FACTORING LARGE SEMI-PRIMES Using S=[σ(N)-N-1]/2

One of the remaining unsolved problems in number theory is to find a quick way to factor large semi-primes of the form N=pq, where p and q are all primes of the form 6n±1 with n≥1. Symbolicaly, we have shown in earlier articles on our MATHFUNC page, that any semi-prime will factor as-

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

, where S=(p+q)/2=[sigma(N)-N-1]/2. Here the sigma function sigma(N) represents the sum of all divisors of N including N and 1. For Ns of less than about 40 digit length the value of σ(N) follows directly in an split second via ones PC using any advanced mathematics program such as Maple or Mathematica. However, when N exceeds this number of digits, as it does for public keys in cryptography, the factoring time required becomes prohibitively long. It is our purpose here to see what the actual limitations are on factoring N as S is allowed to increase.

We begin with constructing a table of factors [p,q] starting with some smaller Ss. Here is such a table-

N	σ(N)	S=[σ(N)-N-1]/2	R=sqrt(S^2-N)	p and q
77	96	9	2	[7,11]
697	755	29	12	[17,41]
3293	3420	63	26	[37,89]
150859	151704	422	165	[257,587]
4416941	4421532	2295	922	[1373,3217]
2603578811	2603683992	52590	12733	[39857,65323]

This table was constructed by finding the values of R and S involving the computer generated value of σ(N).The calculations are accomplished in a split second for each of the Ns shown in the table. The final prime-pairs are given by-

$$[q,p]=S\pm R$$

You will notice that σ(N) is just slightly greater than N and that sqrt(N)<S.

A semi-prime which lies near the limit of my PCs capability is the forty digits long -

N := 1912492750926191821089996842096354214449

My PC, using MAPLE, requires 82 seconds to find that here-

σ(N)= 191249275092619182117880193377264567203 6

From this we have at once that S=44402545838145728793 and R=768721835142210332

Thus-

[p,q]=[36715327486723625473, 52089764189567832113].

A colleage of mine (Dr.R. Fearn,University of Florida, retired) has gone on to factoring an even larger 70 digit semi-prime N using his latest version of Mathematica. It took him a little over one hour to generate σ(10^70) directly.

Clearly what is happening is that it takes longer and longer to find σ(N) as N gets into the 10^100 digit range. However a direct evaluation of σ(10^100) or larger should be possible using the above factoring formula [q,p] . One simply requires a way to find σ(N) for such larger Ns. A two pronged attack to accomplish this will be to *use the latest supercomputers and to use an improved method for finding σ(N) for such larger Ns*. I have no doubt this will become possible shortly, thus making the use of public keys in cryptography obsolete.

U.H.Kurzweg
Gainesville, Florida
Febuary.11, 2021