ON EULER'S TOTIENT FUNCTION

BY D. H. LEHMER*

In this note we discuss the equation

$$k\phi(n) = n - 1, \tag{1}$$

where k is an integer, and $\phi(n)$ is Euler's totient function, giving the number of integers $<n$ and prime to n. Our main purpose is to show that if n is a solution of (1), then n is a prime or the product of seven or more distinct primes. One is tempted to believe the stronger statement that (1) has no composite solutions or, in other words, the integer n is a prime if (and only if) $\phi(n)$ divides $n-1$. We have not been able to establish this, however. The proof of the nonexistence of composite solutions of (1) seems about as remote as the proof of the nonexistence of odd perfect numbers and the two problems though not equivalent are not dissimilar.

Let n be a composite solution of (1) and let a be any number prime to n; then

$$a^{n-1} = (a^{\phi(n)})^k \equiv 1 \pmod{n},$$

so that n furnishes an example of the failure of the strict converse of Fermat's theorem for all values of a prime to n. This involves no contradiction, however. In fact $a^{560} \equiv 1 \pmod{561}$, for all a's prime to 561, although $561 = 3 \cdot 11 \cdot 17$.

Together with (1) we shall consider the equation

$$k\phi(n) = n + 1, \tag{2}$$

and show that it has exactly eight solutions if n has less than seven distinct prime factors. The case $k=1$ may be dispensed with since (2) has no solutions and (1) has a solution n, if and only if n is a prime. We first give a number of necessary conditions which any solution n of (1) or (2) must satisfy.

THEOREM 1. *If $n>2$, then n is a product of distinct odd primes.*

PROOF. From equations (1) and (2) it is obvious that n must be prime to $\phi(n)$, and since $\phi(n)$ is even for $n>2$, n must be odd.

* National Research Fellow.

Also if n contained a square of a prime, $\phi(n)$ would be divisible by this prime. Hence n is a product of distinct odd primes.

We note in passing that $n=2$ is a solution of (1) or (2) with $k=1$, and $k=3$ respectively, and in what follows we shall therefore suppose that $n>2$ and hence odd.

THEOREM 2. *If p is a factor of n, then n contains no prime factor of the form $px+1$.*

PROOF. In fact if p and $px+1$ were prime factors of n, then n and $\phi(n)$ would have a factor p in common.

THEOREM 3. *If n is composite, it is a product of an even or odd number of prime factors of the form $4x-1$, according as it is a solution of* (1) *or* (2).

PROOF. This theorem follows from the fact that $\phi(n)$ and hence $n\pm 1$ must be a multiple of 4.

From Theorem 1 we can write

$$n = p_1p_2p_3 \cdots p_t,$$

where the p's are distinct odd primes, and we will suppose that

$$2 < p_1 < p_2 < \cdots < p_t.$$

We now consider solutions of (1) and (2) for different values of t.

CASE I. $t=1$. This case is easily disposed of. Since n is a prime, it is a solution of (1) only with $k=1$. Equation (2) becomes

$$k(n-1) = n+1 \text{ or } (k-1)(n-1) = 2.$$

Hence the only solutions are $n=2$, $k=3$ and $n=3$, $k=2$.

CASE II. $t=2$. This case is also quite simple. When $n=p_1p_2$, (1) becomes

$$k(p_1-1)(p_2-1) = p_1p_2 - 1 \text{ or } k-1 = \frac{1}{p_1-1} + \frac{1}{p_2-1}.$$

Hence $0<k-1\leqq\frac{1}{2}+\frac{1}{4}<1$, which is impossible since $k-1$ is an integer. The equation (2) for this case becomes

$$0 < k-1 = \frac{1}{p_1-1} + \frac{1}{p_2-1} + \frac{2}{(p_1-1)(p_2-1)},$$

the only solution being $p_1=3$, $p_2=5$, since $k-1<1$ when at least one prime exceeds 5.

Before proceeding to larger values of t we show that we can confine ourselves to the case $k=2$.

THEOREM 4. *If* $2<t\leqq 6$, *then* $k=2$.

PROOF. Solving (1) and (2) for k we have

$$k = \prod_{i=1}^{t} \frac{p_i}{p_i - 1} \pm \frac{1}{\phi(n)}.$$

But since $t\geqq 3$, $n\geqq 105$, and $\phi(n)\geqq 48$. Also since $t\leqq 6$

$$k \leqq \frac{3}{2}\,\frac{5}{4}\,\frac{7}{6}\,\frac{11}{10}\,\frac{13}{12}\,\frac{17}{16} + \frac{1}{48} = \frac{5715}{2048} < 3.$$

The somewhat wasteful inequalities used above may be considerably sharpened if necessary. The following will illustrate.

THEOREM 5. *If* n *is a solution of* (1) *or* (2) *for* $k=3$, *then* n *is a product of more than* 32 *distinct prime factors.*

PROOF. Since n is prime to $k=3$, the smallest prime factor of n is $\geqq 5$. By Theorem 4, $t>6$, so that $n \geqq 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23$, so that $\phi(n)\geqq 18247680$. Then

$$3 = \prod_{i=1}^{t} \frac{p_i}{p_i - 1} \pm \frac{1}{\phi(n)}$$

or

$$\prod_{i=1}^{t} \frac{p_i}{p_i - 1} \geqq 3 - \frac{1}{18247680} > 2.99;$$

but

$$\prod_{i=1}^{t} \frac{p_i}{p_i - 1} \leqq \frac{5\cdot 7\cdot 11\cdots q_t}{4\cdot 6\cdot 10\cdots (q_t - 1)} = \pi_t,$$

where q_t is the tth prime >3. Hence

$$\pi_t > 2.99.$$

Referring to Legendre's table* we see that $q_t>139$ or $t>32$, which proves the theorem.

THEOREM 6. *If* $2<t\leqq 6$, *then* n *is a multiple of* 15.

* *Théorie des Nombres*, vol. 1, 3d edition, Table IX; see also Glaisher, Messenger of Mathematics, vol. 28, p. 2.

PROOF. First suppose that n is prime to 3; then $n \geqq 5 \cdot 7 \cdot 11$ so that

$$k \leqq \frac{5}{4}\,\frac{7}{6}\,\frac{11}{10}\,\frac{13}{12}\,\frac{17}{16}\,\frac{19}{18} + \frac{1}{4 \cdot 6 \cdot 10} = \frac{324091}{184320} < 2,$$

which is absurd. Hence n is a multiple of 3. By Theorem 2, n contains no prime factor of the form $3x+1$. Suppose now that n is not divisible by 5; then $n \geqq 3 \cdot 11 \cdot 17$ and $\phi(n) \geqq 480$.

$$k \leqq \frac{3}{2}\,\frac{11}{10}\,\frac{17}{16}\cdot\frac{23}{22}\,\frac{29}{28}\,\frac{41}{40} + \frac{1}{480} = \frac{4184731}{2150400} < 2.$$

Hence the theorem. With this information we can dispose of the case $t=3$ using the following lemma.

LEMMA 1. *If n_0 is a solution of* (2) *and if p is any prime, then*

I. *$n = n_0 p$ is not a solution of* (1);

II. *$n = n_0 p$ is a solution of* (2) *if and only if $n_0 + 2 = p$.*

PROOF. In order that $n_0 p$ be a solution of (1) or (2)

$$k\phi(n) = k\phi(n_0 p) = k\phi(n_0)(p-1) = (n_0+1)(p-1) = n_0 p \pm 1.$$

Hence $p = n_0$ or $p = n_0 + 2$. The lemma follows since, by Theorem 1, $p \neq n_0$.

CASE III. $t=3$. By Theorem 6, $n = 15p$. But 15 is a solution of (2); hence, by Lemma 1, (1) has no solutions and (2) has the single solution $n = 3 \cdot 5 \cdot 17 = 255$. For $t=4$, 5, 6, we prove the following lemma.

LEMMA 2. *If $k\phi(m) = m + \alpha$, and if p and q are primes for which*

$$k\phi(mpq) = mpq + \epsilon, \tag{3}$$

then

$$(\alpha p - m - \alpha)(\alpha q - m - \alpha) - (m^2 + \alpha m + \alpha\epsilon) = 0. \tag{4}$$

PROOF. Multiplying out the expression (4) and adding and subtracting αmpq we obtain

$$\alpha\{(m+\alpha)(p-1)(q-1) - mpq - \epsilon\} = \alpha\{k\phi(mpq) - mpq - \epsilon\}.$$

But from (3) this is zero, hence the lemma.

Solving (4) for $p-1$ we obtain

$$(4') \qquad p - 1 = \frac{mq + \epsilon}{\alpha q - k\phi(m)}.$$

CASE IV. $t=4$. From Theorem 6, $n=15pq$, $p<q$. Using Lemma 2 with $m=15$, $\alpha=1$, we get from (4)

$$(p - 16)(q - 16) = 240 + \epsilon.$$

For equation (1), $\epsilon=-1$. Since 239 is a prime, $p-16=1$, and $q-16=239$ or $q=255$, not a prime. For equation (2) $\epsilon=+1$. Since 241 is a prime, $p-16=1$ and $q-16=241$ or $p=17$ and $q=257$ gives a solution $n=3\cdot5\cdot17\cdot257$.

CASE V. $t=5$. Writing n in the form $n=3\cdot5\cdot pqr$, we first show that $p<53$. Making use of Theorem 2 and supposing that $p\geqq53$, we find

$$k \leqq \frac{3}{2}\,\frac{5}{4}\,\frac{53}{52}\,\frac{59}{58}\,\frac{83}{82} + \frac{1}{2\cdot4\cdot52\cdot58\cdot82} = \frac{973279}{494624} < 2.$$

Hence $p<53$. By Theorem 2, $p=17$, 23, 29, or 47. Writing $m=3\cdot5\cdot p$ we apply Lemma 2. Thus $\alpha=2\phi(m)-m=1$, 7, 13 or 31. For $\epsilon=-1$ equation (4) becomes, for these various cases,

$$(5) \qquad (q - 256)(r - 256) = 65279 = 29\cdot2251,$$

$$(6) \qquad (7q - 352)(7r - 352) = 121433 = 13\cdot9341,$$

$$(7) \qquad (13q - 448)(13r - 448) = 194867 = \text{prime},$$

$$(8) \qquad (31q - 736)(31r - 736) = 518849 = 211\cdot2459.$$

Since $q<r$, equation (5) implies $(q-256)=1$ or 29, and $r-256=65279$ or 2251. In the first case r is divisible by 5 and in the second case the same is true of q. Hence (5) has no solution (p, q) in primes. Taking (6), (7), and (8) modulo 7, 13, and 31, respectively, we see that these equations have no solutions, even in integers. For $\epsilon=+1$ the right sides of (5), (6), (7), and (8) become $65281=97\cdot673$, $121447=$prime, $194893=79\cdot2467$, and $518911=$prime. The first of these implies

$$\begin{cases} q - 256 = 1, \\ r - 256 = 65281, \end{cases} \quad \text{or} \quad \begin{cases} q - 256 = 97, \\ r - 256 = 673, \end{cases}$$

so that $q=257$, $r=65537$ or $q=353$, $r=929$ are solutions of (2). The other three equations are not solvable in integers. For Case V, then, there are no solutions of (1) and a pair of solutions of (2), namely

$$n = 3\cdot 5\cdot 17\cdot 257\cdot 65537 = 2^{32} - 1 = 4294967295,$$
$$n = 3\cdot 5\cdot 17\cdot 353\cdot 929 = 83623935.$$

CASE VI. $t=6$. This case involves so many trials that space can be given to only a brief account of the work. We find as before that $n=3\cdot 5\cdot pqrs$, where $p=17$, 23, 29, or 47. We shall first discuss the case $p=17$. In this case we can prove that $q\geqq 257$. In fact if $q<257$, then by Theorem 2, $q\leqq 239$ since 241 and 251 are of the form $5x+1$. Hence

$$k > \frac{3}{2}\,\frac{5}{4}\,\frac{17}{16}\left(\frac{239}{238}\right)^3 - \frac{1}{2\cdot 4\cdot 16(238)^3} = \frac{217577459}{107496151} > 2,$$

contrary to Theorem 4. Hence $q\geqq 257$. First let $q=257$ and apply Lemma 2 with $m=3\cdot 5\cdot 17\cdot 257$, $\alpha=1$. For $\epsilon=-1$, (4) becomes $(r-2^{16})(s-2^{16})=4294901759=19\cdot 181\cdot 1248881$. Hence $r=65555$, 65717, or 68975. But r is a prime. Therefore r can only be 65717. But this gives $s=23794275$ which is not a prime. Hence (1) has no solution of the form $n=3\cdot 5\cdot 17\cdot 257\cdot rs$. For $\epsilon=+1$, equation (4) becomes

$$(r - 2^{16})(s - 2^{16}) = 4294901761 = 193\cdot 22253377.$$

Hence $s=4294967297=2^{25}+1=641\cdot 6700417$, or

$$s = 22318913 = 3037\cdot 7349.$$

In neither case is s a prime. Hence (2) has no solution of the form $3\cdot 5\cdot 17\cdot 257\cdot rs$. We next let $q=263$ and obtain

$$(7r - 67072)(7s - 67072) = \begin{cases} 4498183673 = 2731\cdot 1647083 \\ \qquad \text{for } \epsilon = -1, \\ 4498183687 = 60337\cdot 74551 \\ \qquad \text{for } \epsilon = +1. \end{cases}$$

Again there is no solution. The same results are obtained for $q=293$, 317, 347. For $q=353$ we get

$$(97r - 90122)(97s - 90122) = \begin{cases} 4706165747 = \text{prime} \\ \qquad \text{for } \epsilon = -1, \\ 4706165773 = 6577\cdot 715549 \\ \qquad \text{for } \epsilon = +1. \end{cases}$$

For $\epsilon = -1$, $s = 83623935$ is not a prime. For $\epsilon = +1$ we find $r = 929$, $s = 83623937$, both being prime numbers. Hence (2) has the solution*

$$n = 3 \cdot 5 \cdot 17 \cdot 353 \cdot 929 \cdot 83623937 = 6992962672132095.$$

The same method shows that neither (1) nor (2) has a solution for $q = 359$ or 383.

It now becomes much easier to consider equation (4′) written in the form

$$s - 1 = \frac{255qr + \epsilon}{(q - 256)r - 256(q - 1)}, \tag{9}$$

where q is a fixed prime and r varies over primes between such limits as to make the denominator of (9) positive and still have $s > r$. By actual trial division the successive values of r are eliminated very rapidly. No further solutions of (1) and (2) of the form $3 \cdot 5 \cdot 17 \cdot qrs$ exist. The cases $p = 23$, 29 and 47 were dealt with by means of (4′) and no solutions of (1) and (2) were found.

Summing up, we have shown that (1) has no composite solutions involving fewer than 7 distinct prime factors while we have found the following solutions of (2):

$$2,\ 3,\ 3 \cdot 5,\ 3 \cdot 5 \cdot 17,\ 3 \cdot 5 \cdot 17 \cdot 257,\ 3 \cdot 5 \cdot 353 \cdot 929,$$
$$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537,\ 3 \cdot 5 \cdot 17 \cdot 353 \cdot 929 \cdot 83623937.$$

If (2) has any further solutions they are products of 7 or more prime factors.

STANFORD UNIVERSITY

---

* This solution can be also obtained from the solution $n = 3 \cdot 5 \cdot 17 \cdot 353 \cdot 929$ by using Lemma 1. In the same way if 6992962672132097 is a prime

$$n = 3 \cdot 5 \cdot 17 \cdot 353 \cdot 929 \cdot 83623937 \cdot 6992962672132097$$
$$= 48901526933832864378258473353215$$

is a solution of (2).