PROPERTIES OF A NEW FACTORIZATION FORMULA

Recently while studying ways to accelerate the process of factoring large semi-primes we came up with a new formula –

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

whose solution for H(x)=0 produces the prime factors x=[p,q] of the semi-prime N=pq. You will find its derivation at-

https://mae.ufl.edu/~uhk/ MORE-SEMI-PRIMES.pdf

We want in this article to discuss in more detail the properties of this formula.

Let us begin by noting that σ(N) is the sigma function of number theory representing the sum of all divisors of the semi-prime N=pq. That is-

σ(N)=1+p+q+N

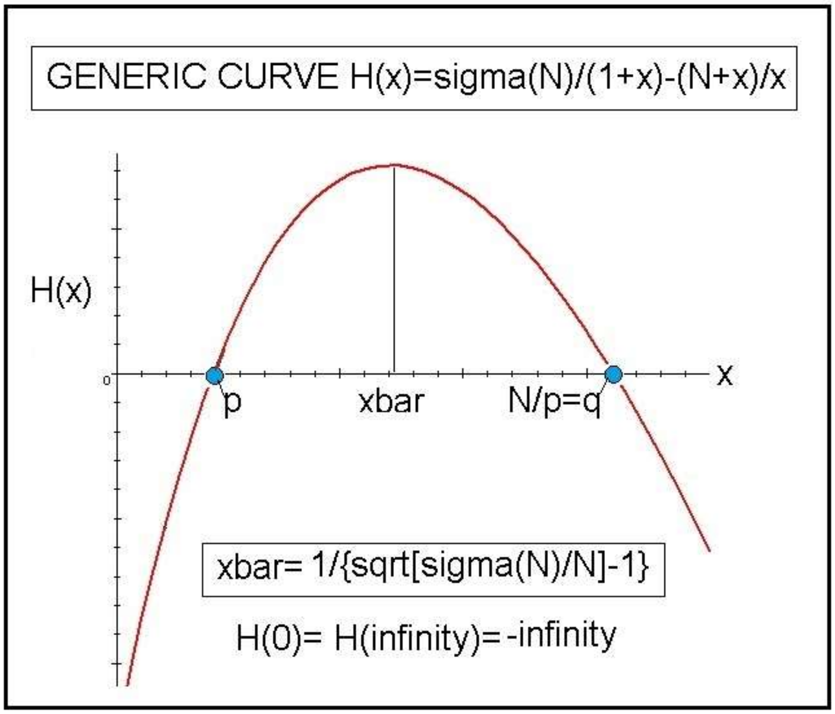
must be a positive even integer since p, q, and N are odd. The value of H(0) goes to minus infinity as does H(∞). Working out the first derivative of H(x), we have-

dH(x)/dx=-σ(N)/(1+x)^2+N/x^2

This has zero value at-

xbar= $\frac{\sqrt{N}}{\sqrt{\sigma(N)}-\sqrt{N}}$ with H(xbar)>0

From this information we know that the curve H(x) will have a parabolic like shape with H(x)=0 at x=[p,q]. Here is a generic graph of H(x)-



We can calculate the value x=[p,q] by evaluating the re-written form of H(x)=0. It has the quadratic representation-

$$x^2+[1+N-\sigma(N)]x+N=0$$

which has the two integer solution x=[p,q]. One is fortunate in that most advanced computer math programs yield σ(N) for Ns up to about 40 integer size in relatively short time. So, for example, the semi-prime-

N=4633 has σ(N)=4788

This produces the quadratic-

$$x^2-154x+4633=0$$

with the solution x=[41,113].

Consider next the larger semi-prime-

N=481267081 with σ(N)= 481314064

To factor this N we need to solve the quadratic-

$$x^2+[481314064-481267081-1]x+481267081=0$$

Its solution is-p=15091 and q=31891

As a third specific example consider the large 38 digit semi-prime-

N=23573050424486730703122918564040352953

for which my PC using MAPLE produces-

σ(N)= 23573050424486730712844388640433415168

in a little less than 60 seconds. Plugging N and sigma(N) into the above quadratic then produces the factored result-

x=[4629013897459001471, 5092456178934060743]

in an additional fraction of a second.

If I were to attempt factoring still larger digit semi-primes the calculation times on my PC would become prohibitive. To be able to handle semi-primes in the 100 digit range, such as used in public key cryptography, will require much faster super-computers and in particular additional work on σ(N) calculations using existing Java language.

U.H.Kurzweg
October 31, 2022
Gainesville, Florida
Halloween