# GENERALIZATIONS OF CARMICHAEL NUMBERS I

ROMEO MEŠTROVIĆ

*Dedicated to the 100th anniversary of birth of Paul Erdős*

Abstract. A composite positive integer $n$ is said to be a *weak Carmichael number* if

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}\equiv \varphi(n) \pmod{n}. \tag{1}$$

It is proved that a composite positive integer $n$ is a weak Carmichael number if and only if $p-1\mid n-1$ for every prime divisor $p$ of $n$. This together with Korselt's criterion yields the fact that every Carmichael number is also a weak Carmichael number.

In this paper we mainly investigate arithmetic properties of weak Carmichael numbers. Motivated by the investigations of Carmichael numbers in the last hundred years, here we establish several related results, notions, examples and computatinoal searches for weak Carmichael numbers and numbers closely related to weak Carmichael numbers. Furthermore, using the software `Mathematica 8`, we present the table containing all non-prime powers weak Carmichael numbers less than $2\times 10^6$.

Motivated by heuristic arguments, our computations and some old conjectures and results for Carmichael numbers, we propose several conjectures for weak Carmichael numbers and for some other classes of Carmichael like numbers.

Finally, we consider weak Carmichael numbers in light of Fermat primality test. We believe that it can be of interest to involve certain particular classes of weak Carmichael numbers in some problems concerning Fermat-like primality tests and the generalized Riemann hypothesis.

## 1. Carmichael numbers, Lehmer numbers and Giuga numbers

**1.1. Lehmer numbers, Carmichael numbers and the main result.** *Lehmer's totient problem* asks about the existence of a composite number such that $\varphi(n)\mid(n-1)$ [48], where $\varphi(n)$ is the *Euler totient function* defined as the number of positive integers less than $n$ which are relatively prime to $n$. These numbers are sometimes reffered to as *Lehmer numbers*. In 1932 D.H. Lehmer

2010 *Mathematics Subject Classification.* Primary 05A19; Secondary 11A51, 05A10, 11A07, 11A15, 11A25, 11A41, 11A05, 11B50.

*Keywords and phrases.* Carmichael number, Lehmer number, Giuga's conjecture, weak Carmichael number, Carmichael function $\lambda(n)$, super Carmichael number, $k$-Lehmer number, Fermat primality test.

[48] showed that every Lehmer number $n$ must be odd and square-free, and that the number of distinct prime factors of $n$ must be greater than 6. However, no Lehmer numbers are known up to date, and computations by Pinch [61] show that any examples must be greater than $10^{30}$. In 1977 Pomerance [64] showed that the number of Lehmer numbers $n \leq x$ is $O(x^{1/2}(\log x)^{3/4})$. In 2011 this bound is improved by Luca and Pomerance [50] to $O(x^{1/2}(\log x)^{1/2+o(1)})$.

Carmichael numbers are quite famous among specialists in number theory, as they are quite rare and very hard to test. *Fermat little theorem* says that if $p$ is a prime and the integer $a$ is not a multiple of $p$, then $a^{p-1} \equiv 1 (\bmod p)$. However, there are positive integers $n$ that are composite but still satisfy the congruence $a^{n-1} \equiv 1 (\bmod n)$ for all $a$ coprime to $n$. Such "false primes" are called *Carmichael numbers* in honour of R.D. Carmichael, who demonstrated their existence in 1912 [18]. A Carmichael number $n$ is a composite integer that is a base-$a$ *Fermat-pseudoprime* for all $a$ with $\gcd(a, n) = 1$. These numbers present a major problem for Fermat-like primality tests. In [34] A. Granville wrote: "*Carmichael numbers are nuisance, masquerading as primes like this, though computationally they only appear rarely. Unfortunately it was recently proved that there are infinitely many of them and that when we go out far enough they are not so rare as it first appears.*"

It is easy to see that every Carmichael number is odd, namely, if $n \geq 4$ is even, then $(n-1)^{n-1} \equiv (-1)^{n-1} = -1 \not\equiv -1 (\mathrm{mod} n)$. In 1899 A. Korselt [47] gave a complete characterization of Carmichael numbers which is often rely on the following equivalent definition.

**Definition 1.1** (Korselt's criterion, 1899)**.** A composite odd positive integer $n$ is a Carmichael number if $n$ is squarefree, and $p - 1 \mid n - 1$ for every prime $p$ dividing $n$.

Korselt did not find any Carmichael numbers, however. The smallest Carmichael number, $561 (= 3 \times 11 \times 17)$, was found by Carmichael in 1910 [17]. Carmichael also gave a new characterization of these numbers as those composite $n$ which satisfy $\lambda(n) \mid n - 1$, where $\lambda(n)$, *Carmichael lambda function*, denotes the size of the largest cyclic subgroup of the group $(\mathbb{Z}/n\mathbb{Z})^*$ of all reduced residues modulo $n$. In other words, $\lambda(n)$ is the smallest positive integer $m$ such that $a^m \equiv 1 (\bmod n)$ for all for all $a$ coprime to $n$ (Sloane's sequence A002322). Since $\lambda(n) \mid \varphi(n)$ for every positive integer $n$, every Lehmer number would also be a Carmichael number. Recall that various upper bound and lower bounds for $\lambda(n)$ have been obtained in [28]. It is easily deduced from Korselt's criterion that every Carmichael number is a product of at least three distinct primes (see e.g., [35]). It was unsolved problem for many years whether there are infinitely many Carmichael numbers. The question was resolved in 1994 by Alford, Granville and Pomerance [1] who proved, not only that the answer is yes, but that there are more than $x^{2/7}$ Carmichael numbers up to $x$, once $x$ is sufficiently large. In 2005 G. Harman [42] has improved the constant

2/7 to 0.33 (for a more general result see [43, Theorem 1.2]). However, there are a very wide gap between these estimates and the known upper bounds for $C(x)$. Related upper bounds and the counting function for the Carmichael numbers were studied in 1956 by P. Erdős [26], in 1980 by C. Pomerance, J.L. Selfridge and Samuel S. Wagstaff [67] and in 1989 by C. Pomerance [66]. In the same paper Erdős proposed a popular method for the construction of Carmichael numbers (cf. [81] and for a recent application of this construction see [35] and [49]). Some other algorihms for constructing Carmichael numbers can be found in [2] and [49] where are constructed Carmichael numbers with millions of components. Recall also that in 1939, Chernick [19] gave a simple method to obtain Carmichael numbers with three prime factors considering the products of the form $(6m+1)(12m+1)(18m+1)$ with $m \geq 1$. Notice also that the number of Carmichael numbers less than $10^n$ is given in [72] as the Sloane's sequence A055553.

Quite recently, T. Wright [80] proved that for every pair of coprime positive integers $a$ and $d$ there are infinitely many Carmichael numbers $m$ such that $m \equiv a (\operatorname{mod} d)$.

*Remark* **1.2.** Quite recently, J.M. Grau and A.M. Oller-Marcén [37, Definition 1] weakened Lehmer property by introducing the concept of $k$-Lehmer numbers. For given positive integer $k$, a *$k$-Lehmer number* is a composite integer $n$ such that $\varphi(n) \mid (n-1)^k$. It is easy to see that every *$k$-Lehmer number* must be square-free. Hence, if we denote by $L_k$ the set that each *$k$-Lehmer number*

$$L_k := \{n \in \mathbb{N} : \varphi(n) \mid (n-1)^k\},$$

then $k$-Lehmer numbers are the composite elements of $L_k$. Then $L_k \subseteq L_{k+1}$ for each $k \in \mathbb{N}$, and define

$$L_\infty := \bigcup_{k=1}^{\infty} L_k.$$

Then it can be easily shown that [37, Proposition 3]

$$L_\infty := \{n \in \mathbb{N} : \operatorname{rad}(\varphi(n)) \mid (n-1)\}.$$

This immediately shows that [37, Proposition 6] if $n$ is a Carmichael number, then $n$ also belongs to the set $L_\infty$. This leads to the following characterization of Carmichael numbers which slightly modifies Korselt's criterion.

**Proposition 1.3.** ([37, Proposition 6]) *A composite number $n$ is a Carmichael number if and only if* $\operatorname{rad}(\varphi(n)) \mid n-1$ *and* $p-1 \mid n-1$ *for every prime divisor $p$ of $n$.*

Obviously, the composite elements of $L_1$ are precisely the Lehmer numbers and the Lehmer property asks whether $L_1$ contains composite numbers or not. Nevertheless, for all $k > 1$, $L_k$ always contains composite elements (cf. Sloane's sequence A173703 in OEIS [72] which presents $L_2$). For further radically weaking the Lehmer and Carmichael conditions see [55].

*Remark* **1.4.** Carmichael numbers can be generalized using concepts of abstract algebra. Namely, in 2000 Everet W. Howe [29] defined a Carmichael number of order $m$ to be a composite integer $n$ such that $n$th power raising defines an endomorphism of every $\mathbb{Z}/n\mathbb{Z}$-algebra that can be generated as a $\mathbb{Z}/n\mathbb{Z}$-module by $m$ elements. The author gave a simple criterion to determine whether a number is a Carmichael number of order $m$. In 2008 G.A. Steele [74] generalized Carmichael numbers to ideals in number rings and proved a generalization of Korselt's criterion for these Carmichael ideals.

Here, as always in the sequel, $\gcd(k,n)$ denotes the *greatest common divisor* of $k$ and $n$, and $\sum_{\substack{\gcd(k,n)=1\\ k\in\mathcal{P}}}\cdot$ denotes the sum ranging over all integers $k$ satisfying the prperty $\mathcal{P}$ and the condition $\gcd(k,n)=1$.

Studying some variations on the "theme of Giuga", in 1995 J.M. Borwein and E. Wong [15] established the following result.

**Theorem 1.5.** ([15, Corollary 8]) *A positive integer $n\ge 2$ satisfies the congruence*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}\equiv \varphi(n)\pmod n \tag{1.1}$$

*if and only if $p-1\mid n-1$ for every prime divisor $p$ of $n$.*

*Remark* **1.6.** Theorem 1.5 was proved in [15] as a particular case of Theorem 11 in [15]. In the proof of this theorem the authors deal with congruences for the sum (1.1) modulo prime powers dividing $n$. In particular, in this proof it was used the *Chinese remainder theorem* to factor the sum (1.1) modulo $n$ into product of $s$ similar "restricted sums", where $s$ is a number of distinct prime factors of $n$. In Section 4 we give another proof of Theorem 1.5 (this is in fact proof of Theorem 2.4). Our proof is based on some congruential properties of sums of powers $\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}$ (Lemmas 4.1–4.7) and Carlitz-von Staudt's result [16] for determining $S_{2k}(m)(\bmod\, m)$ (Lemma 4.8).

A direct consequence of Theorem 1.5 is the following simple characterization of Carmichael numbers.

**Corollary 1.7.** (Corollary 2.8). *A composite positive integer $n$ is a Carmichael number if and only if the following conditions are satisfied.*

(*i*) *$n$ is square-free and*

(*ii*) $\displaystyle\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}\equiv \varphi(n)\pmod n$.

In this paper we mainly investigate arithmetic properties of composite positive integers satisfying the congruence (1.1). Such numbers are called weak Carmichael numbers. Motivated by the investigations of Carmichael numbers in the last hundred years, here we establish several related results, notions, examples and computatioal searches for weak Carmichael numbers and numbers closely related to weak Carmichael numbers.

1.2. **Bernoulli's formula for the sum of powers and von Staudt-Clausen's theorem.** The sum of powers of integers $\sum_{i=1}^n i^k$ is a well-studied problem in mathematics (see e.g., [11], [69]). Finding formulas for these sums has interested mathematicians for more than 300 years since the time of James Bernoulli (1665-1705). These lead to numerous recurrence relations. The first such well known recurrence relation was established by B. Pascal [60]. A related new reccurrence relation is quite recently established in [54, Corollary 1.9]. For a nice account of sums of powers see [24]. For simplicity, here as often in the sequel, for all integers $k\ge 1$ and $n\ge 2$ we denote

$$S_k(n):=\sum_{i=1}^{n-1} i^k = 1^k+2^k+3^k+\cdots+(n-1)^k.$$

The study of these sums led Jakob Bernoulli [10] to develop numbers later named in his honor. Namely, the celebrated *Bernoulli's formula* (sometimes called *Faulhaber's formula*) ([30] and [**?**]) gives the sum $S_k(n)$ explicitly as (see e.g., [33] or [8])

$$S_k(n)=\frac{1}{k+1}\sum_{i=0}^{k}\binom{k+1}{i} n^{k+1-i}B_i \tag{1.2}$$

where $B_i$ $(i=0,1,2,\ldots)$ are *Bernoulli numbers* defined by the generating function

$$\sum_{i=0}^{\infty} B_i\frac{x^i}{i!}=\frac{x}{e^x-1}.$$

It is easy to find the values $B_0=1$, $B_1=-\frac{1}{2}$, $B_2=\frac{1}{6}$, $B_4=-\frac{1}{30}$, and $B_i=0$ for odd $i\ge 3$. Furthermore, $(-1)^{i-1}B_{2i}>0$ for all $i\ge 1$. Recall that several identities involving Bernoulli numbers and Bernoulli polynomials can be found in [59] and [76].

The *von Staudt-Clausen's theorem* is a result determining the fractional part of Bernoulli numbers, found in 1840 independently by K. von Staudt ([73]; see also [41, Theorem 118]) and T. Clausen [20]).

**Theorem 1.8.** (von Staudt-Clausen's theorem). *The denominator of Bernoulli number $B_{2n}$ with $n=1,2,\ldots$ is the product of all primes $p$ such that $p-1$ divides $2n$.*

*Remark* **1.9.** In literature, von Staudt-Clausen's theorem is often formulated as:

$$B_{2n}+\sum_{\substack{p-1\mid 2n\\ p \text{ prime}}}\frac{1}{p}\quad \text{is an integer for each } n=1,2,\ldots,$$

or equivalently (see e.g., [75, page 153]):

$$pB_{2n} \equiv \begin{cases} 0 \pmod p & \text{if } p-1 \nmid 2n \\ -1 \pmod p & \text{if } p-1 \mid 2n, \end{cases}$$

where $p$ is a prime and $k$ a positive integer.

We also point out that in the proof of Theorem 2.4 we use a particular case of a Carlitz-von Staudt's result (see Remark 1.6) which can be easily deduced from the above form of von Staudt-Clausen's theorem.

1.3. **Giuga's conjecture and Giuga numbers.** Notice that if $n$ is any prime, then by Fermat's little theorem, $S_{n-1}(n) \equiv -1 (\bmod\, n)$. In 1950 G. Giuga [32] proposed that the converse is also true via the following conjecture.

**Conjecture 1.10** (Giuga's conjecture)**.** *A positive integer $n \geq 2$ is a prime if and only if*

$$S_{n-1}(n) := \sum_{i=1}^{n-1} i^{n-1} \equiv -1 \pmod{n}. \tag{1.3}$$

A counterexample to *Giuga's conjecture* is called a *Giuga number.* It is easy to show that $S_{n-1}(n) \equiv -1 \,(\bmod\, n)$ if and only if for each prime divisor $p$ of $n$, $(p-1) \mid (n/p-1)$ and $p \mid (n/p-1)$ (see [32], [13, Theorem 1] or [68, p. 22]). Observe that both these conditions are equivalent to the condition that $p^2(p-1) \mid p(n-1)$. Therefore, any Giuga number must be squarefree. Giuga [32] showed that there are no exceptions to the conjecture up to $10^{1000}$. In 1985 E. Bedocchi [9] improved this bound to $n > 10^{1700}$. In 1996 D. Borwein, J.M. Borwein, P.B. Borwein and R. Girgensohn [13] raised the bound to $n > 10^{13887}$. In 2011 F. Luca, C. Pomerance and I. Shparlinski [51] proved that for any real number $x$, the number of counterexamples to Giuga's conjecture $G(x) := \#\{n < x : n \text{ is composite and } S_{n-1}(n) \equiv -1 \,(\bmod\, n)\}$ satisfies the estimate $G(x) = O(\sqrt{x}/(\log x)^2)$ as $x \to \infty$ improving slightly on a previous result by V. Tipu [82]. Quite recently, J.M. Borwein, M. Skerritt and C. Maitland [14, Theorem 2.2] reported that any counterexample to Giuga's primality conjecture is an odd square-free integer with at least 4771 prime factors and so must exceed $10^{19907}$.

Let $\varphi(n)$ be the *Euler totient function.*

**Definition 1.11.** A positive composite integer $n$ is said to be a *Giuga number* if

$$\sum_{k=1}^{n-1} k^{\varphi(n)} \equiv -1 \pmod{n}. \tag{1.4}$$

This definition was given by Giuga [32]. However, it is known (e.g., see [13, Theorem 1]) that a positive composite integer $n$ is a *Giuga number* if and only if $p^2(p-1)$ divides $n-p$ for every prime divisor $p$ of $n$. Moreover, it is easy to see that only square-free integers can be Giuga numbers. For more information about Giuga numbers see D. Borwein et al. [13], J.M. Borwein and E. Wong [15], and E. Wong [79, Chapter 2].

A *weak Giuga number* is a composite number $n$ for which the sum

$$-\frac{1}{n}+\sum_{\substack{p\mid n\\ p\text{ prime}}}\frac{1}{p}$$

is an integer. It is known that each Giuga number is a weak Giuga number and that $n$ is a weak Giuga number if and only if $p^2 \mid n-p$ for every prime divisor $p$ of $n$ (see [13]). Up to date only thirteen weak Giuga numbers are known and all these numbers are even. The first few Giuga numbers are $30, 858, 1722, 66198, 2214408306, 24423128562, 432749205173838$ (see sequence A007850 in [72]).

Independently, in 1990 T. Agoh (published in 1995 [4]; see also [15] and Sloane's sequence A046094 in [72]) proposed the following conjecture.

**Conjecture 1.12.** (Agoh's conjecture). *A positive integer $n\ge 2$ is a prime if and only if $nB_{n-1}\equiv -1 \pmod n$.*

*Remark* **1.13.** Notice that the denominator of the number $nB_{n-1}$ can be greater than 1, but since by *von Staudt-Clausen's theorem* (Theorem 1.8), the denominator of any Bernoulli number $B_{2k}$ is squarefree, it follows that the denominator of $nB_{n-1}$ is invertible modulo $n$. In 1996 it was reported by T. Agoh [13] that his conjecture is equivalent to Giuga's conjecture, hence the name Giuga-Agoh's conjecture found in the litterature. Therefore,

**Proposition 1.14.** *Giuga's conjecture and Agoh's conjecture are equivalent.*

It was pointed out in [13] that this can be seen from the Bernoulli formula (1.2) after some analysis involving von Staudt-Clausen's theorem. The equivalence of both conjectures is in details proved in 2002 by B.C. Kellner [45, Satz 3.1.3, Section 3.1, p. 97] (also see [46, Theorem 2.3]). In a recent manuscript [53, Subsection 2.1] the author of this article proposed several Giuga-Agoh's-like conjectures.

Notice that von Staudt-Clausen's theorem allows one to give the following equivalent reformulation of Korselt's criterion involving the *Bernoulii number* $B_{n-1}$ is (see e.g., [67, Section 2, Remarks after Proposition 2], [78]).

**Definition 1.15.** An odd composite positive integer $n$ is a Carmichael number if and only if $n$ is squarefree and $n$ divides the denominator of the Bernoulli number $B_{n-1}$.

We present the following relationship between Giuga's conjecture and Carmichael numbers.

**Proposition 1.16.** (see e.g., [13, Theorem] or [36, Corollary 4]) *A positive integer $n$ is a counterexample to Giuga's conjecture if and only if it is both a*

*Carmichael and a Giuga number. In other words, a positive integer $n$ satisfies the congruence*

$$\sum_{i=1}^{n-1} i^{n-1} \equiv -1 \pmod{n} \tag{1.5}$$

*if and only if is $n$ is both a Carmichael and a Giuga number.*

In 2011 J.M. Grau and A.M. Oller-Marcén [36] established a new approach to Giuga's conjecture as follows.

**Proposition 1.17.** ([36, Corollary 3]) *If a positive integer $n$ is a counterexample to Giuga's conjecture, then for each positive integer $k$*

$$\sum_{i=1}^{n-1} i^{k(n-1)} \equiv -1 \pmod{n}. \tag{1.6}$$

*Remark* **1.18.** Proposition 1.17 leads to the generalization of Giuga's ideas in the following way [36, Section 3]: Do there exist integers $k$ such that the congruence (1.6) is satisfied by some composite integer $n$? Several open problems concerning Giuga's conjecture can be found in J.M. Borwein and E. Wong [15, 8, E Open Problems].

*Remark* **1.19.** Quite recently, J.M. Grau and A.M. Oller-Marcén [38, Theorem 1] characterized, in terms of the prime divisors of $n$, the pairs $(k, n)$ for which $n$ divides $S_k(n)$. More generally, in [38] it is investigated $S_{f(n)}(b) (\mathrm{mod}\, n)$ for different arithmetic functions $f$.

## 2. Weak Carmichael numbers

2.1. **Sum of powers of coprime residues of $n$.** The *Euler totient function* $\varphi(n)$ is defined as equal to the number of positive integers less than $n$ which are relatively prime to $n$. Each of these $\varphi(n)$ integers is called a *totative* (or "*totitive*") of $n$ (see [69, Section 3.4, p. 242] where this notion is attributed to J.J. Sylvester). Let $t(n)$ denote the set of all totatives of $n$, i.e., $t(n) = \{j \in \mathbb{N} : 1 \leq j < n, \gcd(j, n) = 1\}$. Given any fixed nonnegative integer $k$, in 1850 A. Thacker (see [69, p. 242]) introduced the function $\varphi_k(n)$ defined as

$$\varphi_k(n) = \sum_{t \in t(n)} t^k \tag{2.1}$$

where the summation ranges over all totatives $t$ of $n$ (in addition, we define $\varphi_k(1) = 0$ for all $k$). Notice that $\varphi_0(n) = \varphi(n)$ and $\varphi_k(n) = S_k(n)$ holds if and only if $n = 1$ or $n$ is a prime number.

The following recurrence relation for the functions $\varphi_k(n)$ was established in 1857 by J. Liouville (cf. [69, p. 243]):

$$\sum_{d\mid n}\binom{n}{d}^k\varphi_k(d)=S_k(n+1):=1^k+2^k+\cdots+n^k$$

which for $k=0$ reduces to *Gauss' formula* $\sum_{d\mid n}\varphi(d)=n$. Furthermore, in 1985 P.S. Bruckman [12] established an explicit Bernoulli's-like formula for the *Dirichlet series* of $\varphi_k(n)$ defined as $f_k(s)=\sum_{k=1}^{\infty}\varphi_k(n)/n^s$ (there $\varphi_k(n)$ is called generalized Euler function). Quite recently, in [54, Corollary 1.9] the author of this article proved for all $k\geq 1$ and $n\geq 2$ the following recurrence relation involving the functions $\varphi_k(n)$.

$$\sum_{i=0}^{2k-1}(-1)^i\binom{2k-1}{i}2^{2k-1-i}n^i\varphi_{2k-1-i}(n)=0.$$

2.2. **Weak Carmichael numbers.** Inspired by the previous definitions, results, and considerations we give the following definition.

**Definition 2.1.** A composite positive integer $n$ is said to be a *weak Carmichael number* if

$$\sum_{\substack{\gcd(k,n)=1\\ 1\leq k\leq n-1}}k^{n-1}\equiv\varphi(n)\pmod{n},\tag{2.2}$$

where the summation ranges over all $k$ such that $1\leq k\leq n-1$ and $\gcd(k,n)=1$.

From the above definition we see that each Carmichael number is also a weak Carmichael number; hence the name. This together with the mentioned result that the set of Carmichael numbers is infinite implies the following fact.

**Proposition 2.2.** *There are infinitely many weak Carmichael numbers.*

The following characterization of weak Carmichael numbers may be useful for computational purposes.

**Proposition 2.3.** *Every weak Carmichael number is odd. Furthermore, an odd composite positive integer $n$ is a weak Carmichael number if and only if*

$$2\sum_{i=1}^{\varphi(n)/2}r_i^{n-1}\equiv\varphi(n)\pmod{n},\tag{2.3}$$

*where $r_1<r_2<\cdots<r_{\varphi(n)}$ are all reduced residues modulo $n$.*

As noticed above, the results, definitions and conjectures in this article are mainly based on Theorem 1.5 (a result of Borwein and Wong [15, Corollary 8]) which in terms of weak Carmichael numbers can be reformulated as the following Korselt's type criterion for characterizing weak Carmichael numbers.

**Theorem 2.4.** *Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be a composite integer, where $p_1, p_2, \ldots, p_s$ are distinct odd primes and $e_1, e_2, \ldots, e_s$ are positive integers. Then $n$ is a weak Carmichael number if and only $p_i - 1 \mid n - 1$ for every $i = 1, 2, \ldots, s$.*

*Remark* **2.5.** Any integer greater than 1 and satisfying the congruence (2.2) is called in [15]) a *generalized Carmichael number*. Therefore, by Definition 2.1, the set of all generalized Carmichael numbers is a union of the set of weak Carmichael numbers and the set of all primes. The following result of E. Wong ([79, p. 17, Subsection 2.5.3] where weak Carmichael numbers are called *pseudo-Carmichael numbers*) is immediate by Euler totient theorem and it establish the fact that there are numerous weak Carmichael numbers that are not prime powers nor Carmichael numbers.

Here, as always in the sequel, lcm$(\cdot)$ will denote the *least common multiple function*.

**Proposition 2.6.** *Let $p_1, p_2, \ldots, p_s$ be distinct primes such that $p_i - 1 \not\equiv 0 (\bmod\ p_j)$ for each pair of indices $i, j$ with $1 \le i \ne j \le s$. For all $j = 1, 2, \ldots, s$ put $e_i = \mathrm{lcm}_{\substack{1\le j\le s\\ j\ne i}} \varphi(p_j)$. Then any number of the form $p_1^{k_1 e_1} p_2^{k_2 e_2} \cdots p_s^{k_s e_s}$ with $k_i \ge 1$, is a weak Carmichael number. Conversely, if $n$ is a weak Carmichael number with prime factors $p_1, p_2, \ldots, p_s$, then $p_i - 1 \not\equiv 0 (\bmod\ p_j)$ for each pair of indices $i, j$ with $1 \le i \ne j \le s$.*

**Definition 2.7.** Let $n \ge 3$ be any odd positive integer with a prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$. Then the function $c_w(n)$ of $n$ is defined as

$$c_w(n) = \mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_s - 1). \tag{2.4}$$

From the above definition, the definition of Carmichael function $\lambda(n)$ and its property that $p - 1 = \lambda(p) \mid \lambda(p^e)$ for any odd prime $p$ and $e \ge 2$, we immediately obtain the following result.

**Proposition 2.8.** *For each odd positive integer $n$, $c_w(n) \mid \lambda(n)$. Therefore, for such a $n$ we have $c_w(n) \le \lambda(n)$.*

Using Euler totient theorem, Theorem 2.4 easily yields the following result which gives a possibility for the construction of weak Carmichael numbers via Carmichael numbers.

**Proposition 2.9.** *Let $n = p_1 p_2 \cdots p_s$ be an arbitrary Carmichael number. For any fixed $i \in \{1, 2, \ldots, s\}$ let $d_i$ be a smallest positive divisor of $\varphi(c_w(n/p_i))$ with $c_w(n/p_i) := \prod_{\substack{1\le j\le l\\ j\ne i}} (p_j - 1)$, such that $p_i^{d_i} \equiv 1 (\bmod\ c_w(n/p_i))$. Then $np_i^{md_i}$ is a weak Carmichael number for every positive integer $m$.*

**Examples 2.10.** Consider the smallest Carmichael number $561 = 3 \cdot 11 \cdot 17$. Then $c_w(561/3) = \mathrm{lcm}(10, 16) = 80$, $c_w(561/11) = \mathrm{lcm}(2, 16) = 16$ and $c_w(561/17) = \mathrm{lcm}(2, 10) = 10$, and $d_1 = 4$, $d_2 = 8$, and $d_3 = 4$ are smallest integers for which $3^{d_1} \equiv 1 (\bmod 80)$, $11^{d_2} \equiv 1 (\bmod 16)$ and $17^{d_3} \equiv 1 (\bmod 10)$, respectively. This by Proposition 2.9 shows that $3^{4m+1}\cdot 11\cdot 17$, $3\cdot 11^{8m+1}\cdot 17$ and $3\cdot 11\cdot 17^{4m+1}$ are weak Carmichael numbers for every positive integer $m$ (the smallest such a number $3^5\cdot 11\cdot 17=45441$ occurs in Table 1 as a smallest weak Carmichael number described in Proposition 2.9). Similarly, regarding related values $d_1$ for a smallest prime divisor of the next four Carmichael numbers $1105, 1729, 2465$ and $2821$ (see Table 1), we respectively obtain the following associated sequences for weak Carmichael numbers: $5^{4m+1}\cdot 13\cdot 17$, $7^{6m+1}\cdot 13\cdot 19$, $5^{12m+1}\cdot 17\cdot 29$ and $7^{4m+1}\cdot 13\cdot 31$ with $m\ge 1$.

*Remark* **2.11.** As noticed above, in 1939, Chernick [19] gave a simple method to obtain Carmichael numbers with three prime factors. The distribution of primes with three prime factors has been studied in 1997 by R. Balasubramanian and S.V. Nagaraj [5], who showed that the number of such Carmichael numbers up to $x$ is at most $O(x^{5/(14+o(1))})$. If $n=pqr$ is a Carmichael number then we have $p-1=da$, $q-1=db$ and $r-1=dc$ where $a,b$ and $c$ are coprime and $dabc\mid n-1$. The Chernick form $n=pqr=(6m+1)(12m+1)(18m+1)$ is a special case of the form

$$n=pqr=(am+1)(bm+1)(cm+1)$$

with $a<b<c$, where $a,b$ and $c$ are relatively prime in pairs. Namely, the case $a=1$, $b=2$, $c=3$, leading to $d\equiv 0(\bmod 6)$. We see that most values $(amb,c)$ will lead to a possible congruence for $d$ modulo $abc$, whose smallest solution may be expected to be of the same order as $abc$. As shown in [19, the congruence (5)] in Ore's book [58, Ch. 14], $m=m_0+tabc$ with $t=1,2,3,\ldots$, where $m_0$ is the solution to the linear congruence

$$m_0(ab+ac+bc)\equiv -(a+b+c)\pmod{abc}. \tag{2.5}$$

Thus, for given $a,b,c$ it is easy to find all allowable values of $m$. All that remains is to test the three components for primality for each allowable $m$. In this way a "family" of Carmichael numbers is found corresponding to triplets $(a,b,c)$. In [22, Section 5, Table 2] H. Dubner reported that the counts of $(1,a,b)$ are about 64.4% of the corresponding Carmichael numbers with three prime factors less than $10^n$ for a wide range of $n$. Moreover, the counts of $(1,a,b)$ are about 2.2% of such Carmichael numbers.

However, it is not yet known whether there are infinitely many Carmichael numbers of Chernick form, although this would folow from the more general conjecture of Dickson [21]. In 2002 H. Dubner [22] tabulated the counts of Carmichael numbers of Chernick form up to $10^n$ for each $n<42$. Up to $10^{12}$ and $10^{18}$ there are respectively 1000 and 35586 with three prime factors (see [22, Table 2]). Between these 1000 (resp. 35585) Carmichael numbers, 25 (resp. 783) numbers correspond to the Chernick form with related triplets $(a,b,c)=(1,2,3)$ (see [22, Table 1]).

**Examples 2.12.** Here we present a simple way for constructing weak Carmichael numbers with four prime factors using the Chernick form of product $(6m+$

$1)(12m+1)(18m+1)$. Consider the extended Chernick product in the form

$$C(m;d,l) := (6m+1)(12m+1)(18m+1)\left(\frac{36m}{d}+1\right)^l, \tag{2.6}$$

with $d \mid 36m$ and some $l \geq 1$. Then under the assumptions that $p = 6m+1, q = 12m+1$ and $r = 18m+1$ are primes, a routine calculation shows that $C(m;d,l)$ is a weak Carmichael numbers with four prime factors if and only if $w(m,d) := 36m/d+1$ is a prime different from $p$, $q$ and $r$ such that $(36m/d+1)^l \equiv 1(\bmod 6m)$. In particular, for a given $m$, possible values $d = 1,4,9,12,18,36$ respectively give the following values for $s$: $36m+1, 9m+1, 4m+1, 2m+1, m+1$. For example, Chernick [19, p. 271] observed that the integers $C(m) := (6m+1)(12m+1)(18m+1)$ are Carmichael numbers for $m \in \{1,6,35,45,51,55,56,100,121\}$. For a fixed $m \geq 1$, denote by $W_m$ the set of all odd primes in the set $\{36m/d+1 : d \mid 36\}$. Then $W_1 = \{3,5,7\}$, $W_6 = \{7,13,19,37,217\}$, $W_{35} = \{7,13,19\}$, $W_{45} = \{71\}$, $W_{51} = \{103\}$, $W_{55} = \Phi$, $W_{56} = \{13,2017\}$, $W_{100} = \{401\}$ and $W_{121} = \{4357\}$. Then every $w \in W_m$ for some $m \in \{1,6,35,45,51,55,56,100,121\}$ arise a set of weak Carmichael numbers of the form $C(m;d,l)$ given by (2.6), where $l$ must satisfy the congruence $w^l \equiv 1(\bmod 6m)$. For example, assuming $w = 13 \in W_{35}$, we arrived to the set of weak Carmichael numbers of the form $211 \cdot 421 \cdot 631 \cdot 13^l$ with $l$ such that $13^l \equiv 1(\bmod 210)$. Using the fact that $\varphi(210) = 48$, we can easily verify that $l_0 = 4$ is the smallest value of $l$ satisfying the previous congruence. Consequently, each integer of the form $211 \cdot 421 \cdot 631 \cdot 13^{4u}$ with $u = 1,2,\ldots$ is a weak Carmichael number.

**Definition 2.13.** A weak Carmichael number which can be obtained from certain Carmichael number in the manner described in Proposition 2.9 is called a *Carmichael like number*.

*Remark* **2.14.** From Table 1 we see that there exist many weak Carmichael numbers of the form $n = p_1 \cdots p_{k-1}p_k^f$ with some $k \in \{3,4\}$ and $f \geq 2$, which are not Carmichael numbers. For example, from Table 1 we see that $8625 = 3 \cdot 5^3 \cdot 23$ is the smallest such number, and the smallest such numbers with four distinct prime factors is $54145 = 5 \cdot 7^2 \cdot 13 \cdot 17$.

In terms of the function $c_w(n)$, Theorem 2.4 can be reformulated as follows.

**Theorem 2.4'.** *Let $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ be a composite integer, where $p_1, p_2, \ldots, p_s$ are odd distinct primes and $e_1, e_2, \ldots, e_s$ are positive integers. Then $n$ is a weak Carmichael number if and only $c_w(n) \mid n-1$.*

As an immediate consequence of Theorem 2.4, we establish a surprising result that summing all $\varphi(n)$ congruences $a^{n-1} \equiv 1(\bmod n)$ over $1 \leq a \leq n-1$ with $\gcd(a,n) = 1$, we obtain the congruence which characterizes Carmichael numbers under the assumption that $n$ is a square-free integer.

**Theorem 2.15.** *Let $n > 1$ be a square-free positive integer. Then $n$ is a Carmichael number if and only if*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi(n) \pmod{n}, \tag{2.7}$$

Using the well known fact that every Carmichael number is square-free, as a consequence of Theorem 2.15, we obtain the following simple characterization of Carmichael numbers.

**Corollary 2.16.** *A composite positive integer $n$ is a Carmichael number if and only if the following conditions are satisfied.*
*(i) $n$ is square-free and*
*(ii)* $\displaystyle\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi(n) \pmod{n}$.

Recall that the *Möbius $\mu$-function* is defined so that $\mu(1) = 1$, $\mu(n) = (-1)^s$ if $n$ is a product of $s$ distinct primes, and $\mu(n) = 0$ if $n$ is divisible by the square of a prime. Then the following consequence of Theorem 2.4 gives a characterization of weak Carmichael numbers that are not Carmichael numbers.

**Corollary 2.17.** *An integer $n > 1$ is a weak Carmichael number which is not a Carmichael number if and only if*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi(n) + \mu(n) \pmod{n}.$$

Theorem 2.4 immediately gives the following result which was also observed in [15], and also directly proved in [38, Lemma 1].

**Proposition 2.18.** *Every power $p^e$ of any odd prime $p$ with $e \ge 2$ is a weak Carmichael number.*

**Corollary 2.19.** *If $n$ is a weak Carmichael number, then every power $n^e$ of $n$ with $e = 2, 3, \ldots$ is also a weak Carmichael number. In particular, such a power of any Carmichael number is also a weak Carmichael number.*

Theorem 2.4 and the well known fact that every Carmichael number has at least three distinct prime factors imply the following result.

**Corollary 2.20.** *Let $n = pq$ be a product of distinct odd primes $p$ and $q$. Then $n$ is not a weak Carmichael number.*

*Remark* **2.21.** Recall that in Section 3 we give a direct proof of Corollary 2.20.

Proposition 2.18 shows that weak Carmichael numbers appear to be more numerous than the Carmichael numbers, which can be expressed as follows.

**Corollary 2.22.** *Let $C(x)$ and $C_w(x)$ be the numbers of Carmichael numbers and weak Carmichael numbers in the interval $[1, x]$, respectively. Then*

$$\lim_{x\to\infty}(C_w(x) - C(x)) = +\infty.$$

*Remark* **2.23.** Obviously, Corollary 2.17 may be very significant for computational search of Carmichael numbers. Namely, in order to examine whether a given non-square positive integer $n$ is a Carmichael number, it is sufficient to verify only one congruence modulo $n$. However, for related faster compuations may be useful the following charaterization of Carmichael numbers which immediately follows from Corollary 2.17 and the fact that $\varphi(p_1p_2\ldots p_k) = (p_1-1)(p_2-2)\cdots(p_k-1)$.

**Corollary 2.24.** *Let $n = p_1p_2\cdots p_s$ be a composite positive integer, where $p_1, p_2, \ldots, p_s$ are distinct primes. Let $l_i$ be residues of $n-1$ modulo $p_i$ with $i = 1, 2, \ldots, s$. Then $n$ is a Carmichael number if and only if the following $k$ congruences are satified:*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le l-1}} k^{l_i} \equiv -\frac{1}{p_i-1}\prod_{j=1}^{s}(p_j-1) \pmod{p_i}, \quad i = 1, 2, \ldots, s. \tag{2.8}$$

Proposition 2.6 motivates the following definition.

**Definition 2.25.** A weak Carmichael number $n$ is called a *primitive weak Carmichael number* if $n \ne m^f$ for every weak Carmichael numbers $m$ and all integers $f \ge 2$.

*Remark* **2.26.** Clearly, each weak Carmichael number which is not a power of some integer is also a primitive weak Carmichael number. In particular, this is true for all Carmichael numbers. However, there are primitive weak Carmichael numbers which are powers of some integers. For example, Corollary 2.20 implies that every weak Carmichael number of the form $p^2q^2$ is a primitive weak Carmichael number. From Table 1 we read the following perfect squares of product of distinct primes: 225, 1225, 8281 and 14161. We also see from Table 1 that the numbers $2025 = 3^4 \cdot 5^2$, $18225 = 3^6 \cdot 5^2$ are primitive weak Carmichael numbers, but 2025 is not a primitive weak Carmichael number (in view of the fact that its square root 45 is a weak Carmichael number). Table 1 also shows that there are primitive Carmichael numbers which are aquare of non-square integers (for example, $1071225 = (3^2 \cdot 5 \cdot 23)^2$).

Furthermore, in view of Definition 2.25, Proposition 2.18 we have the following result.

**Corollary 2.27.** *If $p$ is an odd prime, then $p^f$ is a primitive weak Carmichael number if and only if $f$ is a prime.*

The facts that there are infinitely many Carmichael numbers and that every Carmichael number is a weak Carmichael number yield the following result.

**Corollary 2.28.** *There are infinitely many primitive weak Carmichael numbers which are not prime powers.*

Applying the congruence (2.2), we find via `Mathematica` 8 the following table of weak Carmichael numbers up to 25000 and their factorizations. In this table Carmichael numbers are written in boldface, while prime powers are written in italic face. The notion of indices of weak Carmichael numbers which are less than 30000, given in Table 2, are described in Subsection 2.6.

**Table 1.** Weak Carmichael numbers up to 25000

| | | | |
|---|---|---|---|
| $9 = 3^2$ | $25 = 5^2$ | $27 = 3^3$ | $45 = 3^2 \cdot 5$ |
| $49 = 7^2$ | $81 = 3^4$ | $121 = 11^2$ | $125 = 5^3$ |
| $169 = 13^2$ | $225 = 3^2 \cdot 5^2$ | $243 = 3^5$ | $289 = 17^2$ |
| $325 = 5^2 \cdot 13$ | $343 = 7^3$ | $361 = 19^2$ | $405 = 3^4 \cdot 5$ |
| $529 = 23^2$ | $\mathbf{561 = 3 \cdot 11 \cdot 17}$ | $625 = 5^4$ | $637 = 7^2 \cdot 13$ |
| $729 = 3^6$ | $841 = 29^2$ | $891 = 3^4 \cdot 11$ | $961 = 31^2$ |
| $\mathbf{1105 = 5 \cdot 13 \cdot 17}$ | $1125 = 3^2 \cdot 5^3$ | $1225 = 5^2 \cdot 7^2$ | $1331 = 11^3$ |
| $1369 = 37^2$ | $1377 = 3^4 \cdot 17$ | $1681 = 41^2$ | $\mathbf{1729 = 7 \cdot 13 \cdot 19}$ |
| $1849 = 43^2$ | $2025 = 3^4 \cdot 5^2$ | $2187 = 3^7$ | $2197 = 13^3$ |
| $2209 = 47^2$ | $2401 = 7^4$ | $\mathbf{2465 = 5 \cdot 17 \cdot 29}$ | $2809 = 53^2$ |
| $\mathbf{2821 = 7 \cdot 13 \cdot 31}$ | $3125 = 5^5$ | $3321 = 3^4 \cdot 41$ | $3481 = 59^2$ |
| $3645 = 3^6 \cdot 5$ | $3721 = 61^2$ | $3751 = 11^2 \cdot 31$ | $3825 = 3^2 \cdot 5^2 \cdot 17$ |
| $4225 = 5^2 \cdot 13^2$ | $4489 = 67^2$ | $4913 = 17^3$ | $4961 = 11^2 \cdot 41$ |
| $5041 = 71^2$ | $5329 = 73^2$ | $5589 = 3^5 \cdot 23$ | $5625 = 3^2 \cdot 5^4$ |
| $6241 = 79^2$ | $6517 = 7^3 \cdot 19$ | $6525 = 3^2 \cdot 5^2 \cdot 29$ | $6561 = 3^8$ |
| $\mathbf{6601 = 7 \cdot 23 \cdot 41}$ | $6859 = 19^3$ | $6889 = 83^2$ | $7381 = 11^2 \cdot 61$ |
| $7921 = 89^2$ | $8125 = 5^4 \cdot 13$ | $8281 = 7^2 \cdot 13^2$ | $8625 = 3 \cdot 5^3 \cdot 23$ |
| $\mathbf{8911 = 7 \cdot 19 \cdot 67}$ | $9409 = 97^2$ | $9801 = 3^4 \cdot 11^2$ | $10125 = 3^4 \cdot 5^3$ |
| $10201 = 101^2$ | $\mathbf{10585 = 5 \cdot 29 \cdot 73}$ | $10609 = 103^2$ | $10625 = 5^4 \cdot 17$ |
| $11449 = 107^2$ | $11881 = 109^2$ | $12025 = 5^2 \cdot 13 \cdot 37$ | $12167 = 23^3$ |
| $12769 = 113^2$ | $13357 = 19^2 \cdot 37$ | $13833 = 3^2 \cdot 29 \cdot 53$ | $14161 = 7^2 \cdot 17^2$ |
| $14641 = 11^4$ | $15625 = 5^6$ | $\mathbf{15841 = 7 \cdot 31 \cdot 73}$ | $15925 = 5^2 \cdot 7^2 \cdot 13$ |
| $16129 = 127^2$ | $16807 = 7^5$ | $17161 = 131^2$ | $18225 = 3^6 \cdot 5^2$ |
| $18769 = 137^2$ | $19321 = 139^2$ | $19683 = 3^9$ | $21141 = 3^6 \cdot 29$ |
| $22201 = 149^2$ | $22801 = 151^2$ | $23409 = 3^2 \cdot 5 \cdot 23^2$ | $23805 = 3^2 \cdot 5 \cdot 23^2$ |
| $24389 = 29^3$ | $24649 = 157^2$ | | |

*Remark* **2.29.** Table 1 shows that there are 102 weak Carmichael numbers less than 25000, and between them there are 9 Carmichael numbers, 57 odd prime powers, and 36 other composite numbers. Recall that in 2006 R.G.E. Pinch [63] reported that there are 1401644 Carmichael numbers up to $10^{18}$ (also see [62] for a search of total 105212 Carmichael numbers up to $10^{15}$). Notice that $1401644 \approx 1.4 \times (10^{18})^{1/3}$.

**Table 2.** Weak Carmichael numbers up to $2 \times 10^6$ that are not prime powers

| | | |
|---|---|---|
| $45_8 = 3^2 \cdot 5$ | $225_8 = 3^2 \cdot 5^2$ | $325_{48} = 5^2 \cdot 13$ |
| $405_8 = 3^4 \cdot 5$ | $\mathbf{561_{320} = 3 \cdot 11 \cdot 17}$ | $637_{72} = 7^2 \cdot 13$ |
| $891_{20} = 3^4 \cdot 11$ | $\mathbf{1105_{768} = 5 \cdot 13 \cdot 17}$ | $1125_8 = 3^2 \cdot 5^3$ |
| $1225_{24} = 5^2 \cdot 7^2$ | $1377_{32} = 3^4 \cdot 17$ | $\mathbf{1729_{1296} = 7 \cdot 13 \cdot 19}$ |
| $\mathit{2025_8 = 3^4 \cdot 5^2}$ | $\mathbf{2465_{1792} = 5 \cdot 17 \cdot 29}$ | $\mathbf{2821_{2160} = 7 \cdot 13 \cdot 31}$ |
| $3321_{80} = 3^4 \cdot 41$ | $3645_8 = 3^6 \cdot 5$ | $3751_{300} = 11^2 \cdot 31$ |
| $3825_{128} = 3^2 \cdot 5^2 \cdot 17$ | $4225_{48} = 5^2 \cdot 13^2$ | $4961_{400} = 11^2 \cdot 41$ |
| $5589_{44} = 3^5 \cdot 23$ | $5625_8 = 3^2 \cdot 5^4$ | $6517_{108} = 7^3 \cdot 19$ |
| $6525_{224} = 3^2 \cdot 5^2 \cdot 29$ | $\mathbf{6601_{5280} = 7 \cdot 23 \cdot 41}$ | $7381_{600} = 11^2 \cdot 61$ |
| $8125_{48} = 5^4 \cdot 13$ | $8281_{72} = 7^2 \cdot 13^2$ | $8625_{176} = 3 \cdot 5^3 \cdot 23$ |
| $\mathbf{8911_{7128} = 7 \cdot 19 \cdot 67}$ | $9801_{20} = 3^4 \cdot 11^2$ | $10125_8 = 3^4 \cdot 5^3$ |
| $\mathbf{10585_{8064} = 5 \cdot 29 \cdot 73}$ | $10625_{64} = 5^4 \cdot 17$ | $12025_{1728} = 5^2 \cdot 13 \cdot 37$ |
| $13357_{648} = 19^2 \cdot 37$ | $13833_{2912} = 3^2 \cdot 29 \cdot 53$ | $14161_{96} = 7^2 \cdot 17^2$ |
| $\mathbf{15841_{12960} = 7 \cdot 31 \cdot 73}$ | $15925_{288} = 5^2 \cdot 7^2 \cdot 13$ | $18225_8 = 3^6 \cdot 5^2$ |
| $21141_{56} = 3^6 \cdot 29$ | $23409_{32} = 3^4 \cdot 17^2$ | $23805_{176} = 3^2 \cdot 5 \cdot 23^2$ |
| $25425_{896} = 3^2 \cdot 5^2 \cdot 113$ | $26353_{1296} = 19^2 \cdot 73$ | $28033_{1536} = 17^2 \cdot 97$ |
| $28125_8 = 3^2 \cdot 5^5$ | $\mathbf{29341_{25920} = 13 \cdot 37 \cdot 61}$ | $30625 = 5^4 \cdot 7^2$ |
| $31213 = 7^4 \cdot 13$ | $32805 = 3^8 \cdot 5$ | $33125 = 5^4 \cdot 53$ |
| $35425 = 5^2 \cdot 13 \cdot 109$ | $35443 = 23^2 \cdot 67$ | $38637 = 3^6 \cdot 53$ |
| $\mathbf{41041 = 7 \cdot 11 \cdot 13 \cdot 41}$ | $41125 = 5^3 \cdot 7 \cdot 47$ | $45325 = 5^2 \cdot 7^2 \cdot 37$ |
| $45441 = 3^5 \cdot 11 \cdot 17$ | $\mathbf{46657 = 13 \cdot 37 \cdot 97}$ | $47081 = 23^2 \cdot 89$ |
| $47125 = 5^3 \cdot 13 \cdot 29$ | $\mathit{50625 = 3^4 \cdot 5^4}$ | $\mathbf{52633 = 7 \cdot 73 \cdot 103}$ |
| $54145 = 5 \cdot 7^2 \cdot 13 \cdot 17$ | $54925 = 5^2 \cdot 13^3$ | $58621 = 31^2 \cdot 61$ |
| $60025 = 5^2 \cdot 7^4$ | $\mathbf{62745 = 3 \cdot 5 \cdot 47 \cdot 89}$ | $\mathbf{63973 = 7 \cdot 13 \cdot 19 \cdot 37}$ |
| $65025 = 3^2 \cdot 5^2 \cdot 17^2$ | $65341 = 19^2 \cdot 181$ | $72171 = 3^8 \cdot 11$ |
| $74431 = 7^4 \cdot 31$ | $\mathbf{75361 = 11 \cdot 13 \cdot 17 \cdot 31}$ | $78625 = 5^3 \cdot 17 \cdot 37$ |
| $81289 = 13^3 \cdot 37$ | $83125 = 5^4 \cdot 7 \cdot 19$ | $89425 = 5^2 \cdot 7^2 \cdot 73$ |
| $91125 = 3^6 \cdot 5^3$ | $94501 = 11^3 \cdot 71$ | $98125 = 5^4 \cdot 157$ |
| $99541 = 13^2 \cdot 19 \cdot 31$ | $99937 = 37^2 \cdot 73$ | $\mathbf{101101 = 7 \cdot 11 \cdot 13 \cdot 101}$ |
| $\mathit{105625 = 5^4 \cdot 13^2}$ | $106641 = 3^2 \cdot 17^2 \cdot 41$ | $107653 = 7^2 \cdot 13^3$ |
| $107811 = 3^4 \cdot 11^3$ | $111537 = 3^8 \cdot 17$ | $\mathbf{115921 = 13 \cdot 37 \cdot 241}$ |
| $116281 = 11^2 \cdot 31^2$ | $117325 = 5^2 \cdot 13 \cdot 19^2$ | $123823 = 7^3 \cdot 19^2$ |
| $\mathbf{126217 = 7 \cdot 13 \cdot 19 \cdot 73}$ | $128547 = 3^5 \cdot 23^2$ | $134113 = 7^3 \cdot 17 \cdot 23$ |
| $136161 = 3^4 \cdot 41^2$ | $140625 = 3^2 \cdot 5^6$ | $142129 = 13^2 \cdot 29^2$ |
| $146461 = 7^4 \cdot 61$ | $\mathbf{162401 = 17 \cdot 41 \cdot 233}$ | $\mathit{164025 = 3^8 \cdot 5^2}$ |
| $\mathbf{172081 = 7 \cdot 13 \cdot 31 \cdot 61}$ | $177331 = 7^3 \cdot 11 \cdot 47$ | $180225 = 3^4 \cdot 5^2 \cdot 89$ |
| $180625 = 5^4 \cdot 17^2$ | $187461 = 3^3 \cdot 53 \cdot 131$ | $\mathbf{188461 = 7 \cdot 13 \cdot 19 \cdot 109}$ |
| $189225 = 3^2 \cdot 5^2 \cdot 29^2$ | $195625 = 5^4 \cdot 313$ | $203125 = 5^6 \cdot 13$ |
| $203401 = 11^2 \cdot 41^2$ | $203841 = 3^2 \cdot 11 \cdot 29 \cdot 71$ | $207025 = 5^2 \cdot 7^2 \cdot 13^2$ |
| $211141 = 7^2 \cdot 31 \cdot 139$ | $231601 = 31^2 \cdot 241$ | $232897 = 7^4 \cdot 97$ |
| $236321 = 29^2 \cdot 281$ | $239701 = 7 \cdot 11^2 \cdot 283$ | $241129 = 7^3 \cdot 19 \cdot 37$ |
| $251505 = 3^7 \cdot 5 \cdot 23$ | $\mathbf{252601 = 41 \cdot 61 \cdot 101}$ | $253125 = 3^4 \cdot 5^5$ |
| $254221 = 11^3 \cdot 191$ | $261625 = 5^3 \cdot 7 \cdot 13 \cdot 23$ | $269001 = 3^8 \cdot 41$ |
| $\mathbf{278545 = 5 \cdot 17 \cdot 29 \cdot 113}$ | $290521 = 7^4 \cdot 11^2$ | $\mathbf{294409 = 37 \cdot 73 \cdot 109}$ |
| $295245 = 3^{10} \cdot 5$ | $306397 = 7^2 \cdot 13^2 \cdot 37$ | $307051 = 47^2 \cdot 139$ |
| $309825 = 3^6 \cdot 5^2 \cdot 17$ | $312481 = 13^2 \cdot 43^2$ | $314721 = 3^2 \cdot 11^2 \cdot 17^2$ |
| $\mathbf{314821 = 13 \cdot 61 \cdot 397}$ | $319345 = 5 \cdot 13 \cdot 17^3$ | $321201 = 3^2 \cdot 89 \cdot 401$ |
| $\mathbf{334153 = 19 \cdot 43 \cdot 409}$ | $338031 = 3^2 \cdot 23^2 \cdot 71$ | $\mathbf{340561 = 13 \cdot 17 \cdot 23 \cdot 67}$ |
| $341341 = 7 \cdot 11^2 \cdot 13 \cdot 31$ | $354061 = 29^2 \cdot 421$ | $362551 = 7^4 \cdot 151$ |
| $378625 = 5^3 \cdot 13 \cdot 233$ | $388125 = 3^3 \cdot 5^4 \cdot 23$ | $397953 = 3^4 \cdot 17^3$ |

**Table 2.** (Continued)

| | | |
|---|---|---|
| $398125 = 5^4 \cdot 7^2 \cdot 13$ | **$399001 = 31 \cdot 61 \cdot 211$** | $401841 = 3^4 \cdot 11^2 \cdot 41$ |
| $405121 = 41^2 \cdot 241$ | *$405769 = 7^4 \cdot 13^2$* | $409825 = 5^2 \cdot 13^2 \cdot 97$ |
| **$410041 = 41 \cdot 73 \cdot 137$** | $441013 = 53^2 \cdot 157$ | $442225 = 5^2 \cdot 7^2 \cdot 19^2$ |
| $444925 = 5^2 \cdot 13 \cdot 37^2$ | **$449065 = 5 \cdot 19 \cdot 29 \cdot 163$** | $450241 = 11^2 \cdot 61^2$ |
| $453125 = 5^6 \cdot 29$ | $453871 = 11^4 \cdot 31$ | $455625 = 3^6 \cdot 5^4$ |
| $462241 = 13 \cdot 31^2 \cdot 37$ | $468391 = 7^2 \cdot 11^2 \cdot 79$ | $472361 = 41^2 \cdot 281$ |
| **$488881 = 37 \cdot 73 \cdot 181$** | $494209 = 19^2 \cdot 37^2$ | $499681 = 7 \cdot 13 \cdot 17^2 \cdot 19$ |
| $501025 = 5^2 \cdot 7^2 \cdot 409$ | $505141 = 7^2 \cdot 13^2 \cdot 61$ | $511525 = 5^2 \cdot 7 \cdot 37 \cdot 79$ |
| **$512461 = 31 \cdot 61 \cdot 271$** | **$530881 = 13 \cdot 97 \cdot 421$** | $531505 = 5 \cdot 13^2 \cdot 17 \cdot 37$ |
| $544563 = 3^8 \cdot 83$ | **$552721 = 13 \cdot 17 \cdot 41 \cdot 61$** | $554625 = 3^2 \cdot 5^3 \cdot 17 \cdot 29$ |
| $561925 = 5^2 \cdot 7 \cdot 13^2 \cdot 19$ | $566401 = 11^2 \cdot 31 \cdot 151$ | $578125 = 5^6 \cdot 37$ |
| $578641 = 7^4 \cdot 241$ | $595441 = 7 \cdot 11^2 \cdot 19 \cdot 37$ | $600281 = 11^4 \cdot 41$ |
| $604513 = 7^2 \cdot 13^2 \cdot 73$ | $611893 = 47^2 \cdot 277$ | $613089 = 3^6 \cdot 29^2$ |
| $624169 = 7 \cdot 13 \cdot 19^3$ | $652257 = 3^2 \cdot 23^2 \cdot 137$ | **$656601 = 3 \cdot 11 \cdot 101 \cdot 197$** |
| **$658801 = 11 \cdot 13 \cdot 17 \cdot 271$** | **$670033 = 7 \cdot 13 \cdot 37 \cdot 199$** | $690625 = 5^5 \cdot 13 \cdot 17$ |
| $693889 = 7^4 \cdot 17^2$ | $695871 = 3^4 \cdot 11^2 \cdot 71$ | $703125 = 3^2 \cdot 5^7$ |
| $713125 = 5^4 \cdot 7 \cdot 163$ | $714025 = 5^2 \cdot 13^4$ | $717025 = 5^2 \cdot 23 \cdot 29 \cdot 43$ |
| **$748657 = 7 \cdot 13 \cdot 19 \cdot 433$** | $750541 = 11 \cdot 31^2 \cdot 71$ | $750925 = 5^2 \cdot 7^2 \cdot 613$ |
| $765625 = 5^6 \cdot 7^2$ | $767625 = 3 \cdot 5^3 \cdot 23 \cdot 89$ | $777925 = 5^2 \cdot 29^2 \cdot 37$ |
| $780325 = 5^2 \cdot 7^4 \cdot 13$ | $784225 = 5^2 \cdot 13 \cdot 19 \cdot 127$ | $793117 = 13^3 \cdot 19^2$ |
| *$793881 = 3^8 \cdot 11^2$* | $803551 = 7^2 \cdot 23^2 \cdot 31$ | $808561 = 13 \cdot 37 \cdot 41^2$ |
| $811073 = 59^2 \cdot 233$ | $815121 = 3^2 \cdot 41 \cdot 47^2$ | $815425 = 5^2 \cdot 13^2 \cdot 193$ |
| $820125 = 3^8 \cdot 5^3$ | **$825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$** | $838125 = 3^2 \cdot 5^4 \cdot 149$ |
| **$838201 = 7 \cdot 13 \cdot 61 \cdot 151$** | **$852841 = 11 \cdot 31 \cdot 41 \cdot 61$** | $856087 = 43^2 \cdot 463$ |
| $856801 = 11^2 \cdot 73 \cdot 97$ | $860625 = 3^4 \cdot 5^4 \cdot 17$ | $877825 = 5^2 \cdot 13 \cdot 37 \cdot 73$ |
| $879217 = 53^2 \cdot 313$ | $893101 = 11^4 \cdot 61$ | $894691 = 7^2 \cdot 19 \cdot 31^2$ |
| $943041 = 3 \cdot 11 \cdot 17 \cdot 41^2$ | $965497 = 13^2 \cdot 29 \cdot 197$ | $968485 = 5 \cdot 7^2 \cdot 59 \cdot 67$ |
| $970785 = 3^5 \cdot 5 \cdot 17 \cdot 47$ | $979837 = 79^2 \cdot 157$ | $989901 = 3^4 \cdot 11^2 \cdot 101$ |
| **$997633 = 7 \cdot 13 \cdot 19 \cdot 577$** | | |
| $1002001 = 7^2 \cdot 11^2 \cdot 13^2$ | **$1024651 = 19 \cdot 199 \cdot 271$** | $1030393 = 7 \cdot 13^3 \cdot 67$ |
| **$1033669 = 7 \cdot 13 \cdot 37 \cdot 307$** | **$1050985 = 5 \cdot 13 \cdot 19 \cdot 23 \cdot 37$** | $1063651 = 71^2 \cdot 211$ |
| $1071225 = 3^4 \cdot 5^2 \cdot 23^2$ | $1080801 = 3^2 \cdot 29 \cdot 41 \cdot 101$ | **$1082809 = 7 \cdot 13 \cdot 73 \cdot 163$** |
| $1105425 = 3^2 \cdot 5^2 \cdot 17^3$ | $1140625 = 5^6 \cdot 73$ | **$1152271 = 43 \cdot 127 \cdot 211$** |
| $1154881 = 7^4 \cdot 13 \cdot 37$ | $1165537 = 17^2 \cdot 37 \cdot 109$ | $1185921 = 3^4 \cdot 11^4$ |
| **$1193221 = 31 \cdot 61 \cdot 631$** | $1207845 = 3^3 \cdot 5 \cdot 23 \cdot 389$ | $1214869 = 59^2 \cdot 349$ |
| $1221025 = 5^2 \cdot 13^2 \cdot 17^2$ | *$1265625 = 3^4 \cdot 5^6$* | $1269621 = 3^3 \cdot 59 \cdot 797$ |
| $1299961 = 13 \cdot 19^2 \cdot 277$ | $1321029 = 3^4 \cdot 47 \cdot 347$ | $1335961 = 11^2 \cdot 61 \cdot 181$ |
| $1355121 = 3^2 \cdot 17^2 \cdot 521$ | $1357741 = 7^2 \cdot 11^2 \cdot 229$ | $1358127 = 3^{10} \cdot 23$ |
| $1373125 = 5^4 \cdot 13^3$ | $1399489 = 7^2 \cdot 13^4$ | $1401841 = 7^3 \cdot 61 \cdot 67$ |
| $1413721 = 29^2 \cdot 41^2$ | $1416521 = 71^2 \cdot 281$ | $1439425 = 5^2 \cdot 13 \cdot 43 \cdot 103$ |
| $1443001 = 7^4 \cdot 601$ | **$1461241 = 37 \cdot 73 \cdot 541$** | $1468125 = 3^4 \cdot 5^4 \cdot 29$ |
| $1476225 = 3^{10} \cdot 5^2$ | $1498861 = 7^2 \cdot 13^2 \cdot 181$ | *$1500625 = 5^4 \cdot 7^4$* |
| $1506625 = 5^3 \cdot 17 \cdot 709$ | $1529437 = 7^6 \cdot 13$ | $1540081 = 17^2 \cdot 73^2$ |
| $1555009 = 29^2 \cdot 43^2$ | $1566891 = 3^3 \cdot 131 \cdot 443$ | **$1569457 = 17 \cdot 19 \cdot 43 \cdot 113$** |
| $1610401 = 13^3 \cdot 733$ | $1615441 = 31^2 \cdot 41^2$ | **$1615681 = 23 \cdot 199 \cdot 353$** |
| $1653125 = 5^5 \cdot 23^2$ | $1658385 = 3^2 \cdot 5 \cdot 137 \cdot 269$ | $1677025 = 5^2 \cdot 7^2 \cdot 37^2$ |
| $1710325 = 5^2 \cdot 37 \cdot 43^2$ | $1741825 = 5^2 \cdot 19^2 \cdot 193$ | $1742221 = 13^4 \cdot 61$ |
| $1755625 = 5^4 \cdot 53^2$ | **$1773289 = 7 \cdot 19 \cdot 67 \cdot 199$** | $1815937 = 97^2 \cdot 193$ |
| **$1857241 = 31 \cdot 181 \cdot 331$** | *$1896129 = 3^8 \cdot 17^2$* | **$1909001 = 41 \cdot 101 \cdot 461$** |
| $1923769 = 19^2 \cdot 73^2$ | $1935025 = 5^2 \cdot 17 \cdot 29 \cdot 157$ | $1953433 = 79^2 \cdot 313$ |

*Remark* **2.30.** Here, as always in the sequel, the Carmichael number(s) and weak Carmichael number(s) will be often denoted by $CN$ and $WCN$, respectively. A computation via `Mathematica 8` shows that there are "numerous" weak Carmichael numbers that are neither Carmichael numbers nor prime powers. In particular, Table 2 shows that up to $10^6$ there are 235 weak Carmichael numbers which are not prime powers, and between them there are 43 Carmichael numbers. Moreover, up to $2 \times 10^6$ there are 298 $WCN$ which are not prime powers, and between them there are 55 $CN$.

*Remark* **2.31.** It is known [58, p. 338] that a Carmichael number can be a product of two other Carmichael numbers; for example, such a number is

$$(7 \cdot 13 \cdot 19)(37 \cdot 73 \cdot 109) = 1729 \cdot 294409 = 509033161.$$

It can be of interest to consider a related problem extended to the set of $WCN$ which are not prime powers (for example, $10125 = 45 \times 225$, $18225 = 45 \times 405$ and $50625 = 45 \times 1125$).

**Examples 2.32.** Notice that it is easy to determine $WCN$ with two distinct prime factors. In [15] the authors observed that such numbers are all integers of the form $3^{2e}5^f$ for any $e, f \geq 1$, and more generally, given any two odd primes $p < q$ with $q - 1 \not\equiv 0 (\bmod\, p)$, $p^{e\varphi(q-1)}q^{f\varphi(p-1)}$ is a $WCN$. For arbitrary given positive integers $e$ and $f$ such that $e \geq f$ and $e + f \geq 3$, denote by $\mathcal{C}_w(e, f)$ the set of all $WCN$ of the form $n = p^e q^f$ for some distinct odd primes $p$ and $q$. For any odd prime $p$ let $\mathcal{C}_w(p; e, f)$ denote the set of all primes $q$ such that $p^e q^f \in \mathcal{C}_w(e, f)$. Then by Theorem 2.4, $n$ is in $\mathcal{C}_w(e, f)$ if and only if $p-1 \mid q^f-1$ and $q-1 \mid p^e-1$, or equivalently with $p-1 \mid q^f-1$ and $q-1 \mid p^e-1$, respectively. In other words, for any given odd prime $q$, a prime $p$ is in $\mathcal{C}_w(q; e, f)$ if and only if $p - 1 \mid q^f - 1$ and $q - 1 \mid p^e - 1$. For example, when $e = 1$ and $f = 2$, the above two conditions easily reduced to the condition of finding all divisors $d \geq 2$ of $p + 1$ such that the number $q := d(p - 1) + 1$ is a prime. Examining this condition for primes $p \in \{3, 5, 7, 11, 13, \dots, 997\}$ (all 168 primes less than 1000), we find 452 $WCN$ of the form $p^2q$. We have verified also that into prime factorizations of these 452 numbers does not occur only primes 107, 317, 433 and 857 less than 1000, while between other 164 these primes, each of the primes $13, 73, 193, 277, 313, 397, 421, 457, 541, 613, 673, 733, 757$ and 787 occur only as a non-square factor $q$ into $WCN$ $p^2q$ (for example, for the first such number 13, $5^2 \cdot 13$ is a $WCN$, and for the latest between them, 787, $263^2 \cdot 787$ is a $WCN$).

Since for a given $p$ and divisors $d_1 = 2$ and $d_2 = (p + 1)/2$ of $p + 1$, we have the candidates $q_1 = 2p - 1$ and $q_2 = (p^2 + 1)/2$ for $q$, respectively. In the first case, if $2p - 1$ is also a prime, we obtain that $n_1 = p^2(2p - 1)$ is a $WCN$. In the second case, if $(p^2 + 1)/2$ is a prime, then $p^2(p^2 + 1)/2$ is a $WCN$. Notice that it was conjectured that there are infinitely many pairs $(p, 2p + 1)$ such that both $p$ and $2p + 1$ are primes (such a prime $p$ is called a

*Sophie Germain prime*; AOO5384 in OEIS). A computation shows that there are many pairs $(p, 2p-1)$ such that both numbers $p$ and $2p-1$ are primes (up to $10^3$, $10^4$, $10^5$, $10^6$, $10^7$ there are 153, 1206, 9686, 82374 and 711033 such pairs, respectively, while related numbers of Sophie Germain primes are 167, 1222, 9668, 82237 and 711154 respectively). Moreover, there are many triplets $(p, 2p-1, (p^2+1)/2)$ such that the all numbers $p, 2p-1$ and $(p^2+1)/2$ are primes (up to $10^3$, $10^4$, $10^5$, $10^6$, $10^7$ there are 30, 180, 1113, 8029 and 58294 such triplets, respectively.)

Similarly, if $e=3$ and $f=1$, then the corresponding conditions are equivalent to finding all divisors $d \geq 2$ of $p^2+p+1$ such that the number $q := d(p-1)+1$ is a prime. For example, using this condition to the primes $p \in \{3, 5, 7, 11, 13\}$, we obtain the following three numbers in $\mathcal{C}_w(3,1)$: $7^3 \cdot 19 = 6517$, $11^3 \cdot 71 = 94501$ and $11^3 \cdot 191 = 254221$.

A determination of some elements of $\mathcal{C}_w(2,2)$ consists in finding distinct odd primes $p$ and $q$ such that $p-1 \mid q^2-1$ and $q-1 \mid p^2-1$. Using this for $p \in \{3, 5, 7, 11, 13\}$, we get the following numbers in $\mathcal{C}_w(2,2)$: $3^2 \cdot 5^2 = 225$, $5^2 \cdot 7^2 = 1225$, $5^2 \cdot 13^2 = 4225$, $7^2 \cdot 13^2 = 8281$, $7^2 \cdot 17^2 = 14161$, $11^2 \cdot 31^2 = 116281$, $11^2 \cdot 41^2 = 203401$, $11^2 \cdot 61^2 = 450241$, $13^2 \cdot 29^2 = 142129$ and $13^2 \cdot 43^2 = 312481$.

For arbitrary pair $(e, f)$ of integers $e$ and $f$ with $1 \leq e \leq f$ and $e+f \geq 3$, let $\mathcal{P}_w(e, f)$ be a set defined as a a set of all pairs $(p, q)$ of distinct primes $p$ and $q$ such that $p^e q^f \in \mathcal{C}_w(e, f)$. Since $p^e - 1 \mid p^{e'} - 1$ whenever $e \mid e'$, it follows that for every such a pair $(e, e')$, $\mathcal{P}_w(e', f) \subseteq \mathcal{P}_w(e, f)$ holds. We conjecture that the converse statement is also true, that is, we have

**Conjecture 2.33.** *If $\mathcal{P}_w(e', f') = \mathcal{P}_w(e, f)$ then $f = f'$ and $e \mid e'$, or $e = e'$ and $f \mid f'$.*

Furthermore, for the pair $(e, f)$ with $1 \leq e \leq f$ and $e+f \geq 3$ let $\mathcal{Q}_w(e, f)$ be a set defined as

$$\begin{aligned}\mathcal{Q}_w(e, f) = \{p :\ & p \text{ is a prime and there is a prime } q \neq p \text{ such that} \\ & p^e q^f \text{ is a } WCN \text{ or } q^e p^f \text{ is a } WCN\}.\end{aligned}$$

**Conjecture 2.34.** *For arbitrary given pair $(e, f)$ with $1 \leq e \leq f$ and $e+f \geq 3$ the set $\mathcal{Q}_w(e, f)$ has a density 1 with respect to the set of all primes.*

Finally, for every pair $(e, f)$ with $1 \leq e \leq f$ and $e+f \geq 3$, and any odd prime $q$ let $\mathcal{Q}_w(q; e, f)$ be a set defined as

$$\mathcal{Q}_w(q; e, f) = \{p : p \text{ is a prime such that } p^e q^f \text{ is a } WCN \text{ or } q^e p^f \text{ is a } WCN\}.$$

**Conjecture 2.35.** *The union*

$$\bigcup_{1 \leq e \leq f < \infty} \mathcal{Q}_w(q; e, f)$$

*is an infinite set.*

Using arguments from Examples 2.32, we immediiately obtain the following result and its corollary.

**Proposition 2.36.** *Let $p$ and $q$ be two odd distinct primes such that $p < q$ and $q-1$ is not divisible by $p$. Let $u$ and $v$ be the smallest positive integers for which $p^u \equiv 1(\bmod\, q-1)$ and $q^v \equiv 1(\bmod\, p-1)$. Then $p^a q^b$ is a $WCN$ if and only if $a$ and $b$ are positive integers such that $u \mid a$ and $v \mid b$.*

**Corollary 2.37.** *If $n = p^e q^f$ is a weak Carmichael number, then $n = p^{de} q^{lf}$ is also a weak Carmichael number for all positive integers $d$ and $l$.*

**Corollary 2.38.** *Let $p$ and $q$ be odd primes such that $p < q$ and $q-1$ is not divisible by $p$. Then $p^{e\varphi(q-1)} q^{f\varphi(p-1)}$ is a weak Carmichael number for arbitrary pair of positive integers $e$ and $f$.*

*Remark* **2.39.** For any $e \geq 2$ and a fixed prime $p \geq 3$, consider the set $\mathcal{C}_w(p; e, 1)$ of $WCN$ of the form $p^e q$. Then (cf. Example 2.32) $n = p^e q$ is in $WCN$ for some odd prime $q \neq p$ if and only if $p-1 \mid q-1$ and $q-1 \mid p^e - 1$, or equivalently, $q = (p-1)s + 1$ for some divisor $s \geq 2$ of $(p^e - 1)/(p-1) = p^{e-1} + p^{e-2} + \cdots + 1$. If $e$ is even, then assuming $s = 2$, that is, $q = 2p - 1$, it follows that $2p - 1$ belongs to $\mathcal{C}_w(p; e, 1)$ if and only if $2p - 1$ is a prime. By using a "usual" heuristic argument based on the *Prime number theorem* that the probability that an odd integer $m$ is a prime is $2/\log m$, it follows that the "expected number" of the elements of the set $\mathcal{C}_w(e, 1)$ with even $e$ is at least

$$2 \sum_{p \text{ odd prime}} \frac{1}{\log(2p-1)} \geq 2 \sum_{p \text{ odd prime}} \frac{1}{2(p-1)} = \infty.$$

(Here it is used the well known fact that the sum of reciprocals of primes diverges).

The situation is somewhat complicated when $e \geq 3$ is odd. Then consider the set of all odd primes $p$ such that $p \equiv 1(\bmod\, e)$. Then $\sum_{i=0}^{e-1} p^i \equiv 0(\bmod\, e)$, and take $q = e(p-1)+1$. Then the probability that $q = (p-1)e+1$ is a prime is $e/(\varphi(e)\log(e(p-1)+1)$. Using this and the well known fact that the series $\sum_{\substack{p \text{ odd prime} \\ p \equiv 1(\bmod\ e)}} 1/p$ diverges, we find that the "expected number" of the elements that belong to the set $\mathcal{C}_w(e, 1)$ with odd $e \geq 3$ is

$$\frac{e}{\varphi(e)} \sum_{\substack{p \text{ odd prime} \\ p \equiv 1(\bmod\ e)}} \frac{1}{\log(e(p-1)+1)} < \frac{e}{\varphi(e)} \sum_{\substack{p \text{ odd prime} \\ p \equiv 1(\bmod\ e)}} \frac{1}{e(p-1)} = \infty.$$

The above considerations suggest the conjecture that $\mathcal{C}_w(e, 1)$ is infinite set for all $e \geq 2$. This conjecture by Corollary 2.37 implies the same conjecture for all sets $\mathcal{C}_w(e, l)$ with $e \geq 2$ and $l \geq 2$. In accordance to this, some additional computations and the conjecture that for any given integer $s \geq 3$, there are infinitely many $CN$ with exactly $s$ prime factors (cf. a stronger Conjecture 1 in [35] which asserts that this number up to $x$ is at least $x^{1/s+o_s(1)}$), we give the following generalized conjecture.

**Conjecture 2.40.** *Let $s \geq 2$ be an arbitrary integer, and let $(e_1, e_2, \ldots, e_s)$ be any fixed $s$-tuple of integers $e_1, e_2, \ldots, e_s$ with $e_1 \geq e_2 \geq \cdots \geq e_s \geq 1$ and $\sum_{i=1}^{s} e_i \geq 3$. Then there are infinitely many weak Carmichael numbers $n$ with a prime factorization $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, where $p_1, p_2, \ldots, p_s$ are distinct odd primes.*

*Remark* **2.41.** A heuristic argument suggests that for a large odd positive integer $n$ which is neither a $CN$ nor a prime power, the "probability" that $\sum_{i=1}^{\varphi(n)} r_i^{n-1} \equiv \varphi(n) (\bmod\, n)$ is equal to $(n-1)/2$. Consequently, the number of $WCN$ in the interval $[1, n]$ is asymptotically equal to the double harmonic sum $2\sum_{k=1}^{[n/2]} 1/k$ which is $\sim 2\log n$ as $n \to \infty$. Furthermore, as noticed above, the number of $CN$ in the interval $[1, n]$ is greater than $n^{2/7}$ for sufficiently large $n$. Moreover, under certain (widely-believed) assumptions about the distribution of primes in arithmetic progressions, it is shown in [1, Theorem] (see also [35]) that there are $n^{1-o(1)}$ Carmichael numbers up to $n$, as had been conjectured in 1956 by Erdős [26] (see also [70]). On the other hand, it is known that the number of prime powers with exponents $\geq 2$ (the sequence A025475 in [72]) up to $x$ (see e.g., [40, p. 27]) is given by $O(x^{1/2} \log x)$ (more precisely, this number is $2x^{1/2} \log x$). These considerations suggest the following conjecture.

**Conjecture 2.42.** *The numbers of Carmichael numbers and weak Carmichael numbers in the interval $[1, n]$ are asymptotically equal as $n \to \infty$.*

From Table 1 we see that 2465 and 2821 are (the first) twin Carmichael numbers, and 62745 and 63973 are also twin Carmichael numbers in the sense of the following definition.

**Definition 2.43.** Two Carmichael numbers are said to be *twin Carmichael numbers* if there is none weak Carmichael number between them.

Accordingly to the Conjecture 2.42, we can propose the following "twin Carmichael numbers conjecture" which is an immediate consequence of Conjecture 2.42.

**Conjecture 2.44.** *There are infinitely many pairs of twin Carmichael numbers.*

*Remark* **2.45.** We see from Table 2 that the pairs $(656601, 658801)$ and $(658801, 670033)$ are consecutive twin Carmichael numbers.

*Remark* **2.46.** As noticed in Subsection 1.1, Lehmer condition implies that a composite positive integer must be square-free. This also concerns to the Giuga's condition defined by the congruence (1.3). Moreover, all $CN$ and $k$-Lehmer numbers are square-free (see Remark 1.2). However, from Table 2 we see that there are numerous non-square-free composite $WCN$.

*Remark* **2.47.** We believe that the investigation of $WCN$ and their distribution would be more complicated than those on $CN$, Lehmer numbers and Giuga numbers. This also concerns to the $k$-Lehmer numbers presented in Remark 1.2 as well as to the Giuga's-like numbers recently investigated in [39] and [51].

We see from Table 2 that the smallest $WCN$ with three prime distinct factors is the $CN$ 561, and the smallest $WCN$ with four prime distinct factors is the $CN$ 41041. Accordingly, we propose the following curious conjecture.

**Conjecture 2.48.** *Let $k$ be an arbitrary integer $\geq 3$. Then the smallest $WCN$ with $k$ prime distinct factors is a $CN$.*

*Remark* **2.49.** Under the assumption of Conjecture 2.48, every $WCN$ less than the smallest $CN$ with six distinct prime factors $3211197185 = 5 \times 19 \times 23 \times 29 \times 37 \times 137$ has at most five distinct factors.

2.3. **A compuational search of weak Carmichael numbers via the function `Carmichael Lambda`.** As noticed above, Carmichael lambda function $\lambda(n)$ denotes the size of the largest cyclic subgroup of the group $(\mathbb{Z}/n\mathbb{Z})^*$ of all reduced residues modulo $n$. In other words, $\lambda(n)$ is the smallest positive integer $m$ such that $a^m \equiv 1(\bmod\, n)$ for all $a$ coprime to $n$ (Sloane's sequence A002322 [72]). This function was implemented in `Mathematica 8` as the function "`Carmichael Lambda`". For a fast computation of $WCN$ we can use this function in view of the following fact which is immediate from Theorem 2.4 and the fact that for every odd integer $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$, we have $\lambda(n) = \mathrm{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_s^{e_s}))$ with $\lambda(p_i^{e_i}) = \varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1)$ for all $i = 1, 2, \ldots, s$.

**Proposition 2.50.** *Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be an odd composite integer, and let $n' = p_1 p_2 \cdots p_s$. Then $n$ is a weak Carmichael number if and only if*

$$\lambda(n') \mid n - 1. \tag{2.9}$$

Proposition 2.50 suggests the following definition introduced by Erdős in 1948 [25].

**Definition 2.51.** A positive integer $n > 1$ such that $\gcd(n, \varphi(n)) = 1$ is called a *$K$-number.*

Erdős noticed that $n > 1$ is a $K$-number if and only if $n$ is a square-free and it is divisible by none of the products $pq$ of two distinct primes $p$ and $q$ with $q \equiv 1(\bmod\, p)$. Moreover, Erdős [25, Theorem] proved that the number of $K$-numbers less than $x$ is $\sim xe^{-\gamma}/(\log\log\log x)$, where $\gamma$ is the Euler's constant. Proposition 2.50 together with Euler totient theorem and the definition of Carmichael lambda function easily gives the following result.

**Proposition 2.52.** *Let $n > 2$ be a $K$-number. Then $n$ is odd and $n^{d\lambda(n)}$ is a weak Carmichael number for each positive integer $d$. In particular, for such a $n$, $n^{d\varphi(n)}$ is a weak Carmichael number for each positive integer $d$.*

*Furthermore, if $n = p_1 p_2 \cdots p_s$, then*

$$\lambda(n) = \mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_s - 1).$$

Clearly, every Carmichael number is a $K$-number, and hence Proposition 2.52 immediately yields the following result.

**Corollary 2.53.** *Let $n$ be a Carmichael number. Then both $n^{d\lambda(n)}$ and $n^{d\varphi(n)}$ are weak Carmichael numbers for arbitrary positive integer $d$.*

*Remark* **2.54.** For a fast search of some special "types" of $WCN$ it can be used the condition (2.9) to make suitable codes for these purposes. For any fixed $k \geq 2$, let $\mathcal{W}_k$ denote the set of all $WCN$ whose prime factorizations contain exactly $k$ primes. Further, for positive integers $a, b, c, d$ with $a < b$ and $c < d$ take $\mathcal{W}_k(a, b) = \mathcal{W}_k \bigcap [a, b]$, and let $\mathcal{W}_k(a, b; c, d)$ be the set of all elements in $\mathcal{W}_k(a, b)$ whose greatest prime divisor belongs to the interval $[c, d]$. Clearly, $\mathcal{W}_k(a, b; c, b)$ is a set of all elements in $\mathcal{W}_k(a, b)$ whose greatest prime divisor is grater than equal to $c$. The cardinilities of sets $\mathcal{W}_k$, $\mathcal{W}_k(a, b)$ and $\mathcal{W}_k(a, b; c, d)$ are denoted by $W_k$, $W_k(a, b)$ and $W_k(a, b; c, d)$, respectively. For such a set $\mathcal{W}_k(a, b; c, d)$ define

$$\mathcal{P}_k(a, b; c, d) = \{p : \, p \text{ is a prime with } p \mid n \text{ for some } n \in \mathcal{W}_k(a, b; c, d)\},$$

and let $p_k(a, b; c, d)$ be a prime defined as

$$p_k(a, b; c, d) = \max\{p : \, p \in \mathcal{W}_k(a, b; c, d)\},$$

and let $w_k(a, b; c, d)$ be the smallest number in $\mathcal{W}_k(a, b; c, d)$ which is divisible by $p_k(a, b; c, d)$.

If $\mathcal{C}_k$ denotes the set of all Carmichael numbers whose prime factorizations contain exactly $k$ primes, then in the same manner as above, we define the sets $\mathcal{C}_k(a, b)$, $\mathcal{C}_k(a, b; c, d)$ and related numbers $C_k(a, b)$ and $\mathcal{C}_k(a, b; c, d)$ associated to $\mathcal{C}_k$. Also let $C(a, b)$ be the number of all Carmichael numbers that belong to the interval $[a, b]$, and let $P(a, b)$ be the number of all odd prime powers that belong to the interval $[a, b]$. To save the space, the set $\mathcal{C}_k(b)$ will be denoted by $\mathcal{C}_k(1, b)$ and its cardinality by $C_k(b)$. Also let $C(b) = \sum_{k\geq 3} C_k(b)$ be the number of Carmichael numbers which are less than $b$. Similarly, we define the set $\mathcal{W}'_k(b)$ consisting of all $WCN$ in $\mathcal{W}_k(1, b)$ which are not $CN$. The cardinality of $\mathcal{W}'_k(b)$ is denoted here as $W'_k(b)$. Denote by $W'(b)$ the number of all $WCN$ up to $b$ which are neither $CN$ nor prime powers; that is, $W'(b) = \sum_{k\geq 2} W'_k(b)$.

Here we present a computational search of $WCN$ that belong to $\mathcal{W}_2$, i.e., of integers $n = p^e q^f$ with primes $3 \leq p < q$ and some positive integers $e$ and $f$. In particular, our code in `Mathematica 8` for determining different sets of the form $\mathcal{W}_2(a, b; c, d)$ gives results presented in Table 3 (recall that all non-prime powers weak Carmichael numbers less than $2 \times 10^6$ are presented in Table 2).

**Table 3.** Numbers $W_2(a,b;c,d)$, $p_2(a,b;c,d)$, $w_2(a,b;c,d)$ (all written in Table 2 without "$(a,b;c,d)$"), $P(a,b)$ and $C(a,b)$ for $n < 10^{12}$

| $(a,b;c,d)$ | $W_2$ | $p_2$ | $w_2$ | $P(a,b)$ | $C(a,b)$ |
|---|---|---|---|---|---|
| $(1,10^6;1,10^6)$ | 107 | 463 | $856087 = 43^2 \cdot 463$ | 218 | 43 |
| $(10^6,2\cdot 10^6;1,2\cdot 10^6)$ | 25 | 733 | $1610401 = 13^3 \cdot 733$ | 65 | 12 |
| total | 132 | | | 283 | 55 |
| $(2\cdot 10^6,10^7;1,10^3)$ | 69 | 937 | $2632033 = 53^2 \cdot 937$ | 250 | 50 |
| $(2\cdot 10^6,10^7;10^3,10^4)$ | 5 | 1861 | $6924781 = 61^2 \cdot 1861$ | - | - |
| $(2\cdot 10^6,10^7;10^4,10^7)$ | 0 | $-$ | - | - | - |
| total | 74 | | | 250 | 50 |
| $(10^7,10^8;1,10^3)$ | 120 | 997 | $27805333 = 167^2 \cdot 997$ | 846 | 150 |
| $(10^7,10^8;10^3,10^4)$ | 43 | | $81390625 = 5^6 \cdot 5209$ - | - | - |
| $(10^7,10^8;10^4,10^8)$ | 0 | | - | - | - |
| total | 163 | | | 846 | 150 |
| $(10^8,10^9;1,10^3)$ | 156 | | | 2282 | 391 |
| $(10^8,10^9;10^3,10^4)$ | 109 | | | | |
| $(10^8,10^9;10^4,10^9)$ | 9 | | | | |
| total | 274 | | | 2282 | 391 |
| $(10^9,10^{10};1,10^3)$ | 211 | | | 6391 | 901 |
| $(10^9,10^{10};10^3,10^4)$ | 112 | | | | |
| $(10^9,10^{10};10^4,10^{10})$ | 74 | | | | |
| total | 397 | | | 6391 | 901 |
| $(10^{10},10^{11};1,10^3)$ | 247 | | | 18069 | 2058 |
| $(10^{10},10^{11};10^3,10^4)$ | 93 | | | | |
| $(10^{10},10^{11};10^4,10^{11})$ | 253 | | | | |
| total | 593 | | | 18069 | 2058 |
| $(10^{11},10^{12};1,10^3)$ | 266 | | | 51911 | 4636 |
| $(10^{11},10^{12};10^3,10^4)$ | 220 | | | | |
| $(10^{11},10^{12};10^4,10^{12})$ | 689 | | | | |
| total | 1175 | | | 51911 | 4636 |
| total up to $10^{12}$ | 2808 | | | 80032 | 8241 |

Let $W_3'(N)$ be the number of all $n = p^a q^b r^c \in \mathcal{W}CN \setminus \mathcal{C}N$ up to $N$ with odd primes $p < q < r$. Using this notation and the previous notations, counting related numbers in Table, we arrived to the following table.

**Table 4.** Numbers $C_k(N)$ and $W'_k(N)$ with $k = 2, 3, 4, 5$ and $N \in \{10^3, 10^4, 10^5, 10^6, 2 \cdot 10^6\}$.

| Pairs $(N, k)$ | $C_k(N)$ | $C(N)$ | $W'_k(N)$ | $W'(N)$ |
|---|---|---|---|---|
| $(10^3, 2)$ | - | 1 | 6 | 6 |
| $(10^4, 2)$ | - | 7 | 22 | 25 |
| $(10^5, 2)$ | - | 16 | 51 | 70 |
| $(10^6, 2)$ | - | 43 | 107 | 192 |
| $(2 \cdot 10^6, 2)$ | - | 55 | 132 | 243 |
| $(10^3, 3)$ | 1 | | 0 | |
| $(10^4, 3)$ | 7 | | 3 | |
| $(10^5, 3)$ | 12 | | 18 | |
| $(10^6, 3)$ | 23 | | 68 | |
| $(2 \cdot 10^6, 3)$ | 30 | | 89 | |
| $(10^4, 4)$ | 0 | | 0 | |
| $(10^5, 4)$ | 4 | | 1 | |
| $(10^6, 4)$ | 19 | | 17 | |
| $(2 \cdot 10^6, 4)$ | 23 | | 22 | |
| $(10^5, 4)$ | 0 | | 0 | |
| $(10^6, 5)$ | 1 | | 0 | |
| $(2 \cdot 10^6, 5)$ | 2 | | 0 | |
| total up to $N = 2 \cdot 10^6$ | 55 | 55 | 243 | 243 |

For a search of $W'_3(N)$ with $N \leq 10^{12}$, we use a characetrization of $WCN$ given by Theorem 2.4. The three-component Carmichael number counts, $C_3(N)$, presented in the second column of Table 5, are taken from the Granville and Pomerance paper [35]. These counts were calculated by R. Pinch, J. Chick, G. Davies and M. Williams (cf. [22, Table 2]).

**Table 5.** Numbers $C_3(N)$ and $W_3'(N)$ with
$N \in \{10^3, 10^4, 10^5, 10^6, 2\cdot 10^6, 10^7, 10^8, \dots, 10^{12}\}$.

| $N$ | $C_3(N)$ | $W_3'(N)$ | $n = p^a q^b r^c \in \mathcal{W}_3'(N)$ with a maximal $r$ | $n = pqr \in \mathcal{C}_3'(N)$ with a maximal $r$ |
|---|---|---|---|---|
| $10^3$ | 1 | 0 | - | $561 = 3\cdot 11\cdot 17$ |
| $10^4$ | 7 | 3 | $6525 = 3^2\cdot 5^2\cdot 29$ | $8911 = 7\cdot 19\cdot 67$ |
| $10^5$ | 12 | 18 | $25425 = 3^2\cdot 5^2\cdot 113$ | $52633 = 7\cdot 73\cdot 103$ |
| $10^6$ | 23 | 68 | $750925 = 5^2\cdot 7^2\cdot 613$ | $530881 = 13\cdot 97\cdot 421$ |
| $2\cdot 10^6$ | 30 | 89 | $1269621 = 3^3\cdot 59\cdot 797$ | $1193221 = 31\cdot 61\cdot 631$ |
| $10^7$ | 47 | 186 | $8927425 = 5^2\cdot 13^2\cdot 2113$ | $8134561 = 37\cdot 109\cdot 2017$ |
| $10^8$ | 84 | 413 | $52280425 = 5^2\cdot 409\cdot 5113$ | $67902031 = 43\cdot 271\cdot 5827$ |
| $10^9$ | 172 | 863 | $954036721 = 11^2\cdot 19^2\cdot 21841$ | $962442001 = 73\cdot 601\cdot 21937$ |
| $10^{10}$ | 335 | 1590 | $4465266751 = 11^3\cdot 71\cdot 47251$ | $8863329511 = 211\cdot 631\cdot 66571$ |
| $10^{11}$ | 590 | 2866 | $79183494081 = 3^4\cdot 17^3\cdot 198977$ | $74190097801 = 151\cdot 2551\cdot 192601$ |
| $10^{12}$ | 1000 | 4291 | $800903953125 = 3^4\cdot 5^6\cdot 632813$ | $921323712961 = 673\cdot 2017\cdot 678721$ |
| $10^{13}$ | 1858 | | | |
| $10^{14}$ | 3284 | | | |
| $10^{15}$ | 6083 | | | |
| $10^{16}$ | 10816 | | | |
| $10^{17}$ | 19539 | | | |
| $10^{18}$ | 35586 | | | |
| $10^{19}$ | 65309 | | | |
| $10^{20}$ | 120625 | | | |

*Remark* **2.55.** Notice that prime factors of every $WCN$ $n = p^a q^b r^c$ in the fourth column of Table 5 besides the number 6525 satisfy the equlity $r-1 = (p^a q^b - 1)/2$. Similarly, the prime factors $p, q, r$ of $CN$ 561, 8911, 8134561,67902031, 962442001, 8863329511, 74190097801 and 921323712961 in the last column of Table 5 satisfy the equality $r-1 = (pq-1)/2$.

*Remark* **2.56.** Let $\alpha = \alpha(N)$ denote the real number such that $C_3(N) = N^\alpha$, and let $\beta = \beta(N)$ be the real number such that $W_3'(N) = N^\beta$. Then from data in Table 5 we find that $\alpha(10^6) = 0.227$, $\alpha(10^9) = 0.248$, $\alpha(10^{12}) = 0.250$, $\alpha(10^{15}) = 0.252$ $\alpha(10^{18}) = 0.253$, $\alpha(10^{21}) = 0.255$, $\beta(10^6) = 0.305$ $\beta(10^9) = 0.326$ and $\beta(10^{12}) = 0.303$.

2.4. ***k*-Lehmer numbers and weak Carmichael numbers.** Quite recently, J.M. Grau and A.M. Oller-Marcén [37, Definition 1] weakened Lehmer property by introducing the concept of $k$-Lehmer numbers. For given positive integer $k$, a *$k$-Lehmer number* is a composite integer $n$ such that $\varphi(n) \mid (n-1)^k$. Hence, if we denote by $L_k$ the set

$$L_k := \{n \in \mathbb{N} :\, \varphi(n) \mid (n-1)^k\},$$

then $k$-Lehmer numbers are the composite elements of $L_k$. Clearly, $L_k \subseteq L_{k+1}$ for each $k \in \mathbb{N}$, and define

$$L_\infty := \bigcup_{k=1}^{\infty} L_k.$$

Then it can be easily shown that (see [37, Proposition 3])

$$L_\infty := \{n \in \mathbb{N} : \operatorname{rad}(\varphi(n)) \mid n-1\}.$$

This immediately shows that if $n$ is a Carmichael number, then $n$ also belongs to the set $L_\infty$ ([37, Proposition 6]). This leads to the following characterization of Carmichael numbers which slightly modifies Korselt's criterion.

**Proposition 2.57.** *A composite number $n$ is a Carmichael number if and only if* $\operatorname{rad}(\varphi(n)) \mid n-1$ *and $p-1 \mid n-1$ for every prime divisor $p$ of $n$.*

Obviously, the composite elements of $L_1$ are precisely the Lehmer numbers and the Lehmer property asks whether $L_1$ contains composite numbers or not. Nevertheless, for all $k > 1$, $L_k$ always contains composite elements (cf. Sloane's sequence A173703 in OEIS [72] which presents $L_2$). For further radically weakening the Lehmer and Carmichael conditions see [55].

As an immediate consequence of Proposition 2.57 and Theorem 2.4 we obtain the following characterization of Carmichael numbers.

**Corollary 2.58.** *A composite number $n$ is a Carmichael number if and only if $n$ is a weak Carmichael number and* $\operatorname{rad}(\varphi(n)) \mid n-1$.

2.5. **Super Carmichael numbers.** The fact that there are infinitely many weak Carmichael numbers suggests the following definition.

**Definition 2.59.** A weak Carmichael number $n$ is said to be a *super Carmichael number* if

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi(n) \pmod{n^2}, \tag{2.10}$$

where the summation ranges over all $k$ such that $1 \le k \le n-1$ and $\gcd(k,n) = 1$.

The following characterization of super Carmichael numbers may be useful for computational purposes.

**Proposition 2.60.** *An odd composite positive integer $n > 1$ is a super Carmichael number if and only if*

$$2\sum_{i=1}^{\varphi(n)/2} r_i^{n-1} + n\sum_{i=1}^{\varphi(n)/2} r_i^{n-2} \equiv \varphi(n) \pmod{n^2} \tag{2.11}$$

*where $r_1 < r_2 < \cdots < r_{\varphi(n)}$ are all reduced residues modulo $n$.*

Here, as always in the sequel, the super Carmichael number(s) will be often denoted by $SCN$.

*Remark* **2.61.** Using Proposition 2.18, some computations and a heuristic argument, we can assume that the probability that a prime power $p^s$ with an odd prime $p$ and $s \geq 2$, is a $SCN$ is equal to $1/p^s$. Furthermore, applying (2.11), a computation in `Mathematica 8` shows that none prime power $p^s$ less than $3^{16}$ with $s \geq 2$ and $p \leq p_{847} = 6553$ is a $SCN$. This together with the identity $\sum_{i=s+1}^{\infty} 1/p^i = 1/(p^s(p-1))$

$$\Sigma_1 := \sum_{\substack{p \text{ odd prime} \\ s\geq 2 \text{ and } p^s \geq 3^{16}}} \frac{1}{p^s} = 8.91952 \cdot 10^{-7}. \tag{2.12}$$

On the other hand, a computation also gives

$$\begin{aligned} \Sigma_2 :&= \sum_{\substack{p \text{ prime} \\ p>6553}} \sum_{i=2}^{\infty} \frac{1}{p^i} = \sum_{\substack{p \text{ prime} \\ p>6553}} \frac{1}{p(p-1)} < 0.00016 < \sum_{k=6552}^{\infty} \frac{1}{k^2} \\ &= \zeta(2) - \sum_{k=1}^{6551} \frac{1}{k^2} = 0.000152381. \end{aligned} \tag{2.13}$$

Using (2.12), (2.13) and the fact that none prime power $p^s$ less than $3^{16}$ with $s \geq 2$ and $p \leq p_{847} = 6553$ is a $SCN$, we find that the expected number of $SCN$ that occur in the set of all prime powers of the form $p^s$ with $s \geq 2$ is

$$\Sigma_1 + \Sigma_2 < 0.001525.$$

Using the above estimate, we can propose the following conjecture.

**Conjecture 2.62.** *Let $p$ be any odd prime. Then none prime power $p^f$ with $f \geq 2$ is a super Carmichael number.*

Notice that by using a result of I.Sh. Slavutskii [71], it is proved in Section 4 the following result.

**Proposition 2.63.** *Let $p$ be an odd prime greater than 3. Then a prime power $p^f$ with $f \geq 2$ is a super Carmichael number if and only if the numerator of the Bernoulli number $B_{(p^{2f}-p^{2f-1}-1)(p^{2f}-p^{2f-1}-p^f+1)}$ is divisible by $p^{f+1}$.*

*Remark* **2.64.** Using Table 2, a computation in `Mathematica` 8 shows that there are none $SCN$ less than $2 \times 10^6$. Notice that by using Harman's result [42] given in Subsection 1.1, it follows that the "probability" that a sufficiently large positive integer $n$ is a $CN$ is greater than $n^{0.33}/n = 1/n^{0.67}$. Using this, some "little" computations and a heuristic argument, we can assume that the "probability" that a large number $n$ is a $SCN$ is greater than $1/(n \cdot n^{0.67}) = 1/n^{1.67}$. It follows that the "expected number" of $CN$ in a large interval $[1, N]$

is greater than

$$\sum_{n=1}^{N} \frac{1}{n^{1.67}}$$

which tends to $\zeta(1.67) = 2.11628$ as $N \to \infty$. However, as noticed above, under certain assumptions about the distribution of primes in arithmetic progressions, it is shown in [1, Theorem] that there are $x^{1-o(1)}$ Carmichael numbers up to $x$. For this subject, see also [7]. It was also given in [65] a heuristic argument that this number is $x^{1-\varepsilon(x)}$, where $\varepsilon(x) = (1 + o(1)) \log\log\log x/(\log\log x)$. This argument is supported by counts of $CN$ mostly done in 1975 by J.D. Swift [77], in 1990 by G. Jaeschke [44], by R. Pinch [62] in 1993 and R. Pinch [63] in 2006. Accordingly, using the previous arguments, we can assume that the "probability" that a large number $n$ is a $SCN$ is about $1/n^{o(1)}$. It follows that the "expected number" of Carmichael numbers in a very large interval $[1, N]$ is greater than

$$\sum_{k=1}^{N} \frac{1}{k}.$$

This together with the fact that $\sum_{k=1}^{\infty} 1/k = +\infty$ motivates the following conjecture.

**Conjecture 2.65.** *There are infinitely many super Carmichael numbers.*

*Remark* **2.66.** A heuristic argument and considerations given in Remark 2.64 suggest that a search for $SCN$ would be have a "chance" only between $SCN$. In other words, $SCN$ "probably" can occur only between $CN$. Hence, we propose the following conjecture.

**Conjecture 2.67.** *Every super Carmichael number is necessarily a Carmichael number.*

*Remark* **2.68.** Because of Conjecture 2.67, we have omitted the word "weak" in the name "super Carmichael number" given in Definition 2.59.

*Remark* **2.69.** In order to examine whether given $CN$ $n$ is also a $SCN$, it is natural to proceed as follows. Take $n = p_1 p_2 \cdots p_s$, where $p_1, p_2, \ldots, p_s$ are distinct odd primes. Then by the congruence (2.11) of Proposition 2.60, with $r_i$ defined in Proposition 2.60, it follows that $n$ is a $SCN$ if and only if

$$c_n := 2 \sum_{i=1}^{\varphi(n)/2} r_i^{n-1} + n \sum_{i=1}^{\varphi(n)/2} r_i^{n-2} - \varphi(n) \equiv \pmod{n^2}. \tag{2.14}$$

Clearly, the congruence (2.14) holds if and only if

$$c_n \equiv 0 \pmod{p_i^2} \quad \text{for each } i = 1, 2, \ldots, s. \tag{2.15}$$

Now taking $n - 1 = q_i \varphi(p_i^2) + l_i = q_i p_i (p_i - 1) + l_i$ and $n - 2 = t_i \varphi(p_i) + u_i = t_i (p_i - 1) + u_i$ with integers $q_i, t_i \geq 1$ and $0 \leq l_i, u_i \leq p_i - 1$ for all

$i \in \{1,2,\ldots,s\}$. Then by Euler totient theorem and (2.15) and the fact that $\varphi(p_i^2)=p_i^2-p_i$, the congruence (2.14) is satisfied if and only if
(2.16)

$$c_n(p_i):=2\sum_{i=1}^{\varphi(n)/2} r_i^{l_i}+n\sum_{i=1}^{\varphi(n)/2} r_i^{u_i}p_i\equiv 0 \pmod{p_i^2} \text{ for each } i=1,2,\ldots,s.$$

Taking $m_i=\max\{l_i,u_i\}$ for all $i=1,2,\ldots,s$, without loss of generality we can suppose that $m_1\le m_2\le\cdots\le m_s$. Then we firstly verify the congruence (2.16) for $i=1$. If (2.16) is not satisfied modullo $p_1^2$, then we conclude that $n$ is not a $SCN$. Otherwise, we continue the computation passing to $p_2$ etc. Of course, we finish the computation to a first index $i$ for which $c_n(p_i)\not\equiv (\bmod\, p_i^2)$. If it is obtained that $c_n(p_i)\equiv(\bmod\, p_i^2)$ for each $i=1,2,\ldots,k$, then we conclude that $n$ is a $SCN$.

2.6. **Weak Carmichael numbers and the Fermat primality test.** Gauss [31] (Article 329 of *Disquisitiones Arithmeticae*, 1801), let. 329]) wrote:

*The problem of distinguishing prime numbers from composite numbers is one of the most fundamental and important in arithmetic. It has remained as a central question in our subject from ancient times to this day...*

On October 18th, 1640 Fermat wrote, in a letter to his confidante Frenicle, that the fact that $n$ divides $2^n-2$ whenever $n$ is prime is not an isolated phenomenon. Indeed that, if $n$ is prime then $n$ divides $a^n-a$ for all integers $n$; which implies that if $n$ doesn't divide $a^n-a$ for some integer $a$ then $n$ is composite.

As noticed above, as "false primes" Carmichael numbers are quite famous among specialists in number theory, as they are quite rare and very hard to test. Accordingly, these numbers present a major problem for Fermat-like primality tests. Here we give some remarks on Carmichael and weak Carmichael numbers closely related to the Fermat primality test.

*Fermat little theorem* says that if $p$ is a prime and the integer $a$ is not a multiple of $p$, then

$$a^{p-1}\equiv 1 \pmod{p}. \tag{2.17}$$

If we want to test if $p$ is prime, then we can pick random $a$'s in the interval and see if the congruence holds. If the congruence does not hold for a value of $a$ then $p$ is composite. If the congruence does hold for many values of $a$, then we can say that $p$ is "probable prime". It might be in our tests that we do not pick any value for a such that the congruence (2.17) fails. Any $a$ such that $a^{n-1}\equiv 1(\bmod\, n)$ when $n$ is composite is called a *Fermat liar*. In this case $n$ is called *Fermat pseudoprime to base a*. If we do pick an integer $a$ such that $a^{n-1}\not\equiv 1(\bmod\, n)$, then $a$ is called a *Fermat witness* for the compositeness of $n$. Clearly, a Carmichael number $n$ is a composite integer that is *Fermat-pseudoprime* to base $a$ for every $a$ with $\gcd(a,n)=1$. On the other hand, it is known that for "many" (necessarily even) integers $n$ the congruence $a^{n-1}\equiv 1(\mathrm{mod}\, n)$ is satisfied only when $a\equiv 1(\mathrm{mod}\, n)$ (this is Sloane's sequence A111305 of "unCarmichael numbers" [72]; cf. Sloane's A039772 [72]). For any integer $n>1$ let $\mathcal{F}(n)$ be the set defined as

$$\mathcal{F}(n)=\{a\in\mathbb{Z}/n\mathbb{Z}:\ a^{n-1}\equiv 1 \pmod{n}\},$$

and let $F(n)=\#\mathcal{F}(n)$, that is, $F(n)$ is a number of residues $a$ modulo $n$ such that $a^{n-1}\equiv 1(\mathrm{mod}\, n)$ ($F(n)$ is Sloane's sequence A063994). Therefore,

$$F(n)=\#\{a\in\mathbb{Z}/n\mathbb{Z}:\ a^{n-1}\equiv 1(\mathrm{mod}\, n)\},$$

that is, $F(n)$ is a number of Fermat liars for $n$. Clearly, $\mathcal{F}(n)$ is a subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. If $n=p$ is a prime, then $F(p)=p-1$ and $\mathcal{F}(p)=(\mathbb{Z}/p\mathbb{Z})^*$, i.e., $\mathcal{F}(p)$ is the entire group of reduced residues modulo $p$.

The following elegant and simple formula for $F(n)$ was established by Monier [56, Lemma 1] and Baillie and Wagstaff [6] (also see [3]):

$$F(n)=\prod_{p\mid n}\gcd(p-1,n-1). \tag{2.18}$$

We also define the sequence $f(n)$ with $n\ge 2$ as

$$f(n)=\frac{F(n)}{\varphi(n)}=\prod_{p\mid n}\frac{\gcd(p-1,n-1)}{(p-1)p^{e_p-1}}, \tag{2.19}$$

where $n=\prod_{p\mid n}p^{e_p}$.

*Remark* **2.70.** Recall that the index of every $WCN$ up to 26353 $n$ presented in Table 2 denotes a related value $F(n)$ (for example, $F(26353)=1296$). Of course, $F(n)=n-1$ if and only if $n$ is a prime or a $CN$. At the other extreme, there are infinitely many numbers $n$ for which $F(n)=1$. In particular, (2.18) immediately implies that $F(2p)=1$ for every prime $p$. It is possible to show (see [27]) that while these numbers $n$ with $F(n)=1$ have asymptotic density 0, they are much more common than primes. The normal and average size of $F(n)$ for $n$ composite were studied in 1986 [27]. By Lagrange theorem, $F(n)\mid\varphi(n)$ for any $n$. It was proved in [27, p. 263] that $F(n)=\varphi(n)/k$ for an integer $k$ implies $\lambda(n)\mid k(n-1)$, where $\lambda(n)$ is the *Carmichael lambda function* denoting a smallest positive integer such that $a^{\lambda(n)}\equiv 1(\mathrm{mod}\, n)$ for all $a$ with $\gcd(a,n)=1$. Moreover, it was proved in [27, Theorem 6.6] that if $k$ is odd or $4\mid k$, then there are infinitely many $n$ with $F(n)=k$. If $k\equiv 2(\mathrm{mod}\, 4)$, then the equation $F(n)=k$ has infinitely many solutions $n$ or no solutions $n$ depending on whether $k=p-1$ for some prime $p$. In particular, the density of the range of $F$ is 3/4. It was also observed in [27, p. 277] that the *universal exponent* $L(n)$ for the group of reduced residues $a$ modulo $n$ for which $a^{n-1}\equiv 1(\mathrm{mod} n)$, is equal to $\mathrm{lcm}\{(p-1,n-1):\ p\mid n\}$, and that $L(n)=\lambda(n)$ if and only if $F(n)=\varphi(n)$. Moreover, $F(n)\mid\varphi(n)$ for all $n\ge 2$.

Applying Theorem 2.4 to the formula (2.18), we immediately get the following result.

**Proposition 2.71.** *A composite positive integer $n$ is a weak Carmichael number if and only if*

$$F(n) = \prod_{p|n}(p-1) \tag{2.20}$$

*where the product is taken over all primes $p$ such that $p \mid n$. Furthermore, a composite positive integer $n$ is a Carmichael number if and only if $F(n) = \varphi(n)$.*

The equality (2.19) immediately gives

$$f(n) = \prod_{p|n} \frac{\gcd(p-1, n-1)}{(p-1)p^{e_p-1}} \le \prod_{p|n} \frac{(p-1)}{(p-1)p^{e_p-1}} = \prod_{p|n} \frac{1}{p^{e_p-1}},$$

whence we have the following result.

**Corollary 2.72.** *Let $n > 1$ be a positive integer. Then*

$$f(n) \le \prod_{p|n} \frac{1}{p^{e_p-1}},$$

*where equality holds if and only if $n$ is a weak Carmichael number.*

Of course, it can be of interest to consider the function $f(n)$ restricted to the set of positive integers which are not $CN$. For this purpose, we will need the following definition.

**Definition 2.73.** Let $k \ge 2$ be a positive integer. An integer $n = p_1 p_2 \cdots p_s > 1$ with odd primes $p_1, p_2, \dots, p_s$ and $s \ge 2$, is said to be an *almost Carmichael number of order $k$* if the following conditions are satisfied:

(*i*) $p_j - 1 \mid k(n-1)$ for a fixed $j \in \{1, 2, \dots, s\}$,
(*ii*) $n - 1$ is divisible by $m(p_j - 1)$ for none $m \in \{1, \dots, k-1\}$ and
(*iii*) $p_i - 1 \mid n - 1$ for all $i \in \{1, 2, \dots, s\}$ such that $i \ne j$.

*Remark* **2.74.** A computation shows that there exist "numerous" almost Carmichael numbers of order 2. First notice that a product $pq$ of two distinct odd primes $p$ and $q$ with $p < q$ is an almost Carmichael number of order 2 if and only $q = 2p - 1$. Recall that such a $p$ is a *Sophie Germain-type prime*. Namely, if both $p$ and $2p + 1$ are primes, then $p$ is called a *Sophie Germain prime*, and it was conjectured that there are infinitely many Sophie Germain primes. Notice that this conjecture as well as the conjecture that there are infinitely many primes $p$ such that $2p - 1$ is also a prime, are particular cases of a more general *Prime-k-tuples conjecture* due to Dickson in 1904 (see e.g., [68, p. 250]). Furthermore, `Mathematica 8` gives numerous "three-component" almost Carmichael numbers of order 2 in the set $\{n : n = q_i q_j q_k \text{ and } 2 \le i < j < k \le 1000\}$.

Proposition 2.71, Corollary 2.72 and the formula (2.19) easily yield the following result.

**Proposition 2.75.** *The following assertions about a composite positive integer $n$ are true.*

(*i*) $f(n) \leq 1$, *and equality holds if and only if $n$ is a Carmichael number.*

(*ii*) *If $n$ is not a Carmichael number, then $f(n) \leq 1/2$ and equality holds if and only if $n$ is an almost Carmichael number of order* 2.

(*iii*) *If $n$ is neither a Carmichael number nor an almost Carmichael number of order* 2, *then $f(n) \leq 1/3$ and equality holds if and only if $n$ is an almost Carmichael number of order* 3 *or $n$ is a weak Carmichael number with the prime factorization $n = 3^2 p_2 \cdots p_s$, where $3 < p_2 < \cdots < p_s$ are odd primes.*

*Remark* **2.76.** If $n$ is a composite integer which is not $CN$, then by (ii) of Proposition 2.75 we have

$$F(n) \leq \frac{\varphi(n)}{2} \leq \frac{n-1}{2}. \tag{2.21}$$

This shows that for such a $n$, at least half of the integers $a$ in the interval $[1, n-1]$ are Fermat liars for $n$ (the so-called false witnesses for $n$ [27]). These facts lead to the folowing test: given a positive integer $n$, pick $k$ different positive integers less than $n$ and perform the Fermat primality test on $n$ for each of these bases; if $n$ is composite and it is not a Carmichael number, then the probability that $n$ passes all $k$ tests is less than $1/2^k$.

*Remark* **2.77.** Let $\mathcal{WCN}_3$ denote the set of all $WCN$ of the form $n = 3^2 p_2 \cdots p_s$, where $3 < p_2 < \cdots < p_s$ are odd primes. (cf. (iii) of Proposition 2.75). It is easy to see $45 = 3^2 \cdot 5$ is the only number in the set $\mathcal{WCN}_3$ whose prime factorization contains only one prime greater than 3. From Table 2 we see that up to $2 \cdot 10^6$ there are still six numbers belonging to the set $\mathcal{WCN}_3$; these numbers are $13833 = 3^2 \cdot 29 \cdot 53$, $203841 = 3^2 \cdot 11 \cdot 29 \cdot 71$, $321201 = 3^2 \cdot 89 \cdot 401$, $1080801 = 3^2 \cdot 29 \cdot 41 \cdot 101$ and $1658385 = 3^2 \cdot 5 \cdot 137 \cdot 269$. A computation shows that

$$\{9m : m = pq \text{ with } p \text{ and } q \text{ primes such that } 3 < p < q < 10^5\} \cap \mathcal{WCN}_3 = \Phi.$$

Furthermore, if $q_k$ denotes the $k$th prime, then the set $\{9m :\ m = q_i q_j q_k \text{ and } 2 \leq i < j < k \leq 1000\}$ contains the following five numbers of the set $\mathcal{WCN}_3$ which are greater than $2 \cdot 10^6$: $8074881 = 3^2 \cdot 17 \cdot 89 \cdot 593$, $19678401 = 3^2 \cdot 17 \cdot 41 \cdot 3137$, $95682861 = 3^2 \cdot 29 \cdot 53 \cdot 6917$, $359512011 = 3^2 \cdot 23 \cdot 467 \cdot 3719$ and $1955610801 = 3^2 \cdot 53 \cdot 1433 \cdot 2861$.

*Remark* **2.78.** If $n$ is a $CN$, then as noticed above $F(n) = \varphi(n)$. Erdős and Pomerance [27, Section 6] conjectured that not only are there infinitely many $CN$, but that

$$\limsup_{n \text{ composite}} \frac{F(n)}{n} = 1.$$

Notice that by [27, the estimate (2.8)], we have that $F(n)/n^{1-\varepsilon}$ is unbounded on the composites for any $\varepsilon > 0$. On the other hand, by [27, Theorem 6.1],

$$\limsup_{n \text{ composite}} \frac{F(n)\log^2 n}{n} > 0.$$

A computation (cf. Remark 2.77) suggests the following conjecture.

**Conjecture 2.79.** *Let $\mathcal{W}CN_3$ denote the set of all weak Carmichael numbers described in Remark* 2.77*. Then*

$$\limsup_{n\in\mathcal{W}CN_3} \frac{F(n)}{n} = \frac{1}{3}.$$

## 3. Proofs of Propositions 2.3, 2.60, 2.63 and Corollary 2.20

*Proof of Proposition* 2.3. Clearly, $\varphi(n)$ is even for each $n \geq 3$, and the set $R_n$ can be presented as

$$R_n = \{r_1, r_2, \dots, r_{\varphi(n)/2}, n - r_1, n - r_2, \dots, n - r_{\varphi(n)/2}\}. \tag{3.1}$$

Using (3.1) we find that

$$\sum_{\substack{\gcd(k,n)=1\\ 1\leq k\leq n-1}} k^{n-1} \equiv \sum_{i=1}^{\varphi(n)} r_i^{n-1} = \sum_{i=1}^{\varphi(n)/2} (r_i^{n-1} + (n-r_i)^{n-1}). \tag{3.2}$$

If $n$ is odd, the right hand side of (3.2) is

$$\equiv \sum_{i=1}^{\varphi(n)/2} (r_i^{n-1} + (-r_i)^{n-1}) \pmod{n} = 0 \pmod{n}.$$

Hence, every weak Carmichael number must be odd. Finally, if $n$ is odd, using (3.2), we have

$$\sum_{\substack{\gcd(k,n)=1\\ 1\leq k\leq n-1}} k^{n-1} = \sum_{i=1}^{\varphi(n)} r_i^{n-1} = \sum_{i=1}^{\varphi(n)/2} (r_i^{n-1} + (n-r_i)^{n-1}) \equiv 2\sum_{i=1}^{\varphi(n)/2} r_i^{n-1} \pmod{n}. \tag{3.3}$$

This together with Definition 2.1 concludes the proof. $\square$

*Proof of Proposition* 2.60. Applying the binomial formula and using the assumption that $n$ is an odd composite integer, we find that

$$\begin{aligned}\sum_{\substack{\gcd(k,n)\\ 1\le k\le n-1}} k^{n-1} &= \sum_{i=1}^{\varphi(n)} r_i^{n-1} = \sum_{i=1}^{\varphi(n)/2} \left(r_i^{n-1} + (n-r_i)^{n-1}\right)\\ &\equiv \sum_{i=1}^{\varphi(n)/2} r_i^{n-1} - \binom{n-1}{1} n \sum_{i=1}^{\varphi(n)/2} r_i^{n-2} + \sum_{i=1}^{\varphi(n)/2} r_i^{n-1} \pmod{n^2}\\ &= 2\sum_{i=1}^{\varphi(n)/2} r_i^{n-1} + n\sum_{i=1}^{\varphi(n)/2} r_i^{n-2} \equiv \varphi(n) \pmod{n^2}.\end{aligned}$$

This completes the proof. $\square$

*Proof of Corollary* 2.20. Given product $n = pq$ with primes $q < p$, using Fermat little theorem, the sum on the left right hand side of (2.8) in Definition 2.2 is

$$\begin{aligned}S(p,q) :&= \sum_{\substack{\gcd(k,pq)=1\\ 1\le k\le pq-1}} k^{pq-1} = \sum_{j=0}^{q-1}\sum_{i=jp+1}^{(j+1)p-1} i^{pq-1} - \sum_{\substack{s\equiv 0(\bmod q)\\ 1\le s\le p-1}} s^{pq-1}\\ &= \sum_{j=0}^{q-1}\sum_{i=jp+1}^{(j+1)p-1} i^{pq-1} - q^{pq-1}\sum_{i=1}^{p-1} i^{pq-1}\\ &\equiv q\sum_{i=1}^{p-1} i^{pq-1} - q^{pq-1}\sum_{i=1}^{p-1} i^{pq-1} \pmod{p}\\ &= q\sum_{i=1}^{p-1} i^{(p-1)q+(q-1)} - q^{(p-1)q+(q-1)}\sum_{i=1}^{p-1} i^{(p-1)q+(q-1)}\\ &\equiv q\sum_{i=1}^{p-1} i^{q-1} - q^{q-1}\sum_{i=1}^{p-1} i^{q-1} \pmod{p}\\ &= q(1-q^{q-2})\sum_{i=1}^{p-1} i^{q-1} \pmod{p}.\end{aligned} \tag{3.4}$$

Let $a$ be a generator of the multiplicative unit group of $\mathbb{Z}/p\mathbb{Z}$. Then since $q-1 < p-1$ it follows easily that the set $\{1^{q-1}, 2^{q-1}, \ldots, (p-1)^{q-1}\}$ regarding modulo $p$ conicides with the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ of all nonzero residues modulo $p$. This shows that

$$\sum_{i=1}^{p-1} i^{q-1} \equiv \sum_{i=1}^{p-1} i \pmod{p} = \frac{(p-1)p}{2} \equiv 0 \pmod{p}. \tag{3.5}$$

Taking (2.16) into (2.15), we immediately get

$$S(p,q) \equiv 0 \pmod{p}. \tag{3.6}$$

$$S(p,q) := \sum_{\substack{\gcd(k,pq)=1\\1\le k\le pq-1}} k^{pq-1} \equiv 0 \pmod{p}. \tag{3.7}$$

Since $\varphi(n) = (p-1)(q-1) \equiv 1 - q (\bmod\, p)$ from (2.18) we have

$$\sum_{\substack{\gcd(k,pq)=1\\1\le k\le pq-1}} k^{pq-1} - \varphi(pq) \equiv q - 1 \pmod{p}, \tag{3.8}$$

In view of the fact that $q < p$, we conclude that the expression on the left hand side of (2.19) is not divisible by $p$. Theefore, $n = pq$ is not a Carmichael number, and the proof is completed. □

*Proof of Proposition* 2.63. Using Euler totient theorem, we have

$$\sum_{\substack{1\le k\le p^f-1\\(k,p)=1}} k^{p^f-1} \equiv \sum_{\substack{1\le k\le p^f-1\\(k,p)=1}} \frac{1}{k^{p^{2f}-p^{2f-1}-p^f+1}} \pmod{p^{2f}}. \tag{3.9}$$

By the congruence (6) in [71], it follows that if $s$ in an even positive integer and $t = (\varphi(p^{2f}) - 1)s$ then

$$\sum_{\substack{1\le k\le p^f-1\\(k,p)=1}} \frac{1}{k^{p^{2f}-p^{2f-1}-p^f+1}} \equiv p^f B_t \pmod{p^{2f}} \tag{3.10}$$

where
(3.11)
$$t = (\varphi(p^{2f}) - 1)(p^{2f} - p^{2f-1} - p^f + 1) = (p^{2f} - p^{2f-1} - 1)(p^{2f} - p^{2f-1} - p^f + 1)$$

Comparing (3.10) and (3.11) gives

$$\sum_{\substack{1\le k\le p^f-1\\(k,p)=1}} k^{p^f-1} \equiv p^f B_t \pmod{p^{2f}} \tag{3.12}$$

with $t$ given by (3.12). Notice that by von Staudt-Clausen's theorem, the denominator $D_t$ of Bernoulli number $B_t = N_t/D_t$ is the product of all primes $p$ such that $p-1$ divides $t$. In particular, this shows that $p \parallel D_t$. From this and the congruence (3.13) we conclude that $\sum_{\substack{1\le k\le p^f-1\\(k,p)=1}} k^{p^f-1}$ is divisible by $p^{2f}$ if and only if $N_t$ is divisible by $p^{f+1}$. □

## 4. Proof of Theorem 2.4 and Corollary 2.17

Proof of Theorem 2.4 is based on the following three auxiliary results.

**Lemma 4.1.** *Let $p^e$ be a power of an odd prime $p$, and let me be a positive integer such that $m$ is not divisible by $p-1$. Then*

$$\sum_{\substack{1\le k\le p^e-1\\ \gcd(k,p)=1}} k^m \equiv 0 \pmod{p^e}. \tag{4.1}$$

*Proof.* Let $a$ be a primitive root modulo $p^e$. Then $a^m$ is not divisible by $p$. Moreover, it is easy to see that the set $\{aj:\, 1\le j\le p^e-1 \quad \text{and} \quad \gcd(j,p)=1\}$ reduced modulo $p^e$ coincides with the set of all residues modulo $p^e$ which are relatively prime to $p$. This shows that

$$a^m \sum_{\substack{1\le k\le p^s-1\\ \gcd(k,p)=1}} k^m = \sum_{\substack{1\le k\le p^e-1\\ \gcd(k,p)=1}} (ak)^m \equiv \sum_{\substack{1\le k\le p^e-1\\ \gcd(k,p)=1}} k^m \pmod{p^e},$$

whence it follows that

$$(a^m-1) \sum_{\substack{1\le k\le p^e-1\\ \gcd(k,p)=1}} k^m \equiv 0 \pmod{p^e}.$$

This together with the assumption that $a^m\not\equiv 1(\bmod\, p^e)$ immediately yields the desired congruence (4.1). $\square$

**Lemma 4.2.** *Let $n>1$ be a positive integer with a prime factorization $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ where $s\ge 2$. Let $R$ be a set of positive integers less than $n$ and relatively prime to $n$. For any fixed $i\in\{1,2,\ldots,s\}$ set*

$$R(p_i^{e_i})=\{a\in\mathbb{N}: 1\le a\le p_i^{e_i} \quad \text{and} \quad \gcd(a,p_i)=1\}.$$

*For all pairs $(i,j)$ with $i\in\{1,2,\ldots,s\}$ and $j\in R(p_i^{e_i})$ define the set $A_{ij}$ as*

$$A_{ij}=\{a\in R:\, a\equiv j(\bmod\, p_i^{e_i})\}.$$

*Then for any $i\in\{1,2,\ldots,s\}$*

$$|A_{ij}|=\varphi\left(\frac{n}{p_i^{e_i}}\right)=\prod_{\substack{1\le l\le s\\ l\ne i}}(p_l^{e_l}-p_l^{e_l-1}) \quad \text{for all} \quad j\in R(p_i^{e_i}), \tag{4.2}$$

*where $|S|$ denotes the cardinality of a finite set $S$.*

*Proof.* Clearly, it suffices to show that (4.2) is satisfied for $i=1$. Then for any fixed $j\in R(p_1^{e_1})$ consider the set

$$T_j=\{j+rp_1^{e_1}:\, r=0,1,\ldots,\frac{n}{p_1^{e_1}}-1(=p_2^{e_2}\cdots p_s^{e_s}-1)\}.$$

Since for each $t\in T_j$, $j\le t\le j+p_1^{e_1}\left(\frac{n}{p_1^{e_1}}-1\right)\le n-1$, it follows that the set $A_{1j}$ actually consists of these elements in $T_j$ that are relatively prime to $n/p_1^{e_1}$. Notice that the set $T_j$ reduced modulo $n/p_1^{e_1}$ coincides with the set

$\{0,1,2,\ldots,n/p_1^{e_1}-1\}$ of all residues modulo $n/p_1^{e_1}$; namely, if $j+r_1p_1^{e_1} \equiv j+r_2p_1^{e_1} (\bmod n/p_1^{e_1})$ with $0 \le r_1 < r_2 \le n/p_1^{e_1}-1$, then $n/p_1^{e_1} \mid (r_2-r_1)p_1^{e_1}$, and so, $n/p_1^{e_1} \mid (r_2-r_1)$ which is impossible because of $1 \le r_2-r_1 \le n/p_1^{e_1}-1$. This shows that the set $A_{1j}$ contains exactly $\varphi(n/p_1^{e_1})$ elements, which is equal to $(p_2^{e_2}-p_2^{e_2-1})\cdots(p_s^{e_s}-p_s^{e_s-1})$. This completes the proof. □

**Lemma 4.3.** *Let $n$ and $e$ be positive integers and let $p$ be a prime such that $p^e \mid n$ and $p-1 \mid n-1$. Then*

$$k^{n-1} \equiv k^{p^{e-1}-1} \pmod{p^e} \tag{4.3}$$

*for every integer $k$ that is not divisible by $p$.*

*Proof.* Take $n = p^e n'$ with an integer $n'$. Then from the assumption $p-1 \mid n-1$ it follows that $n' \equiv 1 (\bmod (p-1))$, and therefore

$$n-1 = p^e n' - 1 \equiv p^{e-1}-1 \pmod{p^{e-1}(p-1)}.$$

If $k$ is not divisible by $p$, then from the above congruence, the fact that $\varphi(p^e) = p^{e-1}(p-1)$ and Euler totient theorem, we have $k^{p^{e-1}-1} \equiv k^{n-1} (\bmod p^e)$ which immediately implies (4.3). □

**Lemma 4.4.** *Let $n > 1$ be a positive integer with a prime factorization $n = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$. For any fixed $i \in \{1,2,\ldots,s\}$, set*

$$R(p_i^{e_i}) = \{a \in \mathbb{N} : 1 \le a \le p_i^{e_i} \quad \textit{and} \quad \gcd(a,p_i) = 1\}.$$

*Then for every $i \in \{1,2,\ldots,s\}$ there holds*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi\left(\frac{n}{p_i^{e_i}}\right) \sum_{k\in R(p_i^{e_i})} k^{n-1} \pmod{p_i^{e_i}}. \tag{4.4}$$

*If in addition, $p_i - 1 \mid n-1$ for some $i \in \{1,2,\ldots,s\}$, then*

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} \equiv \varphi\left(\frac{n}{p_i^{e_i}}\right) \sum_{k\in R(p_i^{e_i})} k^{p_i^{e_i-1}-1} \pmod{p_i^{e_i}}. \tag{4.5}$$

*Proof.* Consider the set $R$ of all reduced residues modulo $n$ that are relatively prime to $n$, i.e.,

$$R = \{k:\ 1 \le k \le n-1 \text{ and } \gcd(k,n) = 1\}.$$

Let $i \in \{1,2,\ldots,m\}$ be any fixed. For each $j \in R(p_i^{e_i})$ take

$$A_{ij} = \{a \in R:\ a \equiv j (\bmod p_i^{e_i})\}.$$

Then by Lemma 4.2,

$$|A_{ij}| = \varphi\left(\frac{n}{p_i^{e_i}}\right) \quad \text{for all} \quad j \in R(p_i^{e_i}). \tag{4.6}$$

Furthermore, using (4.3) and (4.1) of Lemma 4.1 with $s = n-1$, we have

$$\begin{aligned}\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1} &= \sum_{k\in R} k^{n-1} = \sum_{j\in R(p_i^{e_i})}\sum_{k\in A_{ij}} k^{n-1}\\ &\equiv \varphi\left(\frac{n}{p_i^{e_i}}\right)\sum_{k\in R(p_i^{e_i})} k^{n-1} \pmod{p_i^{e_i}}.\end{aligned}$$

The above congruence implies (4.4). Finally, if $p_i - 1 \mid n-1$ then substituting (4.3) of Lemma 4.3 with $p_i^{e_i}$ instead of $p^e$ into (4.4) we immediately obtain (4.5). $\square$

**Lemma 4.5.** *Let $n$ be a composite positive integer with the prime factorization $n = p_1^{e_1}\cdots p_s^{e_s}$. For any fixed $i \in \{1,2,\ldots,s\}$ take*

$$R(p_i^{e_i}) = \{a \in \mathbb{N} : 1 \le a \le p_i^{e_i} \quad \textit{and} \quad \gcd(a,p_i) = 1\}.$$

*Then $n$ is a weak Carmichael number if and only if for every $i \in \{1,2,\ldots,s\}$ there holds*

$$\left(\sum_{k\in R(p_i^{e_i})} k^{n-1} + p_i^{e_i-1}\right)\varphi\left(\frac{n}{p_i^{e_i}}\right) \equiv 0 \pmod{p_i^{e_i}}. \tag{4.7}$$

*Proof.* Clearly, $n = p_1^{e_1}\cdots p_s^{e_s}$ is a weak Carmichael number if and only if (2.2) is satisfied modulo $p_i^{e_i}$ for all $i = 1,\ldots,s$ which is by (4.3) of Lemma 4.3 (4.4) of Lemma 4.4 equivalent to the congruence

$$\varphi\left(\frac{n}{p_i^{e_i}}\right)\sum_{k\in R(p_i^{e_i})} k^{n-1} \equiv \varphi(n) \pmod{p_i^{e_i}}. \tag{4.8}$$

Since $\varphi(n) = (p_i^{e_i} - p_i^{e_i-1})\varphi(n/p_i^{e_i}) \equiv -p_i^{e_i-1}\varphi(n/p_i^{e_i}) (\bmod\, p_i^{e_i})$, substituting this into (4.8), we immediately obtain (4.7). $\square$

**Lemma 4.6.** *Let $p \ge 3$ be a a prime and let $e \ge 2$ be a positive integer. Define*

$$R(p^e) = \{a \in \mathbb{N} :\, 1 \le a \le p^e \quad \textit{and} \quad \gcd(a,p) = 1\}.$$

*Then*

$$\sum_{k\in R(p^e)} k^{p^{e-1}-1} \equiv \sum_{k=1}^{p^e-1} k^{p^{e-1}-1} \pmod{p^e}. \tag{4.9}$$

*Proof.* From the obvious inequality $p^{e-1} - 1 \ge e$ with $p \ge 3$ and $e \ge 2$ we see that every term in the sum on the right hand side of (4.9) that is divisible by $p$ is also divisible by $p^e$. This yields the desired congruence (4.9). $\square$

The following congruence is known as a *Carlitz-von Staudt's result* [16] in 1961 (for an easier proof see [57, Theorem 3]).

**Lemma 4.7.** *Let $p\ge 3$ be a a prime and let $e$ and $l$ be positive integers such that $p-1$ does not divide $l$. Then*

$$\sum_{k\in R(p^e)} k^l \equiv 0 \pmod{p^e}. \tag{4.10}$$

*Proof.* By a particular case of a result obtained in 1955 by H.J.A. Duparc and W. Peremans [23, Theorem 1] (cf. [71, Corollary 2] or [52, the congruence (58) in Section 8]), if $r$ is a positive integer such that $p-1$ does not divide $r$, then

$$\sum_{k\in R(p^e)} \frac{1}{k^r} \equiv 0 \pmod{p^e}. \tag{4.11}$$

Letting $r=\varphi(p^e)-l=p^e-p^{e-1}-l$ in (4.11) and then applying Euler totient theorem modulo $p^e$, we immediately obtain (4.10). $\square$

**Lemma 4.8.** ([16], [57, Theorem 3]) *Let $l$ and $m\ge 2$ be positive integers. Then*

$$S_l(m):=\sum_{i=1}^{m-1} i^l \equiv \begin{cases} 0 \pmod{\frac{(m-1)m}{2}} & if\ l\ is\ odd \\ -\sum_{(p-1)\mid l,\, p\mid m} \frac{m}{p} \pmod{m} & if\ l\ is\ even \end{cases} \tag{4.12}$$

*where the summation is taken over all primes $p$ such that $(p-1)\mid l$ and $p\mid m$.*

*Proof of Theorem* 2.4. First assume that $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ is a composite integer such that $p_i-1\mid n-1$ for all $i=1,2,\ldots,s$. Then by Lemma 4.5 $n$ is a weak Carmichael number if for every $i\in\{1,2,\ldots,s\}$ there holds

$$\sum_{k\in R(p_i^{e_i})} k^{n-1}+p_i^{e_i-1}\equiv 0 \pmod{p_i^{e_i}}. \tag{4.13}$$

For any fixed $i\in\{1,2,\ldots,s\}$ consider two cases: $e_i=1$ and $e_i\ge 2$.

*Case* 1. $e_i=1$. Then since $n-1\equiv 0 (\bmod\, (p-1))$, using Fermat little theorem, we obtain

$$\sum_{k\in R(p_i)} k^{n-1}+p_i^{1-1}=\sum_{k=1}^{p_i-1} k^{n-1}+1\equiv (p_i-1)+1\equiv 0 \pmod{p_i}. \tag{4.14}$$

Therefore, (4.13) is satisfied.

*Case* 2. $e_i\ge 2$. Then using (4.3) of Lemma 4.3 and (4.10) of Lemma 4.7, with the notations of Lemma 4.4, for any fixed $i\in\{1,2,\ldots,s\}$ we have

$$\begin{aligned}\sum_{k\in R(p_i^{e_i})} k^{n-1} &\equiv \sum_{k\in R(p_i^{e_i})} k^{p_i^{e_i-1}-1} \pmod{p_i^{e_i}}\\ &\equiv \sum_{k=1}^{p_i^{e_i}-1} k^{p_i^{e_i-1}-1} \pmod{p_i^{e_i}}.\end{aligned} \tag{4.15}$$

Furthermore, by the second congruence of (4.12) of Lemma 4.8 (cf. [38, Lemma 1]), we immediately get

$$\sum_{k=1}^{p_i^{e_i}-1} k^{p_i^{e_i-1}-1} \equiv -\frac{p_i^{e_i}}{p_i} = -p_i^{e_i-1} \pmod{p_i^{e_i}}. \tag{4.16}$$

Comparing (4.15) and (4.16) immediately gives (4.13), and therefore, $n$ is a weak Carmichael number.

Conversely, suppose that $n$ is a weak Carmichael number with a prime factorization $n = p_1^{e_1} \cdots p_s^{e_s}$ where $p_1, \dots, p_s$ are odd primes. Suppose that for some $i \in \{1, 2, \dots, s\}$, $n-1$ is not divisible by $p_i - 1$. Then by (4.10) of Lemma 4.7, we have

$$\sum_{k \in R(p_i^{e_i})} k^{n-1} \equiv 0 \pmod{p^e}. \tag{4.17}$$

Substituting (4.17) in (4.7) of Lemma 4.5, we get

$$p_i^{e_i-1} \varphi\left(\frac{n}{p_i^{e_i}}\right) \equiv 0 \pmod{p_i^{e_i}}, \tag{4.18}$$

or equivalently,

$$\varphi\left(\frac{n}{p_i^{e_i}}\right) \equiv 0 \pmod{p_i}. \tag{4.19}$$

The above congruence implies that $p_i \mid \prod_{\substack{1 \le j \le s \\ j \ne i}} p_j^{e_j-1}(p_j - 1)$. It follows that $p_i \mid p_j - 1$ for some $j \ne i$.

We can choose such a $p_i$ to be maximal, i.e.,

$$p_i = \max_{1 \le t \le s} \{p_t : n - 1 \not\equiv 0 \pmod{p_t - 1}\}.$$

Then, as it is proved previously, we must have $p_i \mid p_j - 1$ for some $j \ne i$. It follows that $p_i < p_j$, and hence, by the maximality of $p_i$ we conclude that $p_j - 1 \mid n - 1$. Therefore, $p_i \mid n - 1$, which is impossible because of $p_i \mid n$. A contradiction, and hence $n - 1$ is divisible by $p_i - 1$ for each $i = 1, 2, \dots, s$. This completes the proof of Theorem 2.4. $\square$

*Proof of Corollary* 2.17. If $n$ is a weak Carmichael number that is not Carmichael number, then $\mu(n) = 0$, and hence the congrueence in Corollary 2.17 reduced to the congruence (2.2).

Conversely, if $n > 1$ satisfies the congruence

$$\sum_{\substack{\gcd(k,n)=1 \\ 1 \le k \le n-1}} k^{n-1} \equiv \varphi(n) + \mu(n) \pmod{n}, \tag{4.20}$$

then consider two cases: 1) $n$ is not square-free and 2) $n$ is square-free. In the first case (4.20) becomes

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}\equiv \varphi(n) \pmod{n}, \tag{4.21}$$

whence using Theorem 2.4 we conclude that $n$ is a weak Carmichael number.

In the second case, we have $\mu(n)=\pm 1$, and then (4.20) becomes

$$\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}\equiv \varphi(n)\pm 1 \pmod{n}. \tag{4.22}$$

In view of Corollary 2.16, the above congruence shows that $n$ is not a weak Carmichael number. Then by Theorem 2.4 there exists a prime factor $p$ of $n$ such that $p-1$ does not divide $n-1$. Asuume that $n=p^e n'$ with $n'$ such that $p$ does not divide $n$. Then applying (4.4) and Fermat little theorem, we find that

$$\begin{aligned}\sum_{\substack{\gcd(k,n)=1\\ 1\le k\le n-1}} k^{n-1}&\equiv \varphi\left(\frac{n}{p^e}\right)\sum_{k\in R(p^e)} k^{n-1} \pmod{p}\\ &\equiv \varphi\left(\frac{n}{p^e}\right)|R(p^e)|=\varphi\left(\frac{n}{p^e}\right)\varphi(p^e)=\varphi(n) \pmod{p}.\end{aligned} \tag{4.23}$$

Substituting the congruence (4.23) into (4.22) reduced modulo $p$, we obtain $0\equiv \pm 1 (\bmod\, p)$. A contradiction, and hence, $n$ is a weak Carmichael number which is not a Carmichael number. This concludes the proof. □

## References


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

[2] W.R. Alford, J. Grantham, S. Hayman and A. Shallue, Constructing Carmichael numbers through improved subset-product algorihms, to appear in *Math. Comp.*; preprint `arXiv:1203.6664v1 [math.NT]`, March 2012.

[3] W.R. Alford, A. Granville and C. Pomerance, On the difficulty of finding reliable witnesses, Algorithmic number theory (Ithaca, NY, 1994), *Lecture Notes in Comput. Sci.* vol. 877, Springer, Berlin, 1994, 1994, pp. 1–16.

[4] T. Agoh, On Giuga's conjecture, *Manuscripta Math.* **87** (1995), 501–510.

[5] R. Balasubramanian and S.V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997), 1705–1708.

[6] R. Baillie and S.S. Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.* **35** (1980), 1391–1417.

[7] W.D. Banks and C. Pomerance, On Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* **88** (2010), 313–321.

[8] A.F. Beardon, Sums of powers of integers, *Amer. Math. Monthly* **103** (1996), 201–213.

[9] E. Bedocchi, Nota ad una congettura sui numeri primi, *Riv. Mat. Univ. Parma* **11** (1985), 229–236.

[10] J. Bernoulli, *Ars Conjectandi*, Basel, 1713.

[11] C.B. Boyer, Pascal's formula for the sums of powers of the integers, *Scripta Math.* **9** (1943), 237–244.

[12] P.S. Bruckman, *Problem*, *Amer. Math. Monthly* **92** (1985), p. 434.

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

[14] J.M. Borwein, M. Skerritt and C. Maitland, Computation of an improved lower bound to Giuga's primality conjecture, preprint 2013, `http://www.carma.newcastle.edu.au/jon/`.

[15] J.M. Borwein and E. Wong, *A survey of results relating to Giuga's conjecture on primality*, Proceedings of the 25th Anniversary Conference of the Centre de Récherches Mathématiques, CECM Preprint Series, 95-035:1–23, 1995; available at `http://discerver.carma.newcastle.edu.au/101/`.

[16] L. Carlitz, The Staudt-Clausen theorem, *Math. Mag.* **34** (1960/1961), 131–146.

[17] R.D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1910), No. 5, 232–238.

[18] R.D. Carmichael, On composite numbers $P$ which satisfy the Fermat congruence $a^{P-1} \equiv 1(\bmod P)$, *Amer. Math. Monthly* **19** (1912), 22–27.

[19] J. Chernick, On Fermat's simple theorem, *Bull. Amer. Math. Soc.* **45** (1939), 269–274.

[20] T. Clausen, Lehrsatz aus einer Abhandlung über die Bernoullischen Zahlen, *Astron. Nach.* **17** (1840), 351–352.

[21] L.E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Mathematics* **33** (1904), 155–161.

[22] H. Dubner, Carmichael numbers of the form $(6m+1)(12m+1)(18m+1)$, *J. Integer Seq.* **5** (2002), Article 02.2.1.

[23] H.J.A. Duparc and W. Peremans, On theorems of Wolstenholme and Leudesdorf, Koninkl. Nederl. Akademie Van Wetenschappen-Amsterdam. Reprinted from Proceedings knaw Series A, 58 (1955), No. 4 and *Indag. Math.* **17** (1955), 459–465.

[24] A.W.F. Edwards, A quick route to sums of powers, *Amer. Math. Monthly* **93** (1986), 451–455.

[25] P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc. (N.S.)* **12** (1948), 75–78.

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

[27] P. Erdős and C. Pomerance, On the numbers of false witnesses for a composite number, *Math. Comp.* **46** (1986), 259–279.

[28] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 363–385.

[29] Everet W. Howe, Higher-order Carmichael numbers, *Math. Comp.* **69** (2000), 1711–1719.

[30] J. Faulhaber, *Academia Algebrae*, Darinnen die miraculosische Inventiones zu den höchsten Cossen weiters *continuirt* und *profitiert* werden, Augspurg, bey Johann Ulrich Schönigs, 1631.

[31] C. F. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801 (translated into English by A. C. Clarke, New Haven, CT: Yale University Press, 1966.)

[32] G. Giuga, Su una presumibile proprietà caratteristica dei numeri primi, *Ist. Lombardo Sci. Lett. Rend. A* **83** (1950), 511–528.

[33] R.L. Graham, D.E. Knuth and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley Publishing Company, 1989.

[34] A. Granville, It is easy to determine whether a given integer is prime, *Bull. Amer. Math. Soc.* **42**, (2004), No. 1, 3–38.

[35] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2001), 883–908.
[36] J.M. Grau and A.M. Oller-Marcén, Generalizing Giuga's conjecture; preprint `arXiv:1103.3483v1 [math.NT]`, March 2011.
[37] J.M. Grau and A.M. Oller-Marcén, On $k$-Lehmer numbers, Integers **12** (2012), No. A37, 9 pages.
[38] J.M. Grau and A.M. Oller-Marcén, About the congruence $\sum_{k=1}^{n} k^{f(n)} \equiv 0 (\bmod n)$, submitted.
[39] J.M. Grau, F. Luca and A.M. Oller-Marcén, On a variant of Giuga numbers, *Acta Math. Sin.* (*Engl. Ser.*) **28**, No. 4 (2012), 653–660; preprint `arXiv:1103.3428v1 [math.NT]`, March 2011.
[40] G.H. Hardy, *Ramanujan: Twelve Lectures on Subject Suggested by His Life and Works*, 3rd ed., Chelsea, 1999.
[41] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1979.
[42] G. Harman, On the number of Carmichael numbers up to $x$, *Bull. London Math. Soc.* **37** (2005), 641–650.
[43] G. Harman, Watt's mean value theorem and Carmichael numbers, *Int J. Number Theory* **4** (2008), 241–248.
[44] G. Jaeschke, The Carmichael numbers up to $10^{12}$, *Math. Comp.* **55** (1990), 383–389.
[45] B.C. Kellner, 'Über irreguläre Paare höherer Ordnungen', `http://www.bernoulli.org/~bk/irrpairord.pdf`, 2002.
[46] B.C. Kellner, The equivalence of Giuga's and Agoh's conjectures; preprint `arXiv:math/0409259v1` [math.NT], 2004.
[47] A. Korselt, Problème chinois, *L'intermédiaire des mathematiciens* **6** (1899), 142–143.
[48] D.H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932), No. 10, 745–751.
[49] G. Löh and G. Niebuhr, A new algorithm for constructing large Carmichael numbers, *Math. Comp.* **65** (1996), 823–836.
[50] F. Luca and C. Pomerance, On composite integers $n$ for which $\varphi(n) \mid n-1$, *Bol. Soc. Mat. Mexicana* **17** (2011), 13–21.
[51] F. Luca, C. Pomerance and I. Shparlinski, On Giuga numbers, *Int. J. Mod. Math.* **4** (2009), 13–18.
[52] R. Meštrović, Wolstenholme's theorem: Its Generalizations and Extensions in the last hundred and fifty years (1862–2012); preprint `arXiv: 0911.4433v3 [math.NT]`, December 2011.
[53] R. Meštrović, A congruence modulo $n^3$ involving two consecutive sums of powers and its applications; prprint `arXiv: 1211.15470 [math.NT]`, November 2012.
[54] R. Meštrović, *Some identities in commutative rings with unity and their applications applications*, 11 pages, submitted in *Bull. Korean Math. Soc.*
[55] N. Mcnew, Radically weakening the Lehmer and Carmichael conditions; preprint `arXiv:1210.2001v1 [math.NT]`, October 2012.
[56] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms, *Theoret. Comput. Sci.* **12**, No. 1 (1980), 97–108.
[57] P. Moree, A top hat for Moser's four mathemagical rabbits, *Amer. Math. Monthly* **118** (2011), 364–370.
[58] O. Ore, *Number Theory and its History*, McGraw-Hill New York, 1948.
[59] H. Pan and Z.-W. Sun, New identities involving Bernoulli and Euler polynomials, *J. Combin. Theory Ser. A* **113** (2006), 156–175.

[60] B. Pascal, Sommation des puissances numérique , in *Oeuvres completè s*, vol. III, Jean Mesnard, ed., Desclée-Brouwer, Paris, 1964, 341–367; English translation by A. Knoebel, R. Laubenbacher, J. Lodder, and D. Pengelley, Sums of numerical powers, in *Mathematical Masterpieces: Further Chronicles by the Explorers*, Springer-Verlag, New York, 2007, 32–37.

[61] R.G.E. Pinch, A note on Lehmers totient problem, *Poster presented in* ANTS VII, `http://www.math.tu.-berlin.de/kant/ants/Poster/PinchPoster3.pdf`, 2006.

[62] R.G.E. Pinch, The Carmichael numbers up to $10^{15}$ *Math. Comp.* **61** (1993), 381–391 (Lehmer memorial issue).

[63] R.G.E. Pinch, The Carmichael numbers up to $10^{18}$; preprint `arXiv:math/0604376v1 [math.NT]`, 2006;
`www.chalcedon.demon.co.uk/rgep/carpsp.html`

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

[65] C. Pomerance, On the distribution of pseudoprimes, *Math. Comp.* **37** (1981), 587–593.

[66] C. Pomerance, Two methods in elementary number theory, Number Theory and Applications (Banff, 1988; R.A. Mollin, ed.) *NATO Adv. Sci. Ser. C* **265** (1989), 135–161.

[67] C. Pomerance, J.L. Selfridge and Samuel S. Wagstaff, The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.* **35**, No. 151 (1980), 1003–1026.

[68] P. Ribenboim, 13 *The Little Book of Bigger Primes*, second edition, Springer-Verlag, New York, 2004.

[69] J. Sándor and B. Crstici, *Handbook of Number Theory* II, Kluwer Academic Publishers, Dordrecht, 2004.

[70] D. Shanks, *Solved and unsolved problems in number theory*, 3rd ed., Chelsea, New York, 1985.

[71] I.Sh. Slavutskii, Leudesdorf's theorem and Bernoulli numbers, *Arch. Math.* (*Brno*) **35** (1999), 299–303.

[72] N.J. Sloane, *The On-Line Encyclopedia of Integer Sequences.*

[73] K.G.C. von Staudt, Beweis eines Lehrsatzes die Bernoulli'schen Zahlen betreffend, *J. Reine Angew. Math.* **21** (1840), 372–374.

[74] G.A. Steele, Carmichael numbers in number rings, *J. Number Theory* **128** (2008), No. 4, 910–917.

[75] Z.-H. Sun, Congruences for Bernoulli numbers and Bernoulli polynomials, *Discrete Math.* **163** (1997), 153–163.

[76] Z.-W. Sun and H. Pan, Identities concerning Bernoulli and Euler polynomials, *Acta Arith.* **125** (2006), 21–39.

[77] J.D. Swift, Review 13[9] - table of Carmichael numbers to $10^9$, *Math. Comp.* **29** (1975), 338–339.

[78] E.W. Weinstein, Carmichael number, http://mathworld.wolfram.com/CarmichaelNumber.html.

[79] E. Wong, *Computations on Normal Families of Primes*, *MSc Thesis*, Simon Fraser University, 1997; available at `http://discerver.carma.newcastle.edu.au/view/year/1997.html`.

[80] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, to appear in *Bull. London Math. Soc.*; preprint `arXiv:1212.5850v1 [math.NT]`, December 2012.

[81] M.Z. Zhang, A method for finding large Carmichael numbers, *Sichuan Daxue Xuebao* **29** (1992), no. 4, 472–479.

[82] V. Tipu, A note on Giuga's conjecture, *Canad. Math. Bull.* **50** (2007), 158–160.

Maritime Faculty, University of Montenegro, Dobrota 36, 85330 Kotor, Montenegro
*E-mail address*: romeo@ac.me