ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

SOME ANALOGUES OF A LEHMER PROBLEM ON THE TOTIENT FUNCTION

M. V. SUBBARAO AND V. SIVA RAMA PRASAD

1. Introduction and notation. In 1932, Lehmer [9] considered the equation

$$M\phi(n) = n - 1, \tag{1.1}$$

where $\phi(n)$ is the Euler totient function and asked whether the sets S_M of integers n satisfying (1.1) have any composite numbers. Obviously in the case $M = 1$, the answer is negative. But the problem is not settled for $M > 1$. However, the following partial solutions are known in the latter case. Firstly, Lehmer himself proved that each member of S_M is odd, squarefree and has at least seven distinct prime factors. Later Lieuwens [10], correcting the proof of Schuh [13], showed that $\omega(n) \geqq 11$ for every $n \in S_M$, where $\omega(n)$ denotes the number of distinct prime factors of n. Kishore [7] increased the lower bound of $\omega(n)$ to 13. Recently, Cohen and Hagis [2], using computational methods, established that $\omega(n) \geqq 14$. In another direction, Pomerance [12] proved that every such n is $< r^{2^r}$, where $r = \omega(n)$, and obtained that the number of $n \leqq x$ in any of S_M with $M > 1$ is

$$O(x^{1/2} \log^{3/4} x \cdot (\log \log x)^{-1/2}).$$

In this paper we discuss two analogous problems involving $J_k(n)$, the Jordan totient function of order k and $\phi^*(n)$, the unitary analogue of the Euler totient function. It is well-known that they are given by $J_k(1) = 1$, $\phi^*(1) = 1$, and if $n > 1$,

$$J_k(n) = n^k \prod_{p \mid n} \left(1 - \frac{1}{p^k}\right), \tag{1.2}$$

$$\phi^*(n) = \prod_{p^\alpha \| n} (p^\alpha - 1), \tag{1.3}$$

where the product in (1.2) is over prime divisors of n and that in (1.3) is

Received by the editors December 15, 1983.
Partially supported by NSERC Grant No. A-3103.

over the prime powers unitarily dividing n. (We say that d unitarily divides n, and write $d \| n$, if $d | n$ and $(d, n/d) = 1$).

We prove that, for $k > 1$, $J_k(n)$ divides $n^k - 1$ if and only if n is a prime (Theorem 1). The case $k = 1$ is Lehmer's unsolved problem, since $J_1(n) = \phi(n)$.

One of the authors [**14**] conjectured in 1971 that $\phi^*(n)$ divides $n - 1$ only if n is the power of a prime, the converse being trivially true. This appears to be as deep as Lehmer's problem. Clearly, the conjecture states that, for every $M \geqq 1$, the set S_M^* of integers n satisfying

$$M\phi^*(n) = n - 1 \tag{1.4}$$

contains only prime powers.

Since S_M, defined earlier, contains only squarefree numbers and $\phi^*(n) = \phi(n)$ wherever n is squarefree, it follows that S_M is a proper subset of S_M^*. Therefore, a separate consideration of S_M^* is needed for the study of the equation (1.4).

First, we dispose of (in Theorem 2) the case $M = 1$ and then go to the case $M > 1$. Some significant features of this paper in the latter case are as follows. In §3, we prove that $\omega(n) \geqq 7$, for every $n \in S_M^*$ by a simple argument which is different from that used by Lehmer for his problem. Using this we improve the lower bounds for $\omega(n)$ with varying conditions on n and various values of M in §4. For instance, we prove that if $3|n$ and $n \in S_M^*$, then $\omega(n) \geqq 1850$, which automatically holds for $n \in S_M$ and therefore improves a theorem of Lieuwens [**10**, Theorem 5] which says that $\omega(n) \geqq 212$ whenever $3|n$ and $n \in S_M$. Also, we establish that if n is squarefree and $n \in S_M^*$, then $\omega(n) \geqq 53$, 140 or 200 according as $M = 5$, 6 or 7; these increase the hitherto known lower bounds, namely 33 of $\omega(n)$ for the Lehmer problem. We mention that these improvements are obtained by using methods different from those of earlier writers for that problem. Further, in §5 we show that if $n \in S_M^*$ has r distinct prime factors, then $n < (r-1)^{2^{r}-1}$ improving a result of Pomerance [**12**, Equation (1.2)]. In §6, an order estimate for $N^*(x)$, the number of $n \leqq x$ in any of S_M^*, with $M > 1$, is obtained by showing

$$N^*(x) = O(x^{1/2} \log^2 x \cdot (\log \log x)^{-2}).$$

$\zeta(s)$ denotes the Riemann-Zeta function. It is well known that, for $s > 1$,

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{1.5}$$

where the product is over all primes and that

$$\zeta(2) = \pi^2/6. \tag{1.6}$$

2. The analogous problem for Jordan's totient function.

THEOREM 1. *For $k > 1$, $J_k(n) | n^k - 1$ if and only if n is a prime.*

PROOF. $J_k(n) | n^k - 1$ implies $(n, J_k(n)) = 1$, and, since $p^2 | n$ for some prime p implies $p^k | J_k(n)$, n must be squarefree. Also $J_k(n) = n^k - 1$ if and only if n is prime. Now, for $k > 1$, by (1.2), (1.5), and (1.6),

$$\frac{n^k - 1}{J_k(n)} < \prod_{p | n}\left(1 - \frac{1}{p^k}\right)^{-1} < \prod_{p}\left(1 - \frac{1}{p^2}\right)^{-1} = \zeta(2) = \pi^2/6 < 2,$$

completing the proof of the theorem.

Thus, the analogue of Lehmer's problem for the Jordan totient function is easily settled. One can consider the analogous problems arising out of other generalizations and analogues of the totient function like Schimmel's. However, we find a most interesting and surprisingly difficult case arising when the unitary totient function is taken. The rest of the paper is devoted to that problem.

3. Analogous problem for the unitary totient. The unitary analogue of Lehmer's problem is already mentioned in the introduction. We obtain a preliminary lower bound for $\omega(n)$, where $n \in S_M^*$, in this section. First, we note

THEOREM 2. *$n \in S_1^*$ if and only if $n = p^\alpha$, for some prime p.*

PROOF. If $n = p^\alpha$, it is in S_1^*. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} (r > 1)$, then $\phi^*(n) < n - 1$, proving the theorem.

Throughout the following we take $M > 1$. n always denotes an integer greater than 1 in S_M^*, for some $M > 1$. Then, clearly, we have $(n, M) = 1$, $(n, \phi^*(n)) = 1$, and

$$\frac{n}{\phi^*(n)} > M \geqq 2. \tag{3.1}$$

THEOREM 3. *n is odd and not a powerful number.*

PROOF. If n is even, by (1.4), we have $\phi^*(n)$ is odd. But $\phi^*(n)$ is odd if and only if $n = 2^\alpha$ and, in this case, (1.4) cannot hold with $M > 1$. Hence n must be odd.

We recall that a number is said to be powerful if each exponent in its canonical representation is at least 2.

If n were powerful, then, by (1.3), (1.5), and (1.6), we have

$$\frac{n}{\phi^*(n)} = \prod_{p^\alpha \| n}\left(1 - \frac{1}{p^\alpha}\right)^{-1} < \prod_{p}\left(1 - \frac{1}{p^2}\right)^{-1}$$
$$= \zeta(2) = \pi^2/6 < 2,$$

contradicting (3.1). Hence n cannot be powerful

We denote the sequence of odd primes by $\{q_i\}$. That is, $q_1 = 3$, $q_2 = 5$, $q_3 = 7, \ldots$. For any $r > 1$, we write

$$Q_r = \prod_{i=1}^{r} \left(\frac{q_i}{q_i - 1} \right) \tag{3.2}$$

and

$$Q_r^* = \prod_{i=1}^{r} \left(\frac{q_i^2}{q_i^2 - 1} \right). \tag{3.3}$$

LEMMA 3.1. (i) $\omega(n) \neq 2$.
(ii) *If* $2 < \omega(n) \leqq 6$, *then* $M = 2$ *and* $3|n$.

PROOF. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $p_1 < p_2 < \cdots < p_r$, then, by Theorem 3, $p_i \geqq q_i$, for $i = 1, 2, 3, \ldots, r$, so that (3.1) gives $M < n/\phi^*(n) \leqq \prod_{i=1}^{r} q_i/q_i - 1 = Q_r$.

Since $Q_2 < 2$, (i) follows in view of Theorem 2.

Since $Q_r < 3$ for $2 < r \leqq 6$, we get $M = 2$, again by Theorem 2.

If $2 < r \leqq 6$ and $3 \nmid n$, then $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_6^{\alpha_6}$, where not more than three α_i can be zero and $p_i \geqq q_{i+1}$, for $i = 1, 2, \ldots, 6$. Therefore

$$\frac{n}{\phi^*(n)} = \prod_{\substack{i=1 \\ \alpha_i \neq 0}}^{6} \frac{p_i^{\alpha_i}}{p_i^{\alpha_i} - 1} \leqq \prod_{i=1}^{6} \frac{q_{i+1}}{q_{i+1} - 1} < 2,$$

contradicting (3.1). Hence $3|n$.

LEMMA 3.2. *Suppose primes* p, q *are such that* $p|n$ *and* $q^\beta \equiv 1 \pmod{p}$. *Then* q^β *cannot be a unitary divisor of* n.

PROOF. Given $p|n$ and $q^\beta \equiv 1 \pmod p$, if $q^\beta \| n$, then also $\phi^*(q^\beta) = q^\beta - 1 \mid \phi^*(n)$ so that $p | \phi^*(n)$. Thus, $p | (n, \phi^*(n))$, a contradiction. Hence the lemma.

COROLLARY 3.1. *If primes* p, q *are such that* $p|n$ *and* $q \equiv 1 \pmod p$, *then* $q \nmid n$.

LEMMA 3.3 *If* $3|n$, *then* $M \equiv 1 \pmod 3$.

PROOF. Suppose $n = 3^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then $p_i^{\alpha_i} \not\equiv 1 \pmod 3$ for $i = 1, 2, \ldots, r$, by Lemma 3.2. Now, (1.3) and (1.4) give

$$M(3^\alpha - 1)(p_1^{\alpha_1} - 1) \cdots (p_r^{\alpha_r} - 1) = 3^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} - 1.$$

Writing this equation to the congruence modulo 3, we get the lemma, since $p_i^{\alpha_i} \equiv 2 \pmod 3$, for $i = 1, 2, \ldots, r$.

THEOREM 4. $\omega(n) \geqq 7$.

PROOF. If $2 < \omega(n) \leqq 6$, then $M = 2$ and $3|n$, by Lemma 3.1. But if $3|n$, by Lemma 3.3, we have $M \equiv 1 \pmod 3$ so that $M \geqq 4$. These two contradict each other. Hence $\omega(n) \geqq 7$.

REMARK 3.1. Lehmer proved that $\omega(n) \geqq 7$, for all $n \in S_M$, using a different method. Since S_M is a subset of S_M^*, our proof also holds for the Lehmer problem.

4. Improved lower bounds for ω(n) with conditions on n and M. In this section we obtain lower bound of $\omega(n)$ with different conditions on n and various values of M, using Theorem 4. The following definitions are needed in the proofs of the results in this section.

DEFINITION 4.1. Suppose p is an odd prime. The sequence $G_p = \{P_i\}$ of primes, such that $P_1 = p$ and, for $i \geqq 1$, P_{i+1} is the smallest prime $> P_i$ satisfying $P_{i+1} \not\equiv 1 (\text{mod } P_k)$, for $1 \leqq k \leqq i$, is called the "G-sequence of primes with p as smallest member."

For example, $G_3 = \{3, 5, 17, 23, 29, 47, \ldots\}$ and $G_5 = \{5, 7, 13, 17, 19, 23, 37, \ldots\}$.

It may be noted here that the density and other aspects of G-sequences were studied by Golomb [**4**], Erdös [**3**], and Meijer [**11**].

DEFINITION 4.2. If $A = \{a_1, a_2, \ldots, a_m\}$ is a finite set of numbers each greater than 1, by its "quotient", denoted by A_m, we mean

$$A_m = \frac{a_1 a_2 \cdots a_m - 1}{(a_1 - 1)(a_2 - 1) \cdots (a_m - 1)}.$$

LEMMA 4.1. *Suppose $m \geqq 2$, $A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots, b_m\}$ are two sets of integers such that $1 < a_i \leqq b_i$ for each i, with strict inequality for at least one i. Then $A_m > B_m$.*

PROOF. The lemma can be verified easily in case $a_i = b_i$, for all i, except for one index k, where $a_k < b_k$. By repeated application of the result, the lemma follows.

THEOREM 5. *If $3 | n$, then $\omega(n) \geqq 1850$.*

PROOF. Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $3 = p_1 < p_2 < \cdots < p_r$. Then, by Theorem 4, $r \geqq 7$. Also, by (1.3), (1.4), and Lemma 3.3, we see that the quotient D_r of $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}\}$ satisfies

$$D_r = \frac{n-1}{\phi^*(n)} = M \geqq 4. \tag{4.1}$$

In view of Corollary 3.1, the p_i are such that $p_i \not\equiv 1 (\text{mod } p_j)$, for $i \neq j$, and they are among those that belong to the set $B = \{3, 5, 11, 17, 23, 29, 41, 47, 53, 59, \ldots\}$, which consists of 3 and all odd primes $p \not\equiv 1 (\text{mod } 3)$. Also, if b_i is the ith element of B in increasing order, then $p_i \geqq b_i$, for each i with strict inequality for $i = 2$ or 3 or both. Further, if $i > 6$, b_i is of the form $29 + 6x$, for some $x = 1, 2, 3, \ldots$. But $29 + 6x$ is composite if $x \in L$, where $L = \{x: x \equiv 1(\text{mod } 5), 1(\text{mod } 7), 8(\text{mod } 11), 6(\text{mod } 13), 15(\text{mod } 17), 11(\text{mod } 19) \text{ or } 22(\text{mod } 23)\}$. Therefore B is a subset of $A = \{3, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, \ldots\}$ consisting of 3, 5, 11, 17, 23, and all positive integers in the progression $29 + 6x$ with $x \notin L$. Clearly, if a_i is the ith element of A(in increasing order), then $b_i \geqq a_i$, for all i. Thus, we have, for any $i(1 \leqq i \leqq r)$, that $p_i^{\alpha_i} \geqq p_i \geqq b_i \geqq a_i$, and strict inequality holds, for at least one i, since $r \geqq 7$. Hence, by Lemma 4.1 and (4.1), we see that the quotient A_r of $\{a_1, a_2, \ldots, a_r\}$ satisfies $A_r > D_r \geqq 4$. That is, r is such that

$$\frac{3 \cdot 5 \cdot 11 \cdot 17 \cdot 23}{2 \cdot 4 \cdot 10 \cdot 16 \cdot 22} \prod_{\substack{x=0 \\ x \notin L}}^{r-6} \left(\frac{29 + 6x}{28 + 6x}\right) > 4$$

or

$$\prod_{\substack{x=0 \\ x \notin L}}^{r-6} \left(\frac{29 + 6x}{28 + 6x}\right) > \frac{22528}{12903}.$$

A computer run showed that the smallest such r is 1850, proving the theorem.

THEOREM 6. *If* $3 \nmid n$, $5 | n$, *then* $\omega(n) \geqq 11$.

PROOF. Here we take G_5, the G-sequence of primes with 5 as the smallest member. That is, $G_5 = \{5, 7, 13, 17, 19, 23, 37, 59, 67, 73, \ldots\}$. If p_i is the ith element in this sequence and P^* is the quotient of $\{P_1, P_2, \ldots, P_{10}\}$, we observe that $P^* < 2$.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ with $5 = p_1 < p_2 < \cdots < p_r$ and $r \leqq 10$, we prove the quotient D of $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}\}$ is $\leqq P^*$, from which the theorem is immediate. It suffices to prove this when $r = 10$.

Because of Corollary 3.1, the p_i are from the set $\{5, 7, 13, 17, 19, 23, 29, 37, 43, 47, 53, 59, 67, 73, \ldots\}$ of odd primes $p \geqq 5$ such that $p \not\equiv 1(\text{mod } 5)$. If $p_i = P_i$, for $i = 1, 2, \ldots, 10$, then $D = p^*$, proving our assertion. Therefore, let k be the least positive integer such that $p_k \neq P_k$. Then $2 \leqq k \leqq 10$. For any $k(3 \leqq k \leqq 10)$, we observe that $p_i \geqq P_i$ for $i = 1, 2, \ldots, 10$ so that Lemma 4.1. gives $D \leqq P^*$. Also, if $k = 2$, all choices of p_i are such that $D \leqq P^*$. Hence the theorem.

We state below a theorem which follows on the lines similar to [**2**, Proposition 1].

THEOREM 7. *If* $3 \nmid n$, $5 \nmid n$, *then* $\omega(n) \geqq 17$.

In the rest of this section we prove results which are improvements of [7, Lemma 1].

THEOREM 8. *If* $n \in S_M^*$, *for* $M = 3, 4$ *or* 5, *then* $\omega(n) \geqq 33$.

PROOF. If $3|n$, the theorem follows from Theorem 5.

If $3\nmid n$ and $\omega(n) \leqq 32$, then $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $p_1 < p_2 < \cdots < p_r$, is such that $p_i \geqq q_{i+1}$, for $i = 1, 2, 3, \ldots, r$, so that $n/\phi^*(n) \leqq \prod_{i=1}^{32} q_{i+1}/q_{i+1} - 1 < 3$. But this is a contradiction since

$$\frac{n}{\phi^*(n)} = M + \frac{1}{\phi^*(n)} > 3$$

if $M = 3$, 4 or 5. Hence $\omega(n) \geqq 33$ in this case also.

LEMMA 4.2. *If $n \in S_M^*$ has r distinct prime factors unitarily dividing it, then $Q_r > 8M/\pi^2$ or M according as n has a square factor or not. (Q_r is given by* (3.2)).

PROOF. Suppose $n = m \cdot m'$ where m is squarefree, m' is powerful and $(m, m') = 1$. Then $\omega(m) = r \geqq 1$, by Theorem 3. Let $s = \omega(m')$. Now

$$M < \frac{n}{\phi^*(n)} = \prod_{p\| n}\left(\frac{1}{p-1}\right) \cdot \prod_{p^\alpha \| n}\left(\frac{p^\alpha}{p^\alpha - 1}\right) \leqq Q_r \cdot Q_s^*,$$

where Q_s^* is given by (3.3). Hence $M < Q_r Q_s^*$ or Q_r according as $s \geqq 1$ or $s = 0$. The lemma now follows from the fact that, for $s \geqq 1$,

$$Q_s^* = \prod_{i=1}^{s}\left(1 - \frac{1}{q_i^2}\right)^{-1} = \left(1 - \frac{1}{2^2}\right) \cdot \zeta(2) \cdot \prod_{i=s+1}^{\infty}\left(1 - \frac{1}{q_i^2}\right),$$
$$< \frac{3}{4}\zeta(2) = \frac{\pi^2}{8}, \text{ by (1.6).}$$

THEOREM 9.

(i) *If $n \in S_5^*$ and n is squarefree, then $\omega(n) \geqq 53$.*

(ii) *If $n \in S_6^*$, then $\omega(n) \geqq 140$ or 48 according as n is squarefree or not.*

(iii) *If $n \in S_7^*$, then $\omega(n) > 200$ or 103 according as n is squarefree or not.*

(iv) *If $n \in S_M^*$, for $M \geqq 8$, then $\omega(n) > 200$.*

PROOF. These can be proved easily making use of Lemma 4.2 and Table IX of Legendre [**8**], which gives the values of Q_r^{-1} for $1 \leqq r \leqq 200$.

For instance, when $M = 6$ and n is squarefree we must have $Q_r > 6$, by Lemma 4.2. This requires $r \geqq 140$ from the table, proving the first part of (ii).

THEOREM 10. If $2 < \omega(n) \leqq 16$, *then* $M = 2, 3 \nmid n, 5|n, 7|n$.

PROOF. $3\nmid n$, $5|n$, $M = 2$, respectively, follow from Theorems 5, 7, 8 and 9.

If $7 \nmid n$, then $n/\phi^*(n) = {*}\prod_{i=1}^{21} q_{i+1}/(q_{i+1} - 1)$, where $*$ indicates that the primes $q_i \equiv 1 (\text{mod } 5)$ are excluded in the product. Since the product is < 2, which contradicts (3.1), we get that $7|n$.

REMARK 4.1. Summing up the results of §2 and §3, we have shown that $\omega(n) \geqq 11$, for every $n \in S_M^*$.

5. Upper bound for n with r distinct prime factors. Throughout this section N, denotes an odd natural number.

LEMMA 5.1. *If* $N \in S_M^*$, $m \| N$, $m \neq N$, *then* $m/\phi^*(m) < M$.

PROOF. If $m = 1$, the lemma is obvious.

Assume $m > 1$. It is enough to prove the lemma for m having exactly $(r - 1)$ unitary prime power divisors of N. Let $m' = p^\alpha$ be the complementary unitary divisor of m so that $mm' = N$ and $(m, m') = 1$.

Since $N \in S_M^*$, we have

$$\begin{aligned} 1 &= N - M\phi^*(N) = mm' - M\phi^*(m)(m' - 1) \\ &= m'[m - M\phi^*(m)] + M\phi^*(m), \end{aligned}$$

from which the lemma is immediate because $M\phi^*(m) \geqq M \geqq 2$.

LEMMA 5.2. *Suppose* $(N/\phi^*(N)) > M$. *If* $m \| N$, $m \neq 1$, $m \neq N$ *and* $(m/\phi^*(m)) < M$, *then the least among the prime power divisors of* $m' = N/m$ *is less than* $\omega(m')m$.

PROOF. Since N is odd we have $m \geqq 3$. Let $m' = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$ with $p_1^{\beta_1} < p_2^{\beta_2} < \cdots < p_t^{\beta_t}$. Now $m/\phi^*(m) < M < N/\phi^*(N)$ implies $m'/\phi^*(m') > M(\phi^*(m)/m) \geqq 2$. That is,

$$\prod_{i=1}^{t} \frac{p_i^{\beta_i}}{p_i^{\beta_i} - 1} > 2. \tag{5.1}$$

Also, $p_1^{\beta_1} < p_2^{\beta_2} < \cdots p_t^{\beta_t}$ and each p_i odd implies that $p_i^{\beta_i} \geqq p_1^{\beta_1} + 2(i - 1)$, for $i = 2, 3, \ldots, t$. Therefore, by the decreasing nature of $(x/x - 1)$ and (5.1), we get

$$\prod_{i=1}^{t} \left(\frac{p_1^{\beta_1} + 2i - 2}{p_1^{\beta_1} + 2i - 3}\right)^2 > 4 \tag{5.2}$$

Again, since $x/(x - 1)$ is a decreasing function, we have

$$\frac{p_1^{\beta_1} + 2i - 2}{p_1^{\beta_1} + 2i - 3} < \frac{p_1^{\beta_1} + 2i - 3}{p_1^{\beta_1} + 2i - 4}$$

for each i, from which it follows that

$$\left(\frac{p_1^{\beta_1} + 2i - 2}{p_1^{\beta_1} + 2i - 3}\right)^2 < \frac{p_1^{\beta_1} + 2i - 2}{p_1^{\beta_1} + 2i - 4}. \tag{5.3}$$

Now, from (5.2) and (5.3), we get

$$4 < \prod_{i=1}^{t} \left(\frac{p_1^{\beta_1} + 2i - 2}{p_1^{\beta_1} + 2i - 4}\right) = \frac{p_1^{\beta_1} + 2t - 2}{p_1^{\beta_1} - 2}$$

or $p_1^{\beta_1} < 2 + 2\,t/3 < 3t \leqq mt$, proving the lemma.

LEMMA 5.3. *If* $N \in S_M^*$ *and* $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, *with* $p_1^{\alpha_1} < p_2^{\alpha_2} < \cdots < p_r^{\alpha_r}$, *then*

$$p_i^{\alpha_i} < (r - i + 1)\left(\prod_{j=1}^{i-1} p_j^{\alpha_j}\right)$$

for $i = 2, 3, \ldots, r$.

PROOF. Fix i and write $m = \prod_{j=1}^{i-1} p_j^{\alpha_j}$. Then $m \| N$, $m \neq 1$, $m \neq N$, so that by Lemma 5.1, $m/\phi^*(m) < M$. Also, by (3.1), we have $N/\phi^*(N) > M$. Now, the lemma is immediate from Lemma 5.2.

A result of interest is established in the proof of Lemma 5.2. We record it as the following lemma.

LEMMA 5.4. If $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $p_1^{\alpha_1} < p_2^{\alpha_2} < \cdots < p_r^{\alpha_r}$, *is such that* $N/\phi^*(N) > 2$, *then* $p_1^{\alpha_1} < 2 + 2(r/3)$.

REMARK 5.1. Otto Grün [**5**] proved a similar result for odd perfect numbers. In fact he showed that the least prime factor of an odd perfect number N with $\omega(N) = r$ is $< (2/3)\, r + 2$.

THEOREM 11. *If* $\omega(n) = r$, *then* $n < (r - 1)^{2^r - 1}$.

PROOF. Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, with $p_1^{\alpha_1} < p_2^{\alpha_2} < \cdots < p_r^{\alpha_r}$, so that $n/\phi^*(n) > 2$ and $r \geqq 11$, by (3.1) and Remark 4.1. Therefore, by Lemma 5.4,

$$p_1^{\alpha_1} < \frac{2}{3} r + 2 < r - 1. \tag{5.4}$$

Now, by Lemma 5.3 and (5.4), we successively have

$$p_2^{\alpha_2} < (r - 1)\, p_1^{\alpha_1} < (r - 1)^2,$$

$$p_3^{\alpha_3} < (r - 2) p_1^{\alpha_1} p_2^{\alpha_2} < (r - 2)(r - 1)(r - 1)^2 < (r - 1)^{2^2},$$

More generally, $p_i^{\alpha_i} < (r - 1)^{2^{i-1}}$, for $i = 1, 2, \ldots, r$.

Hence $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} < (r - 1)(r - 1)^2 (r - 1)^{2^2} \cdots (r - 1)^{2^{r-1}}$
$= (r - 1)^{2^r - 1}$.

REMARK 5.2. Theorem 11 gives an improvement of a result of Pomerance [**12**, equation (1.2)] where he showed that $n < r^{2^r}$, for every $n \in S_M$, with $\omega(n) = r$. A similar result for amicable numbers is obtained by Borho [**1**].

6. Order estimate for N*(x). Let $N^*(x)$ be the number of $n \leqq x$ in S_M^*, for some $M > 1$. In this section we obtain an order estimate for $N^*(x)$. We state the following equivalent form of the combinatorial lemma proved by Pomerance [**12**, Lemma 4].

LEMMA 6.1. *Suppose* $\delta \geqq 0$, $0 < a_1 \leqq a_2 \leqq \cdots \leqq a_t$, $B_i = \sum_{j=1}^{i} a_j$, for $1 \leqq i \leqq t$, *and* $a_i \leqq \delta + B_{i+1}$, *for* $1 \leqq i \leqq t - 1$. *Then, given* y *with* $0 \leqq y \leqq B_t$, *there is a subset* S *of* $\{1, 2, 3, \ldots, t\}$ *such that*

$$y - \delta - a_1 < \sum_{i \in S} a_i \leqq y.$$

THEOREM 12. $N^*(x) = O(x^{1/2} \log^2 x \cdot (\log \log x)^{-2})$.

PROOF. Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \in S_M^*$, for some $M > 1$; $p_1^{\alpha_1} < p_2^{\alpha_2} < \cdots < p_r^{\alpha_r}$, and $n \leqq x$. Then, for each i, by Lemma 5.3,

$$p_i^{\alpha_i} < (r - i + 1)\left(\prod_{j=1}^{i-1} p_j^{\alpha_j}\right)$$

so that

$$\log p_i^{\alpha_i} < \log r + \sum_{j=1}^{i-1} \log(p_j^{\alpha_j}).$$

Let $\Delta(x)$ be a function (to be chosen suitably) satisfying $1 \leqq \Delta(x) < x$. Now, for $x \geqq n > \Delta(x)$, we have $\log n > \log \Delta(x)$. Taking $\delta = \log r$, $t = r$, $a_i = \log(p_i^{\alpha_i})$ and $y = \log \Delta(x)$ in Lemma 6.1, we get a unitary divisor m of n such that

$$y - \delta - \log p_1^{\alpha_1} < \log m \leqq y.$$

That is,

$$\frac{\Delta(x)}{r \cdot p_1^{\alpha_1}} < m \leqq \Delta(x). \tag{6.1}$$

Now, by (5.4), and the fact that there is a positive constant c such that $r = \omega(n) < (c \log n)/(\log \log n)$, for $n \geqq 3$ (see [6], p. 335), we get

$$r \cdot p_1^{\alpha_1} < r(r - 1) < r^2 < \frac{c_1 \log^2 x}{(\log \log x)^2}, \tag{6.2}$$

for some $c_1 > 0$.

Then, (6.1) and (6.2) imply that, for every n with $\Delta(x) < n \leqq x$, there is a unitary divisor m of n such that

$$f(x) < m \leqq \Delta(x), \tag{6.3}$$

where

$$f(x) = \frac{\Delta(x)(\log \log x)^2}{c_1 \log^2 x}. \tag{6.4}$$

Now, among the integers $n \in S_M^*(\Delta(x) < n \leqq x)$, we count those n for which a given m is a unitary divisor satisfying (6.3). Since $m \| n$ implies $\phi^*(m) | \phi^*(n)$, any such n must satisfy the congruences $n \equiv 0 (\mathrm{mod}\ m)$ and

$n \equiv 1 (\mathrm{mod}\ \phi^*(m))$. By the Chinese Remainder Threoem, the number of such $n \leqq x$ is at most $[x/m\phi^*(m)]$, where $[t]$ is the greatest integer $\leqq t$.
Hence

$$N^*(x) \leqq \Delta(x) + \sum_{f(x)<m\leqq\Delta(x)} \left[\frac{x}{m\phi^*(m)}\right]$$
$$= O(\Delta(x)) + O\left(x \sum_{f(x)<m\leqq\Delta(x)} \frac{1}{m\phi^*(m)}\right).$$

Now, using a result of Landau, we have

$$\sum_{m>y} \frac{1}{m\phi^*(m)} \leqq \sum_{m>y} \frac{1}{m\phi(m)} = O\left(\frac{1}{y}\right). \tag{6.6}$$

From (6.5) and (6.6), we obtain that

$$N^*(x) = O(\Delta(x)) + O\left(\frac{x}{f(x)}\right) + O\left(\frac{x}{\Delta(x)}\right)$$

Choosing $\Delta(x) = O(x^{1/2} \log^2 x \cdot (\log\log x)^{-2})$, all terms on the right of (6.7) will be $O(\Delta(x))$, proving the theorem.

7. Concluding remarks Using. computational methods similar to that of Kishore, Cohen and Hagis or by some other techniques, it may be possible to improve Theorem 6, by showing, say, $\omega(n) \geqq 13$ whenever $3 \nmid n$ and $5|n$.

Considering the infinite nature of the set complement of S_M in S_M^* the order estimate we obtained for $N^*(x)$ is reasonably good as a first attempt. Further improvements of this are, of course, possible and will be considered in a future paper.

References

1. W. Borho, *Eine Schranke für befreundte Zahlen mit gegenbene, Teileranzahl*, Math. Nachr. **63** (1974), 297–301.

2. G. L. Cohen and P. Hagis, Jr., *On the number of prime factors of n if $\phi(n)|n-1$*, Nieuw Archief Voor. Wiskunde (3) XXVIII (1980), 177–185.

3. P. Erdös, *On a problem of G. Golomb*, J. Australian Math. Soc. **2** (1961/62), 6–8.

4. S. W. Golomb, *Sets of primes with intermediate density*, Math. Scand. **3** (1955), 264–274.

5. O. Grün, *Über ungerade vollkommene Zahlen*, Math. Z. **55** (1952), 353–354.

6. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fourth edition, Oxford, 1960.

7. M. Kishore, *On the number of distinct prime factors of n for which $\phi(n)|n - 1$*, Nieuw Archief Voor Wiskunde, (3) XXV, (1977), 48–53.

8. A. M. Legendre, *Théorie des Nombres*, Vol. I, Libraire Scientifique et Technique, Paris, 1955.

9. D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), 745–751.

10. E. Lieuwens, *Do there exist composite numbers M for which $k\phi(M) = M - 1$ holds?*, Nieuw Archief Voor Wiskunde (3) XVIII (1970), 165–169.

11. H. G. Meijer, *Sets of primes with intermediate density*, Math. Scand., **34** (1974), 37–43.

12. C. Pomerance, *On composite n for which $\phi(n) | n - 1$*, II, Pacific J. Math. **69** (1977), 177–186.

13. Schuh, F.r., *Do there exist composite numbers m for which $\phi(m) | m - 1$* (Dutch), Mathematica Zutpen, B **13** (1944), 102–107.

14. M. V. Subbarao, *On a problem concerning the unitary totient function $\phi^*(n)$*, Notices Amer. Math. Soc. **18** (1971), 940.

UNIVERSITY OF ALBERTA EDMONTON, ALBERTA, CANADA T6G 2G1

OSMANIA UNIVERSITY HYDERABAD, 500007, INDIA