CARMICHAEL NUMBERS WITH SMALL INDEX (ABSTRACT)

RICHARD G.E. PINCH

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^{18} [4].

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 $(N-1)/\lambda(N)$.

Alford, Granville and Pomerance [1] have shown that there are infinitely many Carmichael numbers, but their argument produces numbers N with $i(N) \sim N^{1-\epsilon}$. We consider how small the index of a Carmichael number can be.

Somer [5] proved a result implying that $i(N) \to \infty$ as $N \to \infty$. In this paper 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 $i \leq 100$.

We proceed by showing that for fixed k and z the number of N with exactly k prime factors and $\phi(N)/(N-1) = z$ is finite. We have $\frac{N-1}{\lambda(N)} = \frac{N-1}{\phi(N)} \cdot \frac{\phi(N)}{\lambda(N)}$. But $\frac{\phi(N)}{\lambda(N)}$ is an integer, s say, being the ratio of the order and the exponent of the multiplicative group $(\mathbf{Z}/N)^*$. So we can compute the Carmichael numbers of index i if we can compute the square-free numbers N with $\frac{N-1}{\phi(N)} = \frac{i}{s}$.

We conclude with a heuristic suggesting that there should be many Carmichael numbers N with index less than N^a for fixed a.

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] ———, *The Carmichael numbers up to* 10^{18}, April 2006, Unpublished.

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

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

Date: 4 April 2006.