Théorie des nombres · Number Theory
*J.-M. De Koninck & C. Levesque (éd.)*


# Carmichael's conjecture and some analogues

M.V. Subbarao* and L.W. Yip*

**Abstract**

Let $\varphi(x)$ be the Euler totient and $\Phi_k(x)$ be the Schemmel totient (a generalization of $\varphi(x)$). In this paper, we first review some results concerning the number $N(m)$ of solutions of $\varphi(x) = m$, and in particular the celebrated conjecture of Carmichael that there is no integer $m$ for which $N(m) = 1$. Later in the paper we consider for the first time in the literature, the analogue of Carmichael's conjecture for $\Phi_k(x)$. If $N_k(m)$ denotes the number of solutions of $\Phi_k(x) = m$, we prove that for each odd integer $k > 1$ there exist infinitely many $m$ for which $N_k(m) = 1$. We conjecture that there is no $x$ for which $N_2(\Phi_2(x)) = 1$, and prove that if such an integer $x$ exists, then $x > 10^{120000}$. Some other related conjectures are also given.

## Preliminaries

We write, as usual, $\varphi(n)$ for the Euler totient representing the number of natural numbers not exceeding $n$.

A generalization of $\varphi$ is the Schemmel totient $\Phi_k(n)$ introduced in 1869 (see [4], p. 147). It is a multiplicative function of $n$, with $\Phi_k(1) = 1$, and for primes $p$,

$$\Phi_k(p^a) = \begin{cases} 0 & \text{if } p \le k, \\ p^{a-1}(p-k) & \text{if } p > k. \end{cases}$$

The arithmetic interpretation of $\Phi_k(n)$ is that it gives the number of sets of $k$ consecutive integers not exceeding $n$ each of which is relatively prime to $n$.

At the end of the paper, we briefly refer to the unitary totient function $\varphi^*(n)$ which is a multiplicative function with $\varphi^*(p^a) = p^a - 1$. $\varphi^*(n)$ gives the number of natural numbers not exceeding $n$ and unitarily prime to $n$.

*Supported, in part, by NSERC grant No. A3103.

(An integer $m$ is said to be ***unitarily prime*** to $n$ if the largest divisor of $m$ which is a ***unitary divisor*** of $n$ is unity — a unitary divisor of $n$ being defined as a divisor $d$ of $n$ which is relatively prime to $n/d$.)

We write $N(m)$ (respectively $N_k(m)$) for the number of solutions of $\varphi(x) = m$ (respectively $\Phi_k(x) = m$). $N^*(m)$ has an analogous meaning for $\varphi^*(x) = m$. Also $p, p_1, p_2, \ldots, q_1, q_2, \ldots$ always denote primes. We write $p^a \parallel x$ to mean that $p^a \mid x$ but $p^{a+1} \nmid x$.

$\Psi(x, y)$ denotes the number of integers $n \leq x$ free of prime factors exceeding $y$, and $\Pi(x, y)$ denotes the number of primes $p \leq x$ so that $p - 1$ is free of prime factors exceeding $y$. Also $\pi(x)$ denotes the number of primes $\leq x$.

Finally, $c, c_1, \ldots$ stand for positive constants, not necessarily the same at each occurrence.

## 1. The distribution of values of $N(m)$

There are many interesting problems connected with $N(m)$, one of the oldest of these being Carmichael's conjecture that $N(m)$ never takes the value 1 (which P. Erdös thinks is a very deep problem). The behaviour of the function $N(m)$ is very erratic. For instance, $N(1438) = 2$, $N(1440) = 72$ while $N(1442) = N(1444) = 0$. It is therefore of interest to obtain an asymptotic estimate for $A(x;\varphi) \equiv \sum_{m \leq x} N(m) \equiv$ the number of positive integers $n$ with $1 \leq \varphi(n) \leq x$ (and similar estimates for the functions $N_2(m)$ and $N^*(m)$). Erdös [8] proved that $\lim_{x\to\infty} A(x;\varphi)/x$ exists. R.E. Dressler [6] not only gave a completely elementary proof of the Erdös result, but also evaluated the limit. Once the existence of the limit is known, it is comparatively easy to evaluate it, for example, by an abelian argument:

$$\lim_{x\to\infty} \frac{A(x;\varphi)}{x} = \frac{\zeta(2)\zeta(3)}{\zeta(6)},$$

where $\zeta$ denotes the Riemann zeta function.

In 1972; Bateman [1] gave an estimate for the error term involved, and proved that

$$A(x;\varphi) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}\, x + O\Big(x \exp\{-(1-\varepsilon)(\frac{1}{2}\log x \log\log x)^{1/2}\}\Big), \tag{1.1}$$

and conjectured that the error term is

$$O(x\ \exp\{-(\log x)^{1-\varepsilon}\}) \tag{1.2}$$

and holds for every positive $\varepsilon$. As far as we know, the conjecture is still open. Erdös thinks that possibly the absolute value of the error term is often as big as $x\exp(-c\log x/\log\log x)$ for some positive constant $c$. Some more on this later in Section 2. A. Ivić [13] generalized Bateman's result to cover a number of other arithmetic functions — with a better estimate for the order of the error term. However, Ivić's general result is not applicable to such well known arithmetic functions as $\sigma_r(n)$ (sum of the $r$-th powers of the divisors of $n$), $J_k(n)$ (the Jordan totient of order $k$) and $\Phi_k(n)$ (the Schemmel totient of order $k$). This defect was rectified very recently in a paper by one of us and R. Sitaramachandrarao [24], wherein a very general asymptotic formula with an error term is obtained for

$$A(x;f) \equiv \sum_{1\le m\le x} a_m,$$

where

$$a_m = \text{ number of solutions of the equation } f(n)=m,$$

or equivalently,

$$A(x;f) = \text{ number of natural numbers } n \text{ with } 1\le f(n)\le x.$$

The functions $f$ to which this formula is applicable include the Schemmel totient, the Jordan totient and their unitary analogues, among others.

For the Schemmel totient we have

$$A(x;\Phi_k) = A(\Phi_k)x + O(x(\delta(x))^c),$$

where

$$\begin{aligned} A(\Phi_k) &= \frac{\varphi(k)}{k}\prod_{p>k}\Big(1-\frac{1}{p}+\frac{1}{p-k}\Big), \\ \delta(x) &= \exp(-(\log x)^{(3/8)-\varepsilon}), \end{aligned}$$

and $c$ is any positive constant.

For the unitary totient $\varphi^*$, the corresponding result is

$$A(x;\varphi^*) = A(\varphi^*)x + O(x(\delta(x))^c),$$

where

$$A(\varphi^*) = \prod_p (1-p^{-1})\Big(1+\sum_{m=1}^{\infty}(p^m-1)^{-1}\Big).$$

Results for the upper and lower bounds for $N(m)$ are given in the next section.

Sierpinski conjectured that for each integer $k > 1$, there exist infinitely many $m$ such that $N(m) = k$. Erdös [9] showed that if there is one such $m$, then there are infinitely many. This is true even for $k = 1$, so that if Carmichael's conjecture that $N(m) \neq 1$ fails for one $m$, then it fails for infinitely many $m$. A. Schinzel [22] showed that Sierpinski's conjecture follows from his hypothesis $H$. We do not know if Carmichael's conjecture also follows from hypothesis $H$.

For the convenience of the reader, we quote Hypothesis $H$ below.

**Hypothesis H.** *Let $s$ be a natural number. Let $f_1(x), \ldots, f_s(x)$ be irreducible polynomials with integral coefficients, and for each polynomial the leading coefficient is positive, and there is no natural number $d > 1$ that is a divisor of each of the numbers $P(x) = f_1(x)f_2(x)\ldots f_s(x)$, $x$ being an integer. Then there exist infinitely many natural values of $x$ for which each of the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ is prime.*

## 2. Upper and lower bounds for $N(m)$: the results of Erdös and Pomerance

There are infinitely many $m$, such as $m = 2 \cdot 7^a$ for all $a > 0$, for which $N(m) = 0$. One can therefore ask: how many integers $m \leq x$ are there for which $N(m) > 0$. If $f(x)$ denotes this number, S.S. Pillai showed that

$$f(x) < cx/(\log x)^{(\log 2)/e}.$$

Erdös [7] improved this to

$$f(x) = O(x/(\log x)^{1-\epsilon})$$

for every positive $\varepsilon$ and every $x > x_0(\varepsilon)$. He utilized his result on the normal order of prime factors of $p - 1$ and a classical result of Hardy and Ramanujan on the number of integers $\leq x$ having exactly $k$ distinct prime factors. He also noted that Brun's method gives

$$f(x) > cx(\log\log x)^k/\log x, \qquad \text{for every} \quad k.$$

This has been further improved by Pomerance and Maier-Pomerance [21], wherein it is proved that

$$f(x) = \frac{x}{\log x}\exp\left((c + o(1))(\log\log\log x)^2\right)$$

for a certain explicit constant $c$.

We next ask for the upper and lower bounds for $N(m)$.

Pomerance [18] gave what he believes is the best possible upper bound, namely

$$N(m) \leq m \exp(-(1+o(1)) \log m \log\log\log m / \log\log m).$$

He has a heuristic argument that the above result is best possible in that there are infinitely many $m$ for which equality holds. The essence of this argument is as follows. In a forthcoming paper of Canfield, Erdös and Pomerance it is proved that

$$\frac{1}{x}\, \Psi(x,\ \exp(\log x)^{1/2}) = \exp(-(1+o(1))2^{-1}(\log x)^{1/2} \log\log x). \tag{2.1}$$

Now it is reasonable to expect that

$$\frac{1}{x}\, \Psi(x,y) \sim \frac{1}{\pi(x)} \Pi(x,y) \quad \text{for} \quad x > y \text{ and } y \to \infty.$$

In particular, they conjecture that this holds for $y = \exp(\log x)^{1/2}$. Based on this conjecture the above result (2.1) gives

$$\Pi(\exp((\log\log z)^2), \log z) = \exp((\log\log z)^2 - (1+o(1))(\log\log z)\log\log\log z).$$

With the help of this, Pomerance proves that the upper bound for $N(m)$ is actually attained for infinitely many $m$.

Next, regarding the lower bound for $N(m)$, probably the first result is due to S.S. Pillai who showed ([7]) that there are integers $m$ for which

$$N(m) > c(\log m)^{\log 2/e}.$$

Erdös ([7]) improved this by showing that Brun's method gives

$$N(m) > m^c \qquad \text{for infinitely many } m. \tag{2.2}$$

Actually, as pointed out by Pomerance ([18], Theorem B) one can extract from the paper [7] of Erdös much more than this; namely, suppose there is an $\varepsilon > 0$ such that $\Pi(x, x^u) > \varepsilon\pi(x)$ for all large $x$. Then there are infinitely many integers $m_1 < m_2 < \ldots$ such that $N(m_i) > m_i^{1-u}$ for each $i$, and in fact $\log m_{i+1}/\log m_i \to 1$ as $i \to \infty$.

What is the least upper bound $C$ for the values of $c$ for which (2.2) holds? Erdös conjectures that $C = 1$, and this is still open. Recently there is a succession of improvements to the value of $c$ in (2.2), beginning with Wooldridge's (see [25]) that

$$C \geq 3 - 2\sqrt{2} \approx 0.17157$$

(where he used Selbergs' upper bound sieve) to the latest published results of Pomerance [18] that $C > 0.55655$ and to the further improvement [20] that

$$C \geq 0.68$$

contained in his recent private communication to the first author dated June 16, 1987.

There is still a wide gap between this result and Erdös conjecture that $C = 1$.

**Remark 2.3.** Erdös' result (2.2) shows that the error term in (1.1) is $\neq o(x^c)$ for the same $c$ as in (2.2). After Erdös' conjecture that $C = 1$, Bateman makes the weaker conjecture that the error term in (1.1) is $\neq o(x^\lambda)$ for any $\lambda < 1$.

## 3. The Carmichael conjecture: on finding a counter-example

Several authors worked on the Carmichael conjecture, especially, in trying to find a counter-example to it. These include V.L. Klee ([14], [15]), H. Donnelly [5], E. Grosswald [11], C. Pomerance ([17], [18]), A. Schinzel [22], P. Erdös [9], P. Masai, A. Valette [16], besides of course Carmichael himself ([2], [3]).

Most of these authors tried to find a lower bound for a counter-example to the Carmichael conjecture by examining the structure of the integer $x$ for which $N(\varphi(x)) = 1$. Klee [14] showed that such an $x$ must be greater than $10^{400}$; the best lower bound so far known is $\varphi(x) > 10^{10000}$ due to P. Masai and A. Valette [16]. The technique used to get a lower bound for the counter-example $x$ is to find more prime factors of $x$ if we already know some, and is based on the ideas of Carmichael and Klee in their papers and may be summarized as follows.

**Theorem 3.1.** *Let $x = \prod_A p_i^{a_i}$ ($A$ being the range of $i$) be the intended counter-example $x$ to Carmichael's conjecture. Find a prime $p$ such that $p - 1 = \prod_B p_i^{a_i-1}(p_i - 1)\prod_C p_i^{c_i}$, where $B$ and $C$ are disjoint, possibly empty, subsets of $A$, such that $c_i \leq a_i - 1$ for $i$ in $C$. Then $p \mid x$. Further, if $B$*

*is such that for any $j$ in $B$ any prime divisor of $p_j - 1$ also divides $x$, then $p^2 \mid x$. In particular, this is true when $B$ is empty.*

The proof is simple and is found in [16].

Using simple arguments, we see that $2^2$ and $3^2$ divide $x$. These two factors can be used as a starting point to apply the theorem to get more and more prime factors of $x$, such as 7, 43 etc. If one has the patience and computer money, one can go on almost endlessly on improving the lower bound, because it is likely that we can build an endless sequence of primes $p$ dividing $x$ using the theorem.

## 4. The Pomerance theorem and conjectures

Instead of working on numerical estimates for $x$ for which $N(\varphi(x)) = 1$, Pomerance [17] gave an interesting and elegant sufficient condition for such an $x$ to exist, as follows.

**Theorem 4.1.** *Suppose $x$ is a natural number such that for every prime $p$, $(p-1) \mid \varphi(x)$ implies $p^2 \mid x$. Then $N(\varphi(x)) = 1$.*

However, no such $x$ is likely to exist. He showed that such an $x$ does not indeed exist if the following conjecture of his holds:

**Conjecture 4.2** (Pomerance). *If $p_i$ denotes the $i$-th prime, then for $k \geq 2$,*

$$(p_k - 1) \mid \prod_{i=1}^{k-1} p_i(p_i - 1).$$

If there is an $x$ which satisfies the condition of the theorem, then $2^2 \mid x$; and then the use of this conjecture gives successively that $3^2 \mid x$, $5^2 \mid x, \ldots$ for each of the succeeding squares of primes. This being impossible, there is no such $x$.

As Pomerance noted, his conjecture fails if there is a prime $q$ such that the smallest prime which is $\equiv 1 (\text{mod } q)$ is also $\equiv 1 (\text{mod } q^2)$.

However, there is no such prime $q$ if Schinzel's hypothesis $H_2$ ([23], p. 207) is true. It is quoted below for convenience.

$n(n-1)+k$

**Hypothesis $\mathbf{H_2}$.** *If for a natural number $n$ $(> 1)$ the numbers $1, 2, 3, \ldots, n^2$ are arranged in ascending order in $n$ rows, $n$ numbers in each row, then if $(k, n) = 1$, the $k$-th column contains at least one prime number.*

We see in the next section that these results and conjectures have their

$k$

$k+n$

$k+$

analogues in connection with our own conjecture for the Schemmel totient $\Phi_2(x)$, namely that there is no integer $x$ for which $N_2(\Phi_2(x)) = 1$.

## 5. Conjectures and results relating to $\Phi_2(x)$

Recalling the definition of $\Phi_2(x)$ given in Section 1, we see that $\Phi_2(x) = 0$ for all even $x$. Of course, $\Phi_2(x)$ does not take all odd values. For example, for any odd prime $p$ for which $p+2$ is not a prime, the equation $\Phi_2(x) = p$ has no solution. We recall that $N_2(m)$ denotes the number of solutions of $\Phi_2(x) = m$.

$\Phi_2$ always odd?

Let

$$(5.1) \qquad q_1, q_2, q_3, \ldots$$

be a sequence of primes defined as follows: $q_1 = 3$, and for each $n \geq 1$, $q_{n+1}$ is the smallest prime $> q_n$ for which $(q_{n+1} - 2) \mid (q_1 q_2 \ldots q_n)$.

We used a computer to calculate the first 10000 terms of this sequence. We got

$$q_{10000} = 4873801,$$

this being the 340256-th prime in the sequence of primes 2,3,5,7,11,$\cdots$ .

We make the following

**Conjecture 5.2.** *The sequence (5.1) of primes $q_n$ is infinite.*

**Remark 5.3.** The corresponding sequence of primes in the case of $\varphi(x)$ would be

$$r_1 = 2, r_2, r_3, r_4, \ldots,$$

where $r_{n+1}$ is the smallest prime $> r_n$ for which $r_{n+1} - 1$ divides $r_1 r_2 \ldots r_n$ $(n \geq 1)$. However this sequence has only four terms: 2, $3 = 2 + 1$, $7 = 2 \cdot 3 + 1$ and $43 = 2 \cdot 3 \cdot 7 + 1$. Note that the possible candidates for the next term are $15 = 2 \cdot 7 + 1$, $87 = 2 \cdot 43 + 1$, $259 = 2 \cdot 3 \cdot 43 + 1$, $603 = 2 \cdot 7 \cdot 43 + 1$ and $1807 = 2 \cdot 3 \cdot 7 \cdot 43 + 1$, and all these are composite.

The importance of the sequence (5.1) arises from the following

**Theorem 5.4.** *If there is an integer $m$ for which $\Phi_2(x) \doteq m$ has a unique solution, then $x \equiv 0 (\mathrm{mod}\ q_n^2)$ for each $n$.*

**Proof.** We argue along familiar lines and we give a proof for the sake of completeness.

We have $3 \mid x$, for otherwise $\Phi_2(3x) = \Phi_2(3)\Phi_2(x) = \Phi_2(x)$, contradicting $N_2(m) = 1$. Next $3^2 \mid x$, for otherwise $3 \parallel x$ and so $\Phi_2(x/3) = \Phi_2(x)$, again a contradiction.

Now suppose that $q_i^2 \mid x$ for all $1 \le i \le n$. Then if $q_{n+1} \nmid x$, let $q_{n+1} - 2 = q_{n_1} q_{n_2} \dots q_{n_r}$, where $n_1, n_2, \dots, n_r$ are distinct integers $\le n$, we have $\Phi_2(q_{n+1}(x/(q_{n_1} \cdots q_{n_r}))) = \Phi_2(x)$, contradicting $N_2(m) = 1$. Finally, if $q_{n+1} \parallel x$, then $\Phi_2(x q_{n_1} \dots q_{n_r}/q_{n+1}) = \Phi_2(x)$, a contradiction.

Thus $q_n^2 \mid x$ for all $n$. ∎

Evidently Conjecture 5.2 implies the following

**Conjecture 5.5.** *There is no integer $m$ for which $N_2(m) = 1$.*

In support of this conjecture, we have

**Theorem 5.6.** *If $N_2(\Phi_2(x)) = 1$, then $x > 10^{120000}$.*

**Proof.** By taking the first 10000 terms of the sequence, we get

$$(q_1 q_2 \cdots q_{10000})^2 \mid x.$$

Our conclusion follows from the fact that $\log_{10}(q_1 q_2 \dots q_{10000}) = 60341.9\dots$.
∎

The first few terms of the sequence $q_n$ are

3,5,7,17,19,23,37,53,59,61,71,73,97,107,109,113,
163,179,181,257,293,....

A complete list of the first 2000 terms of the sequence is available with the authors.

**Remark 5.7.** We could have easily constructed primes other than the $q_i$'s that divide $x$ as in the method used by Carmichael and Klee (described earlier in Section 3), but felt no need for them as there is an abundance of the $q_i$'s available.

Analogous to the Pomerance results and conjectures we have the following

**Theorem 5.8.** *If there is a natural number $x$ such that for every odd prime $p$, $(p-2) \mid \Phi_2(x)$ implies $p^2 \mid x$, then $N_2(\Phi_2(x)) = 1$.*

The proof is similar to that of Pomerance for his theorem in [17] and is therefore omitted.

There is no such integer $x$ described in the theorem if the following conjecture holds.

**Conjecture 5.9.** *Let $p_i$ denote the $i$-th odd prime. Then for $k \geq 2$,*

$$(p_k - 2) \mid \prod_{i=1}^{k-1} p_i(p_i - 2).$$

**Remark 5.10.** As Pomerance stated about his conjecture in [17], we wish to note that our conjecture 5.9 fails if there is a prime $p$ such that the smallest prime which is $\equiv 2 (\mathrm{mod}\ p)$ is also $\equiv 2 (\mathrm{mod}\ p^2)$. If Schinzel's hypothesis $H_2$ holds, then there is no such $p$.

**Remark 5.11.** One might be tempted to make a more general conjecture, namely, that for the sequence of primes $p_1 = 2,\ p_2 = 3, \ldots,$

$$(p_{n+1} - k) \mid \prod_{\substack{i \leq n \\ p_i > k}} p_i(p_i - k).$$

However, this can be false in general. For instance, it is false for $k = 3$ (take $p_{n+1} = 7$) and $k = 4$ (take $p_{n+1} = 7$).

## 6. The case $\Phi_k(x)$, $k > 2$

We first prove the following

**Theorem 6.1.** *For any given odd integer $k > 1$, there are infinitely many integers $m$ for which $N_k(m) = 1$.*

**Proof.** Take any odd prime $p > k$ which satisfies

$$p \equiv \begin{cases} 1 (\mathrm{mod}\ 4) & \text{if } k \equiv 3 (\mathrm{mod}\ 4), \\ 3 (\mathrm{mod}\ 4) & \text{if } k \equiv 1 (\mathrm{mod}\ 4), \end{cases}$$

as well as

$$p \equiv (k+1)\ (\mathrm{mod}(2k+1)).$$

We note that there are infinitely many such $p$, in view of $(k+1, 2k+1) = 1$ on utilizing Dirichlet's theorem for primes in an arithmetic progression and Chinese remainder theorem.

Take $m = p^2 - kp$. Then the equation $\varphi_k(x) = m$ has the solution $x = p^2$. We claim that this is the only solution.

Suppose $x_0$ is a solution to $\Phi_k(x) = m = p(p - k)$.

By our choice of $p$, $2 \parallel p(p-k) = \Phi_k(x_0)$. Thus $x_0$ is divisible by only one prime, say $x_0 = q^a$, $q$ being an odd prime. It remains to show that $q = p$ (note that this implies $a = 2$ immediately).

If $q \neq p$, then $p \mid (q-k)$, and so $q > p$. Furthermore, if $a \geq 2$, then

$$\Phi_k(\frac{x_0}{q}) = \frac{\Phi_k(x_0)}{q} = \frac{p(p-k)}{q},$$

which implies $q \mid p(p-k)$, but this is impossible since $q > p > p-k$. Hence $a = 1$, and consequently $q - k = \Phi_k(x_0) = p(p-k)$, and this implies that $q = p(p-k) + k \equiv 0(\mathrm{mod}(2k+1))$ by our choice of $p$. This is possible only if $q = 2k+1$. But then $k+1 = q-k = p(p-k) \geq 2(k+1)$, a contradiction.

Thus we have shown that $q = p$, and the theorem is proved. ∎

We may have $N_k(m) = 1$ for certain even values of $k$ also, as seen from the following

**Theorem 6.2.** *Let $p, q$ be odd primes with $p > q$, $p \neq 2q-1$ such that*

(6.3) $p - q + 1$ *is also a prime,*

(6.4) $2q - 1$ *is not a prime, and*

(6.5) $q(p-q+1) + q - 1$ *is not a prime.*

*Then $N_{q-1}(q(p-q+1)) = 1$, the unique solution being $q^2p$.*

**Proof.** Clearly, $x = q^2p$ is a solution of $\Phi_{q-1}(x) = q(p-q+1)$. The conditions (6.3)–(6.5) ensure that there is no other solution. For instance, if we drop (6.4), then $x = (2q-1)p$ is another solution, and if we drop (6.5), then $x = q(p-q+1) + q - 1$ would provide a solution. ∎

**Example 6.3.** The only solution of $\Phi_{46}(x) = 47 \cdot 7 = 329$ is $x = 47^2 \cdot 53$.

## 7. Concluding remarks

The analogue of Carmichael's conjecture for the unitary totient $\varphi^*$ is false, for if $2^p - 1$ is a Mersenne prime, then $N^*(2^p-1) = 1$. Pomerance noted in a private communication to the first author that $N^*(4(2^p-1)) = 1$ provided $2^p - 1$ is a prime with $p \equiv 1(\mathrm{mod}\ 4)$ (though this primality condition may not be necessary). The determination of all the $n$ for which $N^*(n) = 1$ is an open problem. For some other results concerning the equation $\varphi^*(x) = m$, we refer to [10].

The truth of the Carmichael conjecture implies that:

(7.1) The equation $\varphi(\varphi(x)) = m$ (for a given $m$) has either no solution or at least two solutions. Is the reverse implication also true?

We wish to remark that for certain values of $m$, the equation $\varphi(\varphi(x)) = m$ has exactly two solutions. For instance, when $m = 10$ we have

$$\varphi(\varphi(x)) = 10 \Rightarrow \varphi(x) = 11 \quad \text{or} \quad 22,$$

and this implies $x = 23$ or $46$. More generally, we have the following:

(7.2) Let $m$ be an even integer such that $\frac{1}{2}m$ and $m+1$ and $2m+3$ are all prime. Then the equation

$$\varphi(\varphi(x)) = m$$

has exactly two solutions, namely, $x = 2m+3$ and $4m+6$.

Another observation that we would like to make is the following. There may be certain even integers $k > 2$ for which the analogue of Carmichael's conjecture may hold. We may use here reasoning similar to that employed in section 5. Let $q_1 = k+1$, $q_2 = 2k+1$ be both prime and let $q_{n+1} (n \geq 2)$ be the smallest prime greater than $q_n$ for which $(q_{n+1} - k) | (q_1 q_2 \dots q_n)$. The analogue of theorem 5.4 holds, namely, if $\Phi_k(x) = m$ has a unique solution, then $q_n^2$ divides $x$ for each $n$. Hence if the sequence of prime, $q_1, q_2, \dots$ is infinite, we would have $N_k(m) \neq 1$ for any $m$. The matter is being investigated further and we plan on submitting a separate paper later on.

The authors thank the referee for many useful suggestions.

## REFERENCES

[1] P.T. Bateman, *The distribution of values of the Euler function*, Acta Arith. **21** (1972), 329-345.

[2] R.D. Carmichael, *On Euler's $\phi$-function*, Bull. Amer. Math. Soc. **13** (1907), 241-243.

[3] R.D. Carmichael, *Note on Euler's $\phi$-function*, Bull. Amer. Math. Soc. **28** (1922), 109-110.

[4] L.E. Dickson, *History of the theory of numbers*, **vol.I**, Chelsea, 1971.

[5] H. Donnelly, *On a problem concerning Euler's phi-function*, Amer. Math. Monthly **80** (1973), 1029-1031.

[6] R.E. Dressler, *A density which counts multiplicity*, Pacific J. Math. **34** (1970), 371-378.

[7] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's $\varphi$-function*, Quart. J. Math. (Oxford Series) **6** (1935), 205-213.

[8] P. Erdös, *Some remarks on Euler's $\varphi$ function and some related problems*, Bull. Amer. Math. Soc. **51** (1945), 540-544.

[9] P. Erdös, *Some remarks on Euler's $\varphi$ function*, Acta Arith. **4** (1958), 10-19.

[10] P. Erdös and R.R. Hall, Distinct values of Euler's $\phi$-function, Mathematica **23** (1976), 1-3.

[11] E. Grosswald, *Contribution to the theory of Euler's function $\varphi(x)$*, Bull. Amer. Math. Soc. **79** (1973), 337-341.

[12] M. Ismail and M.V. Subbarao, *Unitary analogue of Carmichael's problem*, Indian J. Math. **18** (1976), 49-55.

[13] A. Ivić, *The distribution of values of some multiplicative functions*, Publications de l'Institut Mathematique, Nouvell serie, **22(33)** (1977), 87-94.

[14] V.L. Klee, *On a conjecture of Carmichael*, Bull. Amer. Math. Soc. **53** (1947), 1183-1186.

[15] V.L. Klee, *Is there an $n$ for which $\phi(x) = n$ has a unique solution?*, Amer. Math. Monthly **76** (1969), 288-289.

[16] P. Masai and A. Valette, *A lower bound for a counterexample to Carmichael's conjecture*, Bollettino delta Unione Matematica Italiana, Serie **VI, 1-A** (1982), 313-316.

[17] C. Pomerance, *On Carmichael's conjecture*, Proc. Amer. Math. Soc. **43** (1974), 297-298.

[18] C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), 84-89.

[19] C. Pomerance, *On the distribution of the values of Euler's function*, Acta Arith. **XLVII** (1986), 63-70.

[20] C. Pomerance, *On the number of groups of square free order*, Proc. Amer. Math. Soc. **99** (1987), 223-231.

[21] H. Maier and C. Pomerance, *On the number of different values of the Euler function*, Acta Arith., to appear.

[22] A. Schinzel, *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961), 1-8.

[23] A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185-208.

[24] M.V. Subbarao and R. Sitaramachandrarao, *The distribution of values of a class of arithmetic functions*, Studia Scientiarum Mathematicarum Hungarica **20** (1985), 77-87.

[25] K.R. Wooldridge, *Values taken many times by Euler's phi function*, Proc. Amer. Math. Soc. **76** (1979), 229-234.

M.V. Subbarao
Department of Mathematics
University of Alberta
Edmonton, Alberta
Canada T6G 2G1

L.W. Yip
Department of Mathematics
University of Alberta
Edmonton, Alberta
Canada T6G 2G1