Indian J. pure appl. Math., **20** (9) : 871-873, September 1989

ON THE FORMS OF n FOR WHICH $\varphi(n) \mid n-1$

V. SIVA RAMA PRASAD AND M. RANGAMMA
Department of Mathematics, Osmania University, Hyderabad 500007

(*Received* 19 *December* 1988)

The forms of n for which $\varphi(n) \mid n-1$, where $\varphi(n)$ is the Euler totient function are obtained in this paper.

§1. Let $\varphi(n)$ denote the Euler totient function. It is obvious that

$$\varphi(n) \mid n-1 \qquad \ldots(1.1)$$

if n is a prime. Lehmer[2] asked whether there is any composite number n for which (1.1) holds. This unsolved problem, which is as deep as the odd perfect number problem, has several partial answers. To mention few, Lehmer[2] has proved that any such n, if exists, is odd, squarefree and that if p, q are distinct prime factors of n then $p \not\equiv 1 \pmod{q}$. More recently Cohen and Hagis[1] established that such n must have at least 14 distinct prime factors, while the authors[3] have proved that certain types of composite numbers can not satisfy (1.1). For further details and analogues of the problem we refer to Subbarao and Prasad[4] and Prasad and Subbarao[5].

In this note we find the forms in which the composite n satisfying (1.1) should be, if exists (Theorem 2.1).

§2. In all that follows n denotes a composite number for which (1.1) is true so that, by the above paragraph we can write

$$n = p_1 p_2 p_3 \ldots p_r \qquad \ldots(2.1)$$

where $p_1 < p_2 < \ldots < p_r$ are odd primes ;

$$p_i \not\equiv 1 \pmod{p_j} \text{ for } i \neq j ; \qquad \ldots(2.2)$$

and if $w(n)$ is the number of distinct prime factors of n then

$$r = w(n) \geqslant 14. \qquad \ldots(2.3)$$

Let s denote the number of $p_i \equiv -1 \pmod 3$. Then we have $s \leqslant r$ and the equality holds if and only if $p_i \equiv -1 \pmod 3$ for $1 \leqslant i \leqslant r$. Moreover if $p_1 = 3$ then by (2.2), we have $s = r - 1$.

Theorem 2.1—Suppose n is as in (2.1)

(i) If $p_1 = 3$ then n is of the form $2^{14}\ 3^2\ m + 81921$ or $2^{14}\ 3^2 m + 131073$ according as s is even or odd.

(ii) If $p_1 > 3$ then n is of the form $2^{14}\ 3m + 1$ or $2^{14}\ 3m + 65537$ according as s is even or odd.

PROOF : Since $\varphi(n) = (p_1 - 1)(p_2 - 1) \ldots (p_r - 1) \equiv O \pmod{2^r}$ we get, by (2.3) and (1.1), that

$$n - 1 \equiv O \pmod{2^{14}}. \qquad \ldots(2.4)$$

(i) Suppose $p_1 = 3$. Then by (2.2), $p_i \equiv -1 \pmod 3$ for $2 \leqslant i \leqslant r$ so that $n/3 = p_2\ p_3 \ldots p_r \equiv (-1)^s \pmod 3$ and therefore

$$n = 9l + 3(-1)^s \text{ for some integer } l. \qquad \ldots(2.5)$$

If s is even, (2.5) gives $n = 9l + 3$ and (2.4) shows that l satisfies the congruence $9l + 2 \equiv O \pmod{2^{14}}$. That is, $l \equiv 9102 \pmod{2^{14}}$. Writing $l = 2^{14}m + 9102$, we get $n = 2^{14}\ 3^2 m + 81921$

If s is odd, (2.5) gives $n = 9l - 3$ for some integer l and by (2.4), l must be such that $9l \equiv 4 \pmod{2^{14}}$. That is $l \equiv 14564 \pmod{2^{14}}$ and hence $n = 2^{14}\ 3^2\ m + 131073$ for some integer m.

(ii) If $p_1 > 3$ then, by (2.1), $n \equiv (-1)^s \pmod 3$.

Now if s is even, then $n \equiv 1 \pmod 3$ which together with (2.4) implies $n \equiv 1 \pmod{2^{143}}$, proving the first part of (ii).

When s is odd, $n = 3u - 1$ for some integer u, which must satisfy the congruence $3u \equiv 2 \pmod{2^{14}}$, by (2.4). That is $u \equiv 21846 \pmod{2^{14}}$ and hence $n = 2^{14}.\ 3m + 65537$ for some integer m.

Theorem 2.2—Suppose n is as in (2.1) with $p_1 > 3$.

(i) If $s < r$ then n is of the form $2^{14}\ 3m + 1$.

(ii) When $s = r$ we have n is of the form $2^{14}\ 3m + 1$ if and only if s is even.

PROOF : (i) If $s < r$ then $p_i \equiv 1 \pmod 3$ for at least one i so that $\varphi(n) \equiv O \pmod 3$ and hence $n \equiv 1 \pmod 3$. This together with (2.4) proves the first part.

(ii) Suppose $s = r$. If s is even, then, by (2.1), $n \equiv 1 \pmod 3$ which combined with (2.4) shows that n is of the form $2^{14}\ 3m + 1$.

Conversely if $n = 2^{14}\ 3m + 1$ then $n \equiv 1 \pmod 3$ and by (2.1), $n \equiv (-1)^s \pmod 3$ so that $(-1)s \equiv 1 \pmod 3$ proving s is even.

Corollary 2.3—Suppose n is as in (2.1) with $p_1 > 3$. Then n is of the form $2^{14}\ 3m + 65537$ if and only if $s = r$ and s is odd.

PROOF : Follows from (ii) of Theorem 2.1 and 2.2.

Remark : Cohen and Hagis[1] have proved that $n > 10^{20}$ while Subbarao and one of the authors[5] showed that $n < (r-1)^{2^{r-1}}$, where $r = w(n)$. Hence if r is an integer such that there is no m in the above forms with $10^{20} < m < (r-1)^{2^{r-1}}$ then $w(n) > r$, for n satisfying (1.1).

REFERENCES

1. G. L. Cohen and P. Hagis Jr, *Nieuw Archief Voor Wiskunde* (3), XXVIII (1980), 177-85.
2. D. H. Lehmer, *Bull. Am. Math. Soc.* **38** (1932), 745-51.
3. V. Sivarama Prasad and M. Rangamma, *Nieuv Archief Voor Wiskunde* **5** (1987), 77-81.
4. M. V. Subbaraoand V. Sivarama Prasad, *Rocky Mountain J. Math.* **15** (1985), 609-20.
5. V. Sivarama Prasad and M. V. Subbarao, *Nieuw Archief Voor Wiskunde* **3** (1985), pp 1-18.