Journal of Integer Sequences, Vol. 23 (2020),
Article 20.10.6

Carmichael Numbers for $\mathrm{GL}(m)$

Eugene Karolinsky and Dmytro Seliutin
Department of Pure Mathematics
Kharkiv National University
Ukraine
ekarolinsky@univer.kharkov.ua
selyutind1996@gmail.com

Abstract

We propose a generalization of Carmichael numbers, where the multiplicative group $\mathbb{G}_m = \mathrm{GL}(1)$ is replaced by $\mathrm{GL}(m)$ for $m \geq 2$. We prove basic properties of these families of numbers and give some examples.

1 Introduction

Recall that a composite number $n \in \mathbb{N}$ is called *Carmichael* if $a^{n-1} \equiv 1 \pmod{n}$ for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. In other words, Carmichael numbers are Fermat pseudoprimes to all values of a that are coprime to n. Alford, Granville, and Pomerance [1] proved that there are infinitely many Carmichael numbers.

Recently, various generalizations and analogues of Carmichael numbers were proposed, see, e.g., [3, 5, 7] and references therein. In this paper, we introduce another analogue of Carmichael numbers, where the multiplicative group $\mathbb{G}_m = \mathrm{GL}(1)$ is replaced by $\mathrm{GL}(m)$ for $m \geq 2$. Namely, we start with the exponent $K_m(p)$ of the group $\mathrm{GL}(m, \mathbb{F}_p)$, extrapolate it naturally to all naturals as $K_m(n)$, and then define a composite number $n \in \mathbb{N}$ to be m-Carmichael if $A^{K_m(n)} = I$ for all $A \in \mathrm{GL}(m, \mathbb{Z}/n\mathbb{Z})$. Thus, the "classical" Carmichael numbers can be recovered as 1-Carmichael numbers.

We study basic properties of m-Carmichael numbers, including an analogue of Korselt's criterion for a number to be Carmichael in terms of its prime divisors. This criterion appears to be practical for numbers of reasonable size. Using this, we compute all m-Carmichael numbers less than or equal to 10^5 for $2 \leq m \leq 10$. Also, we describe the structure of m-Carmichael numbers with given prime factors.

Some properties of m-Carmichael numbers for $m \geq 2$ appear to be rather different from those of the "classical" Carmichael numbers. Namely, m-Carmichael numbers for $m \geq 2$ can be non-squarefree or even. Moreover, all prime powers are m-Carmichael for $m \geq 2$. Possible explanation of these phenomena is the fact that the groups $\mathrm{GL}(m)$ for $m \geq 2$ contain (many copies of) the additive group $\mathbb{G}_a$.

The paper is organized as follows. In Section 2, we define m-Carmichael numbers and discuss their basic properties. The main result of the paper is Theorem 8, an analogue of Korselt's criterion for m-Carmichael numbers. In Section 3, we consider the distribution of m-Carmichael numbers with prescribed prime factors, give several particular examples, and summarize the general pattern in Theorem 16. In Section 4, we list some open questions and discuss possible generalizations. In Appendix, we describe our computations of relatively small m-Carmichael numbers.

Throughout this paper, p denotes a prime number. In particular, $\prod_{p|n}$ stands for a product taken over all prime divisors of n.

2 m-Carmichael numbers

Let $\Phi_k(X)$ be the kth cyclotomic polynomial. The following proposition is well known, but for the reader's convenience we provide a proof.

Proposition 1. *If $a \in \mathbb{Z}$, then*

$$\operatorname{lcm}(a-1, a^2-1, \ldots, a^m-1) = \prod_{k=1}^{m} \Phi_k(a).$$

Proof. We proceed by induction with the obvious base. We have

$$\operatorname{lcm}(a-1, a^2-1, \ldots, a^m-1) = \operatorname{lcm}\left(\prod_{k=1}^{m-1} \Phi_k(a), a^m-1\right) =$$

$$\left(\prod_{d|m, d<m} \Phi_d(a)\right) \cdot \operatorname{lcm}\left(\prod_{k\nmid m, k<m} \Phi_k(a), \Phi_m(a)\right).$$

By [2, Theorem 5] we have $\gcd\left(\Phi_k(a), \Phi_l(a)\right) = 1$ unless $\frac{k}{l}$ is a prime power. Therefore,

$$\gcd\left(\prod_{k\nmid m, k<m} \Phi_k(a), \Phi_m(a)\right) = 1,$$

and

$$\operatorname{lcm}\left(\prod_{k\nmid m, k<m} \Phi_k(a), \Phi_m(a)\right) = \Phi_m(a) \prod_{k\nmid m, k<m} \Phi_k(a),$$

which finishes the proof. □

Recall that the *exponent* of a (finite) group G is the least common multiple of orders of elements of G.

Theorem 2. [4, 6] *The exponent of* $\mathrm{GL}(m, \mathbb{F}_p)$ *equals*

$$p^{\lceil \log_p m \rceil} \operatorname{lcm}(p-1, p^2-1, \ldots, p^m-1) = p^{\lceil \log_p m \rceil} \prod_{k=1}^{m} \Phi_k(p).$$

From now on we assume that $m \geq 2$. Notice that if $p \geq m$, then the exponent of $\mathrm{GL}(m, \mathbb{F}_p)$ equals $p \cdot \prod_{k=1}^{m} \Phi_k(p)$.

Let us introduce the following notation:

$$D_m(n) = \prod_{k=1}^{m} \Phi_k(n),$$

$$\nabla_m(n) = \prod_{p \mid n} p^{\lceil \log_p m \rceil - 1},$$

$$K_m(n) = n \nabla_m(n) D_m(n).$$

In this notation, the exponent of $\mathrm{GL}(m, \mathbb{F}_p)$ equals $K_m(p)$.

Notice also that if $p \geq m$, then $p^{\lceil \log_p m \rceil - 1} = 1$. Therefore,

$$\nabla_m(n) = \prod_{p \mid n,\ p < m} p^{\lceil \log_p m \rceil - 1}.$$

Example 3.

(a) For $m = 2$, we have $\nabla_2(n) = 1$, $D_2(n) = (n-1)(n+1)$. Thus $K_2(n) = n(n-1)(n+1)$.

(b) For $m = 3$, we have $\nabla_3(n) = 1$ for n odd, $\nabla_3(n) = 2$ for n even, and $D_3(n) = (n-1)(n+1)(n^2+n+1)$. Therefore, $K_3(n) = n(n-1)(n+1)(n^2+n+1)$ for n odd and $K_3(n) = 2n(n-1)(n+1)(n^2+n+1)$ for n even.

Definition 4. A composite number $n \in \mathbb{N}$ is called an *m-Carmichael number* if $A^{K_m(n)} = I$ for all $A \in \mathrm{GL}(m, \mathbb{Z}/n\mathbb{Z})$.

First, we show that any prime power is an m-Carmichael number. For this purpose, we need two simple lemmas.

Lemma 5. *If* $a \in \mathbb{Z}$, $k \in \mathbb{N}$, *then* $D_m(a) \mid D_m(a^k)$.

Proof. Consider $D_m(X) = \prod_{k=1}^{m} \Phi_k(X) \in \mathbb{Z}[X]$. Since all roots of $D_m(X)$ are simple, and each root of $D_m(X)$ is a root of $D_m(X^k)$, we have $D_m(X) \mid D_m(X^k)$. Since the polynomial $D_m(X)$ is monic, this implies the lemma. □

Lemma 6. *Let $B \in \mathrm{Mat}(m, \mathbb{Z})$, $B \equiv I \pmod p$. Then for any $k \in \mathbb{N}$ we have $B^{p^{k-1}} \equiv I \pmod{p^k}$.*

Proof. We use induction by k with the obvious base. Let $B^{p^{k-1}} = I + p^k C$. Then, by the binomial theorem, we have

$$B^{p^k} = (I + p^k C)^p = I + p^{k+1} C + \sum_{l=2}^{p} p^{kl} \binom{p}{l} C^l \equiv I \pmod{p^{k+1}}.$$

□

Proposition 7. *If $k \in \mathbb{N}$, $k > 1$, then p^k is an m-Carmichael number.*

Proof. Let $A \in \mathrm{Mat}(m, \mathbb{Z})$, $\gcd(\det A, p) = 1$. By Theorem 2, we have $B := A^{K_m(p)} \equiv I \pmod p$. Therefore, by Lemma 6 we have $B^{p^{k-1}} \equiv I \pmod{p^k}$. Since $\nabla_m(p^k) = \nabla_m(p)$ and, by Lemma 5, $D_m(p) \mid D_m(p^k)$, the equation $B^{p^{k-1}} = A^{p^k \nabla_m(p) D_m(p)} \equiv I \pmod{p^k}$ implies $A^{K_m(p^k)} = A^{p^k \nabla_m(p^k) D_m(p^k)} \equiv I \pmod{p^k}$. □

Now we present the main theorem of the paper, an analogue of Korselt's criterion for a number to be m-Carmichael.

Theorem 8. *Let $n \in \mathbb{N}$ be composite. The following are equivalent:*
(1) n is an m-Carmichael number,
(2) if $p \mid n$, then $D_m(p) \mid K_m(n)$.

Proof. (2) $\implies$ (1): Let $D_m(p) \mid K_m(n)$ for all $p \mid n$. Since $p^{\mathrm{ord}_p(n)} \nabla_m(p) \mid K_m(n)$ and

$$\gcd(p^{\mathrm{ord}_p(n)} \nabla_m(p), D_m(p)) = 1,$$

we have $p^{\mathrm{ord}_p(n)} \nabla_m(p) D_m(p) \mid K_m(n)$ for all $p \mid n$.

Now consider $A \in \mathrm{Mat}(m, \mathbb{Z})$, $\gcd(\det A, n) = 1$. By Theorem 2, we have $A^{p \nabla_m(p) D_m(p)} \equiv I \pmod p$ for all $p \mid n$. Lemma 6 implies $A^{p^{\mathrm{ord}_p(n)} \nabla_m(p) D_m(p)} \equiv I \pmod{p^{\mathrm{ord}_p(n)}}$. Thus, $A^{K_m(n)} \equiv I \pmod{p^{\mathrm{ord}_p(n)}}$ for all $p \mid n$. By the Chinese remainder theorem, $A^{K_m(n)} \equiv I \pmod n$. Therefore, n is an m-Carmichael number.

(1) $\implies$ (2): Conversely, assume that for some $p \mid n$ we have $D_m(p) \nmid K_m(n)$. Since $D_m(p) = \mathrm{lcm}(p-1, p^2-1, \ldots, p^m-1)$, there exists $k \in \{1, 2, \ldots, m\}$ such that $p^k - 1 \nmid K_m(n)$.

We construct an element $A \in \mathrm{GL}(m, \mathbb{Z}/n\mathbb{Z})$ of order $p^k - 1$. Therefore, $A^{K_m(n)} \neq I$, and n is not m-Carmichael.

To this end, let α be a generator of the cyclic group $\mathbb{F}_{p^k}^\times$. Consider the polynomial $(X - \alpha)(X - \alpha^p) \ldots (X - \alpha^{p^{k-1}}) \in \mathbb{F}_p[X]$, and let $B \in \mathrm{GL}(k, \mathbb{F}_p)$ be its Frobenius companion matrix. Then B is of order $p^k - 1$, and the same is true for $C = \mathrm{diag}(B, I) \in \mathrm{GL}(m, \mathbb{F}_p)$. Lift C to an element of $\mathrm{Mat}(m, \mathbb{Z})$. Then $C^{p^k - 1} \equiv I \pmod p$. By Lemma 6, we have $(C^{p^{\mathrm{ord}_p(n)-1}})^{p^k-1} \equiv I \pmod{p^{\mathrm{ord}_p(n)}}$. Moreover, since $\gcd(p^{\mathrm{ord}_p(n)}, p^k - 1) = 1$, we see that $C^{p^{\mathrm{ord}_p(n)-1}} \bmod p^{\mathrm{ord}_p(n)}$ is also of order $p^k - 1$. Finally, by the Chinese remainder theorem, consider $A \in \mathrm{GL}(m, \mathbb{Z}/n\mathbb{Z})$ such that $A \equiv C^{p^{\mathrm{ord}_p(n)-1}} \pmod{p^{\mathrm{ord}_p(n)}}$ and, for example, $A \equiv I \pmod{\frac{n}{p^{\mathrm{ord}_p(n)}}}$. By construction, A is of order $p^k - 1$, which finishes the proof. □

Remark 9. Proposition 7 also follows easily from Theorem 8.

Moreover, applying Theorem 8 and Lemma 5, we get

Corollary 10. *If n is an m-Carmichael number, and $k \in \mathbb{N}$, then n^k is also an m-Carmichael number.*

Finally, we present one necessary condition for a number to be m-Carmichael.

Proposition 11. *Assume that n is an m-Carmichael number. Then $n \not\equiv 2 \pmod 4$.*

Proof. Let $n \in \mathbb{N}$ be composite, $n \equiv 2 \pmod 4$. Then $D_m(n)$ is odd, and thus $\operatorname{ord}_2(K_m(n)) = \lceil \log_2 m \rceil$.

On the other hand, consider an odd $p \mid n$. Since $\Phi_{2^k}(p) = p^{2^{k-1}} + 1$ is even for $k \geq 1$, and $8 \mid \Phi_1(p)\Phi_2(p) = p^2 - 1$, we have $\operatorname{ord}_2(D_m(p)) \geq \lfloor \log_2 m \rfloor + 2 > \lceil \log_2 m \rceil$. Thus, $D_m(p) \nmid K_m(n)$, and n is not m-Carmichael. □

3 m-Carmichael numbers with prescribed prime factors

In Theorem 8, the divisibility condition for small values of m is transparent enough to find some infinite families of m-Carmichael numbers (apart of prime powers).

Let us start with $m = 2$. Let $d_2(p, n)$ denote the condition $D_2(p) \mid K_2(n)$, i.e., $p^2 - 1 \mid n(n^2 - 1)$. We have

- $d_2(2, n)$ is equivalent to $3 \mid n(n^2 - 1)$, which is satisfied for all n.
- $d_2(3, n)$ is equivalent to $8 \mid n(n^2 - 1)$, which is satisfied if and only if n is odd or $8 \mid n$.
- $d_2(5, n)$ is equivalent to $3 \cdot 8 \mid n(n^2 - 1)$, which is also satisfied if and only if n is odd or $8 \mid n$.
- $d_2(7, n)$ is equivalent to $3 \cdot 16 \mid n(n^2 - 1)$, which is satisfied if and only if $n \equiv \pm 1 \pmod 8$ or $16 \mid n$.
- $d_2(11, n)$ is equivalent to $3 \cdot 5 \cdot 8 \mid n(n^2 - 1)$, which is satisfied if and only if $d_2(5, n)$ and $5 \mid n(n^2 - 1)$ are satisfied; the latter is satisfied if and only if $n \equiv 0, \pm 1 \pmod 5$.

Using the above, the following propositions are proven by a direct application of Theorem 8.

Proposition 12. *Let $n \in \mathbb{N}$ be a composite 7-smooth number which is not a prime power. Then n is 2-Carmichael if and only if n belongs to one of the following families:*

1. *$n = 2^k \cdot 3^l \cdot 5^r$, where $k \geq 3$,*

2. $n = 2^k \cdot 3^l \cdot 5^r \cdot 7^s$, *where* $k \geq 4$, $s \geq 1$,

3. $n = 3^l \cdot 5^r$,

4. $n = 3^l \cdot 5^r \cdot 7^s$, *where* $l \equiv r \pmod 2$, $s \geq 1$.

Proposition 13. *Let* $n \in \mathbb{N}$ *be a composite* 11*-smooth number which is not* 7*-smooth and not a prime power. Then* n *is* 2*-Carmichael if and only if* n *belongs to one of the following families:*

1. $n = 2^k \cdot 3^l \cdot 5^r \cdot 11^t$, *where* $k \geq 3$, $r \geq 1$,

2. $n = 2^k \cdot 3^l \cdot 5^r \cdot 7^s \cdot 11^t$, *where* $k \geq 4$, $r \geq 1$, $s \geq 1$,

3. $n = 2^k \cdot 3^l \cdot 11^t$, *where* $k \geq 3$, $k \equiv l \pmod 2$,

4. $n = 2^k \cdot 3^l \cdot 7^s \cdot 11^t$, *where* $k \geq 4$, $s \geq 1$, $k + l + s$ *is even,*

5. $n = 3^l \cdot 5^r \cdot 11^t$, *where* $r \geq 1$,

6. $n = 3^l \cdot 5^r \cdot 7^s \cdot 11^t$, *where* $r \geq 1$, $s \geq 1$, $l + r + t$ *is even,*

7. $n = 3^l \cdot 11^t$, *where* l *is even,*

8. $n = 3^l \cdot 7^s \cdot 11^t$, *where* $s \geq 1$, $l \equiv s \equiv t \pmod 2$.

We now consider $m = 3$ or $m = 4$. We restrict ourselves to composite numbers of the form $n = 2^k 3^l$.

Proposition 14. *Let* $n = 2^k 3^l$, *where* $k, l \geq 1$. *Then* n *is* 3*-Carmichael if and only if* $k \geq 2$, *and* (k, l) *belongs to one of the following families:*

1. $k \equiv 0 \pmod{12}$, $l \equiv 0, 2, 3, 4 \pmod 6$,

2. $k \equiv \pm 2 \pmod{12}$, $l \equiv \pm 4 \pmod 6$,

3. $k \equiv \pm 4 \pmod{12}$, $l \equiv 0, \pm 1, 2, 4 \pmod 6$,

4. $k \equiv 6 \pmod{12}$, $l \equiv 0 \pmod 3$.

Proposition 15. *Let* $n = 2^k 3^l$, *where* $k, l \geq 1$. *Then* n *is* 4*-Carmichael if and only if* $k \geq 3$, *and* (k, l) *belongs to one of the families 1) – 4) in Proposition 14 or to one of the following families:*

5. $k \equiv \pm 1 \pmod{12}$, $l \equiv \pm 2 \pmod 6$,

6. $k \equiv \pm 3 \pmod{12}$, $l \equiv 0 \pmod 3$,

7. $k \equiv \pm 5 \pmod{12}$, $l \equiv \pm 4 \pmod 6$.

Proof of Propositions 14 and 15. We have $D_3(2) = 3 \cdot 7$, $D_4(2) = 3 \cdot 5 \cdot 7$, $D_3(3) = 2^3 \cdot 13$, $D_4(3) = 2^4 \cdot 5 \cdot 13$, $\nabla_3(n) = 2$, $\nabla_4(n) = 2 \cdot 3$. Therefore, n is 3-Carmichael if and only if $K_3(n) = 2n(n^2-1)(n^2+n+1)$ is divisible by 2^3, 3, 7, and 13, which is equivalent to the conditions $4 \mid n$ (i.e., $k \geq 2$), $n \equiv \pm 1, 2, 4 \pmod 7$, $n \equiv \pm 1, 3, 9 \pmod{13}$. Similarly, n is 4-Carmichael if and only if $K_4(n) = 6n(n^2-1)(n^2+n+1)(n^2+1)$ is divisible by 2^4, 3, 5, 7, and 13, which is equivalent to $8 \mid n$ (i.e., $k \geq 3$), $n \equiv \pm 1, 2, 4 \pmod 7$, $n \equiv \pm 1, 3, 9, \pm 5 \pmod{13}$. Since $|\mathbb{F}_7^\times| = 6$, $|\mathbb{F}_{13}^\times| = 12$, and 3 mod 13 is of order 3, we see that the conditions on n modulo 7 and 13 depend only on k mod 12, l mod 6. The corresponding values of k mod 12, l mod 6 are obtained by a direct calculation.

Now we describe the general pattern of the distribution of m-Carmichael numbers with prescribed prime factors.

Let P be a finite nonempty subset of primes. Let $D_m(P)$ denote the least common multiple of $D_m(p)$ for all $p \in P$.

Let us say that $n \in \mathbb{N}$ is a *P-number*, if n is divisible precisely by the primes in P. By Theorem 8, a P-number n is m-Carmichael if and only if $D_m(P) \mid K_m(n)$.

Further, write $D_m(P) = D'_m(P)D''_m(P)$, where $D'_m(P)$ is a product of primes in P, and $D''_m(P)$ is coprime to all $p \in P$. Then a P-number n is m-Carmichael if and only if $D'_m(P) \mid K_m(n)$ and $D''_m(P) \mid K_m(n)$.

First, notice that, since $n \mid K_m(n)$, $\nabla_m(P) := \nabla_m(n)$ depends only on P, and $D'_m(P)$ is coprime to $D_m(n)$, it follows that the condition $D'_m(P) \mid K_m(n)$ is satisfied if and only if $\operatorname{ord}_p n \geq \operatorname{ord}_p D'_m(P) - \operatorname{ord}_p \nabla_m(P)$ for all primes $p \in P$.

Secondly, since a P-number n is, by construction, invertible modulo $D''_m(P)$, we see that the condition $D''_m(P) \mid K_m(n)$ depends only on the values of $\operatorname{ord}_p n \bmod \lambda(D''_m(P))$ for $p \in P$. Here λ is the Carmichael function, i.e., $\lambda(D''_m(P))$ is the exponent of the group $(\mathbb{Z}/D''_m(P)\mathbb{Z})^\times$. Moreover, if $p \in P$, let $v_{m,P}(p)$ denote the order of $p \bmod D''_m(P)$ in the group $(\mathbb{Z}/D''_m(P)\mathbb{Z})^\times$. Then the condition $D''_m(P) \mid K_m(n)$ depends only on the values of $\operatorname{ord}_p n \bmod v_{m,P}(p)$ for $p \in P$.

Thus, we get the following

Theorem 16. *For any $p \in P$, the set of P-numbers which are m-Carmichael is invariant under multiplication by $p^{v_{m,P}(p)}$.*

Corollary 17. *Assume that there exists a P-number which is m-Carmichael. Then there are infinitely many of them.*

Remark 18. Corollary 17 follows also from Corollary 10.

All propositions of this section can be viewed as examples of Theorem 16. For example, for $m = 3$ and $P = \{2, 3\}$ we have $D'_m(P) = 2^3 \cdot 3$, $D''_m(P) = 7 \cdot 13$, and $\lambda(7 \cdot 13) = \operatorname{lcm}(6, 12) = 12$, $v_{m,P}(2) = 12$, $v_{m,P}(3) = 6$, which is in accordance with Proposition 14.

4 Concluding remarks

We list some natural questions that remain open.

- For what m and P are there P-numbers which are m-Carmichael?
- Are there squarefree m-Carmichael numbers for $m \geq 3$?

Remark 19. One can consider an analogous notion for other affine group schemes of finite type defined over $\mathbb{Z}$. Namely, if G is such a group scheme, $K_G(p)$ the exponent of the group $G(\mathbb{F}_p)$, and $K_G(n)$ its reasonable extrapolation to all $n \in \mathbb{N}$, then one can consider G-Carmichael numbers, i.e., composite $n \in \mathbb{N}$ such that $g^{K_G(n)} = 1$ for all $g \in G(\mathbb{Z}/n\mathbb{Z})$.

5 Acknowledgments

The research of the second author was partially supported by the Akhiezer Foundation.

A Numerical experiments

We calculate, via brute force, all m-Carmichael numbers up to 10^5 for $2 \leq m \leq 10$. Let us call an m-Carmichael number *nontrivial* if it is not a prime power. There are 1330 nontrivial 2-Carmichael numbers, 44 nontrivial 3-Carmichael numbers, and 28 nontrivial 4-Carmichael numbers on the researched interval. There are no nontrivial m-Carmichael numbers for $5 \leq m \leq 10$ on the researched interval.

Among 16 Carmichael numbers less than 10^5, the following four, namely,

$$1729 = 7 \cdot 13 \cdot 19, \quad 2465 = 5 \cdot 17 \cdot 29, \quad 6601 = 7 \cdot 23 \cdot 41, \quad 41041 = 7 \cdot 11 \cdot 13 \cdot 41,$$

are 2-Carmichael. None of these Carmichael numbers are m-Carmichael for $3 \leq m \leq 10$. Moreover, none of m-Carmichael numbers for $3 \leq m \leq 10$ on the researched interval are squarefree.

There are 18 numbers on the researched interval, namely,

$$\begin{array}{llll} 48 = 2^4 \cdot 3, & 144 = 2^4 \cdot 3^2, & 1296 = 2^4 \cdot 3^4, & 1728 = 2^6 \cdot 3^3, \\ 2304 = 2^8 \cdot 3^2, & 5760 = 2^7 \cdot 3^2 \cdot 5, & 9216 = 2^{10} \cdot 3^2, & 11664 = 2^4 \cdot 3^6, \\ 20736 = 2^8 \cdot 3^4, & 25600 = 2^{10} \cdot 5^2, & 27000 = 2^3 \cdot 3^3 \cdot 5^3, & 30720 = 2^{11} \cdot 3 \cdot 5, \\ 34992 = 2^4 \cdot 3^7, & 36864 = 2^{12} \cdot 3^2, & 46656 = 2^6 \cdot 3^6, & 62208 = 2^8 \cdot 3^5, \\ 96768 = 2^9 \cdot 3^3 \cdot 7, & 99225 = 3^4 \cdot 5^2 \cdot 7^2, & & \end{array}$$

that are nontrivial m-Carmichael numbers for all $m \in \{2, 3, 4\}$, and one number, $22815 = 3^3 \cdot 5 \cdot 13^2$, that is nontrivial 3-Carmichael and 4-Carmichael, but not 2-Carmichael.

Also, on the researched interval there are 19 numbers, namely,

$$\begin{array}{llll} 160 = 2^5 \cdot 5, & 448 = 2^6 \cdot 7, & 704 = 2^6 \cdot 11, & 800 = 2^5 \cdot 5^2, \\ 1056 = 2^5 \cdot 3 \cdot 11, & 2640 = 2^4 \cdot 3 \cdot 5 \cdot 11, & 3136 = 2^6 \cdot 7^2, & 5929 = 7^2 \cdot 11^2, \\ 7744 = 2^6 \cdot 11^2, & 18144 = 2^5 \cdot 3^4 \cdot 7, & 20000 = 2^5 \cdot 5^4, & 21952 = 2^6 \cdot 7^3, \\ 28672 = 2^{12} \cdot 7, & 29952 = 2^8 \cdot 3^2 \cdot 13, & 31744 = 2^{10} \cdot 31, & 34496 = 2^6 \cdot 7^2 \cdot 11, \\ 39424 = 2^9 \cdot 7 \cdot 11, & 45056 = 2^{12} \cdot 11, & 85184 = 2^6 \cdot 11^3, & \end{array}$$

that are nontrivial 2- and 3-Carmichael, but not 4-Carmichael; 8 numbers, namely,

$$\begin{array}{llll} 216 = 2^3 \cdot 3^3, & 1152 = 2^7 \cdot 3^2, & 2592 = 2^5 \cdot 3^4, & 4000 = 2^5 \cdot 5^3, \\ 5832 = 2^3 \cdot 3^6, & 13824 = 2^9 \cdot 3^3, & 28800 = 2^7 \cdot 3^2 \cdot 5^2, & 73728 = 2^{13} \cdot 3^2, \end{array}$$

that are nontrivial 2- and 4-Carmichael, but not 3-Carmichael; 6 numbers, namely,

$$\begin{array}{lll} 324 = 2^2 \cdot 3^4, & 900 = 2^2 \cdot 3^2 \cdot 5^2, & 1404 = 2^2 \cdot 3^3 \cdot 13, \\ 39204 = 2^2 \cdot 3^4 \cdot 11^2, & 74088 = 2^3 \cdot 3^3 \cdot 7^3, & 74536 = 2^3 \cdot 7 \cdot 11^3, \end{array}$$

that are nontrivial 3-Carmichael, but not 2- or 4-Carmichael. Finally, one number, $26112 = 2^9 \cdot 3 \cdot 17$, is nontrivial 4-Carmichael, but not 2- or 3-Carmichael.

Below we list all nontrivial 2-Carmichael numbers up to 3000 that are not treated by Propositions 12 and 13 (i.e., not 11-smooth).

$$\begin{array}{llll} 104 = 2^3 \cdot 13 & 171 = 3^2 \cdot 19 & 195 = 3 \cdot 5 \cdot 13 & 273 = 3 \cdot 7 \cdot 13 \\ 351 = 3^3 \cdot 13 & 435 = 3 \cdot 5 \cdot 29 & 455 = 5 \cdot 7 \cdot 13 & 609 = 3 \cdot 7 \cdot 29 \\ 615 = 3 \cdot 5 \cdot 41 & 624 = 2^4 \cdot 3 \cdot 13 & 665 = 5 \cdot 7 \cdot 19 & 715 = 5 \cdot 11 \cdot 13 \\ 736 = 2^5 \cdot 23 & 759 = 3 \cdot 11 \cdot 23 & 832 = 2^6 \cdot 13 & 855 = 3^2 \cdot 5 \cdot 19 \\ 903 = 3 \cdot 7 \cdot 43 & 1001 = 7 \cdot 11 \cdot 13 & 1015 = 5 \cdot 7 \cdot 29 & 1045 = 5 \cdot 11 \cdot 19 \\ 1071 = 3^2 \cdot 7 \cdot 17 & 1088 = 2^6 \cdot 17 & 1183 = 7 \cdot 13^2 & 1216 = 2^6 \cdot 19 \\ 1265 = 5 \cdot 11 \cdot 23 & 1352 = 2^3 \cdot 13^2 & 1377 = 3^4 \cdot 17 & 1431 = 3^3 \cdot 53 \\ 1456 = 2^4 \cdot 7 \cdot 13 & 1520 = 2^4 \cdot 5 \cdot 19 & 1539 = 3^4 \cdot 19 & 1560 = 2^3 \cdot 3 \cdot 5 \cdot 13 \\ 1595 = 5 \cdot 11 \cdot 29 & 1625 = 5^3 \cdot 13 & 1729 = 7 \cdot 13 \cdot 19 & 1856 = 2^6 \cdot 29 \\ 1881 = 3^2 \cdot 11 \cdot 19 & 1911 = 3 \cdot 7^2 \cdot 13 & 1984 = 2^6 \cdot 31 & 2001 = 3 \cdot 23 \cdot 29 \\ 2009 = 7^2 \cdot 41 & 2015 = 5 \cdot 13 \cdot 31 & 2080 = 2^5 \cdot 5 \cdot 13 & 2211 = 3 \cdot 11 \cdot 67 \\ 2255 = 5 \cdot 11 \cdot 41 & 2365 = 5 \cdot 11 \cdot 43 & 2375 = 5^3 \cdot 19 & 2457 = 3^3 \cdot 7 \cdot 13 \\ 2465 = 5 \cdot 17 \cdot 29 & 2535 = 3 \cdot 5 \cdot 13^2 & 2565 = 3^3 \cdot 5 \cdot 19 & 2624 = 2^6 \cdot 41 \\ 2639 = 7 \cdot 13 \cdot 29 & 2736 = 2^4 \cdot 3^2 \cdot 19 & 2808 = 2^3 \cdot 3^3 \cdot 13 & 2871 = 3^2 \cdot 11 \cdot 29 \\ 2912 = 2^5 \cdot 7 \cdot 13 & 2925 = 3^2 \cdot 5^2 \cdot 13 & & \end{array}$$

Also, we manage to compute a few larger m-Carmichael numbers for $m \geq 5$. We consider numbers of the form $2^k 3^l$ for relatively small values of k and l and apply Theorem 8. For instance, $2^{22} \cdot 3^2$ is 2- (by Proposition 12), 3- (by Proposition 14), 4- (by Proposition 15), 5- and 6-Carmichael, but not 7- or 8-Carmichael. Similarly, $2^{286} \cdot 3^{36}$ is 2-, 6-, 7-, and 8-Carmichael, but not 3-, 4-, or 5-Carmichael.

References

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

[2] Y. Ge, Elementary properties of cyclotomic polynomials, *Math. Reflec.* **2** (2008).

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

[4] J. B. Marshall, On the extension of Fermat's theorem to matrices of order n, *Proc. Edinb. Math. Soc.* **6** (1939), 85–91.

[5] R. J. McIntosh, M. Dipra, Carmichael numbers with $p + 1 \mid n + 1$, *J. Number Theory* **147** (2015), 81–91.

[6] I. Niven, Fermat's theorem for matrices, *Duke Math. J.* **15** (1948), 823–826.

[7] G. A. Steele, Carmichael numbers in number rings, *J. Number Theory* **128** (2008), 910–917.

2010 *Mathematics Subject Classification*: Primary 11A51, Secondary 11Y11, 20G30.
Keywords: Carmichael number, pseudoprime, general linear group.

(Concerned with sequences A002997 and A336663.)

Received March 3 2020; revised version received July 30 2020. Published in *Journal of Integer Sequences*, October 18 2020.

Return to Journal of Integer Sequences home page.