TECHNICAL NOTES AND SHORT NOTICES

On the Distribution of Mersenne Divisors

By Daniel Shanks and Sidney Kravitz

The Mersenne numbers are those of the form $M_p = 2^p - 1$ with p prime. The only possible divisors of M_p are those of the form $2kp + 1$. Let $f_k(x)$ be the number of M_p with $p \leqq x$ that have a prime divisor $d = 2kp + 1$. As is known, it has not been proven, even for a single k, that

$$f_k(x) \to \infty \tag{1}$$

as $x \to \infty$. It is also known that

$$f_k(x) = 0 \qquad (k = 2, 6, 10, \cdots) \tag{2}$$

for all k of the form $4m + 2$, but, with these values of k excluded, one expects, heuristically, that (1) is true for all other $k = 1, 3, 4, 5, 7, 8, \cdots$. We conjecture, in fact, a stronger result that includes both (1) for these allowed k, and (2) for those excluded:

$$f_k(x) = \bar{Z}(x) \frac{\cos^2(k\pi/4)}{k} \prod_{q \mid k} \left(\frac{q-1}{q-2}\right) \left[1 - \frac{\log(2k)}{\log x} + O\left(\frac{1}{\log^2 x}\right)\right]. \tag{3}$$

In (3) the product is taken over all odd primes q, if any, that divide k, and $\bar{Z}(x)$ is the well-known conjectured estimate for the number of twin-prime pairs $\leqq x$:

$$\bar{Z}(x) = 2 \prod_{p=3}^{\infty} \left(1 - \frac{1}{(p-1)^2}\right) \int_2^x dy/\log^2 y. \tag{4}$$

In a recent note [1], one of us presented a table of $f_k(10^5)$ for $k \leqq 200$. In Table 1 we present a table of $f_k(x)$ for

$$k \neq 4m + 2 \leqq 60, \qquad x = 10^5(10^5)10^6.$$

The larger range of x here, and the sufficient range of k, enables us to make a significant test of (3). We find it convenient, however, to replace the $\bar{Z}(x)$ in (3) by the *actual number* of twins, $Z(x)$, since these are simple integers which are in sufficiently good agreement with $\bar{Z}(x)$. Further, while such a change in (3) makes the infinitude of $f_k(x)$ depend upon that of $Z(x)$, we do not regard this as a defect. On the contrary, it is highly likely that any proof of

$$Z(x) \to \infty$$

could be readily adapted to prove

$$f_k(x) \to \infty \qquad (k \neq 4m + 2)$$

also, and we prefer to emphasize this relationship.

Received August 25, 1966.

TABLE 1
$f_k(x)$

k	$x \cdot 10^{-5} \rightarrow$									
	1	2	3	4	5	6	7	8	9	10
1	581	1042	1441	1816	2190	2528	2883	3246	3574	3912
3	350	624	854	1101	1310	1546	1761	1980	2219	2390
4	266	433	626	792	962	1145	1306	1456	1623	1764
5	141	247	348	445	541	633	725	808	875	939
7	84	137	188	248	293	339	387	436	475	529
8	122	205	287	375	446	516	588	654	720	777
9	115	196	271	344	422	485	549	616	686	743
11	61	92	121	163	184	217	240	276	308	338
12	162	284	377	479	566	686	787	875	970	1082
13	47	75	106	133	163	185	211	234	254	280
15	88	140	209	268	328	377	430	479	536	606
16	56	91	137	175	221	266	305	347	383	426
17	23	52	72	92	109	127	141	161	179	196
19	26	45	57	81	93	120	140	154	172	185
20	56	104	138	184	225	264	307	351	385	427
21	47	89	119	147	181	214	246	268	304	341
23	18	28	39	59	77	92	108	126	137	154
24	68	132	195	234	278	324	361	406	452	497
25	34	52	73	102	110	125	136	158	173	190
27	27	46	69	95	115	138	159	189	207	232
28	37	59	90	117	139	172	203	225	244	262
29	11	23	37	49	62	71	81	93	103	113
31	16	29	42	55	63	66	72	78	84	91
32	24	44	61	79	95	113	129	147	163	176
33	32	48	69	92	110	128	145	163	178	200
35	13	33	51	62	77	89	107	120	135	144
36	41	77	107	145	177	206	243	274	303	333
37	17	31	35	43	50	61	70	76	84	91
39	29	49	73	91	107	121	133	147	158	167
40	25	58	81	96	119	141	154	167	182	198
41	11	13	20	24	29	35	43	52	57	67
43	10	20	29	31	40	43	47	56	60	65
44	19	35	46	59	70	84	96	113	122	133
45	24	43	69	88	108	122	142	159	175	188
47	11	15	18	26	31	32	37	41	47	55
48	39	65	85	111	132	152	176	212	223	256
49	6	15	23	35	37	43	50	57	62	67
51	16	25	34	45	55	69	83	93	102	115
52	15	24	32	45	54	59	70	81	92	99
53	8	14	19	26	33	40	43	51	58	60
55	14	25	34	38	43	46	54	58	69	77
56	30	44	58	65	78	91	103	114	126	137
57	15	27	44	55	67	79	89	98	107	117
59	7	9	16	20	23	31	39	43	49	57
60	47	74	98	132	165	186	214	242	262	279

In Table 2 we list the ratios:

$$r_k(x) = \frac{Z(x)}{f_k(x)} \frac{\cos^2(k\pi/4)}{k} \prod_{q \mid k} \left(\frac{q-1}{q-2}\right) \left[1 - \frac{\log(2k)}{\log x}\right]. \tag{5}$$

The counts $Z(x)$ were taken from [2], and are repeated here in Table 3 for convenience.

Table 2 suggests that our conjectures (3) are true for all k. The deviations from unity seen there are not excessive considering the limited value of x, and the rather small totals found in certain cases, e.g., $f_{59}(10^6) = 57$. The deviations seen, in fact, no doubt are due mostly to fluctuation terms of approximate order $O(\sqrt{x})$, since

TABLE 2
$r_k(x)$

k	$x \cdot 10^{-5} \rightarrow$									
	1	2	3	4	5	6	7	8	9	10
1	0.990	0.978	0.982	0.991	0.987	0.999	0.997	0.989	0.992	0.992
3	0.984	0.984	1.003	0.992	1.003	0.995	0.995	0.989	0.976	0.992
4	0.943	1.035	0.999	1.007	0.998	0.982	0.981	0.984	0.976	0.983
5	0.926	0.946	0.938	0.936	0.928	0.929	0.924	0.927	0.947	0.967
7	0.963	1.059	1.079	1.046	1.067	1.080	1.079	1.072	1.089	1.071
8	0.952	1.018	1.017	0.995	1.009	1.022	1.023	1.029	1.035	1.050
9	0.886	0.935	0.946	0.953	0.937	0.956	0.963	0.961	0.955	0.966
11	0.741	0.885	0.943	0.896	0.958	0.952	0.983	0.957	0.949	0.948
12	0.912	0.938	0.990	0.997	1.019	0.986	0.980	0.987	0.986	0.969
13	0.783	0.886	0.879	0.897	0.883	0.913	0.913	0.922	0.941	0.935
15	0.871	0.989	0.930	0.929	0.916	0.936	0.936	0.941	0.932	0.903
16	0.955	1.062	0.991	0.994	0.950	0.926	0.922	0.908	0.911	0.898
17	1.158	0.927	0.940	0.943	0.961	0.968	0.995	0.976	0.973	0.974
19	0.897	0.939	1.041	0.940	0.989	0.899	0.880	0.897	0.889	0.906
20	0.990	0.966	1.023	0.984	0.972	0.973	0.955	0.936	0.946	0.935
21	1.005	0.962	1.012	1.050	1.031	1.024	1.017	1.046	1.022	0.999
23	1.034	1.206	1.218	1.033	0.956	0.940	0.915	0.878	0.895	0.873
24	0.996	0.931	0.887	0.948	0.965	0.972	0.997	0.993	0.989	0.986
25	0.634	0.753	0.754	0.693	0.777	0.803	0.843	0.813	0.823	0.822
27	1.097	1.171	1.099	1.024	1.023	1.002	0.993	0.937	0.948	0.928
28	0.922	1.052	0.971	0.959	0.976	0.926	0.897	0.907	0.927	0.947
29	1.288	1.121	0.981	0.951	0.909	0.933	0.934	0.912	0.913	0.913
31	0.819	0.823	0.800	0.785	0.829	0.930	0.974	1.008	1.037	1.050
32	1.018	1.011	1.028	1.020	1.026	1.013	1.015	0.998	0.998	1.014
33	0.819	0.995	0.976	0.940	0.951	0.961	0.969	0.967	0.981	0.958
35	1.358	0.975	0.890	0.940	0.916	0.932	0.886	0.886	0.873	0.898
36	1.042	1.012	1.027	0.974	0.966	0.976	0.945	0.940	0.943	0.941
37	0.627	0.627	0.783	0.819	0.853	0.822	0.819	0.846	0.848	0.859
39	0.734	0.793	0.751	0.774	0.797	0.829	0.862	0.875	0.902	0.937
40	1.011	0.796	0.804	0.872	0.852	0.845	0.885	0.915	0.931	0.939
41	0.859	1.328	1.218	1.305	1.308	1.274	1.186	1.100	1.113	1.039
43	0.894	0.817	0.795	0.957	0.898	0.982	1.028	0.968	1.001	1.014
44	0.994	0.987	1.060	1.063	1.085	1.063	1.064	1.014	1.042	1.048
45	0.921	0.940	0.827	0.834	0.823	0.857	0.842	0.843	0.850	0.868
47	0.733	0.983	1.157	1.031	1.047	1.193	1.180	1.195	1.156	1.084
48	0.789	0.867	0.936	0.923	0.940	0.960	0.948	0.883	0.931	0.890
49	1.503	1.101	1.014	0.858	0.983	0.995	0.979	0.963	0.982	0.998
51	0.957	1.122	1.166	1.134	1.124	1.054	1.002	1.004	1.015	0.988
52	1.021	1.170	1.240	1.135	1.146	1.234	1.190	1.154	1.127	1.149
53	0.876	0.917	0.955	0.899	0.858	0.833	0.886	0.838	0.818	0.868
55	0.697	0.716	0.744	0.857	0.918	1.009	0.984	1.028	0.958	0.943
56	0.516	0.645	0.692	0.795	0.803	0.810	0.819	0.830	0.833	0.841
57	0.892	0.909	0.789	0.813	0.809	0.807	0.820	0.836	0.849	0.852
59	0.883	1.261	1.003	1.034	1.089	0.951	0.865	0.881	0.857	0.809
60	0.676	0.788	0.842	0.805	0.781	0.815	0.811	0.805	0.825	0.850

these temporarily dominate (at these values of x) the conjectured actual second term involving $\log (2k)/\log x$.

The heuristic argument for (3) is quite convincing, especially in view of previous successes for similar arguments. A Hardy-Littlewood conjecture is

$$Z(x) \sim \bar{Z}(x), \tag{6}$$

and, similarly, cf. [3], the number of integers $n \leqq x$ such that n and $2kn + 1$ are both prime should be asymptotic to

$$2 \prod_{q \mid k} \left(\frac{q-1}{q-2}\right) \prod_{p=3}^{\infty} \left(1 - \frac{1}{(p-1)^2}\right) \int_2^x dy/\log y \log 2ky. \tag{7}$$

TABLE 3
$Z(x)$

$x \cdot 10^{-5}$	$Z(x)$	$x \cdot 10^{-5}$	$Z(x)$
1	1224	6	5331
2	2160	7	6061
3	2994	8	6766
4	3804	9	7472
5	4565	10	8169

Now the factor

$$\cos^2 (k\pi/4) = \tfrac{1}{2}, 0, \tfrac{1}{2}, \text{ or } 1 \tag{8}$$

for $k \equiv 1, 2, 3$, or $4 \pmod 4$, respectively, and therefore represents the fraction of the primes $2kn + 1$ which have 2 as a quadratic residue:

$$\left(\frac{2}{2kn + 1}\right) = 1. \tag{9}$$

Finally, for such a possible prime divisor $2kn + 1$, we assume that $1/k$ is the probability that 2 is a $(2k)$ic residue of $2kn + 1$, for if g is a primitive root of $2kn + 1$, by (9) we have

$$g^{2s} \equiv 2 \pmod{2kn + 1}$$

for some s, and, we assume, that the probability of $2k \mid 2s$ is $1/k$. For these primes, n and $2kn + 1$, we therefore have $2kn + 1 \mid 2^n - 1$.

Combination of (7), (8), and (4) now yields (3).

Now we wish to suggest two extensions of this work to others, since we think these to be of some importance, but are not satisfied with any efforts that we ourselves have made.

(A) We note, first, that only the case $k = 1$ in (3) is a special case of the Bateman-Horn conjecture [3]. What *generalization* is needed to include other values of k? Consider first $k = 3$. As is known, any $p = 6n + 1$ can be written

$$p = 6n + 1 = a^2 + 3b^2,$$

but only those p where $3 \mid b$ have 2 as a cubic residue. By Landau's generalization of the prime number theorem to *prime ideals*, it follows that $3 \mid b$ occurs $\frac{1}{3}$ of the time, asymptotically speaking. This verifies one case of our "assumption" above, namely, that the probability for $k = 3$ is $\frac{1}{3}$.

It is clear, then, that we wish a generalization of the Bateman-Horn conjecture [3], and also its extension by Schinzel [4], to include not only primes but also prime ideals. But we have not satisfied ourselves that we have obtained this with full generality and proper exactitude.

(B) For no k has (3) been proven. Each such conjecture is essentially equivalent to the twin-prime conjecture (6), and, no doubt, will be proven when, and only when, (6) is proven. As is known, a *much weaker* conjecture has never been proven, namely, that there are infinitely many *Mersenne composites*. If (3) were true for even a single k, then there would certainly be infinitely many composites.

It seems to us that this weaker conjecture is provable, but we have not proved it. While (6) has not been proven, one can also examine the sequences

$$p, p + 2k$$

collectively, for all k. This has been done by Lavrik [5], and results have been obtained there concerning "almost all" k. If the generalization suggested in (A) is carried out successfully, it seems to us that Lavrik's techniques applied to our (3) should suffice to prove that there are infinitely many Mersenne composites, and probably also stronger results concerning a lower bound on their number. Further, one would then also have an upper bound on the number of Mersenne primes.

David Taylor Model Basin
Washington, D.C. 20007

592 Herrick Drive
Dover, New Jersey 07801

1. S. Kravitz, "Distribution of Mersenne divisors," *Math. Comp.*, v. 20, 1966, pp. 448–449.
2. F. Gruenberger & G. Armerding, *Statistics on the First Six Million Prime Numbers*, copy deposited in UMT file and reviewed in RMT **73**, *Math. Comp.*, v. 19, 1965, pp. 503–505.
3. P. T. Bateman & R. A. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.*, v. 16, 1962, pp. 363–367. MR **26** #6139.
4. A. Schinzel, "A remark on a paper of Bateman and Horn," *Math. Comp.*, v. 17, 1963, pp. 445–447. MR **27** #3609.
5. A. F. Lavrik, "On the twin prime hypothesis of the theory of primes by the method of I. M. Vinogradov," *Dokl. Akad. Nauk SSSR*, v. 132, 1960, pp. 1013–1015 = *Soviet Math. Dokl.*, v. 1, 1960, pp. 700–702. MR **28** #1183.

A Counterexample to Euler's Sum of Powers Conjecture

By L. J. Lander and T. R. Parkin

A search was conducted on the CDC 6600 computer for nontrivial solutions in nonnegative integers of the Diophantine equation

$$x_1^5 + x_2^5 + \cdots + x_n^5 = y^5, \qquad n \leqq 6. \tag{1}$$

In general, to decompose t as the sum of n fifth powers assume s is the largest. Then for each s in the range

$$(t/n)^{1/5} \leqq s \leqq t^{1/5},$$

a decomposition is sought in which $t - s^5$ is the sum of $n - 1$ fifth powers each $\leqq s^5$. Applying the algorithm repeatedly a final decomposition is reached of the form

$$u = v^5 + w^5$$

in which $w \leqq v$ and each v in the range $(u/2)^{1/5} \leqq v \leqq u^{1/5}$ is considered. Since $x^5 \equiv x \pmod{30}$ for each integer x, we require $w \equiv u - v \pmod{30}$. A precalculated

Received June 30, 1966. Revised July 29, 1966.