ON THE NUMBER OF PRIME DIVISORS OF HIGHER-ORDER CARMICHAEL NUMBERS

Oleg Eterevsky
St. Petersburg State University, Bibliotechnaya Sq. 2, St. Petersburg, 198904, Russia

Maxim Vsemirnov
Sidney Sussex College, Sidney Street, Cambridge, CB2 3HU, United Kingdom
email: m.vsemirnov@dpmms.cam.ac.uk
(Submitted August 2001–Final Revision February 2002)

1. INTRODUCTION

The classical Carmichael numbers are well known in number theory. These numbers were introduced independently by Korselt in [8] and Carmichael in [2] and since then they have been the subject of intensive study. The reader may find extensive but not exhaustive lists of references in [5, Sect. A13], [11, Ch. 2, Sec. IX].

Recall that a positive composite integer n is a Carmichael number if $a^n \equiv a \pmod{n}$ for every integer a. In other words, the Carmichael numbers are exactly the Fermat pseudoprimes to every base.

This notion can be generalized in several ways. For instance, one may vary pseudoprimality tests. Such generalizations have been considered in [4], [10], [13]; for further references see [6]. Another approach was suggested by Howe [6] who replaced the ring $\mathbb{Z}/n\mathbb{Z}$ by any $\mathbb{Z}/n\mathbb{Z}$-algebra.

Definition 1 ([6]): For a positive integer m, a *Carmichael number of order* m is a positive composite integer n such that the map $x \mapsto x^n$ defines an endomorphism of every $\mathbb{Z}/n\mathbb{Z}$-algebra that can be generated by m elements as a $\mathbb{Z}/n\mathbb{Z}$-module.

This definition is not too useful in practice. But Howe [6] gave a nice criterion for the Carmichael numbers of order m, which generalized Korselt's criterion [8] for the usual Carmichael numbers.

Theorem 1 ([6]): *Let m and n be positive integers with n composite. Then n is a Carmichael number of order m if and only if the following two conditions hold:*

1. *n is squarefree;*
2. *for every prime divisor p of n and for every integer r with $1 \le r \le m$, there is an integer $i_r \ge 0$ such that $n \equiv p^{i_r} \pmod{p^r - 1}$.*

Another generalization is the notion of *rigid* Carmichael numbers of order m. It was also introduced in [6].

Definition 2 ([6]): A rigid Carmichael number of order m is a Carmichael number n of order m such that for every prime divisor p of n and every integer r with $1 \le r \le m$ we have $n \equiv 1 \pmod{p^r - 1}$.

As noted in [5, Sect. A13], rigid Carmichael numbers of order two have already been studied by S. Graham and R. Pinch.

It is naturally to ask what results concerning the usual Carmichael numbers can be strengthened for their higher-order counterparts. For example, it is well known that any Carmichael number has at least three different prime divisors. The proof can be found in many textbooks, e.g., see [7]. The aim of this paper is to prove a lower bound for the number

of prime divisors of higher-order Carmichael numbers. We also consider the rigid Carmichael numbers as a separate case.

We start with such an estimation for all Carmichael numbers of order n. It is simple but the resulting bound is rather rough.

Theorem 2: *Every Carmichael number of order m has at least $m+2$ prime divisors.*

This theorem is proved in section 2. The estimate for rigid Carmichael numbers is asymptotically much better.

Theorem 3: *For $m \geq 2$, a rigid Carmichael number of order m has at least $s+1$ prime divisors, where*

$$s = \sum_{k \leq m} \phi(k) \tag{1}$$

and ϕ denotes, as usual, the Euler totient function.

Remark 1: For s defined by (1), a lower bound was given by Mertens [9] (see also [3, Ch. 5, ref. 36]):

$$\sum_{k \leq m} \phi(k) \geq \frac{3}{\pi^2} m^2 - \frac{1}{2} m \ln m - \left(\frac{\gamma}{2} + \frac{5}{8} \right) m - 1,$$

where $\gamma = 0.57721\ldots$ is Euler's constant.

Theorem 3 together with several auxiliary propositions is proved in section 3. Note that Theorem 2 is stronger than Theorem 3 when $m = 1$ and 2. Moreover, the estimate of Theorem 2 is exact for $m = 1$. An example of a Carmichael number (which is necessarily rigid for $m = 1$) with exactly three prime divisors is $561 = 3 \cdot 11 \cdot 17$. The least (rigid) Carmichael number of order two has 8 prime divisors. It is $17 \cdot 31 \cdot 41 \cdot 43 \cdot 83 \cdot 97 \cdot 167 \cdot 331$. As far as we know, no example of a Carmichael number of order two with smaller number of prime divisors has been found. For $m = 2$, Theorem 2 tells us that at least four divisors are necessary. Thus, there is still a gap between lower and upper bounds. Carmichael numbers of order higher than two are not known. However, Howe [6] gave heuristic arguments suggesting that there are infinitely many such numbers. Note that his construction even for $m = 2$ produces Carmichael numbers with many prime divisors.

For any fixed m, the bound in Theorem 2 can be improved for all but finitely many Carmichael numbers of order m. To state this improvement we must introduce some notation. Let $\Phi_l(x)$ be the l^{th} cyclotomic polynomial. Consider

$$F_m(x) = \prod_{l \leq m} \Phi_l(x) \tag{2}$$

and define the polynomial $G_{m,j}(x)$ as the remainder of x^j modulo $F_m(x)$, i.e.,

$$\deg G_{m,j} < \deg F_m, \tag{3}$$

$$G_{m,j}(x) \equiv x^j \pmod{F_m(x)}. \tag{4}$$

Let M denote the largest number among all absolute values of the coefficients of polynomials $G_{m,j}(x), j = 0, \ldots, \mathrm{lcm}(1, \ldots, m) - 1$. Clearly, there are finitely many Carmichael numbers whose greatest prime divisor is at most $\max\{2Me, s\} + 1$, where s is given by (1).

Theorem 4: *Let n be a Carmichael number of order $m \geq 2$ and p be the greatest prime divisor of n. Take s as in* (1) *and choose M as above. If*

$$p > \max\{2Me, s\} + 1, \tag{5}$$

then n has at least $\frac{s}{2}$ different prime divisors.

We prove this theorem in section 4. Note that Theorem 2 is stronger than Theorem 4 when $m < 7$.

2. THE TRIVIAL BOUND

Proof of Theorem 2: Let n be a Carmichael number of order m. By Theorem 1, we can write $n = p_1 p_2 \dots p_N$ for some $N \geq 2$, where $p_1, \dots, p_N$ are primes and $p_1 < p_2 < \dots < p_N$. There are two cases:

Case 1. $n \equiv 1 \pmod{p_N^m - 1}$. Then there exists a positive integer k such that $n - 1 = kp_N^m - k$. Hence,

$$k - 1 = p_N(kp_N^{m-1} - p_1 p_2 \dots p_{N-1}). \tag{6}$$

If $k = 1$ then we would have $p_N^{m-1} = p_1 \dots p_{N-1}$, which is impossible. Hence, $k > 1$. Since (6) implies $p_N | k - 1$, we have $k > p_N$. Consequently,

$$p_N^N > p_1 \dots p_N = n = k(p_N^m - 1) + 1 \geq (p_N + 1)(p_N^m - 1) + 1 \geq p_N^{m+1}.$$

In particular, $N > m + 1$, i.e., n has at least $m + 2$ prime divisors.

Case 2. $n \equiv p_N^i \pmod{p_N^m - 1}$, where $0 < i < m$. Then $n = p_N^i + k(p_N^m - 1)$. By Theorem 1, n has at least two prime divisors. In particular, $n \neq p_N^i$ and $k > 0$. But n is divisible by p_N and $i > 0$. Hence k is divisible by p_N and $k \geq p_N$. We have

$$p_N^N > p_1 \dots p_N = n = p_N^i + k(p_N^m - 1) \geq p_N^i + p_N(p_N^m - 1) \geq p_N^{m+1}.$$

As in the first case, n has at least $m + 2$ prime divisors. □

3. RIGID CARMICHAEL NUMBERS

Let $n = p_1 p_2 \dots p_N$ be a rigid Carmichael number of order m, where $p_1, \dots, p_N$ are primes and $p_1 < p_2 < \dots < p_N$. By Definition 2, for any $r \leq m$ the congruence $n \equiv 1 \pmod{p_N^r - 1}$ holds. Therefore,

$$n \equiv 1 (\text{mod } \text{lcm}(p_N - 1, p_N^2 - 1, \dots, p_N^m - 1)). \tag{7}$$

Now our aim is to evaluate the above least common multiple.

It would be a trivial problem if we replace the number p_N by the indeterminate x. Indeed, $x^k - 1 = \prod_{d|k} \Phi_d(x)$, and two different cyclotomic polynomials are relatively prime. Therefore,

$$\text{lcm}(x - 1, \dots, x^m - 1) = \prod_{d \leq m} \Phi_d(x) = F_m(x), \tag{8}$$

where F_m is defined by (2). However, for a given p, two numbers $\Phi_d(p)$ and $\Phi_l(p)$ may have non-trivial common factor. Although the relation similar to (8) still holds in this case, its proof becomes more tricky.

The reader familiar with Möbius algebras (see [12, Ch. 3] or [1, Ch. 4]) may recognize the following lemma as a multiplicative analogue of the special case of the general Möbius inversion formula.

Lemma 1: *For all positive integers $a_1, \ldots, a_m$ we have*

$$\operatorname{lcm}(a_1, \ldots, a_m) = \prod_{k=1}^{m} \left(\prod_{i_1 < i_2 < \cdots < i_k} \gcd(a_{i_1}, \ldots, a_{i_k}) \right)^{(-1)^{k-1}}.$$

Proof: Let $\operatorname{ord}_p a$ denote the greatest integer k such that $p^k | a$. Then the claim of the lemma is equivalent to the following one: for every prime p

$$\max_{i=1,\ldots,m} \operatorname{ord}_p a_i = \sum_{k=1}^{m} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} \min_{l=1,\ldots,k} \operatorname{ord}_p(a_{i_l}). \tag{9}$$

Relation (9) now follows from the more general statement [1, Example 4.62]: for any non-negative integers $\alpha_1, \ldots, \alpha_m$,

$$\max_{i=1,\ldots,m} \alpha_i = \sum_{k=1}^{m} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} \min_{l=1,\ldots,k} \alpha_{i_l}. \tag{10}$$

It can be deduced also from the inclusion and exclusion principle. □

Lemma 2: *Let $f_1, \ldots, f_m \in \mathbb{Q}[x]$ be non-zero polynomials. Then*

$$\operatorname{lcm}(f_1, \ldots, f_m) = \prod_{k=1}^{m} \left(\prod_{i_1 < \cdots < i_k} \gcd(f_{i_1}, \ldots, f_{i_k}) \right)^{(-1)^{k-1}}.$$

The proof is similar to the previous one. The following two lemmas recall some well-known facts.

Lemma 3: *For any integer $p > 1$ and positive integers $a_1, \ldots, a_k$ we have*

$$\gcd(p^{a_1} - 1, \ldots, p^{a_k} - 1) = p^{\gcd(a_1, \ldots, a_k)} - 1.$$

Lemma 4: *Let x be an indeterminate. In $\mathbb{Q}[x]$ the following relation holds*:

$$\gcd(x^{a_1} - 1, \ldots, x^{a_k} - 1) = x^{\gcd(a_1, \ldots, a_k)} - 1.$$

Now we are able to evaluate the desired least common multiple.

Lemma 5: *For any integer $p > 1$ and any positive integer m, the relation*

$$\operatorname{lcm}(p - 1, p^2 - 1, \ldots, p^m - 1) = F_m(p)$$

holds, where F_m is defined by (2).

Proof: By Lemma 1 and 3,

$$\operatorname{lcm}(p-1, p^2-1, \ldots, p^m-1) = \prod_{k=1}^{m} \left(\prod_{1 \le i_1 < \cdots < i_k \le m} \left(p^{\gcd(i_1,\ldots,i_k)} - 1 \right) \right)^{(-1)^{k-1}}. \qquad (11)$$

By Lemmas 2 and 4,

$$\operatorname{lcm}(x-1, x^2-1, \ldots, x^m-1) = \prod_{k=1}^{m} \left(\prod_{1 \le i_1 < \cdots < i_k \le m} \left(x^{\gcd(i_1,\ldots,i_k)} - 1 \right) \right)^{(-1)^{k-1}}, \qquad (12)$$

where lcm is taken in $\mathbb{Q}[x]$. Combining (12) with (8), we obtain

$$F_m(x) = \prod_{k=1}^{m} \left(\prod_{1 \le i_1 < \cdots < i_k \le m} \left(x^{\gcd(i_1,\ldots,i_k)} - 1 \right) \right)^{(-1)^{k-1}}.$$

Substituting p in place of x and taking into account (11), we complete the proof. □

Lemma 6: *Let $m \ge 2$. Define s by (1) and F_m by (2). Then*

$$F_m(p) \ge (p-1)^{s-1}(p+1).$$

In particular, $\operatorname{lcm}(p-1, \ldots, p^m-1) \ge (p-1)^{s-1}(p+1)$.

Proof: Write down $|\Phi_l(p)| = \prod_\zeta |p-\zeta|$, where the product is taken over all primitive roots of unity of degree l. Thus, $|\Phi_l(p)| \ge \prod_\zeta (p-1) = (p-1)^{\phi(l)}$ for all l and $|\Phi_2(p)| = p+1$. Now the claim follows from (2) and Lemma 5. □

Proof of Theorem 3: Relation (7) implies

$$n = 1 + k \operatorname{lcm}(p_N - 1, p_N^2 - 1, \ldots, p_N^m - 1)$$

for some $k > 0$. Using Lemma 6 we obtain

$$\begin{aligned} (p_N-1)^{N-1}(p_N+1) &> p_1 p_2 \ldots p_N \\ &= n = 1 + k \operatorname{lcm}(p_N - 1, p_N^2 - 1, \ldots, p_N^m - 1) \\ &\ge 1 + k(p_N-1)^{s-1}(p_N+1) > (p_N-1)^{s-1}(p_N+1). \end{aligned}$$

Hence $N > s$, which completes the proof. □

4. AN IMPROVED ESTIMATE FOR NON-RIGID CARMICHAEL NUMBERS

Let S_m be the set of all roots of unity of degree at most m. In other words, S_m is the set of all roots of F_m, where F_m is given by (2). Consider polynomials $G_{m,j}$ defined by (3)-(4). In particular,

$$G_{m,j}(\xi) = \xi^j \quad \text{for any } \xi \in S_m. \qquad (13)$$

Note that $G_{m,j}$ is uniquely determined by conditions (3) and (13) as the (unique) solution of the corresponding interpolation problem. Moreover, these two conditions allow to define $G_{m,j}$ for negative j's. As a consequence of (13), the sequence of polynomials $G_{m,j}$ is periodic with respect to j and its period is $\mathrm{lcm}(1,\dots,m)$. In addition, the polynomials $G_{m,j}$ for fixed m and $0 \le j < \mathrm{lcm}(1,\dots,m)$, are pairwise distinct.

Lemma 7: *For any j such that* $\deg F_m \le j < \mathrm{lcm}(1,\dots,m)$, *we have* $\deg G_{m,j} \ge \frac{1}{2}\deg F_m$.

Proof: Let $d = \deg G_{m,j}$. First, we show that $G_{m,d-j}(x) = x^d G_{m,j}\left(\frac{1}{x}\right)$. Note that $\deg x^d G_{m,j}\left(\frac{1}{x}\right) \le d < \deg F_m$ and, for any $\xi \in S_m$,

$$\xi^d G_{m,j}(1/\xi) = \xi^{d-j} = G_{m,d-j}(\xi).$$

Hence, $G_{m,d-j}(x)$ and $x^d G_{m,j}\left(\frac{1}{x}\right)$ must coincide. In particular, $\deg G_{m,d-j} \le d$. Next, $G_{m,d-j}(\xi)G_{m,j}(\xi) = \xi^{d-j}\xi^j = \xi^d$ for any $\xi \in S_m$. Therefore,

$$G_{m,d-j}(x)G_{m,j}(x) \equiv x^d \pmod{F_m}. \tag{14}$$

Note that $G_{m,l} = x^l$ for $0 \le l < \deg F_m$. Since $\deg F_m \le j < \mathrm{lcm}(1,\dots,m)$, the polynomial $G_{m,j}$ differs from $G_{m,l}, l = 0,\dots,\deg F_m - 1$, i.e., $G_{m,j}$ is not a monomial. Together with (14) this implies

$$G_{m,d-j}(x)G_{m,j}(x) = x^d + H(x)F_m(x) \tag{15}$$

for some non-zero polynomial H. In particular, the degree of the product in the left-hand side of (15) is at least $\deg F_m$. Consequently, $2d \ge \deg G_{m,d-j} + \deg G_{m,j} \ge \deg F_m$, which completes the proof. □

Now we are able to prove Theorem 4.

Proof of Theorem 4: Let n be a Carmichael number of order m. Write down $n = p_1 \dots p_N$, where $p_1,\dots,p_N$ are primes and $p_1 < \dots < p_N$. Let p be the greatest prime divisor of n, i.e., $p = p_N$.

By Theorem 1, for any $r, 1 \le r \le m$, there exists i_r, such that $0 \le i_r < r$ and

$$n \equiv p^{i_r} \pmod{p^r - 1}. \tag{16}$$

The exponents i_r must satisfy the obvious compatibility condition:

$$p^{i_r} \equiv p^{i_t} \pmod{p^{\gcd(r,t)} - 1},$$

which in turn is equivalent to

$$i_r \equiv i_t \pmod{\gcd(r,t)}. \tag{17}$$

Using the Chinese Remainder Theorem we can find j, such that

$$0 \le j < \mathrm{lcm}(1,\dots,m) \text{ and } j \equiv i_r \pmod{r} \text{ for any } r = 1,\dots,m.$$

Therefore, $p^j \equiv p^{i_r} \pmod{p^r - 1}$ and

$$n \equiv p^j \pmod{F_m(p)} \tag{18}$$

by (16) and Lemma 5. Note that s defined in (1) is exactly the degree of F_m. We are to distinguish several cases.

Case 1: $j = 0$. It was settled in Theorem 3.
Case 2: $0 < j < s$. It can be settled in a way similar to case 1. Namely,

$$\left(1 + \frac{1}{p-1}\right)^{s-1} < e$$

since $p > s$ by hypothesis (5). Therefore, using Lemma 6 and obvious estimates, we have

$$p^j \le p^{s-1} = \left(1 + \frac{1}{p-1}\right)^{s-1} (p-1)^{s-1} \le e(p-1)^{s-1} \le (p-1)^{s-1}(p+1) \le F_m(p).$$

On the other hand, n has at least two prime factors, hence, $n \neq p^j$ and $n > F_m(p)$ in accordance with (18). Combining this inequality with Lemma 6, we have

$$(p-1)^{N-1}(p+1) > p_1 \dots p_N = n > F_m(p) \ge (p-1)^{s-1}(p+1)$$

and $N \ge s$. Note that in the first two cases the estimate is even better than we claimed.
Case 3: $s \le j <$lcm$(1, \dots, m)$. We have

$$n \equiv p^j \equiv G_{m,j}(p) \pmod{F_m(p)}. \tag{19}$$

Recall that M is the largest number among absolute values of coefficients of polynomials $G_{m,j}(x), j = 0, \dots,lcm(1, \dots, m) - 1$. Using assumption (5) and Lemma 6 we deduce

$$\begin{aligned} |G_{m,j}(p)| &\le M \sum_{i=0}^{s-1} p^i = M\frac{p^s - 1}{p-1} < \frac{M}{p-1}p^s \\ &= \frac{M}{p-1}\left(1 + \frac{1}{p-1}\right)^s (p-1)^s < Me(p-1)^{s-1} \le \frac{1}{2}(p-1)^s < \frac{1}{2}F_m(p). \end{aligned} \tag{20}$$

Put $d =$deg$G_{m,j}$. Then

$$|G_{m,j}(p)| \ge p^d - M\sum_{i=0}^{d-1} p^i = p^d - \frac{M}{p-1}(p^d - 1) > p^d - \frac{M}{p-1}p^d > \frac{1}{2}p^d.$$

Combining this inequality with Lemma 7 we get

$$|G_{m,j}(p)| \ge \frac{1}{2}p^{s/2}. \tag{21}$$

If $G_{m,j}(p)$ is positive, then, by (19) and (21),

$$n \ge G_{m,j}(p) \ge \frac{1}{2}p^{s/2}.$$

If $G_{m,j}(p)$ is negative, then (19), (20), and Lemma 6 imply

$$n \geq G_{m,j}(p) + F_m(p) \geq \frac{1}{2}F_m(p) \geq \frac{1}{2}(p-1)^{s-1}(p+1).$$

In any case,

$$n \geq \frac{1}{2}p(p-1)^{s/2-1} \geq p(p-1)^{s/2-2}.$$

In particular,

$$(p-1)^{N-1}p > p_1 \dots p_N = n \geq (p-1)^{s/2-2}p.$$

Consequently, $N > \frac{s}{2} - 1$. Since $s/2$ is an integer for $m \geq 2$, this completes the proof. □

ACKNOWLEDGMENTS

The authors are grateful to an anonymous referee for his valuable suggestions and for providing us a copy of Mertens's paper.

Supported by INTAS (grant 2000-447).

REFERENCES

[1] M. Aigner. *Combinatorial Theory.* Springer-Verlag, 1979.
[2] R.P. Carmichael. "On Composite Numbers p which Satisfy the Fermat Congruence $a^{p-1} \equiv 1 \pmod{p}$." *Amer. Math. Monthly* **19** (1912): 22-27.
[3] L.E. Dickson. *History of the Theory of Numbers.* Volume 1. Washington, 1919.
[4] J. Grantham. "Frobenius Pseudoprimes." *Math. Comp.* **70** (2001): 873-891.
[5] R. Guy. *Unsolved Problems in Number Theory.* Springer-Verlag, 2nd edition, 1994.
[6] E.W. Howe. "Higher-order Carmichael Numbers." *Math. Comp.* **69** (2000): 1711-1719.
[7] N. Koblitz. *A Course in Number Theory and Cryptography.* Volume 114 of Graduate Texts in Math. Springer-Verlag, 2nd edition, 1994.
[8] A. Korselt. "Problème Chinois." *L'Intermédiaire des Mathématiciens* **6** (1899): 142-143.
[9] F. Mertens. "Ueber einige Asymptotische Gesetze der Zahlentheorie." *J. für die reine und angew. Math* **77** (1874): 289-338.
[10] A. Di Porto and P. Filipponi. "Generating m-strong Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **30.4** (1992): 339-343.
[11] P. Ribenboim. *The New Book of Prime Number Records.* Springer-Verlag, 1996.
[12] R. Stanley. *Enumerative Combinatorics.* Volume 1. Wadsworth, Inc., California, 1986.
[13] H.C. Williams. "On Numbers Analogous to the Carmichael Numbers." *Canad. Math. Bull.* **20** (1977): 133-143.

AMS Classification Numbers: 11A51, 11A25

✠ ✠ ✠