A note on Lehmer's Euler phi function conjecture

Kevin A. Broughan and Jethro van Ekeren

University of Waikato, Hamilton, New Zealand

Version: 15th May 2008

E-mail: kab@waikato.ac.nz, jethro.van.ekeren@xtra.co.nz

In 1932 D. H. Lehmer conjectured that if \( \varphi(n) \mid n - 1 \) then necessarily \( n \) must be prime. Here we show that the number \( \#\mathcal{L}(x) \) of composite integers \( n \leq x \) which satisfy this divisibility condition satisfies, for all \( \epsilon > 0 \), as \( x \to \infty \)

\[
\#\mathcal{L}(x) \ll_{\epsilon} \frac{\sqrt{x}}{\log x} \left( \log \log x \right)^{\frac{3}{2} + \epsilon}
\]

where \( \Theta = 0.129398 \ldots \) is an absolute constant.

Key Words: Lehmer’s conjecture, Euler phi function.


1. INTRODUCTION

Rather than tackling Lehmer’s problem directly, we will follow the approach (taken first by Pomerance [8]) of placing an upper bound on the number of integers \( n \in [1, x] \) satisfying Lehmer’s property: \( n \equiv 1 \pmod{\varphi(n)} \). Following Pomerance and subsequent authors we will make our arguments slightly more general, replacing the 1 above with a nonzero integer \( a \).

Now to introduce some notations, let \( a \in \mathbb{Z}\setminus\{0\} \) then

**Definition 1.1.**

\[
\mathcal{L}_a := \{ n \in \mathbb{N} : n \equiv a \pmod{\varphi(n)} \},
\]

\[
\mathcal{L}_a^\prime := \{ n \in \mathcal{L}_a : n \neq pa \text{ for any prime } p \text{ with } p \nmid a \},
\]

and

\[
\mathcal{L}_a^{\prime\prime} := \{ n \in \mathcal{L}_a : n \text{ is square-free} \}.
\]

Lehmer’s original problem relates to the case \( a = 1 \), we have \( \mathcal{L}_1 = \mathcal{L}_1^\prime = \mathcal{L}_1^{\prime\prime} \).

\( \#\mathcal{S}(x) \) denotes \( \# \{ n \in \mathcal{S} : 1 \leq n \leq x \} \). We use Landau’s \( O, o, \) and \( \ll \) notations to describe rates of growth. When no subscript is given to this
latter symbol, it is understood to depend at most on $e$. The expression $A \asymp B$ means $A \ll B$ and $B \ll A$. Let $\log_1 x := \log x$ and for $r \geq 1$, $\log_{r+1} x := \log_r \log x$, it being understood that $x$ is sufficiently large for these definitions to make sense.

Bounds obtained thus far on the growth of $L_a$ are:

\begin{align*}
\# L_a(n) &\ll x^{1/2}(\log x)^{3/4} \quad \text{(Pomerance \cite{Pomerance})}, \\
\# L_a(n) &\ll x^{1/2}(\log x)^{1/2}(\log \log x)^{-1/2} \quad \text{(Shan \cite{Shan})}, \\
\# L_a(n) &\ll x^{1/2}(\log \log x)^{1/2} \quad \text{(Banks and Luca \cite{BanksLuca})}, \\
\# L_a(n) &\ll x^{1/2}(\log x)^{-\Theta+i} \quad \text{(Banks, Gillolu and Nevans \cite{BanksGilloluNevans})}.
\end{align*}

In this note, using a variation on the methods of the last group above, we obtain a small improvement. Indeed we make the parameters $\alpha$ and $\beta$, used as constants in their proof, depend on $x$ and take care of the $\log \log x$ variation to obtain:

**Theorem 1.1.** Let $a$ be a non-zero integer. Then for all $\epsilon > 0$ as $x \to \infty$

$$
\# L^\epsilon_a(n) \ll \frac{\sqrt{x}}{\log x} (\log \log x)^{3+\epsilon}
$$

where $\Theta$ is the least positive solution to the equation

$$
2\Theta(\log \Theta - 1 - \log \log 2) = -\log 2,
$$

Approximately $\Theta \approx 0.129308 \ldots$. Note that each of the 6 steps in the proof of \cite{BanksGilloluNevans} need to be amended when $\alpha$ and $\beta$ are not constant.

2. **Proof of the Theorem**

**Lemma 2.1.** Let $n \geq 16a^2$ and $n \in L^\epsilon_a$ and let $n = p_1p_2 \cdots p_K$ where $p_1 > p_2 > \cdots > p_K$ (so $K = \omega(n)$). For $1 \leq i \leq K$

$$
p_i < (i+1)(1+p_{i+1}p_{i+2} \cdots p_K)
$$

The following ‘combinatorial lemma’ was the primary tool introduced by Pomerance

**Lemma 2.2.** Suppose $\delta \geq 0$, $a_1 \geq a_2 \geq \cdots \geq a_t = 0$ and $a_i \leq \delta + \sum_{j=1}^{t-i+1} a_j$ for $1 \leq i \leq t-1$. Then, for any real number $\rho$ satisfying
0 ≤ ρ < \sum_{i=1}^{t} a_i, there is a subset \mathcal{I} \subseteq \{1, 2, \ldots, t\} such that
\[ ρ - δ < \sum_{i \in \mathcal{I}} a_i ≤ ρ \]

The following result is due to Erdős and Nicolas [3, Proposition 3], we will use it later on.

**Lemma 2.3.** For 0 < λ < 1 define \( \mathcal{V}_λ := \{ n : \omega(n) < λ \log \log n \} \). Also for λ > 1 define \( \mathcal{W}_λ := \{ n : \omega(n) > λ \log \log n \} \). The counting functions \# \mathcal{V}_λ and \# \mathcal{W}_λ are both
\[ O \left( \frac{x}{(\log x)^{\lambda \log \beta (\log \log x)^{1/2}}} \right). \]

Now we begin the proof of Theorem 1.1.

**Proof.**
0. Preliminary definitions: Let ε > 0 be small and fixed. Define
\[
\begin{align*}
α & := 2 \Theta - (4 + 3e) \frac{\log \log x}{\log x} \\
β & := \Theta - (\frac{3}{2} + \epsilon) \frac{\log \log x}{\log x} \\
A & := \log^α x \\
B & := \log^β x.
\end{align*}
\]
Then \( \alpha/2, β \to \Theta \) as \( x \to \infty \). Also, \( \alpha/2 < β < \Theta \) for all sufficiently large \( x \). The fact
\[ (\log x)^{\frac{β}{\log ω x}} = \log \log x \]
will be used without mention.

1. First we show that
\[
P_a^\prime \left( \frac{x}{A} \right) \ll \sqrt{\frac{x}{\log^3 x}}.
\]
Since $\alpha/2 \to \Theta$, $\alpha > \Theta/2$ for sufficiently large $x$. By [2, Theorem 2.1], $L_0^*(x) \ll x^{1/2}(\log x)^{-3\Theta/4}$. Hence

$$L_0^*(\frac{x}{A}) \ll \frac{x^{1/2}}{(\log x)^{\alpha/2}}(\log x)^{-3\Theta/4}$$

$$= x^{1/2}(\log x)^{-3\Theta/4-\alpha/2}$$

$$\ll x^{1/2}(\log x)^{-\Theta}. $$

2. In each of the following steps we restrict $n$ so that $x/A \leq n \leq x$. Let $n = p_1 \cdots p_K$ where $p_1 > p_2 > \cdots > p_K$. We make use of Lemma 2.2 with $\delta = \log(2K)$, $t = K + 1$, $a_i = \log p_i$ for $1 \leq i \leq t - 1$, $a_t = 0$ and $\rho = \log(x^{1/2}/B)$. Lemma 2.1 guarantees that Lemma 2.2 applies.

Lemma 2.2 implies that for some divisor $d$ of $n$,

$$\frac{x^{1/2}}{2B\omega(n)} \leq d \leq \frac{x^{1/2}}{B}. \quad (1)$$

If $m = n/d$ then

$$\frac{Bx^{1/2}}{A} \leq m \leq 2\omega(n)Bx^{1/2}. \quad (2)$$

We discern two cases

Case (I): $n \in W_{20}$.

Case (II): $n \notin W_{20}$.

Consider Case (I) now, that is $\omega(n) > 20\log\log n$. Because $n$ is square-free

$$\omega(d) + \omega(m) = \omega(n) > 20\log\log n$$

so one of these divisors (which we will denote $k$) belongs to $W_{10}$. Examining the inequalities above and using the facts $\omega(n) \leq 2\log x$ and $\alpha/2 < \beta$ (which implies $A \leq B^2$), we have

$$\frac{x^{1/2}}{4B\log x} \leq k \leq 4Bx^{1/2}\log x$$

(which we write as $y \leq k \leq z$).

Let $n \in L_\alpha$ and $k \mid n$, then $n \equiv a(\mod \varphi(k))$ and, as in [8], we note that the number of such $n$ cannot exceed

$$1 + \frac{x}{\text{lcm}[k, \varphi(k)]} \leq 1 + \frac{x\log\log x}{k^2}.$$
With $y$, $z$ as noted above we now have

$$\# \{ n \in W_2 \cap L_a' : x/A \leq n \leq x \} \ll \sum_{y \leq k \leq z \atop k \in W_2} \left(1 + \frac{x \log \log x}{k^2}\right)$$

$$\leq \sum_{k \leq y \atop k \in W_2} 1 + x \log \log x \sum_{k \geq y \atop k \in W_2} \frac{1}{k^2}$$

$$\ll \frac{z}{(\log z)^{14}} + \frac{x \log \log x}{y(y \log y)^{14}}$$

The reduction of the first term is a simple application of Lemma 2.3 and $1 - 10 + 10 \log 10 > 14$, while the second uses

$$\sum_{k \geq y \atop k \in W_2} \frac{1}{k^2} \ll \frac{1}{y(y \log y)^{1-\lambda + \lambda \log \lambda}}$$

which follows from partial summation of Lemma 2.3. Substituting for $y$, $z$ gives

$$\# \{ n \in W_2 \cap L_a' : x/A \leq n \leq x \} \ll \frac{4Bx^{1/2} \log x}{(\log x)^{14}} + \frac{4Bx^{1/2} \log x \log \log x}{(\log x)^{14}}$$

$$\ll \frac{x^{1/2}(\log x)^{5-12}}{x^{1/2}(\log x)^{-\lambda}}$$

3. We now consider Case (II). In place of (1) and (2) we have

$$\frac{x^{1/2}}{40B \log \log x} \leq d \leq \frac{x^{1/2}}{B} \quad (3)$$

and

$$\frac{Bx^{1/2}}{A} \leq m \leq 40Bx^{1/2} \log \log x \quad (4)$$

respectively (since $\omega(n) \leq 20 \log \log x$).

Now let $T$ be the collection of pairs of natural numbers $(d, m)$ such that the product $dm \in L_a''(x)$ and $d$ and $m$ satisfy the inequalities (3) and (4). Clearly

$$\# \{ n \in L_a'' \mid W_2 : x/A \leq n \leq x \} \leq \# T.$$

Now (compare [2, Lemma 4]), we have
Lemma 2.4. If \( x \) is sufficiently large then for every \( m \) there is at most one \( d \) such that \((d, m) \in \mathcal{T}\).

Proof. Let \((d_1, m), (d_2, m) \in \mathcal{T}\), this means that \( \varphi(m) \) divides \( d_1m - a \) and \( d_2m - a \) so \( d_1 \equiv d_2 \pmod{\varphi(m)/\mu} \) where \( \mu = \gcd[m, \varphi(m)] \). We note at this point that \( \mu \mid a \), so \( \mu \ll 1 \). Using Landau’s inequality \([4]\), then \((4)\), we get

\[
\phi(m) \gg \frac{m}{\log \log m} \geq \frac{x^{1/2}(\log x)^{\beta - \alpha}}{\log \log x} = \frac{x^{1/2}}{\log x^\Theta} (\log \log x)^\gamma.
\]

On the other hand, since

\[
\max\{d_1, d_2\} \leq \frac{x^{1/2}}{\log x^\Theta},
\]

\( d_1 = d_2 \) and the lemma follows. \( \Box \)

4. From now on assume \( x \) is large enough that Lemma 2.4 applies. If

\[
\mathcal{M} := \{m : (d, m) \in \mathcal{T} \text{ for some } d\}
\]

then Lemma 2.4 implies \( \#\mathcal{M} = \#\mathcal{T} \).

We now define the constant \( \Theta \) as the unique solution in the interval \((0, 1)\) to the equation

\[
1 - \Theta + \Theta \log \Theta = \Theta \log 2
\]

\( \Theta = 0.373365 \ldots \) With \( \Theta \) as previously defined, \( 2\Theta = \Theta \log 2 \). We next divide Case (II) into two sub-cases: (IIa) and (IIb). These are characterised respectively by \( m \in \mathcal{M}_1 := \mathcal{M} \cap \mathcal{V}_0 \) and \( m \in \mathcal{M}_2 := \mathcal{M} \setminus \mathcal{V}_0 \).

Dealing first with Case (IIa), we claim that

\[
\#\mathcal{M}_1 \ll \frac{x^{1/2}}{(\log x)^\Theta}.
\]

This follows from \((4)\) and Lemma 2.3,

\[
\#\mathcal{M}_1 \ll \mathcal{V}_0(40Bx^{1/2} \log \log x) \leq \frac{x^{1/2}(\log x)^{\beta} \log \log x}{(\log x)^{2\Theta}(\log \log x)^{1/2}} = \frac{x^{1/2}}{(\log x)^\Theta} \cdot (\log x)^{\beta - \Theta} \cdot (\log \log x)^{1/2}
\]

\[
= \frac{x^{1/2}}{\log x^{\Theta}} \cdot (\log \log x)^{-3/2 - i} \cdot (\log \log x)^{1/2}
\]

\[
\ll \frac{x^{1/2}}{(\log x)^\Theta}.
\]
5. Turning now to Case (IIb), we require another lemma (compare Lemma 5 of [2]).

**Lemma 2.5.** For \( x \) sufficiently large, for every \( d \) there is at most one \( m \in M_2 \) such that \( (d, m) \in T \).

**Proof.** Let \( (d, m_1), (d, m_2) \in T \) and \( m_1, m_2 \in M_2 \). Since \( m_1, m_2 \notin V_\theta \) (and using (4)) we see that each has at least

\[ \kappa := \left\lfloor \theta \log \log(Bx^{1/2}/A) \right\rfloor \]

distinct odd prime factors and hence that \( \varphi(m_1), \varphi(m_2) \) are multiples of \( 2^\kappa \). It follows that \( m_1 \equiv m_2 \pmod{2^\kappa \varphi(d)/\mu} \) where \( \mu = \gcd[d, 2^\kappa \varphi(d)] \) (and \( \mu \ll 1 \) as before).

Thus

\[
\frac{2^\kappa \varphi(d)}{\mu} \gg \frac{d}{\log \log d} \cdot 2^\kappa \\
\gg \frac{x^{1/2}}{B \log \log x^2} \cdot \left( \log \frac{Bx^{1/2}}{A} \right)^{\theta \log 2} \\
\gg \frac{x^{1/2} \log x^{2\theta}}{(\log x)^3 (\log \log x)^2} \\
= \frac{x^{1/2} (\log x)^3 (\log \log x) \log \log x}{(\log \log x)^{1+2\theta}}.
\]

On the other hand

\[
\max\{m_1, m_2\} \leq 40Bx^{1/2} \log \log x \ll x^{1/2} (\log x)^3 \log \log x
\]

and we see that \( m_1 = m_2 \). \( \blacksquare \)

6. If

\[
\mathcal{D} := \{d : (d, m) \in T \text{ for some } m \in M_2\}
\]
then

\[ \# M_2 = \# D \leq \frac{x^{1/2}}{B} = x^{1/2} (\log x)^{-\beta} \]

\[ = \frac{x^{1/2}}{(\log x)^{\Theta} (\log x)^{\beta}} \]

\[ = \frac{x^{1/2}}{(\log x)^{\Theta} (\log x)^{1/2+\epsilon}}. \]

7. Finally by 1., 4. and 6. the theorem is proved. □

REFERENCES

1. Banks, W.D. and Luca, F. Composite integers \( n \) for which \( \phi(n) \mid n - 1 \), Acta Math. Sinica, English Series 23, p1915-1918.
2. Banks, W.D., Guloğlu, A.M. and Wesley Nevans, C. On the congruence \( n \equiv a \mod \phi(n) \) (preprint).
6. Pomerance, C. On the congruences \( \sigma(n) \equiv a \mod n \) and \( n \equiv a \mod \phi(n) \), Acta Arith. 26 (1974/75), p263-272.
7. Pomerance, C. On composite \( n \) for which \( \phi(n) \mid n - 1 \), Acta Arith. 28 (1977/78), p177-186.
8. Pomerance, C. On composite \( n \) for which \( \phi(n) \mid n - 1 \), II, Pacific J. Math. 69 (1977), p177-186.