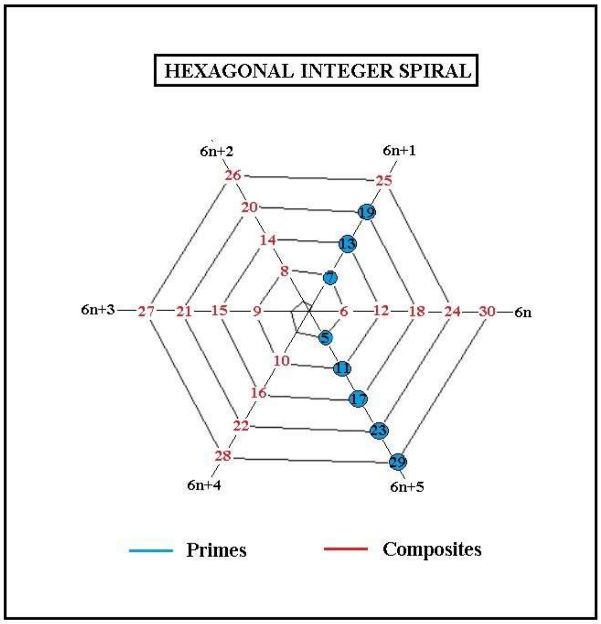
THE HEXAGONAL INTEGER SPIRAL AND SEMI-PRIMES

Over the last decade or so we have been examining prime numbers and composites in detail. In the process we have come up with several new functions including the number fraction f(N)=[sigma(N)-N-1]/N, a formula for factoring semi-primes N=pq, and most importantly the hexagonal integer spiral which clearly distinguishes primes from composites. The last allows one to represent all positive integers as points at the intersection of two radial lines 6n+1 and 6n-1 and the vertexes of the straight line edges of the hexagonal integral spiral z=x+iy=exp(inπ/3).Here is a graph of this integer spiral-



We note that the spiral unwraps in a counter-clockwise sense with the integers appearing in sequence. All composite numbers are shown in red with all primes greater than three shown as blue circles. The important new result, apparently not found previously by those individuals studying the related Ulam Spiral, is that –

All primes greater than three must have the form 6n+1 or 6n-1 without exception

This is a necessary but not sufficient condition for N to be a prime as noted, for example, by N= 6(4)+1= 25, which is clearly composite. We note that each turn of the spiral equals an increase of six units. This means that we have a mod(6) situation allowing us to write-

N mod(6)=6n+1   or   N mod(6)=6n-1 (equivalent to 6n+5)

To see along which radial line a number N lies one needs to simply carry out the operation N mod(6). Consider the special case of the twenty-four digit long number-

N=105462258160149569920441 where N mod(6)=1

Here we have N lying along the radial line 6n+1. So it might be a prime. However an analysis shows it to be a composite. It factors as-

N=pq= 190898885521 x 552450884521

Note here that both p and q are primes as can be verified by the computer operations isprime(p)=true and isprime(q)=true. All gaps found along the lines 6n±1 are filled with products of two or more primes.

There are many other observations one can make about the above integer spiral. We see, for instance, that twin primes (those which differ from each other by two units) must have the form q=6n+1and p=6n-1 so that the mean value of the twin primes must equal 6n, n=1,2,3,5,7,.. .Here is a short table of the first ten of these-

N	6n	p=6n-1	q=6n+1
1	6	5	7
2	12	11	13
3	18	17	19
5	30	29	31
7	42	41	43
10	60	59	61
12	72	71	73
17	102	101	103
18	108	107	109
23	138	137	139

The computer program which generates these twin primes is-

```
for n from 1 to 24 do {n,6*n,6*n-1,isprime(6*n-1),6*n+1,isprime(6*n+1)]od;
```

By extending the range of n, one can generate the nearest twin prime to n=1000. It produces p=6089 and q=6091 at n=1015.

Let us next consider the semi-prime-

N=6089 x 6091=37088099

.A mod(6) operation produces N mod(6)= 5 , 6089 mod(6)=5, and 6091 mod(6)=1

Collecting the mod values then says-

$$N=pq \quad \rightarrow \quad -1=-1 \times 1$$

since 5 and -1are interchangeable in mod(6) language. Such a balance continuous to hold for all semi-primes. So if we take –

N=379489597027 which yields N mod(6)=1

we expect that p mod(6) and q mod(6) will have the same mod form of either 1,1 or 5,5. This last semi-prime factors asp= 279353 which has a mod(6)=5 and q=1358459 which also has mod(6) of 5.

Consider next factoring the semi-prime-

N=88091 which has N mod(6)=5=-1

This suggests p=6n-1 and q=6m+1. Multiplying things out produces-

$$(6n-1)(6m+1)=N$$

On expanding we have-

$$6nm+(n-m)=(N+1)/6=14682$$

Now we note that 6nm>>(m-n), so nm lies near 14682/6=2447. Letting U=nm and V=n-m, we get the equation-

$$6U+V=14682$$

To solve this Diophantine equation we let-

$$U=nm=2447+\varepsilon \text{ and } V=n-m=-6\varepsilon$$

Eliminating m we get a quadratic in n which reads-

$$n^2+6\varepsilon n-(2447+\varepsilon)=0$$

Solving, we have-

$$n=-3\varepsilon+\sqrt{9\varepsilon^2+\varepsilon+2447}$$

Since the n must be a positive integer , this means the radical must also be.This can only happen if ε=14 for which the radical is 65. So we find m=107 and n=23.This means-

$$p=6(23)-1=137 \qquad \text{and} \qquad q=6(107)+1=643$$

This last procedure for factoring semi-primes works for all N provided the primes p and q are greater than three. It does however involve an ever increasing number of trials for ε before an integer value for the radical appearing in the n or m solutions.

A way I have found for getting around this situation is to note that-

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

, where S is a new point function S=(p+q)/2=[σ(N)-N-1]/2 representing the mean of p and q. Here σ(N) is the sigma function of number theory representing the sum of all divisors of semi-prime N=pq. One is fortunate that most advanced mathematics programs have sigma built into its library out to at least twenty places. Thus one needs only find the value of σ(N) and hence S to factor any semi-prime. For the above case N=88091 yields σ(N)=88872 and S=390. So we find-

$$[p,q]=390\mp\sqrt{390\text{^}2-88091}=[137,643]$$

This result was obtained in a split second and suggests that future attempts to break large public keys in cryptography should concentrate on obtaining values of σ(N) for semi-primes of 100 or larger digit lengths.

U.H.Kurzweg
July 16, 2020
Gainesville, Florida.