Mersenne Number $2^n - 1$

Mersenne Numbers

A Mersenne number, M_n, is a natural number of the form $2^n - 1$.
$M_1 = 1$, $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_4 = 2^4 - 1 = 15$.
A Mersenne Prime is a Mersenne number that is a prime number.
M_2 is a Mersenne Prime.
For $n \leq 128$, if $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ then M_n is prime.
The Mersenne number $2^{11} - 1$ is not prime even though 11 is prime.
$2^{11} - 1 = 2047 = 23 * 89$
The Mersenne number $2^{67} - 1$ is not prime even though 67 is prime.
The Mersenne number $2^{74,207,281} - 1$ is prime, the largest found so far. It has around 22 million digits.

$x^n - 1$

Consider $x^n - 1$.

Since $1^n - 1 = 0$ i.e. 1 is a root of $x^n - 1$
i.e. 1 is a solution of $x^n - 1 = 0$ then
$(x - 1)$ is a factor of $x^n - 1$.
i.e. $x^n - 1 = (x - 1) * f(x)$, some $f(x)$.
e.g.
$3^3 - 1$
$= 26$
$= 2 * 13$
$= (3 - 1) * 13$

$x^n - 1$ Cont'd

Determine $\frac{x^n-1}{x-1}$ as a series:

$$
\begin{array}{r|l}
 & x^{n-1} + x^{n-2} \quad \dots \quad +1 \\
\hline
x-1 & x^n - 1 \\
 & x^n - x^{n-1} \\
\cline{2-2}
 & x^{n-1} - 1 \\
 & x^{n-1} - x^{n-2} \\
\cline{2-2}
 & x^{n-2} - 1 \\
 & \qquad \ddots \\
 & \qquad\qquad x - 1 \\
 & \qquad\qquad x - 1 \\
\cline{2-2}
 & \qquad\qquad\ 0
\end{array}
$$

Check:

If $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + x + 1 \dots$ then

$x^n - 1 = (x-1) * (x^{n-1} + x^{n-2} + \cdots + x + 1)$

.

$x^n - 1$ Cont'd

$$
\begin{aligned}
&(x-1)*(x^{n-1}+x^{n-2}+\cdots+x+1)\\
&= x*(x^{n-1}+x^{n-2}+\cdots+x+1) - 1*(x^{n-1}+x^{n-2}+\cdots+x+1)
\end{aligned}
$$

$$
= \begin{array}{ccccccccccc}
x^n & + & x^{n-1} & + & x^{n-2} & \dots & + & x & & \\
 & - & x^{n-1} & - & x^{n-2} & \dots & - & x & - & 1
\end{array}
$$

$$= x^n - 1$$

Example

$$
\begin{aligned}
&3^3 - 1\\
&= (3-1)*(3^2+3+1)\\
&= 2*13\\
&= 26
\end{aligned}
$$

For $a \in \mathbb{N}, a > 1$, if $a^n - 1$ is prime then n is prime and $n = 2$

Theorem

For $a \in \mathbb{N}$,$a >: 1$, if $a^n - 1$ is prime then n is prime and $n = 2$

This has the form: $P \rightarrow Q \wedge R$
From Logic: $A \rightarrow B = \neg B \rightarrow \neg A$
$P \rightarrow Q \wedge R$
$= \neg(Q \wedge R) \rightarrow \neg P$
$= \neg Q \vee \neg R \rightarrow \neg P$
$= (\neg Q \rightarrow \neg P) \wedge (\neg R \rightarrow \neg P)$

To prove: if $a^n - 1$ is prime then n is prime and $n = 2$, prove

- If n is not prime then $a^n - 1$ is not prime
- If $n \neq 2$ then $a^n - 1$ is not prime.

.

Cont'd

- If n is not prime then $a^n - 1$ is not prime

Proof:
Assume n is not prime then $n = p * q$ where $p > 1$ and $q > 1$.
$a^n - 1 = a^{p*q} - 1 = (a^p)^q - 1$

Since $x^n - 1 = (x - 1) * (x^{n-1} + x^{n-2} + \cdots + x + 1)$
$(a^p)^q - 1 = (a^p - 1) * ((a^p)^{q-1} + (a^p)^{q-2} + \cdots + a^p + 1)$
$\therefore a^n - 1 = (a^p)^q - 1$ has factors > 1 such as
$(a^p - 1)$ and $((a^p)^{q-1} + (a^p)^{q-2} + \cdots + a^p + 1)$
$\therefore a^n - 1$ is not prime

Cont'd

- If $n \neq 2$ then $a^n - 1$ is not prime.

In this case the contrapositive is used i.e.
Show, if $a^n - 1$ is prime then $a = 2$
Proof:
$(a^n - 1) = (a - 1) * (a^{n-1} + a^{n-2} + \cdots + a + 1)$
If $a^n - 1$ is prime then $(a - 1) = 1$
otherwise $a^n - 1$ has a factor > 1.
If $(a - 1) = 1$ then $a = 2$.

Mersennne numbers when n is not prime

From above, if n is not prime then $a^n - 1$ is not prime.
In particular,

$$\text{if } n \text{ is not prime then } 2^n - 1 \text{ is not prime.}$$

Example

$2^6 - 1 = 63$ which is not prime since 6 is not prime.
$2^6 - 1 = 2^{2*3} - 1 = (2^2)^3 - 1$
$(2^2)^3 - 1$
$= (2^2 - 1) * ((2^2)^2 + 2^2 + 1)$
$= 3 * (4^2 + 4 + 1)$
$= 3 * 21$
$= 63$