# THE CARMICHAEL NUMBERS UP TO $10^{21}$

RICHARD G.E. PINCH

## 1. Introduction

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 [2]: 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 $10^{16}$ [3], $10^{17}$ [4], $10^{18}$ [5], $10^{20}$ [6] and now to $10^{21}$, using similar techniques. We present further statistics and refine a conjecture on the asymptotic distribtion.

## 2. 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 $p_1, \ldots, p_d$. Put $P_r = \prod_{i=1}^{r} p_i$, $Q_r = \prod_{i=r+1}^{d} p_i$ and $L_r = \operatorname{lcm}\{p_i - 1 : i = 1, \ldots, r\}$. 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 $10^{21}$.

### 2.1. A large prime variation.

Finally we employed a different search over large values of $p_d$, in the range $2.10^6 < p_d < 10^{10.5}$, 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

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

*Date*: 4 Feb 2008.

## 3. Statistics

In the Table below we tabulate the function $k(X)$, defined by Pomerance, Selfridge and Wagstaff [7] 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 [8],[9] 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 $k$.

| $n$ | $C(10^n)$ | $k(10^n)$ |
|---|---:|---|
| 3 | 1 | |
| 4 | 7 | 2.19547 |
| 5 | 16 | 2.07632 |
| 6 | 43 | 1.97946 |
| 7 | 105 | 1.93388 |
| 8 | 255 | 1.90495 |
| 9 | 646 | 1.87989 |
| 10 | 1547 | 1.86870 |
| 11 | 3605 | 1.86421 |
| 12 | 8241 | 1.86377 |
| 13 | 19279 | 1.86240 |
| 14 | 44706 | 1.86293 |
| 15 | 105212 | 1.86301 |
| 16 | 246683 | 1.86406 |
| 17 | 585355 | 1.86472 |
| 18 | 1401644 | 1.86522 |
| 19 | 3381806 | 1.86565 |
| 20 | 8220777 | 1.86598 |
| 21 | 20138200 | 1.86619 |

Table 1. Distribution of Carmichael numbers up to $10^{21}$.

## 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] ———, *The Carmichael numbers up to* $10^{16}$, March 1998, `arXiv:math.NT/9803082`.
[4] ———, *The Carmichael numbers up to* $10^{17}$, April 2005, `arXiv:math.NT/0504119`.
[5] ———, *The Carmichael numbers up to* $10^{18}$, April 2006, `arXiv:math.NT/0604376`.
[6] ———, *The Carmichael numbers up to* $10^{20}$, July 2006, Poster for ANTS VII, Berlin.
[7] 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.
[8] Carl Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
[9] ———, *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.

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
*E-mail address*: `rgep@chalcedon.demon.co.uk`