MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 191
JULY 1990, PAGES 383-389

THE CARMICHAEL NUMBERS TO 10^{12}

GERHARD JAESCHKE

ABSTRACT. An algorithm is presented which determines all Carmichael numbers up to a given limit having a prescribed number of factors. An overview over all Carmichael numbers less than 10^{12} is given.

INTRODUCTION

In [3] all composite numbers $n < 25 \cdot 10^9$ were tested for their pseudoprimality character, and 2163 numbers n turned out to be Carmichael numbers. (These are composite numbers n with $a^{n-1} \equiv 1 \bmod n$ for all a relatively prime to n.) While the underlying method of finding the pseudoprimes in that note had an analytic character, we tried a synthetic approach of building up the Carmichael numbers from their factors. So it was possible to determine the Carmichael numbers up to 10^{12} by a reasonable amount of computer time.

After describing the general method for determining all Carmichaels with a fixed number r of prime factors, we present a special approach for $r = 3, 4$ which in some cases is faster than the general procedure. Finally, we give an overview of the Carmichael numbers $< 10^{12}$ in the form of some special tables containing the cardinalities of some sets of Carmichael numbers. The 6075 Carmichael numbers between $25 \cdot 10^9$ and 10^{12} cannot be tabulated here and will be deposited in the UMT-file.

It should be mentioned that already in 1975 the Carmichael numbers below 10^9 have been computed by J. D. Swift and deposited in the UMT-file (see [4]).

1. GENERAL METHOD

Our algorithm for determining Carmichaels is based upon the following three well-known facts (see, e.g., [1]).

Fact 1. All Carmichael numbers are square-free.

Fact 2. All Carmichael numbers have at least three prime factors.

Fact 3. The product of r different primes $p_1, \dots, p_r$ is a Carmichael number if and only if

$$n \equiv 1 \bmod p_i - 1 \quad \text{for } i = 1, \dots, r.$$

Received November 4, 1988; revised February 20, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A15.

©1990 American Mathematical Society
0025-5718/90 \$1.00 + \$.25 per page

Before we discuss the algorithm, we describe its underlying ideas. Let r be an integer ≥ 3, and let $p_1, \ldots, p_{r-1}$ be primes which satisfy the conditions

$$p_1 < p_2 < \cdots < p_{r-1}, \tag{1}$$

$$p_i \not\equiv 1 \mod p_k \quad \text{for } 1 \leq k < i \leq r-1. \tag{2}$$

Put further

$$R = p_1 p_2 \cdots p_{r-1} \tag{3}$$

and

$$K = \operatorname{lcm}(p_1 - 1, \ldots, p_{r-1} - 1), \tag{4}$$

where lcm denotes the 'least common multiple'. In view of (1) and (2), $\gcd(R, K) = 1$, where gcd denotes the 'greatest common divisor'. Thus, the multiplicative inverse of $R \mod K$ exists, and we put

$$a = R^{-1} \mod K. \tag{5}$$

Finally, let

$$g = \gcd(a - 1, K, R - 1). \tag{6}$$

Under these assumptions the following theorem holds.

Theorem 1. *$n = p_1 \cdots p_r$ is a Carmichael number with r prime factors if and only if the following two statements are valid*:

$$p_r \text{ is a prime with } p_r \equiv a \mod K, \tag{7}$$

$$\frac{R-1}{g} \equiv 0 \mod \frac{p_r - 1}{g}. \tag{8}$$

Proof. (a) Assume that (7) and (8) hold. Then, in view of (3), (7), (5), we obtain

$$n = Rp_r \equiv Ra \equiv 1 \mod K,$$

hence, by (4),

$$n - 1 \equiv 0 \mod p_i - 1 \quad \text{for } i = 1, \ldots, r-1.$$

(8) yields $R - 1 \equiv 0 \mod p_r - 1$, hence, $n - 1 \equiv 0 \mod p_r - 1$, and n is a Carmichael number.

(b) Let n be a Carmichael number $n = p_1 \cdots p_r$ with r prime factors. Then p_r is prime, and since $n \equiv 1 \mod p_i - 1$ for $i = 1, \ldots, r-1$, we have by definition of K, $n \equiv 1 \mod K$, i.e., $Rp_r \equiv 1 \mod K$ and $p_r \equiv a \mod K$ by (5). Therefore (7) is satisfied. From $n \equiv 1 \mod p_r - 1$ we obtain $R - 1 \equiv 0 \mod p_r - 1$, and in view of (6),

$$\frac{R-1}{g} \equiv 0 \mod \frac{p_r - 1}{g}.$$

This proves the theorem. □

Theorem 1 suggests the following procedure for determining all Carmichael numbers having r prime factors and being less than a given limit u.

Algorithm.

Input: u, r.

Step 1. Determine $r-1$ primes $p_1, \dots, p_{r-1}$ as follows:

$$p_1 < u^{1/r}$$

$$p_2 < \left(\frac{u}{p_1}\right)^{1/(r-1)} \wedge p_2 > p_1 \wedge p_2 \not\equiv 1 \mod p_1$$

....

$$p_k < \left(\frac{u}{p_1 \cdots p_{k-1}}\right)^{1/(r-k+1)} \wedge p_k > p_{k-1} \wedge p_k \not\equiv 1 \mod p_i \quad \text{for } i = 1, \dots, k-1.$$

Step 2. Calculate R, K, a, g according to (3), (4), (5), (6) and put

$$h = \min\left\{\frac{R-1}{2}, \left[\frac{u}{R}\right]\right\}.$$

Step 3. For all $\lambda = 0, 1, \dots, \max\{0, [(h-a)/K]\}$ test whether (8) is satisfied for $p_r = \lambda K + a$ and $p_r > p_{r-1}$ is a prime. In each such case, $n = R \cdot p_r$ is a Carmichael number.

Continue with Step 1 and determine another $(r-1)$-tuple of primes $p_1, \dots, p_{r-1}$.

Example. Let $u = 10^{12}$ and $r = 4$ and, in addition, $p_1 = 17$, $p_2 = 241$, $p_3 = 401$. Then we find $R = 1642897$, $K = 1200$, $a = 433$, $g = 48$, and $h = 608680$. For $\lambda = 0, 1, \dots, 506$ we test whether $25\lambda + 9$ is a divisor of 34227 and find that this is the case only for $\lambda = 0$ and $\lambda = 456$. Since $547633 = 433 + 1200 \cdot 456$ is not prime, the only Carmichael number with the factors 17, 241, 401 that is composed of four factors and is less than 10^{12} is $n = 17 \cdot 241 \cdot 401 \cdot 433 = 711374401$.

2. Special method for Carmichael numbers with four prime factors

In this section we present an algorithm for determining Carmichael numbers with four prime factors $p_1, \dots, p_4$ that is much faster than the method of §1 in those cases where $p_1 p_2$ is relatively small. The algorithm is based on the following theorem.

Theorem 2. *Let p_1, p_2, p_3, p_4 be primes with $p_1 < p_2 < p_3 < p_4$. If $p_1 p_2 p_3 p_4$ is a Carmichael number, and if we put $q = p_1 p_2$ and $m = (qp_3 - 1)/(p_4 - 1)$, then the following statements are valid:*

$$m \in \{2, 3, \dots, q-1\}, \tag{9}$$

$$qp_3 \equiv 1 \mod m, \tag{10}$$

$$p_2 p_3 (m + qp_3 - 1) \equiv m \mod m(p_1 - 1), \tag{11}$$

$$p_1 p_3 (m + qp_3 - 1) \equiv m \mod m(p_2 - 1), \tag{12}$$

$$q(m + qp_3 - 1) \equiv m \mod m(p_3 - 1). \tag{13}$$

Conversely, if $m \in \{2, \ldots, q-1\}$ *and if* p_1, p_2, p_3 *are primes and* p_3 *satisfies* (10)–(13) *for given* m, p_1, p_2, *and if* $p_4 = 1 + (qp_3 - 1)/m$ *is a prime, then the product* qp_3p_4 *is a Carmichael number.*

Proof. I. Let $n = p_1p_2p_3p_4$ be a Carmichael number with four prime factors and let q, m be defined as above. Then, by Fact 3 (cf. §1), $qp_3 \equiv 1 \bmod p_4 - 1$, hence m is an integer. By definition of m we have $m < q$ and $m \neq 1$, i.e., $m \in \{2, \ldots, q-1\}$. Further, we have

$$mp_4 = m + qp_3 - 1, \tag{14}$$

which implies (10). Again by Fact 3, we obtain the system

$$\begin{aligned} p_2p_3p_4 &\equiv 1 \mod p_1 - 1, \\ p_1p_3p_4 &\equiv 1 \mod p_2 - 1, \\ p_1p_2p_4 &\equiv 1 \mod p_3 - 1, \end{aligned} \tag{15}$$

hence

$$\begin{aligned} p_2p_3p_4m &\equiv m \mod m(p_1 - 1), \\ p_1p_3p_4m &\equiv m \mod m(p_2 - 1), \\ p_1p_2p_4m &\equiv m \mod m(p_3 - 1), \end{aligned} \tag{16}$$

from which by (14) we immediately obtain (11), (12), and (13).

II. Now, let p_1, p_2, p_3 be primes with $p_1 < p_2 < p_3$, $m \in \{2, \ldots, q-1\}$, let p_3 satisfy (10)–(13), and let $p_4 = 1 + (qp_3 - 1)/m$ be prime. In view of (14), the system (11), (12), (13) is equivalent to (16), hence equivalent to (15), and we obtain

$$n = p_1p_2p_3p_4 \equiv 1 \mod p_i - 1, \qquad i = 1, 2, 3.$$

Finally, $qp_3 = 1 + m(p_4 - 1)$ implies $n \equiv 1 \bmod p_4 - 1$, hence n is a Carmichael number. □

Remark. (13) implies $q(m + q - 1) \equiv m \bmod p_3 - 1$ or, equivalently,

$$(q-1)(m+q) \equiv 0 \mod p_3 - 1. \tag{17}$$

This simplification is important in the algorithm below, since p_3 does not occur in the left-hand expression of (17).

Algorithm. Choose $q = p_1p_2$ for fixed primes $p_1 < p_2$. For each $m \in \{2, \ldots, q-1\}$ those primes $p_3 > p_2$ are determined which satisfy (17). For each such prime p_3 we test whether (10)–(13) are fulfilled. If not, we proceed to the next m, where we can restrict ourselves to those m with $\gcd(q, m) = 1$. If the above conditions hold for a pair m, p_3, then $p_4 = 1 + (qp_3 - 1)/m$ is tested for primality.

In the case of success, qp_3p_4 is a Carmichael number. When only Carmichael numbers $\leq u$ are wanted, only those p_3 have to be taken into account for which

$$p_3 \leq \min\{2q^2 - 3q + 2, \sqrt{u/q}\}$$

holds.

Example. Let $p_1 = 3$, $p_2 = 5$. Here we have $q = 15$ and m runs through the values $2, 4, 7, 8, 11, 13, 14$. When $m = 4$, there is no prime $p_3 > 5$ for which (17) holds. For $m = 11, 13, 14$ there exists no prime satisfying (10) and (17). For $m = 2, 7$ there are primes satisfying (10), (11), (12), and (17) but not (13). Finally, for $m = 8$ we find $p_3 = 47$ and $p_4 = 89$, so that $n = 3 \cdot 5 \cdot 47 \cdot 89 = 62745$ is the only Carmichael number that has four factors and is divisible by 15.

3. Special method for Carmichael numbers with three prime factors

Analogously to the algorithm in §2 for Carmichaels with four factors, we proceed in the case of Carmichaels with three factors. If p_1 is a given prime, then for all $m = 2, \dots, p_1 - 1$ we perform the following steps.

Step 1. Determine the primes $p_2 > p_1$ for which

$$m(p_2 - 1) \quad \text{divides} \quad p_1^2 p_2 + p_1(m-1) - m.$$

Step 2. For each prime p_2 found in Step 1 we test whether

$$p_1 p_2^2 + p_2 \cdot (m-1) \equiv m \mod m \cdot (p_1 - 1).$$

Step 3. Proceed with the next m if the conditions in Step 2 are not satisfied. Otherwise calculate $p_3 = 1 + (p_1 p_2 - 1)/m$ and check for primality.

Step 4. When p_3 is not prime proceed with the next m. Otherwise $p_1 p_2 p_3$ is a Carmichael number.

Since for each p_1, m runs only through $p_1 - 2$ values, the algorithm is very fast for relatively small p_1.

4. Results

Denote by $C(r, u)$ the number of Carmichael numbers which are less than u and have exactly r prime factors. Then the third column of Table 1 represents the new results.

Table 1

r	$C(r, 25 \cdot 10^9)$	$C(r, 10^{12})$
3	412	1000
4	795	2102
5	756	3156
6	192	1713
7	8	260
8	0	7
9	0	0

The sum

$$C(10^{12}) = \sum_{r=1}^{8} C(r, 10^{12})$$

yields the total number of Carmichaels below 10^{12}, namely $C(10^{12}) = 8238$.

Remark. It is easy to show that no Carmichael number exists below 10^{12} with more than eight prime factors.

With $Q(r)$ denoting the number of $(r-1)$-tuples $(p_1, \dots, p_{r-1})$ which have to be tested in order to find all Carmichaels smaller than 10^{12}, we obtain Table 2.

TABLE 2

r	$Q(r)$
3	2260848
4	8372508
5	8613292
6	2924698
7	304934
8	6904

The values of Table 2 shed some light on the requirements of computer time for finding the Carmichaels less than 10^{12}. It took several hundred hours on an IBM 3083 at the Scientific Center in Heidelberg.

Remark. The values $Q(3)$ and $Q(4)$ are included in Table 2, since we did not compute the total requirements for the special algorithms in §§2 and 3.

Let $C(x)$ denote the number of Carmichael numbers less than x, and let $\log_k x$ denote the k-fold iteration of the natural logarithm.

Put, according to [3],

$$F(x) = x \cdot \exp\left(-\log x \cdot \frac{(1 + \log_3 x)}{\log_2 x} \right),$$

and let

$$J(x) = x \cdot \exp\left(-\frac{\log x}{\log_2 x} \left(\log_3 x + \log_4 x + \frac{\log_4 x - 1}{\log_3 x} + \frac{7.1287 \log_4^2 x - 0.2289 \log_4 x + 2.0161}{\log_3^2 x} \right) \right).$$

Then we obtain Table 3 (the values in columns 3, 4 are rounded to integers).

It turns out that $C(x)/F(x)$ decreases relatively fast in accordance with the result $C(x) = o(F(x))$ in [2]. The approximation $J(x)$ relies on the heuristics of [2] and gives rise to a relative error of at most 1.4 percent for all integers in the range $10^{10} \leq x \leq 10^{12}$, and at most 1 percent in the range $25 \cdot 10^9 \leq x \leq 10^{12}$.

TABLE 3

x	$C(x)$	$F(x)$	$J(x)$	$C(x)/F(x)$	$C(x)/J(x)$
10^9	646	547	640	1.18	1.0089
10^{10}	1547	1470	1547	1.05	0.9999
$25 \cdot 10^9$	2163	2189	2173	0.9882	0.9952
10^{11}	3605	4016	3605	0.8977	0.9999
10^{12}	8238	11141	8238	0.7394	0.9999

This is obtained by computing the values of $J(x)$ for all x and $x - 1$, where x is a Carmichael number, and the fact that J increases in the range under consideration.

In [3], Table 4 shows the distribution of Carmichaels less than $25 \cdot 10^9$ in different residue classes. Since the distribution of Carmichaels in the range $< 10^{12}$ is a similar one, we give here only the values for the odd residue classes mod 12.

TABLE 4

Class mod 12	Carms < 25000000000	Carms < 1000000000000
1	2071	7966
3	0	1
5	20	64
7	47	147
9	25	60
11	0	0

ACKNOWLEDGMENT

I wish to thank the referee for his valuable criticisms and the suggested improvement of the $C(x)$-approximation formula in §4.

BIBLIOGRAPHY

1. W. Knödel, *Carmichaelsche Zahlen*, Math. Nachr. **9** (1953), 343–350.
2. C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
3. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.
4. J. D. Swift, Review **13**, Math. Comp. **29** (1975), 338–339.

IBM SCIENTIFIC CENTER HEIDELBERG, TIERGARTENSTRASSE 15, 6900 HEIDELBERG, WEST GERMANY