FACTORING LARGE SEMI-PRIMES USING A PARABOLA

In several recent notes on this Tech-Blog we have shown a new way to factor semi-primes using a heretofore un-recognized parabola. We want in the present article to re-derive this approach for factorization of large semi-primes N=pq and add some further details on the method.

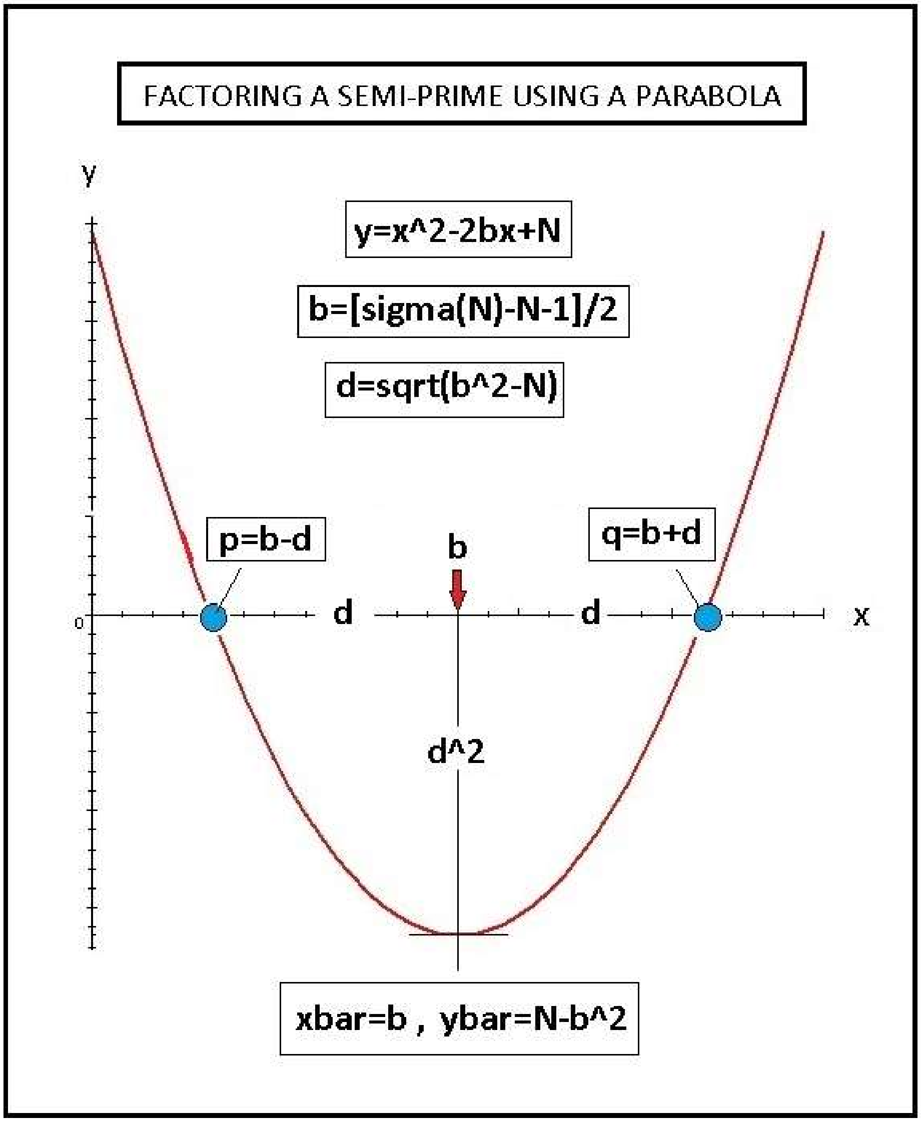
Our starting point are the two equations-

$$xy = N \quad \text{and} \quad x+y= \sigma(N)-N-1=2b$$

Here σ(N) is the sigma fumction of number threory representing the sum of all divisors of the semi-prime N. The number b represents the mean value of p and q. Eliminatig y from these equations produces-

$$x^2-2bx+N=0$$

Next comes the trick of replacing the zero on the right of this last quadratic by y This yields the herrtofore un-recognized parabola shown in the following graph—



The curve is symmetric about the vertical line x=b and has its vertex at [xbar,ybar]=[b,N-b^2]. Most importantly, the two primes associated with N lie along the x axis and on the parabola. The values of p and q follow -

p=b-d and q=b+d

I have indicated these primes by two blue circles. Note the constant ratio of d to d^2 holds for all semi-primes. Evaluating the parabola at y=0, shows one that –

d=sqrt(b^2-N)

So knowing b , and hence σ(N), allows one to find d and hence p and q.

To demonstrate the factorization process for a specific large semi-prime consider the nine digit semi-prime-

N=387896423

Within a split second, our Maple computer program says that the corresponding sigma function becomes σ(N)=387936120. From it we have at once that-

b=[σ(N)-N-1]/2=19848

Also we find-

d=sqrt(b^2-N)=2459

Combining b and d produces the final factored result-

p=b-d=17389 and q=b+d=22307

It is amazing how simple this approach is for factoring semi-primes as long as σ(N) does not exceed much above forty digit length. Above these digit values, determining the sigma function on my laptop using either Maple or Mathematica becomes progressively more and more time consuming, takes about a day to find σ(N) when the sigma function is some 80 digits long . If one could find a way to speed up the σ(N) search, present day electronic cryptography using open public keys would become obsolete.

U.H.Kurzweg
October 15, 2024
Gainesville, Florida