A GEOMETRIC WAY TO FACTOR LARGE SEMI-PRIMES

It has been of consideravble interest in the last few decades to find methods which can quickly factor semi-primes N=pq. Here p and q are the contained primes. A new way to look at such numbers is to begin by taking the sigma function of both sides of the semi-prime definition. We have the following-

$$\sigma(N)=\sigma(pq)=\sigma(p)*\sigma(q)=\sigma(p)*\sigma(N/p)$$

, where σ(N) is the sigma function of semi-prime N. The sigma-function represents the sum of all divisors of N and hence equals 1+p+q+N. Substituting this expansion into the above equality produces-

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

This result maybe writen as-

$$H(x)=\frac{\sigma(N)}{1+x}-\frac{N+x}{x}$$

, where x=[p,q] and H(x) vanishes only for those xs which are the prime factors. H(x) will generally have a parabolic shape peaking near sqrt(N). This new formula for factoring semi-primes may also be writen as-

$$H(x)=\frac{1+N+2\{sqrt(N)+n\}}{1+x}-\frac{N+x}{x}$$

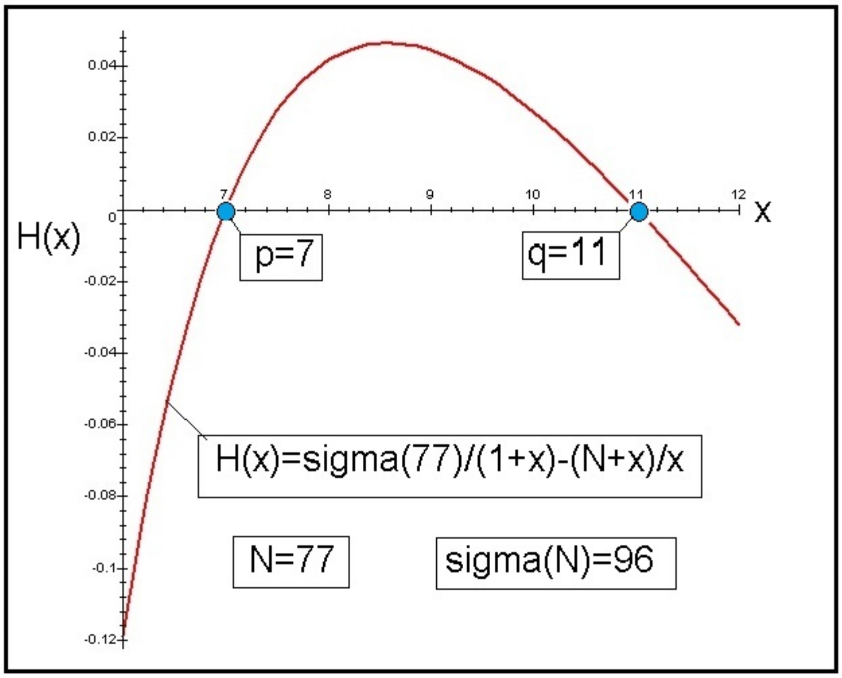
Here sqrt(N) is the nearest integer to the square root of N and n=0,1,2,3, etc is varied until H(x) hits zero at x=p and x=q . This second form for H(x) works for all semi-primes N=pq but will take longer than the σ(N) route when this function is available on one's PC. Typically, as long as N has less than about

40 digit length, the first of the two forms for H(x) is prefered since the number of trials can become huge for large Ns.

Let us demonstrate the solution approach for a very simple example involving the semi-prime –

$$N=77 \text{ with } \sigma(77)=96$$

Plugging these values into the first H(x) equation above produces the folowing geometric curve-



We see that H(x) crosses the x axis at the primes x=7 and x=11. The H(x) curve reaches its maximum near sqrt(77) ≈ 9 . The second H(x) equation above will give the same result when n is set to zero. It will however take longer than the sigma route when this value is available on one's computer. On setting H(x)=0, we find the two prime roots given by the quadratic-

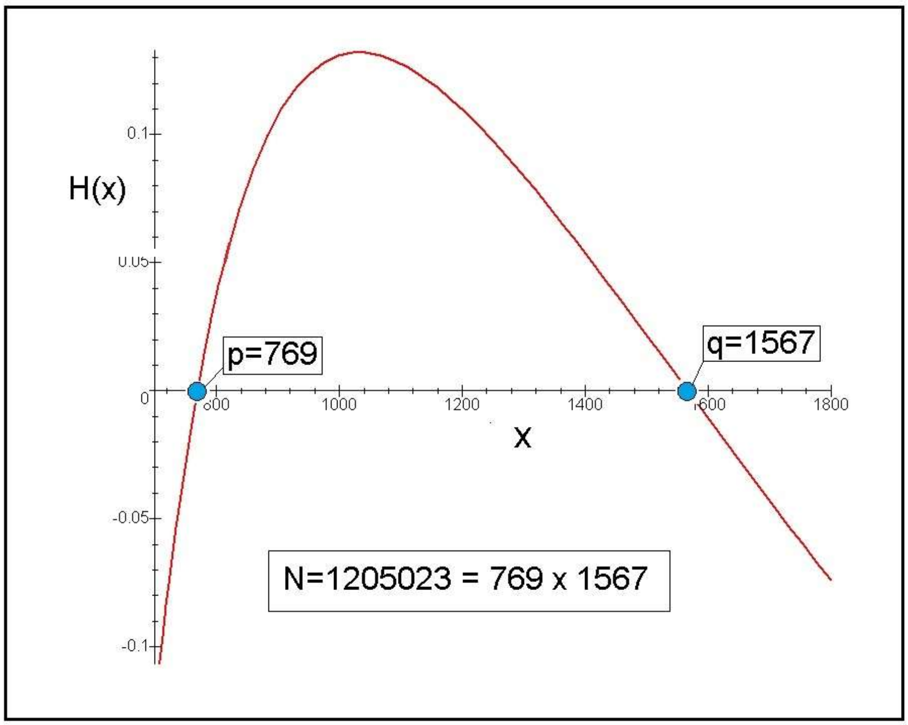
$$x^2-18x+77=0$$

This means p=7 and q=11. The difference between q and p can be read off of the graph as 4 units.

Consider next a larger semi-prime N=1205023 with σ(N)=1207360. Here we have-

$$H(x)=\frac{1207360}{1+x}-\frac{1205023+x}{x}$$

A plot of this equation follows-



Note the values p and q as the H(x) curve crosses the x axis. The difference between the primes is the even number q-p=798. The peak of the curve lies near sqrt(N)≈1098.

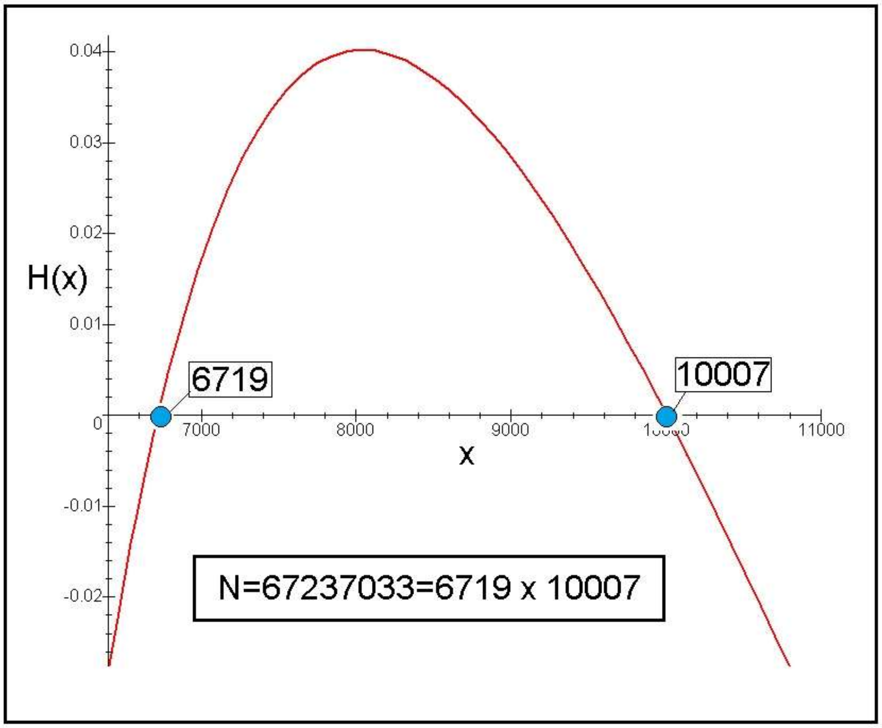
As a final semi-prime to factor by the present geometrical method, we choose the eight digit long number-

N=67237033 where sigma(N)=67253760

Here-

$$H(x)=\frac{67253760}{1+x}-\frac{67237033+x}{x}$$

It plots as -



H(x) is seen to have a parabolic like shape with a max near sqrt(N)≈8200. The average value of p and q is (p+q)/2=8363. So not far removed from 8200. You will notice that when N gets large the value of σ(N) lies just slightly above N. The reason for this is that the definition σ(N)=1+p+q+N has 1+p+q<<N for large N.

The present procedure can be taken to larger Ns including the hundred digit long semi-primes ncountered in pubic key cryptography. It does however require knowledge of σ(N) or its equivalent form-

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

, where sqrt(N) represents the nearest integer approximation to the root of N and n is appropriately chosen to make p and q odd integers and not fractions.

U.H.Kurzweg
December 3, 2022
Gainesville, Florida