A necessary condition for Mersenne primes

Souvik Sarkar

July 25, 2025

Introduction

Mersenne primes are prime numbers of the form $2^p - 1$ where p is also prime. Named after the French monk Marin Mersenne (1588-1648), these primes have fascinated mathematicians for centuries due to their connection to perfect numbers and their computational significance in modern cryptography.

The search for Mersenne primes is one of the most intensive computational endeavors in number theory. As of 2025, only 51 Mersenne primes are known, with the largest being $2^{136279841} - 1$, discovered through the Great Internet Mersenne Prime Search (GIMPS) project.

A natural question arises: *what conditions must p satisfy for $2^p - 1$ to be prime?* While this question remains largely open, we can establish a fundamental necessary condition that immediately eliminates infinitely many candidates from consideration.

Theorem

Main Theorem

Theorem. *Let $n \in \mathbb{N}$ and $n > 1$. We claim that if n is* not *a prime number, then the number $2^n - 1$ is* also not *prime.*

Primes $2^p - 1$ are called **Mersenne primes**, if p is also a prime. This theorem gives a *necessary* condition for Mersenne primality, but *not a sufficient one.*

Proof

Suppose n is **not** prime. Then there exist natural numbers $a, b \in \mathbb{N}$, such that: $n = a \cdot b, \quad 1 < a < n, \quad 1 < b < n$

The key insight is that this composite structure of n will allow us to factor $2^n - 1$ in a non-trivial way. Our goal is to show that $2^n - 1$ is not prime by explicitly **factoring** it into two factors, each greater than 1.

Factorization identity

The crucial observation is that we can use the algebraic identity for geometric series. Since $n = ab$, we have: $2^n - 1 = 2^{ab} - 1$

We can think of 2^{ab} as $(2^b)^a$, which allows us to apply the factorization formula $x^a - 1 = (x-1)(x^{a-1} + x^{a-2} + \cdots + x + 1)$ with $x = 2^b$:

$2^n - 1 = 2^{ab} - 1 = (2^b - 1)\left(2^{b(a-1)} + 2^{b(a-2)} + \cdots + 2^b + 1\right)$

This identity is the heart of the proof—it shows that the composite nature of n directly translates into a factorization of $2^n - 1$.

Defining the factors

For clarity, let's name our two factors:

$$x := 2^b - 1 \tag{1}$$

$$y := 2^{b(a-1)} + 2^{b(a-2)} + \cdots + 2^b + 1 \tag{2}$$

The first factor x is simply $2^b - 1$, which we know is at least 3 since $b \geq 2$.

The second factor y is a geometric series with a terms, where each term is a power of 2^b. We can write it more compactly as: $y = \sum_{k=0}^{a-1} (2^b)^k = \sum_{k=0}^{a-1} 2^{bk}$

Then our factorization becomes: $2^n - 1 = 2^{ab} - 1 = x \cdot y$

Verifying that both factors are non-trivial

To prove that $2^n - 1$ is composite, we need to show that both x and y are strictly between 1 and $2^n - 1$. This ensures we have a genuine factorization (not just $1 \times (2^n - 1)$ or $(2^n - 1) \times 1$).

For the first factor $x = 2^b - 1$:

Since $b > 1$ (because n is composite and $b < n$), we have: $x = 2^b - 1 \geq 2^2 - 1 = 3 > 1$

Also, since $b < n = ab$, we have $2^b < 2^{ab} = 2^n$, so $x = 2^b - 1 < 2^n - 1$.

For the second factor y:

The factor y is a sum of a positive terms: $y = \sum_{k=0}^{a-1} 2^{bk} = 1 + 2^b + 2^{2b} + \cdots + 2^{b(a-1)}$

Since each term is positive and we have at least two terms (because $a \geq 2$), we get: $y \geq 1 + 2^b \geq 1 + 2^2 = 5 > 1$

To see that $y < 2^n - 1$, note that y consists of only a terms from the full geometric series expansion of $2^n - 1$, so y is strictly smaller than the complete sum.

Therefore, we have established that $1 < x < 2^n - 1$ and $1 < y < 2^n - 1$, which means: $2^n - 1 = x \cdot y$ is composite

Conclusion

If n is not prime, then $2^n - 1$ is not prime either.

Remarks

Remark. *This result completely eliminates all composite numbers from consideration as potential Mersenne prime exponents. It's a powerful sieve that immediately rules out infinitely many candidates. The theorem is classical in elementary number theory, though it's sometimes overlooked in introductory treatments of Mersenne primes.*

The proof technique—using the factorization of $x^{ab} - 1$—is a beautiful example of how algebraic identities can reveal deep structural properties of numbers.

Remark. *The **converse is not true**, and this is what makes the search for Mersenne primes so fascinating: There are many prime values of n for which $2^n - 1$ is **not** prime.*

For instance, consider $n = 11$ (which is prime): $2^{11} - 1 = 2047 = 23 \times 89$

This shows that being prime is necessary but not sufficient for n to yield a Mersenne prime $2^n - 1$. The search for actual Mersenne primes among the remaining candidates (where n is prime) remains one of the most computationally intensive problems in number theory.

As of 2025, only 51 Mersenne primes are known, with the largest being $2^{136279841} - 1$, discovered through the Great Internet Mersenne Prime Search (GIMPS) project.