

1) A Mersenne prime is a prime number of the form  $2^p - 1$ , where  $p$  is prime.

In 1644, Mersenne categorized all numbers of the form  $2^n - 1$  as either prime or not, for  $n = 1, 2, \dots, 257$

2) Theorem: If a number of the form  $a^n - 1$  is a prime, where  $n > 1$  and  $a > 0$ , then  $a = 2$  and  $n$  is prime, i.e.,  $a^n - 1 = 2^p - 1$  for some prime  $p$ . (So if  $a^n - 1$  is prime, it is a Mersenne prime)

[Examples  $2^2 - 1 = 3$ ,  $2^3 - 1 = 7$ ,  $2^5 - 1 = 31$ ,  $2^7 - 1 = 127$   
 $2^{11} - 1 = 2047$  is not,  $2^{13} - 1 = 8191 \dots$ ]

3) Proof: We assume  $a > 0$ ,  $n > 1$ , and  $a^n - 1$  is prime  
Then  $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1)$   
Clearly,  $a - 1 = 1$ , so  $a = 2$  (why?)

Also, if  $n$  is not prime (i.e., is composite), say  $n = rs$  with both  $r, s > 1$ , then

$$2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \dots + 2^r + 1)$$

Since  $r, s > 1$ , both factors on the right hand side are greater than 1, so  $2^{rs} - 1$  would be composite, a contradiction.

So  $n$  is prime,  $a = 2$ , and  $a^n - 1 = 2^p - 1$ , a Mersenne prime. Q.E.D.

Mersenne Primes have the form  $2^p - 1$

$M_{48}$  is the largest known prime.

Claim: If  $a^N - 1$  is prime for  $a, N \in \mathbb{N}$   
and  $a > 0$  and  $N > 1$ , then  $a = 2$  and  $N$  is prime.

Proof.

1st:  $a^N - 1 = (a-1)(a^{N-1} + a^{N-2} + \dots + a^2 + a + 1)$

$\Rightarrow a-1 = 1$  since  $a^N - 1$  is  $> 1$  prime.

$\Rightarrow a = 2.$

2nd: NTS  $N$  is prime.

Assume  $N$  is not prime. That is

$N = r \cdot s$  where  $r, s \in \mathbb{N}$  and  $r, s > 1$ .

$\Rightarrow a^N - 1 = 2^N - 1$

$= 2^{rs} - 1$

$= \underbrace{(2^r - 1)}_{> 1} (2^{r(s-1)} + 2^{r(s-2)} + \dots + 2^{rn} + 2^r + 1)$

$\Rightarrow 2^{r(s-1)} + 2^{r(s-2)} + \dots + 2^r + 1 = 1$  (since  $a^N - 1$  is prime).

$\Rightarrow \Leftarrow$

Hence  $N$  is prime and  $a = 2$ .

Q.E.D.

That is, the only primes of the form  $a^N - 1$  are Mersenne primes  $2^p - 1$