q_k(x)$ behave very differently, on average, for different values of k. Moreover, it is natural to ask the question of for what values of k Equation (2) obtains.

To state the primary result of this paper, we first must define an appropriate analog $\mathcal{C}$ of the aforementioned set $\mathcal{S}$. Toward that end, we isolate the following two properties which a positive integer n may possess.

Property 1. There is no pair p, q of primes for which $pq^2 \mid n$, and $q \equiv 1 \bmod p$.

PROPERTY 2. For any prime q, let $M(n,q)$ be the number of prime divisors p of n such that $p \equiv 1 \bmod q$, and let $N(n,q)$ denote the number of squares of primes p^2 dividing n with the property that $p \equiv -1 \bmod q$. Then $M(n,q) + N(n,q) \leq 1$ for all $q \,|\, n$.

DEFINITION. Let

$$\mathcal{C} = \{g(n) : n \text{ odd and cubefree, } n \text{ satisfies Properties 1 and 2}\}.$$

THEOREM 1. *If $k \in \mathcal{C}$, then there exists a positive, computable constant $c = c(k)$ for which*

$$F_k(x) \geq C_k(x) \gg_k x(L_2 x)^{-c}.$$

For k contained in $\mathcal{S}$, the result is an immediate consequence of Theorem 1 of [11]. Therefore, to verify that Theorem 1 of the present paper is not subsumed under previous results, we must show that $\mathcal{C}$ is not contained in $\mathcal{S}$. In fact, we have the following, stronger, result.

THEOREM 2. *The set $\mathcal{C}$ properly contains the set $\mathcal{S}$.*

2. The proof of Theorem 2. Before proving this theorem, we introduce some notation. If G is a group, and H is a subset of G, we write $\langle H \rangle$ for the group generated by the elements of H. If $x_1, \ldots, x_t \in G$, we write $\langle x_1, \ldots, x_t \rangle$ to mean $\langle \{x_1, \ldots, x_t\} \rangle$. Similarly, if K is a subset of G, we put $\langle H, K \rangle$ for $\langle H \cup K \rangle$. And, we denote the group of automorphisms of G by $\operatorname{Aut} G$, the order of G by $|G|$, and the order of x_1 by $|x_1|$. Finally, let $\mathbb{Z}_n$ be the cyclic group of order n, and let $G \otimes L$ denote the direct product of the groups G and L.

Proof of Theorem 2. To show that $\mathcal{C}$ contains $\mathcal{S}$, we apply Lemma 3 on p. 5 of [4], with $y = 4$. To establish that this containment is proper, we consider the example of $n = 7^2 97^2$. Clearly, n is cubefree, odd, and satisfies Properties 1 and 2. Thus, it suffices to prove that $g(n) = 7$. Let G be any group of order n. By the Sylow theorems, G has a normal Sylow 97-subgroup P, and a Sylow 7-subgroup Q. Clearly, $|P| = 97^2$, and $|Q| = 7^2$. Let the elements of Q act on the elements of P by conjugation. We have two cases, according to whether all of the elements of Q act trivially on P.

Case (i): The elements of Q all act trivially on P. Since P and Q intersect trivially, it follows that $\langle P, Q \rangle$ is the direct product of P and Q. Moreover, both this direct product and G have order $7^2 97^2$, so that G is this direct product. By the Fundamental Theorem on Abelian Groups, G is one of the groups $\mathbb{Z}_n$, $\mathbb{Z}_{n/7} \otimes \mathbb{Z}_7$, $\mathbb{Z}_{n/97} \otimes \mathbb{Z}_{97}$, or $\mathbb{Z}_7 \otimes \mathbb{Z}_7 \otimes \mathbb{Z}_{97} \otimes \mathbb{Z}_{97}$.

Case (ii): At least one element of Q does not act trivially on P. Then 7 divides $|\operatorname{Aut} P|$. And, since $|P| = 97^2$, P is either cyclic or isomorphic to $\mathbb{Z}_{97} \otimes \mathbb{Z}_{97}$. In the first case, $|\operatorname{Aut} P| = 97 \cdot 96$ is not divisible by 7. In the

second case, Aut P is isomorphic to the group of 2 by 2 nonsingular matrices over the field of 97 elements, acting on the two-dimensional column vectors over this field.

In particular, the order of Aut P is $(97^2-1)(97^2-97)$, which is exactly divisible by 7^2. By the proof of Theorem 8.3 on p. 42 of [4], Aut P contains a cyclic subgroup of order $97^2-1 = 7^2 \cdot 192$, so that the Sylow 7-subgroups of Aut P are cyclic of order 7^2. Since Q does not act trivially on P, the kernel of this action has order either 7 or 1. If the kernel has order 1, then Q must be cyclic. So, $\langle P, Q\rangle$ is isomorphic to the semidirect product of P by an automorphism of P of order 7^2. But since 7^2 exactly divides $|\mathrm{Aut}\, P|$, and since 7 does not divide $|P|$, the semidirect product of P by any automorphism of order 7^2 is isomorphic to $\langle P, Q\rangle$. And, as in our earlier cases, we have $\langle P, Q\rangle = G$. Thus, there exists a unique group, up to isomorphism, with the kernel of the aforementioned action trivial.

So, assume that the kernel has order 7. Let x be a nontrivial element of this kernel, and let y be an element of Q not belonging to the kernel. If Q is not cyclic, then we have $Q = \langle x, y\rangle$, so that Q is the direct product of $\langle x\rangle$ and $\langle y\rangle$.

Since $|Q| = 49$, Q is the direct product of $\langle x\rangle$ and $\langle y\rangle$. Thus, $G = \langle P, Q\rangle$ is the direct product of $\langle P, \langle y\rangle\rangle$ and $\langle x\rangle$. Hence, G is isomorphic to the direct product of $\mathbb{Z}_7$ with the semidirect product of P by an automorphism of P of order 7. As in the situation in the last paragraph, any group which is the direct product of $\mathbb{Z}_7$ with a semidirect product of P by an automorphism of P of order 7, must be isomorphic to G. Hence, there exists a unique group, up to isomorphism, with the kernel of the action of Q on P having order 7, and with Q noncyclic.

Finally, assume that this kernel has order 7, but that Q is cyclic. Then $Q = \langle x\rangle$. So, x^7 acts trivially on P, whereas x does not. Consider the semidirect product of P by the automorphism of Aut P given by the action of x on P. That group is generated by the normal subgroup, which we identify with P and write as P, and an element y of order 7 for which

$$y^{-1}gy = x^{-1}gx \quad \text{for each } g \in P.$$

Consider the direct product of $\mathbb{Z}_{49}$ with this semidirect product, and write it as

$$\langle y, w, P\rangle, \tag{6}$$

where w has order 49 and commutes with $\langle y, P\rangle$. By inspection, we have

$$(wy)^{-1}g(wy) = x^{-1}gx \quad \text{for all } g \in P, \tag{7}$$

and $|wy| = 49$. Therefore, $\langle wy, P\rangle$ and $\langle x, P\rangle$ are isomorphic. Moreover, we have shown that all subgroups of Aut P of order 7 are conjugate, so that any two semidirect products of P by an automorphism of order 7 are

isomorphic. Hence, there is at most one such group (up to isomorphism). To show that there is such a group, let η be any automorphism of P of order 7, construct the semidirect product of P by η, and find the element y of the semidirect product which acts on the Sylow 97-subgroup by conjugation as η acts on P. Then, construct the direct product (6), and consider the element wy as in (7). The group $\langle wy, P\rangle$ has order $7^2 97^2$, and has the asserted form.

Accordingly, there is a unique isomorphism class of groups G with cyclic Sylow 7-subgroups, where the action of a Sylow 7-subgroup on the Sylow 97-subgroup has a kernel of order 7. Taking each sub-case into account, and totalling the results, gives $g(n) = 7$. ∎

N o t e. As an alternate proof, one could construct the semidirect product of P by $\operatorname{Aut} P$ with $\operatorname{Aut} P$ represented as the aforementioned group of matrices, and then find all subgroups of order 97^2, $7^1 97^2$, and $7^2 97^2$. In each case, one could take the direct product with a group of order a power of 7, and study possible subgroups G of the right order. Then, examination of Cayley tables would yield the theorem, after some argument reducing the number of cases to study.

3. Graphs associated with odd cubefree numbers. For the remainder of this paper, n will denote an odd cubefree positive integer. For convenience of exposition, we associate with n the following digraph.

Definition. Associate with n the digraph $\mathcal{G}(n)$ whose vertices are the nontrivial prime powers exactly dividing n, and whose edges are determined by the following rules: If p^k and q^l are nontrivial prime powers exactly dividing n, then

(i) place one directed edge from p^k to q^l if $k = 1$ and $p \mid q-1$ or if $k = 1$, $l \geq 2$, and $p \mid q+1$;

(ii) place one directed edge from p^k to q^l if $p \parallel q-1$ or if $l = 2$, and $p \parallel q+1$;

(iii) place two directed edges from p^k to q^l if $k = 2$ and $p^2 \mid q-1$;

(iv) place two directed edges from p^k to q^l if $k = 2$, $l \geq 2$, and $p^2 \mid q+1$.

N o t e. If $p \mid q-1$ or $p \mid q+1$, then there is at least one directed edge from p to q.

Definition. Let m and n be odd positive cubefree integers. We say that the digraphs $\mathcal{G}(m)$ and $\mathcal{G}(n)$ are *equivalent*, and write $\mathcal{G}(m) \sim \mathcal{G}(n)$, if there exists a bijection $\mathcal{B}$ from the vertices of $\mathcal{G}(m)$ to the vertices of $\mathcal{G}(n)$ such that if p^k and q^l are vertices of $\mathcal{G}(m)$, then there are the same number of directed edges from p^k to q^l in $\mathcal{G}(m)$ as there are from $\mathcal{B}(p^k)$ to $\mathcal{B}(q^l)$ in $\mathcal{G}(n)$, and such that $\mathcal{B}(p^k)$ is the kth power of a prime for all vertices p^k of $\mathcal{G}(m)$.

We put $\widetilde{\mathcal{G}}(n)$ for the equivalence class containing $\mathcal{G}(n)$.

Definition. Write $\mathcal{G}(n)$ as the disjoint union of its connected components, thus:

$$\mathcal{G}(n) = \bigcup_{i=1}^{t} \mathcal{G}_i.$$

Let n_i be the product of the vertices of $\mathcal{G}_i$, for $1 \le i \le t$. We say that the integers n_i are the *connected components* of n. It follows from the definition of $\mathcal{G}(n)$ that $(n_i, n/n_i) = 1$ for all i.

Notes. Our goal is to show that $g(n)$ is completely determined by the equivalence class $\widetilde{\mathcal{G}}(n)$, provided that n fulfills Properties 1 and 2. By inspection, if p and q are any primes, then we have $\mathcal{G}(p^i) \sim \mathcal{G}(q^i)$ for $i = 1, 2$. If m and n are odd and cubefree, and $\mathcal{G}(n) \sim \mathcal{G}(m)$, then m and n have the same number of prime factors. Call this number $\omega(n)$.

Lemma 1. *If the connected components of n are $n_1, \ldots, n_t$, then any group G of order n can be written as the direct product of groups $H_1, \ldots, H_t$ with $|H_i| = n_i$ for all i. It follows that $g(n) = g(n_1) \cdot \ldots \cdot g(n_t)$.*

Proof. For the first statement, we argue by induction on t. The result is clear for $t = 1$. Assume that T is an integer exceeding 1, and that the result is true for $1 \le t \le T - 1$. Since n_T is a connected component of n, we have $(n/n_T, n_T) = 1$. Let G be any group of order n_T. Then, let p and q be any primes with p dividing n/n_T and q dividing n_T, and choose k and m so that p^k exactly divides n/n_T, and q^m exactly divides n_T. Since $|G|$ is odd and cubefree, G is solvable. So, it follows from a theorem of P. Hall (see Theorem 4.1 on p. 231 of [4]), that there is a subgroup H of G, with $|H| = p^k q^m$. In H, the number of Sylow p-subgroups is 1 or q if $m = 1$, and 1, q, or q^2 if $m = 2$. But since n_T is a connected component of n, p divides n/n_T, and q divides n_T, we cannot have $q \equiv 1 \bmod p$, and if $m = 2$ then we cannot have $q^2 \equiv 1 \bmod p$. So, there is only 1 Sylow p-subgroup in H. Call it P. Then P is normal in H. Similarly, Q is normal in H. Thus, $H = P \otimes Q$ (see Theorem 3.6 on p. 11 of [4]). It follows that Q centralizes P. Let P_1 be any Sylow p-subgroup of G, and let C be the centralizer of P_1 in G. Since P is also a Sylow p-subgroup of G, there exists an element $\alpha \in G$ for which $\alpha^{-1} P \alpha = P_1$. We deduce that the Sylow q-subgroup $\alpha^{-1} Q \alpha$ of G is contained in C, so that $q^m \,|\, |C|$. Since $q \,|\, n_T$ was arbitrary, and m is the exact power to which q divides n_T, it follows that $n_T \,|\, |C|$. Moreover, from the fact that $(n_T, n/n_T) = 1$, we can deduce that $(n_T, |C|/n_T) = 1$. Hence, the aforementioned theorem of P. Hall implies the existence of a subgroup K of C, with $|K| = n_T$. Now K is a subgroup of G with $(|K|, n/|K|) = 1$. Moreover, if C_1 is the centralizer of K in G, then C_1 contains a Sylow p-subgroup of G. Now let r be any prime dividing n/n_T. By the above argument, there exists a subgroup K_1 of G for which

the centralizer of K_1 in G contains a Sylow r-subgroup of G. But K and K_1 are conjugate in G, by P. Hall's Theorem. Accordingly, C_1 contains a Sylow r-subgroup of G. So, the exact power of r dividing $|C_1|$ equals the power to which r divides n/n_T. Since r was an arbitrary prime divisor of n/n_T, we can conclude that n/n_T divides the order of C_1. Therefore, we can deduce from P. Hall's Theorem that C_1 contains a subgroup M of order n/n_T. Now M centralizes K in G, and $|M|$ and $|K|$ are coprime. Hence, $M \cap K$ is trivial. Therefore, $\langle M, K\rangle = M \otimes K$. And, $|M|\,|K| = n = |G|$, whence $G = M \otimes K$. It follows from the Induction Hypothesis that M is the direct product of subgroups $H_1, \ldots, H_{T-1}$ of M, with $|H_i| = n_i$ for $1 \leq i \leq T-1$. So, the initial statement of the lemma holds with $H_T = K$. For the second statement, we note that if $G = H_1 \otimes \ldots \otimes H_T$, with $|H_i| = n_i$ for $1 \leq i \leq T$, then H_i is the unique subgroup of G of order n_i. And, if $H_1, \ldots, H_T$ are any groups with $|H_i| = n_i$ for $1 \leq i \leq T$, then we clearly have $|H_1 \otimes \ldots \otimes H_T| = n$. ∎

The next lemma will enable us to anchor the induction when proving that if n satisfies Properties 1 and 2, then $g(n)$ depends only on $\widetilde{\mathcal{G}}(n)$ (see Lemma 5, below).

LEMMA 2. *Let p and q be primes with $q > p > 3$. Then*

(i) $g(p) = 1$,
(ii) $g(p^2) = 2$,
(iii) $g(pq) = 2$ *if* $p \,|\, q-1$,
(iv) $g(pq^2) = 3$ *if* $p \,|\, q+1$,
(v) $g(p^2q) = 4$ *if* $p \,\|\, q-1$,
(vi) $g(p^2q) = 5$ *if* $p^2 \,|\, q-1$,
(vii) $g(p^2q^2) = 6$ *if* $p \,\|\, q+1$,
(viii) $g(p^2q^2) = 7$ *if* $p^2 \,|\, q+1$.

COROLLARY 1. *If $\omega(n) \leq 2$, and n satisfies Property* 1, *then $g(n)$ depends only on $\widetilde{\mathcal{G}}$.*

Proof. For $\omega(n) = 1$, we have $n = p$ or $n = p^2$ for some prime p. So, $\mathcal{G}(n) \sim \mathcal{G}(s)$ or $\mathcal{G}(n) \sim \mathcal{G}(s^2)$. Parts (i) and (ii) of Lemma 2 imply that $g(n) = 1$ in the first instance, and $g(n) = 2$ in the second case. Otherwise, write $n = p^\alpha q^\beta$, where p and q are primes with $q > p > 2$, and $\alpha, \beta \in \{1, 2\}$. If n has two connected components, then the connected components of n are p^α and q^β, and $\mathcal{G}(n)$ is equivalent to $\mathcal{G}(m)$, for some element m of $\{5 \cdot 7, 5^2 \cdot 7, 5^2 \cdot 7^2\}$. In each case, we can conclude from Lemma 1 and Lemma 2(i), (ii) that $g(n) = g(p^\alpha)g(q^\beta) = g(m)$. Now, assume that n is connected. We observe that since n is odd, and $q > p \geq 3$, we have neither $q \,|\, p+1$ nor $q \,|\, p-1$. And, we can conclude from the fact that n fulfills Property 1 that $p \nmid q-1$ if $\beta = 2$. Therefore, the connectedness of n implies

that $\mathcal{G}(n)$ is contained in one of the equivalence classes $\widetilde{\mathcal{G}}(m) : m = 5 \cdot 11$, $5^2 \cdot 11, 5^2 \cdot 101, 5 \cdot 19^2, 5^2 \cdot 19^2, 7^2 \cdot 97^2$. The corollary now follows from Lemma 2. ∎

Proof of Lemma 2. Cases (i), (ii), and (iii) are listed as I–III on p. 51 of [5]. For the remainder, we observe that if $2 < p < q$; $\alpha, \beta \in \{1, 2\}$; and G is a group of order $p^\alpha q^\beta$, then the number of Sylow q-subgroups of G is 1, p, or p^2. Since this number is congruent to 1 modulo q, it follows that under the hypotheses of any of cases (iv)–(viii), there exists a normal Sylow q-subgroup of any group of the given order. We first consider the cases (v) and (vi). Here, G has order p^2q. Now the Sylow q-subgroup of G is cyclic of order q. Let $x \in G$ be a generator of this subgroup, and let P be a Sylow p-subgroup of G. Let P act on $\langle x \rangle$ by conjugation. The kernel of this action has order 1, p, or p^2. If the action is trivial, then we have $G = P \otimes \langle x \rangle$, so that G is isomorphic to one of the groups

$$\mathbb{Z}_p \otimes \mathbb{Z}_p \otimes \mathbb{Z}_q, \qquad \mathbb{Z}_{p^2} \otimes \mathbb{Z}_q. \tag{8}$$

If the kernel of this action has order p, then there exists an element y of P of order p, for which y and x commute. We have two cases: either P is cyclic, or P is noncyclic. In the latter case, there is an element z of P such that $|z| = p$, and $P = \langle y, z \rangle$. Now z does not commute with x, since P does not commute with x. So, since $\langle x \rangle$ is normal in G, $\langle z, x \rangle$ is a nonabelian group of order pq. Consequently, $G = \langle y \rangle \otimes \langle z, x \rangle$. So, up to isomorphism, we have

$$G = \mathbb{Z}_p \otimes \mathbb{N}_{pq}, \tag{9}$$

where $\mathbb{N}_{pq}$ is the nonabelian group of order pq. In the former case, let $P = \langle w \rangle$, where w has order p^2, and $w^p = y$. Hence, w^p fixes x. Since $\langle x \rangle$ is normal, we have $w^{-1}xw = x^m$ for some primitive pth root m of 1 modulo q. Now the action of w on $\langle x \rangle$ gives rise to an automorphism of $\langle x \rangle$ of order p. The semidirect product of $\langle x \rangle$ by this automorphism is isomorphic to

$$N = \langle v, x : v^p = x^q = 1,\ v^{-1}xv = x^m \rangle. \tag{10}$$

Consider the direct product

$$\begin{aligned} &\mathbb{Z}_{p^2} \otimes N \\ &\qquad \simeq \langle u, v, x : u^{p^2} = v^p = x^q = 1,\ v^{-1}xv = x^m,\ uv = vu,\ ux = xu \rangle. \end{aligned} \tag{11}$$

The subgroup

$$\langle uv, x \rangle \tag{12}$$

of $\mathbb{Z}_{p^2} \otimes N$ is isomorphic to G by the sentence containing (10). So, we have exactly one group of order p^2q in this case (up to isomorphism), and it is the subgroup (12). Lastly, we consider what happens when the kernel has order 1. Then, P acts faithfully on $\langle x \rangle$. Now $\operatorname{Aut}\langle x \rangle \simeq \operatorname{Aut} \mathbb{Z}_q$ is cyclic of

order $q-1$, so that P must be cyclic. By analogy with the derivation of (10) or by Theorem 9.4.3 on p. 146 of [5], we can conclude that

$$G = \langle w, x : w^{p^2} = x^q = 1,\ w^{-1}xw = x^m \rangle, \tag{13}$$

where m is a primitive p^2th root of 1 modulo q. To show that G is unique, we recall the result that if k is any other primitive p^2th root of 1 modulo q, and if d is an integer satisfying $k^d \equiv m \bmod q$, then the group $\langle u, v : u^{p^2} = v^q = 1, u^{-1}vu = v^k \rangle$ is isomorphic to G, under the isomorphism $v \mapsto x$, $u^d \mapsto w$. To show when G exists, we can construct the semidirect product of $\mathbb{Z}_q$ by an element of $\operatorname{Aut} \mathbb{Z}_q$ of order p^2, if such an element exists. Since $\operatorname{Aut} \mathbb{Z}_q$ is cyclic of order $q-1$, the group (13) exists and has order p^2q in case (vi), but not in case (v). So, in case (v), we have the four isomorphism classes of groups given by (8), (9), and (12), and no others, while in case (vi), we have the groups listed in (8), (9), (12), and (13), and no more isomorphism classes of groups.

For (viii), we can reason as in the proof that $g(7^2 97^2) = 7$, in the proof of Theorem 2. We leave the details to the reader. For (vii), the argument is the same as in (viii), but one case does not arise, namely the case analogous to the situation where the kernel is trivial in the proof that $g(7^2 97^2) = 7$. The reason that case does not give any groups is similar to the reason that we get one more isomorphism class of groups in case (vi) than we get in case (v). Again, we leave it to the reader to put in the details. For (iv), we observe that if G is a group of order pq^2, then $G \otimes \mathbb{Z}_p$ is a group of order p^2q^2. Accordingly, the reader who has done (vii) and (viii) immediately has (iv). ∎

LEMMA 3. *Assume that n satisfies Properties* 1 *and* 2. *Let q and r be distinct odd primes, and let α and β be contained in $\{1, 2\}$. Assume that in the notation of Property* 2, *we have*

$$M(n, q) = M(n, r) = N(n, q) = N(n, r) = 0, \tag{14}$$

and that

$$(qr, n) = (r^i - 1, n) = 1, \tag{15}$$

but that

$$q \,|\, r + (-1)^\alpha. \tag{16}$$

Finally, suppose that

$$(n, q-1) = 1 \quad \text{if } \alpha = 2. \tag{17}$$

Then

$$g(nq^\alpha r^\beta) = g(nq^\alpha)g(r^\beta) + g(n)(g(q^\alpha r^\beta) - g(q^\alpha)g(r^\beta)). \tag{18}$$

P r o o f. Let G be any group of order $nq^\alpha r^\beta$. Since $|G|$ is odd and cube-free, G is solvable. So, it follows from P. Hall's Theorem that G contains a subgroup H of order nr^β. Let R be a Sylow r-subgroup of H. Consider any prime divisor s of n. Choose γ so that s^γ exactly divides n. Another application of P. Hall's Theorem implies that R is contained in a subgroup S of H, with $|S| = r^\beta s^\gamma$. It follows from the Sylow theorems and (14) that R is normal in S. Now if $\beta = 1$, then R is isomorphic to $\mathbb{Z}_r$, while if $\beta = 2$, then r is either isomorphic to $\mathbb{Z}_{r^2}$, or to $\mathbb{Z}_r \otimes \mathbb{Z}_r$. Thus, there exists no automorphism of R of order either s or s^2. So, a Sylow s-subgroup of S centralizes R. Let C be the centralizer of R in H. We have shown that $s^\gamma \,|\, |C|$. Since s^γ was an arbitrary nontrivial prime power exactly dividing n, we deduce that $n \,|\, |C|$. But n and $|C|/n = r^\beta$ are clearly coprime. Hence, P. Hall's Theorem guarantees the existence of a subgroup K of C with $|K| = n$. A further application of P. Hall's Theorem yields the existence of a subgroup L of G of order $q^\alpha r^\beta$, with $R \subseteq L$. We can conclude from (16) and the Sylow theorems that R is normal in L. Consequently, the order of the normalizer of R in G is divisible by both $|L|$ and $|K|$. Now since $|G| = |K|\,|L|$, and $|K|$ and $|L|$ are coprime, we can conclude that $G = \langle K, L\rangle$. Hence, R is normal in G.

By P. Hall's Theorem, there is a subgroup M of G with $|M| = nq^\alpha$, and with $K \subseteq M$. Let Q be a Sylow q-subgroup of M. The reasoning of the last paragraph shows that Q is normal in M, and that $M = \langle K, Q\rangle$. So, $G = \langle K, Q, R\rangle$. Since R is normal in G, the set

$$QR = \{gh : g \in Q,\ h \in R\} \tag{19}$$

forms a group of order $|Q|\,|R| = q^\alpha r^\beta$.

If Q centralizes R, then M centralizes R because M is generated by K and Q. Furthermore, M and R intersect trivially, because their orders are coprime. Thus,

$$G = \langle M, R\rangle = M \otimes R. \tag{20}$$

If Q does not centralize R, then we will establish that

$$G = K \otimes QR. \tag{21}$$

Then, we will use the fact that at least one of (20) and (21) holds to enable us to apply the Inclusion/Exclusion Principle to enumerate the groups of order $nq^\alpha r^\beta$.

Assume that Q fails to centralize R. Then QR is a nonabelian group of order $q^\alpha r^\beta$. We have the following cases:

(i) $\alpha = 1$;
(ii) $\alpha = 2$, Q is cyclic;
(iii) $\alpha = 2$, Q is not cyclic.

Our goal in each case will be to verify that K centralizes Q. It will follow at

once that K centralizes QR, so that (21) holds. If K does not centralize Q, then there is some element z of K of prime power order s^γ, such that z does not commute with every element of Q. Clearly, z commutes with every element of R.

If $Q \simeq \mathbb{Z}_q$, write $Q = \langle w \rangle$. Consider $x = zwz^{-1}w^{-1}$. If $h \in R$, then we have

$$x^{-1}hx = wzw^{-1}(z^{-1}hz)wz^{-1}w^{-1} = w(z(w^{-1}hw)z^{-1})w^{-1} = h, \tag{22}$$

because z centralizes R. But $zwz^{-1} = w^\alpha$ for some integer $a \not\equiv 1 \bmod q$. Thus, $x = w^{\alpha-1}$ is a generator of Q. It follows that Q centralizes R which is a contradiction. Accordingly, (21) holds in case (i).

Now, assume that $\alpha = 2$. Then there is no prime divisor p of n with $q \equiv 1 \bmod p$, by (14). But if Q is cyclic, then we must have $s \,|\, |\mathrm{Aut}\, Q| = q(q-1)$, because z has order s^γ. Thus, we have a contradiction in case (ii).

If $|Q| = q^2$, then $Q \simeq \mathbb{Z}_q \otimes \mathbb{Z}_q$. As in the last paragraph, we have $s \,|\, |\mathrm{Aut}\, Q|$. Thus, $s \,|\, q+1$. If z centralized some nontrivial element a of Q, then conjugation of Q by z would generate an automorphism η of $Q/\langle a \rangle$. Now η would have order 1, s, or s^2, since $|z| = s^\gamma$. Moreover, since $|a| = q$, the order of η would divide $|\mathrm{Aut}\langle a \rangle| = q-1$. So, η would have to be trivial. It would follow that z centralizes Q (see Theorem 3.15 on p. 187 of [4]), contrary to assumption. So, $\{g \in Q : zg = gz\} = 1$.

Now, let v and w be any nontrivial elements of Q, and let $x = zvz^{-1}v^{-1}$, and $y = zwz^{-1}w^{-1}$. By the derivation of (22), both x and y commute with R. Moreover, by the last paragraph, both x and y are nontrivial elements of Q. If $y = x^j$ for some integer j, then $zvz^{-1}v^{-1} = (zwz^{-1}w^{-1})^j$. Since both zwz^{-1} and w^{-1} are elements of Q, and Q is abelian, we have $zvz^{-1}v^{-1} = (zwz^{-1})^j w^{-j}$. Therefore, $zvz^{-1}v^{-1} = zw^j z^{-1}w^{-j}$. Simplification yields $w^{-j}vz^{-1}v^{-1}w^j z = 1$, so that z commutes with $v^{-1}w^j$. Consequently, $v^{-1}w^j$ is trivial, from which we get $w^j = v$. Accordingly, we have shown that if we choose v and w to be generators of Q, then the elements x and y are also generators of Q, so that R commutes with Q. It therefore follows that (20) holds, from the paragraph containing it. Thus, at least one of Equations (20) and (21) holds in case (iii).

We are now ready to apply the Inclusion/Exclusion Principle. If both (20) and (21) are true, then we have

$$G = M \otimes R = K \otimes QR.$$

From the pairwise coprimality of $|K|$, $|Q|$, and $|R|$, we can deduce that

$$G = K \otimes Q \otimes R \tag{23}$$

in this case. So, we have

$$g(|G|) = N_1 + N_2 - N_3, \tag{24}$$

where N_i is the number of (isomorphism classes of) groups G of the form given by Equation $(20+i)$, for $i = 1, 2, 3$. But since $|M|$ and $|R|$ are coprime, the number of groups of the form $M \otimes R$ is just $g(|M|)g(|R|)$. Similarly, the number of groups of the form $K \otimes QR$ is $g(|K|)g(|QR|)$, and the number of groups of the form $K \otimes Q \otimes R$ is merely $g(|K|)g(|Q|)g(|R|)$. Consequently, (18) follows from (24). ∎

Lemma 4. *Let n have connected components $n_1, \ldots, n_t$, assume that p is an odd prime, and choose $\alpha \in \{1, 2\}$. Suppose that $n_i p^\alpha$ is connected and that p^α is the unique vertex of $\mathcal{G}(n_i p^\alpha)$ of out-degree 0, for $1 \le i \le t$. Further assume that np^α satisfies Properties 1 and 2.*

(i) *If $\alpha = 1$, then $g(np^\alpha) = \prod_{i=1}^{t} g(n_i, p)$.*
(ii) *If $\alpha = 2$, then $g(np^\alpha) = \prod_{i=1}^{t}(g(n_i, p^2) - g(n_i)) + g(n)$.*

Proof. By construction, the vertex p^α of $\mathcal{G}(np^\alpha)$ has out-degree 0. Select any group G of order np^α. Choose an arbitrary prime power q^β exactly dividing n. By P. Hall's Theorem, there is a subgroup H of G with $|H| = p^\alpha q^\beta$. Since the number of Sylow p-subgroups of H is congruent to 1 modulo p and divides q^β, and since the vertex p^α of $\mathcal{G}(np^\alpha)$ has out-degree 0, there is only one Sylow p-subgroup of H. Call it P, and denote its normalizer in G by N. Let P_0 be any Sylow p-subgroup of G, and denote its normalizer in G by N_0. Since any two Sylow p-subgroups of G are conjugate, N is conjugate to N_0, so that $|N_0| = |N|$. And, inasmuch as $H \subseteq N_0$, we have $pq^\beta \,||N|$. But q^β was an arbitrary prime power exactly dividing n. Hence, $np^\alpha \,||N|$, so that $N = G$. It follows that $P = P_0$ is normal in G.

By P. Hall's Theorem, there is a subgroup K of G with $|K| = n$. Moreover, by Lemma 1, there are subgroups $A_1, \ldots, A_t$ of K for which

$$|A_i| = n_i \quad \text{for } 1 \le i \le t, \tag{25}$$

and

$$K = A_1 \otimes \ldots \otimes A_t. \tag{26}$$

Since P is normal in G, we have

$$|\langle A_i, P\rangle| = |A_i|\,|P| = n_i p^\alpha \quad \text{for } 1 \le i \le t. \tag{27}$$

Assume that $\alpha = 1$. We will prove (i) by induction on t. For $t = 1$, the result is clear. Assume that the result holds for $1, 2, \ldots, t-1$, where $t > 1$. Let A and B be groups with $|A| = (n/n_1)p$, and $|B| = n_1 p$. By the argument of the first paragraph, each of the groups A and B possesses a normal Sylow p-subgroup. In each case, this group is isomorphic to $\mathbb{Z}_p$, since $g(p) = 1$. Let $\langle a\rangle$ be the Sylow p-subgroup of A, and $\langle b\rangle$ be the Sylow p-subgroup of B. Then $A \otimes B$ has a normal Sylow p-subgroup, namely

$$\langle a\rangle \otimes \langle b\rangle = \langle a, b : a^p = b^p = a^{-1}b^{-1}ab = 1\rangle.$$

Identify A and B with their images under the natural embeddings of A and B into $A \otimes B$. Then A normalizes $\langle ab \rangle$, since A normalizes $\langle a \rangle$, and centralizes $\langle b \rangle$. Similarly, B normalizes $\langle ab \rangle$. By P. Hall's Theorem, there exists a subgroup D of A with $|D| = n_1$, and a subgroup E of B with $|E| = n/n_1$. Then $D \otimes E$ is a subgroup of $A \otimes B$ of order n. Since $\langle ab \rangle$ is normalized by both A and B, it is normalized by $D \otimes E$. Accordingly, we can deduce that

$$|\langle D, E, \langle ab \rangle \rangle| = |D|\,|E|\,|\langle ab \rangle| = np$$

from the fact that $|\langle ab \rangle|$ is coprime to $|D \otimes E|$. Thus,

$$g(np) \leq g(n,p)g((n/n_1)p).$$

By the Induction Hypothesis, we have

$$g(np) \leq \prod_{i=1}^{t} g(n_i p).$$

On the other hand, equation (27) and its derivation yield

$$g(np) \geq \prod_{i=1}^{t} g(n_i p),$$

which completes the induction and proves (i).

Suppose that $\alpha = 2$. We will establish (ii) by verifying the following two formulae:

(iii) The number of isomorphism classes of groups of order np^α with a cyclic Sylow p-subgroup is $g(n)$;

(iv) The number of isomorphism classes of groups of order np^α with a noncyclic Sylow p-subgroup is $\prod_{i=1}^{t}(g(n_i p) - g(n_i))$.

Assume that $P \simeq \mathbb{Z}_{p^2}$. Then $|\mathrm{Aut}\, P| = p(p-1)$. Since np^2 satisfies Property 1, there exists no prime divisor q of n with $q \,|\, |\mathrm{Aut}\, P|$. Therefore, if z is any element of G of order coprime to p, then z acts trivially on P by conjugation, whence K centralizes P. Consequently, $G = K \otimes P$. Conversely, if K is any group of order n, then $K \otimes \mathbb{Z}_{p^2}$ has order np^2. And, if K_1 and K_2 are groups of order n, then $K_1 \otimes P$ and $K_2 \otimes P$ are isomorphic if and only if K_1 is isomorphic to K_2, because $K_i \simeq K_i \otimes \mathbb{Z}_{p^2}/\mathbb{Z}_{p^2}$ for all i. Accordingly, (iii) holds.

Now, suppose that $P \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Then each of the groups $\langle A_i, P \rangle$ in (27) has a noncyclic Sylow p-subgroup, and no two of these groups have the same order. Furthermore, if F_i is any subgroup of G of order $n_i p^2$, then F_i is conjugate to $\langle A_i, p \rangle$ in G, by P. Hall's Theorem. In particular,$F_i \simeq \langle A_i, P \rangle$. Consequently, the isomorphism class of each group $\langle A_i, P \rangle$ is determined

completely by G. So, we deduce from (iii) that

$$g(n) \geq \prod_{i=1}^{t} (g(n_i p^2) - g(n_i)). \tag{28}$$

On the other hand, if $E_1, \ldots, E_t$ are any groups with $|E_i| = n_i p^2$ for $1 \leq i \leq t$, each of which possesses a noncyclic Sylow p-subgroup $P_i = \langle x_i, y_i \rangle$ (where $x_i^p = y_i^p = x_i^{-1} y_i^{-1} x_i y_i = 1$), then we argue as in the first paragraph of the proof of this lemma that P_i is normal in E_i for all i. Now P. Hall's Theorem guarantees the existence of a subgroup D_i of E_i with $|D_i| = n_i$, for all i. Embed each group E_i in $E_1 \otimes \ldots \otimes E_t$ in the canonical manner. Consider the elements $x = x_1 \cdot \ldots \cdot x_t$, and $y = y_1 \cdot \ldots \cdot y_t$. Then for all i, the action of E_i on $\langle x, y \rangle$ by conjugation is identical to the action of E_i on $\langle x_i, y_i \rangle$ by conjugation, since E_i centralizes x_j and y_j for $j \neq i$. It follows that $\langle x, y \rangle$ is normal in $E_1 \otimes \ldots \otimes E_t$. Consequently,

$$|\langle D_1, \ldots, D_t, \langle x, y \rangle \rangle| = np^2,$$

and $\langle x, y \rangle$ is a noncyclic Sylow p-subgroup of $\langle D_1, \ldots, D_t, \langle x, y \rangle \rangle$. Thus, (28) holds with $\geq$ replaced by $\leq$. ∎

The next lemma shows the importance of Properties 1 and 2 for the estimation of $C_k(x)$.

Lemma 5. *Let m and n be odd cubefree positive integers, both satisfying each of Property* 1 *and Property* 2. *If $\mathcal{G}(m) \sim \mathcal{G}(n)$, then $g(m) = g(n)$.*

Proof. We argue by induction on $\omega(n)$. If $\omega(n) = 1$, then the desired conclusion follows from the notes preceding Lemma 1. Otherwise, let $\mathcal{B}$ be a bijection from the vertices of $\mathcal{G}(m)$ to the vertices of $\mathcal{G}(n)$, for which there are the same number of directed edges from v to w in $\mathcal{G}(m)$ as there are from $\mathcal{B}(v)$ to $\mathcal{B}(w)$ in $\mathcal{G}(n)$ for every pair of vertices v, w of $\mathcal{G}(m)$ and such that $\mathcal{B}$ maps primes to primes and maps squares to squares. If m has more than one connected component, let the connected components of m be $m_1, \ldots, m_t$. Then, by construction $\mathcal{B}$ maps connected components to connected components. In detail, if for all i, n_i is the product of the vertices $\mathcal{B}(v)$ of n as v ranges over the nontrivial prime powers exactly dividing m_i, then $n_1, \ldots, n_t$ are the connected components of n. Therefore, the Induction Hypothesis yields $g(m_i) = g(n_i)$ for all i. Moreover, we can conclude from Lemma 1 that $g(m) = g(m_1) \cdot \ldots \cdot g(m_t)$, and that $g(n) = g(n_1) \cdot \ldots \cdot g(n_t)$, so that $g(m) = g(n)$.

Therefore, we may assume that m has exactly one connected component. Then, the same is true of n. If $\omega(n) = 2$, then we can deduce the lemma from Lemma 1 and our definition of equivalence of graphs. Thus, we are allowed to suppose that $\omega(n) \geq 3$. Let r^β be the unique vertex of $\mathcal{G}(m)$ of out-degree 0. Then $\mathcal{B}(r^\beta)$ is the unique vertex of $\mathcal{G}(n)$ of out-degree 0.

Since m has only one connected component, the in-degree of r^m is at least 1. Let $\{q_1^{\alpha_1}, \dots, q_t^{\alpha_t}\}$ be the set of vertices of $\mathcal{G}(m)$ for which there exists at least one edge with v for its initial point, and r^β for its final point. Then $\mathcal{B}(q_1^{\alpha_1}), \dots, \mathcal{B}(q_t^{\beta_t})$ are the vertices V such that there exists at least one edge with initial point V and terminal point $\mathcal{B}(r^\beta)$. If $t = 1$, then we apply Lemma 3 twice, and invoke the Induction Hypothesis, to obtain

$$\begin{aligned} g(m) &= g(mr^{-\beta})g(r^\beta) + g(mq^{-\alpha}r^{-\beta})(g(q^\alpha r^\beta) - g(q^\alpha)g(r^\beta)) \\ &= g(nR^{-\beta})g(R^\beta) + g(nQ^{-\alpha}R^{-\beta})(g(Q^\alpha R^\beta) - g(Q^\alpha)g(R^\beta)) \\ &= g(n), \end{aligned}$$

where $q = q_1$, $Q^\alpha = \mathcal{B}(q_1^\alpha)$, and $R^\beta = \mathcal{B}(r^\beta)$. If $t \geq 2$, denote the connected component of m/r^β containing $q_i^{\alpha_i}$ by m_i, and let n_i be the product of $\mathcal{B}(v)$ as v ranges over the vertices of m_i, for $1 \leq i \leq t$. Then n_i is the connected component of $n/\mathcal{B}(r^\beta)$ containing $q_i^{\alpha_i}$. We now utilize Lemma 4 twice, and apply the Induction Hypothesis, to get the desired result. Thus, if $\beta = 1$, we obtain

$$g(m) = \prod_{i=1}^{t} g(m_i r) = \prod_{i=1}^{t} g(n_i \mathcal{B}(r)) = g(n).$$

If $\beta = 2$, we get

$$\begin{aligned} g(m) &= \prod_{i=1}^{t} (g(m_i r^2) - g(m_i)) + g(mr^{-2}) \\ &= \prod_{i=1}^{t} (g(n_i r^2) - g(n_i)) + g(n\mathcal{B}(r^2)^{-1}) = g(n). \ \blacksquare \end{aligned}$$

4. Further preliminary results. Fix $k \in \mathcal{C}$ throughout the remainder of this paper. Our primary goal in this section is to produce a sufficiently dense set of positive cubefree integers at which the group-counting function assumes the value k (see Lemma 10, as well as the proof of Theorem 1, below). Our construction relies partly on the following theorem of Linnik [7] on the least prime in an arithmetic progression.

LEMMA 6. *There exist positive absolute constants c_1 and c_2 such that if h and l are any coprime integers with $l > 0$, then the smallest prime $p \equiv h \bmod l$ satisfies $p \leq c_2 l^{c_1}$.*

Jing-Run Chen and J.-M. Liu [1] have published a proof that Lemma 6 holds with $c_1 = 13.5$. D. Roger Heath-Brown holds the present record, namely $c_1 = 5.5$ (see Theorem 6 on p. 269 of [6]). For more data, we refer the reader to the introduction to [6].

Lemma 7. *Assume that y is a sufficiently large positive real number. (Here, sufficiently large may depend on k.) Then there are positive constants c_3 and ω, depending only on k, for which there exists a positive integer n, for which Properties* 1 *and* 2 *hold, satisfying the following* 3 *criteria*:

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

Proof. Assume that y is a real number exceeding 10. Now since $k \in \mathcal{C}$, there must be an odd cubefree integer m satisfying Properties 1 and 2, such that

$$g(m) = k. \tag{29}$$

Suppose that the prime factorization of m is

$$m = \prod_{i=1}^{\omega} q_i^{\alpha_i}, \tag{30}$$

and that

$$2 < q_1 < \ldots < q_\omega. \tag{31}$$

Then if $1 \le j < i \le \omega$, exactly one of the following statements obtains:

$$q_j \text{ divides neither } q_i + 1 \text{ nor } q_i - 1; \tag{32}$$

$$\alpha_i = \alpha_j = 1, \quad q_i \equiv 1 \bmod q_j; \tag{33}$$

$$\alpha_i = 2, \quad \alpha_j = 1, \quad q_i \equiv -1 \bmod q_j; \tag{34}$$

$$\alpha_i = \alpha_j = 2, \quad q_j \parallel q_i + 1; \tag{35}$$

$$\alpha_i = \alpha_j = 2, \quad q_j^2 \mid q_i + 1; \tag{36}$$

$$\alpha_i = 1, \quad \alpha_j = 2, \quad q_j \parallel q_i - 1; \tag{37}$$

$$\alpha_i = 1, \quad \alpha_j = 2, \quad q_j^2 \mid q_i - 1. \tag{38}$$

In addition, in view of (31), the equivalence class $\widetilde{\mathcal{G}}(m)$ to which the graph $\mathcal{G}(m)$ belongs is determined entirely by the exponents $\alpha_1, \ldots, \alpha_\omega$, and by the relationships (32)–(38) for the subscripts i, j with $1 \le j < i \le \omega$.

Recursively select primes $p_1, \ldots, p_\omega$ to fulfill the following conditions:

$$y \le p_1 \le 2y; \tag{39}$$

if $i \le \omega$, and $p_1, \ldots, p_{i-1}$ have been selected, then choose p_i so that

$$p_i \equiv 4 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (32) holds;} \tag{40}$$

$$p_i \equiv 1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (33) holds;} \tag{41}$$

$$p_i \equiv -1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (34) holds;} \tag{42}$$

$$p_i \equiv p_j - 1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (35) holds;} \tag{43}$$

$$p_i \equiv -1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (36) holds;} \tag{44}$$

$$p_i \equiv p_j + 1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (37) holds;} \tag{45}$$

$$p_i \equiv 1 \bmod p_j^{\alpha_j} \quad \text{if } j < i, \quad \text{and (38) holds.} \tag{46}$$

The existence of p_1 is guaranteed by Bertrand's Postulate. Once $p_1, \ldots, p_{i-1}$ have been chosen, the Chinese Remainder Theorem enables us to rewrite the system of $i-1$ simultaneous congruences, given as (40)–(46) as a single congruence modulo $\prod_{j=1}^{i-1} p_j^{\alpha_j}$, since exactly one of the conditions (32)–(38) is true for each pair i, j with $i > j$. And, we can conclude from the last lemma that there exists a solution p_i to this last congruence with

$$p_i \le c_2\Big(\prod_{j=1}^{i-1} p_j^{\alpha_j}\Big)^{c_1}. \tag{47}$$

Choose p_i to satisfy (47) at each stage. Now (40)–(46) imply that $p_i > p_j$, since at least one of the conditions (32)–(38) holds, and because the solution to each congruence (40)–(46) between 1 and $p_j^{\alpha_j}$ is not prime. So,

$$10 < y \le p_1 < \ldots < p_\omega. \tag{48}$$

Let

$$n = \prod_{j=1}^{\omega} p_j^{\alpha_j},$$

so that (ii) holds. By construction, n is odd and has Properties 1 and 2, so that $\mathcal{G}(n)$ is defined. According to the last sentence of the first paragraph of this proof, the graphs $\mathcal{G}(m)$ and $\mathcal{G}(n)$ are equivalent. Consequently, we can deduce (i) from (29) and Lemma 5.

Now $\alpha_j \le 2$ for all j. Accordingly, combining (48) with (47) yields

$$p_i \le c_2\Big(\prod_{j=1}^{i-1} p_{j-1}^2\Big)^2 = c_2 p_{i-1}^{(i-1)c_1\omega}.$$

If $y \ge c_2$, then (48) guarantees that $p_{i-1} \ge c_2$, from which we get

$$p_i \le p_{i-1}^{(i-1)c_1\omega+1} \le p_{i-1}^{(\omega-1)c_1\omega+1}.$$

Since the exponent $(\omega-1)c_1\omega+1$ does not depend upon i, we can iterate this relationship to obtain

$$p_i \le p_1^{((\omega-1)c_1\omega+1)^{i-1}} \qquad \text{for } 1 \le i \le \omega.$$

It therefore follows from (39) that

$$p_i \le (2y)^{((\omega-1)c_1\omega+1)^{i-1}} \le (y^2)^{((\omega-1)c_1\omega+1)^{i-1}} \le y^{c_3}$$

for all i, where $c_3 = 2((\omega-1)c_1\omega+1)^{\omega-1}$. This inequality, combined with (47), yields (iii). ∎

Lemma 8. *Let m and n be odd positive integers with m squarefree and n cubefree, and assume that Properties 1 and 2 hold for n. If*

$$(\phi(m), m) = (\phi(m), n) = (\phi(n), m) = (m, n) = \Big(\prod_{p,\, p^2 \mid n} (p+1), m \Big) = 1, \tag{49}$$

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

Proof. Recall that

$$\phi(h) = \prod_{p \mid h} p^{\nu_p(h)-1}(p-1) \tag{50}$$

for each positive integer h, where $\nu_p(h)$ is the integer for which $p^{\nu_p(h)}$ exactly divides h. Hence, if p is any prime divisor of h, then $p-1$ divides $\phi(h)$. So, $(m, \phi(n)) = 1$ implies that $(m, p-1) = 1$ for every prime divisor p of n. Similarly, we have $(n, p-1) = (m, p-1) = 1$ for every prime p dividing m. In addition, $(p+1, m) = 1$ if $p^2 \mid n$. Accordingly, the fact that n fulfills Properties 1 and 2 insures that mn fulfills Properties 1 and 2. Moreover, mn is odd and cubefree, inasmuch as m is odd and squarefree, n is odd and cubefree, and m and n are coprime. We immediately deduce that $\mathcal{G}(mn)$ exists, and that the connected components of mn are the connected components of n and the prime divisors of m. Consequently, the lemma follows from Lemma 1. ∎

5. The proof of the main theorem

Proof of Theorem 1. Let $k \in \mathcal{C}$, let x be sufficiently large, and set $y = (L_2 x)^2$. According to Lemma 7, there exist positive constants c_2 and c_3, and ω for which the conclusion of that lemma holds for some positive cubefree integer $n = \prod_{i=1}^{\omega} p_i^{\alpha_i}$. In particular,

$$y < p_1 < \ldots < p_\omega < y^{c_3}. \tag{51}$$

As $g(n) = k$, we can conclude from the last lemma that

$$C_k(x) = \sum_{\substack{m, mn \le x \\ (49) \text{ holds}}} 1.$$

If $P(m)$ denotes the smallest prime dividing m, then we must have

$$C_k(x) \ge \sum_{\substack{m \le x/n \\ (49) \text{ holds} \\ P(m) > z}} 1, \tag{52}$$

where

$$z \doteqdot (L_2 x)^{10 c_3} > y^{c_3}.$$

Note that if (49) holds, then $\phi(m)$ is relatively prime to m, so that m is squarefree. Now by (50) and (51), $n\phi(n)\prod_{p,p|n}(p+1)$ has no prime divisor greater than z. Consequently, (52) implies that

$$C_k(x) \geq \sum_{\substack{m\leq x/n \\ (\phi(m),m)=(\phi(m),n)=1 \\ P(m)>z}} 1.$$

The proof of the main theorem of [11] from equation (27) of that paper to the end of Section 3 of that paper is identical to the remainder of the proof of the present Theorem 1. We therefore omit the details. ∎

References

[1] J.-R. Chen and J.-M. Liu, *On the least prime in an arithmetical progression (III), (IV)*, Science in China Ser. A 32 (1989), 654–673, 782–809.

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

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

[4] D. Gorenstein, *Finite Groups*, Series in Modern Mathematics, Harper and Row, New York, 1968, xv+527.

[5] M. Hall, *The Theory of Groups*, Twelfth Printing, The Macmillan Company, New York, 1973, xiv+434.

[6] D. R. Heath-Brown, *Zero-free regions for Dirichlet's L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. 64 (1992), 265–338.

[7] Yu. V. Linnik, *On the least prime in an arithmetic progression. II. The Deuring–Heilbronn Phenomenon*, Rec. Math. [Math. Sbornik] N.S. 15 (57) (1994), 345–368.

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

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

[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] C. A. Spiro-Silverman, *When the group-counting function assumes a prescribed integer value at squarefree integers frequently, but not extremely frequently*, Acta Arith. 61 (1992), 1–12.

MATHEMATICS/SCIENCE DIVISION
BABSON COLLEGE
BABSON PARK, MASSACHUSETTS 02157
U.S.A.

Received on 18.2.1994
and in revised form on 6.9.1994 (2565)