FACTORING OF N=pq USING k

In several earlier notes we have found that a semi-prime N=pq ,with primes p<q, can be factored into the forms p=6n±1 and q=6m±1, where n and m are integers whose values depend on finding integer solutions of –

$$R[k]=\sqrt{(H+6k)^2-4(B-k)} \quad when \quad N \bmod(6)=1$$
$$or$$
$$S[k]=\sqrt{(H+6k)^2+4(B-k)} \quad when \quad N \bmod(6)=5$$

Here A=(N-1)/6 for the first case and A=(N+1)/6 for the second case. Also H=A mod(6) and B=(A-H)/6. For smaller and intermediate sized Ns the above radicals are easy to solve to produce integer values. However, when N is large it becomes difficult to find the right value of variable k which allows this. The values of n and m are given as-

$$[n,m]=\frac{1}{2}[(H+6k)\pm R] \quad or \quad [n.-m]=\frac{1}{2}[(H+6k)\pm S]$$

For a typical semi-prime the quantities B and H will be known, so one needs to only find the value of k which makes the radical an integer. Although B is typically much smaller than k, k can nevertheless become large so that a brute force evaluation of one or the other of the radicals can become extremely time consuming.

We show here how to get around this difficulty by estimating a value for k designated by k1. The procedure works as follows. It is known that –

p= 6n±1=αsqrt(N) and q=6m±1=(1/α)sqrt(N) with o<α<1

Thus for large N, we can say that-

n≈αsqrt(N)/6 , m≈(1/α)sqrt(N)/6, and $p/q\approx\alpha^2$

The range for α is 0<α<1 with α=1 meaning that n=m and p=q.

Now we can get an estimate for the desired value of k by eliminating n from its two definitions. For the case of N mod(6)=1, we get-

$$\frac{\alpha\sqrt{N}}{6}=\left(\frac{1}{2}\right)\{(H+6k)-R\}$$

and for N mod(6)=5, we have-

$$\frac{\alpha\sqrt{N}}{6} = \left(\frac{1}{2}\right)\{(H+6k)-S\}$$

Solving for k in these last two expressions, we have, after noting H<<6k and 1<<αsqrt(N), that -

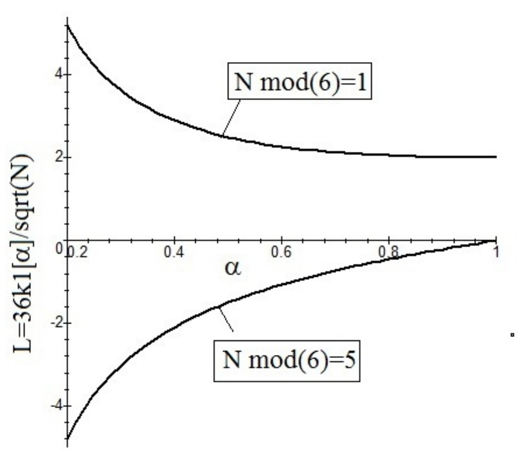
$$k1[\alpha] =\approx \frac{\alpha\sqrt{N}}{36}\left\{1+\frac{1}{\alpha^2}\right\} \quad for \quad N \bmod(6)=1$$

and

$$k1[\alpha] \approx \frac{\alpha\sqrt{N}}{36}\left\{1-\frac{1}{\alpha^2}\right\} \quad for \quad N \bmod(6)=5$$

These values can now be used to search for the k which should lie close to k1 and which makes the radical an integer. The values for k1 depend not only on the root of N but also on α. Typically large semi-primes will require large k1s and the size of |k1| will increase with decreasing α. The following graph characterizes this behavior-

NON-DIMENSIONAL K1 VERSUS ALPHA



In the graph we have run the non-dimensional quantity L=36k1[α]/sqrt(N) over the range 0.2<α< for both types of semi-primes. The increase in L with decreasing α is at first small but then increases rapidly for values of α in the given range. Typically we have L≈2 for Nmod(6)=1 and L≈ -1 for N mod(6)=5 provided α lies between 0.5 and 1. We also find the unique value of L=2 occuring for those semi=primes N where p=q.

Let us next demonstrate the above points by working out a few explicit factorizations of larger semi-primes. Take first –

N=155505643 where sqrt(N)=12470.19, N mod(6)=1,A=(N-1)/6-25917607,H=A mod(6)=1, and B=(A-H)/6=4319601.
We assume first that α=1, so that we have the k1[1] estimate -

$$k1[1] = \sqrt{N}/18 = 692.79$$

If α<1, then k1[α] increases to a value of sqrt(N)/36}{α+1/α}.

Now carrying out the following computer search-

for k from 693 to 723 do {k,sqrt((1+6*k)^2-4*(4319601-k))}od

yields R=1017 at k=713. So we have our solution –

[n, m]=(1/2)(1+6(713)±1017)=[1631, 2648]

which means that-

155505643={6(1631)+1}{6(2648)+1}=9787 x 15889

As a side benefit, we now know the value of α. It equals α=sqrt(p/q)=0.7848.
If we had used this value of α instead of α=1 then k1[0.7848]=713.22 and so essentially matches the solution of k= 713. The advantage of using k1[1] in our calculations is that we know for the N mod(6)=1 case that it offers a lower bound on the actual k1[α] considerably larger than k=0.

Another interesting point following from the N mod(6)=1 case is that k1[1]=sqrt(N)/18 for all positive integer semi=primes including the one hundred digit long Ns used in public key cryptography. So for a semi-prime of 100 digit length the k to be used in an integer search for R must be some 48 digit long or longer k1[1].

Consider next an N where N mod(6)=5. Such an example is-

N=3475379339=(6n-1)(6m+1) where N mod(6)=5 and sqrt(N)=58952.348.

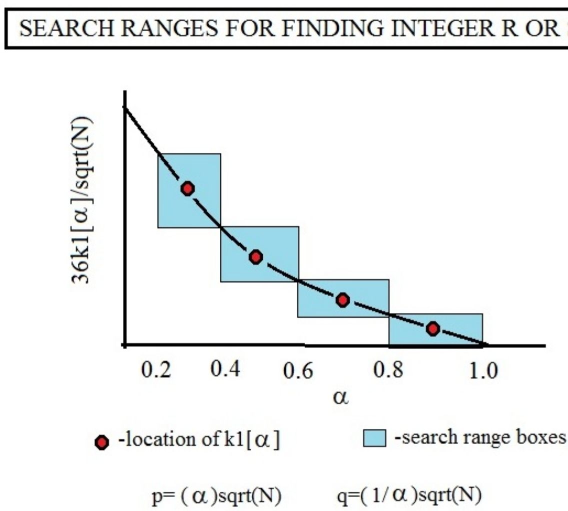
Here A=(N+1)/6=579229890, H=0 and B=(A+h)/6=96538315. Although the k1[1] case is here equal to zero, one can use the neighboring value corresponding to α=0.8. This yields the search starting point of k1[0.8]=-736.90. Carrying out a search with this last value leads to an integer S=20314 at k=-858. Thatvis it took 122 operations to find an integer answer.the rest of the problem is now easy. We have-

[n,-m]=(1/2){(-6(858)±20314}=[7583,12731]

From this result follows the factorization-

3475379339=45497 x 76387

In both of the above case the factoring of nine and ten digit long semi-primes was fairly easy to accomplish compared to other existing methods such a elliptic curve factorization and generalized grid methods. It is very likely that even larger semi-primes can be factored by the present approach. To prevent rapid factorization will require that N have values of α lying in a range 0<α<0.1. There it becomes difficult to find a k1 close to k since α is not known before hand. The most consistent approach to factoring by the present method is to determine several different k1[α] values for a given N and then search within a limited range for integer solutions of R or S for a given k1[α]. If no solution appears after a 10% search range proceed on to the next k1[α]. This stepping procedure will eventually lead to an integer solution for R or S and thus factorization. Here is a schematic of such a search method for the N mod(6)=1 case-



One can start the search for integer R or S within any of the boxes centered on a given k1[α].

U.H.Kurzweg
April 17, 2017