USE OF NUMBER SYMMETRY TO FACTOR ANY SEMI-PRIME

We have shown in a previous note on this TECH-BLOG web page that any semi-prime N=pq can be factored into its prime components –

$$[p,q]=(p+q)/2 \mp (q-p)/2 \quad \text{with} \quad p< \sqrt{N} <q .$$

Using the definition of the sigma function σ(N)=1+p+q+N for any semi-prime, we can re-write the above as-

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

Thus if one knows the value of the sigma function, the values of p and q will follow regardless of the magnitude of N. To demonstrate the exactness of the last result we can take the trivial case of N=77 for which σ(N)=96. This yields-

$$[p,q]=(96-1-77)/2 \mp \sqrt{[(96-1-77)/2]^2-77}=9 \mp 2=[7,11]$$

One is fortunate that values of the sigma function up to around forty digit length are given by most advanced computer mathematics programs (such as Maple or Mathematica) in split seconds. Thus the above factoring formula works well for semi-primes with smaller N values but fails by time consumption when trying to factor larger semi-primes above one hundred digit length such as are encountered in public key cryptography. It suggests one find a new way to quickly factor larger semi-primes by expressing σ(N) in an alternate form from its basic definition . It is our purpose here to do this.

We begin with the basic definition for the sigma function for N=pq. It reads-

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

With the exception of p or q being equal to the prime two, we see that both 1+N and p+q are even numbers, thus σ(N) will also always be an even number. Since p is taken as less than sqrt(N) and q is greater than sqrt(N), we can make the <u>symmetry approximation</u> that –

$$(p+q) \approx 2\sqrt{N}$$

This suggests that we can re-write-

$$\sigma(N)=1+2(a+b)+N$$

, where 'a' is the nearest integer to sqrt(N) and 'b' a positive integer to be found.

With this form of σ(N) , the above factorization formula becomes-

$$[p,q]=(a+b) \mp \sqrt{[(a+b)^2-N]}$$

For the case of the semi-prime N=77 discussed above, we have a=9 and b=0. Thus p=7 and q=11. In the general case we will typically have b<<a which means that σ(N) lies only slightly above N.

We next apply the present factorization technique to the semi-prime-

N=455839 , where sqrt(N)=675.1584 so that a=675 .

To get b we solve R which must be an integer-

R=sqrt((675+b)^2-455839).

This occurs for b=5 yielding the integer R=81. It produces the factorization-

[p,q]=(a+b)∓R=680∓81=[599,761]

It is interesting to note that N=455839 has been used in the literature to demonstrate the elliptic curve approach for factoring semi-primes. The elliptic curve approach is actually much slower in factoring semi-primes than the approach used here .

When N gets very large the radical appearing in the factorization will get progressively larger meaning b will also increase in size. Under those conditions it is wise to use the following computer program-

```
for b from 0 to B do({b,sqrt((a+b)^2-N)})od;
```

So if the semi-prime is –

N=4758979 we have sqrt(N)=2181.508 so that a=2182 .

The program produces in a split second that b=120 at R=735. So we get the factors-

[p,q]=(2182+120)∓ 735=[1567,3037]

What is clear from the above examples is that b increases dramatically with increasing size of N but the ratio of b/a approaches zero. With high speed supercomputers the present approach should work for semi-primes of one hundred or larger digits. The advantage of the present factoring approach compared to others is that a good part of the calculations involving large numbers is avoided by noting that a^2 lies fairly close to N, especially when N gets large.

U.H.Kurzweg
March 20, 2024
Gainesville, Florida