Three New Mersenne Primes and a Statistical Theory

By Donald B. Gillies

If p is prime, $M_p = 2^p - 1$ is called a Mersenne number. If $u_1 = 4$ and $u_{i+1} = u_{i+1}^2 - 2$, then M_p is prime if and only if $u_{p-1} \equiv 0 (\mathrm{mod}\ M_p)$. This is called the Lucas test (see Lehmer [4]).

The primes M_{9689}, M_{9941}, and M_{11213} which are now the largest known primes, were discovered by Illiac II at the Digital Computer Laboratory of the University of Illinois. The computing times were 1 hour 23 minutes, 1 hour 30 minutes, and 2 hours 15 minutes respectively, and the calculations were checked by repetition. This brings to 23 the number of known Mersenne primes, namely for

p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213.

The Lucas test was applied to all M_p, $p < 12{,}000$ for which no factor is known and the residue u_{p-1} was printed in modified octal (one base 4 digit and 14 octal digits per word). It was verified that there are just 20 prime M_p for $p < 7000$. The last five octal digits of the residues, R, are shown in Table 3 for $7000 < p < 12{,}000$. As an indication of the speed of Illiac II, the residue for M_{8191} took 100 hours on Illiac I (D. J. Wheeler), 5.2 hours on an IBM 7090 (Hurwitz [2]) and 49 minutes on Illiac II. The three values agree.

An Illiac II word has a 45-bit mantissa and a 7-bit exponent. The program checks the multiple precision arithmetic modulo $2^{44} - 1$. Four errors were found in the residues given in Hurwitz [2], namely

p	Correct Residue	Hurwitz' Residue
3637	53313	67413
3847	14400	57652
4397	44327	40174
4421	03013	25131

and ten errors were found in the results of M. Berg and S. Kravitz, privately communicated, for the range $6000 < p < 7000$. For the range $5000 < p < 6000$ the residues agree with those obtained by Hurwitz and Selfridge. In no case has the Illiac II program obtained different results on different runs.

The author is indebted to J. Brillhart for a list of prime factors $< 2^{34}$ of Mersenne numbers. For the range $5000 < p < 17{,}000$ a wider range factor table was computed by Illiac II and Table 4 gives factors q in the range $2^{34} \leqq$ prime factor $\leqq 2^{36}$ not covered by Brillhart. These were used to exclude some values M_p from the Lucas test.

Received June 1, 1963. Revised August 23, 1963.

For $p = 5387, 5591, 5641, 5987, 6089, 6661, 6779, 6907$ and certain larger values, Table 4 gives the first known prime factor. The factor program was written after the Lucas residues were communicated to Kravitz and Berg.

The very large gap in p, 4423 to 9689, between successive Mersenne primes raises the question of what the distribution is of Mersenne primes and of factors of Mersenne composites. I. J. Good [1] suggested that the number of prime $M_p < x$ is asymptotic to 2.3 log log x, and D. Shanks [7] in effect suggests approximately $\frac{5}{\log 10} \log \log x$. It will be suggested in what follows that $\frac{2}{\log 2} \log \log x$ is the correct asymptotic function. Since the number of Mersenne primes is a slowly varying function of x, a stronger assumption will be made, which implies the above and can be tested by studying the distribution of prime factors of Mersenne composites.

It has been proved by Fermat and Euler that all factors of M_p must be of the form $2kp + 1$ and simultaneously of the form $8l \pm 1$. This means that, depending on p, k is constrained to one of the sequences

$$1, 4, 5, 8, 9, 12, \cdots \quad \text{and} \quad 3, 4, 7, 8, 11, 12, \cdots .$$

Thus the smallest potential factor is either $2p + 1$ or $6p + 1$ and thereafter potential factors are spaced an average of $4p$ apart. In the conjecture that follows, we suggest that statistically, this theorem sets a lower bound on potential divisors, but does not change the expected probability density of divisors above that lower bound—the low density of potential divisors is just compensated for by a high conditional probability that any one of these actually divides M_p.

The prime number theorem implies that a randomly chosen integer in the range s to $s + \Delta s$ is prime with probability $\sim \frac{1}{\log s}$, as $s, \Delta s \to \infty$ but $\frac{\Delta s}{s} \to 0$, and that the probability that such a number is prime and also divides some large random number $N \gg s$ is $\frac{1}{s \log s}$.

As A, $B - A$, $N \to \infty$, the expected number of prime divisors of N in the range $A \leqq$ prime divisor $\leqq B \leqq \sqrt{N}$ is

$$\sim \int_A^B \frac{ds}{s \log s} = \log (\log B/\log A).$$

CONJECTURE. *If $A < B \leqq \sqrt{M_p}$, as B/A and $M_p \to \infty$, the number of prime divisors of M_p in the interval $[A, B]$ is Poisson distributed with*

$$\textit{mean} \sim \textit{log } (\textit{log } B/\textit{log } A) \textit{ if } A \geqq 2p$$

$$\textit{or} \sim \textit{log } (\textit{log } B/\textit{log } 2p) \textit{ if } A < 2p.$$

If true, this conjecture implies that

(1) The number of Mersenne primes less than x is $\sim \frac{2}{\log 2} \log \log x$.

(2) The expected number of Mersenne primes in the interval $[x, 2x]$ in p is $2 + 2 \log \left(\frac{\log 2x}{\log x}\right)$ which is ~ 2.

(3) The probability that M_p is prime is $\sim \frac{2 \log 2p}{p \log 2}$.

The observed frequency of Mersenne primes in the interval $[x, 2x]$ in p is shown in

TABLE 1

x	5	10	20	40	80	160	320	640	1280	2560	5120
Number of primes in $[x, 2x]$	2	3	1	1	3	0	2	1	2	3	2

The total number of prime factors less than 2^{36} of Mersenne numbers in the interval $5000 < p < 7000$ was estimated as

$$[\pi(7000) - \pi(5000)] \log \left(\frac{\log 2^{36}}{\log 12{,}000}\right)$$

and was also counted using the factor table prepared. Similar calculations were done for other intervals of length 2000 in p and the results are shown in

TABLE 2

Range of p	5000 to 7000	7000 to 9000	9000 to 11000	11000 to 13000	13000 to 15000	15000 to 17000
Prime Factors $<2^{36}$ observed	223	209	206	192	175	169
Predicted number	226	205	206	192	184	181

Digital Computer Laboratory
University of Illinois
Urbana, Illinois

1. I. J. GOOD, "Conjectures concerning Mersenne numbers," *MTAC* v. 9, 1955, p. 120, 121.
2. A. HURWITZ, "New Mersenne primes," *Math. Comp.* v. 16, 1962, p. 249–251.
3. S. KRAVITZ, "Divisors of Mersenne numbers $10{,}000 < p < 15{,}000$," *Math. Comp.* v. 15, 1961, p. 292–293.
4. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.* v. 31, 1930, p. 419–448.
5. H. RIESEL, "Mersenne numbers," *MTAC* v. 12, 1958, p. 207–213.
6. H. RIESEL, "All factors $q < 10^8$ in all Mersenne numbers $2^p - 1$, p prime $< 10^4$," *Math. Comp.* v. 16, 1962, p. 478–482.
7. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, Spartan Books, Washington, 1962, p. 198.

TABLE 3. *Lucas Residues R for* $7000 < p < 12{,}000$

p	R	p	R	p	R
7069	07313	8887	23230	10501	77772
7109	76754	8893	47223	10531	35724
7121	11254	8923	41014	10597	42547
7127	70746	8941	01034	10639	70051
7177	64624	8999	36025	10667	55573
7213	35572	9011	74242	10709	21742
7229	21270	9013	56660	10711	33125
7237	44431	9041	56532	10723	26405
7243	75126	9091	53605	10729	55703
7247	21344	9133	17234	10771	50555
7309	16030	9151	36255	10781	00164
7321	03466	9187	75427	10789	27651
7331	55736	9203	23113	10831	42672
7333	40632	9209	75536	10909	63265
7351	43525	9227	07577	10937	47503
7369	60027	9241	25121	10939	63332
7433	13456	9257	62553	10957	64103
7477	34613	9277	02036	11003	37656
7481	56621	9281	62622	11027	10024
7489	31253	9319	62503	11057	60335
7507	62414	9377	66277	11069	64651
7523	54030	9413	17541	11093	03231
7559	01556	9433	25035	11113	24506
7577	74000	9437	43446	11117	57045
7603	42610	9463	63616	11131	50752
7607	04024	9473	02247	11159	12377
7621	43263	9533	43134	11161	50166
7649	17277	9551	33274	11177	45677
7699	15637	9587	05303	11213	—
7703	11617	9623	26262	11239	44172
7723	56523	9631	02445	11251	02106
7727	65716	9649	10710	11257	17745
7753	00553	9661	27003	11261	21260
7757	35327	9679	75063	11279	40455
7793	01165	9689	—	11351	22147
7817	00650	9697	24211	11369	27670
7867	12212	9719	32015	11383	17361
7927	35532	9721	13527	11393	01511
7937	36343	9749	37416	11411	74045
7949	55402	9767	03263	11423	03630
8009	55062	9769	51126	11443	65257
8069	61334	9781	34012	11447	51354
8089	24237	9787	21740	11467	55443
8117	07547	9839	12364	11483	03450
8147	32143	9857	23533	11489	57555
8191	03624	9871	32316	11549	76107
8233	75260	9887	33416	11551	47006
8263	73755	9901	15526	11593	12504
8291	31062	9907	01401	11597	07213
8297	63521	9929	44612	11657	53703
8311	72342	9931	25643	11681	13417
8329	64615	9941	—	11689	23607
8363	55516	9967	56346	11717	06015
8369	76051	10037	34070	11743	76351
8389	21672	10061	30610	11779	14053
8443	14744	10069	23577	11789	71203
8447	05235	10079	70743	11801	41730
8521	47055	10099	11311	11807	64000
8527	06705	10159	47661	11821	64453
8543	63267	10169	37134	11839	25215
8581	17603	10177	75465	11867	70645
8609	52627	10259	72321	11887	10035
8647	12277	10273	50763	11897	42220
8681	35061	10303	21613	11927	14155
8707	37065	10313	45100	11933	25571
8753	32153	10343	40266	11941	23743
8819	24665	10369	21740	11987	33200
8831	51436	10399	12436	12043	05651
8837	25460	10453	62061	12071	40741
8861	22326	10463	52513	12097	51143
8863	03214	10477	67452	12109	20110
		10487	05675	12143	27361

TABLE 4

Prime Factors $q < 2^{36}$ *and* $> 2^{34}$ *of* M_p *for* $5000 < p < 17{,}000$

p	q	p	q
5297	45566266567	10631	31946920433
5387	35028913631	10657	39041962129
5591	52462455217	10883	22123941871
5641	49748069257	11087	21232248047
5987	60583758167	11197	33954656167
6089	52969672361	11353	21935540009
6427	52235468209	11399	21834921289
6563	34128597577	11471	48126649327
6607	26285724863	11617	56778668351
6661	33930121529	11731	33949138609
6673	19551502967	11827	41696632543
6779	35331931073	11831	24583043351
6907	60312932423	11863	17998472423
6997	67983747617	11923	54654960463
7001	39107810033	11953	26739410839
7013	54547899457	11971	45647912969
7307	42715085233	12373	23482147543
7517	27743142241	12379	44996897503
7669	40807239817	12437	35512186943
7691	23104702303	12511	30515054639
7717	57756173327	12577	25131864481
7829	39555975527	12619	54388520951
7933	46405939823	12641	18198590369 ·
8081	36263568311 ·		41249479151
	56994371767	12653	34300536887
8093	29811811823	12659	47013095473
8111	25919771153	12809	39970407647
8573	21973130527	13001	18880338223
8641	46880604889	13381	49300715543
8747	21021997487	13451	25744353137
8779	57336421553	13901	39030421543
8783	46912673033	14011	52635964361
8971	59568301217	14029	19858217849
9043	37268518009	14389	52946109737
9067	21497004703	14533	45439197527
9619	53840698033	14593	63369110177
9629	27152451199	14669	22222684199
9803	63388001753	14717	25671863857
9817	26619050743	14827	56787558271
9883	21258273703	15233	67894547311
10039	45613381103	15439	18568948471
10067	34439287537	15461	58311965473
10151	62820641017	15473	67117263047
10267	35491478951	15913	18951969263 ·
10427	35037410167		29723415311
10457	31794194791	16567	68395501007
10529	37429900087	16889	49565127863