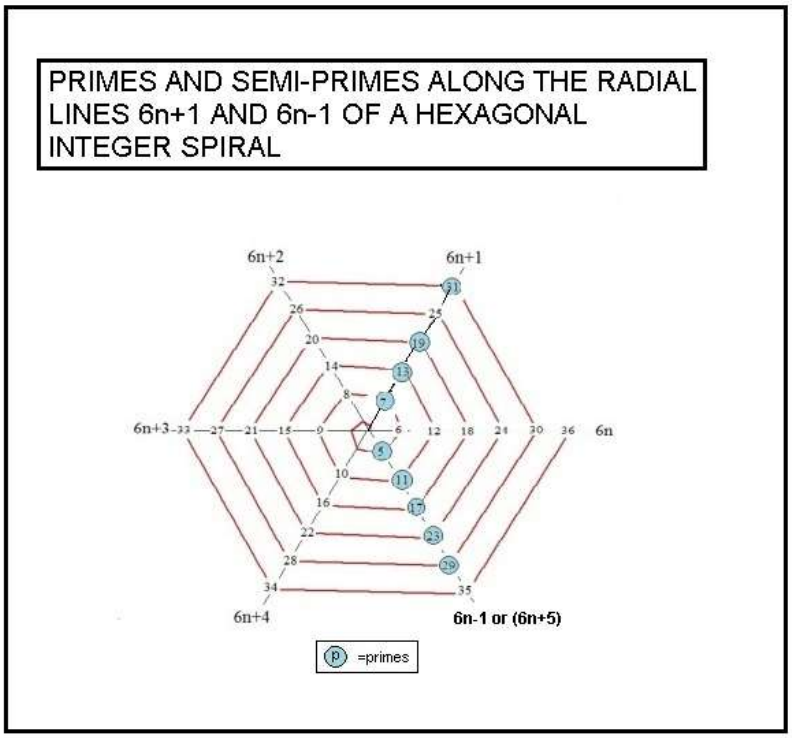
**SOME UNCONVENTIONAL METHODS FOR FACTORING LARGE SEMI-PRIMES**

**INTRODUCTION:**

During the last decade we have spent considerable time finding some new unconventional approaches for factoring large semi-primes N=pq, where p and q are prime numbers. As already shown in several earlier articles on this web page, we know that p, q, and N must have the form $6n \pm 1$, provided n is an integer one or greater. Thus the semi-prime N=6(13)-1=77 has p=6(1)+1=7 and q=6(2)-1=11. A convenient way to plot such numbers is via a hexagonal integer spiral, discovered by us about ten years ago. The graph looks as follows-




You will notice that all primes five or greater fall strictly along the lines $6n \pm 1$ and differ from each other along a given radial line by factors of six. You will notice that some non-prime (composite) numbers such as 25 and 35 also exist along these two radial lines. It has taken a few years for others in the mathematical community to recognize the beauty of this form of prime and semi-prime representation. As an example, the graph shows at once why all twin primes

must have a mean value of 6n. It also shows why it is impossible to have three primes in a row differing from each other by a factor of two units each.

With the above graph in mind, it is now possible to derive some formulas which factor any semi-prime N=pq. One of these non-conventional approaches uses the sigma function of number theory while the second involves using the closest integer value to the square root of N.

**USE OF THE SIGMA FUNCTION:**

Here we begin with the sigma function definition for semi-primes-

σ(N)=1+p+q+N

Combining this with the semi-prime definition N=pq, we find the quadratic formula-

x^2-[σ(N)-N-1]x+n=0 with x=[p,q]

Solving, we have-

[p,q]=[σ(N)-N-1]/2$\mp sqrt\{[\sigma(N)-N-1]^2/4-N\}$

Thus, if we know the sigma function of N, the semi-prime can be factored. Look, for example, at N=77 where σ(N)=96. Here –

[p,q]=(96-78)/2+sqrt{[96-78]^2/4-77}=9$\mp 2 = [7,11]$

This form of factoring is quite elementary compared to elliptic curve methods or grid techniques, but gets the answer much more rapidly. The present limitation to this sigma function approach is that one's PC, using MAPLE or Mathematica, is able to furnish values for sigma(N) up to only about forty digit length. For any semi-primes below this value the present approach is to be favored over other known techniques.

As a second example, consider the semi-prime N=455839. Here my PC yields σ(N)=457200 in a split second. This produces-

[p,q]=(457200-455840)/2$\mp sqrt(680^2-455839)$=[599,761]

This semi-prime is used in the literature to demonstrate Lenstra's Elliptic Curve factoring method. Unlike the very simple result given here, his technique takes

minutes of computer effort and additional calculations to arrive at the same result.

As a third semi-prime we take one which is 40 digits long and lies near the limit of our PCs capability. It reads-

N=6877519904317175519940418227241938352 97

Here our Lenovo thinkpad, using the math program Maple, produces-

σ(N):= 687751990431717552047876571921844708116

in a little less than one minute. Plugging these numbers into the above [p,q] program produces in a split second the result-

p:= 20851645882358199637 and q:= 32983103315292673181

I should point out that the semi-prime N was originally created from p and q using the irrational number quotients –

F=exp(3)*ln(23)/Pi^7 +96 and G=ln(5)*exp(2)*sqrt(13)/13 +8

As we have already shown in earlier notes, this prime number generation procedure has certain advantages over random number generation especially in storage. This sigma function approach to factoring holds for all semi-primes for which one's PC yields values for σ(N) in short time and hence typically for N of forty digit or less length. To go beyond this will require generating sigma for values beyond these. Additional work needs to be done in order to accomplish this.

**FACTORING METHOD BASED ON THE ROOT OF N:**

An alternate non-conventional way to factor large Ns is to note that when p=q these primes each equal sqrt(N). This suggests that one take ( A+n) as the mean value for p and q, where A is the nearest integer value to sqrt(N). That is-

(p+q)/2=(A+n)

, where n is a to be found integer. Combining this last result with N=pq produces the result-

x^2-2x(A+n)+N=0 where x=[p,q]

On solving this quadratic, we find

$$[p,q]=(A+n)\mp\text{sqrt}[(A+n)^2-N]$$

To get an explicit result one now needs to vary n until the square root becomes an integer.

Let us demonstrate for the semi-prime N=31877, where sqrt(N)=178.5413, so that A=179. Running the program-

for n from 0 to 20 do({n,solve(x^2-2x(179+n)+31877=0,x)}od;

results in-

n=10, p=127, and q=251

So it took ten trials until n=10 was reached. Although this procedure, involving root of N, works for any N the search can become rather time consuming when N gets very large.

Comparing the [p,q] values given for the sigma N and root N factored results, tells us that

$$\sigma(N)=2(A+n)+N+1$$

Thus for N=77 we have σ(N)=96 so that n=0. For N=455889 we have σ(N)= 457200 so that n=5. Therefore it takes 0 and 5 trials using the sqrt(N) method to factor N=77 and N=455889, respectively.

**6n$\pm$ 1 FORMS FOR p, q, AND N:**

We have mentioned earlier in this article that p, q, and N Have certain unique forms of 6n$\pm$1 .These forms follow prior to factoring by use of the mod(6) operator. Let us demonstrate things for the semi-prime N= 31877. Here N mod(6)=5 meaning N has the form 31877=6(5313)-1. This means N lies along the radial line 6n-1 at the 5313 turn of the hexagonal integer spiral. To balance things, this must mean that p=6s+1 and q=6t-1, with s and t being to be found integers. It means we must have-

$$(6s+1)(6t-1)=6(5313)-1$$

From this follows-

$$6st+(t-s)=5313$$

Also we have –

$$\sigma(N)=32256=1+31877+6(s+t)$$

So that –

$$378=6(s+t)$$

Combining, we find s= 21 and t= 42 . This leaves us with the factored result-

$$31877=[6(21)+1][6(42)-1] =127*251.$$

**CONCLUSIONS:**

We have shown two un-conventional methods for factoring large semi-primes N=pq. The first of these is based on the use of the sigma function σ(N) and works quickly for N up to about forty digit length. The second approach employees the root of N and works for all N. It does however become rather lengthy if dealing with very large semi-primes such as encountered in cyber-security. Our suggestion is that one work on methods to find the sigma function for Ns of the one-hundred digit length and larger. If a method can be found to do this, present day cyber-security will become obsolete.

U.H.Kurzweg
April 17, 2023
Gainesville, Florida