CONDITIONS FOR $\phi(N)$ TO PROPERLY DIVIDE $N - 1$

DAVID W. WALL
University of New Mexico, Albuquerque, NM 87106

This paper is concerned with limitations upon solutions in integers $k > 1$ and $n > 0$ to the equation

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

where ϕ is the Euler phi-function. The question of whether or not (1) has a solution was first raised by Lehmer [1] and, more recently, was proposed as an "elementary problem" by Marshall [4] and as a research problem by Alter [5].

Here we review some previous results (Theorems A and B below) and then derive additional limitations (Theorems 1-4) on possible solutions (k,n) to (1).

In all that follows, we assume that n is a composite positive integer for which $k\phi(n) = (n - 1)$, k integral and at least 2. We represent n as the product $p_1p_2p_3 \cdots p_r$ of r positive primes. It is occasionally convenient to express n as $(t_1 + 1)(t_2 + 1) \cdots (t_r + 1)$, where $t_i + 1 = p_i$ for $1 \le i \le r$.

We begin with a few basic results which have appeared previously in various places.

Theorem A:

(i) If n satisfies (1), then n is odd, square-free, and the product of at least three primes.

(ii) If n satisfies (1) and p is a prime in n, then n has no prime of the form $px + 1$ where x is a positive integer.

Part (i) was first demonstrated by Lehmer [1]; part (ii) by Schuh [2]. Both are fairly direct consequences of the formula

$$\phi(m) = m\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_r}\right)$$

where $m = (q_1^{e_1})(q_2^{e_2}) \cdots (q_r^{e_r})$ is the representation of m as the product of powers of distinct primes.

Indeed, from this formula we see that if n satisfies (1), then

$$\begin{aligned}\phi(n) &= p_1p_2 \cdots p_r(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)\\ &= (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)\\ &= t_1t_2 \cdots t_r\end{aligned}$$

and that

$$k = \frac{p_1p_2 \cdots p_r - 1}{(p_1 - 1) \cdots (p_r - 1)} = \frac{(t_1 + 1)(t_2 + 1) \cdots (t_r + 1) - 1}{t_1t_2 \cdots t_r}$$

$$= 1 + \sum\nolimits_1 + \sum\nolimits_2 + \cdots + \sum\nolimits_{r-1}$$

where $\sum_j$ is the sum of the products of the inverses of the t_i taken j at a time. This immediately implies the following result, noted by Lieuwens [3].

Theorem A:

(iii) If in the index set $\{1, 2, \ldots, r\}$ an index j exists such that $q_j < q_j'$ and if $q_i \le q_i'$ for all other indices i, then

$$\frac{q_1q_2 \cdots q_r - 1}{(q_1 - 1) \cdots (q_r - 1)} > \frac{q_1'q_2' \cdots q_r' - 1}{(q_1' - 1) \cdots (q_r' - 1)}.$$

Thus, increasing some or all of the primes in n acts to decrease $(n - 1)/\phi(n)$.

Lieuwens showed in addition that if the smallest prime factor of n is not 5 then n is the product of at least 13 primes, and that if 3 is a factor of n then n is the product of at least 213 primes. Watterberg [6] showed that if 5 is a factor of n then n is still the product of at least 13 primes. We offer yet another addition to this set of results with the following.

Theorem 1: If n satisfies (1) and the smallest prime in n is at least 7, then n is the product of at least 26 primes.

Proof: Since for a given number r of primes in n, increasing any one of the primes decreases the value of $(n - 1)/\phi(n)$, it follows that we can bound this ratio above by making n the product of the first r primes. A better bound is possible, however, since we know that 2 is not in n and that both p and $mp + 1$ cannot be in n at the same time.

In seeking this upper bound, it is necessary to achieve a balance between these considerations. For example, it should be better to use 7 in n instead of 29, because that will give the higher ratio. But by including 7 in n, we must exclude 43, 71, 113, 127, ... as well as 29. Thus, if we accept 7 as a factor of n, how many of the $7m + 1$ can we exclude from n and still be guaranteed an upper bound?

Now,

$$(n - 1)/\phi(n) = \frac{p_1 p_2 \cdots p_r - 1}{(p_1 - 1) \cdots (p_r - 1)} < \frac{p_1 \cdots p_r}{(p_1 - 1) \cdots (p_r - 1)} = \frac{n}{\phi(n)}.$$

If we use this last ratio as an upper bound, one approach might be to calculate $p/(p - 1)$ along with the product of as many $(mp + 1)/(mp)$ as we need to consider and simply see which is larger. This lends itself to useful results in specific cases, but a more general approach follows.

To begin with, we need only consider $mp + 1$ with m even, since we want $mp + 1$ to be an odd prime. Since

$$\begin{aligned}(2p + 1)(4p + 1)(6p + 1)(p - 1) &= 48p^4 - 4p^3 - 32p^2 - 11p - 1 \\ &< 48p^4 \text{ since } p > 0,\end{aligned}$$

$$\frac{(2p + 1)}{2p} \frac{(4p + 1)}{4p} \frac{(6p + 1)}{6p} = \frac{(2p + 1)(4p + 1)(6p + 1)}{48p^3} < \frac{p}{p - 1}.$$

Hence, we get a higher value of $n/\phi(n)$ by using p and omitting three $mp + 1$, regardless of the values of p and the $mp + 1$.

Considering the next case,

$$\begin{aligned}(2p + 1)(4p + 1)(6p + 1)(8p + 1)(p - 1) &= 384p^5 + 16p^4 - 260p^3 - 120p^2 - 19p - 1 \\ &< 384p^5 + 16p^4 - 260p^3 - 120p^2 \\ &= 384p^5 + 4p^2(4p^2 - 65p - 30).\end{aligned}$$

For positive p, $4p^2 - 65p - 30$ is negative if p is less than 16. Hence,

$$(2p + 1)(4p + 1)(6p + 1)(8p + 1)(p - 1) < 384p^5 \text{ if } p < 16, \text{ or}$$

$$\frac{2p + 1}{2p} \frac{4p + 1}{4p} \frac{6p + 1}{6p} \frac{8p + 1}{8p} < \frac{p}{p - 1} \text{ if } p < 16.$$

By the same reasoning as before, then, we can eliminate four $mp + 1$ when p is in n if p is 3, 5, 7, 11, or 13, and still be guaranteed an upper bound for $(n - 1)/\phi(n)$.

Applying this result for primes at least 7, we derive the sequence of 25 integers 7, 11, 13, 17, 19, 31, 37, 41, 47, 59, 61, 73, 97, 101, 107, 109, 127, 139, 151, 163, 167, 173, 179, 181, 193 which, when multiplied together to produce n, give

$$\frac{n}{\phi(n)} = \frac{1683\ 931359\ 756224\ 971448\ 190042\ 001610\ 486666\ 623927}{842\ 103229\ 776040\ 364896\ 736617\ 728835\ 584000\ 000000} < 2.$$

But this ratio is an upper bound of $(n - 1)/\phi(n)$ for all n with fewer than 26 primes. Since it is less than 2, n cannot satisfy (1) if it is the product of fewer than 26 primes. Hence, if all prime factors of n are 7 or greater, n is the product of at least 26 primes.

We next look at an unrelated result which deals with the powers of two in $\phi(n)$. Define $e(p)$ to be the largest j such that 2 divides $p - 1$. We have seen that all primes in n are odd, and thus that all the $t = p - 1$ are even. Hence $e(p)$ is at least 1 for all p in n. The following interesting result then emerges.

Theorem 2: If n satisfies (1), then $e(p)$ is minimal for an even number of primes p in n.

Proof: Let $n = p_1 p_2 p_3 \cdots p_r$ and let m be the smallest value of $e(p_i)$ over $1 \le i \le r$. Suppose without loss of generality that p_1 satisfies $e(p_1) = m$. Since $k\phi(n) = n - 1$,

$$k(p_1 - 1) \ldots (p_r - 1) = p_1p_2 \ldots p_r - 1$$

or

$$kt_1t_2 \ldots t_r = (t_1 + 1) \ldots (t_r + 1) - 1$$

$$= t_1t_2 \ldots t_r + \sum t_{i_1} \ldots t_{i_{r-1}} + \cdots + \sum t_{i_1}t_{i_2} + \sum t_i.$$

Since m is the minimum $e(p)$ and m is at least 1, any product of two or more t_i is a multiple of 2^{m+1}. Thus, taking residuals modulo 2^{m+1} in the preceding equation, we see

$$0 \equiv 0 + 0 + \cdots + 0 + \sum t_i \pmod{2^{m+1}},$$

i.e.,

$$0 \equiv \sum t_i \pmod{2^{m+1}}.$$

Some terms in $\sum t_i$ are themselves multiples of 2^{m+1}—specifically, all those t_i for which $e(p_i)$ is at least $m + 1$. These terms also vanish modulo 2^{m+1}, leaving only those t_i for which $e(p_i) = m$. The sum of all such t_i must thus be a multiple of 2^{m+1}. Since each of these t_i are *odd* multiples of 2^m, there must be an even number of them to produce as a sum a multiple of 2^{m+1}.

Hence $e(p)$ is minimal with a value of m for an even number of primes p in n.

Lastly, we consider an extension of the technique involved in the following theorem of Schuh.

Theorem B: If 3 divides n, then k is of the form $3x + 1$.

Proof (from Schuh): Suppose $n = 3p_2p_3 \ldots p_r$. No prime p_i is of the form $3x$, since it is then either 3 or not prime, and by Theorem A we see that in this case no prime in n can be of the form $3x + 1$. Hence, all the p_i must be of the form $3x + 2$. Since $k\phi(n) = n - 1$,

$$k(2)(p_2 - 1) \ldots (p_r - 1) = 3p_2p_3 \ldots p_r - 1.$$

Taking residuals modulo 3 in this equation, we find that

$$(k)(2)(1)(1) \ldots (1) \equiv 0 - 1 \pmod 3$$

or

$$2k \equiv -1 \pmod 3$$

and thus $k \equiv 1 \pmod 3$; i.e., k is of the form $3x + 1$.

This result cannot be extended in the same form, as the limitation upon the form of the p_i becomes less specific as the known factor of n (in this case, 3) increases. However, certain combinations of k and the p_i can be shown to be incompatible, and we can tabulate the possible combinations, in the following manner:

If p is prime, then the set $\{1, 2, 3, \ldots, p - 1\}$ is a group under multiplication modulo p. In particular, every member of the set has an inverse in the set, and (since no prime except p is divisible by p) all the other $p_2, p_3, \ldots, p_r$ in n are congruent modulo p to members of this set. Suppose then that p is a prime in n and that $n = pp_2p_3 \ldots p_r$. Then we can associate those primes in n which are inverses modulo p, and from this extract a few results.

At this point it becomes clearer to consider specific cases. Suppose $n = 5p_2p_3 \ldots p_r$. Then the p_i may be congruent to 2, 3, or 4 modulo 5. If i_2, i_3, i_4 are the number of primes in n congruent to 2, 3, or 4, respectively, $k\phi(n) = n - 1$ implies that

$$k(2 - 1)^{i_2}(3 - 1)^{i_3}(4 - 1)^{i_4} \equiv -1 \pmod 5$$

or

$$k(1^{i_2})(2^{i_3})(3^{i_4}) \equiv k(2^{i_3})(3^{i_4}) \equiv -1 \pmod 5$$

Now, 2 and 3 are inverses and of order 4 under multiplication modulo 5, so

$$(2^{i_3})(3^{i_4}) \equiv 2 \pmod 5$$

and this is congruent to 2^j for some $j = 0, 1, 2$, or 3. Hence, we have the following.

Theorem 3: $k(2^j) \equiv -1$ (modulo 5), where j is the number in $\{0, 1, 2, 3\}$ that is congruent modulo 4 to $i_3 - i_4$.

This relation between j and k gives rise to Table 1.

TABLE 1

$i_3 - i_4$ (mod 4)	k (mod 5)
0	4
1	2
2	3
3	1

The next case, when 7 divides n, is naturally a bit more complicated. Defining i_2, i_3, i_4, i_5, i_6 in the same manner as before, we obtain

$$k(1^{i_2})(2^{i_3})(3^{i_4})(4^{i_5})(5^{i_6}) \equiv -1 \pmod 7.$$

Inverse pairs are 2, 4 (of order 3) and 3, 5 (of order 6, so we have

Theorem 4: $k(2^{i_3 - i_5})(3^{i_4 - i_6}) \equiv -1 \pmod 7$, where $i_3 - i_5$ may be reduced modulo 3 and $i_4 - i_6$ may be reduced modulo 6.

This relationship is shown in Table 2.

TABLE 2

$i_3 - i_5$ (mod 3) \ $i_4 - i_6$ (mod 6)	0	1	2	3	4	5
	k (mod 7)					
0	6	2	3	1	5	4
1	3	1	5	4	6	2
2	5	4	6	2	3	1

The same method can be applied to whatever case is desired: the next case, when 11 divides n, yields a four-dimensional table with 2500 entries.

REFERENCES

1. D. H. Lehmer. "On Euler's Totient Function." *Bull. Amer. Math. Soc.* 38 (1932):745-751.
2. Fr. Schuh. "Do There Exist Composite Numbers m for Which $\phi(m) | m - 1$?" (Dutch) *Mathematica Zutphen* B 13 (1944):102-107.
3. E. Lieuwens. "Do There Exist Composite Numbers M for Which $k\phi(M) = M - 1$ Holds?" *Nieuw Arch. voor Wiskunde* (3), 18 (1970):165-169.
4. Arthur Marshall. Problem E 2337. *American Math. Monthly* 77, No. 5 (1970):522.
5. Ronald Alter. "Can $\phi(n)$ Properly Divide $n - 1$?" *American Math. Monthly* 80, No. 2 (1973):192-193.
6. P. A. Watterberg. "Conditions for $\phi(n)$ To Properly Divide $n - 1$." Abstract 73T-A252, *Notices of the American Math. Society* (August 1973).

*****

ON FIBONACCI NUMBERS OF THE FORM $x^2 + 1$

RAY STEINER

Bowling Green State University, Bowling Green, OH 43403

Let F_n (n nonnegative) be the nth term of the Fibonacci sequence, defined by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$, and let L_n (n nonnegative) be the nth term of the Lucas sequence, defined by $L_0 = 2$, $L_1 = 1$, $L_{n+2} = L_{n+1} + L_n$. In a previous paper [3], we showed that the equation

$$F_n = y^2 + 1 \tag{1}$$

holds only for $n = 1$, 2, 3, and 5. However, the proof given was quite complicated and depended upon some deep properties of units in quartic fields. Recently, Williams [4] has given a simpler solution of (1) which depends on some very pretty identities involving the Fibonacci and Lucas numbers. In this note, we present a completely elementary solution of