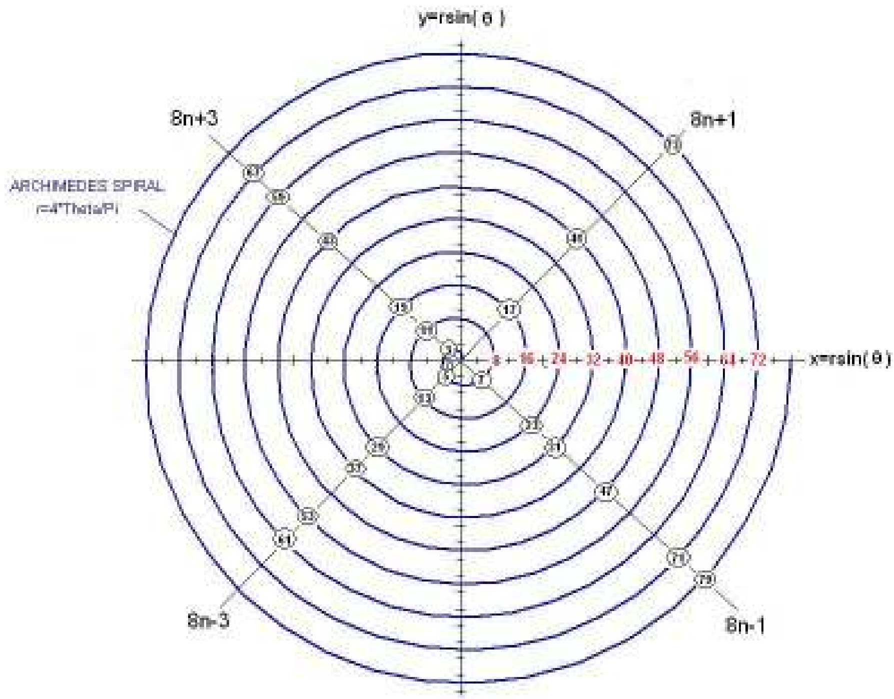
COMPOSITE AND PRIME NUMBERS GENERATED BY THE FORMULAS $S=2^n\pm1$ AND $S=2^n\pm3$

In several of our earlier discussions above we have shown how all real integers may be represented as the points of intersection of the Archimedes Spiral $r=(4/\pi)\theta$ and the axes $x=r\cos(\theta)$ and $y=r\sin(\theta)$ or the diagonal lines $y=x$ and $y=-x$. One has a picture as follows-



Note that the location of all even integers lie along the x and y axes while all odd integers are found along the diagonal lines. One notes that the intersections of the spiral along the positive x axis occur at 8, 16, 24,..8n and that the radial distance from the origin to any integer just represents its magnitude. All odd integers lie along the four diagonal lines 8n+1, 8n+3, 8n-3 and 8n-1 in the first, second, third and fourth quadrant, respectively. I have indicated the first few prime numbers , all of which must fall on these diagonal lines(n=2 excluded), by the circled numbers shown in the figure. To determine the location of a particular integer is a simple matter of measuring off the radial distance from the origin and noting among which of the total of eight radial lines shown it lies. For example, n=67 is equal to 8(8)+3 and so is located on the diagonal in the second quadrant at he 8^{th} turn of the spiral. Also the Mersenne prime $n=2^{13}-1= 8191$ is located at the 1024^{th} turn of the Archimedes spiral along the diagonal in the fourth quadrant. The Fermat prime $n=2^{16}+1=65,537$ is located along the diagonal in the first quadrant at the (65,537-1)/8= 8192th turn of the spiral. It is not obvious apriori which of the odd integers found along the diagonals are prime without first applying some prime tests such as those of Fermat, Lucas, and Lehmer. However, what is clear is that all primes(except for n=2) must necessarily fall along one of the four diagonal lines shown. One can use canned programs to test whether a given odd number is prime or composite(non-prime)). Using MAPLE , we have , for example, that the input-

$N:=2^{20}$-3: isprime(N); evalf(N,7) produces the output true 1,048,573

Here are the values of n for which the numbers P1, P2, P3, and P4 are prime numbers with the given values-

First Quadrant P1(n)=8n+1 :

n={2,5,9,11,12,14,17.24,29,30,32,35,39,42,44,50…}with
P1(n)={17,41,73,89,97,113,137,193,233,241,257,281,313,337,353,401}
binary ending= …001

Second Quadrant P2(n)=8n+3 :

n={1,2,5,7,8,10,13,16,17,.20,22,26,28,31,35,38,41,43,47…
P2(n)={11,19,43,67,83,107,131,139,163,179,211,227,251,283,307,331,347,379}
binary ending= ...011

Third Quadrant P3=8n-3 :

n={1,2,4,5,7,8,13,14,19,20,22,23,25,29,34,35,37,40,44,47,49,50...}
P3(n)={5,13,29,37,53,61,101,109,149,157,173,181,197,229,269,277,293,317,349,3873,389,397}
binary ending= …101

Fourth Quadrant P4=8n-1 :

n={1,3,4,6,9,10,13,16,19,21,24,25,28,30,33,34,39,45,46,48…}
P4(n)={7,23,31,47,71,79,103,127,151,167,191,199,223,239,363,271,311,359,367,383}
binary ending= …111

Each of these four sequences in n appear to be infinite and hence that an infinite number of prime numbers exist. We also note that subsets of P1(n), P2(n), P3(n) and P4(n)can be generated by the polynomials $4k^2+20k+17$, $8k^2+11$, $4k^2+4k+5$, and $4k^2+4k+23$, respectively, for certain integer values k. These polynomials are obtained by evaluating the polynomial coefficients using the first three prime numbers in each group. Examples of such primes are -

$$4(21307009)^2+20(21307009)+17=1815954956244521$$

$$8(56789164)^2+11=25800073182551179$$

$$4(345678933)^2+4(345678933)+5=477975700262789693$$

and-

$$4(12345678985)^2 + 4(12345678985) + 23 = 609663158452065236863$$

As another special sub-class of primes one can consider the Mersenne and Fermat primes defined as-

Mersenne Primes $PM=2^n-1$: n={2,3,5,7,13,17,19,31,61,89,107,127,…}

Fermat Primes $PF=2^{(2^n)}+1$: n={0,1,2,3,4}

It is presently believed that the number of Mersenne Primes is infinite(so far some 46 have been found-(see http://en.wikipedia.org/wiki/Mersenne_prime) while those of Fermat consist of just five (although Fermat thought there were in infinite number while Euler proved later that $2^{32}+1$ was not). No Fermat primes corresponding to n=5 or higher have ever been found although several generalized Fermat numbers of the form $A^{(2^n)}+1$, where A is an even integer greater than 2 and n exceeding four, have been found to be prime (see http://en.wikipedia.org/wiki/Fermat_number).

What is clear from our above discussion is that these classical Mersenne and Fermat primes must lie along the diagonal in the 4th quadrant and the diagonal in the first quadrant, respectively. We have found no discussion in the literature concerning any subsets of primes of the form 2^n+3 and 2^n-3 lying along the diagonals in the second and third quadrant. Let us do this now. We consider the four sets of numbers-

$$S1=2^n+1, \quad S2=2^n+3, \quad S3=2^n-3, \text{ and } S4=2^n-1$$

Of these S4 are just the Mersenne numbers , S1 is a set somewhat larger but similar to the Fermat numbers, while S2 and S3 are a subset of the numbers falling along the diagonals in the second and third quadrant, respectively. Using our MAPLE program we find that the values of n for which S1, S2, S3, S4 are prime numbers are-

n={1,2,4,8,16} for S1,

n={1,2,3,4,6,7,12,15,16,18,28,30,55,…) for S2,

n={2,3,4,5,6,9,10,12,14,20,22,24,29,116,122,…} for S3 , and

n={2,3,5,7,13,17,19,31,61,…} for S4 .

Clearly the values of n for S4 just produces the Mersenne primes. Those for S1 correspond to the known Fermat primes. S2 and S3 for the specified values of n represent two infinite sets of new prime numbers. Examples of such primes are-

$2^{55}+3=36028797018963971$

and

$2^{122}-3=5316911983139663491615228241121378301$

A very interesting observation concerning S1 is that there are apparently no prime values for n>16 .This seems somewhat puzzling since the prime numbers S1 are a subset of the infinite number of primes generated by P1=8n+1. On searching, we have not been able to find any primes for S1 for all integer values of n between n=17 and n=3000. One is thus led to the conjecture that-

2^n+1 is a composite number for all positive integer values of n not equal to 1, 2, 4, 8, or16 .

Or even better, we can state that-

$2^{2n+1}+1$ is composite for all integers n=1, 2, 3,….∞

Thus the large number $2^{123456789}+1$ is composite although I am unable to come up with its factors. We have, however, tested $2^{(2n+1)}+1$ for primality through n=2048 and find none. In all these runs one observes that $2^{2n+1}+1$ is divisible by 3 . That is, the number $N(n)= (2^{2n+1}+1)/3$ is an integer and even becomes prime for n={1,2,3,5,6,8,9,11,15,21,30,39,50,63,83,95,99,156,173,350,854,…}.
One notes that N(n+1)= 4*N[n]-1 and that N(n) for even and odd n ends with the integers 1 and 3 , respectively. A necessary but not sufficient condition for the primality of N(n) is that the exponent 2n+1 is a prime number. Thus-

$N(63)= (2^{127} +1)/3=56713727820156410577229101238628035243$ is prime

but

$N(65)=(2^{131} +1)/3=2722258935367507707706996859454145691648$ is not.

while both 127 and 131 are prime numbers. These primes, referred to as Wagstaff primes, have the form N(n)=8*integer+3≡ integer(mod8)+3 and thus form a subgroup of S2. They all lie along the diagonal in the second quadrant. One also has that –

$$3N(n)=M(n)+2$$

where $M(n)=2^{(2n+1)}-1$ is a Mersenne number. Thus-

$$N(6)=2731=[M(6)+2]/3=[8291+2]/3$$

Notice that M(n) composite does not necessarily imply that N(n) is also composite. Thus $M(5)=2^{11}-1=2047$ is composite while $N(5)=(2^{11}+1)/3=683$ is prime and $M(11)= 2^{23}-1= 8388607$ is composite while $N(11)=(2^{23}+1)/3=2796203$ is prime. There also exist values of n for which both M(n) and N(n) are simultaneously prime. This occur at n=1,2,3,6,8,9,15,30,…For the case n=30, one has the primes-

N(30)=768614336404564651 and M(30)=2305843009213693951

One can test for primality of a number via Fermat's Little Theorem (see http://home.att.net/~numericana/answer/modular.htm#modulo)
In its simplest form, it reads-

$$p \text{ is prime if } \left[\frac{(2^{p-1}-1)}{p}\right] = Integer$$

And is valid for most primes. This quotient at first glance appears to be somewhat unwieldy for large p, but in actuality takes on relatively simple forms when expressed in modular arithmetic language. One can also replace the integer 2 with any other integer a. In mod terms the theorem reads-

$$a^p = a \pmod{p} \quad or \quad [a^{p-1}-1] \bmod p = 0$$

These forms can readily be programmed on a computer and form the basis for most primality tests. Using our MAPLE program, we find for p=683 and a=3 the following-

(3^682-1) mod 683; = 0

so that 683 must be a prime number.

The size of the numbers S1, S2, S3, and S4 for which they are prime increases rapidly with increasing values of n. For example,

$S2=2^{55}+3=36,028,797,018,963,971$

$S4=2^{61}-1=2,305,843,009,213,693,951$

Also one has the 94 digit prime

$[2^{2(156)+1}+1]/3=55624662393773700062370356931498752984445430269704499217370$
$8752037036386922041809901813043473$1

and the number $S1=2^{2501}+1$ which has 753 digits and is confirmed by my computer to be composite.

January 27, 2009