The Number of Prime Divisors of Certain Mersenne Numbers*

By John R. Ehrman

It has been conjectured by Gillies [1] that if $M_p = 2^p - 1$ is the Mersenne number for some prime p, and if $A < B \leqq \sqrt{M_p}$ as B/A and $M_p \to \infty$, then the number of prime divisors of M_p in the interval $[A, B]$ is Poisson distributed, with mean

$$
\begin{aligned}
(1) \qquad & m \sim \log(\log B/\log A) \quad \text{if} \quad A \geqq 2p\,, \text{or} \\
& m \sim \log(\log B/\log 2p) \quad \text{if} \quad A < 2p\,.
\end{aligned}
$$

It is the purpose of this paper to describe two tests of a modified form of this conjecture.

It is known that all divisors of M_p must be of the form $2kp + 1$ and simultaneously of the form $8k' \pm 1$, where k and k' are arbitrary integers. Also, the prime divisors of M_p may be of one of the forms $4n + 1$ or $4n + 3$. Thus if $p = 4n + 1$, the smallest possible divisor q is $6p + 1$, and if $p = 4n + 3$, the smallest possible divisor is $q = 2p + 1$. Thus Eq. (1) is modified slightly: the expected number of prime divisors of M_p in the interval $[Q, B]$, where Q is not less than the smallest possible divisor of M_p, $Q < B \leqq \sqrt{M_p}$, and as B/Q, $M_p \to \infty$, is Poisson distributed with mean

$$
(2) \qquad m_Q \sim \log(\log B/\log Q)\,.
$$

Since the observed results in a group are drawn from two populations corresponding to the two forms of p, there is a question as to what value m should be used for the estimated mean number of divisors. It would be possible, for example, to separate the two populations and test the samples independently. It was felt, however, that a fuller test of the applicability of the conjecture (2) could be made by testing all primes with no distinction as to form.

In calculating an estimate of the mean m to be used in statistical tests, it was noted that

(a) the sum of two independent random variables from Poisson distributions with parameters m_1 and m_2 has a Poisson distribution with parameter $(m_1 + m_2)$;

(b) if $\pi(x; k, t)$ is the number of primes $p \equiv t \pmod{k}$ which do not exceed x, and if $(k, t) = 1$, then [2]

$$
\pi(x; k, t) \sim \pi(x)/\phi(k)\,.
$$

This means that one may expect nearly equal numbers of primes of the forms $4n + 1$ and $4n + 3$ in a large sample of primes; this is the justification for not distinguishing the primes as to form.

Thus an unbiased asymptotic estimate of the mean may be taken to be

Received November 9, 1966. Revised February 13, 1967.
* Work supported by U. S. Atomic Energy Commission.

$$m = \tfrac{1}{2}\,(m_{2p+1} + m_{6p+1})\,. \tag{3}$$

Thus, for example, in the interval $100000 < p < 102500$, it is found that $m_{2p+1} = 0.5645$ and $m_{6p+1} = 0.4784$, so that the Mersenne number corresponding to a prime drawn at random in the interval would be expected to have an average of 0.52 divisors less than 2^{31}.

The tests performed on the results given in [3] were a test of the mean number of divisors, and a test of their Poisson distribution. Because the change in p over each of the intervals tested is relatively small, the value of p used in computing m from Eq. (3) was simply the midpoint of the interval in p from which the sample was drawn.

A program was written for an IBM System/360 (Model 50) computer which tested for divisors of M_p using the congruence

$$2^p \equiv 1 \pmod q\,.$$

The test was coded [4] in the following manner:

1. In binary form, $p = \sum_{i=0}^{n} a_i 2^i$, and $2^p = \prod_{i=0}^{n} (2^{2^i})^{a_i}$.
2. Let $R_i \equiv 2^{2^i} \pmod q \equiv R_{i-1}^2 \pmod q$, and $S_j = \prod_{i=0}^{j} (R_i)^{a_i} \pmod q$.
Thus S_j need be computed from S_{j-1} only if $a_j = 1$.
3. If $S_n = 1$, $q | M_p$.
4. The first five steps of the calculation may be done in one step by taking the five low-order bits of p to compute $R_4 = 2^{p \,(\mathrm{mod}\ 32)}$.

Divisors $q < 2^{31}$ were computed for $100000 < p < 300000$. To compare the observed distribution of primes with that predicted by Eqs. (2) and (3), the values of p were grouped so that p fell into one of the 80 groups defined by

$$100000 + 2500i < p < 102500 + 2500i\,,$$

$i = 0(1)79$. In each group, the total number of primes observed and the number of primes with j divisors were counted. These results are tabulated in Table I. For each p which has one or more divisors $q < 2^{31}$, the value of p and the associated values of $k = (q - 1)/2p$ are tabulated in [3].

To test the estimate of m, N samples of p were observed between limits L and U, where $N = \pi(U) - \pi(L)$, and $L < p < U$. The total number of divisors T was counted, and the sample mean $\bar{x} = T/N$ was computed. The sample variance was found from

$$s^2 = \frac{1}{N} \sum_{j=1}^{N} D_j^2 - (\bar{x})^2 = \frac{1}{N} \sum_{n=1}^{5} n^2 K_n - (\bar{x})^2\,,$$

where D_j is the number of divisors observed for the jth prime in the sample, and K_n is the number of Mersenne numbers in the interval with n divisors. (Because of the method used, no tests were made for multiple factors.) As the number of observations becomes large, it is expected that the variable

$$t = (N - 1)^{1/2} (\bar{x} - m)/s$$

should become normally distributed (0, 1). The observed values of N, D, and t for each group are given in Table I. The expected number of divisors E is simply the product of m and N.

TABLE I

Interval in P	N	N_1	K_0	K_1	K_2	K_3	K_4	K_5	T	E	χ^2	t
100000–102500	222	117	138	64	17	3	0	0	107	115	0.720	−0.844
102500–105000	210	93	112	72	21	4	1	0	130	109	3.776	1.846
105000–107500	210	106	139	50	19	2	0	0	94	108	4.951	−1.454
107500–110000	219	106	133	66	11	5	4	0	119	112	0.102	0.484
110000–112500	209	106	129	60	17	3	0	0	103	107	0.414	−0.435
112500–115000	209	106	122	68	16	3	0	0	109	107	0.334	0.189
115000–117500	215	103	132	61	18	4	0	0	109	109	0.612	−0.075
117500–120000	215	105	136	61	16	2	0	0	99	109	0.900	−1.056
120000–122500	221	104	132	70	17	1	1	0	111	112	0.201	−0.110
122500–125000	212	109	131	61	13	7	0	0	108	107	0.299	0.069
125000–127500	206	96	126	63	13	2	1	1	104	103	0.203	0.010
127500–130000	219	121	129	69	19	2	0	0	113	110	0.233	0.282
130000–132500	208	96	128	66	12	2	0	0	96	104	1.405	−0.881
132500–135000	209	108	116	70	21	1	1	0	119	104	2.526	1.374
135000–137500	226	117	129	74	20	2	1	0	124	112	1.319	1.034
137500–140000	208	102	127	67	11	3	0	0	98	103	1.398	−0.561
140000–142500	212	110	117	74	18	3	0	0	119	105	2.946	1.347
142500–145000	200	101	108	74	15	2	1	0	114	98	4.719	1.487
145000–147500	212	111	132	70	8	2	0	0	92	104	4.674	−1.396
147500–150000	214	106	133	58	20	3	0	0	107	105	1.616	0.167
150000–152500	217	108	124	77	14	2	0	0	111	106	3.199	0.470
152500–155000	207	105	130	66	11	0	0	0	88	101	3.043	−1.554
155000–157500	210	104	125	69	13	3	0	0	104	102	0.971	0.154
157500–160000	201	98	124	59	17	1	0	0	96	97	0.049	−0.194
160000–162500	202	98	127	56	17	2	0	0	96	98	0.531	−0.213
162500–165000	208	106	134	57	14	2	1	0	95	100	0.718	−0.565
165000–167500	209	106	125	61	21	2	0	0	109	101	1.662	0.774
167500–170000	195	95	115	60	19	1	0	0	101	94	1.029	0.723
170000–172500	212	106	120	74	17	1	0	0	111	101	2.836	0.933
172500–175000	207	109	127	63	13	4	0	0	101	99	0.057	0.163
175000–177500	208	107	141	50	15	2	0	0	86	99	3.378	−1.412
177500–180000	218	115	127	76	13	2	0	0	108	104	3.076	0.397
180000–182500	195	94	130	50	11	3	1	0	85	92	1.787	−0.796
182500–185000	208	104	113	72	19	3	1	0	123	98	5.753	2.205
185000–187500	219	108	138	67	13	0	1	0	97	103	1.035	−0.725
187500–190000	206	99	119	70	15	2	0	0	106	97	2.072	0.867
190000–192500	199	99	125	54	19	0	1	0	96	94	1.199	0.192
192500–195000	204	98	137	48	16	3	0	0	89	96	3.483	−0.722
195000–197500	205	100	128	63	12	2	0	0	93	96	0.562	−0.377

197500–200000	206	112	123	61	20	2	0	0	107	96	1.921	1.000
200000–202500	201	102	121	64	14	2	0	0	98	94	0.612	0.392
202500–205000	196	101	127	57	11	0	1	0	83	91	1.071	−0.963
205000–207500	210	100	131	67	8	2	2	0	97	98	1.911	−0.108
207500–210000	216	112	141	60	13	2	0	0	92	100	0.692	−0.912
210000–212500	203	97	120	69	12	2	0	0	99	94	2.321	0.485
212500–215000	203	96	129	59	12	3	0	0	92	94	0.101	−0.238
215000–217500	195	98	121	63	11	0	0	0	85	90	1.980	−0.645
217500–220000	210	103	136	54	18	2	0	0	96	97	1.640	−0.118
220000–222500	200	105	133	48	16	3	0	0	89	92	2.836	−0.339
222500–225000	202	99	131	55	16	0	0	0	87	93	0.341	−0.679
225000–227500	202	100	125	59	16	2	0	0	97	92	0.345	0.413
227500–230000	215	115	142	58	13	2	0	0	90	98	0.788	−0.923
230000–232500	200	92	111	69	16	4	0	0	113	91	5.221	2.068
232500–235000	196	95	120	60	16	0	0	0	92	89	0.350	0.250
235000–237500	186	92	119	58	6	3	0	0	79	85	2.369	−0.691
237500–240000	202	96	134	51	13	3	1	0	90	92	1.346	−0.211
240000–242500	209	103	132	62	11	4	0	0	96	95	0.121	0.079
242500–245000	203	104	121	64	14	4	0	0	104	92	1.345	1.149
245000–247500	198	100	123	64	8	2	1	0	90	89	2.041	0.010
247500–250000	213	109	120	67	25	1	0	0	120	96	8.077	2.246
250000–252500	199	99	127	58	13	1	0	0	87	90	0.099	−0.340
252500–255000	195	99	114	60	18	3	0	0	105	88	3.679	1.664
255000–257500	200	105	113	67	17	2	1	0	111	90	4.755	1.999
257500–260000	199	93	126	54	15	3	1	0	97	89	1.221	0.701
260000–262500	190	94	114	59	15	1	1	0	96	85	1.299	1.077
262500–265000	203	98	128	57	17	1	0	0	94	91	0.535	0.298
265000–267500	207	106	126	64	17	0	0	0	98	92	0.810	0.560
267500–270000	205	109	120	71	14	0	0	0	99	91	3.641	0.810
270000–272500	207	103	127	62	15	2	1	0	102	92	0.779	0.919
272500–275000	189	96	100	67	21	1	0	0	112	84	11.253	2.849
275000–277500	202	94	130	59	10	2	1	0	89	90	0.298	−0.106
277500–280000	192	90	113	65	9	4	1	0	99	85	2.740	1.339
280000–282500	212	102	124	75	11	2	0	0	103	94	5.023	0.941
282500–285000	199	103	122	56	19	2	0	0	100	88	3.008	1.168
285000–287500	187	99	124	50	10	2	1	0	80	82	0.361	−0.301
287500–290000	194	107	136	45	12	1	0	0	72	85	3.007	−1.591
290000–292500	200	100	117	64	16	3	0	0	105	88	3.264	1.660
292500–295000	192	99	121	57	13	1	0	0	86	84	0.166	0.144
295000–297500	191	95	113	63	13	1	1	0	96	84	2.332	1.233
297500–300000	190	93	119	56	11	4	0	0	90	83	0.285	0.661

Average $\chi^2 = 1.947$ Average $t = 0.247$

To test the hypothesis of Poisson distribution, a chi-squared test was performed on the observed distribution of divisors. The counts were put in three classes: no divisors, one divisor, and two or more divisors; the numbers of primes with i divisors are listed in the columns K_i for $i = 0(1)5$. (See also reference [5].) The computed values of chi-squared for each of the eighty groups are given in Table I. The values of chi-squared were computed from the formula

$$\chi^2 = (Ne^{-m} - K_0)^2 + (Nme^{-m} - K_1)^2 + (N(1 - e^{-m} - me^{-m}) - K_2 - K_3 - K_4 - K_5)^2,$$

and are given in Table I in the column headed χ^2.

To test for the possibility that distinguishing between primes of the form $4n + 1$ and $4n + 3$ might lead to significantly different results, t and χ^2 were also computed for $m = (1/N)[N_1 m_{6p+1} + (N - N_1)m_{2p+1}]$, where N_1 is the number of primes $p \equiv 1 \pmod 4$ observed in the interval. The average values of t and χ^2 obtained were slightly larger than those given at the end of Table I.

A comparison of the expected and observed distributions of t and χ^2 is given in Table II. The agreement is seen to be satisfactory.

TABLE II

Observed distribution of t and chi-squared.
In both cases, the expected number of values in the ranges indicated is 10.

Upper Limit on t	*Number of Values*	*Upper Limit on Chi-Squared*	*Number of Values*
−1.15	5	0.266	10
− .674	11	0.576	12
− .319	7	0.940	9
0.0	10	1.386	10
+ .319	13	1.962	8
+ .674	8	2.772	8
+1.15	12	4.158	14
∞	14	∞	9

I wish to thank J. C. Butcher for several stimulating and helpful discussions, and the referee for several suggestions.

Stanford Linear Accelerator Center
Stanford University
Stanford, California

1. D. B. Gillies, "Three new Mersenne primes and a statistical theory," *Math. Comp.*, v. 18, 1964, p. 94; Also, Digital Computer Laboratory Report No. 138, Univ. of Illinois, Urbana, Ill. MR **28** #2990.

2. W. J. LeVeque, *Topics in Number Theory*, Vol. 2, Addison-Wesley, Reading, Mass., 1956, p. 252. MR **18**, 283.

3. J. R. Ehrman, "Prime divisors of Mersenne numbers," TN–66–40, Stanford Linear Accelerator Center, Stanford, Calif.

4. Sidney Kravitz, "Divisors of Mersenne numbers 10,000 $< p <$ 15,000," *Math. Comp.*, v. 15, 1961, p. 292. MR **23** #A833.

5. Review No. 113, *Math. Comp.*, v. 19, 1965, p. 686.