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 $p \leq x$ that have a prime divisor $d = 2kp + 1$. As is known, it has not been proven, even for a single $k$, that

$$f_k(x) \to \infty$$

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

$$f_k(x) = 0 \quad (k = 2, 6, 10, \ldots)$$

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 $k = 1, 3, 4, 5, 7, 8, \ldots$. We conjecture, in fact, a stronger result that includes both (1) for these allowed $k$, and (2) for those excluded:

$$f_k(x) = \mathcal{Z}(x) \frac{\cos^2(k\pi/4)}{k} \prod_{q|k} \left(1 - \frac{\log(2k)}{\log x} + O\left(\frac{1}{\log^2 x}\right)\right).$$

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

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

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

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

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 $\mathcal{Z}(x)$ in (3) by the actual number of twins, $Z(x)$, since these are simple integers which are in sufficiently good agreement with $\mathcal{Z}(x)$. 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

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

also, and we prefer to emphasize this relationship.

Received August 25, 1966.
The counts \( Z(x) \) were taken from [2], and are repeated here in Table 3 for convenience.

In Table 2 we list the ratios:

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

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., \( f_{60}(10^6) = 57 \). The deviations seen, in fact, no doubt are due mostly to fluctuation terms of approximate order \( O(\sqrt{x}) \), since
both prime should be asymptotic to
and, similarly, cf. [3], the number of integers \( n \leq x \) such that \( n \) and \( 2kn + 1 \) are
previous successes for similar arguments. A Hardy-Littlewood conjecture is
\[
2 \prod_{q \mid k} \left( \frac{q - 1}{q - 2} \right) \prod_{p = 3}^{\infty} \left( 1 - \frac{1}{(p - 1)^2} \right) \int_2^x dy / \log y \log 2ky.
\]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Table 3

<table>
<thead>
<tr>
<th>$x \cdot 10^{-6}$</th>
<th>$Z(x)$</th>
<th>$x \cdot 10^{-6}$</th>
<th>$Z(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1224</td>
<td>6</td>
<td>5331</td>
</tr>
<tr>
<td>2</td>
<td>2160</td>
<td>7</td>
<td>6061</td>
</tr>
<tr>
<td>3</td>
<td>2994</td>
<td>8</td>
<td>6766</td>
</tr>
<tr>
<td>4</td>
<td>3804</td>
<td>9</td>
<td>7472</td>
</tr>
<tr>
<td>5</td>
<td>4565</td>
<td>10</td>
<td>8169</td>
</tr>
</tbody>
</table>

Now the factor

$$\cos^2 \left( \frac{k \pi}{4} \right) = \frac{1}{2}, 0, \frac{1}{2}, \text{ or } 1$$

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

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

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


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

\[
x_1^5 + x_2^5 + \cdots + x_n^5 = y^5, \quad n \leq 6.
\]

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

\[
(t/n)^{1/5} \leq s \leq t^{1/5},
\]

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

\[
u = v^5 + w^5
\]

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

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