SOME NEW OBSERVATIONS ON MERSENNE NUMBERS AND PRIMES

Euclid observed several thousand years ago in his book "The Elements" that -

1+2=3
1+2+4=7
1+2+4+8=15
1+2+4+8+16=31
1+2+4+8+16+32=63
1+2+4+8+16+32+64=127
1+2+4+8+16+32+64+128=255

In this set of equations one sees that many of the sums including 3, 7, 31, 127 are prime numbers. In modern notation for a finite geometric series of this type one has-

$$S[N] = \sum_{n=0}^{N} 2^n = 2^{N+1} - 1$$

Here S[N] is a prime number for N=1,2,4,6,.. but fails to be prime for N=3,5.7,.. The French priest and mathematician Marin Mersenne(1588-1648) observed from Euclid's results that 2^2-1=3, 2^3-1=7, 2^5-1=31, and 2^7-1=127 are all prime numbers. This led him to the conclusion that-

Any number of the form $M[p_n]= 2^{(p_n)}-1$, where p_n is the nth prime number, is likely to be a prime

Today one refers to the $M[p_n]$s as Mersenne Numbers and so far 48 of these have been found to be prime. The majority of the $M[p_n]$ s , however, are composite numbers such as 2^{11}-1=2047=23·89 and 2^{23}-1= 8388607 =47·178481. The larger the prime p_n the larger will be the value of $M(p_n)$. It is our purpose here to re-examine the Mersenne Numbers and Primes to see if one can come up with some new properties heretofore unrecognized.

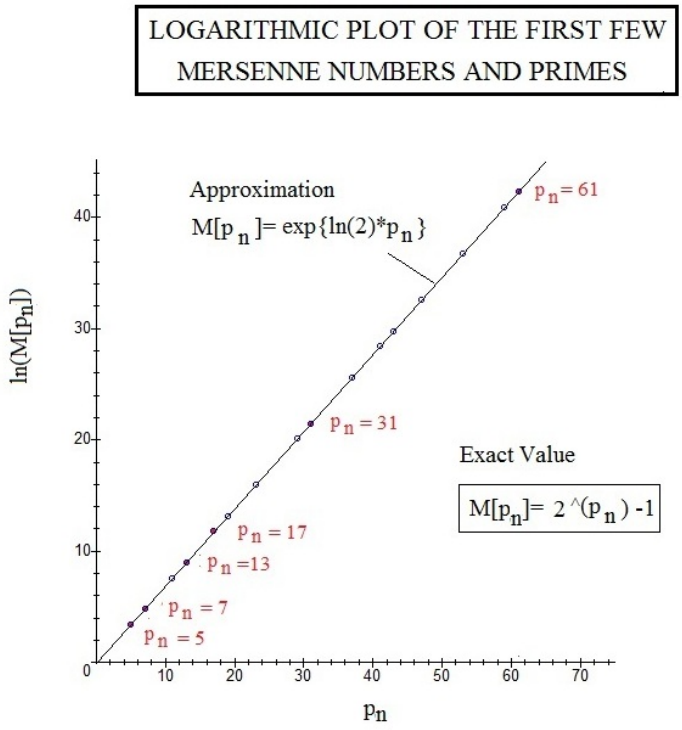
Our starting point is to run the following MAPLE search program-

for n from 1 to 18 do { n, ithprime(n), 2^ithprime(n)-1, isprime(2^ithprime(n)-1)}od;

This yields the results-

Integer, n	Prime number, p_n	Value of $M[p_n]=2^{\wedge p}{}_n-1$	Prime (P)or Composite(C)
2	3	7	P
3	5	31	P
4	7	127	P
5	11	2047	C
6	13	8191	P
7	17	131071	P
8	19	524287	P
9	23	8388607	C
10	29	536870911	C
11	31	2147483647	P
12	37	137438953471	C
13	41	2199023255551	C
14	43	8796093022207	C
15	47	140737488355327	C
16	53	9007199254740991	C
17	59	576460752303423487	C
18	61	2305843009213693951	P

We see from these results that the size of Mersenne Numbers and Primes increase rapidly with increasing n, and that they always end in 1 or 7. Also one notices that **$M[p_n]$ mod(6) is always equal to 1**. Thus $(2^{1571}-1)\text{mod}(6)=1$, 1571 is a prime, but $2^{1571}-1$ is a composite.The binary version of all $M[p_n]$s contain only 1s. Thus $p_n=127$ in decimal reads 1111111 in binary. We have plotted the logarithm of these Mersenne Numbers and Primes in the graph below. Note that an excellent approximation to the value of a Mersenne Number for larger p_n is given by $M[pn]=\exp\{\ln(2)*p_n\}$ since for larger p_ns the term $2^{\wedge}(p_n)$ is much larger than 1.



Let us look at the first seven Mersenne Primes in this table and write down the differences from their nearest neighbor . The results are summarized in the following table-

n	p_n	$M[p_n]$	$M[p_{n+1}]-M[p_n]$
2	3	7	24
3	5	31	96=4·24
4	7	127	8064=336·24=84·96=21·384
6	13	8191	122880=5120·24=1280·96=320·384=80·1536=20·6144 =5·24576
7	17	131071	393216=16384·24=4096·96=1024·384=256·1536=64·6 144=16·24576=4·98304=1·393216
8	19	524287	2146959360=89456640·24=22364160·96=5591040·384 =1397760·1536=349440·6144=87360·24576=21840·98 304=5460·393216=1365·1572864
11	31	2147483647	2305843007066210304=96076791961092096·24=24019 197990273024·96=6004799497568256·384=150119987 4392064·1536=375299968598016·6144=938249921495 04·6144=23456248037376·24576=5864062009344·983 04=1466015502·393216

You will notice that the difference between neighboring Mersenne Numbers, be they prime or composite, will always be an integer multiple of 24. This number was recently found by us when we observed that all Mersenne Numbers M[p] lie along a diagonal in the 4th quadrant of an integer spiral defined in polar coordinates as $[r,\theta]=[n,2\pi n/8]$ and along a diagonal in the 1st quadrant of an integral spiral defined as $[r,\theta]=[n,2\pi n/6]$. The spacing between odd numbers along the specified diagonals are 8 and 6, respectively. Hence the lowest number divisible by both 6 and 8 is 24 and this leads to the conclusion that-

$$\{M[p_m]-M[p_n]\}/24=\text{integer for } 3\leq n<m$$

In terms of modular arithmetic, this statement is equivalent to saying-

$$\mathbf{\{M[p_m]-M[p_n]\}\ mod(24)=0}$$

We can calculate the value of the above integer by noting that-

$$\{\{(2^{p_m}-1)-(2^{p_n}-1)\}/24=2^{p_n}(2^{(p_m-p_n)}-1)/24=\text{integer}$$

To test these results consider the Mersenne Numbers $M[211]=2^{211}-1$ and $M[313]=2^{313}-1$. One finds-

$$[(2^{313}-1)-(2^{211}-1)]\,\mathrm{mod}(24)=2^{211}(2^{102}-1)\,\mathrm{mod}(24)=0$$

with-

integer=$2^{211}(2^{102}-1)/24=$
6953082799221712507796294616435972869257911112011266594519228275042135889970827973886539202 56

One notices from the last table that the spacing between $M[p_m]$ and $M[p_n]$ as n increases will increase to an ever larger spacing of $24(4^k)$, where the integer k is 1 for $p_n\geq 5$, 2 for $p_n\geq 7$, 5 for $p_n\geq 13$ and 7 for $p_n\geq 17$. An estimate for the spacing is about $24(4^{(p_n/2)})=24(2^{(p_n)})$. The actual spacing $G[p_n]$ between the primes M[107] and M[127] is found to be-

G[107]= ((2^127-1)-(2^107-1))=170141021201192402518323912137873817600

We can write the value of G[107] as -

$$G[107]=349525\cdot 24(4^{52})=349525\cdot 486777830487640090174734030864384$$

The factor $24(4^{52})$ is seen to lie in the ball-park of the spacing estimate of $24(2^{107})$.

Since all Mersenne Numbers and Primes are of the form 6n+1, we can distinguish composite(C) from prime (P) forms of $M[p_n]$ by looking at-

$$m = \frac{(M[p_n] - p_k{}^2)}{6p_k} \quad for \quad k = 3,5,7,11,...sqrt(M[p_n])$$

If an integer solution for m exists then $M[p_n]$ is composite. Otherwise it will be prime.(See our earlier pdf file on the Sieve of Eratosthanes of why this is so). A more elegant way to express this last equation is to say that $M[p_n]$ is prime if-

$$\{M[p_n] - p_k{}^2\} \bmod(6p_k) \neq 0 \quad for \quad p_k = 3,5,7,11,..sqrt(M[p_n]$$

If we look at M[11]=2047, we find that p_k=23 yields zero in the mod operation. Hence the Mersenne Number M[11]=23{23+6(11)}=23·89 is a composite. On the other hand, M[13]=8191 produces no zero mod in $3<p_k<89$ and so is prime. This test is just as useful as the classic Lucas-Lehmer test and has the advantage that the factors for a composite number appear directly and that it works for all odd numbers of the form N=6n+1.

The largest Mersenne Prime known as of February 2013 is-

$$M[57885161]=2^{57885161}-1$$

This number is only the 48th Mersenne Prime found so far. It is suspected that there are an infinite number of such primes but trying to find more of these appears to be a rather unrewarding effort similar to calculating π beyond a billions places. The $M[p_n]$ primes are useless for applications in cryptography since they are so well known, and because they mostly exceed in digit length anything which could be of use for public keys.

U.H.Kurzweg
July 2013