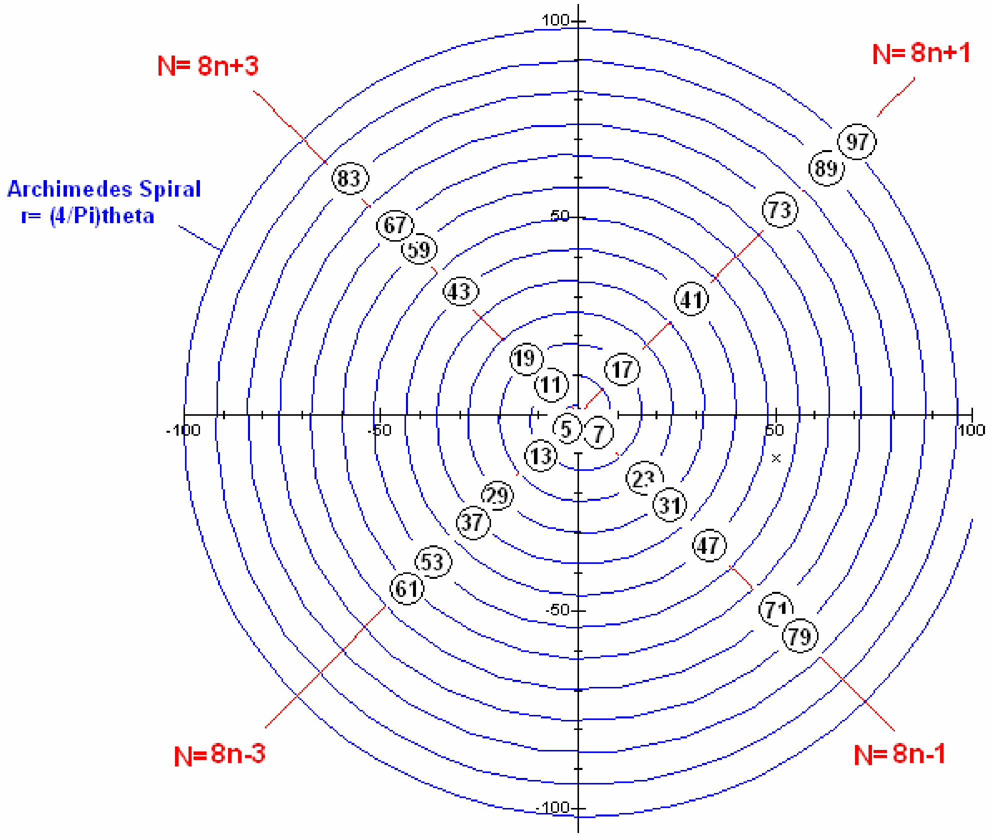
BINARY REPRESENTATIONS OF PRIME NUMBERS AND CALCULATIONS FOR PRIMALITY

In several notes above we have shown that it is possible to represent all real positive odd numbers as points of the intersections of the Archimedes Spiral r=(4/π)θ and the diagonal lines y=±x. The distance from the origin to the intersection represents the value of the number N. Since all prime numbers (with the exception of 2) are also odd numbers they will fall along the same diagonal lines. We indicate their location and value for all values 4<N<100 below.

Distribution of the Primes for 4<N<100



Note that the spacing between the primes along a given diagonal is always a multiple of 8 so that, for example, 73-41=4*8 and 83-11=12*8. What is not clear apriori is what values of n lead to primes and which will be composite numbers. In studying this point further, it is of advantage to cast the four groups of numbers shown into their binary form. This produces the four tables-

First Quadrant: N=8n+1

n	Decimal N	Binary N
2	17	10001
5	41	101001
9	73	1001001
11	89	1011001
12	97	1100001

Second Quadrant: N=8n+3

n	Decimal N	Binary N
1	11	1011
2	19	10011
5	43	101011
7	59	111011
8	67	1000011
10	83	1010011

Third Quadrant: N=8n-3

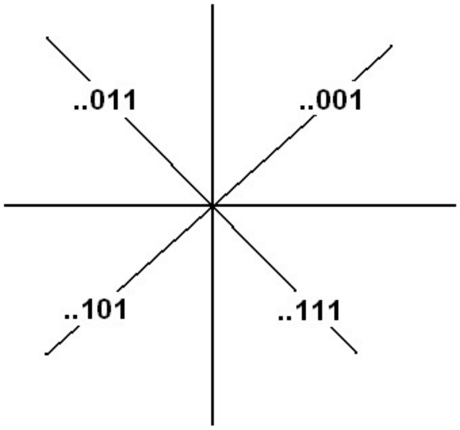
n	Decimal N	Binary N
1	5	101
2	13	1101
4	29	11101
5	37	100101
7	53	110101
8	61	111101

Fourth Quadrant: N=8n-1

n	Decimal N	Binary N
1	7	111
3	23	10111
4	31	11111
6	47	101111
9	71	1000111
10	79	1001111

What is clear from these binary representations of the primes below N=100 is that they all begin and end in 1 . This is of course no surprise since any even number plus 2^0=1 produces an odd number. Furthermore the last three digits of the binary representations for the numbers N=8n+1 are 001, those corresponding to N=8n+3 end in 011, those corresponding to N=8n-3 end in 101, and those corresponding to N=8n-1 end in 111. We summarize this result by the diagram-

LOCATION OF PRIMES AS DETERMINED BY THEIR BINARY ENDINGS



Thus one can see at once along which diagonal a given number will lie. Furthermore, one has the interesting observation that the Mersenne primes 2^n-1 have the form 11111…11111 and lie along the diagonal in the 4th quadrant, while one of our own set of primes 2^(2n+1)+1)/3 has the form 10101010…101011 in binary and lie along the diagonal in the second quadrant. One finds the primes

$$2^{13}-1=11111111111 \quad \textit{and} \quad (2^{17}+1)/3=1010101010101011$$

in binary. Unfortunately the binary three digit endings apply whether the number is prime or just an odd number. Thus the Mersenne number 2^11-1=2047 also reads 11111111111 but is not prime since 2047=23*89. So the question arises how does one distinguish between prime and composite versions of N=8n±1 and 8n±3. A method we use is a slight modification of the sieve of Eratosthenes consisting of dividing the number N along a given diagonal by the all numbers 8n±1 and 8n±3 up to values equal to less than the square root of N . The calculations begin with the lowest values of n and the first divisor is chosen to match that of the particular diagonal along which the number N lies. If any of the resultant quotients turn out to be integer one can stop the calculation knowing the number is composite. If no integer quotient values are found, one continues on with the calculations trying the other forms of the denominator. If all fail to produce an integer value, then the number is prime.

To test the primality of the Mersenne number N=2047=8(231)-1 , which in binary reads 11111111111 , we first notice that it lies along the diagonal in the 4th quadrant as characterized by its 111 binary ending. We then divide N by 8n-1 up to n=6 since 8(6)-1 is about equal to sqrt(2047)=45.24.. . If any of the fractions become integer, then the number is composite. Here our one line MAPLE program reads-

```
for n from 1 to 6 do {n,evalf((2^11-1)/(8*n-1))} od;
```

For n=3 it spits out the integer value 89 and hence 2047=89*23 is composite and no further tests are necessary. In the event one had found no integer result, divisions by 8n+1, 8n+3 and 8n-3 would follow.

Take next the case-

```
for n from 1 to 52 do {n,evalf((2^19+1)/(3*(8*n+1)))} od;
```

which corresponds to(2^(19)+1)/3=174763 or 10101010101010101011 in binary. One finds no factor of 8n+1 up to n=52 and hence must try the other three cases. These again yield no integer quotient and hence one can conclude that 2^19+1)/3 is prime.

As a third example consider the number N=1234567=8(154321)-1. Here the sqrt(N)=1111.11.. and hence maximum n needed is about n=139. The program for the prime evaluation reads-

```
for n from 1 to 139 do {n,evalf((1234567)/(8*n-1))} od;
```

and is found to have an integer solution of 9721 at n=16. So we conclude that N=1234567 is composite and equal to (8*16-1)(9721). The problem with this approach , which clearly always works, is that the computing become unwieldy when N is large. It is the resultant long computing times required to factor large numbers which makes public key electronic cryptography possible.

As a final demonstration consider the famous ten digit Fermat number-

$$N = 2^{2^5} + 1 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 8(536870912) + 1$$

In binary it reads- 1000000000000000000000000000000000001 and thus lies along the diagonal in the first quadrant. One needs to test up to 8n+1=sqrt(N) or n=8192. The test is run in units of 100 beginning with the smallest values of n. The first run will be-

```
for n from 1 to 100 do {n,evalf(4294967297/(8*n+1))} od;
```

One is lucky here since the program already finds an integer quotient at n=80. Hence one can conclude (as did Euler without the benefit of electronic computer) that this Fermat number is not prime since it factors into-

$$4{,}294{,}967{,}297 = [8(80)+1][6700417] = 641 \cdot 6700417$$

Note here that the components 641 and 6700417 are both prime numbers. Typically I find, in carrying out such factoring operations, it is best to start with the lowest values of n as this tends to often save computing time when the number is composite.

May 2009