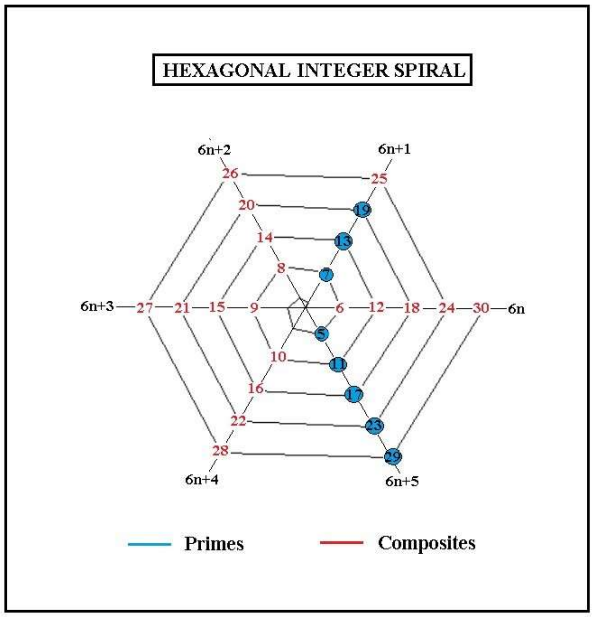
FACTORING OF LARGE SEMI-PRIMES USING SIMPLE DIOPHANTINE EQUATIONS

We have shown in several earlier notes on this web page that all primes p and q plus semi-primes N=pq have the form 6(r)$\pm$1provided primes p and q are five or greater. Geometrically it means such numbers sit at the vertexes of a hexagonal integer spiral at the points where the radial lines 6n+1 and 6n-1 cross these vertexes. Here is a picture representing such primes and semi-primes-



The blue circles represent primes five or greater while the number 25 along the radial line 6n+1 is a semi-prime N=5 x 5. One identifies primes and semi-primes along these two radial lines 6n+1 and 6n-1 as N(mod(6)=1 and N(6n-1=5, respectively.

Consider first the factoring of one of the semi-primes N=pq=6r+1 or N=pq=6r-1. To keep things simple we begin with the semi-prime-

$$N=253=6(42)+1 \text{ with } N(\text{mod}6)=1$$

We see from this form that 253 lies along the 6n+1 radial line meaning we have-

$$p=6n+1 \text{ with } q=6m+1 \quad \text{or} \quad p=6n-1 \text{ with } q=6m-1$$

Trying the first of the two possible combinations we write-

$$(6n+1)(6m+1)=6(42)+1$$

Rewriting things, we arrive at the relatively simple non-linear Diophantine equation-

$$n = \frac{42-m}{6m+1}$$

We note here that 42>m and 6m>1. This implies that a reasonable value for the integer product nm=42/6=7. It means we should look for an m of three or less. Making a table we find-

m=1	m=2	m=3
n=41/7	n=40/13	n=39/19

None of these produce an integer n, hence the above second form for the pq product must be used. This form produces a second Diopantine equation-

$$n=\frac{42+m}{6m-1}$$

This produces the table-

m=1	m=2	m=3
n=43/5	n=4	n=39/17

Thus we have the integer solution [n,m]=[4,2]. Note here that r/6=42/6=7 lies close to nm=4 x 2=8.The final prime factors thus are-

p=6(4)-1=23 and q=6(2)-1=11

As a second semi-prime we choose –

N=551=6(92)-1 with N(mod6)=5

This means we should try p=6n-1 and q=6m+1 or alternatively p=6n+1 and q=6m-1.

Using he first combination, we find-

$$n=\frac{92+m}{6m+1}$$

and the approximate value nm=92/6. This implies an m search range of 0<m<sqrt(92/6)=3.92. Running a search we find one integer solution at m=3 yielding-

[n,m]=[5,3]

That is , we have the prime factors-

p=6(5)-1=29 and q=6(3)+1=19

Note that this time the first combination worked so that there was no need to use the second combination.

You will note that for these Diophantine equations there are only two possible integer values for m. The first is the non-interesting solution n=r as m goes to zero. It is the second integer solution which one seeks. The fact that nm~r/6 for these type of Diophantine equations is very helpful in establishing the range of m inside of which an integer solution for n may be found.

To factorize N we need to solve the following Diophantine equations-

If N=pq=6r+1 we have n=(r+m)/(6m-1) or n=(r-m)/(6m+1)

If N=pq=6r-1 we have n=(r-m)/(6m-1) or n=(r+m)/(6m+1)

By the nature of these Diophantine equations we always have the good approximation $r/6 \approx nm$ for the integer solution of interest.

Let us finish our discussion with the semi-prime-

N=455839=6(75973)+1

This number. where r=75973, is often used in verifying the Lenstra elliptic factorization approach. Its factorization by the present Diophantine equation method involves solving-

n=(r+m)/(6m-1) or n=(r-m)/(6m+1)

in the range 1<m<sqrt(r/6)=112.5. Applying our search progam-

```
for m from 1 to 112 do ({m,evalf((75973+m)/(6*m-1))})od;
```

to the first of these Diophantine equation yields [n,m]=[127,100] . Hence we have the factors-

p=6(127)-1 =761 and q=6(100)-1=599

As you can see, this result was obtained much faster than use of the elliptic curve factorization method.

U.H.Kurzweg
July 12, 2020
Gainesville, Florida