A NEW WAY TO FACTOR LARGE SEMI-PRIMES

INTRODUCTION:

We recently found a new way to factor semi-primes N=pq into their prime components p and q by use of the new variables –

$$x=[(p+q)/2]-R \qquad \text{and} \qquad 2y=q-p.$$

Here R is the nearest integer above sqrt(N), p+q)/2 is the mean value of the prime components, and q-p the difference between the two primes. Upon combining N, x, and y, these produce the single Diophantine equation-

$$(x+R)^2-y^2=N$$

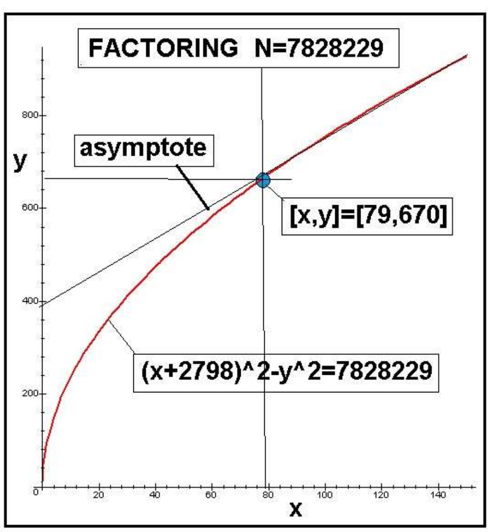
which has the shape of a shifted hyperbola containing just one integer solution [x,y]. It is the purpose of the present note to show how [x,y] is obtained and hence obtain a unique Quad Q=[N,R,y,x] for N.

FACTORING OF N=7828229

We apply our present solution technique to the seven digit long semi-prime N=7828229, where R=2798. It satisfies the Diophantine equation-

$$(x+2798)^2-y^2=7828229$$

which has the shape of a hyperbola when all points and not just integers are considered. Here is its plot-



The blue circle is where the desired integer pair solution is found. Typically it can be expected a little below were the hyperbola merges with its asymptote. To find [x,y] we use the one line computer program-

```
for Δ from b to c do({Δ,sqrt(-N+(R+x)^2)})od;
```

For the number considered here we choose b=75 from the graph and run things through c=80. The integer result we find is [x,y]=[79,670]. It means it took just four trials to obtain the quad Q=[7828229,2798,670,79]. The values of p and q become-

p=(R+x)-y=(2798+79)-670=2207 and q=(R+x)+y=2798+79)+670=3547

FACTORING OF SOME ADDITIONAL SEMI-PRIMES:

Consider factoring two other semi-primes. Taking N=169331977 with R=1303. The corresponding hyperbola suggests we start our trials with b= 1600 and run to c=1650. It produces Q=[169331977,13013,6732,1638] and the prime components p=7919 and q=21383. As a second new semi-prime take N=3330853711 with R=57714. A hyperbola plot suggests that here b=1200 and we go up to c=1400. This produces the integer solutions [x,y]=[1366,12633] and a quad of Q=[3330853711,57714,12633,1366]. From it we find, with little extra effort, that –

p=46447 and q=71713

, whose product equals N.

CONCLUDING REMAKS:

We have shown that one can factor any semi-prime by first finding R corresponding to N and then make an implicitplot of x versus y. Using this graph as a starting search point near the beginning of the asymptotic part to give an estimate for b, we proceed with a search until [x,y] is found. Having this we write down the Quad and from it write out the prime components p and q. The number of calculations will increase with increasing N but with the right choice of b the required calculations will remain reasonable.

U.H.Kurzweg
May 21, 2023
Gainesville, Florida