ON COMPOSITE *n* FOR WHICH $\varphi(n) | n - 1$, 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 $\varphi(n) \mid n-a$, α an arbitrary integer.

1. Introduction. In 1932, D. H. Lehmer [6] asked if there are any composite integers n for which $\varphi(n)|n-1$, 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 $\varphi(n)|n-1$. Although Erdös was not specifically considering the problem of estimating N(L, x), as a corollary of his paper [2], we have

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

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

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

There is still clearly a wide gap between the possibility $L = \emptyset$ 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,

then

$$(1.2) n < K^{2^K}.$$

This result is similar to a result of Borho [1] dealing with amicable numbers.

We establish results analogous to (1.1) and (1.2) for other sets of positive integers analogous to L. Recalling notation from [10], [11], we let

$$F(a) = \{n \colon n \equiv a \pmod{\varphi(n)}\}\$$

for each integer a. From Sierpiński [12, p. 232], we have

(1.3)
$$F(0) = \{1\} \cup \{2^i \cdot 3^j : i > 0, j \ge 0\}.$$

We have seen in [10] that F(0) plays a special role for the sets F(a). Indeed, if $a \notin F(0)$, then F(a) has no member of the form pa with p prime, $p \nmid a$. However, if $a \in F(0)$, then every such number pa is in F(a). Hence we are naturally led to consider the subsets

$$F'(a) = \{n \in F(a): n \neq pa \text{ for } p \text{ prime, } p \nmid a\}$$
.

Note that $F'(1) = L \cup \{1\}$. We shall prove

$$(1.4) N(F'(a), x) = O(x^{1/2}(\log x)^{3/4})$$

for every integer a, where the implied constant depends on a. Note that (1.3) implies $N(F(0), x) = O((\log x)^2)$, so that (1.4) is true for a = 0. However other results we prove will not be true for a = 0. Throughout the remainder of this paper, a will represent a nonzero integer.

We also prove that if $n \in F'(a)$ and n is divisible by precisely K distinct primes, then

$$n < \max \{16 |a|^3, |a| \cdot K^{2K}\}$$
.

Certain results of Norton [9] (see Suryanarayana [13]) enable us to state our theorems in a sharper form than could be done otherwise. The results of Meijer [8] might yield further improvements.

We wish to thank the referee who carefully read the paper and made several helpful suggestions.

2. Preliminary results. If n is an integer at least 2, denote by $\omega(n)$ the number of distinct prime factors of n, P(n) the largest prime factor of n, and p(n) the least prime factor of n.

In our work with the sets F'(a) it will be convenient to isolate the square free members. Note that every member of F'(1) is

square free. Let

$$F''(a) = \{n \in F'(a): n \text{ is square free}\}$$
.

LEMMA 1. $N(F'(a), x) \leq 4a^2 + \sum_{d|a} N(F''(a/d), x/d)$.

Proof. Let $n \in F'(a)$, $4a^2 < n \le x$. If n = pa for some prime p, then $p \mid a$, so $n \le a^2$. Hence $n \ne pa$ for every prime p. Let m be the maximal square free divisor of n and let d = n/m. Then every prime factor of d also divides m. Hence $\varphi(m) = \varphi(n)/d$, so that $d \mid a$ and $m \in F(a/d)$. Since $m \ne pa/d$ for every prime p, we have $m \in F''(a/d)$.

Hence all we need verify is that if n_1 , $n_2 \in F'(a)$ with maximal square free divisors m_1 , m_2 , and if n_1 , $n_2 > 4a^2$, then $m_1 = m_2$ implies $n_1 = n_2$. Now for any n we have

(Sierpiński [12, p. 230]). Suppose $m_1 = m_2$. Then n_1 and n_2 have the same set of prime factors. This implies $n_1/\varphi(n_1) = n_2/\varphi(n_2)$. Let $k_i = (n_i - a)/\varphi(n_i)$ for i = 1, 2. Then

$$k_1 + a/\varphi(n_1) = k_2 + a/\varphi(n_2)$$
.

From (2.1) and the assumption n_1 , $n_2 > 4a^2$, we have $0 < |a/\varphi(n_i)| < 1$ for i = 1, 2. But k_1 , k_2 are integers and $a/\varphi(n_1)$, $a/\varphi(n_2)$ have the same sign, so

$$a/\varphi(n_1) = a/\varphi(n_2)$$
.

But $n_1/\varphi(n_1) = n_2/\varphi(n_2)$, so $n_1 = n_2$, which was to be proved.

LEMMA 2. If $n \ge 16a^2$, $n \in F''(a)$, then

- (i) $k \doteq (n-a)/\varphi(n)$ is a positive integer at least 2;
- (ii) if $m \mid n$, $m \neq n$, then $m/\varphi(m) < k$;
- (iii) there is a prime q > P(n) with $nq/\varphi(nq) > k$;
- (iv) $\omega(n) \geq 3$.

Proof. (i) First we note that n is composite. Indeed if n=p, a prime, then the condition $p \in F''(a)$ implies p-1|a-1 and $a \neq 1$. Then $p \leq |a| + 2 < 16a^2$, a contradiction.

Now $n = k\varphi(n) + a$, so if $k \le 0$, then $n \le a$. Suppose k = 1. Since n is composite, n has a divisor d with $\sqrt{n} \le d < n$. Then $\varphi(n) \le n - d \le n - \sqrt{n}$. Then

$$a = n - \varphi(n) \ge \sqrt{n} \ge 4|a|$$
,

a contradiction.

(ii) It is sufficient to prove (ii) for m=n/p where p=P(n). From (2.1) and the assumption $n\geq 16a^2$, we have $|a/\varphi(n)|<1/2$. Hence from the equation $n/\varphi(n)=k+a/\varphi(n)$ and (i) we have

$$(3/4)k \le k - 1/2 < n/\varphi(n) < k + 1/2.$$

Then $m/\varphi(m) < k + 1/2 < 2k$, so

(2.3)
$$k\varphi(m) > m/2$$
.

Now

(2.4)
$$a = n - k\varphi(n) = mp - k\varphi(mp) = p(m - k\varphi(m)) + k\varphi(m)$$
.

If $m = k\varphi(m)$, then (2.4) implies $a = k\varphi(m)$, so that a = m and $n \notin F''(a)$. Hence $m \neq k\varphi(m)$. If $m > k\varphi(m)$, then (2.3), (2.4) imply

$$a \ge p + k\varphi(m) > p + m/2 \ge (2pm)^{1/2} > n^{1/2} \ge 4|a|$$

a contradiction. Hence $m < k\varphi(m)$.

(iii) If a>0, clearly any prime q>P(n) will do. Hence assume a<0. We first prove

(2.5)
$$P(n) < n/2 |a|$$
.

Indeed from (2.2) we have (with m = n/P(n))

$$\frac{3}{4}k < \frac{n}{\varphi(n)} = \frac{m}{\varphi(m)} \cdot \frac{P(n)}{P(n) - 1} \le \frac{2m}{\varphi(m)}$$
.

Then from (ii) and (2.4) we have

$$P(n) = (a - k\varphi(m))/(m - k\varphi(m)) \le |a| + k\varphi(m) < |a| + (8/3)m$$
.

If (2.5) fails, we have $m = n/P(n) \le 2|a|$, and it follows that P(n) < (19/3)|a| and $n = mP(n) < 16a^2$, a contradiction.

By Chebyshev's theorem there is a prime q with n/2|a| < q < n/|a|, and by (2.5), q > P(n). Also

$$egin{split} rac{nq}{arphi(nq)} &> rac{n}{arphi(n)} \cdot rac{n/|a|}{n/|a|-1} = rac{n^2}{arphi(n)(n+a)} \ &= rac{kn^2}{(n-a)(n+a)} > k \; , \end{split}$$

since $n^2 > n^2 - a^2 > 0$.

(iv) We noted in the proof of (i) that $\omega(n) \ge 2$. Suppose $\omega(n) = 2$. Let n = pq with p < q. Let r be a prime with r > q and $pqr/\varphi(pqr) > k \ge 2$ (using (i) and (iii)). Since (2/1)(3/2)(5/4) < 4, we have k = 2 or 3.

If k=3, then since (2/1)(5/4)(7/6)<3, we have $n=pq=6<16a^2$.

Suppose k=2. Since (5/4)(7/6)(11/10) < 2, we have p=2 or 3. By (ii), $p/\varphi(p) < 2$, so p=3. Since (3/2)(7/6)(11/10) < 2, we have q=5. That is, $n=pq=15<16a^2$.

LEMMA 3. Suppose k, n are natural numbers with n square free and $n/\varphi(n) > k$. If $m \mid n$ and $m/\varphi(m) < k$, then

$$p(n/m) < \omega(n/m) \cdot (m+1)$$
.

Proof. Let $r = \omega(n/m)$, p = p(n/m). Then

$$k < \frac{n}{\varphi(n)} \le \frac{m}{\varphi(m)} \cdot \left(\frac{p}{p-1}\right)^r$$
,

so that

$$m/k\varphi(m) > (1 - 1/p)^r \ge 1 - r/p$$
.

Hence

$$p<rac{rkarphi(m)}{karphi(m)-m}=r\Bigl(1+rac{m}{karphi(m)-m}\Bigr)\leqq r(m+1)$$
 .

3. Members of F'(a) with K prime factors.

THEOREM 1. Suppose $n \ge 16a^2$, $n \in F''(a)$, $K = \omega(n)$. Let the prime factorization of n be $p_1p_2 \cdots p_K$ where $p_1 > p_2 > \cdots > p_K$. Then for $1 \le i \le K$, we have

$$p_i < (i+1)(1+\prod\limits_{j=i+1}^{K}p_j)$$
 .

Proof. Let $m = \prod_{j=i+1}^K p_j$. By (iii) of Lemma 2 there is a prime $q > p_1$ with $nq/\varphi(nq) > k$. By (ii) of Lemma 2, $m/\varphi(m) < k$. Since $p_i = p(nq/m)$ and $i + 1 = \omega(nq/m)$, Lemma 3 completes the proof.

THEOREM 2. Suppose $n \ge 16a^2$, $n \in F''(a)$, $K = \omega(n)$. Then there is a positive constant β independent of the choice of a, n such that

$$(3.1) p(n) < \beta K^{1/2} (\log K)^{1/2}.$$

In addition, if $K \ge 4$, then $p(n) \le K - 1$.

Proof. Let p=p(n). Since there is a prime q>P(n) with $nq/\varphi(nq)>k\geq 2$ ((i) and (iii) of Lemma 2), it follows from Norton [9, Theorem 4] that there is an absolute constant $\beta_1>0$ with

$$K+1=\omega(nq)>\beta_1p^2/\log p$$
.

By Theorem 1, $\log p < \log (2(K+1)) < \beta_2 \log K$ for some $\beta_2 > 0$ ((iv) of Lemma 2). Hence there is an absolute constant $\beta > 0$ such that $p^2 < \beta^2 K \log K$, which proves (3.1).

Now assume $K \ge 4$. Then $p \le K-1$ if p=2 or 3. From $nq/\varphi(nq) > 2$, we have $K+1 \ge 7$ if p=5, so $p \le K-1$ in this case too. If $p \ge 7$ we similarly get $K+1 \ge 15$, so that using a result of Grün [3], we have

$$p < (2/3)(K+1) + 2 < K-1$$
.

Theorem 3. If $n \in F''(a)$, $K = \omega(n)$, then $n < \max \{16a^2, K^{2^K}\} .$

Proof. Assume $n \ge 16a^2$. By (iv) of Lemma 2 we have $K \ge 3$. If K = 3, we can show as follows that $n \le 435 < 3^{2^3}$. Write n = pqr where p < q < r are primes. By Lemma 2 there is a prime s > r such that

$$pqrs/arphi(pqrs)>k\geqq 2$$
 ,

(3.3)
$$pq/\varphi(pq) < k$$
.

We proceed as with the proof of (iv) of Lemma 2. Say $k \ge 3$. Then (3.2) implies k=3, p=2, $q \le 5$ or k=4, n=pqr=30. In the former case, (3.3) implies q=5, so (3.2) implies n=pqr=70. Now say k=2. Then (3.2), (3.3) imply p=3. Then (3.2) implies q=5, $r \le 29$ (so $n \le 3 \cdot 5 \cdot 29 = 435$) or q=7, $r \le 13$ (so $n \le 3 \cdot 7 \cdot 13 = 273$).

Assume $K \ge 4$. Let the prime factorization of n be $p_1 p_2 \cdots p_K$ where $p_1 > p_2 > \cdots > p_K$. By Theorem 2,

$$p_{\kappa}+1\leq K$$
.

By Theorem 1, $p_{K-1} < K(p_K + 1) \le K^2$. Hence

$$p_{\kappa-1}p_{\kappa} + 1 < K^3$$
.

Again by Theorem 1, $p_{K-2} < (K-1)(p_{K-1}p_K + 1)$, so that

$$p_{{\scriptscriptstyle{K-2}}}p_{{\scriptscriptstyle{K-1}}}p_{{\scriptscriptstyle{K}}} + 1 < p_{{\scriptscriptstyle{K-2}}}(p_{{\scriptscriptstyle{K-1}}}p_{{\scriptscriptstyle{K}}} + 1) < (K-1)K^6 < K^7$$
 .

Continuing in this fashion we get

$$n = p_{\scriptscriptstyle 1} p_{\scriptscriptstyle 2} \cdots p_{\scriptscriptstyle K} < K^{\scriptscriptstyle 2^K - 1} < K^{\scriptscriptstyle 2^K}$$
 .

THEOREM 4. If $n \in F'(a)$, $K = \omega(n)$, then $n < \max \{16 \mid a \mid^3, \mid a \mid \cdot K^{2^K} \}.$

Proof. Assume $n \ge 16 |a|^3$. Following the proof of Lemma 1,

we find a positive integer d with $d \mid (n, a)$ and $n/d \in F''(a/d)$. Then $n/d \ge 16a^2$, so Theorem 3 implies $n/d < K^{2^K}$. Hence

$$n < d \cdot K^{2^K} \leq |a| \cdot K^{2^K}$$
.

4. A combinatorial lemma.

LEMMA 4. Suppose $\delta \geq 0$, $a_1 \geq a_2 \geq \cdots \geq a_t > 0$, $B_i = \sum_{j=i}^t a_j$ for $1 \leq i \leq t$, and

$$a_i \leq \delta + B_{i+1}$$

for $1 \le i \le t - 1$. Then given any y with $0 \le y < B_1$, there is a subset S of $\{1, 2, \dots, t\}$ with

$$y - \delta - a_t < \sum\limits_{i \in S} a_i \leqq y$$
 .

Proof. We may assume $y \ge \delta + a_t$ for otherwise take $S = \emptyset$. We have

$$(4.2a,b) B_1 > y , \quad B_t \leq y .$$

Let s(0) = 0. Say we have either constructed a set S as called for or we have inductively found an integer sequence $s(0) < s(1) < \cdots < s(i-1) < t$ where $i \ge 1$ and

(4.3a)
$$\sum_{i=1}^{i-1} a_{s(i)} + B_{s(i-1)+1} > y ,$$

$$(4.3b) \qquad \qquad \textstyle\sum\limits_{j=1}^{i-1} a_{s(j)} \, + \, B_t \leqq y \; .$$

Let s(i) be maximal with

$$\sum\limits_{j=1}^{i-1} a_{s(j)} + B_{s(i)} > y$$
 .

By (4.3a), (4.3b), s(i) exists and s(i-1) < s(i) < t. Then since $a_{s(i)} + B_{s(i)+1} = B_{s(i)}$, we have

(4.4a)
$$\sum_{j=1}^{i} a_{s(j)} + B_{s(i)+1} > y.$$

Note that $\sum_{j=1}^{i-1} a_{s(j)} + B_{s(i)+1} \leq y$. Then we may assume

(4.5)
$$\sum_{i=1}^{i-1} a_{s(i)} + B_{s(i)+1} \leq y - \delta - a_t,$$

for otherwise we may take

$$S = \{s(1), s(2), \dots, s(i-1), s(i) + 1, s(i) + 2, \dots, t\}$$
.

Then from (4.5) and from (4.1) applied to $a_{s(i)}$, we have

$$egin{aligned} \sum_{j=1}^{i} a_{s(j)} \, + \, B_t &= \sum_{j=1}^{i} a_{s(j)} \, + \, a_t \ & \leq \sum_{j=1}^{i-1} a_{s(j)} \, + \, \delta \, + \, B_{s(i)+1} \, + \, a_t \leq y \end{aligned}$$
 ;

that is,

Since there is not an infinite increasing sequence of positive integers all less than t, this process must terminate with the construction of a suitable set S.

5. Estimates for N(F'(a), x).

THEOREM 5. For every a, $N(F'(a), x) = O(x^{1/2}(\log x)^{3/4})$, where the implied constant depends on a.

Proof. In view of Lemma 1, it will be sufficient to prove for every a that $N(F''(a), x) = O(x^{1/2}(\log x)^{3/4})$, where the implied constant depends on a. We record for future reference: there are positive constants α , γ with

$$(5.1) n/\varphi(n) < \alpha \log \log n , \quad n \ge 3$$

(5.2)
$$\omega(n) < \gamma \log n / \log \log n$$
, $n \ge 3$.

(Hardy and Wright [4, pp. 353-355].)

Let $n \in F''(a)$, $16a^2 \le n \le x$, $K = \omega(n)$. Let the prime factorization of n be $p_1p_2 \cdots p_K$ where $p_1 > p_2 > \cdots > p_K$. We may assume $n > x^{1/2}(\log x)^{3/4}$. Theorem 1 implies

$$\log \, p_i < \log \, (2K) + \sum\limits_{i=i+1}^K \log \, p_i$$
 , $1 \leqq i \leqq K-1$.

We apply Lemma 4 with

$$\delta = \log \left(2K
ight)$$
 , $t = K$, $a_i = \log p_i$, $y = \frac{1}{2}\log x + \frac{3}{4}\log\log x$.

Hence there is an integer m with $m \mid n$ and

$$y - \delta - \log p_{\kappa} < \log m \le y$$
.

Then

$$x^{1/2}(\log x)^{3/4}/2Kp_K < m \le x^{1/2}(\log x)^{3/4}$$
 .

By (3.1), (5.2), we have

$$egin{aligned} 2Kp_{\scriptscriptstyle{K}} &< 2eta K^{3/2} (\log K)^{\scriptscriptstyle{1/2}} \ &< 2eta (\gamma \log x/\log\log x)^{3/2} (\log (\gamma \log x/\log\log x))^{\scriptscriptstyle{1/2}} \ &< \gamma' (\log x)^{3/2} (\log\log x)^{-1} \end{aligned}$$

for some $\gamma' > 0$. Hence

$$f(x) \doteq (1/\gamma')x^{1/2}(\log x)^{-3/4}\log\log x < m$$

 $\leq x^{1/2}(\log x)^{3/4} \doteq g(x)$.

For each integer m in the above interval we now count the number of choices for $n \in F''(a)$ with $n \leq x$ and $m \mid n$. Since $\varphi(m) \mid \varphi(n)$ for such n, we have

$$n \equiv 0 \pmod{m}$$
, $n \equiv a \pmod{\varphi(m)}$,

so by the generalized Chinese remainder theorem, there are at most $1 + x/[m, \varphi(m)]$ choices for such n (here [,] denotes least common multiple). Now $(m, \varphi(m))|(n, \varphi(n))$ and $(n, \varphi(n))|a$. Hence for each m, there are at most (using (5.1))

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

choices for $n \in F''(a)$ with $n \leq x$ and $m \mid n$.

Hence we have

$$egin{aligned} N(F''(a),\,x) & \leq 16a^2 + x^{1/2}(\log x)^{3/4} + \sum\limits_{f(x) < m \leq g(x)} \left(1 + |a| lpha x \log\log x/m^2
ight) \ &= O(x^{1/2}(\log x)^{3/4}) + O(x\log\log x \sum\limits_{f(x) < m} 1/m^2) \ &= O(x^{1/2}(\log x)^{3/4}) + O(x\log\log x/f(x)) \ &= O(x^{1/2}(\log x)^{3/4}) \;. \end{aligned}$$

REMARK. Both the referee and D. Suryanarayana kindly suggest the use of a fact due to Landau,

$$\sum_{m>y} 1/m\varphi(m) = O(1/y)$$
,

in the proof of Theorem 5, rather than (5.1). This enables us to get the slightly stronger estimate

(5.3)
$$N(F'(a), x) = O(x^{1/2}(\log x)^{3/4}(\log \log x)^{-1/2})$$

where the implied constant depends on a. In addition we note that if those $n \leq x$ for which $p(n) \leq (\log x)^{1/4}$ are treated separately from the remaining choices for n, then an extra factor of $1/\log \log x$ may be introduced on the right of (5.3). It is conceivable that further

improvements are possible, even in the exponent on $\log x$ (perhaps by considering a sharper version of Lemma 4 where the constant δ is replaced by a variable δ_i which is usually small). It would seem to take a completely new idea however to lower the exponent on x.

REFERENCES

- W. Borho, Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl, Math. Nachr., 63 (1974), 297-301.
- 2. P. Erdös, On pseudoprimes and Carmichael numbers, Publ. Math. Debrecen, 4 (1956), 201-206.
- 3. O. Grün, Über ungerade vollkommene Zahlen, Math. Z., 55 (1952), 353-354.
- 4. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers (Fourth Edition), Oxford, 1960.
- 5. M. Kishore, On the equation $k\varphi(M)=M-1$, Not. Amer. Math. Soc., 22 (1975), A-501-A-502.
- D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc., 38 (1932), 745-757.
- 7. E. Lieuwens, Do there exist composite numbers M for which $k\varphi(M) = M 1$ holds? Nieuw Arch. Wisk., (3), 18 (1970), 165-169.
- 8. H. G. Meijer, Sets of primes with intermediate density, Math. Scand., 34 (1974), 37-43.
- 9. K. K. Norton, Remarks on the number of factors of an odd perfect number, Acta Arith., 6 (1961), 365-374.
- 10. C. Pomerance, On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$, Acta Arith., **26** (1975), 265-272.
- 11. C. Pomerance, On composite n for which $\varphi(n) \mid n-1$, Acta Arith., 28 (1976), 387-389.
- 12. W. Sierpiński, Elementary Theory of Numbers, Warsaw, 1964.
- 13. D. Suryanarayana, On odd perfect numbers, Math. Student, 41 (1973), 153-154.

Received October 28, 1975.

University of Georgia