FACTORING SEMI-PRIMES USING THE S FUNCTION

We have shown in several earlier notes found on our MATHFUNC web page that a semi-prime N=pq can always be factored into its prime components p and q via the formula-

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

Here S=(p+q)/2= [σ(N)-N-1]/2, with σ(N) being the sigma function of number theory. The radical in this definition is equal to (q-p)/2 provided q>p. One is fortunate in that the sigma function σ(N) is given in most advanced mathematics programs for semi-primes as large as twenty digits , so that p and q follow directly for any semi-primes N smaller than about 10^20. For Ns greater than this a second route must be used to achieve factoring using the S function. We want in this note to show details of the two approaches which can be used to generate S and hence factor N=pq.

Let us start with the first approach by obtaining the S point function directly using our PC. For this purpose we choose to examine the seven digit long semi-prime-

N=4416941.

Here the sigma function equals 4421532 as can be obtained in a split second. From it we find the S function to be-

S=(4421532-4416941-1)/2=2295.

Substituting into the original formula then gives -

[q,p]=2295±sqrt(2295^2-4416941)= 2295±922=[3217,1373]

It is amazing to see the rapidity with which the factors p and q are obtained. Note that all semi-primes have the form N=6n+1 or N=6n-1.That is, N mod(6)=1 or -1. In the above case 4416941=6(736157)-1.

Next we use the second approach to find S for the same N. First of all we note that S can also be written as-

$$S=\{(1/2)[\alpha+(1/\alpha)]\mathrm{sqrt}(N)\} +\varepsilon =S_0+\varepsilon$$

, where the term in the curly bracket S_0 is taken to the nearest integer since the unknown ε must also be an integer. Also by definition we have-

p=αsqrt(N) and q=(1/α)sqrt(N) so that pq=N

and 0<α<1. Note that S_0 will be known once α has been chosen and N given.
Next we construct a table applicable for N=4416941. It reads-

α	S_0	$\sqrt{\ }$	ε
1	2101	922	194
0.9	2112	922	183
0.8	2153	922	142
0.7	2236	922	59
0.6	2440	922	-145
0.5	2626	922	-331

from the table we see that the smallest epsilon ε lies somewhere around α=0.7.
So the exact value of S becomes 2236+59=2295. This result matches exactly the result obtained earlier directly via our PC, namely, [q,p]=2295±922=[3217,1373]. In searching for the α which makes ε lie near zero, one can evaluate things over the more limited range –b<ε<b, where b will be less than about 10% of S.

Of the two above approaches for finding S, the direct computer route is the fastest when dealing with semi-primes less than about 20 digit length. However when dealing with still larger semi-primes the second approach is the only one which at the present will work despite of the extra effort involved.

Let us finish things up by looking at the 39 digit long semi-prime-

N=23573050424486730703122918564040352953

This number still lies within the range were a direct computer evaluation is possible to achieve a factorization.
We find-

sigma(N)= 23573050424486730712844388640433415168.

On combining terms, this in turn yields-

S=[sigma(N)-N-1]/2= 4860735038196531107

So we have the prime factors

[q,p]=S±sqrt(S^2-N)=[5092456178934060743, 4629013897459001471]

obtained in a ittle over one minute.

I have no doubt that this same 39 digit long semi-prime can also be evaluated by the second approach although I do not carry out such an evaluation here. In addition, someone will shortly figure out how to extend direct computer methods for finding S for semi-primes of 100 digit length or so. If this is achieved then existing public key approaches used in present day cryptography will become obsolete.

U.H.Kurzweg
January 19, 2021
Gainesville, Florida