PROPERTIES OF MERSENNE NUMBERS AND PRIMES

If one looks at the sequence of numbers-

M(p)= 3, 7, 31, 127, 2047 , 8291, 131071, 524287

one notices that its elements are, with the exception of 2047, prime numbers defined by –

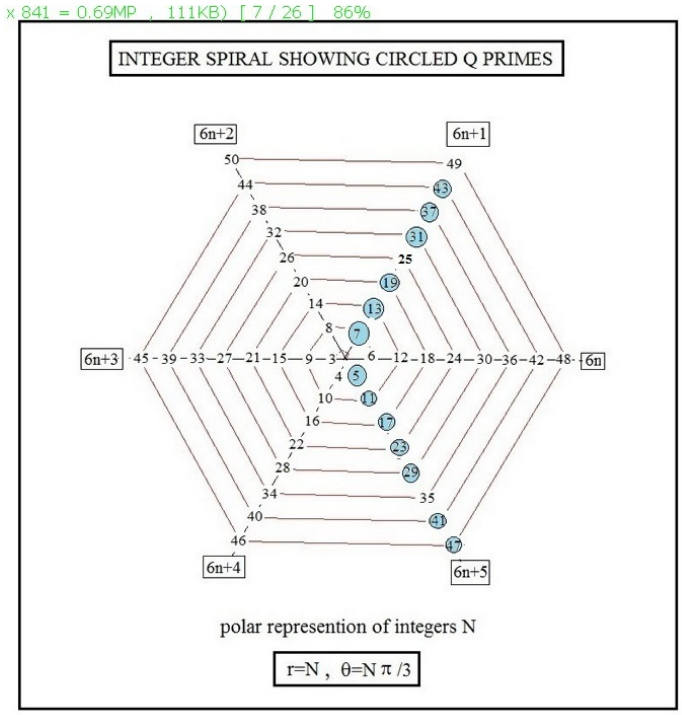
$$M(p) = 2^p - 1 \quad with \quad p \quad being \quad the \quad primes \quad 2, 3, 5, 7, 11, 13, ...$$

These numbers for any prime p are known as Mersenne Numbers named after the French cleric and mathematician Marin Mersenne(1588-1648). To date less than fifty of these numbers have found to be prime. The vast majority of the numbers M(p) are composite numbers especially at large p. It is our purpose here to examine these Mersenne Numbers in more detail.

The first thing we notice is that they are always odd numbers when p≥3 ending in either 1 or 7 . This means that –

M(p) mod(6) =1

whenever p≥3 without exception. It implies that Mersenne Numbers lie along the radial line 6n+1 in the following hexagonal integer spiral diagram-



The M(p) primes are quite sparse compared to the Q Primes along this same radial line of 6n+1. Only M(p)= 7 and 31 are shown in the diagram. Now 7 and 31 differ from each other by 24= 6x4. The next gap for M(p) will be 127-31=96=6x16=12x8=24x4=48x2. These observations suggests that we might identify Mersenne Numbers by mod values mod(6) followed by mod(12), mod(24), etc. We have done so and get the following results-

p	M(p)	M(p) mod(6)	M(p) mod(12)	M(p) mod(24)	M(p) Mod(48)	M(p) Mod(96)
2	3	-	-	-	-	-
3	7	1	-	-	-	-
5	31	1	7	7	-	-
7	127	1	7	7	31	31
11	2047	1	7	7	31	31
13	8191	1	7	7	31	31
17	131971	1	7	7	31	31
19	524287	1	7	7	31	31
23	8388607	1	7	7	31	31
29	536870911	1	7	7	31	31
31	2147483647	1	7	7	31	31

The table shows that the mod operations using 6, 12 ,24, 48, 96, etc yields the same constant number for a fixed mod. The mod sequence reads-

1, 7, 31, 127, 511, 2047, 8191, …

where the elements are recognized as–

$$2^{2m+1}-1 \quad with \quad m = 0, 1, 2, 3, 4, 5,...$$

For mod(6x2m), the Mersenne Prime will lie along only the single radial line $(6x2^n)$+const , where the constant represents the appropriate constant for a given mod. This means, for example , that M(p)=127 will lie along the radial line 48(k)+31 at k=2 in an integer spiral with 48 radial lines. The next Mersenne Number along this line will be 48(k)+31=2047 with k=42.

In the above table the Merseene Numbers corresponding to p=11, 23, and 29 are composite, while the others are primes. The mod operations do not distinguish between the two types of numbers, namely, composite or prime. This distinction must be found by some type of primality test. The simplest of such tests is that of Fermat known as Fermat's Little Theorem. It states that a number is prime if-

$$\frac{(a^{p-1}-a)}{p} = \text{integer}$$

, where a is a low integer such as 2, 3, 4,… . One can simplify this result by recasting things using modular arithmetic. Its equivalent form reads-

$$(a^{p-1}-1)\ \mathrm{mod}(p)=0$$

So if p=127, we get-

$$(2^{126}-1)\mathrm{mod}(127)=0$$

, meaning 127 is a prime. What about the Mersenne Number M(11)=2047? Here we get-

$$(3^{2046}-1)\mathrm{mod}(2047)=1012$$

indicating that M(11) is a composite. Note that here using a=2 would not work as a test.

Since in modular arithmetic we have the identity-

$$(AxBxC)\ \mathrm{mod}(N)=[A\ \mathrm{mod}(N)]x[B\ \mathrm{mod}(N)]x[C\ \mathrm{mod}(N)]$$

we can simplify the Fermat test for primeness by writing-

$$(a^{p-1}-1)\,\mathrm{mod}(p)=[(a^{(p-1)/2}-1)\,\mathrm{mod}(p)]x[(a^{(p-1)/2}+1)\,\mathrm{mod}(p)]$$

Sometimes this type of breakup can be continued for several more terms making the mod operations a lot easier. Take the Mersenne Number 8191. To test if it is prime we write-

$$(2^{8190}-1)\,\mathrm{mod}(8191)=$$

$$[(2^{4095}-1)\,\mathrm{mod}(8191)]x[(2^{4095}+1)\,\mathrm{mod}(8191)]=[0]x[2]=0$$

So it is a Mersenne Prime. To make super-sure, we can replace 2 by any other positive integer. Doing so, we find-

$$(3^{8190}-1)\,\mathrm{mod}(8191)=0$$

and the primeness of M(13) is confirmed.

A question often asked is how did Mersenne come up with the form for M(p). The answer is that he was studying the works of the ancient Greek mathematician Euclid. In Euclid's book it is shown 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

or, in general, that-

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

Now, if N+1=p, then the right hand side of this last expression just represents the Mersenne Number M(p). It yields the identity-

$$\sum_{n=0}^{p-1} 2^n = 2^p - 1 = M(p)$$

This is most likely the way Mersenne came up with his number. It says, for example, that –

M(7)=1+2+4+8+16+32+64=127

It should be pointed out that the Mersenne Numbers are not the only numbers capable of producing primes via the above approach. By generalizing the above 2^n series, we have-

$$\sum_{m=0}^{N} a^n = \frac{(a^{N+1} - 1)}{N} \quad where \quad a = 2, 3, 4, 5, ...$$

If we now take the odd number a=3, then a^{N+1} will also be odd. Since prime numbers above p=2 are also odd numbers, it suggests one define a generalized Mersenne number sequence given by-

F(a,N,b)= $a^N + b.$ *with* $a = 2,3,4,5,..$ *and* $b = \pm 1, \pm 2, \pm 3, ...$

In an integral spiral with six radial lines the function F(a,N,b) will lie either along the line 6N+1 or 6N-1. The corresponding mod operation will yield 1 or 5.

We have played around with various combinations of a and b and find one of the richest forms for yielding primes is-

F(3,N,2)=K(N)

Here K(N) mod(6)=5 meaning these numbers all lie along the radial line 6N-1 in the above integral spiral. We have used our PC to find the values of N for which K(N) is a prime. Here are the results when running over the range 0<N<2000 :

N=1,2,3,4,8.10.14,15,24,26,36,63,98,110,123,126,,139,235,243,315,363,386,391, 494,1131,1220,1503,1858,

This shows a total of 28 primes in the range considered , making the numbers K(N) more dense in primes than the standard Mersenne Primes of which less than 50 have been found to date. Here is the prime number corresponding to K(1858) :

$3^{1858}+2=$
309949734826573254479851471276200892985304310069565946859202148256633266191137690576952135474844404538372461230101006691271009555759919127457869223148660164613467627385033860708738672704316650862181089633382991315337701542754751372995001149340588749380743536244008880419755202390383627639285895496613970962701489924969795727825590048078397355734118492863593725501268400567250135296630863031128376511219475662720257626805673311452744631321737696232779367051782399514104280263667180701547531032088649276210976147452750560033145878420041510221647182900875021810238965863623224904713399693521685908522220999474927503580442427935550946200830198700373449243582744499189296500580263454833210298365535155326181801482295213278862293406357314198353241285393759520549296816928599853248072473293309376537937390628464770980014113878906045022870019937434926857282944448276114607243265213141322025447691

This 790 digit long prime has, as expected, the value K(1858) mod(6)=5.

We have also played around with other values of ‘a’ and ‘b’. None are found to be quite as rich in primes as the K(N) numbers.

An additional generalized Mersenne Number sequence which we examined in some detail is-

$$F(2,N,1)=2^N+1$$

Searching this function for primes, we were able to find only the five primes given in the following table-

N	F(2,N,1)
1	3
2	5
4	17
8	257
16	65537

In looking at the progressions of N in the table it is clear that they are given by $N=2^n$. That is, the number F(2,N,1) can also be written as-

$$F(2,2^n,1)=2^{2^n}+1$$

But this function is recognized at once as representing the Fermat Numbers. Fermat originally thought all these numbers are prime for any positive integer N, but Euler proved him wrong by showing that $2^{32}+1$ factors into

$$4294967297=641 \times 6700417$$

Since that time no additional Fermat Primes have been found, so it is safe to say that $F(2,2^n,1)$ are all composite numbers when $n\geq 5$. Also we have searched F(2,N,1) over the entire range $16<N<1000$ and find no additional primes. It leads to the conjecture that –

The infinite sequence of numbers F(2,N,1) contains only five primes corresponding to N=1,2,4,8,16 and no more.

Finally we point out that there are an infinite number of other number sequences which have a much higher prime number density then the Mersenne Numbers. One of these which comes to mind is $G(N)=N^2+(N\pm 1)$. It has a total number of 83 primes out of the first 200 possibilities ($1<N<100$ for both + and – case).

U.H.Kurzweg
Septemver 18, 2015