FACTORING LARGE SEMI-PRIMES USING THE SIGMA FUNCTION

In several earlier articles on this web page we have shown that the primes p and q in a semi-prime N=pq are given by

$[p,q]=S\pm sqrt(S^2-N)$, with $S=(p+q)/2$

At first glance this result says no more than [p,q]=[p,q]. So to get a unique answer it is necessary for the terms p and q in S to disappear. One way to do this (and first recognized by us several years ago) is to note that the summation function for any semi-primes equals-

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

This means that-

$$S=[\sigma-(N+1)]/2$$

Substituting this last result into [p,q] yields the unique closed form solution-

$$\mathbf{[p,q]=(1/2)\{(\sigma-(N+1))\pm\sqrt{\sigma^2-2\sigma(N+1)+(N-1)^2}\}}$$

If one now knows sigma for N, the primes p and q will be given. It is the purpose of this article to find p and q for several large semi-primes.

We begin with the relatively small semi-prime N=77. My computer program (MAPLE) shows that here σ=96. So we get-

$$[p,q]=(1/2)\{(96-78)\pm sqrt(96^2-192(78)+5776)\}=9\pm sqrt(4)=[7,11]$$

As the next semi-prime consider N=31877 for which our computer program yields σ=32256. So we find-

$$[p,q]=(1/2)\{(32256-31878)\pm sqrt(32256^2 \quad -2\sigma(31878)+31876^2)$$

$$=(1/2)\{378\pm sqrt(15376)\}=[127,251]$$

Take next the semi-prime N=455839 where σ=457200. Here we get-

$$[p,q]=(1/2)\{(457200-455840)\pm sqrt(457200^2-2(457200)(455840)+(455838^2))\}$$

$$=(1/2)\{1360\pm sqrt(26244)\}=[599,761]$$

We can factor an additional infinite number of semi-primes using the above formula shown in blue. Here is a table for six additional factorizations for large semi-primes-

N=pq	σ=1+p+q+N
7828229	7833984
169331977	169361280
4294967297	4301668356
70101936959157221369663	70101936959763106877568
8164965809321643374650557094363	8164965809339781368743057430968
19332243053975764648861655842869467707	19332243053975764668065491906109053240

The information found in this table allow us to quickly calculate p and q for the Ns shown. For the largest 38 digit long semi-prime s in the table we have-

[p,q]= (18137993642342178523) (1065842420897407009)

In this case it took 18 seconds to calculate σ(N) with the rest of the calculation performed in a split second with aid of my thinkpad laptop. Note that the search times for σ(N)increase rapidly with further increase in N size. The reverse is true for smaller semi-primes of 30 or shorter lengths where calculations are made in split seconds. Note that σ(N) is always a bit larger than N with the difference becoming smaller as N gets larger. This is important information for anyone wishing to reduce the factorization times for larger semi-primes N such as are used in RSA cryptography. As expected from the definition, the sigma function will always be an even number meaning one does not need to worry about odd values in a σ(N) search.

In summary we can state that the above approach for factoring semi-primes when N=pq gets large appears superior to other known factorization methods. It will become even more effective if ways can be found to speed up the JAVA programming approach for finding σ(N).

U.H.Kurzweg
July 2, 2023
Gainesville, Florida