Carmichael numbers with small index

Richard G.E. Pinch

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K. rgep@chalcedon.demon.co.uk

Introduction

We define the *index* of a Carmichael number N as the quotient $i(N) = (N-1)/\lambda(N)$. We show that $i(N) \to \infty$ and $N \to \infty$ by giving an algorithm for listing all the numbers with given value of i. We illustrate by listing numbers with $i \le 100$.

Carmichael numbers

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

For background on Carmichael numbers and details of previous computations we refer to our previous paper [3]: in that paper we described the computation of the Carmichael numbers up to 10^{15} and presented some statistics. These computations have since been extended to 10^{20} (see another poster at this conference).

We define the Carmichael *lambda function* $\lambda(N)$ to be the exponent of the multiplicative group $(\mathbf{Z}/N)^*$. The definition of Carmichael number is equivalent to the condition $\lambda(N)|N-1$. We define the *index* $i(N)$ to be the integer $(N-1)/\lambda(N)$.

Somer [4] proved a result implying that $i(N) \to \infty$ as $N \to \infty$.

Theorem 1. *There are only finitely many Carmichael numbers of given index i.*

We give a simple proof of this result and an algorithm for computing all N with a given value of i. We illustrate by listing the Carmichael numbers with $i \le 100$.

In Table 1 we list the Carmichael numbers known to have index less than 100.

Carmichael numbers with given index

We fix parameters r, I and ℓ and aim to list all Carmichael numbers $N > M$ with r prime factors and index at most I. Since the index of such a Carmichael number is at least 2^{r-1} we see that for given I there are only finitely many values of r which can occur.

We choose $M = 10^{15}$ and use the results of [3] to list the Carmichael numbers less than M.

Let $E(P,q,d,k)$ be the set of numbers N such that $N = Pq_1 \cdots q_d$ with the q_i primes such that $q < q_1 < \cdots < q_d$ and such that N satisfies $\frac{N-1}{\phi(N)} = k$.

Clearly

$$E(P,q,d,k) = \bigcup_{q_1 > q} E(Pq_1, q_1, d-1, k)$$

where q_1 runs over primes greater than q. We show that the union is in fact finite. Put $Q = \prod_{i=1}^{d} q_i$. We have $N = PQ$ and $\frac{N-1}{\phi(N)} = \frac{PQ-1}{\phi(P)\phi(Q)} = k$.

If $k < \frac{P}{\phi(P)}$ then for $N = PQ \in E(P,q,d,k)$ we have

$$\frac{P}{\phi(P)} > k = \frac{PQ-1}{\phi(PQ)} = \left(1 - \frac{1}{PQ}\right)\frac{P}{\phi(P)}\frac{Q}{\phi(Q)}$$

so that

$$1 > \left(1 - \frac{1}{PQ}\right)\frac{Q}{\phi(Q)} > \left(1 - \frac{1}{Q}\right)\frac{Q}{\phi(Q)} = \frac{Q-1}{\phi(Q)}$$

so that $\phi(Q) > Q-1$, which is impossible.

If $\frac{P}{\phi(P)} \le k$ then for $N = PQ \in E(P,q,d,k)$ we have

$$q_1 < \left(1 - \left(\frac{1}{k}\frac{P}{\phi(P)}\right)^{1/d}\right)^{-1}$$

as an upper bound for q_1.

We now observe that if n is a Carmichael number of index i with d prime factors, then $\lambda(n) \le \phi(n)/2^{d-1} < (n-1)/2^{d-1}$, so that $i \ge 2^{d-1}$. Hence the set of Carmichael numbers with index $i \le I$ is contained in

$$\bigcup_{1<j<i<I,\, 2^{d-1} \le I} E(1,2,d,i/j)$$

which is finite.

We have established Theorem 1. The proof gives a recursive procedure for finding all Carmichael number with given index.

Rate of growth of the index

Alford, Granville and Pomerance [1] show that there are infinitely many Carmichael numbers. For the numbers N produced by their argument we have $\log \lambda(N)$ of the order of a power of $\log\log N$, so that the index $i(N)$ is greater than $N^{1-\varepsilon}$.

There is a similar heuristic argument suggesting that there should be infinitely many Carmichael numbers N with $i(N) > N^A$ for an absolute constant A. It would be interesting to prove such a result.

i	N	factors
5	6601	$7 \cdot 23 \cdot 41$
7	561	$3 \cdot 11 \cdot 17$
18	42018333841	$11 \cdot 47 \cdot 1049 \cdot 77477$
18	55462177	$17 \cdot 23 \cdot 83 \cdot 1709$
18	8885251441	$11 \cdot 47 \cdot 1109 \cdot 15497$
21	10585	$5 \cdot 29 \cdot 73$
22	2465	$5 \cdot 17 \cdot 29$
23	1105	$5 \cdot 13 \cdot 17$
25	11921001	$3 \cdot 29 \cdot 263 \cdot 521$
31	62745	$3 \cdot 5 \cdot 47 \cdot 89$
37	11972017	$43 \cdot 433 \cdot 643$
37	67902031	$43 \cdot 271 \cdot 5827$
39	334153	$19 \cdot 43 \cdot 409$
43	52633	$7 \cdot 73 \cdot 103$
44	15841	$7 \cdot 31 \cdot 73$
45	8911	$7 \cdot 19 \cdot 67$
47	2821	$7 \cdot 13 \cdot 31$
48	1729	$7 \cdot 13 \cdot 19$
49	1208361237478669	$53 \cdot 653 \cdot 26479 \cdot 1318579$
50	4199932801	$29 \cdot 499 \cdot 503 \cdot 577$
52	206955841	$17 \cdot 71 \cdot 277 \cdot 619$
53	1271325841	$17 \cdot 31 \cdot 179 \cdot 13477$
54	4169867689	$13 \cdot 29 \cdot 383 \cdot 28879$
55	271794601	$13 \cdot 19 \cdot 743 \cdot 1481$
60	6840001	$7 \cdot 17 \cdot 229 \cdot 251$
61	1962804565	$5 \cdot 103 \cdot 149 \cdot 25579$
65	1745094470986967126132341	$109 \cdot 173 \cdot 2063 \cdot 179687 \cdot 249649359173$
65	365376903642671522645639268043801	$67 \cdot 3677 \cdot 5147 \cdot 220523477 \cdot 1306663196317481$
65	844154128953833755776750022681	$73 \cdot 599 \cdot 24989 \cdot 546558263 \cdot 1413470422229$
67	11985924995083901	$29 \cdot 101 \cdot 1427 \cdot 16349 \cdot 175403$
67	410041	$41 \cdot 73 \cdot 137$
70	162401	$17 \cdot 41 \cdot 233$
76	4752717761	$11 \cdot 17 \cdot 107 \cdot 173 \cdot 1373$
81	35575075809505	$5 \cdot 197 \cdot 223 \cdot 353 \cdot 458807$
81	299195475860503405763765113861	$83 \cdot 4919 \cdot 10243 \cdot 4694111 \cdot 15241214653541$
82	1496405933740345	$5 \cdot 47 \cdot 317 \cdot 40253 \cdot 499027$
83	142159958924185	$5 \cdot 37 \cdot 107 \cdot 58379 \cdot 123017$
83	158664761899885	$5 \cdot 37 \cdot 107 \cdot 53987 \cdot 148469$
83	204370370140285	$5 \cdot 37 \cdot 107 \cdot 48677 \cdot 212099$
83	24831908105124205	$5 \cdot 29 \cdot 719 \cdot 3023 \cdot 78790717$
83	5969360321185871106354001	$31 \cdot 251 \cdot 31583 \cdot 2146673 \cdot 11315483219$
85	171189355538562901	$23 \cdot 71 \cdot 983 \cdot 1031 \cdot 103437589$
90	3778118040573702001	$11 \cdot 47 \cdot 1051 \cdot 67967 \cdot 102302009$
92	520178982961	$11 \cdot 29 \cdot 131 \cdot 607 \cdot 20507$
94	12782849065	$5 \cdot 7 \cdot 269 \cdot 317 \cdot 4283$
95	8956911601	$11 \cdot 17 \cdot 127 \cdot 131 \cdot 2879$
97	5472940991761	$199 \cdot 241 \cdot 863 \cdot 132233$
97	721574219707441	$167 \cdot 241 \cdot 5039 \cdot 3557977$
97	9729822470631481	$127 \cdot 409 \cdot 110681 \cdot 1692407$
97	83565865434172201	$103 \cdot 1993 \cdot 9551 \cdot 42622169$
99	438253965870337	$43 \cdot 139 \cdot 49409 \cdot 1484009$

Carmichael numbers with small index

References

[1] W.R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Maths **139** (1994), no. 3, 703–722.

[2] Jean-Marie De Koninck and Claude Levesque (eds.), *Number theory: proceedings of the international number theory conference, Université de Laval, 1987*, Berlin, Walter de Gruyter, 1989.

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

[4] Lawrence Somer, *On Fermat d-pseudoprimes*, in De Koninck and Levesque [2], pp. 841–860.