A NEW APPROACH FOR THE FACTORING OF LARGE SEMI-PRIMES

INTRODUCTION:

One of the incompletely solved problems in number theory is the rapid factoring of large semi-primes N=pq into their prime components p and q. The most common way to produce such factoring is the general number field grid. It works but becomes impractical when attempting to factor semi-primes of 100 digit length or larger such as occur in public key cryptography. Over the last decade or so I have been involved in developing an alternate factoring method for any large semi-prime N=pq. Our procedure starts with the obvious identity-

$$[p,q]= (p+q)/2 \pm (q-p)/2 \quad , \text{with } q>p$$

Letting S=(p+q)/2 be the mean value and R=sqrt(S^2-N) the half difference, we get the starting identity-

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

This result tells us that if we know the value of S the problem solved. Furthermore S can be expressed in several other ways such as-

$$S=[\sigma(N)-N-1]/2=Nf(N)/2$$

Here σ(N) is the sigma function given in most advanced mathematics programs to at least Ns of twenty digit length and the f(N) is our own number fraction parameter defined as (p+q)/N for semi-primes.

Using the above formulas, we have at once that N=455839 yields σ=457200 so that S=680. This means-

$$[p,q]=680\mp\text{sqrt}(680^2-455839)=[599,761]$$

We point out that this particular semi-prime is used in the literature to support the Lenstra Elliptic Curve Method for semi-prime factoring. The present factoring approach is much faster.

When N gets much larger than about 40 digit length my math program (MAPLE) takes too long to find the sigma function value. In that case one must return to evaluating S directly by going back to the original equation for [p,q] given above. Here is the procedure-

FINDING S=(p+q)/2:

We begin by noting that –

$$p=\alpha\ \text{sqrt}(N) \qquad \text{and} \qquad q=(1/\alpha)\text{sqrt}(N)$$

, with the unknown α lying in the range 0<α<1. This implies that-

$$S=[(1+\alpha^2)/(2\alpha)]\ \text{sqrt}(N)$$

When p and q are equal to each other, S is given by the nearest integer to sqrt(N). Since α is an unknown beforehand, one makes the substitution-

$$[p,q]=(S_0+\varepsilon)\mp\text{sqrt}[(S_0^2-N)+2S_0\varepsilon+\varepsilon^2]$$

, where S_0 =[(1+α^2)/(2α)]sqrt(N) to the nearest integer. Here ε is a positive or negative integer which vanishes only when the correct value of α is used.

Let is demonstrate the procedure. Consider the seven digit semi-prime-

N=4416941 with the root of N being sqrt(N)=2101.651962

Next choose α=0.7. This yields S_0=(1.49/1.4)sqrt(N)=2237 to the nearest integer. Next search

R until an integer value is found. The search program reads-

for ε from -80 to 80 do {ε,sqrt[(S_0^2-N)+4474ε+ε^2]}od

Solving, we get ε=58 and R=922. That is, S=S_0+58=2295. So we have the factorization-

[p.q]=2295$\mp$sqrt(2295^2-N)=2295$\mp$922=[1373,3217]

LOCATING THE VALUE OF ALPHA FOR WHICH EPSILON VANISHES:

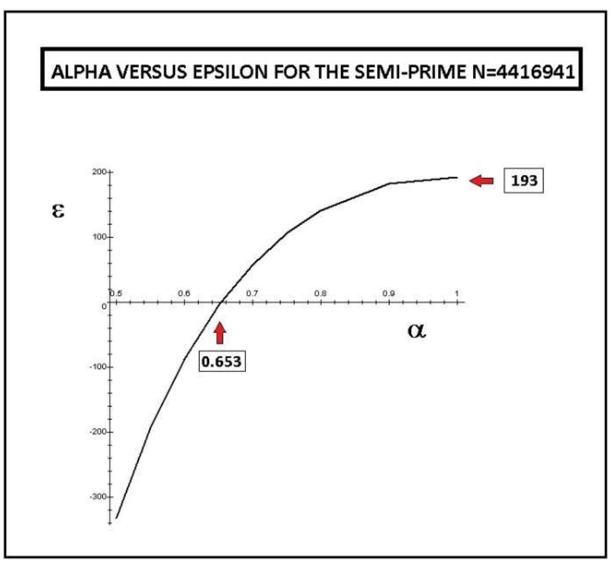
Once R has been found for one value of α, the value of α for which ε vanishes can be gotten by noting that R=922 remains unchanged for any other α in 0<α<1. So we have-

(922)^2=S_0^2-N

A little manipulation allows us to re-write this as a quadratic in α –

α^2+[2(922)/sqrt(N)]α-1=0

Solving, produces the result α=0.6533329 for which ε vanishes. The following gives a graph of α versus ε for N=4416941-



The critical value is found at [α,ε]=[0.653,0]. Such a cross-over point will also be found for other Ns but located at different points along the α axis. The amount of searching will be greatly reduced if one is lucky enough to start with an α near the critical value.

SPEEDING UP THE SEARCH:

One way to decrease the number of searches for integer value R is to carry out brief limited searches for different values of α over a restricted range of –b<ε<+b. Most of these shorter searches will yield no integer values. However some lying near the critical value of α for a given N will register an integer solution. If one of these is found , the problem has essentially been solved. Let us demonstrate this search approach for the semi-prime-

N=53891777 where sqrt(N)=7341.10189

Starting a restricted search in the strip o<ε< 30 with α=0.9 we get no solution. Next using α=0.8, we find a solution at ε=26 yielding R=1768. This produces an S=7525+26=7551 and the factoring-

[p,q]=7551∓ sqrt(7551^2 -53891777)=7551∓ 1768=[5783,9319]

The critical value is here determined by-

α^2+[2R/sqrt(N)]α-1=0

Solving for α yields α=0.7877. Note that we only needed to use positive ε in the search since α=0.8 lies close to α=1 were ε is positive. Negative ε will be found if α<0.7877.

CONCLUDING REMARKS:

We have shown that large semi-primes N=pq can be factored by a method based on the value of S=(p+q)/2=(σ-N-1)/2=(1+α^2)/(2α)sqrt(N). On modifying the S to S+ε, we vary ε until an integer value of the radical R=sqrt((S+ε)^2-N) is found. By evaluating R over only smaller values of ε (at fixed α) the evaluation process is greatly speeded up. Several specific evaluations for Ns as high as eight digit length are factored.

U.H.Kurzweg
April 20, 2021
Gainesville, Florida