The Editor's Corner: The New Mersenne Conjecture

P. T. Bateman, J. L. Selfridge*, and S. S. Wagstaff, Jr.**

It is well known that Mersenne stated in his *Cogitata* [**4**] that, of the fifty-five primes $p \leqslant 257$, $2^p - 1$ is itself prime only for the eleven values

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, \text{ and } 257.$$

It is also well known that his list had five errors: $p = 67$ and 257 should have been removed from the list while $p = 61$, 89, and 107 should have been added to it.

Several authors [**1, 2, 3**] have speculated about how Mersenne formed his list. It is easy to notice that all numbers on his (incorrect) list lie within 3 of some power of 2. However, Mersenne certainly knew that $2^{11} - 1$ is composite and hence that not all primes $p = 2^k \pm 3$ produce prime $M_p = 2^p - 1$. The next prime of this form not on Mersenne's list is $p = 29$. He surely knew that M_{29} is composite, as it has the small divisor 233. Also 263 divides $2^{131} - 1$. Mersenne's list is explained by the rule

$$M_p \text{ is prime if and only if } p \text{ is a prime of one of the forms } 2^k \pm 1 \text{ or } 2^{2k} \pm 3 \quad (1)$$

except for the omission of $p = 61$. In fact Mersenne stated in [**5**, Chap. 21, p. 182] a rule very similar to (1). (The verb "differs"—not "exceeds," as some have guessed—is omitted from his sentence, but Mersenne supplied it in a corrigendum on the back of page 235.) Drake [**2**] quotes this sentence from [**5**], locates the missing verb and argues that (1) was in fact Mersenne's rule. He suggests that 61 was missing from [**4**] either because of a typographical error or because Mersenne mistakenly believed that M_{61} is composite. When copying a list, like "$\ldots, 61, 67, \ldots$", containing two adjacent similar items, it is a common error to omit the first of these (here "61").

Now the question presents itself: Is there a neat way to distinguish the Mersenne hits like 31, 61, 127 from the Mersenne misses like $67, 257, \ldots$ and $89, 107, \ldots$? When $(2^{127} + 1)/3$ was proved prime, we began looking at the other $(2^p + 1)/3$. We noticed that they were prime for the hits and composite for the misses! Is this accidental? Will "a little more computing" find a counterexample?

We replace (1) by this new, related conjecture that when both sides of (1) are true, $(2^p + 1)/3$ is prime, and when (1) is false, $(2^p + 1)/3$ is composite. Restating this conjecture we get the

New Mersenne Conjecture. *If two of the following statements about an odd positive integer p are true, then the third one is also true.*

(a) $p = 2^k \pm 1$ or $p = 4^k \pm 3$.
(b) M_p is prime.
(c) $(2^p + 1)/3$ is prime.

It is not necessary to assume that p is prime, for if p is composite (or 1), then statements (b) and (c) are both false and the conjecture holds.

It is easy to find examples of primes p for which all three statements are true ($p = 3, 5, 7, 13, 17, 19, 31, 61, 127$) or all three are false ($p = 29, 37, 41, 47, \ldots$) or

*Department of Mathematical Sciences, Northern Illinois University, DeKalb, IL 60115
**Department of Computer Sciences, Purdue University, West Lafayette, IN 47907

Table for "The New Mersenne Conjecture"

p	$p = 2^k \pm 1$ or $4^k \pm 3$?	$2^p - 1$ prime?	$(2^p + 1)/3$ prime?
3	yes (−1)	yes	yes
5	yes (+1)	yes	yes
7	yes (−1 or +3)	yes	yes
11	no	no: 23	yes
13	yes (−3)	yes	yes
17	yes (+1)	yes	yes
19	yes (+3)	yes	yes
23	no	no: 47	yes
31	yes (−1)	yes	yes
43	no	no: 431	yes
61	yes (−3)	yes	yes
67	yes (+3)	no: 193707721	no: 7327657
79	no	no: 2867	yes
89	no	yes	no: 179
101	no	no: 7432339208719	yes
107	no	yes	no: 643
127	yes (−1)	yes	yes
167	no	no: 2349023	yes
191	no	no: 383	yes
199	no	no: 164504919713	yes
257	yes (+1)	no: 535006138814359	no: 37239639534523
313	no	no: 10960009	yes
347	no	no: 14143189112952632419639	yes
521	no	yes	no: 510203
607	no	yes	no: 115331
701	no	no: 796337	yes
1021	yes (−3)	no: 40841	no: 10211
1279	no	yes	no: 706009
1709	no	no: 379399	yes
2203	no	yes	no: 13219
2281	no	yes	no: 22811
2617	no	no: 78511	yes
3217	no	yes	no: 7489177
3539	no	no: 7079	yes (prp)
4093	yes (−3)	no	no
4099	yes (+3)	no: 73783	no: 2164273
4253	no	yes	no: 118071787
4423	no	yes	no
8191	yes (−1)	no: 338193759479	no
9689	no	yes	no: 19379
9941	no	yes	no
11213	no	yes	no
16381	yes (−3)	no	no: 163811
19937	no	yes	no
21701	no	yes	no: 43403
23209	no	yes	no: 4688219
44497	no	yes	no: 2135857
65537	yes (+1)	no	no
65539	yes (+3)	no	no: 58599599603
86243	no	yes	no
110503	no	yes	no
131071	yes (−1)	no: 231733529	no: 2883563
132049	no	yes	no
216091	no	yes	no
262147	yes (+3)	no: 268179002471	no: 4194353
524287	yes (−1)	no: 62914441	no

exactly one is true ($p = 67, 257, 1021, \ldots$ for only (a) true; $p = 89, 107, 521, \ldots$ for only (b) true; and $p = 11, 23, 43, 79, \ldots$ for only (c) true). However, the New Mersenne Conjecture is true for all p less than 100000, which is the current limit of the search for Mersenne primes. It is valid also for all p between 10^5 and 10^6 for which at least one of the three statements is known to hold. We expect that the three statements are true simultaneously only for the nine primes mentioned above.

The Table above summarizes what is known about our conjecture. It lists all odd primes p satisfying at least one of these three conditions:

(1) $p < 1000000$ and $p = 2^k \pm 1$ or $p = 4^k \pm 3$.
(2) $p < 100000$ and $2^p - 1$ is prime.
(3) $p < 4000$ and $(2^p + 1)/3$ is prime.

When a number is asserted to be composite, a factor is given if one is known. The factors of M_{131071} and M_{524287} were found by Robinson [6]. The 1065-digit number $(2^{3539} + 1)/3$ passed a probabilistic primality test, but we did not give a complete proof that it is prime.

It is a simple consequence of quadratic reciprocity that if $p \equiv 1 \pmod 4$, then the factors of $2^p - 1$ are congruent to 1 or $6p + 1 \pmod{8p}$, and if $p \equiv 3 \pmod 4$, then the factors of $2^p - 1$ are congruent to 1 or $2p + 1 \pmod{8p}$. This observation is the starting point for a heuristic argument [7] which concludes that the number of p less than y for which M_p is prime is about $e^\gamma \log_2 y \approx 1.78 \log_2 y$, where γ is Euler's constant.

Likewise, one can show that if $p \equiv 1 \pmod 4$, then the factors of $(2^p + 1)/3$ are congruent to 1 or $2p + 1 \pmod{8p}$, and if $p \equiv 3 \pmod 4$, then the factors of $(2^p + 1)/3$ are congruent to 1 or $6p + 1 \pmod{8p}$. A heuristic argument like the one mentioned above concludes that the number of p less than y for which $(2^p + 1)/3$ is prime is also about $e^\gamma \log_2 y$.

The total number of natural numbers less than y with one of the forms $2^k \pm 1$ or $4^k \pm 3$ is about $3 \log_2 y$. Hence, the number of primes less than y with one of these forms is $O(\log y)$.

In view of the foregoing heuristics and the fact that there are about $y/\log y$ primes less than y, the probability that any one of the three statements holds for a randomly chosen prime p less than y is $O(y^{-1} \log^2 y)$. If the three statements were independent random events, then the expected number of primes p greater than L for which at least two of the statements hold is about $C\int_L^\infty y^{-2} \log^4 y\, dy$, which is finite. Substituting $L = 100000$ gives an upper bound on the expected number of failures of the New Mersenne Conjecture. Assuming a reasonable value for C (about 9) we find that the expected number of failures is less than 1. This is one reason why we believe that the conjecture is true. Another reason is that it holds for all p less than 100000 as well as those larger p for which it has been tested.

We are grateful to Duncan A. Buell and Jeff Young for testing the primality of $(2^p + 1)/3$ for several $p > 50000$, using a Cray 2 computer.

REFERENCES

1. R. C. Archibald, Mersenne's numbers, *Scripta Math.*, 3 (1935), 113.
2. Stillman Drake, The rule behind 'Mersenne's numbers', *Physis–Riv. Internaz. Storia Sci.*, 13 (1971) 421–424. MR 58#26870.

3. Malcolm R. Heyworth, A conjecture on Mersenne's conjecture, *New Zealand Math. Mag.*, 19 (1982) 147–151. MR 85a:11002.
4. M. Mersenne, Cogitata Physico Mathematica, Parisiis, 1644, Praefatio Generalis No. 19.
5. ______, Novarum Observationum Physico-Mathematicarum, Tomus III, Parisiis, 1647.
6. Raphael M. Robinson, Some factorizations of numbers of the form $2^n \pm 1$, *Math. Tables Aids Comput.* 11 (1957) 265–268, MR 20 #832.
7. S. S. Wagstaff, Jr., Divisors of Mersenne numbers, *Math. Comp.*, 40 (1983) 385–397, MR 84j: 10052.