The Carmichael numbers up to 10^{21}

Richard G.E. Pinch

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.

rgep@chalcedon.demon.co.uk

Introduction

We extend our previous computations to show that there are 20138200 Carmichael numbers up to 10^{21}. As before, the numbers were generated by a back-tracking search for possible prime factorisations together with a "large prime variation". We present further statistics on the distribution of Carmichael numbers.

Organisation of the search

We used improved versions of strategies first described in [2].

The principal search was a depth-first back-tracking search over possible sequences of primes factors $p_1, \dots, p_d$. Put $P_r = \prod_{i=1}^{r} p_i$, $Q_r = \prod_{i=r+1}^{d} p_i$ and $L_r = \operatorname{lcm}\{p_i - 1 : i = 1, \dots, r\}$. We find that Q_r must satisfy the congruence $N = P_r Q_r \equiv 1 \bmod L_r$ and so in particular $Q_d = p_d$ must satisfy a congruence modulo L_{d-1}: further $p_d - 1$ must be a factor of $P_{d-1} - 1$. We modified this to terminate the search early at some level r if the modulus L_r is large enough to limit the possible values of Q_r, which may then be factorised directly.

We also employed the variant based on proposition 2 of [2] which determines the finitely many possible pairs (p_{d-1}, p_d) from P_{d-2}. In practice this was useful only when $d = 3$ allowing us to determine the complete list of Carmichael numbers with three prime factors up to 10^{21}.

A large prime variation

Finally we employed a different search over large values of p_d, in the range $2.10^6 < p_d < 10^{9.5}$, using the property that $P_{d-1} \equiv 1 \bmod (p_d - 1)$.

If q is a prime in this range, we let P run through the arithmetic progression $P \equiv 1 \bmod q - 1$ in the range $q < P < X/q$ where $X = 10^{21}$. We first check whether $N = Pq$ satisfies $2^N \equiv 2 \bmod N$: it is sufficient to test whether $2^N \equiv 2 \bmod P$ since the congruence modulo q is necessarily satisfied. If this condition is satisfied we factorise P and test whether $N \equiv 1 \bmod \lambda(N)$.

The approximate time taken for $X^t \le q < X^{1/2}$ is

$$\sum_{X^t < q < X^{1/2}} \frac{X}{q^2} \approx X^{1-t}.$$

Statistics

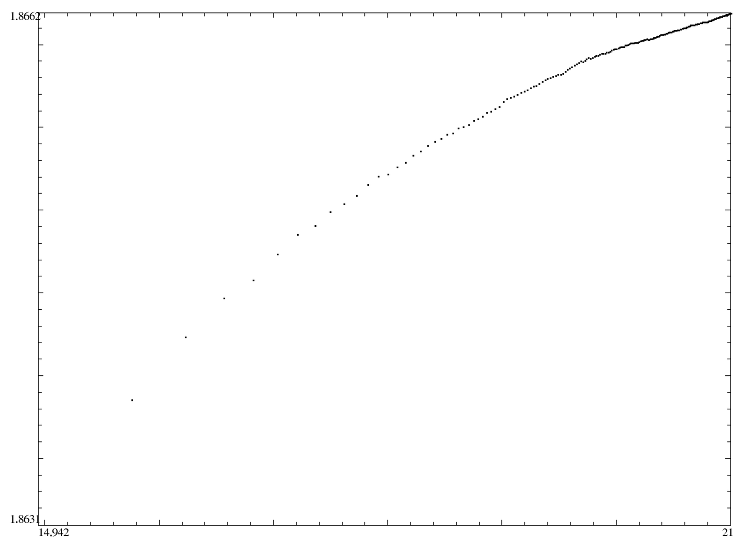
n	12	13	14	15	16	17	18	19	20	21
$C(n)$	8241	19279	44706	105212	246683	585355	1401644	3381806	8220777	20138200

Distribution of Carmichael numbers up to 10^{21}.

X	3	4	5	6	7	8	9	10	11	12	total
3	1	0	0	0	0	0	0	0	0	0	1
4	7	0	0	0	0	0	0	0	0	0	7
5	12	4	0	0	0	0	0	0	0	0	16
6	23	19	1	0	0	0	0	0	0	0	43
7	47	55	3	0	0	0	0	0	0	0	105
8	84	144	27	0	0	0	0	0	0	0	255
9	172	314	146	14	0	0	0	0	0	0	646
10	335	619	492	99	2	0	0	0	0	0	1547
11	590	1179	1336	459	41	0	0	0	0	0	3605
12	1000	2102	3156	1714	262	7	0	0	0	0	8241
13	1858	3639	7082	5270	1340	89	1	0	0	0	19279
14	3284	6042	14938	14401	5359	655	27	0	0	0	44706
15	6083	9938	29282	36907	19210	3622	170	0	0	0	105212
16	10816	16202	55012	86696	60150	16348	1436	23	0	0	246683
17	19539	25758	100707	194306	172234	63635	8835	340	1	0	585355
18	35586	40685	178063	414660	460553	223997	44993	3058	49	0	1401644
19	65309	63343	306310	849564	1159167	720406	196391	20738	576	2	3381806
20	120625	98253	514381	1681744	2774702	2148017	762963	114232	5804	56	8220777
21	224763	151566	846627	3230120	6363475	6015901	2714473	547528	42764	983	20138200

Values of $C(X)$ and $C_d(X)$ for X in powers of 10 up to 10^{21}.

We have shown that there are 20138200 Carmichael numbers up to 10^{21}, all with at most 12 prime factors. We let $C(X)$ denote the number of Carmichael numbers less than X and $C(d, X)$ denote the number with exactly d prime factors. Table 1 gives the values of $C(X)$ and Table 2 the values of $C(d, X)$ for X in powers of 10 up to 10^{21}.



$k(X)$ versus $\log_{10} X$.

In Table 3 and Figure 1 we tabulate the function $k(X)$, defined by Pomerance, Selfridge and Wagstaff [3] by

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

They proved that $\liminf k \ge 1$ and suggested that $\limsup k$ might be 2, although they also observed that within the range of their tables $k(X)$ is decreasing: Pomerance [4],[5] gave a heuristic argument suggesting that $\lim k = 1$. The decrease in k is reversed between 10^{13} and 10^{14}: see Figure 1. We find no clear support from our computations for any conjecture on a limiting value of k.

n	$\log C(10^n)/(n \log 10)$	$C(10^n)/C(10^{n-1})$	$k(10^n)$
4	0.21127	7.000	2.19547
5	0.24082	2.286	2.07632
6	0.27224	2.688	1.97946
7	0.28874	2.441	1.93388
8	0.30082	2.429	1.90495
9	0.31225	2.533	1.87989
10	0.31895	2.396	1.86870
11	0.32336	2.330	1.86421
12	0.32633	2.286	1.86377
13	0.32962	2.339	1.86240
14	0.33217	2.319	1.86293
15	0.33480	2.353	1.86301
16	0.33700	2.335	1.86406
17	0.33926	2.373	1.86472
18	0.34148	2.394	1.86522
19	0.34363	2.413	1.86565
20	0.34574	2.431	1.86598
21	0.34781	2.450	1.86619

$C(X)$ as a power of X, the growth of $C(X)$ and the function $k(X)$ for $X = 10^n$ up to 10^{21}.

Conclusion

We consider that there is no clear evidence that $k(x)$ approaches any limit.

References

[1] R.A. Mollin (ed.), *Number theory and its applications*, Dordrecht, Kluwer Academic, 1989, Proceedings of the NATO Advanced Study Institute on Number Theory and Applications.

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

[3] C. Pomerance, J.L. Selfridge, and S.S. Wagstaff jr, *The pseudoprimes up to* 25.10^9, Math. Comp. **35** (1980), no. 151, 1003–1026.

[4] Carl Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.

[5] ———, *Two methods in elementary analytic number theory*, in Mollin [1], Proceedings of the NATO Advanced Study Institute on Number Theory and Applications, pp. 136–161.