DECOMPOSITION OF SEMI-PRIMES

A semi-prime is defined as N=pq , where p and q are its prime components. It is easy to construct a semi-prime from its two prime components but extremely difficult to reverse the procedure and break a semi-prime into its components when N gets large. It is this fact which makes semi-primes ideal for public keys in cryptography. t is our purpose here to relook at the problem of factoring large semi-primes based on a different approach not recognized by other approaches.

We start with the basic new definitions –

S=(p+q)/2=[σ(N)-N-1]/2 and R=(q-p)/2

Here sigma(N) is the summation formula encountered in number theory, S represents the mean value of p and q. R is half the distance between q and p with q>p. In terms of these variables we can write after a little manipulation that-

[p,q]=S$\mp R = S \mp \sqrt{S^2 - N}$

Since p q and S are integers, it is also necessary that the radical R be an integer. The factoring problem thus reduces to finding a positive integer value of R, namely,-

R= Int.=sqrt(S^2-N)

From this the following ps and qs are obtained-

p=S-sqrt(S^2-N) and q=S+sqrt(S^2-N).

To demonstrate the effectiveness of this general solution, take the small semi-prime N=77 , where R=sqrt(9^2-77)=2. Thus the prime factors are p=7 and q=11.

When N gets large, the finding of S (which makes R a positive integer) will require multiple trials using different integer S greater than sqrt(N) or a knowledge of the value sigma(N).

Let us next factor the six digit long semi-prime-

N=455839 , where sqrt(N)=675 =S_{min} to the nearest integer.

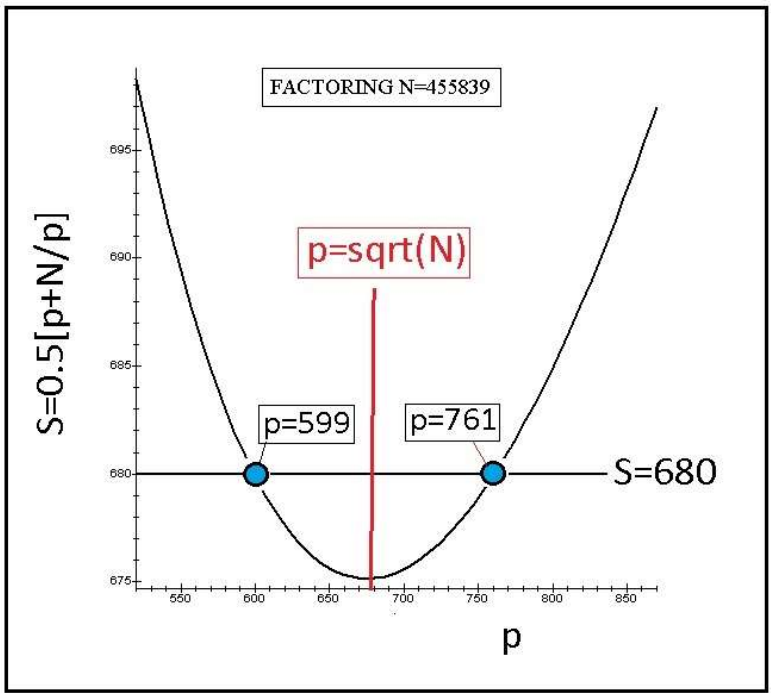
To find integer R we use the one line search program-

for S from 675 to 685 do ({S,evalf(sqrt(S^2-N))})od;

This produces after five trials the result R=81 for S=680. Hence we have the factors p=599 and q=761 An alternate way to get this result is to go directly to my PC to find σ(455839)=457200.

Hence S=[σ(N)-N-1]/2=680. This second approach is faster but works only for Ns smaller than about forty digit length.

A geometrical description for factoring N=455839 follows-



We see that the curve S=[p+N/p]/2 represents an un-symmetric parabola with a minimum at S=sqrt(N). The integer value for S first occurs at S=680. This lies some five units above sqrt(N) requiring five trials. The corresponding R=81. Note that p and q always have the same integer value for S.

To demonstrate the effectiveness of the present approach of factoring still larger Ns consider the 30 digit long semi-prime-

N:=336012709462653305275991544713

Here our PC yields-

S:=2524330965584067 and R=[sqrt(S^2-N)=2456874867457424

In a split second. Hence we have the factored primes-

p:= 67456098126643 and q:=4981205833041491

Multiplying p and q together yields N and hence the answer must be correct.

Should one be able to use the present σ(N) approach for the factoring of public keys of 100 digit length or so using supercomputers, it will call into question the use of "unbreakable" public keys used in present day electronic cryptography.

We have shown above via several examples that the factoring of semi-primes N involves just thee unique parameters. They are-

N=pq S=[p+q]/2=[σ(N)-N-1]/2 and R=[q-p]/2=sqrt(S^2-N)

Every semi-prime will be characterized by its own unique triplet {N,B,R] . A brief table showing eight of an infinite number of these follow-

Semi-Prime, N=pq	Mean Value, S=[p+q]/2	Half Difference R=sqrt(S^2-N}
15	4	1
35	6	1
77	9	2
779	30	11
3007	64	33
22601	165	68
455839	680	81
9436561	3119	540

On sees that N>S>R. Also p and q can be read off as S∓R. The sigma function σ(N)=2S+N+1. Thus σ(77)=18+77+1=96. Given the triple [N,S,R]=[24617,70,27], what will be the solution [p,q] and the minimum value of S in an S versus p curve? Note that S and R have opposite symmetry.

One can think of the triplet [N,S,R] as new subclass of numbers in number theory with numerous not so obvious identities. For example, we have N=S^2-R^2. That is, 9436561=3119^2-540^2. Also one can construct S. R, and N starting with prime values for p and q chosen randomly. Here is a table-

Q	p	S=[p+q]/2	R=[q-p]/2	N=S^2-R^2
13	5	9	4	65
17	11	14	3	187
41	23	32	9	943
59	23	41	18	1357
123	97	110	13	11931
541	317	429	112	541317
3217	1319	2268	949	131983217

Another identity is-

$$(S^2+R^2)=(p^2+q^2)/2$$

So at N=943, we have-

$$(32^2+9^2)=(41^2+23^2)/2=1105$$

The simplest way to factor any semi-prime N=pq goes as follows-

1.-Pick a Semi-Prime
2.-Use your PC to find σ(N)
3.-Evalute S=[σ(N)-N-1]/2
4.-Solve for R=sqrt(S^2-N)
5.-Get the result p=S-R and q=S+R

U.H.Kurzweg
July 23, 2021
Gainesville, Florida