FACTORING SEMI-PRIMES USING THE SIMULTANIOUS EQUATIONS X+Y=A and XY=B

It is known from earlier articles on this Tech-Page that the two primes x and y of a semi-prime N=xy are given by the solution of the simultaneous equations-

$$xy=N \text{ and } x+y=\sigma(N)-N-1$$

Here N is a known semi-prime and σ(N) is the sigma function of number theory representing the sum of all divisors of N. Thus, for example, N=77 has σ(77)=1+7+11+77=96. Substituting these numbers into the above simutaneous equations produces-

$$xy=77 \text{ and } x+y=18$$

Eliminating either x or y from these equations produces-

$$[x,y]=[7, 11]$$

As a second example consider the semi-prime-

$$N=1327703491 \text{ where } \sigma(N)=137728800$$

Here we find the two equations-

$$x+y=25308 \text{ and } xy=1327703491$$

These can be combined as a single quadratic equation which factors as-

$$[x,y]=[7919, 17389]$$

Note that here the σ(N) term follows directly from the use of a Maple advanced math program and one does not need to add terms manually. The time required to find σ(N) when N is less than twenty digit length follows from our Maple program in a fraction of a second.

This quick evaluation slows down considerably when N approaches forty digits such as for

N=1774319431086405772344947305713375666887

Here, such as occurs for public keys in cryptography, the Maple program yields the sigma function of-

σ(N)= 1774319431086405772436364835972631404176

in about three minutes. Note that σ(N) is always an even number just slightly larger than N. Substitution these values of N and σ(N) into the above simultaneous equations yields the two twenty digit long prime factors-

[x,y]=[27961320846321079937, 634562094129346573 51]

, requiring just an extra split second of computer time. Clearly what is happening is that the present solution route requires longer and longer computer times to find σ(N)when N approaches one hundred digit length as it does in present day public key cryptography. If one could find a quicker way to determine the sigma function for large semi-primes, present day electronic cryptography would become obsolete. So far we have not found a way to do this but I am quite confident that someone in the next few years will find a way to quickly evaluate in a split second σ(N)s for N greater than one hundred digit length.

In the meanwhile let us work out a few additional properties of the simultaneous equations-

x+y=σ(N)-N-1 and xy=N

when N is a large semi-prime. First of all one sees that the sigma function for any semi-prime is-

σ(N)=1+x+y+xy=[(N+x)(1+x)]/x

So we get, if N=77 and x=7, that σ(77)=(77+7)(1+7)/7=96. This is the same value as given above found by adding all devisors of N. Also note that it is always true that

σ(N)=(1+x)(1+y)

This means that if you have the two prime components of any semi-prime, you know what σ(n) will be. Taking the second example above , where N=1327703491, you find-

$$\sigma(N)=(7919+1)(17390+1)=137728800$$

Note again that σ(N) is even and just a little in value above N.

A way to get around needing values of σ(N) for large semi-prime is to take the earlier derived formula –

$$[x,y]=S\pm sqrt(S^2-N)$$

, where S=[σ(N)-N-1]/2.We get rid of the sigma function by rewriting S as [x+y]/2. In this form, we recognize S as being the average value of the two prime components of the semi-prime N. One can then concentrate on the radical which must have a positive integer value.

This means one can carry out a computer search starting with S=sqrt(N). Stopping at the first positive integer value of the radical to yield the departure from the average value of x and y. Let us demonstrate things for the semi-prime N=509081 which has sqrt(N)=713.499. Applying the search formula-

```
for n from 0 to 50 do({714+n,evalf(sqrt(715+1428*n+n^2))})od;
```

we find the radical to be 200 at S=741.Thus we have the factored product-

$$509081=541 \text{ x } 941 \quad .$$

It took a total of 28 simple calculations starting with n=0 to get the radical value of integer 200. This last approach suffers from the same difficulty as when the computer stored sigma function is used. Namely, the number of evaluations increase dramatically as N gets large. Getting around this difficulty is the topic of multiple present day efforts worldwide, but no realy fast solutions have been found so far.

U.H.Kurzweg
September 8, 2024
Gainesville, Florida