PRIMES OF THE FORM N(n,a)=(2^n)+a

We have shown in several earlier pages on our Tech-Blog Web Page that all prime numbers five or greater must have the form $6n\pm1$ without exception. Among this infinite set of primes there are two sub-sets known as Mersenne and Fermat Primes, which among the primes have drawn the most attention. They are defined , respectively, as-

$$M(p)=2^p-1 \quad \text{and} \quad F(n)=2^{(2^n)}+1$$

Here p is a prime number and n a positive integer. At the present time there have been just 51 Mersenne Primes M(p) found although there will be more coming in the future. On the other hand, there are just five known Fermat primes F(n)=(3, 5, 17, 257, 65537) with no further primes expected. In looking at M and F, one sees that they have a generalized form-

$$N(n,a)=(2^n)+a$$

, where n has certain integer values with 'a' either a positive or negative integers. It is the purpose of this note to look at the conditions for which N(n,a) is a prime number. In the discussion below we will see that, in addition to Mersenne and Fermat primes, there are an infinite number of additional primes described by this general formula.

Prime Forms of N(n,a):

We start with the identity-

$$p=6m\pm1=2^n+a$$

valid as long as the prime p equals five or greater and m, n, and 'a' have certain integer values. Next we choose a value for m, say m=3. This yields the primes p=19 or 17. From this result we have-

$$19 \text{ or } 17=2^n+a$$

Choosing n=4 produces the primes-

$$19=2^4+3 \quad \text{and} \quad 17=2^4+1$$

, while n=5 yields the primes-

$$19=2^5-13 \quad \text{and} \quad 17=2^5-15$$

Note that to keep the magnitude of 'a' small one chooses a 2^n near the mean of 19 and 17. If we had taken n=3 , the two forms of N(n,a) would have been –

$19=2^3+11$ and $17=2^3+9$

What is clear from these last results is that we can represent any prime via N(n,a) for the right choices of m, n and 'a'. So, for instance, p=89=6(15)-1=2^6+25. That is,-

$$N(6,25)=89$$

We can test the primeness of 89 by demanding that (89+1)=σ(89)=90. Here σ(89) is the sigma divisor function of Number Theory.

For any prime we have p= 2^n+a. On solving this produces-

$$n=\ln(p-a)/\ln(2)\sim\ln(p)/\ln(2)$$

with often 'a'<<p. Take the case of the prime

p=524287 where-

n~ln(524287)/ln(2)=18.999. So we try n=19 to get the identity-

$$524287=2^{19}-1$$

This result is recognized as the Mersenne Prime M(19).

Another form for N(n,a) follows from p=2852149 where

n~ln(2852149)/ln(2)=21.44. So we try n=21, to get the identity-

$$2852149=2^{21}+754997$$

Here 'a' is quite large but could be brought down by changing p to another prime p=2097169 which lies closer to 2^21. This produces the prime -

$$2097169=2^{21}+17$$

Since 2^n is always even, it is necessary that 'a' will need to be odd such as -1, 17 and 754997 above.

Relation between N(n+k,a+b) and N(n,a):

One can relate two different N(n,a) to each other as follows. Start by expanding-

$$N(n+k,a+b)=2^{(n+k)}+a+b=2^k(2^n+a)-a2^k+a+b=2^kN(n,a)+b+a(1-2^k)$$

This produces the identity-

$$N(n+k,a+b)=2^k\, N(n,a)+a(1-2^k)+b$$

So, If we let a=-1, b=2, k=3, and n=5, one finds-

N(8,1)=2^3[N(5,-1)+1]+1=257

Also we can use this identity to relate two separate Mersenne Primes to each other by letting n=5, k=8, a=-1, and b=0. This produces-

N(13,-1)=2^8[N(5,-1)+1]+1

Also N(5,-1) equals the Mersenne Prime M(5)=2^5-1=31. Hence the Mersenne Prime –

M(13)=256(31)+255=8193

This procedure can speed up a lot the finding of higher Mersenne and other primes.

Prime Density versus 'a':

By fixing 'a' as an integer near zero, one can check on the number of primes found in a given range of n. We call this number the prime density. It will be low for many 'a's with a few exceptions. The density of Mersenne Primes where 'a'=-1 can be considered of intermediate density while for the value of a=15 we find the density to be large compared to its neighbors. Indeed we find twenty-six primes for 2^n+15 when evaluating things over the range n=1 to n=200 as shown in the following graph-

N(n,15)=2^n+15

1, 17, *true*
2, 19, *true*
3, 23, *true*
4, 31, *true*
5, 47, *true*
6, 79, *true*
8, 271, *true*
10, 1039, *true*
11, 2063, *true*
12, 4111, *true*
15, 32783, *true*
16, 65551, *true*
22, 4194319, *true*
23, 8388623, *true*
26, 67108879, *true*
30, 1073741839, *true*
32, 4294967311, *true*
40, 1099511627791, *true*
42, 4398046511119, *true*
46, 70368744177679, *true*
61, 2305843009213693967, *true*
72, 4722366482869645213711, *true*
76, 75557863725914323419151, *true*
155, 45671926166590716193865151022383844364247891983, *true*
180, 1532495540865888858358347027150309183618739122183602191, *true*
198, 401734511064747568885490523085290650630550748445698208825359, *true*

We see from the graph that the tenth prime is 4111. This indicates a much higher prime density than that for Mersenne (2^n-1) where the tenth prime is a 27 digit long number. In view of the simplicity of how primes are generate for some different ‘a’s suggests that the GIMP approach to find the next higher Mersenne prime is to a large extent a waste of time since there are an infinite number of other primes given by $N(n,a)=2^n+a$ for lower n which may find more direct applications including for cybersecurity.

U.H.Kurzweg
March 4, 2023
Gainesville, Florida