PROPERTIES OF THE S FUNCTION

When dealing with the factoring of large semi-primes $N=pq$, one encounters the point function-

$$S=(p+q)/2=(1/2)[\alpha+(1/\alpha)]\mathrm{sqrt}(N)=(1/2)[\sigma(N)-N-1]$$

Here $\sigma(N)$ is the sigma function of number theory, $p=\alpha\sqrt{N}$ and $q=(1/\alpha)\sqrt{N}$ with $0 <\alpha <1$. The prime components p and q also satisfy $p<q$. A simple mathematical manipulation of the forms of S given above shows that the prime factors must satisfy-

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

Since the primes are odd integers (2 excepted), it is clear that S must be an integer as is the radical. Once S is known the problem is solved. It is our purpose here to look further into the properties of S.

The simplest way to find S is to use $\sigma(N)$ when this is available. Most advanced mathematics programs such as Maple or Mathematica give the value of the sigma function for Ns of up to about 40 digit length. Thus the semi-prime-

$$N:=4294967297$$

, which happens to be one of the Fermat numbers $2^{32}+1$, has-

$$\sigma(N)= 4301668356$$

So, $S=(4301668356-4294967297-1)/2=3350529$. This in turn produces the factors-

$$[q,p]=3350529\pm3349888=[6700417, 641]$$

This result was arrived at in a fraction of a second compared to months of effort it took by the famous Swiss mathematician Leonard Euler over 200 years ago.

Unfortunately the direct computer use to factor semi-primes larger than about 40 digits will fail on any home PC because of the time involved. Thus the following 100 digit long semi-prime, which we first constructed several years ago,-

$$N=pq=4232645070331114502389141379272067425948811706763611499183494431736227631344523325922189543223660977$$

cannot be factored directly at the present time here at home, although the world's fastest supercomputers can probably factor this number shortly without the need for the use of grid or elliptic equation methods. We do know that N here has the form 6n-1 since N mod(6)=5. This means that $p=6n+1$ and $q=6m-1$. If someone can come up with a fast way to determine $\sigma(N)$ for Ns greater than about 10^40, then the present approach will make public key cryptography obsolete. Remember that $S=[\sigma(N)-N-1]/2=(p+q)/2$. We can also introduce the additional variable $T=(q-p)/2$. Here S represents the mean value of p and q while T equals half the distance between q and p.

A table of the quantities p, q, N, S and T for some smaller semi-primes N=pq looks as follows-

p	q	N	σ(N)	S=(p+q)/2	T=(q-p)/2
7	11	77	96	9	4
13	19	247	280	16	6
37	59	2183	2280	48	22
257	419	107683	108360	338	81
3797	5683	21578351	21587832	4740	943

On examining this table, one sees that p, q and N are all odd positive integers of the form 6n+1 or 6n-1, that $\sigma(N)$ lies slightly above N getting closer as N becomes large, and that the sigma function for semi-primes and 2S are always even. The prime components form N=215578351 can be directly read off of the table as-

$$[q,p]=S\pm T=4740\pm 943=[5683, 3797]$$

Since finding the primes p and q by direct home computer evaluation of $\sigma(N)$ for Ns above 10^40 is impractical, one must introduce a second method for using S to find the components of N when N is much larger than this. The way to do this is to start with a guess for α and then use the definition-

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

to find the value of ε which makes $T=\mathrm{sqrt}(S^2-N)$ an integer. Repeating such an evaluation for several different α will produce a map where ε changes sign. The closers ε is to zero, the closer one is to the true non-integer α value. Using this value of α produces the correct S for the problem and p and q become known. This procedure is valid for all sizes of N.

Let us demonstrate the procedure for the last N in the above table, namely,-

$$N= 21578351 \quad \text{where} \quad \mathrm{sqrt}(N)=4645.250\ldots$$

For the first guess for alpha we take α=0.75. This produces-

S=(1/2)[0.75+(1/0.75)[sqrt(N)+ε = 4839+ε

to the nearest integer. We now have to find the epsilon which makes-

T=sqrt[(4839+ε)^2-N]

an integer. The search program to do this is-

```
for ε from -100 to 100 do{ε,sqrt(S^2-N)}od
```

The integer solution becomes ε=-99 so that S=4740 and T=943

The larger negative -99 for epsilon says we will find a smaller epsilon if we take the larger initial guess of α=0.8. This produces ε=-21, S=4740, and T=943. The S and T point functions are equal to each other for the two alphas considered. A linear interpolation yields an estimate of α=0.82 for producing an ε at or near zero. Indeed, S=4737+ε produces ε=3.We have q=S+T=5683 and p=S-T=3797. The only drawback of his last approach for finding S and T is that ε can become large when the initial α guess is far removed from the exact value. Part of this difficulty can be overcome by evaluating in only a limited strip of epsilon so that there will be no epsilon found until one is close to the exact value of α.

U.H.Kurzweg

January 22, 2021

Gainesville, Florida