MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 381–391

THE CARMICHAEL NUMBERS UP TO 10^{15}

R. G. E. PINCH

Dedicated to the memory of D. H. Lehmer

ABSTRACT. There are 105212 Carmichael numbers up to 10^{15} : we describe the calculations. The numbers were generated by a back-tracking search for possible prime factorizations, and the computations checked by searching selected ranges of integers directly using a sieving technique, together with a "large-prime variation".

0. INTRODUCTION

A *Carmichael number* N is a composite number N with the property that for every x prime to N we have $x^{N-1} \equiv 1 \bmod N$. It follows that a Carmichael number N must be squarefree, with at least three prime factors, and that $p-1 \mid N-1$ for every prime p dividing N: conversely, any such N must be a Carmichael number.

For background on Carmichael numbers we refer to Ribenboim [24 and 25]. Previous tables of Carmichael numbers were computed by Pomerance, Selfridge, and Wagstaff [23], Jaeschke [13], Guillaume [11], Keller [14], and Guthmann [12]. Yorinaga [28] also obtained many Carmichael numbers.

We have shown that there are 105212 Carmichael numbers up to 10^{15}, all with at most nine prime factors. Let $C(X)$ denote the number of Carmichael numbers less than X; let $C(d, X)$ denote the number with exactly d prime factors. Table 1 gives the values of $C(X)$ and $C(d, X)$ for $d \leq 9$ and X in powers of 10 up to 10^{15}.

We have used the same methods to calculate the smallest Carmichael numbers with d prime factors for d up to 20. The results are given in Table 2.

It has recently been shown by Alford, Granville and Pomerance [1] that there are infinitely many Carmichael numbers: indeed $C(X) > X^{2/7}$ for sufficiently large X. Their proof is described by Granville [10].

1. SOME PROPERTIES OF CARMICHAEL NUMBERS

In this section we gather together various elementary properties of Carmichael numbers. We assume throughout that N is a Carmichael number with exactly d prime factors, say, $p_1, \ldots, p_d$ in increasing order.

Received by the editor May 12, 1992 and, in revised form, October 8, 1992 and January 5, 1993.

1991 *Mathematics Subject Classification*. Primary 11Y99; Secondary 11A51, 11Y11.

Proposition 1. *Let N be a Carmichael number less than X.*

(1) *Let $r < d$ and put $P = \prod_{i=1}^{r} p_i$. Then $p_{r+1} < (X/P)^{1/(d-r)}$ and p_{r+1} is prime to $p_i - 1$ for all $i \le r$.*

(2) *Put $P = \prod_{i=1}^{d-1} p_i$ and $L = \mathrm{lcm}\{p_1 - 1, \dots, p_{d-1} - 1\}$. Then $Pp_d \equiv 1 \bmod L$ and $p_d - 1$ divides $P - 1$.*

(3) *Each p_i satisfies $p_i < \sqrt{N} < \sqrt{X}$.*

Proof. Parts (1) and (2) follow at once from the fact that $p_i - 1$ divides $N - 1$ for each i. For part (3), consider the largest prime factor p_d. From (2), $N = Pp_d$ and $p_d - 1 \mid P - 1$, so that $p_d < P$. But now $p_d^2 < Pp_d = N$. $\square$

Proposition 2. *Let $P = \prod_{i=1}^{d-2} p_i$. There are integers $2 \le D < P < C$ such that, putting $\Delta = CD - P^2$, we have*

$$p_{d-1} = \frac{(P-1)(P+D)}{\Delta} + 1, \tag{1}$$

$$p_d = \frac{(P-1)(P+C)}{\Delta} + 1, \tag{2}$$

$$P^2 < CD < P^2 \left(\frac{p_{d-2} + 3}{p_{d-2} + 1} \right). \tag{3}$$

Proof. For convenience we put $q = p_{d-1}$ and $r = p_d$. We have $r - 1 \mid Pq - 1$ and $q - 1 \mid Pr - 1$, say

$$D = \frac{Pq - 1}{r - 1} \quad \text{and} \quad C = \frac{Pr - 1}{q - 1}.$$

Since $q < r$ we have $D < P < C$, and since $Pq \ne r$ we have $D \ne 1$, that is, $D \ge 2$. Substituting for r, we have

$$P\left(\frac{Pq - 1}{D} + 1 \right) - 1 = C(q - 1),$$

and so

$$CD(q-1) = P^2 q - P + PD - D.$$

Putting $\Delta = CD - P^2$, we have

$$\Delta(q-1) = (CD - P^2)(q-1) = P^2 - P + PD - D = (P-1)(P+D).$$

So, $\Delta > 0$ and

$$q = \frac{(P-1)(P+D)}{\Delta} + 1;$$

similarly,

$$r = \frac{(P-1)(P+C)}{\Delta} + 1.$$

Now $q \ge p_{d-2} + 2$ and $D < P$, so

$$p_{d-2} + 1 \le \frac{(P-1)(P+D)}{\Delta} < \frac{2P^2}{\Delta},$$

giving

$$CD - P^2 < P^2 \left(\frac{2}{p_{d-2} + 1} \right),$$

whence

$$CD < P^2 \left(\frac{p_{d-2}+3}{p_{d-2}+1}\right)$$

as required. □

Corollary. *There are only finitely many Carmichael numbers* $N = \prod_{i=1}^{d} p_i$ *with a given set of* $d-2$ *prime factors* $p_1, \dots, p_{d-2}$. □

Parts (1) and (2) of Proposition 2 are contained in Satz B(e) of Knödel [15]. The Corollary was obtained by Beeger [2] for the case $d = 3$ and by Duparc [9] in general.

Proposition 3. *Let* $P = \prod_{i=1}^{d-2} p_i$. *Then*
(1) $p_{d-1} < 2P^2$,
(2) $p_d < P^3$.

Proof. We use Proposition 2. Putting $\Delta \geq 1$ and $D < P$ in (1), we have $p_{d-1} < (P-1)(2P)+1 < 2P^2$. Putting $D \geq 2$ and $p_{d-2} \geq 3$ in (3), we have $C \leq 3P^2/4$; substituting this in (2), we have $p_d < P^3$ as required. □

A slightly stronger form of this result was obtained by Duparc [9].

2. Organization of the search

Assume throughout that N is a Carmichael number less than some preassigned bound X and with exactly d prime factors. We obtain all such N as lists of prime factors by a back-tracking search.

We produce successive lists of $p_1, \dots, p_{d-2}$ by looping at each stage over all the primes permitted by Proposition 1(1).

At search level $d-2$ we put $P = \prod_{i=1}^{d-2} p_i$. If P is small enough, then we proceed by using Proposition 2, looping first over all D in the range 2 to $P-1$, and then over all C with CD satisfying the inequalities of Proposition 2(3). For each such pair (C, D), we test whether the values of p_{d-1} and p_d obtained from 2(1) and 2(2) are integral and, if so, prime. Finally, we test whether $N-1$ is divisible by $p_{d-1}-1$ and p_d-1.

If the value of P at level $d-2$ is large, then we loop over all values of p_{d-1} permitted by Proposition 1(1) and Proposition 3(1). Now put $L = \operatorname{lcm}\{p_1-1, \dots, p_{d-1}-1\}$. The innermost loop runs over all primes p with $Pp \equiv 1 \bmod L$ for which $p-1$ divides $P-1$ and which satisfy the bounds of Propositions 1(3) and 3(2). Such p are possible p_d.

This innermost loop is speeded up considerably by splitting the range of such p into two parts. For small values of p we compute P' with $PP' \equiv 1 \bmod L$ and let p run over the arithmetic progression of numbers congruent to $P' \bmod L$, starting at the first term which exceeds p_{d-1}. For each such p we test whether p is prime and $p-1$ divides $P-1$. For large values of p we run over small factors f of $P-1$. Putting $p = (P-1)/f + 1$, we then test whether $Pp \equiv 1 \bmod L$ and p is prime.

We note that testing candidates for p_i for primality is required at every stage of the calculation. We found that precomputing a list of prime numbers up to a suitable limit produced a considerable saving in time.

Finally we note that using Proposition 1(3) ensures that, in the range up to 10^{15}, the candidate p_i are all less than 2^{25}, so that 32-bit integer arithmetic is always sufficient.

3. Checking ranges by sieving

We used a sieving technique to verify that the list of Carmichael numbers produced by the method of §2 was complete in certain ranges.

Suppose that we wish to list those Carmichael numbers in a range up to X which are divisible only by primes less than Y. We precompute the list $\mathscr{L}$ of primes up to Y. We form a table of entries for the integers up to X; for each p in $\mathscr{L}$ we add $\log p$ into the table entries corresponding to numbers t with $t > p$, $t \equiv 0 \bmod p$, and $t \equiv 1 \bmod (p-1)$: that is, $t \geq p^2$ and $t \equiv p \bmod p(p-1)$. At the end of this process we output any N for which the table entry is equal to $\log N$. Such an N has the property that N is squarefree, all the prime factors p of N are in $\mathscr{L}$, and that $N \equiv 1 \bmod (p-1)$ for every p dividing N: that is, N is a Carmichael number whose prime factors are all in $\mathscr{L}$.

From Proposition 1(3), it is sufficient to take $Y = \sqrt{X}$ to obtain all the Carmichael numbers up to X.

The time taken to sieve over all the numbers up to X will be bounded by

$$X + \sum_{p \leq Y} \left\lfloor \frac{X}{p(p-1)} \right\rfloor \leq X + X \sum_{p} \frac{1}{p(p-1)} = \mathrm{O}(X),$$

which is an improvement over a direct search for Carmichael numbers[1] but still considerably slower in practice than the search technique.

We therefore consider a "large-prime variation". After sieving with $Y = X^{\frac{1}{3}}$, we use a further technique to deal with those Carmichael numbers which have a prime factor q greater than $X^{\frac{1}{3}}$. For each prime q in the range $X^{\frac{1}{3}}$ to $X^{\frac{1}{2}}$, we consider all numbers P in the range $q < P \leq X/q$ which satisfy $P \equiv 1 \bmod (q-1)$. For each such P we first test whether $(2^P)^q \equiv 2 \bmod P$. If so, $N = Pq$ is a Fermat pseudoprime to base 2 and hence a candidate to be a Carmichael number. The number of P tested at this stage is

$$\sum_{X^{\frac{1}{3}} < q < X^{\frac{1}{2}}} \frac{X}{q(q-1)} = \mathrm{O}(X^{\frac{2}{3}}).$$

Let C_X denote the number of P which pass on to the second stage. We next factorize such P, checking that the primes p dividing P are distinct, less than q and have the property that $N \equiv 1 \bmod (p-1)$. If so, then N is a Carmichael number with q as largest prime factor. The time taken to perform the second stage, using trial division, is $\mathrm{O}(\sqrt{P/q}) = \mathrm{O}(X^{\frac{1}{3}})$ for each value of P coming from a given prime q, so $\mathrm{O}(C_X X^{\frac{1}{3}})$ in total. Hence, the total time taken for the large prime variation is $\mathrm{O}(X^{\frac{2}{3}} + C_X X^{\frac{1}{3}})$. Since C_X is noticeably smaller than $X^{\frac{2}{3}}$, the large-prime variation gives an improvement over the estimate in the previous paragraph.

[1]Testing the condition $2^{N-1} \equiv 1 \bmod N$ for all N up to X would take time $\mathrm{O}(X \log X)$.

4. Comparison with existing tables

Carmichael in his original paper [3] gave four examples with three prime factors and later [4] a further ten examples with three prime factors and one example with four prime factors. Swift [26] described a computation of the Carmichael numbers to 10^9, searching over possible lists of prime factors, and discusses earlier tables. Yorinaga [28] gave examples of Carmichael numbers with up to 15 prime factors. Pomerance, Selfridge, and Wagstaff [23] listed the Fermat pseudoprimes base 2 up to $25 \cdot 10^9$, and selected the Carmichael numbers from this list by testing the prime factors. Jaeschke [13] computed the Carmichael numbers up to 10^{12} by a search strategy. These results are summarized by Ribenboim [24, 25]. Guillaume [11] computed the Carmichael numbers up to 10^{12} using a method similar to the "large-prime variation". Keller [14] obtained the Carmichael numbers up to 10^{13} by a search strategy and Guthmann [12] used a sieving method very similar to that of §3 on a vector computer to obtain the Carmichael numbers up to 10^{14}.

Our results are consistent with the statistics of the computations described above with two exceptions. Jaeschke [13] reports three fewer Carmichael numbers up to 10^{12}. He has stated[2] that this discrepancy is due to his computer program having terminated prematurely when testing numbers very close to the upper bound of the range. Keller [14] reports one less Carmichael number up to 10^{13}. He has stated[3] that this was missed by a book-keeping error.

We have further checked our tables by extracting the Carmichael numbers from the tables of Fermat pseudoprimes base 2 of Pomerance, Selfridge, and Wagstaff [23], and Pinch [20]. Morain has checked our tables up to 10^{12} against those of Guillaume. In each case there is no discrepancy.

Keller has recently verified the computation up to 10^{15} by a different method.

5. Description of the calculations

We ran the search procedure of §2 with upper limits of $X = 10^n$ for each value of n up to 15 independently. As a consequence, the list of Carmichael numbers up to 10^{14} was in effect computed twice, that up to 10^{13} three times and so on. The computer programs were written in C, using 32-bit integer arithmetic, and run on a Sun 3/60 or a Sparc workstation. As a check, both on the programs and the results, some of the runs, including all those up to 10^{12}, were duplicated using the rather strict Norcroft C compiler on an IBM 3084Q mainframe. A total of about 200 hours of CPU time was required. All the results were consistent.

The sieving process of §3 turned out to be too expensive to run over the whole range up to 10^{15}. We therefore applied the sieving technique to various subranges.

As a preliminary check, we ran the "large-prime variation" for Carmichael numbers up to 10^{12} with a prime factor between 10^4 and 10^6, and for Carmichael numbers up to 10^{15} with a prime factor between 10^5 and $10^{7.5}$. The lists matched those found by the search process: there were 2347 such numbers in the list up to 10^{12}, and 4245 in the list up to 10^{15}. These checks took about 100 hours of CPU time on a Sun 3/60 workstation.

[2] Letter dated 21 January 1992.

[3] Electronic mail dated 5 May 1992.

In order to check our results against those of [13], we carried out the sieve for the range $10^{12} - 10^{10}$ to 10^{12} using primes up to 10^5. The search method had previously found 24 Carmichael numbers in this range, 20 having all prime factors less than 10^5. The sieve found these 20 as expected, and the run of the large-prime variation for this range had already found the other four. This check took about 20 hours of CPU time on a Sparc workstation.

The sieving method was run up to 10^{12} with a set of primes including those up to 10^6 as part of the calculations in Pinch [20].

We also used the sieve on a number of randomly chosen intervals of length 10^6 up to 10^{15}. In each case the results were again consistent with the results of the search.

6. Statistics

Let $C(X)$ denote the number of Carmichael numbers less than X, and $C(d, X)$ denote the number which have exactly d prime factors. In Table 1 we give $C(d, X)$ and $C(X)$ for values of X up to 10^{15}. No Carmichael number in this range has more than nine prime factors. We have $C(10^{15}) = 105212$.

Table 1. The number of Carmichael numbers with d prime factors up to 10^{15}

	d							
$\log_{10} X$	3	4	5	6	7	8	9	total
3	1	0	0	0	0	0	0	1
4	7	0	0	0	0	0	0	7
5	12	4	0	0	0	0	0	16
6	23	19	1	0	0	0	0	43
7	47	55	3	0	0	0	0	105
8	84	144	27	0	0	0	0	255
9	172	314	146	14	0	0	0	646
10	335	619	492	99	2	0	0	1547
11	590	1179	1336	459	41	0	0	3605
12	1000	2102	3156	1714	262	7	0	8241
13	1858	3639	7082	5270	1340	89	1	19279
14	3284	6042	14938	14401	5359	655	27	44706
15	6083	9938	29282	36907	19210	3622	170	105212

In Table 2 we give the smallest Carmichael number with d prime factors for d up to 20.

In Table 3 (see p. 388) we tabulate the function $k(X)$, defined by Pomerance, Selfridge, and Wagstaff [23] by

$$C(X) = X \exp\left(-k(X)\frac{\log X \log\log\log X}{\log\log X}\right),$$

and the ratios $C(10^n)/C(10^{n-1})$ investigated by Swift [26]. Pomerance, Selfridge, and Wagstaff [23] proved that $\liminf k \geq 1$ and suggested that $\limsup k$ might be 2, although they also observed that within the range of their tables $k(X)$ is decreasing. This decrease is reversed between 10^{13} and 10^{14}; Swift's ratio, again initially decreasing, also increases again before 10^{15}. Pomerance [21, 22] gave a heuristic argument suggesting that $\lim k = 1$.

TABLE 2. The smallest Carmichael numbers with d prime factors, $3 \leq d \leq 20$

d	N factors
3	561 3.11.17
4	41041 7.11.13.41
5	825265 5. 7.17.19.73
6	321197185 5.19.23.29.37.137
7	5394826801 7.13.17.23.31.67.73
8	232250619601 7.11.13.17.31.37.73.163
9	9746347772161 7.11.13.17.19.31.37.41.641
10	1436697831295441 11.13.19.29.31.37.41.43.71.127
11	60977817398996785 5. 7.17.19.23.37.53.73.79.89.233
12	7156857700403137441 11.13.17.19.29.37.41.43.61.97.109.127
13	1791562810662585767521 11.13.17.19.31.37.43.71.73.97.109.113.127
14	87674969936234821377601 7.13.17.19.23.31.37.41.61.67.89.163.193.241
15	6553130926752006031481761 11.13.17.19.29.31.41.43.61.71.73.109.113.127.181
16	1590231231043178376951698401 17.19.23.29.31.37.41.43.61.67.71.73.79. 97.113.199
17	35237869211718889547310642241 13.17.19.23.29.31.37.41.43.61.67.71.73. 97.113.127.211
18	32809426840359564991177172754241 13.17.19.23.29.31.37.41.43.61.67.71.73. 97.127.199.281.397
19	2810864562635368426005268142616001 13.17.19.23.29.31.37.41.43.61.67.71.73.109.113.127.151.281.353
20	349407515342287435050603204719587201 11.13.17.19.29.31.37.41.43.61.71.73.97.101.109.113.151.181.193.641

In Table 4 (next page) we give the number of Carmichael numbers in each class modulo m for $m = 5, 7, 11$, and 12.

In Tables 5 and 6 (see p. 389) we give the number of Carmichael numbers divisible by primes p up to 97. In Table 5 we count all Carmichael numbers divisible by p: in Table 6 we count only those for which p is the smallest prime factor. The largest prime factor of a Carmichael number up to 10^{15} is 21792241, dividing

$$949803513811921 = 17 \cdot 31 \cdot 191 \cdot 433 \cdot 21792241,$$

and the largest prime to occur as the smallest prime factor of a Carmichael number in this range is 72931, dividing

$$651693055693681 = 72931 \cdot 87517 \cdot 102103.$$

TABLE 3. The functions $k(10^n)$ and $C(10^n)/C(10^{n-1})$

n	$k(10^n)$	$C(10^n)/C(10^{n-1})$
3	2.93319	
4	2.19547	7.000
5	2.07632	2.286
6	1.97946	2.688
7	1.93388	2.441
8	1.90495	2.429
9	1.87989	2.533
10	1.86870	2.396
11	1.86421	2.330
12	1.86377	2.286
13	1.86240	2.339
14	1.86293	2.319
15	1.86301	2.353

TABLE 4. The number of Carmichael numbers congruent to c modulo m for $m = 5, 7, 11, 12$

m	c	25.10^9	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}
5	0	203	312	627	1330	2773	5814
	1	1652	2785	6575	15755	37467	90167
	2	82	154	327	702	1484	3048
	3	102	172	344	725	1463	3059
	4	124	182	368	767	1519	3124
7	0	401	634	1334	2774	5891	12691
	1	1096	1885	4613	11447	28001	69131
	2	105	186	432	967	2109	4599
	3	152	232	496	1055	2178	4707
	4	129	211	450	985	2122	4592
	5	138	222	454	1033	2224	4777
	6	142	235	462	1018	2181	4715
11	0	335	547	1324	3006	7032	16563
	1	640	1131	2770	6786	16548	40891
	2	139	217	473	1068	2361	5338
	3	142	220	457	1045	2348	5319
	4	104	187	442	1026	2317	5261
	5	152	243	466	1066	2370	5316
	6	116	198	440	1061	2400	5384
	7	122	195	458	1023	2223	5165
	8	129	222	475	1107	2450	5449
	9	131	218	465	1042	2285	5179
	10	153	227	471	1049	2372	5347
12	1	2071	3462	7969	18761	43760	103428
	3	0	0	1	2	2	5
	5	20	32	64	124	228	448
	7	47	75	147	289	547	1027
	9	25	36	60	103	165	294
	11	0	0	0	0	4	10

It is well known that the probability, $P_R(N)$, say, of an odd composite N passing the Rabin test for a random base modulo N is at most $\frac{1}{4}$: it is easy to show that this bound is achieved if and only if N is a Carmichael number with exactly three prime factors, all $\equiv 3 \bmod 4$; call this class $\mathscr{C}_3$.

TABLE 5. The number of times a prime $p \le 97$ occurs in a Carmichael number

p	25.10^9	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}
3	25	36	61	105	167	299
5	203	312	627	1330	2773	5814
7	401	634	1334	2774	5891	12691
11	335	547	1324	3006	7032	16563
13	483	807	1784	3998	9045	20758
17	293	489	1182	2817	6640	16019
19	372	608	1355	3345	7797	18638
23	113	207	507	1282	3135	7716
29	194	336	832	2094	5158	12721
31	335	571	1320	3086	7270	17382
37	320	535	1270	2926	6826	16220
41	227	390	1001	2418	5896	14344
43	184	296	772	1920	4663	11594
47	53	80	199	492	1223	2873
53	92	160	351	813	2041	5143
59	26	41	92	262	644	1611
61	269	453	1075	2542	6047	14429
67	110	178	407	1063	2540	6306
71	104	194	521	1320	3351	8546
73	198	348	849	2145	4925	11929
79	64	107	247	686	1728	4318
83	14	24	56	137	340	838
89	68	131	320	788	1951	4981
97	123	193	495	1277	3123	7594

TABLE 6. The number of times a prime $p \le 97$ occurs as the least prime factor of a Carmichael number

p	25.10^9	10^{11}	10^{12}	10^{13}	10^{14}	10^{15}
3	25	36	61	105	167	299
5	202	309	624	1325	2765	5797
7	364	579	1218	2557	5461	11874
11	263	428	1071	2509	5979	14397
13	237	431	1058	2462	5699	13514
17	117	206	496	1318	3244	8114
19	152	244	532	1401	3358	8141
23	37	78	207	535	1360	3317
29	55	103	284	729	1822	4659
31	101	168	390	876	2116	5153
37	60	95	219	551	1401	3418
41	35	68	171	414	1092	2736
43	35	65	168	403	943	2308
47	14	16	36	81	195	459
53	19	30	55	147	363	973
59	2	4	11	43	100	272
61	34	58	148	364	851	1978
67	8	18	50	123	317	815
71	15	25	66	161	389	979
73	14	28	68	175	406	1015
79	4	10	17	66	175	467
83	1	1	4	8	39	79
89	10	16	23	55	148	409
97	10	20	50	106	261	606

McDonnell [18] showed that if $P_R(N) \geq \frac{11}{64}$ for $N \geq 11$, then $N \in \mathscr{C}_3$, or else one of $3N+1$, $8N+1$ is a square. (Damgård, Landrock, and Pomerance [5, 6] prove a similar result for $P_R(N) > \frac{1}{8}$.) Numbers in $\mathscr{C}_3$ are also those for which Davenport's "maximal 2-part" refinement [7] gives no strengthening of the Rabin test. There are 487 $\mathscr{C}_3$-numbers up to 10^{15}, and 868 up to 10^{16}, the first being $8911 = 7 \cdot 19 \cdot 67$.

Lidl, Müller, and Oswald [16, 17, 19] characterize a *strong Fibonacci pseudoprime* as a Carmichael number $N = \prod p_i$ with one of the following properties: either (*Type* I) an even number of the p_i are $\equiv 3 \bmod 4$ with $2(p_i+1) \mid N-1$ for the $p_i \equiv 3 \bmod 4$ and $p_i + 1 \mid N \pm 1$ for the $p_i \equiv 1 \bmod 4$; or (*Type* II) there is an odd number of p_i, all $\equiv 3 \bmod 4$, and $2(p_i+1) \mid N - p_i$ for all p_i. (A strong Fibonacci pseudoprime is termed a *strong* (-1)*-Dickson pseudoprime* in [19].) They were not able to exhibit any such numbers. We found just one Type-I strong Fibonacci pseudoprime up to 10^{15}, namely

$$443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331,$$

and none of Type II. This also answers the question of Di Porto and Filipponi [8].

Williams [27] asked whether there are any Carmichael numbers N with an odd number of prime divisors and the additional property that for $p \mid N$, $p+1 \mid N+1$. There are no such Carmichael numbers up to 10^{15}.

Finally we note that $C(274859381237761) = 65019$ gives the smallest value of X for which $C(X) > X^{\frac{1}{3}}$.

7. Acknowledgments

The author is grateful to D. Guillaume, W. Keller, F. Morain, and W. Müller for helpful discussions and for providing preprints and details of unpublished work. Thanks are also due to Professor S. S. Wagstaff, Jr., for providing a file containing the tables described in [23] and to the referee of the first version of this paper for valuable comments.

Bibliography

1. W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (to appear).
2. N. G. W. H. Beeger, *On composite numbers* n *for which* $a^{n-1} \equiv 1 \bmod n$ *for every* a *prime to* n, Scripta Math. **16** (1950), 133–135.
3. R. D. Carmichael, *Note on a new number theory function*, Bull. Amer. Math. Soc. **16** (1909–1910), 232–238.
4. ———, *On composite numbers* P *which satisfy the congruence* $a^{P-1} \equiv 1 \bmod P$, Amer. Math. Monthly **19** (1912), 22–27.
5. I. Damgård and P. Landrock, *Improved bounds for the Rabin primality test*, preprint, 12 March 1992, Coding and Cryptography III, Proc. 3rd IMA Conf. on Coding and Cryptography (M. Ganley, ed.), Cirencester, December 1991 (to appear).
6. I. Damgård, P. Landrock, and C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177–194.
7. J. H. Davenport, *Primality testing revisited*, preprint, 20 April 1992, Proceedings ISSAC 1992 (P. S. Wang, ed.), ACM, New York, 1992.
8. A. Di Porto and P. Filipponi, *A probabilistic primality test based on the properties of certain generalized Lucas numbers*, Advances in Cryptology—Eurocrypt' 88 (C. G. Günther, ed.), Lecture Notes in Comput. Sci., vol. 330, Springer-Verlag, Berlin and New York, 1988, pp. 211–223.

9. H. Duparc, *On Carmichael numbers*, Simon Stevin **29** (1951–1952), 21–24.

10. A. Granville, *Primality testing and Carmichael numbers*, Notices Amer. Math. Soc. **39** (1992), 696–700.

11. D. Guillaume, *Table des nombres de Carmichael inférieurs à* 10^{12}, preprint, May 1991.

12. A. Guthmann, *On the computation of Carmichael numbers*, Universität Kaiserslautern, preprint 218, April 1992.

13. G. Jaeschke, *The Carmichael numbers to* 10^{12}, Math. Comp. **55** (1990), 383–389.

14. W. Keller, *The Carmichael numbers to* 10^{13}, Abstracts Amer. Math. Soc. **9** (1988), 328–329.

15. W. Knödel, *Carmichaelsche Zahlen*, Math. Nachr. **9** (1953), 343–350.

16. R. Lidl and W. B. Müller, *A note on strong Fibonacci pseudoprimes*, Advances in Cryptology—AUSCRYPT '90 (J. Seberry and J. Pieprzyk, eds.), Lecture Notes in Comput. Sci., vol. 453, Springer-Verlag, Berlin and New York, 1990, pp. 311–317.

17. R. Lidl, W. B. Müller and A. Oswald, *Some remarks on strong Fibonacci pseudoprimes*, Applicable Algebra in Engineering, Communication and Computing **1** (1990), 59–65.

18. F. J. McDonnell, *Rabin's algorithm and the proportion of 'liars' for various families of numbers*, University of Warwick, preprint, March 1989.

19. W. B. Müller and A. Oswald, *Dickson pseudoprimes and primality testing*, Advances in cryptology—EUROCRYPT '91 (D.W. Davies, ed.), Lecture Notes in Comput. Sci., vol. 547, Springer-Verlag, Berlin and New York, 1991, pp. 512–516.

20. R. G. E. Pinch, *The pseudoprimes up to* 10^{12}, preprint, June, 1992.

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

22. ——, *Two methods in elementary analytic number theory*, Number Theory and Applications (R. A. Mollin, ed.), Kluwer, Dordrecht, 1989.

23. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* 25.10^9, Math. Comp. **35** (1980), 1003–1026.

24. P. Ribenboim, *The book of prime number records*, Springer-Verlag, Berlin and New York, 1988.

25. ——, *The little book of big primes*, Springer-Verlag, Berlin and New York, 1991.

26. J. D. Swift, *Review* 13—*Table of Carmichael numbers to* 10^9, Math. Comp. **29** (1975), 338–339.

27. H. C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), 133–143.

28. M. Yorinaga, *Numerical computation of Carmichael numbers*, Math. J. Okayama Univ. **20** (1978), 151–163; II, **21** (1979), 183–205.

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS, UNIVERSITY OF CAMBRIDGE, 16 MILL LANE, CAMBRIDGE CB2 1SB, UNITED KINGDOM
E-mail address: rgep@phx.cam.ac.uk