On a variant of Giuga numbers

José María Grau
Departamento de Matemáticas
Universidad de Oviedo
Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain
grau@uniovi.es

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx
and
The John Knopfmacher Centre
for Applicable Analysis and Number Theory
University of the Witwatersrand, P.O. Wits 2050, South Africa

Antonio M. Oller-Marcén
Departamento de Matemáticas
Universidad de Zaragoza
C/Pedro Cerbuna 12, 50009 Zaragoza, Spain
oller@unizar.es

January 15, 2013

Abstract

In this paper, we characterize the odd positive integers n satisfying the congruence $\sum_{j=1}^{n-1} j^{\frac{n-1}{2}} \equiv 0 \pmod{n}$. We show that the set of such positive integers has an asymptotic density which turns out to be slightly larger than 3/8.

1 Introduction

Given any property $\mathbf{P}$ satisfied by the primes, it is natural to consider the set $\mathcal{C}_{\mathbf{P}} := \{n \text{ composite} : n \text{ satisfies } \mathbf{P}\}$. Elements of $\mathcal{C}_{\mathbf{P}}$ can be thought of as pseudoprimes with respect to the property $\mathbf{P}$. Such sets of pseudoprimes have been of interest to number theorists.

Putting aside practical primality tests such as Fermat, Euler, Euler–Jacobi, Miller–Rabin, Solovay–Strassen, and others, let us have a look at some interesting, although not very efficient, primality tests as summarized in the table below.

	Test	Pseudoprimes	Infinitely many
1	$(n-1)! \equiv -1 \pmod{n}$	None	No
2	$a^n \equiv a \pmod{n}$ for all a	Carmichael numbers	Yes
3	$\sum_{j=1}^{n-1} j^{\phi(n)} \equiv -1 \pmod{n}$	Giuga numbers	Unknown
4	$\phi(n) \mid (n-1)$	Lehmer numbers	No example known
5	$\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$		No example known

In the above table, $\phi(n)$ is the Euler function of n.

The first test in the table, due to Wilson and published by Waring in [19], is an interesting and impractical characterization of a prime number. As a consequence, no pseudoprimes for this test exist.

The pseudoprimes for the second test in the table are called Carmichael numbers. They were characterized by Korselt in [10]. In [1], it is proved that there are infinitely many of them. The counting function for the Carmichael numbers was studied by Erdős in [6] and by Harman in [9].

The pseudoprimes for the third test are called Giuga numbers. The sequence of such numbers is sequence A007850 in OEIS. These numbers were introduced and characterized in [4]. For example, a Giuga number is a squarefree composite integer n such that p divides $n/p - 1$ for all prime factors p of n. All known Giuga numbers are even. If an odd Giuga number exists, it must be the product of at least 14 primes. The Giuga numbers also satisfy the congruence $nB_{\phi(n)} \equiv -1 \pmod{n}$, where for a positive integer m the notation B_m stands for the mth Bernoulli number.

The fourth test in the table is due to Lehmer (see [11]) and it dates back to 1932. Although it has recently drawn much attention, it is still not known whether any pseudoprimes at all exist for this test or not. In a series of papers (see [14], [15], and [16]), Pomerance has obtained upper bounds for the counting function of the Lehmer numbers, which are the pseudoprimes for this test. In his third paper [16], he succeded in showing that the counting function of the Lehmer numbers $n \le x$ is $O(x^{1/2}(\log x)^{3/4})$. Refinements of the underlying method of [16] led to subsequent improvements in the exponent of the logarithm in the above bound by Shan [17], Banks and Luca [2], Banks, Güloğlu and Nevans [3], and Luca and Pomerance [12], respectively. The best exponent to date is due to Luca and Pomerance [12] and it is $-1/2 + \varepsilon$ for any $\varepsilon > 0$.

The last test in the table is based on a conjecture formulated in 1959 by Giuga [8], which states that the set of pseudoprimes for this test is empty. In [4], it is shown that every counterexample to Giuga's conjecture is both a Carmichael number and a Giuga number. Luca, Pomerance and Shparlinski [13] have showed that the counting function for these numbers $n \le x$ is $O(x^{1/2}/(\log x)^2)$ improving slightly on a previous result by Tipu [18].

In this paper, inspired by Giuga's conjecture, we study the odd positive integers n satisfying the congruence

$$\sum_{j=1}^{n-1} j^{(n-1)/2} \equiv 0 \pmod{n}. \tag{1}$$

It is easy to see that if n is an odd prime, then n satisfies the above congruence. We characterize such positive integers n and show that they have an asymptotic density which turns out to be slightly larger than 3/8.

For simplicity we put

$$G(n) = \sum_{j=1}^{n-1} j^{\lfloor (n-1)/2 \rfloor},$$

although we study this function only for odd values of n.

2 On the congruence $G(n) \equiv 0 \pmod{n}$ for odd n

We put

$$\mathfrak{P} := \{n \text{ odd} : G(n) \equiv 0 \pmod{n}\}.$$

It is easy to observe that every odd prime lies in $\mathfrak{P}$. In fact, by Euler's criterion, if p is an odd prime, then $j^{(p-1)/2} \equiv \left(\frac{j}{p}\right) \pmod{p}$, where $\left(\frac{j}{p}\right)$ denotes the Legendre symbol of j with respect to p. Thus,

$$G(p) \equiv \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \equiv 0 \pmod{p},$$

so that $p \in \mathfrak{P}$.

We start by showing that numbers which are congruent to $3 \pmod{4}$ are in $\mathfrak{P}$.

Proposition 1. *If $n \equiv 3 \pmod{4}$, then $n \in \mathfrak{P}$.*

Proof. Writing $n = 4m + 3$, we have that $(n-1)/2 = 2m + 1$ is odd. Now,

$$\begin{aligned} 2G(n) &= \sum_{j=1}^{n-1} \left(j^{2m+1} + (n-j)^{2m+1}\right) \\ &= n \sum_{j=1}^{n-1} \left(j^{2m} + j^{2m-1}(n-j) + \cdots + (n-j)^{2m}\right), \end{aligned}$$

so $n \mid 2G(n)$. Since n is odd, we get that $G(n) \equiv 0 \pmod{n}$, which is what we wanted. $\square$

The next lemma is immediate.

Lemma 2. *Let p be an odd prime and let $k \geq 1$ be an integer. Then*

$$\gcd\left(\frac{p^k-1}{2}, \varphi(p^k)\right) = \gcd\left(\frac{p^k-1}{2}, p-1\right) = \begin{cases} p-1 & \text{if } k \text{ is even,} \\ (p-1)/2 & \text{if } k \text{ is odd.} \end{cases}$$

With this lemma in mind we can prove the following result.

Proposition 3. *Let p be an odd prime and let $k \geq 1$ be any integer. Then, $p^k \in \mathfrak{P}$ if and only if k is odd.*

Proof. Let $\alpha \in \mathbb{Z}$ be an integer whose class modulo p^k is a generator of the unit group of $\mathbb{Z}/p^k\mathbb{Z}$. We put $\beta := \alpha^{(p^k-1)/2}$. Suppose first that k is odd. We then claim that $\beta - 1$ is not zero modulo p. In fact, if $\alpha^{(p^k-1)/2} \equiv 1 \pmod p$, then since also $\alpha^{p-1} \equiv 1 \pmod p$, we get, by Lemma 2, that $\alpha^{(p-1)/2} \equiv 1 \pmod p$, which is impossible.

Now, since $\beta - 1$ is coprime to p, it is invertible modulo p^k. Moreover, since also $k \leq (p^k-1)/2$, we have that

$$\begin{aligned} G(n) &= \sum_{j=1}^{n-1} j^{(p^k-1)/2} \equiv \sum_{\substack{\gcd(j,p)=1 \\ 1 \leq j \leq n-1}} j^{(p^k-1)/2} \pmod{p^k} \\ &\equiv \sum_{j=1}^{\varphi(p^k)} \left(\alpha^{(p^k-1)/2}\right)^i \pmod{p^k} \equiv \sum_{i=1}^{\phi(p^k)} \beta^i \pmod{p^k} \\ &= \frac{\beta^{\varphi(p^k)+1} - \beta}{\beta - 1} \equiv 0 \pmod{p^k}. \end{aligned}$$

Assume now that k is even. Observe that

$$(p^k-1)/2 = (p-1)((1 + p + \cdots + p^{k-1})/2) := (p-1)m,$$

and m is an integer which is coprime to p. Thus, $\beta = \alpha^{(p^k-1)/2} = (\alpha^{(p-1)})^m$ has order p^{k-1} modulo p^k, and so does α^{p-1}. Moreover, again since $k \leq$

$(p^k-1)/2$, we may eliminate the multiples of p from the sum defining $G(n)$ modulo n and get

$$\begin{aligned} G(n) &= \sum_{j=1}^{n-1} j^{(p^k-1)/2} \equiv \sum_{\substack{\gcd(j,p)=1\\ 1\le j\le n-1}} j^{(p^k-1)/2} \pmod{p^k} \\ &\equiv \sum_{i=1}^{\varphi(p^k)} \left(\alpha^{(p^k-1)/2}\right)^i \equiv \sum_{i=1}^{p^{k-1}(p-1)} \left(\alpha^{(p-1)}\right)^{im} \pmod{p^k} \\ &\equiv (p-1)\sum_{i=1}^{p^{k-1}} \left(\alpha^{p-1}\right)^i \pmod{p^k}. \end{aligned} \tag{2}$$

Since α^{p-1} has order p^{k-1} modulo p^k, it follows that $\alpha^{p-1} = 1 + pu$ for some integer u which is coprime to p. Then

$$\sum_{i=1}^{p^{k-1}} \left(\alpha^{p-1}\right)^i = \alpha\left(\frac{\alpha^{p^{k-1}}-1}{\alpha-1}\right). \tag{3}$$

Since $\alpha^{p^{k-1}} \equiv 1 + p^k u \pmod{p^{k+1}}$, it follows that $(\alpha^{p^{k-1}}-1)/(\alpha-1) \equiv p^{k-1} \pmod{p^k}$, so that

$$\alpha\left(\frac{\alpha^{p^{k-1}}-1}{\alpha-1}\right) \equiv \alpha p^{k-1} \pmod{p^k} \equiv p^{k-1} \pmod{p^k}. \tag{4}$$

Calculations (3) and (4) together with congruences (2) give that $G(n) \equiv (p-1)p^{k-1} \pmod{p^k}$. Thus, p^k is not in $\mathfrak{P}$ when k is even. $\square$

Note that Proposition 3 does not extend to powers of positive integers having at least two distinct prime factors. For example, $n = 2021 = 43 \times 47$ has the property that both n and n^2 belong $\mathfrak{P}$.

3 A characterization of $\mathfrak{P}$ and applications

Here, we take a look into the arithmetic structure of the elements lying in $\mathfrak{P}$. We start with an easy but useful lemma.

Lemma 4. *Let* $n = \prod_{p^{r_p}\|n} p^{r_p}$ *be an odd integer, and let* A *be any positive integer. If* $\gcd(A, p-1) < p-1$ *for all* $p \mid n$*, then*

$$\sum_{\substack{\gcd(j,n)=1\\ 1\le j\le n-1}} j^A \equiv 0 \pmod{n}.$$

Proof. It suffices to prove that the above congruence holds for all prime powers $p^{r_p}\|n$. So, let p^r be such a prime power and let α be an integer which is a generator of the unit group of $\mathbb{Z}/p^r\mathbb{Z}$. Put $\beta := \alpha^A$. An argument similar to the one used in the proof of Proposition 3 (the case when k is odd) shows that the condition $\gcd(A, p-1) < p-1$ entails that $\beta - 1$ is not a multiple of p. Thus, $\beta - 1$ is invertible modulo p. We now have

$$\begin{aligned}
\sum_{\substack{\gcd(j,n)=1\\ 1\le j\le n-1}} j^A &\equiv \left(\frac{\phi(n)}{\phi(p^r)}\right) \sum_{\substack{\gcd(j,p)=1\\ 1\le j\le p}} j^A \pmod{p^r} \equiv \phi(n/p^r) \sum_{i=1}^{\phi(p^r)} \alpha^{Ai} \pmod{p^r}\\
&\equiv \phi(n/p^r) \sum_{i=1}^{\phi(p^r)} \beta^i \pmod{p^r} \equiv \phi(n/p^r)\frac{\beta^{\phi(p^r)+1} - \beta}{\beta - 1} \pmod{p^r}\\
&\equiv 0 \pmod{p^r},
\end{aligned}$$

which is what we wanted to prove. ◻

Theorem 5. *A positive integer* n *is in* $\mathfrak{P}$ *if and only if* $\gcd((n-1)/2, p-1) < p-1$ *for all* $p \mid n$.

Proof. Assume that n is odd and $\gcd((n-1)/2, p-1) < p-1$. By Lemma 4,

$$\sum_{\substack{(j,n)=1\\ 1\le j\le n-1}} j^{(n-1)/2} \equiv 0 \pmod{n}.$$

Now, let d be any divisor of n. Observe that

$$\sum_{\substack{(j,n)=d\\ 1\le j\le n-1}} j^{\frac{n-1}{2}} = d^{\frac{n-1}{2}} \sum_{\substack{(i,n/d)=1\\ 1\le i\le n/d-1}} i^{\frac{n-1}{2}}. \tag{5}$$

The last sum in the right–hand side of (5) above is, by Lemma 4, a multiple of n/d, so that the sum in the left–hand side of (5) above is a multiple of n.

Summing up these congruences over all possible divisors d of n and noting that
$$G(n) = \sum_{d|n} \sum_{\substack{\gcd(j,n)=d \\ 1\le j\le n-1}} j^{(n-1)/2},$$
we get that $G(n) \equiv 0 \pmod{n}$, so $n \in \mathfrak{P}$.

Conversely, say $n \in \mathfrak{P}$ is some odd number and assume that there exists a prime factor p of n such that $p-1 \mid (n-1)/2$. Write $(n-1)/2 = (p-1)m$. Observe that m is coprime to p. Assume that $p^r \| n$. Then, modulo p^r, we have

$$G(n) = \sum_{j=1}^{n-1} j^{(n-1)/2} \equiv (n/p^r) \sum_{\substack{\gcd(j,p)=1 \\ 1\le j\le p^r-1}} j^{(n-1)/2} \pmod{p^r} \equiv (n/p^r) \sum_{\substack{\gcd(j,p)=1 \\ 1\le j\le p^r-1}} j^{(p-1)}.$$

The argument used in Proposition 3 (the case when k is even), shows that the second sum is not zero modulo p^r, and since n/p^r is also coprime to p, we get that p^r does not divide $G(n)$, a contradiction.

This completes the proof of the theorem. $\square$

Here are a few immediate corollaries of Theorem 5.

Corollary 6. *Let n be any integer. Assume that one of the following conditions hold:*

i) $\gcd((n-1)/2, \varphi(n))$ *is odd;*

ii) $\gcd((n-1)/2, \lambda(n))$ *is odd, where* $\lambda(n)$ *the Carmichael function.*

Then $n \in \mathfrak{P}$.

Corollary 7. *If $n^k \in \mathfrak{P}$ for some $k \geq 1$, then $n \in \mathfrak{P}$.*

Proof. Observe that $\gcd((n-1)/2, p-1)$ divides $\gcd\left((n^k-1)/2, p-1\right)$ for every k and every prime number p. Now the corollary follows from Theorem 5. $\square$

We add another sufficient condition which is somewhat reminiscent of the characterization of the Giuga numbers.

Proposition 8. *Let $n = \prod_{p^{r_p} \| n} p^{r_p}$ be an odd integer. If $p-1$ does not divide $n/p^{r_p} - 1$ for every prime factor p of n, then $n \in \mathfrak{P}$.*

Proof. By Theorem 5, if $n \notin \mathfrak{P}$, then there exists a prime factor p of n such that $p-1$ divides $(n-1)/2$. In particular, $p-1 \mid n-1$. Since $p-1$ also divides $p^{r_p} - 1$, it follows that $p-1$ divides $n - p^{r_p} = p^{r_p}(n/p^{r_p} - 1)$. Since $p-1$ is obviously coprime to p^{r_p}, we get that $p-1$ divides $n/p^{r_p} - 1$, which is a contradiction. □

It is also easy to determine whether numbers of the form $2^m + 1$ are in $\mathfrak{P}$. Indeed, assume that $2^m + 1 \notin \mathfrak{P}$ for some positive integer m. Then, by Theorem 5, there is some prime $p \mid 2^m + 1$ such that $p - 1 \mid ((2^m + 1) - 1)/2 = 2^{m-1}$. Thus, $p = 2^a + 1$ for some $a \le m-1$, and so p is a Fermat prime. In particular, $a = 2^\alpha$ for some $\alpha \ge 0$. Since $p = 2^{2^\alpha} + 1$ is a proper divisor of $2^m + 1$, it follows that $2^\alpha \mid m$ and $m/2^\alpha$ is odd. This is possible only when 2^α is the exact power of 2 in m and m is not a power of 2. So, we have the following result.

Proposition 9. *Let $n = 2^m + 1$ and $m = 2^\alpha m_1$ with $\alpha \ge 0$ and odd $m_1 > 1$. Then $n \in \mathfrak{P}$ unless $2^{2^\alpha} + 1$ is a Fermat prime.*

4 Asymptotic density of $\mathfrak{P}$

Let $\mathbb{I}$ be the set of odd positive integers. In order to compute the asymptotic density of $\mathfrak{P}$, or to even prove that it exists, it suffices to understand the elements in its complement $\mathbb{I} \backslash \mathfrak{P}$. It turns out that this is easy. For an odd prime p let

$$\mathcal{F}_p := \{p^2 \pmod{2p(p-1)}\}.$$

Observe that $\mathcal{F}_p \subseteq \mathbb{I}$.

Theorem 10. *We have*

$$\mathbb{I} \backslash \mathfrak{P} = \bigcup_{p \ge 3} \mathcal{F}_p. \tag{6}$$

Proof. By Theorem 5, we have that $n \notin \mathfrak{P}$ if and only if $p-1$ divides $(n-1)/2$ for some prime factor p of n. This condition is equivalent to $n \equiv 1 \pmod{2(p-1)}$. Write $n = pm$ for some positive integer m. Since p is invertible modulo $2(p-1)$, it follows that m is uniquely determined modulo $2(p-1)$. It suffices to notice that the class of m modulo $2(p-1)$ is in fact p since then $pm \equiv p^2 \equiv 1 \pmod{2(p-1)}$ with the last congruence following because $p^2-1 = (p-1)(p+1)$ is a multiple of $2(p-1)$. This completes the proof. $\square$

Observe that $\mathcal{F}_p$ is an arithmetic progression of difference $1/(2p(p-1))$. Since the series

$$\sum_{p \geq 3} \frac{1}{2p(p-1)}$$

is convergent, it follows immediately that $\mathbb{I}\backslash\mathfrak{P}$; hence, also $\mathfrak{P}$, has a density. This also suggests a way to compute the density of $\mathfrak{P}$ with arbitrary precision. Namely, say $\varepsilon > 0$ is given. Let $3 = p_1 < p_2 < \cdots$ be the increasing sequence of all the odd primes. Let $k := k(\varepsilon)$ be minimal such that

$$\sum_{j \geq k} \frac{1}{2p_j(p_j-1)} < \varepsilon.$$

It then follows that numbers $n \notin \mathfrak{P}$ which are divisible by a prime p_j with $j \geq k$ belong to $\bigcup_{j \geq k} \mathcal{F}_{p_j}$, which is a set of density $< \varepsilon$. Thus, with an error of at most ε, the density of the set $\mathbb{I}\backslash\mathfrak{P}$ is the same as the density of

$$\bigcup_{j<k} \mathcal{F}_{p_j},$$

which is, by the Principle of Inclusion and Exclusion,

$$\sum_{s \geq 1} \sum_{1 \leq i_1 < i_2 < \cdots < i_s \leq k-1} \frac{\varepsilon_{i_1,i_2,\ldots,i_s}}{\operatorname{lcm}[2p_{i_1}(p_{i_1}-1), \ldots, 2p_{i_s}(p_{i_s}-1)]}, \tag{7}$$

with the coefficient $\varepsilon_{i_1,i_2,\ldots,i_s}$ being zero if $\bigcap_{t=1}^{s} \mathcal{F}_{p_{i_t}} = \emptyset$, and being $(-1)^{s-1}$ otherwise. Taking $\varepsilon := 0.00082$, we get that $k = 29$,

$$\rho\Big(\bigcup_{j<29} \mathcal{F}_{p_j}\Big) = \frac{27451063230328339490722228724697099 4037}{22842689075166883974006211084468817520 20} \approx 0.120174,$$

and consequently $\rho(\mathfrak{P})$ belongs to $[0.379005, 0.379826]$. So, we can say that

$$\rho(\mathfrak{P}) = 0.379\ldots$$

Here and in what follows, for a subset $\mathcal{A}$ of the set of positive integers we used $\rho(\mathcal{A})$ for its density when it exists.

These computations were carried out with *Mathematica*, for which it was necessary to have a good criterion to determine when the intersection of $\mathcal{F}_p$ for various odd primes p is empty. We devote a few words on this issue. Let us observe first that the condition $n \in \mathcal{F}_p$, which is equivalent to the fact that $p \mid n$ and $p-1$ divides $(n-1)/2$, can be formulated as the pair congruences

$$\begin{array}{rcll} n & \equiv & 1 & \pmod{2(p-1)}; \\ n & \equiv & 0 & \pmod{p}. \end{array} \tag{8}$$

Assume now that $\mathcal{P}$ is some finite set of primes. Let us look at $\bigcap_{p\in\mathcal{P}} \mathcal{F}_p$. Put $m := \prod_{p\in\mathcal{P}} p$. The first set of congruences (8) for all $p \in \mathcal{P}$ is equivalent to

$$n \equiv 1 \pmod{2\lambda(m)}, \tag{9}$$

where $\lambda(m) = \mathrm{lcm}[p-1 : p \in \mathcal{P}]$ is the Carmichael λ-function of m. The second set of congruences for $p \in \mathcal{P}$ is equivalent to

$$n \equiv 0 \pmod{m}. \tag{10}$$

Since 1 is not congruent to 0 modulo any prime q, it follows that a necessary condition for (9) and (10) to hold simultaneously is that m and $2\lambda(m)$ are coprime. This is also sufficient by the Chinese Remainder Lemma in order for the pair of congruences (9) and (10) to have a solution n. Since m is also squarefree, the condition that $m > 1$ is odd and m and $2\lambda(m)$ are coprime is equivalent to $m > 2$ and m and $\phi(m)$ are coprime. Put

$$\mathcal{M} := \{m > 2 : \gcd(m, \phi(m)) = 1\}. \tag{11}$$

Thus, we proved the following result.

Proposition 11. *Let $\mathcal{P}$ be a finite set of primes and put $m := \prod_{p\in\mathcal{P}} p$. Then $\bigcap_{p\in\mathcal{P}} \mathcal{F}_p$ is nonempty if and only if $m \in \mathcal{M}$, where this set is defined at* (11) *above. If this is the case, then the set $\bigcap_{p\in\mathcal{P}} \mathcal{F}_p$ is an arithmetic progression of difference $1/(2m\lambda(m))$.*

The condition that $m \in \mathcal{M}$ can also be formulated by saying that m is odd, squarefree and $p \nmid q-1$ for all primes p and q dividing m. We recall that the set $\mathcal{M}$ has been studied intensively in the literature. For example, putting $\mathcal{M}(x) = \mathcal{M} \cap [1, x]$, Erdős [5] proved that

$$\#\mathcal{M}(x) = e^{-\gamma}(1+o(1))\frac{x}{\log\log\log x} \qquad \text{as} \quad x \to \infty.$$

In particular, it follows that if $\mathcal{P}$ is a finite set of primes, then $\bigcap_{p\in\mathcal{P}} \mathcal{F}_p \neq \emptyset$ if and only if $\mathcal{F}_p \bigcap \mathcal{F}_q \neq \emptyset$ for any two elements p and q of $\mathcal{P}$.

Finally, let us observe that with this formalism and the Principle of Inclusion and Exclusion, as in (7) for example, we can write that

$$\rho(\mathfrak{P}) = \sum_{m\in\mathcal{M}\cup\{1\}} \frac{(-1)^{\omega(m)}}{2m\lambda(m)}.$$

Here, $\omega(m)$ is the number of distinct prime factors of m. The fact that the above series converges absolutely follows easily from the inequality $\lambda(m) > (\log m)^{c\log\log\log m}$ which holds with some positive constant c for all sufficiently large m (see [7]), as well the fact that the series

$$\sum_{m\geq 2} \frac{1}{m(\log m)^2}$$

converges. We give no further details.

References

[1] W.R. Alford, A. Granville and C. Pomerance, "There are infinitely many Carmichael numbers", *Ann. Math. (2)* **139** (1994), 703–722.

[2] W. D. Banks and F. Luca, "Composite integers n for which $\phi(n) \mid n-1$", *Acta Math. Sinica* **23** (2007), 1915–1918.

[3] W. D. Banks, A. M. Güloğlu, C. W. Nevans, "On the congruence $N \equiv A \pmod{\phi(N)}$", *INTEGERS* **8** (2008), A59.

[4] D. Borwein, J. M. Borwein, P. B. Borwein and R. Girgensohn, “Giuga’s conjecture on primality”, *Amer. Math. Monthly* **103** (1996), 40–50.

[5] P. Erdős, “Some Asymptotic Formulas in Number Theory”, *J. Indian Math. Soc. (N. S.)* **12** (1948), 75–78.

[6] P. Erdős, “On pseudoprimes and Carmichael numbers”, *Publ. Math. Debrecen* **4** (1956), 201–206.

[7] P. Erdős, C. Pomerance and E. Schmutz, “Carmichael’s λ function”, *Acta Arith.* **58** (1991), 363–385.

[8] G. Giuga, “Su una presumibile proprietá caratteristica dei numeri primi”, *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3)* **14(83)** (1950), 511–528.

[9] G. Harman, “On the number of Carmichael numbers up to x”, *Bull. London Math. Soc.* **37** (2005), 641–650.

[10] A. Korselt, “Problème chinois”, *L’intermédiaire des mathematiciens* **6** (1899), 142–143.

[11] D. H. Lehmer, “On Euler’s totient function”, *Bull. Amer. Math. Soc.* **38** (1932), 745–751.

[12] F. Luca and C. Pomerance, “On composite n for which $\phi(n) \mid n-1$”, *Bol. Soc. Mat. Mexicana*, to appear.

[13] F. Luca, C. Pomerance and I. E. Shparlinski, “On Giuga numbers”, *Int. J. Modern Math.* **4** (2009), 13–18.

[14] C. Pomerance, “On the congruences $\sigma(n) \equiv a \pmod n$ and $n \equiv a \pmod{\phi(n)}$”, *Acta Arith.* **26** (1974/1975), 265–272.

[15] C, Pomerance, “On composite n for which $\phi(n) \mid n-1$”, *Acta Arith.* **28** (1975/1976), 387–389.

[16] C. Pomerance, “On composite n for which $\phi(n) \mid n-1$. II”, *Pacific J. Math.* **69** (1977), 177–186.

[17] Z. Shan, “On composite n for which $\phi(n) \mid n-1$”, *J. China Univ. Sci. Tech.* **15** (1985), 109–112.

[18] V. Tipu, “A note on Giuga’s conjecture”, *Canadian Math. Bull.* **50** (2007), 158–160.

[19] E. Waring, *Meditationes algebraicæ*, Amer. Math. Soc. **1991**.