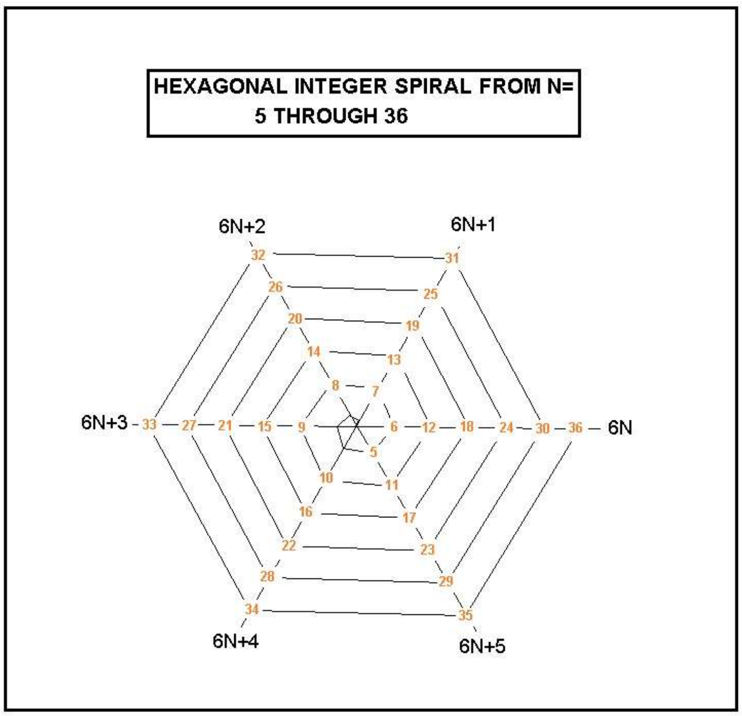
LOCATION OF PRIMES AND SEMI-PRIMES AT THE INTERSECTION OFF THE RADIAL LINES 6N±1 AND THE VERTEXES OF A HEXAGONAL INTEGER SPIRAL

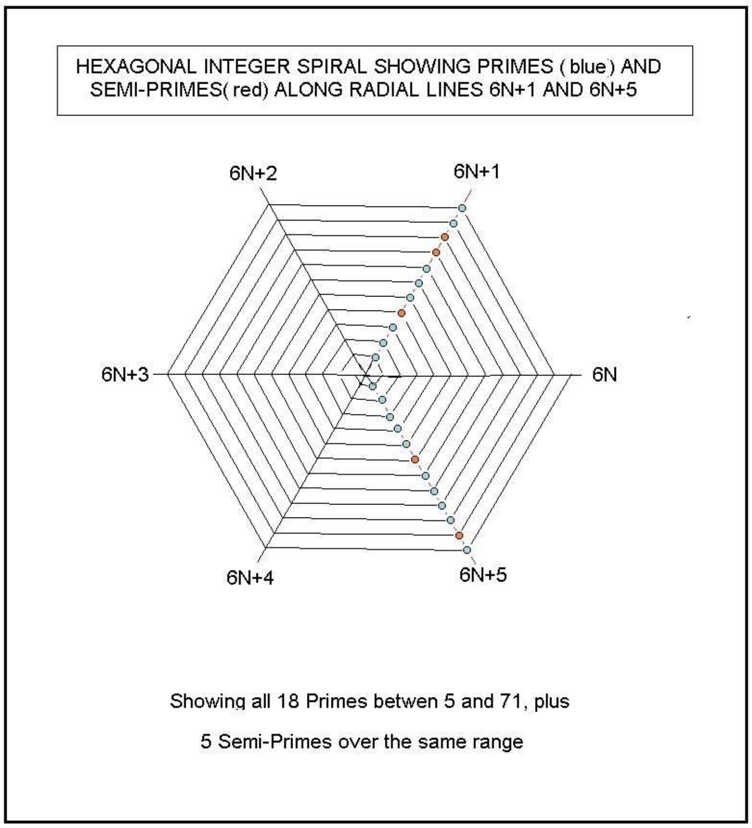
About a decade ago we first showed that the standard Ulam Spiral , in which primes appear in a semi-random manor, can be converted into a much simpler form in which all prime numbers five and above fall along just two radial lines 6N±1 intersecting the vertexes of a hexagonal integer spiral (see-https://www2.mae.ufl.edu/~uhk/MORPHING-ULAM.pdf). We wish in this note to extend this discussion to also include semi-primes N=pq , where p and q are prime numbers. Such semi-primes , when N gets large, play an important role in public key cryptography

To locate all primes and semi-primes, we begin with the hexagonal integer spiral shown-



It extends from N=5 through N=36 with integers located at the vertexes [r,θ]=[N,πN/3] through which six radial lines pass. The hexagonal spiral is made complete by connecting straight lines between neighboring vertex points. By looking carefully at the last graph, one notes that the only radial lines along which prime numbers exist are 6N+1 and 6N-1 (equivalent to one turn of 6N+5). That is

all primes five or greater must satisfy the condition that N mod(6)=1 or N mod(6)=5. This is equivalent to saying that primes five or greater lie along the radial lines 6N±1. We first came up with this observation several years ago while studying the behavior of the newly defined <u>number fraction</u> f(N)=[σ(N)-N-1]/N and noting that f=0 whenever N equals a prime. Here σ(N) is the sigma function of number theory equal to the sum of all divisors of N and also equal to Nf(N)+N+1. If we mark all primes between 5 and 71 by blue circles, we get the following-



As already mentioned, all primes in the lasts hexagonal spiral graph lie along 6N+1 or 6N+5 . A few points along these two radial lines are not primes but rather semi-primesN=pq or higher. For the given range 5<N<72 the red circles correspond to all semi-primes. Note that there are <u>no semi-primes other than those lying along 6N+1 and 6N+5</u> .That is, we have that for both primes and semi-primes that N mod(6)=1 or 5. This observation ceases to hold for triple primes and higher. The simplest way to test whether a Number is a prime or a composite is to note the value of f(N). Take for example the Fermat Number-

$$N=2^{32}+1=4294967297$$

It yields N mod(6)=5 and so could possibly be a prime lying along 6N+5. However, a f(N) evaluation yields f=σ(N)-N-1]/N=0.001560211647. So it is not a prime number as Leonard Euler

first showed via some elaborate but unnecessary efforts several hundred years ago. My PC yields ithprime(N)= (641)*(6700417), so that N is a Semi-Prime..

To prove that all Semi-Primes must also lie along the two radial lines 6N±1 , we can set any semi-prime as

N= pq=(6n+1)(6m+1) , (6n+1)(6m-1), or (6n-1)(6n-m)

In each of the tree cases we find N=pq=6(integer)±1, so that the Semi-Prime N=pq will also lie along the radial lines 6n+1 or 6n+5, without exception. Note such a restriction will cease to hold for triple primes N=pqr or higher. The first triple prime lying along the 6N+1 radial line is N=5x7x11=385. The first triple-prime along the 6N+5 radial line is N=5x7x13=455.

Two of the semi-primes (35 and 55) shown in red in the above Hex Graph, factor as follows. At N=35=5x7, we have f=[sigma(35)-35-1/35=48-35-1]/N=12/35. So Nf(N)=12=p+q with pq=35. So solving, we get p=5 and q=7. Next take N=55=p+q, where f=sigma[55]-56]/55=(72-56)/55=16/55. So p+q=55(16/55)=16. Solving, we find [p,q]=[5,11].

For larger semi-primes N=pq, we first check whether N has the form 6n+1 or 6m+5.

Then we proceed to find S=Nf(N)/2=[σ(N)-N-1]/2. This is easy to evaluate with one's PC as long as N is less than about 20 digits length. Next having found S, the prime components of N=p become-

$$[p,q]=S\mp\sqrt{S^2-N}$$

This formula should work for all semi-primes provided sigma(N) and hence S can be deduced. Let us demonstrate things for the 15 digit long number-

N=164281698339637

Here N mod(6)=1 and sigma(N)= 164281764713760. So S=[sigma(N)-N-1]/2=33187061.

This leaves us with –

[p,q]= 33187061∓30612078=[2574983, 63799139]

From this last example, it has become clear that one can factor any Semi-Prime provided sigma(N) can be found. It suggests that people in cryptography involved with the factoring of Semi-Primes in the 100 digit length concentrate on finding improved methods to more quickly determine σ(N) for N above 40 digit length. I have been trying to get our computer specialists here on campus to see how large an σ(N) they can generate using their latest supercomputer. So far no luck but I remain optimistic.

U.H.Kurzweg
January 2, 2022
Gainesville.Florida