Canad. Math. Bull.Vol. **34** (3), 1991 pp. 401–404

ON SIERPINSKI'S CONJECTURE CONCERNING THE EULER TOTIENT

M. V. SUBBARAO AND L. W. YIP

ABSTRACT. If $\Phi_k(n)$ denotes the Schemmel totient (so that $\Phi_1(n)$ becomes the Euler totient) we conjecture that for each $k \geq 1$ and any given integer $n > 1$ there exist infinitely many m for which the equation $\Phi_k(x) = m$ has exactly n solutions. For the case $k = 1$, this gives Sierpinski's conjecture.

We prove that on the basis of Schinzel's Hypothesis H, our conjecture holds for any $k \geq 3$ of the form $p_0^\alpha - 2$ where p_0 is an odd prime and $\alpha \in \mathbb{N}$. In 1961 Schinzel proved the case $k = 1$ assuming his Hypothesis H.

1. **Introduction.** Let $\varphi(n)$ denote, as usual, the Euler totient representing the number of natural numbers not exceeding n and relatively prime to n. This function has been generalized in several directions. Here we will concern ourselves with the generalization known as the Schemmel totient Φ_k (for a fixed natural number k). Φ_k is defined as follows: $\Phi_k(1) = 1$, $\Phi_k(n) = 0$ if n contains a prime factor not exceeding k, and if all the prime factors of n are greater than k, then

$$\Phi_k(n) = \prod_{p^a \| n} p^{a-1}(p-k),$$

where $p^a \| n$ means $p^a | n$ and $p^{a+1} \nmid n$.

More than thirty years ago, W. Sierpinski (see [3]) made the following conjecture:

For any given integer $n > 1$, there exist infinitely many m for which the equation $\varphi(x) = m$ has exactly n solutions.

A. Schinzel [4] showed that his Hypothesis H (quoted in Section 2) implies the truth of Sierpinski's conjecture.

The purpose of this paper is to make a similar conjecture for the function Φ_k, and prove that for a certain type of integers k, this conjecture follows also from Hypothesis H. However, we are unable to settle this conjecture for an arbitrary k even on the basis of Hypothesis H.

2. **Preliminaries.** Denote by $\mathbb{N}$ the set of all natural numbers.

Let $N_k(m)$ denote the number of solutions of the equation $\Phi_k(x) = m$. We write $N(m)$ for $N_1(m)$. It is easy to see that $N_k(m) = 0$ whenever k and m (> 1) are of same parity. Similar to Sierpinski's conjecture, we make the following:

The first author was supported in part by an NSERC research grant.
Received by the editors November 16, 1989.

CONJECTURE 2.1. *Let k be a fixed natural number (including 1). For any given integer $n > 1$, there exist infinitely many m such that $N_k(m) = n$.*

REMARK 2.2. We exclude the case $n = 1$ because of the still unproved conjecture of Carmichael ([1], [2]) which says that $N(m)$ is never equal to 1. Incidentally, the Carmichael conjecture can be extended to N_k for some even natural numbers k (see [6] or [7]).

We now state Schinzel's Hypothesis H ([4], [5]) in two equivalent forms.

2.3. Let $s \in \mathbf{N}$. 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 integer $d > 1$ that is a divisor of each of the numbers $f_1(x) \cdot f_2(x) \cdots f_s(x)$, x being an integer. Then there exist infinitely many natural values of x for which the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ are all primes.

2.4. Let $f_1(x), f_2(x), \ldots, f_s(x)$, $g_1(x), g_2(x), \ldots, g_t(x)$ be irreducible integer-valued polynomials of positive degree with positive leading coefficients. If there does not exist any integer > 1 dividing the product $f_1(x) \cdot f_2(x) \cdots f_s(x)$ for every $x \in \mathbf{N}$, and if $g_j(x) \not\equiv f_i(x)$ for all $i \le s, j \le t$, then there exist infinitely many positive integers x such that the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ are primes and the numbers $g_1(x), g_2(x), \ldots, g_t(x)$ are composite.

REMARK 2.5. We wish to point out that while Hypothesis H implies Sierpinski's conjecture, it is an open problem whether it also implies the truth of the Carmichael conjecture.

3. The main result.

We prove the following:

THEOREM 3.1. *Let $k \geqq 3$ be of the form $p_0^\alpha - 2$, where p_0 is an odd prime and $\alpha \in \mathbf{N}$. Then Hypothesis H implies that for any given integer $n > 1$, there exist infinitely many integers m such that $N_k(m) = n$.*

PROOF. Let q_0 denote the smallest prime factor of $k + 4$, and let $r = \frac{(p_0-1)(q_0-1)}{2}$.

Set $A = \{a \in \mathbf{N} : (p_0 - 1) \nmid a\} = \{a_1, a_2, a_3, \ldots\}$, where $1 = a_1 < a_2 < a_3 < \ldots$ (note that $a_i < 2i$ for all i since A contains all odd numbers).

For any given $n > 1$, consider the irreducible polynomials defined by

$$f_i(x) = 2x^{a_i} + k, \quad f_{n+i}(x) = 2x^{m-a_i} + k, \quad i = 1, 2, \ldots, n; \quad f_{2n+1}(x) = x.$$

The irreducibility of $2x^a + k$ follows from Eisenstein's criterion.

EISENSTEIN'S CRITERION. Let I be a unique factorization domain. If $f(x)$ is a polynomial $f(x) = a_0 + a_1x + \cdots a_nx^n$ in $I[x]$ such that for a prime element p in I, $a_n \not\equiv 0 \pmod p$, $a_{n-1} \equiv a_{n-2} \equiv \cdots \equiv a_0 \equiv 0 \pmod p$ but $a_0 \not\equiv \quad (\mathrm{mod}\ p^2)$ then $f(x)$ is irreducible over the field of quotients of I.

Note that since k is odd, the criterion is applicable to $2x^a + k$ with $p = 2$. Note also that $m - a_n > a_n$, so that $f_{n+i}(x)$ $(1 \le i \le n)$ is distinct from $f_1(x), \ldots, f_n(x)$.

We have $\prod_{i=1}^{2n+1} f_i(1) = p_0^{2\alpha n}$. Let u be a primitive root modulo p_0. Observe that $2u^a + k \equiv 0 \pmod{p_0}$ if and only if $(p_0 - 1)|a$. Since, by the definition of A, $(p_0 - 1) \not| a_i$ and $(p_0 - 1) \not| (m - a_i)$ for all $1 \leq i \leq n$, we conclude that $p_0 \not| \prod_{i=1}^{2n+1} f_i(u)$. Therefore, the condition of Hypothesis H is satisfied.

Define $b_1 < b_2 < \ldots < b_{(r-2)n}$ in such a way that

$$\{b_1, b_2, \ldots, b_{(r-2)n}\} = \{1, 2, \ldots, rn\} \setminus \bigcup_{i=1}^{n} \{a_i, m - a_i\},$$

and define

$$g_j(x) = 2x^{b_j} + k, \quad j = 1, 2, \ldots, (r-2)n;$$

By Hypothesis H (2.4), there exist infinitely many integers x_0—which we may obviously assume to be different from g_0—such that all the $f_i(x_0)$ $(1 \leq i \leq 2n+1)$ are prime and all the $g_j(x_0)$ $\big(1 \leq j \leq (r-2)n+1\big)$ are composite (in particular, $2x_0^m + k$ and $4x_0^m + k$ are composite).

Also $4x_0^m + k$ is composite when x is a prime different from q_0. This follows from Fermat's theorem since $(q_0 - 1)$ divides r and the fact that q_0 divides $k + 4$.

Consider, for such an x_0 with $x_0 > k + 4$, the equation

3.2 $$\Phi_k(y) = 4x_0^m.$$

If y is a solution of (3.2), then obviously y can have at most two distinct prime factors, i.e. y is of the form p^a or $p^a q^b$ $(p, q$ denote primes). If $a > 1$, then $p(p-k)|4x_0^m$, so $p = x_0$ and $(x_0 - k)|4x_0^m$, which is impossible since $x_0 > k + 4$. Similarly we must have $b = 1$ in the latter case. If $y = p$, then $p - k = 4x_0^m$, i.e. $p = 4x_0^m + k$, contradicting the compositeness of $4x_0^m + k$. Now we conclude that $y = pq$ for some distinct primes p, q, and we may write (3.2) as

$$\left(\frac{p-k}{2}\right)\left(\frac{q-k}{2}\right) = x_0^m.$$

Both factors on the left-hand side are greater than 1 (otherwise we would get a contradiction to the compositeness of $2x_0^m + k$). It follows that $\{p, q\} = \{f_{i_0}(x_0), f_{n+i_0}(x_0)\}$ for some $1 \leq i_0 \leq n$, i.e. $y = f_{i_0}(x_0) f_{n+i_0}(x_0)$.

Obviously, for any $i \in \{1, 2, \ldots, n\}$, $f_i(x_0) f_{n+i}(x_0)$ is a solution of (3.2). Thus (3.2) has exactly n solutions. This completes the proof.

REMARK 3.3. It is shown elsewhere that for any odd $k > 1$, there are infinitely many integers m for which $N_k(m) = 1$ (see [6] or [7]). That is why we exclude the case $n = 1$ in the above theorem. In a certain sense, this theorem is an extension of Schinzel's work on Sierpinski's conjecture. We would expect that this theorem holds for any k as stated in Conjecture 2.1. However, it seems to be extremely difficult to settle this problem.

The authors sincerely thank the referee for valuable suggestions.

REFERENCES

1. R. D. Carmichael, *On Euler's ϕ-function*, Bull. Amer. Math. Soc. **13**(1907), 241–143.

2. ______, *Note on Euler's ϕ-function*, Bull. Amer. Math. Soc. **28**(1922), 109–110.

3. P. Erdős, *Some remarks on Euler's φ-function*, Acta Arith. **4**(1958), 10–19.

4. A. Schinzel, *Remarks on the paper 'Sur certaines hypothèses concernant les nombres premiers'*, Acta Arith. **7**(1961), 1–8.

5. A. Schinzel and W. Sierpinski, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4**(1958), 185–208.

6. M. V. Subbarao and L. W. Yip, *Carmichael's conjecture and some analogues*. Proc. Int. Number Theory Conf. Univ. Laval 1987, De. Koninck and Levesque ed., Berlin: Walter de Gruyter, 1989, 928–941.

7. L. W. Yip, *On Carmichael type problems for the Schemmel totients and some related questions*. Doctoral Thesis, Univ. of Alberta, 1989.

Department of Mathematics
University of Alberta
Edmonton, Alberta T6G 2G1