INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A59

ON THE CONGRUENCE $N \equiv A \pmod{\varphi(N)}$

William D. Banks[1]
Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
bbanks@math.missouri.edu

Ahmet M. Güloğlu
Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
ahmet@math.missouri.edu

C. Wesley Nevans
Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
nevans@math.missouri.edu

Received: 4/1/08, Revised: 9/30/08, Accepted: 10/15/08, Published: 12/23/08

Abstract

D. H. Lehmer asked whether there are any composite integers for which $\varphi(n) \mid n-1$, where φ is the Euler function. In this paper, we show that the number of such integers $n \leqslant x$ is $o(x^{1/2})$ as $x \to \infty$.

1. Introduction

Let $\varphi(n)$ be the *Euler function*, which is defined as usual by

$$\varphi(n) = n \prod_{p \mid n} \left(1 - p^{-1}\right) \qquad (n \in \mathbb{N}).$$

In 1932, D. H. Lehmer [4] asked whether there are any *composite* numbers n for which $\varphi(n) \mid n-1$, and the answer to this question is still unknown.

In what follows, for any set $\mathcal{S} \subseteq \mathbb{N}$ we put $\mathcal{S}(x) = \mathcal{S} \cap [1, x]$ for all $x \geqslant 1$. In a series of papers (see [5, 6, 7]) C. Pomerance considered the problem of bounding the cardinality of $\mathcal{L}(x)$, where $\mathcal{L}$ is the (possibly empty) set of composite numbers n such that $\varphi(n) \mid n-1$.

[1]Corresponding author

In his third paper, Pomerance [7] established the bound

$$\#\mathcal{L}(x) \ll x^{1/2}(\log x)^{3/4} \tag{1.1}$$

and remarked:

> *There is still clearly a wide gap between the possibility that $\mathcal{L} = \varnothing$ and (1.1), for the latter does not even establish that the members of $\mathcal{L}$ are as scarce as squares!*

Refinements of the underlying method of [7] led to subsequent improvements of the bound (1.1):

$$\#\mathcal{L}(x) \ll x^{1/2}(\log x)^{1/2}(\log\log x)^{-1/2} \qquad \text{(Shan [8])}$$
$$\#\mathcal{L}(x) \ll x^{1/2}(\log\log x)^{1/2} \qquad \text{(Banks and Luca [1]).}$$

In the present note, we use similar techniques to show that the members of $\mathcal{L}$ are *scarcer than squares*, i.e., that $\#\mathcal{L}(x) = o(x^{1/2})$ as $x \to \infty$. More precisely, we prove the following:

Theorem 1. *For any fixed $\varepsilon > 0$ the bound*

$$\#\mathcal{L}(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}}$$

holds, where $\Theta = 0.129398\cdots$ is the least positive solution to the equation

$$2\Theta(\log\Theta - 1 - \log\log 2) = -\log 2. \tag{1.2}$$

As in the earlier papers [1, 5, 6, 7, 8] where bounds on the cardinality of $\mathcal{L}(x)$ are given, Theorem 1 admits a natural generalization. For an arbitrary integer a, let

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

and put

$$\mathcal{L}'_a = \big\{n \in \mathcal{L}_a \ : \ n \neq pa \text{ for } p \text{ prime}, p \nmid a\big\}.$$

Since $\mathcal{L}'_1 = \mathcal{L} \cup \{1\}$, Theorem 1 is the special case $a = 1$ of the following:

Theorem 2. *Let $a \in \mathbb{Z}$ and $\varepsilon > 0$ be fixed. Then,*

$$\#\mathcal{L}'_a(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}}\,,$$

where Θ is the least positive solution to the equation (1.2).

We remark that for $a = 0$ one has $\#\mathcal{L}'_0(x) \asymp (\log x)^2$, which follows from the result of Sierpiński [9, p. 232]:

$$\mathcal{L}'_0 = \{1\} \cup \big\{2^i\, 3^j \ : \ i \geqslant 1,\ j \geqslant 0\big\}.$$

Hence, we shall assume that $a \neq 0$ in the sequel.

2. Preliminaries

According to [7, Lemma 1] the inequality

$$\#\mathcal{L}'_a(x) \leqslant 4a^2 + \sum_{d\,|\,a} \#\mathcal{L}''_{a/d}(x/d)$$

holds, where

$$\mathcal{L}''_a = \big\{n \in \mathcal{L}'_a : n \text{ is square-free}\big\}.$$

Thus, to prove Theorem 2 it suffices to show that

$$\#\mathcal{L}''_a(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta-\varepsilon}}\,. \tag{2.1}$$

The following result is due to Pomerance [7, Theorem 1]:

Lemma 1. *Suppose that $n \geqslant 16a^2$, $n \in \mathcal{L}''_a$, and $K = \omega(n)$. Let the prime factorization of n be $p_1 \cdots p_K$, where $p_1 > \cdots > p_K$. Then, for $1 \leqslant i \leqslant K$ we have*

$$p_i < (i+1)\left(1 + \prod_{j=i+1}^{K} p_j\right).$$

We also need the following lemma from [8]:

Lemma 2. *Suppose that $\delta \geqslant 0$, $a_1 \geqslant \cdots \geqslant a_t = 0$, and $a_i \leqslant \delta + \sum_{j=i+1}^{t} a_j$ for $1 \leqslant i \leqslant t-1$. Then, for any real number ρ such that $0 \leqslant \rho < \sum_{i=1}^{t} a_i$, there is a subset $\mathcal{I}$ of $\{1,\ldots,t\}$ such that $\rho - \delta < \sum_{i\in\mathcal{I}} a_i \leqslant \rho$.*

Our principal tool is the next lemma, which is a simplified and weakened version of [2, Proposition 3]. For convenience, our lemma is stated in terms of $\log\log n$ rather than $\log\log x$ as in [2], but this change is easily justified in view of the term $(\log x)^{o(1)}$ that we include in our estimates.

Lemma 3. *For fixed $0 < \lambda < 1$, the counting function of the set*

$$\mathcal{V}_\lambda = \big\{n \;:\; \omega(n) < \lambda \log\log n\big\}$$

satisfies the bound

$$\#\mathcal{V}_\lambda(x) \leqslant \frac{x}{(\log x)^{1+\lambda\log(\lambda/e)+o(1)}} \qquad (x \to \infty).$$

For fixed $\lambda > 1$, the counting function of the set

$$\mathcal{W}_\lambda = \big\{n \;:\; \omega(n) > \lambda \log\log n\big\}$$

satisfies the bound

$$\#\mathcal{W}_\lambda(x) \leqslant \frac{x}{(\log x)^{1+\lambda\log(\lambda/e)+o(1)}} \qquad (x \to \infty).$$

Finally, we recall the well-known inequality of Landau [3]:

$$\frac{n}{\varphi(n)} \ll \log\log n \qquad (n \geqslant 3). \tag{2.2}$$

3. Proof of Theorem 2

We write the bound of [1] in the form:

$$\#\mathcal{L}''_a(x) \leqslant \#\mathcal{L}'_a(x) \leqslant x^{1/2}(\log x)^{o(1)} \qquad (x \to \infty). \tag{3.1}$$

Let $\varepsilon > 0$ be a small fixed parameter. Let α and β be fixed real numbers such that

$$\Theta - \varepsilon < \alpha/2 < \beta < \Theta,$$

where Θ is defined as in Theorem 1, and put

$$A = (\log x)^{\alpha} \qquad \text{and} \qquad B = (\log x)^{\beta}.$$

Note that (3.1) implies

$$\#\mathcal{L}''_a(x/A) \leqslant x^{1/2}(\log x)^{-\alpha/2+o(1)} \qquad (x \to \infty),$$

and since $\alpha/2 > \Theta - \varepsilon$ it follows that

$$\#\mathcal{L}''_a(x/A) \ll x^{1/2}(\log x)^{-\Theta+\varepsilon}. \tag{3.2}$$

Now let $n \in \mathcal{L}''_a$ be fixed with $16a^2 \leqslant x/A < n \leqslant x$. Put $K = \omega(n)$, and factor $n = p_1 \cdots p_K$ where $p_1 > \ldots > p_K$. By Lemma 1 we have

$$\log p_i < \log(2K) + \sum_{j=i+1}^{K} \log p_j \qquad (1 \leqslant i \leqslant K).$$

Applying Lemma 2 with $\delta = \log(2K)$, $t = K+1$, $a_i = \log p_i$ for $1 \leqslant i \leqslant K$, $a_t = 0$, and $\rho = \log(x^{1/2}/B)$, we conclude that n has a positive divisor d such that $\rho - \delta < \log d \leqslant \rho$; in other words,

$$\frac{x^{1/2}}{2\,\omega(n)B} \leqslant d \leqslant \frac{x^{1/2}}{B}\,. \tag{3.3}$$

Setting $m = n/d$, it is also clear that

$$\frac{x^{1/2}B}{A} \leqslant m \leqslant 2\,\omega(n)Bx^{1/2}. \tag{3.4}$$

First, suppose that $n \in \mathcal{W}_{20}$. Since n is square-free we have

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

hence either $d \in \mathcal{W}_{10}$ or $m \in \mathcal{W}_{10}$. Using the trivial bound $\omega(n) \leqslant 2\log x$ and the inequality $A \leqslant B^2$, we see that n has a divisor $k \in \mathcal{W}_{10}$ such that

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

Note that $\gcd(k, \varphi(k)) \mid a$ since $k \mid n$ and $n \equiv a \pmod{\varphi(n)}$. On the other hand, if k is fixed with the above properties, and n is a number in $\mathcal{L}_a$ that is divisible by k, then

$$n \equiv 0 \pmod{k} \qquad \text{and} \qquad n \equiv a \pmod{\varphi(k)}.$$

By the Chinese Remainder Theorem, we see that n is uniquely determined modulo $\mathrm{lcm}[k, \varphi(k)]$. Hence, the number of integers $n \leqslant x$ with $n \in \mathcal{L}''_a \cap \mathcal{W}_{20}$ and $k \mid n$ does not exceed

$$1 + \frac{x}{\mathrm{lcm}[k, \varphi(k)]} \leqslant 1 + \frac{xa}{k\varphi(k)} \ll 1 + \frac{x\log\log x}{k^2},$$

where we have used (2.2) in the last step. Put $y = x^{1/2}/(4B\log x)$ and $z = 4Bx^{1/2}\log x$. Summing the contributions over all such integers k, we derive that

$$\begin{aligned}
\#\big\{n \in \mathcal{L}''_a \cap \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\big\} &\ll \sum_{\substack{y \leqslant k \leqslant z \\ k \in \mathcal{W}_{10}}} \left(1 + \frac{x\log\log x}{k^2}\right) \\
&\leqslant \sum_{\substack{k \leqslant z \\ k \in \mathcal{W}_{10}}} 1 + x\log\log x \sum_{\substack{k \geqslant y \\ k \in \mathcal{W}_{10}}} \frac{1}{k^2} \\
&\ll \frac{z}{(\log z)^{14}} + \frac{x\log\log x}{y(\log y)^{14}}.
\end{aligned}$$

Here, we have used Lemma 3, the inequality $1 + 10\log(10/e) > 14$, and the estimate

$$\sum_{\substack{k \geqslant y \\ k \in \mathcal{W}_\lambda}} \frac{1}{k^2} \ll \frac{1}{y(\log y)^{1+\lambda\log(\lambda/e)+o(1)}} \qquad (y \to \infty),$$

which follows from Lemma 3 by partial summation. Inserting the definitions of y, z and B into the bound above, and noting that $\beta < \Theta < 1$, we derive that

$$\begin{aligned}
\#\big\{n \in \mathcal{L}''_a \cap \mathcal{W}_{20} \ : \ x/A \leqslant n \leqslant x\big\} &\ll \frac{Bx^{1/2}\log\log x}{(\log x)^{13}} \\
&\ll x^{1/2}(\log x)^{\beta-12} \\
&\ll x^{1/2}(\log x)^{-\Theta}.
\end{aligned} \tag{3.5}$$

Next, we consider the case that $n \notin \mathcal{W}_{20}$. Since $\omega(n) \leqslant 20\log\log x$, the inequalities (3.3) and (3.4) can be replaced by

$$\frac{x^{1/2}}{40B\log\log x} \leqslant d \leqslant \frac{x^{1/2}}{B} \tag{3.6}$$

and

$$\frac{x^{1/2}B}{A} \leqslant m \leqslant 40Bx^{1/2}\log\log x, \tag{3.7}$$

respectively. Let $\mathcal{T}$ be the collection of pairs (d,m) of natural numbers such that $dm \in \mathcal{L}_a''$ and the inequalities (3.6) and (3.7) hold. Then,

$$\#\big\{n \in \mathcal{L}_a'' \setminus \mathcal{W}_{20} \;:\; x/A \leqslant n \leqslant x\big\} \leqslant \#\mathcal{T}. \tag{3.8}$$

Lemma 4. *If x is sufficiently large, then for every integer m there is at most one integer d such that $(d,m) \in \mathcal{T}$.*

Proof. Suppose (d_1,m) and (d_2,m) both lie in $\mathcal{T}$. Since d_1m and d_2m are numbers in $\mathcal{L}_a''$, we have

$$\varphi(m) \mid d_1m - a \qquad \text{and} \qquad \varphi(m) \mid d_2m - a.$$

Hence it follows that

$$d_1 \equiv d_2 \pmod{\varphi(m)/\mu}, \tag{3.9}$$

where $\mu = \gcd(m,\varphi(m))$; note that $\mu \ll 1$ since $\mu \mid a$. By (3.6) we have the bound

$$\max\big\{d_1,d_2\big\} \leqslant \frac{x^{1/2}}{B} = x^{1/2}(\log x)^{-\beta},$$

whereas by (2.2) and (3.7) we have

$$\frac{\varphi(m)}{\mu} \gg \frac{m}{\log\log m} \geqslant x^{1/2}(\log x)^{\beta-\alpha+o(1)} \qquad (x \to \infty).$$

Since $\beta > \alpha/2$, it follows that for all sufficiently large x, both d_1 and d_2 are smaller than the modulus in (3.9), so the congruence becomes an equality $d_1 = d_2$. This completes the proof. $\square$

From now on, we assume that x is large enough to yield the conclusion of Lemma 4. Let $\mathcal{M}$ denote the set of integers m such that $(d,m) \in \mathcal{T}$ for some integer d. By Lemma 4, the map $(d,m) \mapsto m$ provides a bijection $\mathcal{T} \overset{\sim}{\longleftrightarrow} \mathcal{M}$; in particular, $\#\mathcal{T} = \#\mathcal{M}$, and (3.8) can be restated as

$$\#\big\{n \in \mathcal{L}_a'' \setminus \mathcal{W}_{20} \;:\; x/A \leqslant n \leqslant x\big\} \leqslant \#\mathcal{M}. \tag{3.10}$$

Let $\vartheta = 0.373365\cdots$ be the unique solution in the interval $(0,1)$ to the equation

$$1 + \vartheta\log(\vartheta/e) = \vartheta\log 2.$$

From (1.2) it follows that

$$2\Theta = 1 + \vartheta\log(\vartheta/e) = \vartheta\log 2. \tag{3.11}$$

We now express $\mathcal{M}$ as a disjoint union $\mathcal{M}_1 \cup \mathcal{M}_2$, where

$$\mathcal{M}_1 = \mathcal{M} \cap \mathcal{V}_\vartheta \qquad \text{and} \qquad \mathcal{M}_2 = \mathcal{M} \setminus \mathcal{V}_\vartheta.$$

Using Lemma 3, (3.7) and (3.11) we derive the bound

$$\#\mathcal{M}_1 \leqslant \#\mathcal{V}_\vartheta(40Bx^{1/2}\log\log x) = x^{1/2}(\log x)^{\beta-2\Theta+o(1)} \qquad (x\to\infty).$$

Since $\beta<\Theta$, it follows that

$$\#\mathcal{M}_1 \ll x^{1/2}(\log x)^{-\Theta}. \tag{3.12}$$

Lemma 5. *If x is sufficiently large, then for every integer d there is at most one integer $m\in\mathcal{M}_2$ such that $(d,m)\in\mathcal{T}$.*

Proof. Suppose (d,m_1) and (d,m_2) both lie in $\mathcal{T}$, where $m_1,m_2\in\mathcal{M}_2$. From the lower bound of (3.7) we see that both numbers m_1 and m_2 have at least $\kappa=\lfloor\vartheta\log\log(x^{1/2}B/A)\rfloor$ distinct odd prime divisors; hence both integers $\varphi(m_1)$ and $\varphi(m_2)$ are divisible by 2^κ. Since dm_1 and dm_2 are numbers in $\mathcal{L}_a''$, we can write

$$dm_1 = a+2^\kappa\varphi(d)s_1 \qquad\text{and}\qquad dm_2=a+2^\kappa\varphi(d)s_2$$

for some natural numbers s_1,s_2. Hence it follows that

$$m_1\equiv m_2 \pmod{2^\kappa\varphi(d)/\mu} \tag{3.13}$$

where $\mu=\gcd(d,2^\kappa\varphi(d))$; as before we have $\mu\ll 1$ since $\mu\mid a$. By (3.7) we have the bound

$$\max\big\{m_1,m_2\big\}\leqslant 40Bx^{1/2}\log\log x = x^{1/2}(\log x)^{\beta+o(1)} \qquad (x\to\infty).$$

On the other hand, since $\kappa=(\vartheta+o(1))\log\log x$ as $x\to\infty$, using (2.2), (3.6) and (3.11) we derive the lower bound

$$\frac{2^\kappa\varphi(d)}{\mu}\gg\frac{d\cdot 2^\kappa}{\log\log d}\geqslant\frac{x^{1/2}(\log x)^{\vartheta\log 2+o(1)}}{B(\log\log x)^2}=x^{1/2}(\log x)^{2\Theta-\beta+o(1)}.$$

Since $\beta<\Theta$, it follows that $2^\kappa\varphi(d)/\mu>\max\{m_1,m_2\}$ once x is sufficiently large. The congruence (3.13) then becomes an equality $m_1=m_2$, which finishes the proof. □

We now assume that x is large enough to yield the conclusion of Lemma 5. Let $\mathcal{D}$ denote the set of integers d such that $(d,m)\in\mathcal{T}$ for some integer $m\in\mathcal{M}_2$. Applying Lemma 5 and using the upper bound of (3.6), we see that

$$\#\mathcal{M}_2=\#\mathcal{D}\leqslant\frac{x^{1/2}}{B}=x^{1/2}(\log x)^{-\beta}.$$

Since $\beta>\Theta-\varepsilon$ we obtain

$$\#\mathcal{M}_2\leqslant x^{1/2}(\log x)^{-\Theta+\varepsilon}. \tag{3.14}$$

Combining (3.2), (3.5), (3.10), (3.12) and (3.14), and taking into account that $\#\mathcal{M}=\#\mathcal{M}_1+\#\mathcal{M}_2$, we derive the bound (2.1), and this finishes the proof of Theorem 2.

References

[1] W. D. Banks and F. Luca, Composite integers n for which $\varphi(n) \mid n-1$, *Acta Math. Sinica, English Series* **23** (2007), no. 10, 1915–1918.

[2] P. Erdős and J.-L. Nicolas, Sur la fonction: nombre de facteurs premiers de N, *Enseign. Math. (2)* **27** (1981), no. 1-2, 3–27.

[3] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig, 1909.

[4] D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.*, **38** (1932), 745–757.

[5] C. Pomerance, On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$, *Acta Arith.* **26** (1974/75), no. 3, 265–272.

[6] C. Pomerance, On composite n for which $\varphi(n) \mid n-1$, *Acta Arith.* **28** (1975/76), no. 4, 387–389.

[7] C. Pomerance, On composite n for which $\varphi(n) \mid n-1$, II, *Pacific J. Math.* **69** (1977), no. 1, 177–186.

[8] Z. Shan, On composite n for which $\varphi(n)|n-1$, *J. China Univ. Sci. Tech.*, **15** (1985), 109–112.

[9] W. Sierpiński, *Elementary Theory of Numbers*, Warsaw, 1964.