

# A NEW LOWER BOUND FOR ODD PERFECT NUMBERS

RICHARD P. BRENT AND GRAEME L. COHEN

## ABSTRACT

We describe an algorithm for proving that there is no odd perfect number less than a given bound  $K$  (or finding such a number if one exists). A program implementing the algorithm has been run successfully with  $K = 10^{160}$ , with an elliptic curve method used for the vast number of factorizations required.

## COMMENTS

Only the Abstract is given here. The full paper appeared as [1]. For a sequel which extended the result to  $K = 10^{300}$ , see [2]. The integer factorizations used in the proofs are available by anonymous ftp [3].

## REFERENCES

- [1] R. P. Brent, and G. L. Cohen, “A new lower bound for odd perfect numbers”, *Mathematics of Computation* 53 (1989), 431–437. Supplement, *ibid*, S7–S24. MR 89m:11008. Also appeared as Report TR-CS-88-05, Computer Sciences Laboratory, ANU, February 1988, 50 pp. rpb100.
- [2] R. P. Brent, G. L. Cohen and H. J. J. te Riele, “Improved techniques for lower bounds for odd perfect numbers”, *Mathematics of Computation* 57 (1991), 857–868. MR 92c:11004. rpb116.
- [3] R. P. Brent, *Factor: An Integer Factorization Program for the IBM PC*, Report TR-CS-89-23, Computer Sciences Laboratory, ANU, October 1989, 7 pp. rpb117.

(Brent) COMPUTER SCIENCES LABORATORY, AUSTRALIAN NATIONAL UNIVERSITY, CANBERRA, AUSTRALIA  
*E-mail address:* rpb@cslab.anu.edu.au

(Cohen) SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF TECHNOLOGY, SYDNEY, PO BOX 123,  
BROADWAY, NSW 2007, AUSTRALIA  
*E-mail address:* glcohen@utscsd.oz

---

1991 *Mathematics Subject Classification*. Primary 11-04; Secondary 11A25, 11A51, 11Y05, 11Y70.

*Key words and phrases*. Perfect number, odd perfect number, lower bound, tree search, integer factorization, elliptic curve method, ECM.

The research was carried out while the second author was a Visiting Fellow at the Australian National University.

Copyright © 1989, American Mathematical Society.

Comments © 1993, R. P. Brent.

rpb100a typeset using  $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{L}\mathcal{T}\mathcal{E}\mathcal{X}$ .