

## *Primality-testing Mersenne Numbers (II)*

Article

Accepted Version

Haworth, G. M. ORCID: <https://orcid.org/0000-0001-9896-1448>  
(1986) Primality-testing Mersenne Numbers (II). Abstracts of  
papers presented to the American Mathematical Society, 7 (2).  
pp. 224-225. ISSN 0192-5857 Available at  
<https://centaur.reading.ac.uk/4572/>

It is advisable to refer to the publisher's version if you intend to cite from the  
work. See [Guidance on citing](#).

Publisher: American Mathematical Society

All outputs in CentAUR are protected by Intellectual Property Rights law,  
including copyright law. Copyright and IPR is retained by the creators or other  
copyright holders. Terms and conditions for use of this material are defined in  
the [End User Agreement](#).

[www.reading.ac.uk/centaur](http://www.reading.ac.uk/centaur)

**CentAUR**

Central Archive at the University of Reading

Reading's research outputs online

Abstracts of the American Mathematical Society, Vol. 7, No. 2, pp. 224-225. ISSN 0192-5857:

\*86T-11-857 G M<sup>C</sup>C HAWORTH: 33, Alexandra Rd., Reading, Berks UK, RG1 5PG.  
Primality-testing Mersenne Numbers (II). Preliminary Report.

$M_p = 2^p - 1$ , index  $p$  prime, is a Mersenne Number. Let  $S_1 = 4$  and let  $S_{n+1} = S_n^2 - 2 \bmod M_p$ . The  $M_p$  Lucas-Lehmer primality test ( $M_p$ -LLT) is " $M_p$  prime  $\Leftrightarrow$  residue  $S_{p-1} = 0$ " for  $p > 2$ .

Codes A and B exercised  $M_p$ -LLT [AMS Abstracts, v4 no2 (Feb '83) p196, 83T-10-82] over the  $p < 62982$  range, including all  $M_p$  for which no factor was known. By November '84, Code C had extended the coverage, testing the 1362  $M_p$  for which no factor was known in the range  $62982 < p < 100000$ . The three codes run on the ICL DAP at QMC London and use Fast Fermat-number-transform multiplication.

Code C tested 16  $M_p$  in parallel and checked the squaring modulo  $2^{16} - 1$  without signalling any faults. It confirmed  $M_{86243}$  prime in effectively 2318 seconds and also confirmed 520 other known  $M_p$ -LRs.

The consolidated and filed results comprise:

- a)  $M_{50021} - f_1$ ,  $M_{50023} - f_1$  and 2620  $M_p - f_1$  for  $50024 < p < 100000$
- b) the previous 2828 second-sourced  $M_p$ -LRs for  $p < 50024$
- c) 1837 single-sourced  $M_p$ -LRs for  $50024 < p < 100000$
- d) references to  $M_p - f_1$  tables for  $p < 50000$  and to known  $M_p$ -LR sources.

The author gratefully acknowledges the computing provided by the National DAP Service at Queen Mary College and the assistance of Grant Bowgen and Steve Davies who produced the final computations.

(Received November 8, 1985) (Sponsored by Samuel S. Wagstaff, Jr.)