FACTORIZATION OF ANY LARGE SEMI-PRIME AND THE EVALUATION OF THE CORRESPONDING SIGMA FUNCTION

In a previous article on this web page we have shown that there exists a new function –

$$H(x)=\sigma(N)/(1+x)-(N+x)/x$$

which can be used to factor any semi-prime N=pq into its prime components x=[p,q]. Here σ(N) is the sigma function of number theory defined for semi-primes as –

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

Upon setting H(x) to zero one is left with the quadratic equation-

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

Here the term in the square bracket just equals p+q .

This equation can always be solved in closed form once σ(N) is known. Fortunately most advanced computer math problems such as MAPLE and MATHMATICA can produce sigma values in sub-second time intervalls for Ns of less than 40 digit length. Above this, such as for the 100 digit length semi-primes involved in modern day public key cryptography, things at this time can not yet be evaluated even using the fastest supercomputers and methods such as elliptic curve factorization or grid methods. As will be shown below, we can get around this shortcoming of the sigma function by using a new factorization method which uses only the value of N and its integer adjusted square root to find x=[p,q].

Let us elucidate our new approach for factoring any semi-prime by starting with the important equality that

$$\sigma(N)=\text{the sum of all divisors of } N=!+p+q+N$$

and that the sigma function for semi-primes is always an even number. The latter observation can be seen in the examples σ(15)=1+3+5+15=24 and σ(319)=1+11+29+319=360. Also we can introduce the related sigma form –

$$\sigma_0(N)=1+\text{sqrt}(N)+\text{sqrt}(N)+N=(1+\text{sqrt}(N)]^2$$

following by setting p=q=sqrt(N). By adjusting the sqrt(N) to its nearest even integer, we see that

$$\sigma(N)-\sigma_0(N)=2n \quad \text{with } n=0,1,2,..$$

Next, rewriting the above quadratic equation we get-

$$x^2-2x[sqrt(N)+n]+N=0$$

The solution of this new equation yields the prime factors x=[p,q] once sqrt(N) is replaced by its nearest integer. What is most interesting about this quadratic is that σ(N) no longer appears explicitly. This means that the 40 digit size restriction on N for finding σ(N) no longer holds . It means in theory one can now handle semi-primes in the 100 digit long form as encountered in public key cryptography

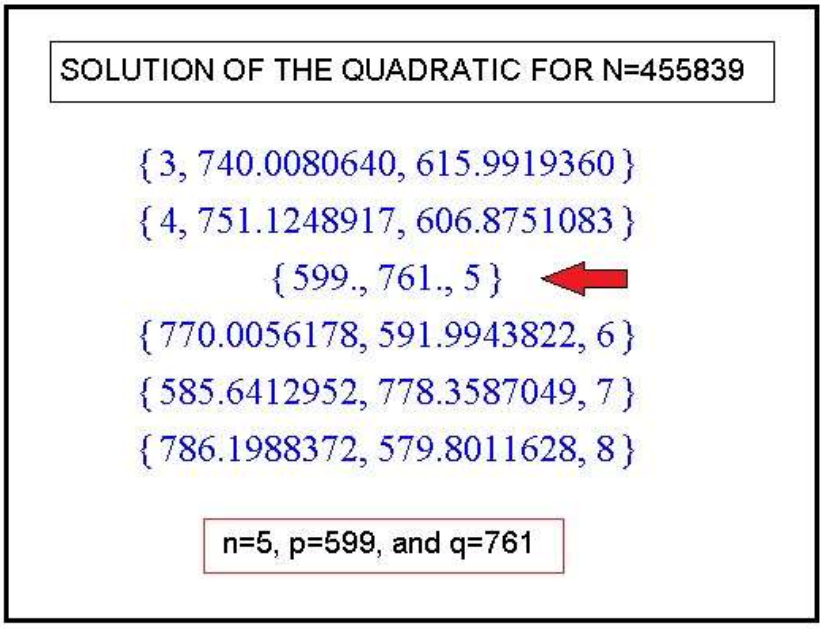
Let us demonstrate the present method for the semi-prime-

N=455839 where sqrt(N)=675.158

The following one line program in MAPLE will factor this N as follows-

```
for n from 2 to 8 do({n,solve(x^2-2x (675+n)+455839=0,x)})od;
```

Running the program produces the table-



This solution is obtained in sub-second run times starting with n=0. At n=5 we arrive at the answer–

x=[p,q]=[599,761]

We point out that this particular semi-prime has been used earlier in the literature to demonstrate the elliptic curve factorization method of Lenstra. Our present approach is much much faster and as seen requires no fancy mathematics..

In theory, this new approach does not require explicit values for σ(N).Thus it should be applicable for any semi-prime. Jts only noted drawback is that the value of n can become quite large requiring numerous trials until the right integer value for n is found.

Let us consider a second specific example, namely,-

N=67237033 where the adjusted root is sqrt(N)=8200

Evaluating the program-

for n from 0 to 200 do{{n,solve(x^2-2*x*(8200+n)+67237033=0,x)})od;

produces x=[6719,10007] at n=163 in a split second. Note that for this last example it took a total of 163 trials to get the answer. This is not a problem when one looks at the simple mathematical manipuations involved. Note also that our PC gives directly the sigma function as

σ(N)=67253760

This sigma function can be plugged into the first quadratic equation at the beginning of this article to recover the same two values for x. The advantage of the present approach is that we no longer need σ(N) directly for finding x=[p,q].

An important new result provided by our N-sqrt(N) approach is that we can now generate σ(N) directly from-

[σ(N)-N-1]=2[sqrt(N)+n]

Thus if x has been found using the right side of this equality, the sigma function will have been found. This should continue to work even when σ(N) exceeds 40 digit length. We generate the sigma function from the quality-

σ(N)=1+N+2[sqrt(N)+n]

Applying this resut to the semi-prime N=455839 where n=5 and sqrt(N)=675 adjusted, produces-

σ(455839)=1+455839+2(675+5)=457200

This equals precisely what my PC predicts for σ(455839).

U.H.Kurzweg
November 10, 2022
Gainesville, Florida