# FACTORING SEMI-PRIMES USING THE SIGMA FUNCTION

We have shown in several earlier articles found on this web page that the prime components p and q of a semi-prime N=pq are given by-

$$[p,q]=\frac{(\sigma(N)-N-1)}{2}\mp\sqrt{\left[\frac{\sigma(N)-N-1}{2}\right]^2-N}$$

regardless of the magnitude of N. Here $\sigma$(N) is the sigma point function of number theory equal to the sum of all its divisors. Thus for the semi-prime N=pq=77 we have $\sigma$(77)=1+7+11+77=96, so that-

$$[p,q]=(96\text{-}78)/2\mp\sqrt{81-77}=9\mp2=[7,11]$$

From the above general formula we see that finding p and q requires mainly that one knows the value of $\sigma$(N). This in turn requires that one knows the positive integer value R of the square root shown or takes the value of sigma directly from one's computer using either Maple or Mathematica. These programs handle $\sigma(N)s$ out to about forty digit length.

Let us demonstrate the factoring procedure by the R route for the six digit long semi-prime-

N= 455839

Here our starting point for finding an integer R value is to try the approximation-

$$\sigma \cong 1+2\text{sqrt}(N)+N=457{,}190$$

and then run the program-

```
for s from 457190 to 457210 do ({s,sqrt((s-N-1)/2)^2-N)})od;
```

It produces in a split second that R=81 at s= $\sigma$ =457200 and the factors become-

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

Note that for any semi-prime the number $\sigma(N)$ will always be an even number since both p and q are odd. Its value will be slightly above N.

Let us next consider factoring the larger ten digit long semi-prime-

$$N=2144058041$$

Our Maple program here yields in a split second that –

$$\sigma(N)=2144157300$$

Substituting this sigma value into the above [p,q] equation yields-
R=17869 . We thus find –

$$[p,q]=[31769, 67489]$$

The alternate, but longer way to find [p,q] is to start with the guess

$$\sigma(N)\approx 1+2\mathrm{sqrt}(N)+N=2144150650$$

and run the above search program 6650=2144157300-2144150650 times to get the same answer. Clearly here, and also for still larger semi-primes, getting the value of sigma(N) directly from our computer is always a much faster approach for finding sigma(N) , especially when N becomes still larger as occurs .for example, for public keys used in cybersecurity. At the present time our laptop can deliver $\sigma(N)$ values up to about forty digit length. Efforts should be made immediately to extend this range to one hundred or so digit length. If this can be achieved, present day cybersecurity will have become obsolete.

U.H.Kurzweg
June 8, 2024
Gainesville, Florida