PACIFIC JOURNAL OF MATHEMATICS
Vol. 69, No. 1, 1977

ON COMPOSITE n FOR WHICH $\varphi(n) \mid n-1$, II

CARL POMERANCE

The problem of whether there exists a composite n for which $\varphi(n) \mid n-1$ (φ is Euler's function) was first posed by D. H. Lehmer in 1932 and still remains unsolved. In this paper we prove that the number of such n not exceeding x is $O(x^{1/2}(\log x)^{3/4})$. We also prove that any such n with precisely K distinct prime factors is necessarily less than K^{2^K}. There are appropriate generalizations of these results to integers n for which $\varphi(n) \mid n-a$, a an arbitrary integer.

1. Introduction. In 1932, D. H. Lehmer [6] asked if there are any composite integers n for which $\varphi(n) \mid n-1$, φ being Euler's function. The answer to this question is still not known. Lieuwens [7] has shown that any such n is divisible by at least 11 distinct primes; Kishore [5] has recently announced the analogous result for 13 primes.

If S is any set of positive integers, denote by $N(S, x)$ the number of members of S which do not exceed x. Let L denote the set of composite n for which $\varphi(n) \mid n-1$. Although Erdös was not specifically considering the problem of estimating $N(L, x)$, as a corollary of his paper [2], we have

$$N(L, x) = O(x \exp(-c \log x \log\log\log x / \log\log x))$$

for some $c > 0$. In [11] we proved

$$N(L, x) = O(x^{2/3}(\log\log x)^{1/3}) .$$

One result of this paper is

$$N(L, x) = O(x^{1/2}(\log x)^{3/4}) . \tag{1.1}$$

There is still clearly a wide gap between the possibility $L = \varnothing$ and (1.1), for the latter does not even establish that the members of L are as scarce as squares! Note that we conjectured in [11] that for every $\varepsilon > 0$,

$$N(L, x) = O(x^{\varepsilon}) .$$

Important in proving (1.1) is the consideration for $n \in L$ of the distribution in the interval $[0, \log n]$ of the numbers $\log d$ for $d \mid n$. We show that these numbers do not leave any large gaps, in that any reasonable subinterval will contain some $\log d$.

We also prove another result of independent interest about the set L: if $n \in L$ and n is divisible by precisely K distinct primes,