[6] János Galambos, *The largest coefficient in continued fractions and related problems* in *Diophantine Approximation and its Applications*, ed. by Charles Osgood, Academic Press, 1973.
[7] — *An iterated logarithm type theorem for the largest coefficient in continued fractions*, Acta Arith. 25 (1974), pp. 359–364.
[8] Walter Philipp, *Some metrical theorems in number theory*, Pacific J. Math. 20 (1967), pp. 109–127.
[9] — *Some metrical theorems in number theory II*, Duke Math. J. 37 (1970), pp. 447–458, Errata, ibid., p. 788.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois

Received on 21.2.1974 (535)

ACTA ARITHMETICA
XXVIII (1976)

On composite n for which $\varphi(n) \mid n-1$

by

CARL POMERANCE (Athens, Ga.)

§ 1. Introduction. In [4], D. H. Lehmer asked if there are any composite natural numbers n for which $\varphi(n) \mid n-1$, where φ is Euler's function. This is still an unanswered question, many people feeling it is as difficult as the odd perfect number problem. There have been partial results however, such as: if such an n exists then n is divisible by at least 11 distinct primes, and if $3 \mid n$, then $n > 5.5 \cdot 10^{570}$ and n is divisible by at least 212 distinct primes (Lieuwens [5]).

If A is an arbitrary set of positive integers, then we denote by $N(A, x)$ the number of members of A which do not exceed x. Let F denote the set of composite n for which $\varphi(n) \mid n-1$. In [6] we proved

$$N(F, x) = O\left[x \exp\left(-c_1 (\log x \log\log x)^{1/2}\right)\right] \tag{1}$$

for some $c_1 > 0$. If $n \in F$, then $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ for every a with $(a, n) = 1$, that is, n is a Carmichael number (also called an absolute pseudoprime). Hence a result of Knödel [3] dealing with Carmichael numbers also implies (1). However, a result of Erdös [1], also dealing with Carmichael numbers, gives the better estimate

$$N(F, x) = O\left[x \exp\left(-c_2 \log x \log\log\log x / \log\log x\right)\right]$$

for some $c_2 > 0$. In the present note, borrowing somewhat the methods of Knödel and Erdös, we prove

$$N(F, x) = O\left(x^{2/3} (\log\log x)^{1/3}\right). \tag{2}$$

In fact we prove a more general theorem for which (2) is a special case. Indeed, in [6] we considered the sets

$$F(a) = \{n:\ n \equiv a \left(\mathrm{mod}\, \varphi(n)\right)\},$$
$$F'(a) = \{n \in F(a):\ n \neq pa \text{ for each prime } p \nmid a\},$$

where a is an arbitrary integer. We prove that for any a,

$$N\left(F'(a), x\right) = O\left(x^{2/3} (\log\log x)^{1/3}\right). \tag{3}$$

Since $F'(1) = F\cup\{1\}$, by taking $a = 1$ in (3), we have (2).

The proof we present below is fairly simple. In a paper to appear using more complicated methods we shall prove an estimate stronger than (3). We record the following

CONJECTURE. *For every integer a and every $\varepsilon > 0$, we have*

$$N(F'(a), x) = O(x^{\varepsilon}).$$

§ 2. The proof of (3). From Theorem 328 in Hardy and Wright [2], p. 267, it follows that there is a constant α such that

$$\alpha > n/\varphi(n)\log\log n \tag{4}$$

for every $n \geqslant 3$. We now restate a lemma from [6]:

LEMMA. *Let a be an integer, c a natural number, and p_1, p_2 primes with* (i) $p_i \nmid c$, (ii) $p_i > 1+2\alpha\log\log c$ *if* $c \geqslant 3$, (iii) $p_i c > 64a^2$, *and* (iv) $p_i c \in F'(a)$ *for* $i = 1, 2$. *Then* $p_1 = p_2$.

We now show that (3) holds for every a. We first note that (3) is true if $a = 0$. Indeed, Sierpiński ([7], p. 232) showed that

$$F(0) = \{1\}\cup\{2^i\cdot 3^j\colon\ i > 0, j \geqslant 0\},$$

so that $N(F(0), x) \sim (\log x)^2/2\log 2\log 3$. Hence we may assume $a \neq 0$.

Let now x be large, $n \leqslant x$, $n \in F'(a)$. We may assume that $n > x^{2/3}(\log\log x)^{1/3}$. Consider the two cases:

(i) there is a prime $p|n$ with $p > x^{1/3}(\log\log x)^{-1/3}$;

(ii) every prime $p|n$ satisfies $p \leqslant x^{1/3}(\log\log x)^{-1/3}$.

Suppose case (i) holds. If $p^2|n$, then $p|\varphi(n)$, so $p|a$. Clearly this fails for large x (since $a \neq 0$), so we may assume $n = pc$ where $p \nmid c$. Then $c < x^{2/3}(\log\log x)^{1/3}$. Note that for large x, the lemma guarantees for such c at most a single choice for $p > x^{1/3}(\log\log x)^{-1/3}$ with $pc \in F'(a)$. Hence the number of n for which (i) holds is less than $x^{2/3}(\log\log x)^{1/3}$.

Suppose now case (ii) holds. Then n has a proper divisor m with

$$x^{1/3}(\log\log x)^{2/3} < m \leqslant x^{2/3}(\log\log x)^{1/3}. \tag{5}$$

Note that

$$n \equiv 0 \pmod{m} \quad\text{and}\quad n \equiv a\left(\operatorname{mod}\varphi(m)\right). \tag{6}$$

For each m there are at most (using (4))

$$\begin{aligned}1+x/[m, \varphi(m)] &= 1+x\left(m, \varphi(m)\right)/m\varphi(m)\\ &\leqslant 1+|a|x/m\varphi(m) < 1+|a|\alpha x\log\log x/m^2\end{aligned}$$

choices for $n \leqslant x$ for which (6) holds. Hence the number of n for which (ii) holds is less than

$$\sum{}'(1+|a|\alpha x\log\log x/m^2) < (1+|a|\alpha)x^{2/3}(\log\log x)^{1/3}$$

where $\sum{}'$ denotes the sum over all m satisfying (5).

We thus have for sufficiently large x,

$$N(F'(a), x) < (3+|a|\alpha)x^{2/3}(\log\log x)^{1/3},$$

which proves (3).

References

[1] P. Erdös, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen 4 (1956), pp. 201–206.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Fourth Edition), Oxford 1960.

[3] W. Knödel, *Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x*, Arch. Math. 4 (1953), pp. 282–284.

[4] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. 38 (1932), pp. 745–757.

[5] E. Lieuwens, *Do there exist composite numbers M for which $k\varphi(M) = M-1$ holds?*, Nieuw Arch. Wisk. (3) 18 (1970), pp. 165–169.

[6] C. Pomerance, *On the congruences* $\sigma(n) \equiv a(\operatorname{mod} n)$ *and* $n \equiv a(\operatorname{mod}\varphi(n))$, Acta Arith. 26 (1975), pp. 265–272.

[7] W. Sierpiński, *Elementary Theory of Numbers* (translated from Polish by A. Hulanicki), Warsaw 1964.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GEORGIA
Athens, Georgia

Received on 12. 3. 1974 (544)