LATEST ON N=pq FACTORIZATION

Introduction:

Consider any semi-prime N=pq , where (as we have shown in earlier articles) the two primes must have the form p=6n±1 and q=6m±1 provided both equal five or greater in value. We also can set p=α sqrt(N) and q=(1/α) sqrt(N), so that pq=N and 0<α<1 is a measure of how far p and q are removed from their mean value of S=(p+q)/2=(α+1/α)sqrt(N)/2. We can write symbolically that a factorization is achieved by working out the following identity-

$$[p,q]=S\mp\sqrt{(S^2-N)}=(p+q)/2\mp(1/2)\sqrt{(q^2-2pq+p^2)}=\{(p+q)\mp(q-p)\}/2$$

An inspection shows that the [p,q] factorization will be known once S has been determined. We have found two distinct method for finding S for semi-primes. These are (1) finding the integer value of sqrt(S^2-N) or (2) looking up the value of the sigma function σ(N)=2S+N+1 on our PC. Let us quickly summarize these two methods by looking at two large Ns.

(1)-Finding the Integer Value of R=sqrt(S^2-N):

We start with the semi-prime-

N=455839 where sqrt(N)=675.15849…

Here we see that the integer S=[(1+α^2)/(2∝)]sqrt(N)>sqrt(N). The radical R must also be a real positive integer. The non-integer ∝ is unknown to begin with other than that it is less than one and greater than zero. This inequality suggests that one try S=bsqrt(N)+ε, where bsqrt(N) is an integer greater than sqrt(N) with b≥1. So let us look at the radical-

$$R=\sqrt{\{(b\ sqrt(N)+\varepsilon)^2-N\}}=\text{Positive Integer}$$

and take b sqrt(N)=676. This produces the quadratic-

$$R=\sqrt{(1137+1352\varepsilon+\varepsilon^2)}$$

The search program-

```
for ε from 0 to 10 do {ε,evalf(R)}od;
```

then produces the result R=81 at ε=4. Thus we have S=676+4=680 and-

$$[p,q]=680\mp81=[599,761]$$

As seen this approach is extremely fast provided p and q are of comparable size. It becomes more cumbersome as N gets larger since the guess for b may lie far away from b=1.

(2)-Using the Computer given Value for the Sigma Function:

A second way to factor large semi-primes N=pq makes use of the sigma function $\sigma(N)$ of number theory. For semi-primes it equals –

$$\sigma(N)= p+q +N+1=2S+N+1$$

Now it is fortunate that this function is stored in most advanced computer programs such as MAPLE or MATHEMATICA up to at least semi-primes of 40 digit length.

Let us consider the 24 digit long semi-prime-

$$N=137249026253905045859383$$

, where our PC yields-

$$\sigma(N)= 137249026254653576221728$$

in less than 1 second. So we have-

$$S=[\sigma(N)-N-1]/2= 374265181172$$

This produces the factoring-

$$[p,q]=374265181172\mp\sqrt{(374265181172^2-137249026253905045859383}$$

$$=[321110693273,427419669071]$$

As seen, this procedure requires only very elementary mathematical operations.

Conclusion:

We have shown that large semi-primes N=pq can be factored into their prime components by either evaluating a radical R or using $\sigma(N)$ directly from one's computer. The second approach is the faster factoring method as long as N remains small enough so that $\sigma(N)$ is given. Future work on factoring large semi-primes , such as the public keys encountered in cryptography, should mainly concentrate on finding a method which speeds up the generation of $\sigma(N)$ for semi-primes N of one-hundred or larger digit size.

U,H,Kurzweg
July 29, 2020
Gainesville, Florida