Primality-testing Mersenne Numbers (II)

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

*86T-11-857 G M^{c}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.)