A GRAPHICAL TECHNICE FOR FACTORING LARGE SEMI-PRIMES

One of the more important unsolved problems in number theory is how to quickly factor a large semi-prime N=pq into its two component p and q. Our own efforts over the last decade concerning the factoring of such semi-primes has led to the closed form result-

$$[p,q]=a\pm sqrt(a^2-N)$$

, where a=(p+q)/2=[σ(N)-N-1]/2=Nf(N)/2. Here σ(N) is the sigma function of number theory and f(N) the number fraction discovered by us earlier. The definition of f(N) is-

$$f(N)=\sigma(N)-N-1)/N$$

It is a slowly increasing function of N with f(p) and f(q) both equal to zero. Explicit values for p and q are thus obtainable if σ(N) or f(N) are known. One is fortunate in that most advanced math computer programs, such as Maple or Mathematica, give sigma for values of N as high as 40 digit length, meaning that prime components as high as twenty digits each can be found by the above [p,q] formula. For still larger semi-primes , such as found in public key cryptography , some additional work on quickly finding sigmas for Ns above forty digits length is needed.

It is the purpose of this note to introduce a new graphical approach for factoring large semi-primes. Hopefully this will offer some clues as to how to find larger σ(N) for Ns of greater than forty digit length.

Our starting point is the basic definition for any semi-prime-

$$N=pq$$

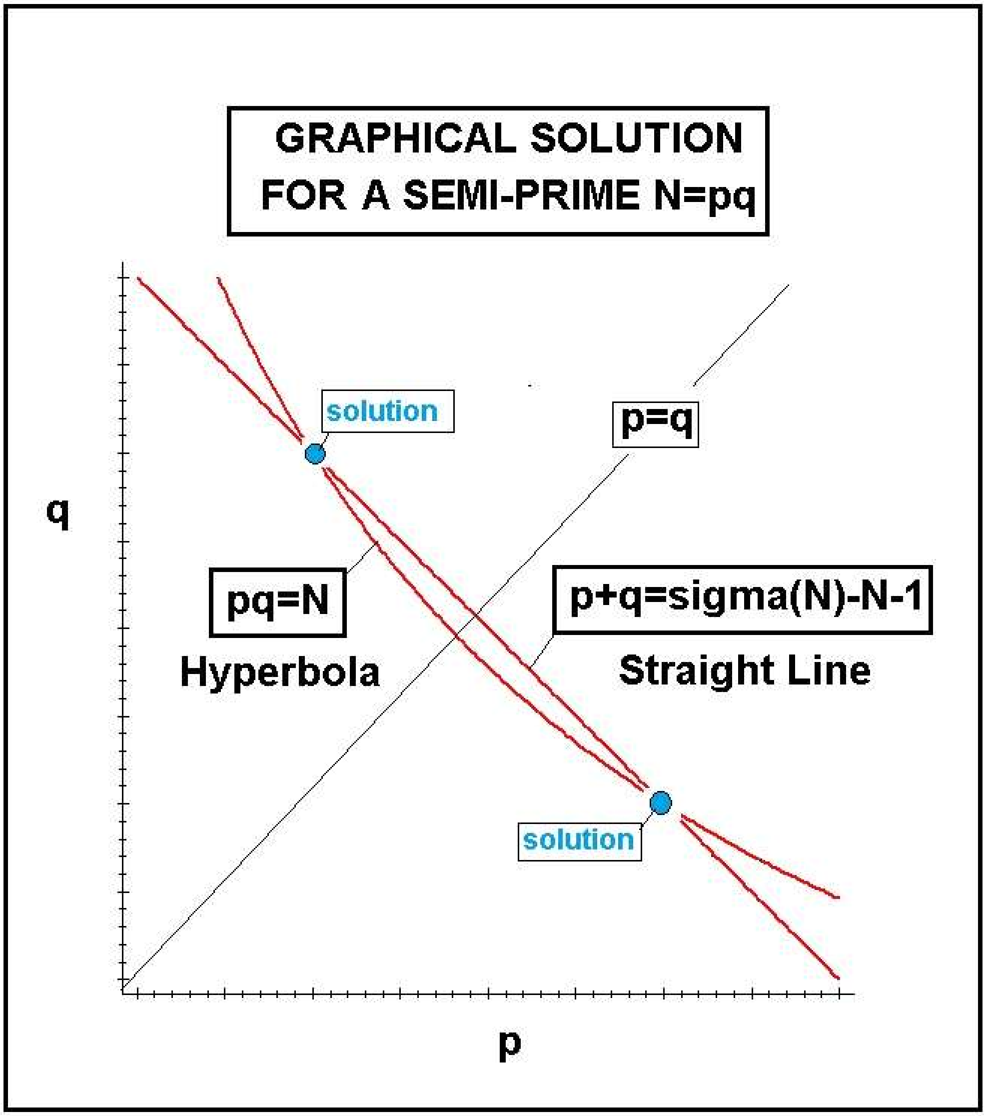
When looking at this function graphically we have a hyperbola symmetric about line p=q. Next we introduce the sigma function for N with the property that-

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

Expanding this definition we get-

$(p+q)=\sigma(N)-N-1$

Graphically this represents a straight line in the p-q plane which cuts the hyperbola at two points both representing the solution [p,q]. Here is the combined graph-



Note that the straight line is also symmetric about p=q.

A more convenient way to describe our solution is to eliminate q to get-

$y=x^2-x(\sigma(N)-N-1)+N$

in the x-y plane. Here p=x and y=0 corresponds to our two solutions . Note that this y=y(x) equation is a parabola which may be written as-

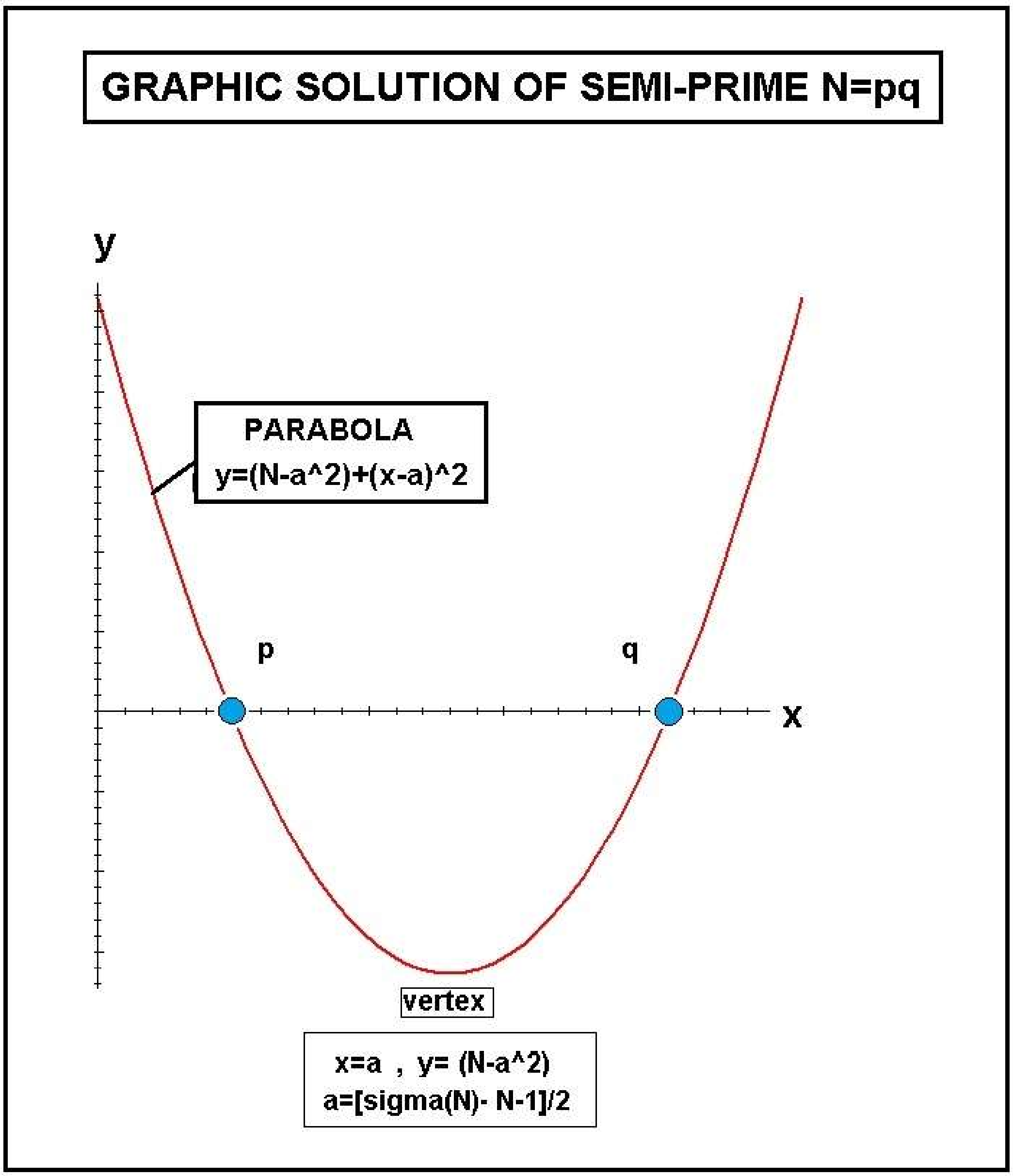
$$y=(N-a^2)+(x-a)^2$$

Its vertex lies at x=a and y=N-a^2. Here-

$$a=[\sigma(N)-N-1]/2=Nf(N)/2$$

as already defined earlier.

This last expression is an important parameter which locates the parabola in the x-y plane. Here is a plot of the parabola for a typical semi-prime N=pq-



The mean x value between the two solutions is x=a . Also note that 'a' is approximately equal to sqrt(N). Let us demonstrate this graphical approach for factoring a couple of specific large semi-primes.

The first example involves factoring the semi-prime-

N=455839 .

With aid of our Maple program, we find σ(N)=457200 in a split second. This information then yields-

a=457200-455839-1=1360

This leads to the parabola-

y=(N-a^2)+(x-a)^2=-6561+(x-680)^2.

On setting y to zero we get the solution-

x=680$\pm$81

That is-

p=599 and q=761

This particular N has been used in the literature to demonstrate the elliptic curve factorization method of Lenstra for semi-primes. It takes considerable more effort by that method to arrive at the same result for p and q.

As a second factorization consider the Fermat Number-

N=2^32+1=4294967297

which Fermat thought to be prime but proven later by Euler to be a composite.

Its sigma function value is given by our Maple program in a split second and reads-

$\sigma(N)$ **=4301668356**

This produces-

a=[sigma(N)-N-1]/2=3350529

Next setting y to zero, we arrive at $x=a\pm sqrt(a^2-N)$. This in turn leads to the solution-

$$p=x=641 \qquad \text{and} \qquad q=N/p=6700417$$

What took Euler weeks to arrive at is here gotten in a split second.

Although we could factor numerous number of additional semi-primes for Ns up to about 40 digit length, what is now needed is to find a way to speed up the search for sigma(N)s for N >10^40. If this can be archived, then present day public key cryptography will become obsolete.

U.H.Kurzweg
July 22, 2024
Gainesville, Florida