USE OF A DIOPHANTINE EQUATION TO FACTOR ANY SEMI-PRIME

Several years ago we showed on this web page how one can factor the semi-prime N=pq using the equation-

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

, where S=(p+q)/2=(σ(N)-N-1)/2 and σ(N) is the sigma function of number theory.

The approach works well as long as N=pq is less than about forty digits long. Within this limit the advanced math programs Mathematica or Maple yield closed form values for σ(N). For Ns in excess of these lengths the finding of σ(N) becomes cumbersome and thus impractical for still larger semi-primes such as the ones encountered in cyber-security. We wish here to extend the factoring process to large semi-primes by a new technique involving a new function x heretofore recognized.

We start by noting that if p=q, then both primes equal sqrt(N). Since both p and q are odd integers sqrt(N) must be modified to integer form. We let-

R =nearest integer above sqrt(N)

This suggests the new definition-

2(R+x)=p+N/p

On rewriting we get-

P^2-2p(R+x)+N=o

On solving we nave-

p=(R+x)-sqrt((R+x)^2-N

For p to be integer as well as x and R, we arrive at the new non-linear Diophantine equation-

(R+x)^2-N=y^2

, with y also a positive integer. Once this has been solved by the one line program-

```
for x from 0 to b do({x,sqrt((x+R)^2-N)})od
```

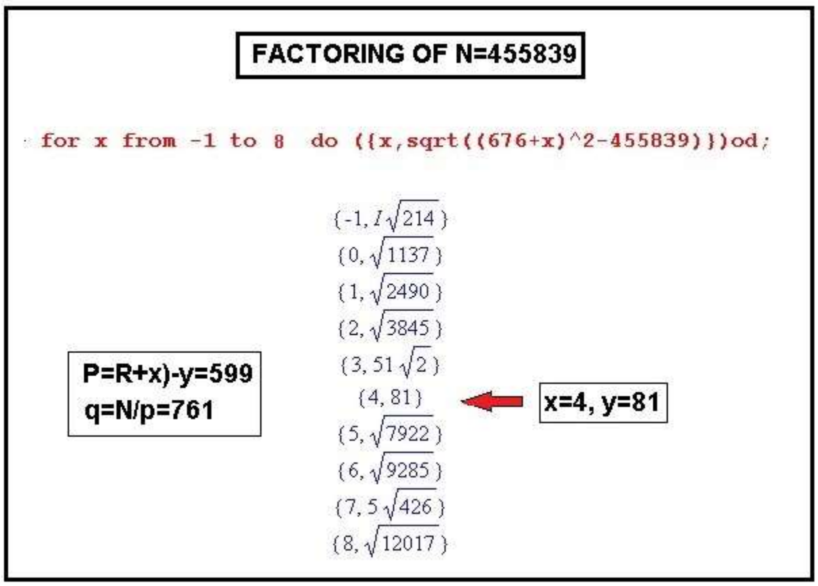
we can recover both p and q at once. Typically, when x is an integer a lot smaller than R, there will be only a small number of trials involved in finding both integer x and y. When x gets larger it is best to use the re-written Diophantine form-

y^2=(R^2-N)+2xR+x^2

and to note that typically 2xR is large compared to both (R^2-N) and x^2.So that y^2 equals an integer a little above 2xR.

Let us demonstrate the new factoring approach with N=2201 where R=47. Solving we find [x, y]=[4, 20]. So p=(R+x-y=31 and q=N/p=71. The speed with which the result was obtained is impressive requiring only four trails.

Take next the larger six digit long semi-prime N=455839. Here R=676 . Running the program from x=0 to x=8 we obtain the following table-



This result can also be obtained by the Lenstra elliptic curve method but only for at a considerable amount of extra work.

Finally let is consider the nine digit long semi-prime-

N:=137703491 where R=11735

Here it takes a total of 919 trials, starting with x=1, to arrive at [x,y]=[919, 4735]. From this solution we deduce that-

p=R+x-y=7919 and q=N/p=17389

Notice the rapid increase in the value of x as N gets larger than about eight digits. Under those conditions it might be a good idea to start the search at x=0.1*R=1174 and then search in the neighborhood. At trial x=-255 you will find your answer.

We have shown that the semi-prime $N=pq$ can be factored into its two prime components by solving the Diophantine Equation $(R+x)^2-N=y^2$, where R is the first integer value above $\sqrt{N}$. Once the integer values of [x,y] have been found, the values of p and q follow from-

$p=(R+x)-y$ and $q=N/p$ with $p<q$

The value of x increases with increasing N but typically stays below about ten percent of R.

U.H.Kurzweg
Gainesville, Florida
September 30, 2023