Publ. Math. Debrecen
52 / 3-4 (1998), 683–698

A companion to a Lehmer problem

By M. V. SUBBARAO (Edmonton)

Dedicated to Professors Zoltán Daróczy and Imre Kátai on their 60th birthday

Abstract. We here consider a new problem analogous to Lehmer's problem concerning n for which $\varphi(n)|n-1$, which is just as challenging as the Lehmer problem. A particular case of this problem is as follows: if $p_1,\dots,p_r$ are distinct odd primes and if $(p_1+1)\dots(p_r+1)\equiv 1 \pmod{p_1\dots p_r}$, is $r=1$?

0. Introduction

In 1932 D. H. Lehmer [3] raised a question which has now become one of the most famous unsolved problems of elementary number theory. If $\varphi(n)$ denotes the Euler totient, he asked if there is an integer n for which $\varphi(n)$ is a proper divisor of $n-1$, i.e. a divisor other than 1 and $n-1$ itself. One can easily show that this is equivalent to the following problem: If $p_1,\dots,p_r$ are distinct odd primes and if we have

$$(p_1,\dots p_r)-1\equiv 0 \bigl(\operatorname{mod}(p_1-1)\dots(p_r-1)\bigr),$$

does it necessarily follow that $r=1$?

Mathematics Subject Classification: 11A25.
Key words and phrases: Euler totient, unitary totient, $\sigma^*(n)$, Dedekind function $\psi(n)$.
Supported in part by an NSERC Grant.
Some of the results of this paper were presented at the special session of the American Mathematical Society held in 1993 at the Northern Illinois University, De Kalb, Illinois, U.S.A. in honour of Paul Erdös.

For forty years after Lehmer's paper was published, it was completely ignored as Lehmer lamented. But from the early seventies on, it attracted much attention and numerous papers were published since 1972, though the problem remains unsolved. In 1971, this author [12] considered the unitary analogue (stated below) of Lehmer's Problem; later he and Prasad [13] obtained several new results concerning these problems.

If $\varphi^*(n)$ denotes the unitary analogue of $\varphi(n)$ (so that if $n=p_1^{a_1}\dots a_r^{a_r}$, then $\varphi^*(n) = (p_1^{a_1}-1)\dots(p_r^{a_r}-1)$), the author's question is whether $\varphi^*(n)|(n-1)$ necessarily implies that n is a prime power. If the answer to this is in the affirmative, then so is the answer to Lehmer's question but not the reverse.

In this paper, we raise "companions" to these problems which seem just as difficult as the Lehmer problem. Namely, if $p_1,\dots,p_r$ are distinct primes, and if $(p_1+1)\dots(p_r+1) \equiv 1 \pmod{p_1\dots p_r}$, is r necessarily $=1$? The author conjectures that this is so. More generally, the author conjectures that for arbitrary positive integers $a_1,\dots,a_r$ and distinct odd primes $p_1,\dots,p_r$ the relation $(p_1^{a_1}+1)\dots(p_r^{a_r}+1) \equiv 1 \pmod{p_1^{a_1}\dots p_r^{a_r}}$ implies $r=1$.

1. Notation and definitions

Unless otherwise stated, we use throughout the following notation

$$1 < n = p_1^{a_1}\dots p_r^{a_r}$$

where $p, p_1,\dots,p_r$ are distinct primes

$\varphi(n)$ is Eulers totient

$\sigma(n) =$ sum of the positive divisors of n

$\omega(n) =$ number of distinct prime divisors of n

$\varphi^*(n) = \prod_{i=1}^{r}(p_i^{a_i}-1)$, the unitary totient

$\sigma^*(n) =$ sum of the unitary divisors of n, where by a "unitary divisor of n''

we mean a divisor d of n such that d and n/d are relatively prime.

$\psi(n) =$ the Dedekind function given by

$$\psi(n) = n\prod_{p|n}\left(1+\frac{1}{p}\right) = \sum_{d\delta=n}\mu^2(d)\delta =$$

sum of those divisors of n whose conjugates are square free.

2. Lehmer's Problem: Generalization and some conjuectures

As already mentioned Lehmer asked the equivalent of: If $\varphi(n)|n-1$, is n a prime? Several people worked on this still unsolved problem (Lehmer [3], Schuh [7], Lieuwens [4], Kishore [2], Cohen and Hagis [1], Hagis [5], Pomerance [6], Prasad, Rangamma [8], Prasad and Subbarao ([9], [12], [13]) and several others).

For $M \geq 1$, define

$$S_M = \{n > 1 : M\varphi(n) = n - 1\}.$$

Clearly, S_1 is the set of primes. The question then is: Does S_M have any composite numbers for $M > 1$. Clearly, for $M > 1$, $n \in S_M$ implies that n is odd and square-free. For $n \in S_M,\ M > 1$, (this is assumed in all that follows)

$$\begin{aligned} \omega(n) &\geq 7 && \text{(Lehmer [7])} \\ \omega(n) &\geq 13 && \text{(Keshore [2])} \\ &\geq 14 && \text{(Peter Hagis, Jr. [5])} \\ 3|n \Longrightarrow \omega(n) &\geq 212 && \text{(Lieuwens [4])} \\ &\geq 1850 && \text{(Prasad and Subbarao [9])} \\ &\geq 29884 && \text{(Hagis [5])} \end{aligned}$$

The set S_M has density 0 (Pomerance [6]).

(1) For each $n \in S_M$, $M > 1$, we have $n < r^{2^r}$, where $r = \omega(n)$

(Pomerance (1977, [6]). Prasad and Subbarao [13] improved this in 1985 to $n < (r-1)^{2^{r-1}}$. Pomerance [6], proved that the number of $n \leq x$ in any

$$S_M\ (M > 1) \quad \text{is } 0\big(x^{1/2} \log^{3/4} x (\log\log x)^{-1/2}\big).$$

Conjecture (Pomerance [6]). *The number of $n \leq x$ in all S_n, $n > 1$, is $0(n^{\varepsilon})$ for every $\varepsilon > 0$.*

The author formally makes the following

Conjecture A. $\varphi(n)|(n-1)$, $n>1 \Longleftrightarrow n$ *is a prime.*

LEHMER [3] himself said that he was tempted to make this conjecture.

Lehmer's problem as a limiting case. We first state the following:

Theorem. *For* $r=2,3,\ldots$ *and* $n>1$, *we have*

$$n^r - 1 \equiv 0 \pmod{\varphi(n)\sigma\big(n^{r-1}\big)} \tag{2}$$

if and only if n *is a prime.*

The proof is easy and is omitted.

Remark. The case $r=1$ is the Lehmer Problem.

Remark. We note that the relation (2) implies that n is square-free.

Hence the result (2) is equivalent to

Theorem. *For any given integer* $k>1$ *and finite number of distinct primes* $p_1,\ldots,p_r$, *the congruence*

$$p_1^k \ldots p_r^k \equiv 1 \pmod{(p_1^k-1)\ldots(p_r^k-1)}$$

is possible if and only if $r=1$.

This itself is a special case of

Theorem. *For any any finite set of distinct primes* $p_1,\ldots,p_r$ *and for arbitrary positive integers* $a_1,\ldots,a_r$, *and for all integers* $k\geq 2$, *the relation*

$$p_1^{ka_1}\ldots p_r^{ka_r} - 1 \equiv 0 \pmod{(p_1^{ka_1}-1)\cdots(p_r^{ka_r}-1)}$$

holds if and only if $r=1$.

Again, we shall omit the proof.

Remark. In 1971 this author [12] made the conjecture which in effect says that the last Theorem holds for $k=1$ also.

Equivalently,

Conjecture B (SUBBARAO [12])**.** *For* $n>1$, *the relation* $\varphi^*(n)|(n-1)$ *implies that* n *is a prime power.*

Remark. If Conjecture B holds so also Conjecture A. The reverse implication is false.

3. Some results connected with Conjecture B

In this section we assume that n satisfies $\varphi^*(n)|(n-1)$. Define

$$S^*(M) = \{n : M\varphi^*(n) = n-1,\, n > 1\}$$

and

$$N^*(x) = \#\{n : n \le x,\, n \in S^*(n) \quad \text{for some} \quad n > 1\}.$$

Then we can show ([13]) that n is odd and is not a powerful number (an integer is powerful whenever in its canonical form, all powers of primes are ≥ 2). Moreover

$$\omega(n) \ge 11 \quad \text{and } n > 10^{17}.$$

These can be further improved easily.

$$N^*(x) = 0\big(x^{1/2}\ \log^2 x(\log\ \log\ x)^{-2}\big)$$

If $\omega(n) = r$ then

$$n < (r-1)^{2^{r-1}}.$$

Note that this improves Pomerance's result (1). If $p \mid n$, $q \equiv 1 \pmod p$, then $q \nmid n$.

$$3 \mid n \Longrightarrow \omega(n) > 1850.$$

4. A Companion to the Lehmer problem

We first prove the

Theorem. *For every integer $k{>}1$, the relation (p_i are distinct primes)*

$$(p_1^k+1)\dots(p_r^k+1) \equiv 1 \pmod{p_1^k \dots p_r^k} \tag{3}$$

implies that $r=1$.

More generally, for arbitrary positive integers $a_1,\dots,a_r$ and every integer $k>1$, the congruence

$$(p_1^{a_1k}+1)\dots(p_r^{a_rk}+1) \equiv 1 \ \big(\mathrm{mod} p_1^{a_1k}\dots p_r^{a_rk}\big) \tag{4}$$

implies that $r = 1$.

PROOF. Write (3) as

$$(p_1^k + 1) \dots (p_r^k + 1) = 1 + M(p_1^k \dots p_r^k)$$

where M is an integer ≥ 1. This implies

$$\begin{aligned} 1 \leq M &< \prod_{i=1}^{r} \bigl(1 + \frac{1}{p_i^k}\bigr) < \prod_{i=1}^{r} \bigl(1 - p_i^{-k}\bigr)^{-1} \\ &< \prod_{i=1}^{r} \bigl(1 - p_i^{-2}\bigr)^{-1}, \quad \text{since } k \geq 2 \\ &< \prod_{q} (1 - q^{-2})^{-1} = \zeta(2) = \pi^2/6 < 2, \end{aligned}$$

where q ranges over all primes, and $\zeta(s)$ is the Riemann zeta function.

Hence $M = 1$, giving

$$(p_1^k + 1) \dots (p_r^k + 1) = (p_1^k \dots p_r^k) + 1,$$

which is impossible if $r > 1$, since then the left side is

$$(p_1^k + 1)(p_2^k \dots p_r^k)$$

which is greater than the right side.

Proof of the more general result (4) is similar.

Remark. Recalling that for $n = p_1^{a_1} \dots p_r^{a_r}$, $\sigma_k^*(n) =$ (sum of the k-th powers of the unitary divisors of n) $= (p_1^{ka_1} + 1) \dots (p_r^{ka_r} + 1)$, we can state the last theorem as

Theorem. *For $r = 2, 3, \dots,$ we have $\sigma_r^*(n) \equiv 1 \pmod n \Longrightarrow n =$ a prime power.*

The author believes that this result holds for $r = 1$ also.

Conjecture C (SUBBARAO).

(5) $\sigma^*(n) \equiv 1 \pmod n \Longleftrightarrow n$ *is a prime power.*

In particular, for arbitrary distinct primes $p_1, \dots, p_r$, $r \geq 1$,

(6) $(p_1 + 1) \dots (p_r + 1) \equiv 1 \pmod{p_1 p_2 \dots p_r} \Longleftrightarrow r = 1.$

Equivalently, $\psi(n) \equiv 1 \pmod n \iff n = a$ *prime.*

Some results related to (6).

Adapting the ideas and methods of our earlier paper [13], we can derive marry results concerning Conjecture C analogous to those in that paper. We content ourselves mentioning below a few of them, mostly skipping proofs.

Definitions. For $M = 1, 2, 3, \dots$

$$\begin{aligned} T(M) &= \{n : \psi(n) = 1 + Mn\} \\ T^*(M) &= \{n : \sigma^*(n) = 1 + Mn\} \\ &= \{n : (p_1^{a_1} + 1) \dots (p_r^{a_r} + 1) \equiv 1 + Mn\} \end{aligned}$$

Remarks. All the n in $T(M)$ and $T^*(M)$ are square-free.

$$\begin{aligned} T(M) &\subset T^*(M) \\ T(1) &= \{\text{set of all primes}\} \\ T^*(1) &= \{\text{set of all prime powers}\}. \end{aligned}$$

Our Conjecture C is that for $M > 1$, $T(M)$, $T^*(M)$ are empty.

In the sequel we assume that $M > 1$, unless stated otherwise explicitly.

(7) $$n \in T^*(M) \Longrightarrow n \text{ is not a powerful number.}$$

M is odd ≥ 3 and $\omega(n) \geq 16$, $n > 10^{20}$.

Taking $\{q_i\}$ to be the sequence of odd primes, the last two results in (7) follow from (writing $n = \prod_{i=1}^{r} p_i^{a_i}$)

$$\begin{aligned} M \underset{i=1}{\overset{r}{<}} \prod (p_i^{a_i} + 1) p_i^{a_i} &< \prod_{i=1}^{r} (p_i + 1)/p_i \\ &\leq \prod_{i=1}^{r} (q_i + 1)/q_i < 3 \quad \text{if} \quad r \leq 15. \end{aligned}$$

Hence, M being odd, we have $r \geq 16$ and $n \geq q_1 q_2 \dots q_{16} \geq (9.6)10^{20}$.

We easily obtain the following result. If $n \in T^*(M),\ M > 1$, we then obtain: if $p \mid n$ and $q^\beta + 1 \equiv 0 \pmod p$ then q^β cannot be a unitary divisor of n. In particular, if p and q are prime such that $p \nmid n$ and $q + 1 \equiv 0 \bmod p$, then $q \nmid n$.

We can get improved lower bounds for $\omega(n)$ with conditions on n. For example

Theorem. *If* $n \in T(M),\ M > 1$, *then*

$$3 \mid n \Longrightarrow \omega(n) \geq 185. \tag{8}$$

We here use only simple arguments, but we can improve this result using computer-oriented methods as in [5].

Proof of (8). We adapt an idea used in [10]. Since n is square free, say $n = p_1 \dots p_r$ we have

$$(p_1 + 1) \dots (p_r + 1) = \psi(p_1 \dots p_r) = M p_1 \dots p_r + 1.$$

Let $p_1 = 3$. Since $p_i \not\equiv -1 \pmod{p_i}$ for $j \neq i$ we have

$$p_i \equiv 1 \pmod 3, \quad i \geq 2 \tag{9}$$

and so $p_i + 2 \equiv 0 \pmod 3$, $p_i + 4 \equiv 2 \pmod 4$ so that in view of (9), $p_i + 2$ and $p_i + 4$ cannot divide n. It follows that

$$p_{i+1} \geq p_i + 6 \quad \text{for} \quad 2 \leq i \leq r - 1. \tag{10}$$

In particular, $p_2 \geq 7$.

We now show that

$$M < \left(\frac{4}{3}\right)\left(\frac{p_2 + 1}{p_2}\right)\left(\frac{p_3 + 6r - 17}{p_3 - 5}\right)^{1/6}.$$

Using (10) we have

$$p_4 \geq p_3 + 6, \quad p_5 \geq p_4 + 6 \geq p_3 + 12,$$

and in general $p_i \geq p_3 + 6i - 18, \quad 3 \leq i \leq r$. Thus

$$M < \left(1 + \frac{1}{p_1}\right) \dots \left(1 + \frac{1}{p_r}\right) = \left(1 + \frac{1}{3}\right)\left(1 + \frac{1}{p_2}\right) \prod_{i=3}^{r} \left(1 + \frac{1}{p_i}\right).$$

Noting that $\frac{x+1}{x}$ is a decreasing function of x for $x > 0$ we get

$$M < \frac{4}{3}\left(\frac{p_2+1}{p_2}\right)\prod_{i=3}^{r}\left(\frac{p_3+6i-17}{p_3+6i-18}\right).$$

Thus

$$M^6 < \left(\frac{4}{3}\right)^6\left(\frac{p_2+1}{p_2}\right)^6\prod_{i=3}^{r}\left(\frac{p_3+6i-17}{p_3+6i-18}\right)^6.$$

This gives, on using the fact that

$$\frac{x-a}{x-(a+1)} < \frac{x-(a+1)}{x-(a+2)} \quad \text{for } a = 17, 18, \ldots$$

that

$$\begin{aligned} M^6 &\leq \left(\frac{4}{3}\right)^6\left\{\left(\frac{p_2+1}{p_2}\right)^6\prod_{i=3}^{r}\left(\frac{p_3+6i-17}{p_3+6i-18}\right)\right. \\ &\quad \left.\times\left(\frac{p_3+6i-18}{p_3+6i-19}\right)\cdots\left(\frac{p_3+6i-22}{p_3+6i-23}\right)\right\} \\ &= \left(\frac{4}{3}\right)^6\left(\frac{p_2+1}{p_2}\right)^6\cdot\left(\frac{p_3+6r-17}{p_3-5}\right). \end{aligned}$$

From this we can deduce that if $7 \nmid n$ so that $p_2 \geq 13$, $p_3 \geq 19$, then

$$r > \frac{1}{3}\left(\frac{13M}{21}\right)^6 - \frac{1}{3}.$$

Use the fact that $\frac{p_3+6r-17}{p_3-5}$ is a decreasing function of p_3 and that $\frac{x+1}{x}$ is a decreasing function of x for $x > 0$; we get on using $p_2 = 13$, $p_3 = 19$, that

$$\begin{aligned} M &< \frac{4}{3}\cdot\left(\frac{14}{13}\right)\left(\frac{19+6r-17}{19-5}\right)^{1/6} \\ &< \left(\frac{56}{39}\right)\left(\frac{6r+2}{14}\right)^{1/6} = \left(\frac{56}{39}\right)\left(\frac{3r+1}{7}\right)^{1/6}. \end{aligned}$$

This gives

$$M^6 < \left(\frac{56}{39}\right)^6\cdot\frac{3r+1}{7}.$$

Hence
$$r > \frac{7}{3}\left(\frac{39M}{56}\right)^6 - \frac{1}{3}.$$
Utilizing the fact that $M \geq 3$, this gives
$$\omega(n) = r \geq \frac{7}{3}\left(\frac{117}{56}\right)^6 - 1$$
from which we get the theorem in the case when $7 \nmid n$.

In the case $7 \mid n$, then $p_1 = 3$, $p_2 = 7$, $p_3 \geq 19$, $p_4 \geq 31$, so $p_i \geq p_4 + 6i - 24$ for $i \geq 4$. Proceeding as in the previous case, we get
$$\begin{aligned} M &< \frac{3+1}{3} \cdot \frac{7+1}{7} \cdot \frac{(p_3+1)}{p_3} \prod_{i=4}^{r} \frac{p_4 + 6r - 23}{p_4 + 6r - 29} \\ &< \frac{3+1}{3} \cdot \frac{7+1}{7} \cdot \left(\frac{p_3+1}{p_3}\right)\left(\frac{p_4 + 6r - 23}{p_4 - 5}\right)^{1/6} \end{aligned}$$
since $p_3 \geq 19$, $p_4 \geq 31$, this gives
$$M < \frac{32}{21} \cdot \frac{20}{19} \cdot \left(\frac{31 + 6r - 23}{31 - 5}\right)^{1/6} = \frac{640}{399}\left(\frac{3r+4}{13}\right)^{1/6}.$$
Hence
$$r > \frac{13}{3}\left(\frac{399M}{640}\right)^6 - \frac{4}{3}.$$
Since $M \geq 3$, this gives $r > 185$.

Hence the theorem follows in this case also.

Remark. Using the computer, one can get better results similar to those of Peter Hagis [5] adapting his methods. One can also improve the result (8) by using the method adopted in the proof of ([13], Theorem 5) by proving that $3 \mid n \Longrightarrow \omega(n) > 2557$; $n > (5.9)10^{10766}$. Details will appear elsewhere.

Remark. It is easy to show that if $3 \mid n$, $n \in T(M)$, that $\omega(n)$ is odd while if $3 \mid M$, then $\omega(n)$ is even.

Several of the results of our earlier paper [13] have their analogues for the function $\psi(n)$ on suitably modifying the ideas and details there. For instance can prove

Theorem. *If $n \in T^*(M)$ with $\omega(n) = r$, then $n < (r-1)^{2^{r-1}}$.*

We give a complete proof of this here.

Lemma. *If $n \in \overline{T}^*_M$, $m \| N$, $1 \leq m < N$, then $\sigma^*(m)/m < n$.*

Proof. For $m = 1$, the lemma is obvious, let us assume that $m > 1$ has exactly $(r-1)$ unitary prime power divisors of N, where $\omega(N) = r$. Write $m' = N/m$, so that $(m, m') = 1$, and $m' =$ a prime power $= p^\alpha$, say.

Since $N \in T^*_M$, we have

$$\begin{aligned} 1 &= \sigma^*(N) - MN = \sigma^*(m)\sigma^*(m') - Mmm' \\ &= \sigma^*(m)(m'+1) - Mmm' \\ &= m'\big(\sigma^*(m) - Mm\big) + \sigma^A(m). \end{aligned}$$

Since $\sigma^*(m) \geq 2$, this gives $\sigma^*(m) - Mm < 0$, from which the lemma follows.

Lemma. *Suppose $N \in T^*_M$, $M > 1$. If $m \| N$, $1 < m < N$, and $\sigma^*(m)/m < M$, then the least among the prime power divisors of $m' = N|m$ is less that $m\omega(m')$.*

Proof. Since N is odd, we have $m \geq 3$. Write $m' = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ with $p_1^{\beta_1} < p_2^{\beta_2} < \cdots < p_r^{\beta_r}$. Then

$$\sigma^*(m)/m < M < \sigma^*(N)/N = \frac{\sigma^*(m)}{m} \cdot \frac{\sigma^*(m')}{m'}$$

which implies $\sigma^*(m')/m' > Mm/\sigma^*(m) \geqq 2$, on using the previous lemma. This gives

$$\prod_{i=1}^{r} \frac{(p_i^{\beta_i} + 1)}{p_i^{\beta_i}} > 2. \tag{11}$$

Since $p_1^{\beta_1} < p_2^{\beta_2} < \cdots < p_r^{\beta_r}$ and each p_i is odd, we get $p_i^{\beta_i} \geq p_2^{\beta_2} + 2(i-1)$ for $i = 2, 3, \dots, t$. Hence, by the decreasing nature of $x/(x-1)$ and (11), we get

$$\prod_{i=1}^{r} \Big(\frac{p_1^{\beta_1} + 2i - 1}{p_1^{\beta_1} + 2i - 2}\Big)^2 > 4. \tag{12}$$

Again, using the fact that $x/(x-1)$ is a decreasing function of x, we have

$$\frac{p_1^{\beta_1}+2i-1}{p_1^{\beta_1}+2i-2} < \frac{p_1^{\beta_1}+2i-2}{p_i^{\beta_1}+2i-3}$$

for each i, from which we get from (12).

$$4 < \prod_{i=1}^{r} \left(\frac{{}_1^{\beta_1}+2i-1}{p_1^{\beta_1}+2i-2}\right)^2 < \prod_{i=1}^{r} \left(\frac{p_1^{\beta_1}+2i-1}{p_1^{\beta_1}+2i-2}\right)\left(\frac{p_i^{\beta_1}+2i-2}{p_1^{\beta_1}+2i-3}\right)$$

$$= \prod_{i=1}^{t} \left(\frac{p_i^{\beta_1}+2i-1}{p_i^{\beta_1}+2i-3}\right) = \frac{p_i^{\beta_1}+2t-1}{p_1^{\beta_1}-1}.$$

This gives

$$p_1^{\beta_1} < 1+2t/3 < 3t \le mt,$$

thus proving the lemma.

Lemma. *If $N \in T_M^*$ so that $\sigma^*(\omega)/N > M$, and $N = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$, with $p_1^{a_1} < p_2^{a_2} < \dots p_r^{a_r}$, then for $i = 2, 3, \dots, r$, we have*

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

Proof. Fix i and write $m = \prod_{j=1}^{i-1} p_j^{a_j}$. Then $m \| N$, $m \neq 1$, $m \neq N$, so that by the Lemma, $\sigma^*(m)/m < M$. Also using $\sigma^*(N) = 1 + MN$, we have $\sigma^*(N)/N > M$.

Now the result of the following lemma follows from the last lemma.

Lemma. *If $N = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r}$, with $p_1^{a_1} < p_2^{a_r}\dots p_r^{a_r}$, is such that $\sigma^*(N)/N > 2$, then $p_1^{a_1} < 1+2(r/3)$.*

Proof. This is implied in the result of the previous lemma (see the last sentence in its proof).

Proof of the last Theorem. Suppose $n = p_1^{a_1} < p_2^{a_2} < \cdots < p_r^{a_r}$, so that $\sigma^*(n)/n > 2$ and $r \ge 16$. Hence the last lemma gives $p_1^{a_1} < 1 + (2r/3) < r - 4$.

Now from the two last lemmas we successively have

$$\begin{aligned} p_2^{a_2} &< (r-1)p_1^{a_1} < (r-4)(r-1) < (r-1)^2 \\ p_3^{a_3} &< (r-2)p_1^{a_1}p_2^{a_2} < (r-2)(r-1)(r-4)(r-1) \\ &= (r-2)(r-4)(r-1)^2 < (r-1)^{2^2} \end{aligned}$$

and so on.

Hence

$$\begin{aligned} n &= p_1^{a_1}p_2^{a_2}\dots p_r^{a_r} \\ &< (r-1)(r-1)^2(r-1)^{2^2}\dots(r-1)^{2^{r-1}} \\ &= (r-1)^{2^{r-1}}. \end{aligned}$$

We can also establish the following theorem analogous to those for the φ and φ^* cases proved by Pomerance [6] and Prasad and Subbarao [13].

Theorem. *The number of $n \le x$ for which $n \in T^*(n)$ for any $n \ge 3$ is*

$$0\big(x^{1/2}\log^2 x(\log\log x)^{-1/2}\big).$$

We omit the proof.

Using computational methods as it was done by Hagis [5], we can obtain several results analogous to those of Hagis. For example,

Theorem. *If $\psi(n) = 1 + Mn$, where $M \ge 3$ and $(15, n) = 1$, then* $\omega(n) \ge 269$.

Proof. We adapt an idea due to Hagis [5]. From the relation $\psi(n) = 1 + Mn$, we get

$$M < \frac{\psi(n)}{n} = \prod_{p|n}(p+1)/p.$$

Assume now that $(15, n) = 1$. Take the set

$$S = \{7, 11, 17, 19, 23, 29, 31, 37, 41\}.$$

We shall say that a subset A (including possibly a nul set) of S is *feasible* if whenever $p \in A$ and $q \in A$, then $q+1 \not\equiv 0 \pmod{p}$. For each feasible subset A, define for $P \geq 41$ a prime,

$$F_A(P) = \prod_{pA} (p+1)/p \cdot \prod_{q=43}^{p}{}^{*} (q+1)/q,$$

where Π^* indicates that the product is taken over all primes q such that $q+1 \not\equiv 0 \pmod{p}$ if $p \in A$. If Q_A denotes the smallest prime P such that $F_A(P) \geq 3$, it follows from $M < (p+1)/p$ that if the set of prime factors of n which do not exceed 41 in A, then $\omega(n) \geq$ the number of prime factors in $F_A(Q_A)$ and $n \geq \prod_{p<A} p \cdot \prod_{q=43}^{Q_A}{}^{*} q$. A computer search showed $\min_A Q_A = 11981$ when A ran over all the feasible subsets of S. Also the 'minimal A' is

$$B = \{7, 11, 17, 19, 23, 29, 31\}$$

and the minimal product is

$$\prod_{p \in B} p \cdot \prod_{q=43}^{11981}{}^{*} q$$

and the minimal $\omega(n) = 269$. Hence the theorem follows.

Theorem. *If $\psi(n) = 1 + Mn$ and $3 \nmid n$, $n \neq$ a prime (so that $M \geq 3$), we have $\omega(n) \geq 123$.*

Proof. We proceed as in the previous theorem taking $S = \{5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$ and find $Q_A = 761$, and the minimal feasible set is $B = \{5, 7, 11, 17, 23, 31\}$.

5. Concluding remarks

We have considered only a few of the several possible results analogous to those for φ and φ^*.

The Lehmer problem and its unitary analogue can be integrated into a single general problem as was done by Prasad and this author [9] in terms of Narkiewich's regular convolution: However we shall not go into its details.

Finding *possible* characterizations of primes involving congruences for arithmetic functions is generally not an easy thing except in "obvious" cases. Thus it is easy to see that $\sigma(n)\varphi(n)|(n^2-1)$ is a characterization for n to be a prime. For distinct odd primes $p_1,\dots,p_r$, the result

$$p_1^2\dots p_r^2-2\equiv 0 \pmod{(p_1^2-2)\dots(p_r^2-2)}$$

is possible only if $r=1$. The author does not know if the same conclusion holds when the p_i^2 in the above are replaced by p_i^r for $r=1$ or $r>2$.

Consider the conguences

$$n\sigma(n)\equiv 2 \pmod{\varphi(n)}$$

and

$$\varphi(n)\tau(n)+2=0 \pmod{n}$$

which are satisfied by all primes. The only composite solutions of the former are $4, 6, 22$, whereas no composite solution other than 4 for the latter congruence is known so far. We refer to [15] for details.

References

[1] G. L. Cohen and Peter Hagis Jr., On the number of prime factors of n with $\varphi(n)|n-1$, *Nieuw Archief Voor Wiskinde* **XXVIII** no. 3 (1980), 177–185.

[2] M. Kishore, On the number of distinct prime factors of n for which $\varphi(n)|n-1$, *Nieuw Archief Voor Wiskunde* **XXV** no. 3 (1977), 48–53.

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

[4] E. Lieuwens, Do there exist composite M for which $k\varphi(M)=M-1$ holds?, *Nieuw Archief Voor Wiskunde* **XVIII** no. 3 (1970), 165–169.

[5] Peter Hagis Jr., On the equation $M\varphi(n)=n-1$, *Nieuw Archief Voor Wiskunde* **6** (1988), 255–261.

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

[7] Fr. Schuh, Do there exist composite numbers m for which $\varphi(m)|m-1$?, *(Dutch), Mathematica Zutpen* **B13** (1944), 102–107.

[8] V. Siva Rama Prasad and M. Rangamma, On composite n satisfying a problem of Lehmer, *Indian J. Pure. Math.* **16** no. 11 (1985), 1244–1248.

[9] V. Siva Rama Prasad and M.V. Subbarao, Regular convolutions and a related Lehmer problem, *Nieuw Archief Voor Wiskunde* **3** no. 4 (1985), 1–18.

[10] V. Siva Rama Prasad and M. Rangamma, On composite n for which $\varphi(n)|n-1$, *Nieuw Archief Voor Wiskunde, 4,* **V** (1989), 77–81.

[11] V. Siva Rama Prasad and M. Rangamma, On the forms of n for which $\varphi(n)|n-1$, *Indian J. Pure Maths.* **20** no. 9 (1989), 871–873.

[12] M. V. Subbarao, On the problem concerning unitary totient function $\varphi^*(n)$, *Notices Amer. Math. Soc.* **18** (1971), 940.

[13] M. V. Subbarao and V. Siva Rama Prasad, Some analogues of a Lehmer problem on the totient function, *Rocky Mountain Journal Math.* **15** (1985), 609–620.

[14] M. V. Subbarao, On composite n satisfying $\psi(n) \equiv 1 \pmod{n}$, *AMS Abstract #881-11-60* **14** (1993), 418.

[15] M. V. Subbarao, On two congruences for primality, *Pacific J. Math.* **52** (1974), 261–268.

M.V. SUBBARAO
UNIVERSITY OF ALBERTA
DEPARTMENT OF MATHEMATICAL SCIENCES
EDMONTON, ALBERTA
T6G 2G1
CANADA

(Received November 3, 1997; revised February 18, 1998)