FACTORING PARABOLA FOR SEMI-PRIMES

For the past decade or so we have been studying ways to quickly factor large semi-primes N=pq into its their prime components p and q. We have found numerous ways to accomplish this as described in earlier articles on this Tech Blog. Here we want to discuss a new approach based on a parabola which, when evaluated at y=0, produces the solution [p,q] in a straight forward manner.

We start out by setting-

$$N=xy \quad \text{and} \quad x+y=2b$$

, where b= (p+q)/2=[σ(N)-N-1]/2 is the average value of the prime components p and q. Eliminating y from these two equations produces-

$$(x-b)^2+(N-b^2)=0$$

On replacing 0 by y, we get the parabola-

$$\mathbf{y=(x-b)^2+(N-b^2)=x^2-2xb+N}$$

We call this the **factoring parabola**. The two roots to this equation, as y is allowed to approach zero, are the primes p and q. If the value of the sigma function σ(N) is known, then b will be known and the factors [p,q] will follow directly. Most advanced mathematics programs give values of σ(N) in a split second when N is less than about forty digit length.

Let us demonstrate the factoring for the six digit long semi-prime-

$$N=455839 \quad \text{where} \quad \sigma(N)=457200$$

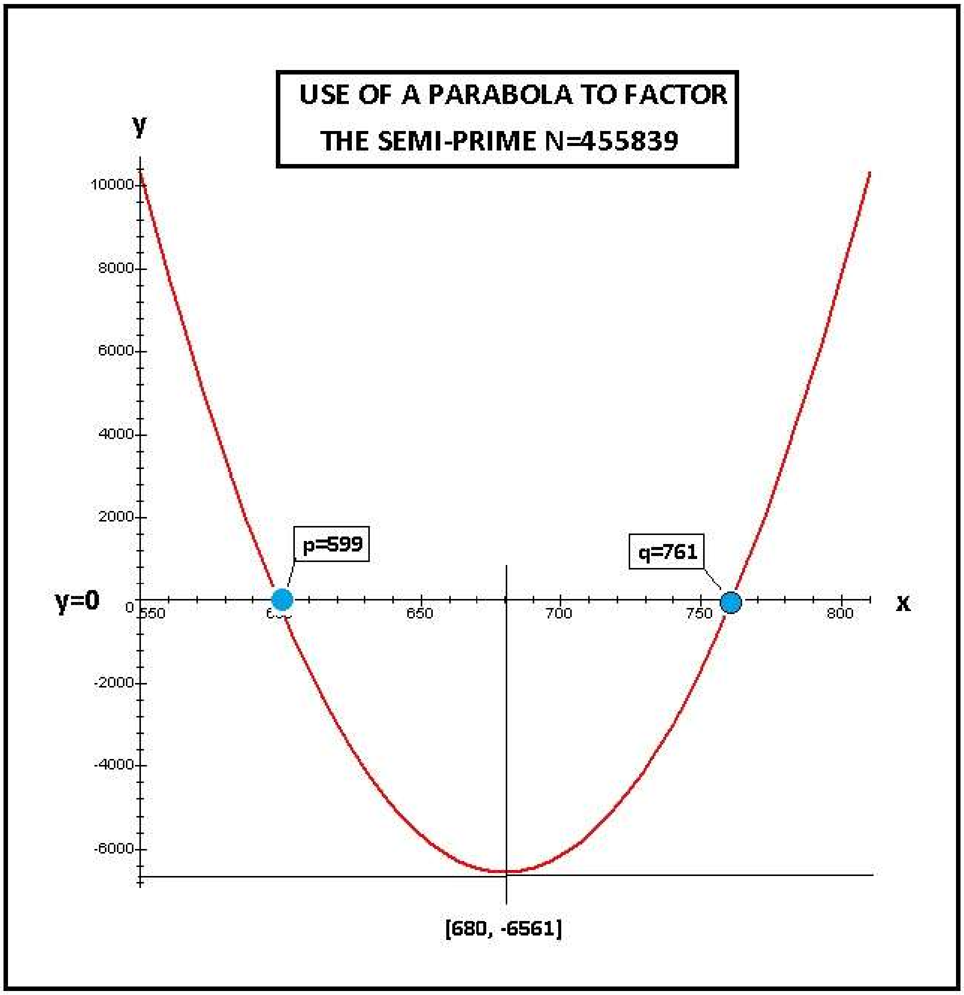
This produces b=680 and the quadratic formula-

$$0=x^2-1360+455839$$

Solving we have the factors-

[p,q]=[599, 761]

A picture of the factoring formula for this case follows-



Note here that the parabola is symmetric about the vertical line x=b , that the shortest distance from the parabola vertex and the line y=0 is b^2-N, and that the half distance between q and p along the y=0 axis is sqrt(b^2-N). These properties will hold for any semi-prime including the hundred plus digit semi-primes N used in modern day cryptography.

An alternative way to solve for the components of any semi-prime N=pq is to go back to the above factoring parabola and set-

$$b= sqrt(N)+\Delta$$

, with sqrt(N) being the nearest integer neighbor to the root of N and

Δ to be found integer values near Δ=0. Note that if p=q these primes are both equal to sqrt(N). Solving the factoring parabola for y=0, then produces-

$$[p,q]=(sqrt(N)+\Delta)\mp sqrt\{(sqrt(N)+\Delta)^2-N)\}$$

Since we know that p and q are odd integers, the term in the right bracket term musr also be an integer. Hence Δ can be found by the one line program-

for n from 0 to +c do({n,sqrt((sqrt(N)+n)^2-N)})do;

The value of Δ=n which makes the bracket an integer will typically not be too large for practical calculations.

Lets try things for the same earlier semi-prime N=455839 where the nearest integer to the root becomes sqrt(N)=675. Running the program between n=0 and n=5 yields the table-

n	Sqrt((675+n)^3-N)
0	953.49 i
1	33.719
2	49.895
3	62.080
4	72.124
5	81.000 ← **solution**

We see that n=5 yields the integer radical root 81 and the factorization becomes-

$$p=680-81=599 \quad \text{and} \quad q=680+81=761$$

This is the same result found earlier using the σ(N) function. Both approaches take up only a split second of computer time for such six digit long semi-primes. The search will become progressively longer as the number of digits increases.

Also, when going to a larger 40 digit long semi-primes, the sigma function factoring approach takes about four minutes of computer time using my think-pad lap computer and a MAPLE math program. It becomes hours when dealing with semi-primes of 100 digit length or so. It would be well worth while if someone where to discover a way to speed up the finding of sigma functions of such extended length for it would then make public key cryptography obsolete.

U.H.Kurzweg
September 24, 2024
Gainesville, Florida