New Mersenne Primes

By Alexander Hurwitz

If p is prime, $M_p = 2^p - 1$ is called a Mersenne number. The primes M_{4253} and M_{4423} were discovered by coding the Lucas-Lehmer test for the IBM 7090. These two new primes are the largest prime numbers known; for other large primes see Robinson [4]. The computing was done at the UCLA Computing Facility. This test is described by the following theorem (see Lehmer [1, p. 443–4]).

THEOREM. *If $S_1 = 4$ and $S_{n+1} = S_n^2 - 2$ then M_p is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$.*

The test takes about 50 minutes of machine time for $p = 4423$. These results bring the number of known Mersenne primes to 20. The values of p for these twenty primes are listed in Table 1.

If M_p is prime it is of interest to know the sign of the least absolute penultimate residue, that is, whether $S_{p-2} \equiv +2^r \pmod{M_p}$ or $S_{p-2} \equiv -2^r \pmod{M_p}$ where $2r = p + 1$. The Lucas-Lehmer test can also be used with $S_1 = 10$. The various penultimate residues of the known Mersenne primes were computed and the results appear in Table 1 (see Robinson [3]).

In addition to testing the above Mersenne primes each Mersenne number with $p < 5000$ was tested unless a factor of M_p was known. The residues of S_{p-1} (mod M_p) are available for checking purposes. The results for $3300 < p < 5000$ are summarized in Table 2. The computer program also found (see [3, p. 844]) that M_{8191} is not prime.

The residue S_{p-1} (mod M_p) for $p > 3300$ is output from the computer in a modified octal notation. That is, the residue is stored in the computer in 35 bit binary words and the output is a word by word conversion of the 35 bit words into octal (base 8) numbers. Thus the leading digit of each is quaternary (base 4). For $p < 3300$ the residue was printed in hexadecimal notation (see Robinson [3] and Riesel [2]).

TABLE 1

p	$S_1 = 4$	$S_1 = 10$	p	$S_1 = 4$	$S_1 = 10$
2			107	−	+
3	+	−	127	+	+
5	+	−	521	−	+
7	−	−	607	−	−
13	+	+	1279	−	−
17	−	+	2203	+	−
19	−	+	2281	−	+
31	+	+	3217	−	+
61	+	+	4253	+	+
89	−	+	4423	−	−

Received November 3, 1961. The preparation of this paper was sponsored by the U. S. Office of Naval Research.

TABLE 2

p	R	p	R
3301	72013	4241	11012
3307	62061	4253	00000
3313	10050	4259	46007
3331	51270	4261	55632
3343	76415	4283	74774
3371	57040	4339	41356
3373	36120	4349	74465
3389	64705	4357	74271
3413	50261	4363	61114
3461	03241	4397	40174
3463	57665	4409	51070
3467	23046	4421	25131
3469	21765	4423	00000
3547	75574	4481	70216
3559	45350	4493	36053
3583	42507	4519	01571
3607	45062	4523	22235
3617	35431	4567	74267
3631	14530	4583	46556
3637	67413	4591	47243
3643	04606	4621	74601
3671	04031	4643	51444
3673	01626	4651	00707
3691	54715	4663	52442
3697	53743	4673	40333
3709	06427	4679	14305
3739	22413	4703	54013
3769	00747	4721	04420
3821	52075	4729	40137
3833	45453	4733	12774
3847	57652	4783	77350
3877	46507	4789	02364
3881	34503	4799	04305
3889	30737	4817	70020
3919	16520	4831	33213
3943	33442	4877	75412
4007	17770	4889	24410
4027	60265	4909	61113
4049	31260	4937	26525
4051	63236	4951	22271
4091	55650	4973	03354
4093	26670	4987	72275
4111	20437		
4133	66046	8191	03624
4157	43640		
4159	62544		
4177	16076		
4201	53211		
4219	51756		
4231	51457		

The five least significant octal digits of the residue appear in Table 2 for each $p > 3300$ tested. If p $(3300 < p < 5000)$ is omitted from Table 2 a factor of $2^p - 1$ is known. Some of these factors are not yet published but were communicated to the author by John Brillhart.

My thanks to the Computing Facility for their help in this work, especially J. L. Selfridge and F. H. Hollander.

University of California at Los Angeles
Los Angeles, California

1. D. H. Lehmer, "An extended theory of Lucas' functions," *Ann. of Math.* v. 31, 1930, p. 419–448.
2. H. Riesel, "Mersenne numbers," *MTAC*, v. 12, 1958, p. 207–213.
3. R. M. Robinson, "Mersenne and Fermat numbers," *Proc. Amer. Math. Soc.* v. 5, 1954, p. 842–846.
4. R. M. Robinson, "A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers," *Proc. Amer. Math. Soc.* v. 9, 1958, p. 673–681.