MATHEMATICS OF COMPUTATION, VOLUME 35, NUMBER 152
OCTOBER 1980, PAGES 1387–1390

The 25th and 26th Mersenne Primes

By Curt Noll and Laura Nickel

Abstract. The 25th and 26th Mersenne primes are $2^{21701} - 1$ and $2^{23209} - 1$, respectively. Their primality was determined with an implementation of the Lucas-Lehmer test on a CDC Cyber 174 computer. The 25th and 26th even perfect numbers are $(2^{21701} - 1)\, 2^{21700}$ and $(2^{23209} - 1)\, 2^{23208}$, respectively.

Definitions.

Mersenne number – an integer of the form $M_n = 2^n - 1$.

Mersenne prime – a Mersenne number that is prime.

Perfect number – a natural number n such that the factors of n less than n sum to n.

It is known that if M_p is prime, p is prime; the converse is false. The test for primality was discovered by Lucas in 1876 and improved upon by Lehmer in 1930. The test, known as the Lucas-Lehmer test, is as follows:

Given an odd prime p

let $u_2 = 4$,

$$u_3 \equiv u_2^2 - 2 \pmod{2^p - 1},$$
$$\vdots \qquad \vdots$$
$$u_n \equiv u_{n-1}^2 - 2 \pmod{2^p - 1},$$

then $2^p - 1$ is prime iff $u_p \equiv 0$ [3].

To implement the test, we represented the required numbers in $d = \lceil p/47 \rceil$ digits in base $2^{47} = \beta$. The squaring of the multi-precision integers,

$$u = \sum_{i=1}^{d-1} X_i \beta^i,$$

was performed in the following manner:

$$u^2 = \sum_{k=0}^{d-1} X_k^2 \beta^{2k} + \sum_{k=1}^{2d-3} \beta^k \cdot 2 \sum X_i X_j$$

(where the rightmost summation runs over all (i, j) such that $i + j = k$ and $0 \leqslant i < j \leqslant d - 1$). Because the Cyber 174 floating multiply unit operates on integers in a special manner we were able to use the floating and integer multiply instructions to achieve the required 94-bit cross products.

In 1963 Gillies announced that M_{9689}, M_{9941}, and M_{11213} were prime after testing the range from M_{5000} to M_{11400} [1]. In 1971, Tuckerman announced that

Received February 9, 1979; revised October 3, 1979.
1980 *Mathematics Subject Classification.* Primary 10A25.

0025-5718/80/0000-0181/$02.00

M_{19937} was prime after testing through M_{20000} [8]. We later learned that Tuckerman continued testing, and stopped at M_{21000} without finding another prime [9].

We first eliminated 31 M_p for $21000 < p < 21701$ by using a factor table prepared by Wagstaff [10]. In this table, Wagstaff gave factors $< 2^{35}$ for M_p. On October 30, 1978 at 9:40 pm, we found M_{21701} to be prime [6]. The CPU time required for this test was 7:40:20. Tuckerman and Lehmer later provided confirmation of this result [4], [9].

The smallest factor of $2^P - 1$
(from Wagstaff's table)

$F \mid 2^P - 1$ where $F = 2kP + 1$

P	k	P	k	P	k	P	k
21011	1	21997	16175	22853	3	23629	1047
21019	320	22031	7360	22901	3831	23663	220
21023	25	22039	27704	22907	147604	23671	708
21061	8	22063	41	22937	4	23747	4
21067	9	22073	3	22943	1	23761	33095
21089	172	22079	1	22963	12	23801	120
21107	60469	22093	190835	22993	8	23819	1
21121	5520	22109	432	23003	25	23831	13
21179	1	22123	53	23017	135	23833	291
21221	15	22147	5	23021	7080	23857	200
21227	4	22157	267	23027	185140	23873	3
21247	44	22159	3260	23029	267	23879	4
21313	1595	22171	343605	23041	164	23887	36237
21347	4	22193	33396	23053	3	23917	3
21379	57	22247	25	23057	64	23957	3
21383	1	22259	1	23063	21	23977	131355
21391	272828	22271	1	23081	51	23993	95551
21397	284	22273	105800	23087	12	24007	80
21401	348288	22277	2427	23099	1	24019	276
21407	1252	22279	1785	23131	473	24023	12
21419	1	22291	3041	23143	16868	24029	267
21433	3	22343	1	23167	2849	24043	1320
21493	3	22349	7	23197	27	24049	10475
21521	4	22369	95	23251	36	24061	15219
21529	560	22381	191	23269	60	24097	54960
21557	661587	22397	255	23279	1	24103	34997
21587	9	22409	15	23293	8	24107	324
21611	1	22433	541803	23297	4	24109	27356
21617	427	22447	8	23311	9645	24137	7
21649	15	22453	11	23321	528	24169	22287
21661	56	22481	4	23327	536973	24179	4
21727	180	22483	113676	23333	148	24203	1
21767	4	22511	21	23339	1	24229	360
21787	3444	22531	6929	23369	11472	24239	1
21803	1	22543	4220	23371	116	24247	22424
21817	599787	22549	1259	23399	1705	24317	1464
21821	280	22567	13608	23417	7	24329	36
21839	1872	22619	69	23459	1	24337	3
21841	5003	22679	9009	23497	3	24359	16
21863	45	22709	19	23531	205	24371	24
21871	993	22717	3	23539	365	24373	431087
21893	7207	22727	27117	23557	73544	24379	24
21929	118371	22739	4	23567	16264	24391	5
21937	163820	22751	1	23593	132	24413	193552
21943	94436	22769	171564	23599	10700	24419	12
21961	228	22777	24	23603	1	24439	5741
21977	67	22807	89	23609	410431	24499	9

LUCAS RESIDUES (R) FOR $2^P - 1$

(MOD 2^{15}).

P	R	P	R	P	R	P	R
21001	22167	21683	00532	22651	64546	23627	30230
21013	43631	21701	PRIME	22669	04145	23633	20166
21017	15476	21713	25422	22691	16706	23669	22751
21031	52200	21737	70117	22697	23007	23677	15473
21059	54560	21739	32026	22699	47767	23687	20104
21101	72022	21751	64730	22721	77111	23689	35070
21139	14444	21757	55670	22741	36173	23719	77150
21143	17334	21773	22321	22783	36067	23741	61240
21149	34525	21799	22140	22787	31203	23743	47034
21157	16203	21851	55774	22811	21766	23753	67770
21163	54514	21859	44313	22817	70745	23767	75375
21169	41315	21881	67101	22859	26653	23773	41627
21187	24217	21911	26047	22861	01711	23789	70524
21191	57116	21991	03446	22871	36761	23813	76565
21193	67705	22003	75446	22877	25526	23827	25176
21211	56211	22013	46152	22921	77227	23869	75051
21269	32636	22027	72245	22961	07411	23893	13651
21277	66175	22037	31565	22973	56750	23899	37121
21283	03020	22051	45260	23011	04607	23909	61071
21317	66051	22067	56051	23039	20007	23911	35013
21319	03332	22091	72501	23059	31241	23929	43422
21323	27410	22111	37114	23071	37716	23971	44402
21341	44535	22129	56330	23117	72614	23981	46073
21377	74317	22133	34153	23159	12223	24001	45737
21467	25152	22153	26761	23173	42766	24071	53203
21481	00057	22189	43203	23189	77456	24077	61762
21487	21321	22229	45706	23201	56151	24083	47001
21491	44543	22283	12633	23203	21500	24091	55517
21499	57364	22303	23264	23209	PRIME	24113	61244
21503	40475	22307	45066	23227	05321	24121	20440
21517	32365	22367	17214	23291	15151	24133	46206
21523	77053	22391	02566	23357	53157	24151	42421
21559	47601	22441	50616	23431	41570	24181	42161
21563	07120	22469	03633	23447	25202	24197	62523
21569	34402	22541	27254	23473	60476	24223	06747
21577	66332	22571	00214	23509	32462	24251	24431
21589	37570	22573	61446	23537	72274	24281	56776
21599	75740	22613	62600	23549	63457	24407	42761
21601	45246	22621	31456	23561	12032	24421	54676
21613	75545	22637	16617	23563	37447	24443	56170
21647	47635	22639	64640	23581	15772	24469	71364
21673	52310	22643	47455	23623	45666	24473	37661
						24481	76122

Using a revised form of the program, the first-named author then tested M_p for $21701 < p < 24500$. He was able to eliminate 157 M_p using Wagstaff's table. Of the 125 remaining M_p only M_{23209} was found to be prime [7]. The test was completed on February 9, 1979 at 4:06 after 8:39:37 of CPU time. Lehmer and McGrogan later confirmed the result [4], [5].

We give above two tables. The first lists Wagstaff's smallest factor for the 188 M_p which did not require Lucas-Lehmer tests. The second lists the final Lucas residue, in octal (mod 2^{15}), for the 169 Lucas-Lehmer tests that were computed.

On April 9, 1979, Dr. Slowinski and H. Nelson found M_{44497} to be prime by using a similar implementation of the Lucas-Lehmer test on a CRAY 1 [11].

The amount of computation needed to check the primality of M_p is $O(p^3)$. Here, the major computational effort is in squaring the u_k since division by $2^n - 1$ is readily accomplished by shifting. It may be possible to implement a faster multiplication method. For example, Schoenhage and Strassen [2] have an algorithm, based on fast Fourier transforms, which may be promising.

We would like to thank Dr. Jurca, Dr. Lehmer and Dr. Simon for their help, and Dr. Wagstaff for the use of his tables. We would also like to thank California State University at Hayward for use of their computer facilities.

California State University at Hayward
25800 Carlos Bee Boulevard
Hayward, California 94542

1. DONALD B. GILLIES, "Three new Mersenne primes, and a statistical theory," *Math. Comp.*, v. 18, 1964, pp. 93–97.

2. DONALD E. KNUTH, *Art of Computer Programming,* Vol. 2, Addison-Wesley, Reading, Mass., 1963, pp. 269–275.

3. D. H. LEHMER, "On Lucas's test for the primality of Mersenne's numbers," *J. London Math. Soc.*, v. 10, 1935, pp. 162–165.

4. D. H. LEHMER, Private communication with, University of California at Berkeley, Department of Mathematics, Berkeley, Calif. 94720.

5. STEVE McGROGAN, Private communication with, 19450 Yuma Drive, Castro Valley, Calif. 94546.

6. LAURA A. NICKEL & CURT L. NOLL, "The 25th Mersenne prime," *Dr. Dobb's Journal,* v. 4, issue 6, p. 6.

7. CURT L. NOLL, "Discovering the 26th Mersenne prime," *Dr. Dobb's Journal,* v. 4, issue 6, pp. 4–5.

8. BRYANT TUCKERMAN, "The 24th Mersenne prime," *Proc. Nat. Acad. Sci. U.S.A.*, v. 68, 1971, pp. 2319–2320.

9. BRYANT TUCKERMAN, Private communication with, International Business Machines Corporation, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598.

10. S. WAGSTAFF, JR., Private communication with, University of Illinois, Urbana, Illinois 61801.

11. DAVID SLOWINSKI, "Searching for the 27th Mersenne prime," *J. Recreational Math.*, v. 11, 1979, pp. 258–261.