

Primality-testing Mersenne numbers

Article

Accepted Version

Holmes, S. M., Hunt, D. J., Lake, T. W., Marron, P. J., Reddaway, S. F., Westbury, N. and Haworth, G. M. ORCID: <https://orcid.org/0000-0001-9896-1448> (1983) Primality-testing Mersenne numbers. Abstracts of papers presented to the American Mathematical Society, 4 (2). p. 196. ISSN 0192-5857 Available at <https://centaur.reading.ac.uk/4555/>

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

CentAUR

Central Archive at the University of Reading

Reading's research outputs online

Abstracts of the American Mathematical Society, Vol. 4, No. 2, p. 196. ISSN 0192-5857:

83T-10-82 S M HOLMES, D J HUNT, T W LAKE, P J MARRON, S F REDDAWAY, N WESTBURY and G M^C HAWORTH:
ICL, Reading, RG1 8PN, UK. Primality-testing Mersenne Numbers. 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 Lucas-Lehmer primality test (LLT) is " M_p prime \Leftrightarrow residue $S_{p-1} = 0$ ". We have exercised the LLT on an index-set P using Fast Fermat-number-transform multiplication. Codes A and B ran on an ICL DAP, an SIMD parallel processor having 4096 elementary processing elements. Code C is under test.

P is a comprehensive set of primes for two reasons. First, the code for the relatively complex transform algorithm deserves the fullest testing. Secondly, the LLT is non-constructive and its history includes some incorrect residues which were temporarily thought to 'prove' their M_p composite. We believe an 'LLT proof' must include two independent residue computations. Thus, while we did not include almost all $p < 38220$ like Nelson, P otherwise contains all p for which we knew or presumed the LLT had been applied. P also contains all $p < 62982$ for which we knew of no M_p -factor.

Our codes checked the squaring mod-7 and were run twice over their respective ranges. Code A for $p < 31488$ tested M_{31487} in 142 seconds; Code B for $p < 62976$ tested M_{62929} in 562 seconds.

For some 2828 p less than the previous search-limit of 50024 we confirmed and filed a definitive set of residues. We thus validated the results, as sometimes corrected, of Hurwitz/Selfridge, Kravitz/Berg, Gillies, Tuckerman, Nickel/Noll and Nelson/Slowinski. For the range $50024 < p < 62982$, our 475 new residues are all non-zero and so reveal no new prime M_p : we invite their confirmation.

(Received October 22, 1982) (Introduced by R. P. Brent)