MORE ON THE FACTORING OF LARGE SEMI-PRIMES

We have shown in several earlier articles on this web page that any semi-prime N=pq can be factored into its prime components p and q via the equation-

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

Here S=(p+q)/2 is the average of the prime components and the radical represents the departure from the mean. We can also write S as the identity-

$$S = [(\sqrt{N})_I + \varepsilon] = \frac{(\sigma - N - 1)}{2}$$

, with the subscript I denoting the nearest integer value. Also ε is an integer small compared to sqrt(N) to be found and σ is the well known sigma divisor function of number theory. Since most advanced computer programs can generate σ to at least twenty places, a simple substitution can factor semi-primes up to that same number of places. Beyond that point, when getting into the N equal 100 digit range as encountered in public key cryptography, required in public key cryptography, one needs to first generate larger values for σ or evaluate the values of S directly by evaluating the radical R=sqrt[S^2-N]) directly until an integer for R is found by varying the integer ε.

Let us first consider factoring the twenty-four digit long semi-prime-

N:=137249026253905045859383

This time the digit length of N is less than the limit allotted by our MAPLE program , so it produces-

σ(N):=137249026254653576221728

and S=σ(N)-N-1=374265181172. This yields-

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

=321110693273 x 427419669071 .

This evaluation was accomplished in a split second on our home PC.

Next pushing the limits of our home computer we looked at the 38 digit long semi-prime-

N= 79259796022025569219580682646178858411

It took three minutes to yield-

$\sigma(N)$= 792597960238138836412570661237812168 32

and-

$S=\sigma(N)-N-1$=178831442167638347760235 8420 .

Plugging this N and S into the original equation for [p,q], we arrive at the answer-

[p,q]= (178831442167638343328140 7327) x (44320951093)

Going to even larger digit semi-primes will take still longer to produce a factoring. A profitable alternate approach for finding the S point function for greater than the 40 digit length limitation of our home PC would be to evaluate the radical R directly using the following search program-

for ε from 1 to b do {ε,R}od;

, where again-

$$R=\sqrt{(\sqrt{N_I}+\varepsilon)^2-N}$$

The search starts with ε=1 and goes up to the value which first produces an integer value for R. Such an approach will always work no matter what the size of N is, but will require an ever large number of trials before R is found. Once R has been established, the rest of the factoring process becomes straight forward. Let us demonstrate the procedure for-

N=455839 with $\text{sqrt}(N)_I$=675

Carrying out the computer search, we find after just five trials that R=81 at ε=5. Hence the semi-prime is factored as-

[p,q]=[680-81,680+81]=[599,761]

Although this last procedure will always work, the number of searches for integer R can become rather large as N becomes large.

We suggest, from the two factoring approaches demonstrated above, that one concentrate on the first approach which does not require multiple trial runs. It will however require an accelerated method for finding $S=\sigma(N)-N-1$. If this can be aqccomplished, the factoring of semi-primes of 100 digit length or more will become possible allowing one to question the use of public keys in electronic cryptography.

U.H.Kurzweg
Feb.2, 2020

Gainesville, Florida