Two Mersenne Prime Conjectures

Samuel S. Wagstaff, Jr.
Center for Education and Research in Information Assurance and Security
and
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907-1398
USA
ssw@cerias.purdue.edu

Abstract

We discuss two conjectures about Mersenne numbers, an old one and a new one. Heuristic arguments support both conjectures.

1 Introduction

The Mersenne numbers, Sequence A083420 in the *On-Line Encyclopedia of Integer Sequences* (OEIS) [6], are the integers $M_p = 2^p - 1$ for all primes p. If M_p is prime, then p must be prime. These exponents p form Sequence A000043 and the prime M_p are Sequence A000668. There are only 52 primes p for which M_p is known to be prime. Mersenne numbers have been studied for centuries. We recall a conjecture about them made in 1989 and then examine a new conjecture made in 2025. We give evidence that both conjectures are probably true.

2 The 1989 New Mersenne Conjecture

In 1644, Mersenne made a famous conjecture about which Mersenne numbers with $1 < p \le 257$ are prime. In 1989, Bateman, Selfridge, and the author [1] made the following conjecture about Mersenne numbers that might help explain how Mersenne made his conjecture. See [1] for details.

Conjecture 1. 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 $p = 4^k \pm 3$ for some positive integer k.

(b) M_p is prime.

(c) $(2^p + 1)/3$ is prime.

The prime numbers $(2^p + 1)/3$ in (c) are Sequence A000979 (Wagstaff primes) and their exponents p are Sequence A000978. This conjecture holds in the range of all known Mersenne primes, that is, for p up to about 10^8. It is easy to find examples in this range where exactly 0, 1, or 3 of the statements hold. All three of the statements are true when $p < 10^8$ only for $p = 3, 5, 7, 13, 17, 19, 31, 61$, and 127 (Sequence A107360). The sequence of p in Statement (a) clearly grows exponentially. A heuristic argument by the author [8] concludes that the sequence of p in Statement (b) also grows exponentially. A similar heuristic argument by Bateman, Selfridge, and the author [1] says that the sequence of p in Statement (c) grows exponentially. The heuristic argument in support of the New Mersenne Conjecture is that the intersection of two sequences of random integers that grow exponentially is likely empty or at least finite. Thus, if there is no p between 128 and 10^8 for which more than one statement holds, then probably there is no larger such p. We expect that all three statements hold only for the nine primes p mentioned above and that no more than one statement is true for each $p > 127$. See the web pages [4] and [5] for recent work on this conjecture.

3 Chen's Mersenne Conjecture of 2025

Fermat's little theorem implies that $M_p \equiv 1 \pmod{p}$ if p is prime. (We have $2^{p-1} \equiv 1 \pmod{p}$, so $2^p \equiv 2 \pmod{p}$ and $M_p = 2^p - 1 \equiv 2 - 1 = 1 \pmod{p}$.) Recently, Chen [2] made this conjecture.

Conjecture 2. If M_p is prime, then it is the smallest Mersenne prime $\equiv 1 \pmod{p}$.

If the conjecture were false for M_p, then there would be a prime $q < p$ such that M_q is prime and $M_q \equiv 1 \pmod{p}$. Chen [2] writes

> For example, M_{127} is prime, and it is the smallest Mersenne prime $\equiv 1 \pmod{127}$. Although M_{29}, M_{43}, M_{71}, and M_{113} are all $\equiv 1 \pmod{127}$, none of these Mersenne numbers is prime, so M_{127} is not a counterexample. Also, M_{17} is a Mersenne prime $\equiv 1 \pmod{257}$, but M_{257} is not prime, so M_{257} is not a counterexample either.

One can construct other false counterexamples if one assumes that certain composite Mersenne numbers are prime. True counterexamples might occur if certain double Mersenne numbers are prime (Sequence A103901). For example, $2^{89} \equiv 1 \pmod{2^{89} - 1}$ because M_{89} is prime. Since 89 divides 19936, we have $2^{19936} \equiv 1 \pmod{2^{89} - 1}$, so $M_{19937} = 2^{19937} - 1 \equiv 1 \pmod{M_{89}}$. If $M_{M_{89}}$ is prime, then it would be a counterexample to Chen's conjecture because the earlier Mersenne prime M_{19937} is also $\equiv 1 \pmod{M_{89}}$. Since $86243 \equiv 1 \pmod{107}$, if $M_{M_{107}}$ is prime, it and M_{86243} would give another counterexample.

We used the list [3] of all 52 known Mersenne primes to check that there is no counterexample with one of these numbers as M_p. We next describe how we performed this check.

For prime p, let n_p be the order of 2 modulo p. That is, n_p is the smallest positive integer n for which $2^n \equiv 1 \pmod{p}$. If $q < p$ and M_q is a counterexample to the conjecture for M_p, then $2^q - 1 = M_q \equiv 1 \pmod{p}$ or $2^q \equiv 2 \pmod{p}$. Since p must be odd we have $2^{q-1} \equiv 1 \pmod{p}$, so n_p divides $q-1$. For each known Mersenne prime M_p with odd p we computed n_p. These values are shown in Table 1. This table also shows the ratio $t_p = (p-1)/n_p$ to be used later. We checked that for each p in Table 1, n_p does not divide $q-1$ for each Mersenne prime M_q with $q < p$.

p	n_p	t_p	p	n_p	t_p	p	n_p	t_p
3	2	1	4253	4252	1	2976221	2976220	1
5	4	1	4423	737	6	3021377	1510688	2
7	3	2	9689	4844	2	6972593	871574	8
13	12	1	9941	9940	1	13466917	4488972	3
17	8	2	11213	11212	1	20996011	6998670	3
19	18	1	19937	9968	2	24036583	12018291	2
31	5	6	21701	21700	1	25964951	12982475	2
61	60	1	23209	967	24	30402457	1266769	24
89	11	8	44497	2781	16	32582657	1018208	32
107	106	1	86243	86242	1	37156667	1955614	19
127	7	18	110503	6139	18	42643801	21321900	2
521	260	2	132049	11004	12	43112609	10778152	4
607	303	2	216091	43218	5	57885161	28942580	2
1279	639	2	756839	378419	2	74207281	7420728	10
2203	734	3	859433	61388	14	77232917	77232916	1
2281	190	12	1257787	139754	9	82589933	82589932	1
3217	804	4	1398269	1398268	1	136279841	13627984	10

Table 1: Order of 2 modulo p for Mersenne prime exponents

Now we offer a heuristic argument similar to that in Section 2 to support Chen's conjecture.

Now $t_p = 1$ if and only if 2 is a primitive root modulo p, and this is the most popular value for t_p. Note that t_p is usually a small positive integer. Assuming the Generalized Riemann Hypothesis one can compute, for each positive integer t, the fraction of all primes p for which $t_p = t$. The answer is stated for general base a as Theorem 2.2 of Wagstaff [7] and specifically for $a = 2$ in the first example on Page 143 of that paper. The fraction for t is $c(t)/t^2$, where $c(t)$ is a positive constant that depends only on the residue class of t modulo 8. As t increases, the fractions decrease in proportion to t^{-2}. Since t_p is small for most primes p, n_p is almost always a large fraction of p.

If M_q is a counterexample to Chen's conjecture for M_p, then q must satisfy all four of these conditions:

(a) $2 < q < p$,

(b) q is prime,

(c) M_q is prime, and

(d) n_p divides $q - 1$.

We noted in Section 2 that the sequence of q for which M_q is prime grows exponentially, so it has few members in the interval $n_p - 2 < q < p$. Since n_p is a large integer these four conditions on q make it very unlikely that Chen's conjecture is false.

On January 16, 2011, Joerg Arndt added this comment to the OEIS Sequence A000043 of exponents p with M_p prime.

> The (prime) number p appears in this sequence if and only if there is no prime $q < 2^p - 1$ such that the order of 2 modulo q equals p; . . . .

This statement uses some of the words in this section, but it is not a restatement of Chen's conjecture. Our definition of *order of* 2 *modulo* q requires the order to be $< q$. Arndt uses an alternate definition of this order as a positive integer n for which $2^n \equiv 1 \pmod{q}$. With this definition it is easy to prove (the contrapositive of) his comment: If M_p is composite, then some prime $q < 2^p - 1$ divides $M_p = 2^p - 1$, so $2^p \equiv 1 \pmod{q}$. If some prime $q < 2^p - 1$ satisfies $2^p \equiv 1 \pmod{q}$, then q divides $2^p - 1 = M_p$, so M_p is composite.

4 Acknowledgments

I am grateful to the CERIAS Center at Purdue University for their support of this work. I thank Xinyao Chen for helpful comments about earlier versions of this paper.

References

[1] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr., The Editor's Corner: The new Mersenne conjecture, *Amer. Math. Monthly* **96** (1989), 125–128.

[2] Xinyao Chen. Personal communication, August 18, 2025.

[3] Great Internet Mersenne Prime Search, List of known Mersenne primes. Available at `https://www.mersenne.org/primes` , accessed on August 20, 2025.

[4] Mersenneplustwo, Mersenneplustwo factorizations. Available at `https://sites.google.com/site/bearnol/math/mersenneplustwo` , accessed on August 29, 2025.

[5] New Mersenne Conjecture, New Mersenne conjecture. Available at `http://www.hoegge.dk/mersenne/NMC.html` , accessed on August 29, 2025.

[6] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, 2025. Available at `https://oeis.org`.

[7] S. S. Wagstaff, Jr., Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.* **41** (1982), 141–150.

[8] S. S. Wagstaff, Jr., Divisors of Mersenne numbers, *Math. Comp.* **40** (1983), 385–397.

2020 *Mathematics Subject Classification*: Primary 11Y55, Secondary 11Y11, 11A51.
Keywords: Mersenne number, Mersenne prime, Wagstaff prime.

(Concerned with sequences A000043, A000668, A000978, A000979, A083420, A103901, and A107360.)
