INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A06

# ON THE EQUATION $m - 1 = a\varphi(m)$

**Marian Deaconescu**
*Kuwait University, Kuwait*
deacon@mcs.sci.kuniv.edu.kw

*Dedicated to Haidar Khajah*

*Received: 12/5/04, Revised: 9/19/05, Accepted: 2/12/06, Published: 2/22/06*

**Abstract**

Let $\varphi$ denote Euler's totient function. It is shown that if $r \geq 2$ there exist only finitely many positive integers $n$ such that $\varphi(n)$ divides $n - 1$ and $\varphi(n)^2 \equiv r \pmod{n}$. It is also shown that if $k \geq 2$ there exist only finitely many positive integers $n$ such that $\varphi(n)$ divides $n - 1$ and $\varphi(n)^k \equiv 1 \pmod{n}$.

## 1. Introduction

Let $\varphi$ denote Euler's totient function. D.H. Lehmer [5] proposed the following:

**Conjecture.** *If $a \geq 2$ is an integer, then there is no positive integer $m$ such that*

$$a\varphi(m) = m - 1.$$

In other words, if $m \geq 2$, then $\varphi(m)$ divides $m - 1$ if and only if $m$ is a prime. I will refer in the sequel to Lehmer's conjecture as to $(L)$. The interested reader may consult R.K. Guy's book [3] for a list of references.

The aim of this note is to derive more information on (hypothetical) counterexamples to Lehmer's conjecture. Two finiteness results are proved by elementary methods, information that can be viewed as an argument for the veracity of $(L)$.

From now on $n$ will denote a counterexample to $(L)$ and $\phi = \varphi(n)$ for the sake of simpler

notation. Since $n$ is a counterexample to $(L)$, we can find an integer $a \geq 2$ such that

$$n - 1 = a\phi. \tag{1}$$

Since $(n, \phi) = 1$, we see that $n$ must be composite, square-free and odd, thus $n = \prod_{i=1}^{s} p_i$ for some $s \geq 2$ and for some distinct odd primes $p_i$, $1 \leq i \leq s$. We have $\phi = \varphi(n) = \prod_{i=1}^{s}(p_i - 1)$ and for simplicity we will use also the notation $\psi = \psi(n) = \prod_{i=1}^{s}(p_i - 2)$. D.H. Lehmer proved in [5] that $s \geq 7$ and subsequently it was shown by Cohen and Hagis [1] that $s \geq 14$.

The starting point of this note was the following simple observation:

$$\phi^2 \not\equiv 1 \pmod{n}.$$

To prove this, note first that since $n$ is composite and odd we have $\phi > \sqrt{n}$ and thus, by (1), $a < \sqrt{n}$. If $n|\phi^2 - 1$, then, by (1), $n|(\frac{n-1}{a})^2 - 1$, implying $n|a^2 - 1 < n$ and forcing $a = 1$, a contradiction since $a \geq 2$.

Since $\phi^2 > n$, division of $\phi^2$ by $n$ gives a positive quotient $q$ and a remainder $r$ such that

$$\phi^2 = qn + r,\ 2 \leq r \leq n - 1. \tag{2}$$

This raises the following question: if $r \geq 2$ , what can be said of the counterexamples $n$ to $(L)$ that satisfy the condition $\phi^2 \equiv r \pmod{n}$? Though we don't even know whether or not such counterexamples do exist at all, something sensible can be said, namely:

**Theorem 1.1.** *If $r \geq 2$ is fixed, there exist only finitely many counterexamples $n$ to $(L)$ such that $\phi^2 \equiv r \pmod{n}$.*

Another question suggested by the remark that $\phi^2 \not\equiv 1 \pmod{n}$ is related to the order of $\phi$ modulo $n$. This is the smallest positive integer $k = |\phi|$ satisfying $\phi^k \equiv 1 \pmod{n}$. By Lagrange's theorem, $k$ divides $\phi$ since $\phi$ is the order of the group of units of the ring $Z_n$ of residue classes modulo $n$. Since $n$ is composite, the group of units is not cyclic, so $3 \leq k \leq \frac{\phi}{2}$. If $k \geq 3$ is fixed, it is natural to ask about the number of counterexamples $n$ to $(L)$ that satisfy $\phi^k \equiv 1 \pmod{n}$:

**Theorem 1.2.** *If $k \geq 3$ is fixed, there exist only finitely many counterexamples $n$ to $(L)$ such that $\phi^k \equiv 1 \pmod{n}$.*

Finally, information on the counterexamples to $(L)$ leads to characterizations of primes as follows:

**Theorem 1.3.** *Let $m \geq 2$ be an integer and assume that $m \equiv 1 \pmod{\varphi(m)}$. Then the following are equivalent:*

*a) $m$ is a prime.*

*b)* $\varphi(m)^2 \equiv 1 \pmod{m}$.

*c)* $\varphi(m)^3 \equiv -1 \pmod{m}$.

*d)* $\varphi(m)^4 \equiv 1 \pmod{m}$.

## 2. Preliminaries

This section contains several remarks on a counterexample $n$ to Lehmer's conjecture $(L)$. Since $n$ is composite, the following result from [2] is useful: $\phi(\phi-1) > (n-1)\psi$. By (1), $n-1 = a\phi$ and we obtain $\phi - 1 > a\psi$, hence

$$\phi \geq a\psi + 2. \tag{3}$$

From (1) and (2) one obtains that

$$n(\phi - aq) = \phi + ar, \quad \phi(\phi - aq) = q + r. \tag{4}$$

Clearly, $\phi - aq \geq 1$, whence $q \leq \frac{\phi-1}{a}$. By (1) and (2), $q+r \leq \frac{\phi-1}{a} + n - 1 = \frac{\phi-1}{a} + a\phi < (a+1)\phi$. Since by (4) $\phi | q+r$, we see that $q+r \leq a\phi = n-1$ and thus by (4) again $\phi(\phi - aq) = q+r \leq a\phi$, giving $q \geq \frac{\phi-a}{a}$. And since $r = \phi^2 - qn$ we obtain

$$\frac{\phi - a}{a} \leq q \leq \frac{\phi - 1}{a}, \quad 1 \leq \phi - aq \leq a, \quad \frac{n-\phi}{a} \leq r \leq n - \frac{\phi}{a}. \tag{5}$$

By (5), $r - q \geq \frac{n-\phi-\phi+1}{a} > \frac{1}{a}$, so

$$r \geq q + 1. \tag{6}$$

By (3) and (5), $q \geq \frac{\phi-a}{a} \geq \frac{a\psi+2-a}{a} > \psi - 1$, whence

$$q \geq \psi. \tag{7}$$

By (5) and (3) again, $r \leq n - \frac{\phi}{a} \leq n - \frac{a\psi+2}{a} = n - \psi - \frac{2}{a} < n - \psi$, hence

$$r \leq n - (\psi + 1). \tag{8}$$

We also need a lower bound for $\phi$ in terms of $a$. Observe first that $\psi \geq a+1$, for if not, then $n = a\phi + 1 \geq \psi\phi + 1$, a contradiction for $s \geq 2$. Now use (3) to get $\phi \geq a\psi + 2 \geq a(a+1) + 2 = a^2 + a + 2$ and record this last inequality as

$$\phi \geq a^2 + a + 2. \tag{9}$$

## 3. Proofs

*Proof of Theorem 1.1.* To prove the Theorem, note that (6) and (7) imply $r \geq \psi + 1$ and note that only finitely many $n$'s may satisfy this inequality for a fixed $r$.

But this line of proof ultimately depends on an elementary result from [2] and it is worth including here a short and elegant proof, due to one of the editors, a proof that rests on Th. 328 of Hardy and Wright's book [4].

The proof goes as follows. Since $n - 1 = a\phi$ , then by Th. 328 of [4] we have that $a = O(\log\log n)$. If $\phi^2 \equiv r \pmod{n}$, then $a^2 r \equiv 1 \pmod{n}$. Now, if $|r| < \frac{n}{(\log\log n)^2}$, then $a^2 r = o(n)$ and for sufficiently large $n$ we cannot have $a^2 r \equiv 1 \pmod{n}$ unless $a^2 r = 1$. Thus, for a fixed $r$ such that $|r| < \frac{n}{(\log\log n)^2}$, there exist only finitely many counterexamples $n$ satisfying $\phi^2 \equiv r \pmod{n}$. And it is clear that, for $r$ fixed, there are only finitely many positive integers n such that $|r| \geq \frac{n}{(\log\log n)^2}$, which completes the proof.

*Proof of Theorem 1.2.* It is easy to show that the number of counterexamples to $(L)$ having a fixed number $s$ of prime divisors is finite. Indeed, let $s \geq 2$ be fixed and let $n = a\phi + 1$ be a counterexample to $(L)$ having $s$ prime factors. Since $a = \sum_{\substack{d|n \\ d<n}} \frac{1}{\varphi(d)} < (\frac{3}{2})^s$, we see that there are only finitely many such $a$'s possible. Fix now such an $a$. Since there are exactly $2^s - 1$ divisors $d$ of $n$ with $d < n$ and since $1 = \sum_{\substack{d|n \\ d<n}} \frac{1}{a\varphi(d)}$, it is clear that $n$ cannot be arbitrarily large.

Suppose now that $\phi^k \equiv 1 \pmod{n}$. Since $n - 1 = a\phi$, it follows that $n|a^k - 1$ if $k$ is even and $n|a^k + 1$ if $k$ is odd. In any case, $n \leq a^k + 1$, giving $a\phi \leq a^k$. Thus $\phi \leq a^{k-1} < (\frac{3}{2})^{s(k-1)}$.

So $k - 1 > \frac{1}{s} log_{\frac{3}{2}}(\phi) > \frac{1}{s} log_{\frac{3}{2}}(2^s s!)$. This implies in turn that $k - 1 - log_{\frac{3}{2}} 2 > \frac{1}{s} log_{\frac{3}{2}}(s!)$ and it is now clear that there exist only finitely many values of $s$ satisfying the last inequality. The result now follows from the first paragraph.

*Proof of Theorem 1.3.* The implications $a) \Rightarrow b), c), d)$ are clear and the implication $b) \Rightarrow a)$ was proved in the Introduction. Note that if $n$ is a counterexample to $c) \Rightarrow a)$, or to $d) \Rightarrow a)$, then $n$ is a counterexample to $(L)$ and we can use the notation and the partial results in the Preliminaries.

Let $n$ be a counterexample to $c) \Rightarrow a)$, so $\phi^3 \equiv r\phi \equiv a\phi \equiv -1 \pmod{n}$. Then $n|\phi(r - a)$, giving $n|r - a$ and forcing $r = a$. But, by (6), (7), and the fact that $\psi \geq a+1$ we get $r \geq \psi + 1 > a$, a contradiction. Finally, let $n$ be a counterexample to $d) \Rightarrow a)$, that is $\phi^4 \equiv r^2 \equiv a^2 r \equiv 1 \pmod{n}$. Then $n|r^2 - a^2 r = r(r - a^2)$, forcing, as above, $r = a^2$. Then, by (5), we have $a^2 = r \geq \frac{n-\phi}{a} = \frac{(a-1)\phi+1}{a}$, which gives $a^3 - 1 \geq (a - 1)\phi$. Thus $\phi \leq a^2 + a + 1$, contradicting (9) and completing the proof.

## 4. Remarks

The lower bound $\psi+1$ given for $r$ in the proof of Theorem 1.1 is not the best possible. The fact that $r \in [\psi+1, n-(\psi+1)]$ serves only the purpose of providing a "symmetric" interval for $r$. A better lower bound is $\frac{\phi+2}{2}$ and this is obtained by combining (5), (3) and the fact that $a \geq 2$.

By Cohen and Hagis' result, if $N$ denotes the smallest odd square-free integer with 14 prime factors satisfying $(N, \varphi(N)) = 1$ and if $r \leq \frac{\varphi(N)}{2}$, then there is no counterexample $n$ to $(L)$ satisfying $\phi^2 \equiv r \pmod{n}$. In particular, if $r \leq 10^{23}$, there is no counterexample $n$ to $(L)$ such that $\varphi(n)^2 \equiv r \pmod{n}$.

Suppose that $a = 2$, so $n = 2\phi + 1$. Then, by (5), we derive at once that $q = \frac{\phi-2}{2}$ and $r = \frac{3\phi+2}{2}$. Unfortunately, these equalities don't seem to provide an apparent contradiction able to show that such an $n$ doesn't exist.

Based on the information at hand it is not difficult to show that if $\phi^k \equiv 1 \pmod{n}$, then $k \geq 5$. Indeed, suppose first that $k = 3$, that is $\phi^3 \equiv r\phi \equiv a^2 r \equiv 1 \pmod{n}$. Then $n | r\phi - ra^2 = r(\phi - a^2)$. But from (2) it is clear that $(n, r) = 1$, thus $n | \phi - a^2$. Since $\phi, a^2 < n$, this gives $\phi - a^2 = 0$, contradicting (9). As a direct consequence of Theorem 1.3, $k \neq 4$.

Lehmer's conjecture can be rephrased in group theoretical terms. Those familiar with group theory will quickly realize that $(L)$ is equivalent to the following group-theoretical statement: if $G$ is a finite group and if $|Aut(G)|$ divides $|G| - 1$, then the holomorph of $G$ is a Frobenius group. Unfortunately, this change of language doesn't seem to provide any clue for a general method of attack of $(L)$.

Theorem 1.3 suggests an interesting question: are there positive composite integers $m$ such that $m | \varphi(m)^3 + 1$? Or, more generally, is it possible , for such a composite integer $m$, to find a *positive* integer $k$ such that $m | \varphi(m)^{2k+1} + 1$? If $m$ is a prime, then $m | \varphi(m) + 1$ (in this case $k = 0$).

The smallest possible example one can think of is $k = 1$ and $m = pq$, where $p, q$ are odd primes. It is a simple exercise to check that $pq | (\varphi(pq))^3 + 1$ is equivalent to $p | q^2 - q + 1$ *and* $q | p^2 - p + 1$. That these two divisibilities cannot hold in the same time was established by Geoff Bailey (a.k.a. *Fred the Wonder Worm* ) on December 9th 2004 in The Math Forum@Drexel (http://mathforum.org/sci.math.research).

Bailey's observation raises suggests another interesting open problem. Let $n \geq 3$, let $p_i$, $1 \leq i \leq n$ be distinct primes and let $f(p_i) = {p_i}^2 - p_i + 1$. Is it possible that the product of all $p_i$'s divides the product of all $f(p_i)$'s?

## References

1. G.L. Cohen and P. Hagis, *On the number of prime factors of $n$ if $\phi(n)|n-1$*, Niew Arch. Wisk. (3) **28** (1980), 177–185.

2. M. Deaconescu, *Adding units mod n*, El. Math. **55** (2000), 123–127.

3. R.K. Guy, *Unsolved Problems in Number Theory*, third edition, Springer Verlag , New York, 2004.

4. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Clarendon Press, Oxford, 1979.

5. D.H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), 745-751.