A remark on Giuga’s conjecture and Lehmer’s totient problem

WILLIAM D. BANKS
Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
bankswd@missouri.edu

C. WESLEY NEVANS
Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
cwnxxb@mizzou.edu

CARL POMERANCE
Mathematics Department, Dartmouth College
Hanover, NH 03755 USA
carl.pomerance@dartmouth.edu

June 11, 2009

Abstract

Giuga has conjectured that if the sum of the \((n-1)\)-st powers of the residues modulo \(n\) is \(-1\) \((\text{mod } n)\), then \(n\) is 1 or prime. It is known that any counterexample is a Carmichael number. Lehmer has asked if \(\varphi(n)\) divides \(n-1\), with \(\varphi\) being Euler’s function, must it be true that \(n\) is 1 or prime. No examples are known, but a composite number with this property must be a Carmichael number. We show that there are infinitely many Carmichael numbers \(n\) that are not counterexamples to Giuga’s conjecture and also do not satisfy \(\varphi(n) \mid n - 1\).

*MSC Numbers: 11A07, 11N25
1 Introduction

1.1 Carmichael numbers

In a letter to Frenicle dated October 18, 1640, Fermat wrote that if \( p \) is a prime number, then \( p \) divides \( a^{p-1} - 1 \) for any integer \( a \) not divisible by \( p \). This result, known as Fermat’s little theorem, is equivalent to the statement:

\[
a^p \equiv a \pmod{p} \quad \text{for all } a \in \mathbb{Z}.
\]

Almost three centuries later, Carmichael [5] began an in-depth study of composite natural numbers \( n \) with the property that

\[
a^n \equiv a \pmod{n} \quad \text{for all } a \in \mathbb{Z};
\]

these are now called Carmichael numbers. More than eighty years elapsed after Carmichael’s initial investigations before the existence of infinitely many Carmichael numbers was established by Alford, Granville, and Pomerance [1]. Denoting by \( C \) the set of Carmichael numbers, it is shown in [1] that for every \( \varepsilon > 0 \) and all sufficiently large \( X \), the lower bound

\[
|\{n \leq X : n \in C\}| \geq X^{\beta-\varepsilon}
\]

holds, where

\[
\beta = \beta_0 = \frac{5}{12} \left(1 - \frac{1}{2\sqrt{e}}\right) = 0.290306 \ldots > \frac{2}{7}.
\]

More recently, Harman [7] has shown that the lower bound (1) holds with the larger constant \( \beta = \beta_1 = 0.3322408 \).

The purpose of the present note is to show that the bound (1) with \( \beta = \beta_1 \) also holds with a set of Carmichael numbers \( n \leq X \) that are consistent with Giuga’s conjecture and support the nonexistence of examples to Lehmer’s totient problem. Our results are described in more detail below.

1.2 Giuga’s conjecture

Fermat’s little theorem implies

\[
p \mid 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} + 1
\]

\]
for every prime $p$. In 1950, Giuga [6] conjectured that the converse is true, i.e., that there are no composite natural numbers $n$ for which
\[ 1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \pmod{n}, \]
and he verified this conjecture for all $n \leq 10^{1000}$. Any counterexample to Giuga’s conjecture is called a Giuga number.

Denoting by $\mathcal{G}$ the (presumably empty) set of Giuga numbers, Giuga showed that $n \in \mathcal{G}$ if and only if $n$ is composite and
\[ p^2(p - 1) \mid n - p \quad \text{for every prime } p \text{ dividing } n. \quad (2) \]
As this condition implies that $n$ is squarefree, every Giuga number is a Carmichael number in view of the following criterion.

**Korselt’s criterion.** For a positive integer $n$, $a^n \equiv a \pmod{n}$ for all integers $a$ if and only if $n$ is squarefree and $p - 1$ divides $n - 1$ for every prime $p$ dividing $n$.

The condition (2) appears to be a much stronger requirement for a composite natural number $n$ to satisfy than Korselt’s criterion, thus it is reasonable to expect that there are infinitely many Carmichael numbers which are not Giuga numbers. Indeed, it is widely believed (see [1]) that
\[ \left| \{ n \leq X : n \in \mathcal{C} \} \right| = X^{1+o(1)} \quad \text{as } X \to \infty, \]
whereas Luca, Pomerance and Shparlinski [10] have established the bound
\[ \left| \{ n \leq X : n \in \mathcal{G} \} \right| \ll \frac{X^{1/2}}{(\log X)^2}, \quad (3) \]
improving slightly on a result of Tipu [15]. However, the result that $\mathcal{C} \setminus \mathcal{G}$ is an infinite set does not follow from (3) and the unconditional bound (1) with $\beta = \beta_1$. Nevertheless, we are able to prove the following result.

**Theorem 1.** For any fixed $\varepsilon > 0$ and all sufficiently large $X$, we have
\[ \left| \{ n \leq X : n \in \mathcal{C} \setminus \mathcal{G} \} \right| \geq X^{\beta_1 - \varepsilon}. \]
It is known that if $n$ is a Giuga number, then
\[ \frac{-1}{n} + \sum_{p|n} \frac{1}{p} \in \mathbb{N}. \] (4)

There are known composites that satisfy (4), for example $n = 30$. A \textit{weak Giuga number} is a composite number $n$ satisfying (4). Denoting by $W$ the set of weak Giuga numbers, we have $G \subset W$, hence Theorem 1 is an immediate consequence of the following theorem.

**Theorem 2.** For any fixed $\varepsilon > 0$ and all sufficiently large $X$, we have
\[ \left| \{ n \leq X : n \in C \setminus W \} \right| \geq X^{\beta_1 - \varepsilon}. \]

Our proof of Theorem 2 is given in §2 below.

### 1.3 Lehmer’s totient problem

Let $\varphi$ denote \textit{Euler’s function}. In 1932, Lehmer [8] asked whether there are any \textit{composite} natural numbers $n$ for which $\varphi(n) \mid n - 1$. This question, known as Lehmer’s totient problem, remains unanswered to this day.

Denote by $L$ the (possibly empty) set of composite natural numbers $n$ such that $\varphi(n) \mid n - 1$. It follows easily from Euler’s theorem that every element of $L$ is a Carmichael number. On the other hand, one expects that there are infinitely many Carmichael numbers which do \textit{not} lie in $L$.

In a series of papers (see [11, 12, 13]), Pomerance considered the problem of bounding the number of natural numbers $n \leq X$ that lie in $L$. In his third paper [13], he established the bound
\[ \left| \{ n \leq X : n \in L \} \right| \ll X^{1/2}(\log X)^{3/4}. \] (5)

Refinements of the underlying method of [13] led to subsequent improvements of the bound (5) by Shan [14], Banks and Luca [4], Banks, Güloğlu and Nevans [3], and Luca and Pomerance [9]; however, it is still unknown whether the bound
\[ \left| \{ n \leq X : n \in L \} \right| \ll X^\alpha \]
holds with some constant $\alpha < 1/2$. In particular, the result that $C \setminus L$ is an infinite set does not follow from only the unconditional bound (1) with $\beta = \beta_1$. In this note we prove the following theorem.
Theorem 3. For any fixed $\varepsilon > 0$ and all sufficiently large $X$, we have
\[ \left| \{ n \leq X : n \in \mathcal{C} \setminus \mathcal{L} \} \right| \geq X^{\beta_1 - \varepsilon}. \]

Our proof of Theorem 3 is given in §2 below.

2 Construction

Let $\mathcal{N}$ denote the set of composite natural numbers $n$ such that
\[ \sum_{p|n} \frac{1}{p} < \frac{1}{3}. \]

Lemma 1. The sets $\mathcal{N}$ and $\mathcal{W}$ are disjoint.

Proof. Let $n \in \mathcal{N}$. Since
\[ \frac{1}{n} < \sum_{p|n} \frac{1}{p} < \frac{1}{3} < 1 + \frac{1}{n}, \]
it is clear that
\[ \sum_{p|n} \frac{1}{p} \not\equiv \frac{1}{n} \pmod{1}, \]
hence $n$ is not a weak Giuga number. \qed

Lemma 2. The sets $\mathcal{N}$ and $\mathcal{L}$ are disjoint.

Proof. Let $n \in \mathcal{N}$. Using the inequality
\[ \log(1 - t) > -2t \quad (0 < t \leq 1/2), \]
we have
\[ \log \frac{\varphi(n)}{n} = \log \prod_{p|n} \left( 1 - \frac{1}{p} \right) = \sum_{p|n} \log \left( 1 - \frac{1}{p} \right) > -2 \sum_{p|n} \frac{1}{p} > -\frac{2}{3}. \]
Consequently,
\[ \frac{n - 1}{\varphi(n)} < \frac{n}{\varphi(n)} < e^{2/3} < 2, \quad (6) \]
and it follows that $n \not\in \mathcal{L}$. Indeed, (6) and the condition $\varphi(n) \mid n - 1$ together imply that $n = 1$ or $\varphi(n) = n - 1$, which possibilities cannot occur for a composite natural number $n$. \qed
In view of Lemmas 1 and 2, Theorems 2 and 3 follow from the following result.

**Theorem 4.** For any fixed $\varepsilon > 0$ and all sufficiently large $X$, we have

$$\left| \left\{ n \leq X : n \in C \cap N \right\} \right| \geq X^{\beta_1 - \varepsilon}.$$ 

**Proof.** With the existing proofs of the infinitude of Carmichael numbers given in [1] and [7], a careful reading, or with small changes, shows that the Carmichael numbers constructed lie in $N$. Since Harman [7, Theorem 1] has the stronger result, we give the details on how that proof supports our assertion. As mentioned, he has shown that for every $\varepsilon > 0$ and all sufficiently large $X$, the lower bound

$$\left| \left\{ n \leq X : n \in C \right\} \right| \geq X^{\beta_1 - \varepsilon} \quad (7)$$

holds. To prove Theorem 4, it suffices to show that the Carmichael numbers constructed by Harman all lie in $N$ if $X$ is large enough. We begin with the following statement, which is [7, Theorem 3].

**Lemma 3.** Let $\varepsilon > 0$, and suppose $y \geq y_0(\varepsilon)$. Put

$$\delta = \frac{\varepsilon \theta}{1.888}, \quad x = \exp \left( y^{1+\delta} \right), \quad \theta = \frac{1}{0.2961}.$$

Then there is a positive integer $k < x^{0.528}$ and a set of squarefree numbers $B$ such that

(i) $B \subset [x^{0.4}, x^{0.472}]$;

(ii) $|B| > x^{\beta_1 - \varepsilon}$;

(iii) $dk + 1$ is prime for every $d \in B$;

(iv) if $p \mid d$, then

$$0.5 y^\theta < p < y^\theta, \quad p \nmid k, \quad P(p - 1) < y,$$

where $P(n)$ denotes the greatest prime factor of $n$.

Let $n$ be one of the Carmichael numbers constructed in [7, Theorem 1]. Such a number $n$ is composed of at most $t = \exp \left( y^{1+\delta/2} \right)$ primes of the form $p = dk + 1$ with $d \in B$, so that
• $n \leq X$, where $X = x^t$;
• $p \geq x^{0.4}$ for every prime $p \mid n$.

Taking into account that $t = x^{o(1)}$ as $x \to \infty$, it follows that
\[
\sum_{p \mid n} \frac{1}{p} \leq t x^{-0.4} < \frac{1}{3}
\]
if $x$ is sufficiently large. Since the value of $x$ is determined uniquely by $X$, this shows that the Carmichael number $n$ lies in $\mathcal{N}$ once $X$ is large enough, completing the proof.

We remark that in [2] it is shown that for each fixed $k$ there are infinitely many Carmichael numbers $n$ with $\sum_{p \mid n} 1/p < 1/(\log n)^k$. This result too supports our principal assertion that $\mathcal{C} \cap \mathcal{N}$ is infinite, but the bound for the counting function proved here is even smaller than that given in [1]. On the other hand, it is not known if there is some $\varepsilon > 0$ such that for infinitely many Carmichael numbers $n$ we have $\sum_{p \mid n} 1/p > \varepsilon$. In particular, it is not known if the set $\mathcal{C} \setminus \mathcal{N}$ is infinite.

Acknowledgment. The third author was supported in part by NSF grant DMS-0703850.

References


