LATEST ON FACTORING SEMI-PRIMES

One of the remaining tasks in number theory is to find a way to quickly factor any semi-prime N=pq into its prime components p and q. If this can be achieved for semi-primes of hundred digit or more length, modern day cryptography relying on public keys will become obsolete. Present day computers are not yet able to accomplish this factoring for very large Ns, but it is quite certain that future work using ever higher speed computers and/or quantum-computers will make this possible. We want here to present our latest thoughts on a simple factoring process employing a non-conventional approach.

To do this, we start with the obvious equality –

[p,q]= {Average Value of p and q$\}\mp$ {Half the Distance between q and p}

= (p+q)/2 $\mp(q-p)/2.$

It is assumed without loss of generality, that p<sqrt(N) and q>sqrt(N) and that both p and q are integers. Next we introduce the well known sigma function for semi-primes-

σ(N)=1+p+q+N

plus the newly found number fraction-

f(N)=(p+q)/N

first discovered and defined by us about a decade ago.

Eliminating p and q from these last two definitions, we find-

σ(N)=1+N+Nf(N))

For large N the number σ(N) will be lie just slightly above N and f(N) will be a small rational fraction just slightly above zero. For example, N=77 has σ=96 and f=18/77=(p+q)/pq. Also by inspection we find p=7 and q=11. So by the above definition [p,q] becomes-

[p,q]=(7+11)/2$\mp(11-7)/2$ = 9 ± 2

Now for any semi-prime we have the general statement q=N/p and f=(p+q)/N. This produces the quadratic in p of-

p^2-pNf(N)+N=0

This in turn produces the semi-prime factors of-

[p,q]=Nf(N)]/2∓sqrt{(Nf(N)/2)^2-N}

On eliminating Nf(N) in this last solution we also have the equivalent form-

[p,q[=[σ(N)-1-N]/2 ∓sqrt{[(σ(N) − 1 − N)/2]^2 -N }

Here the average value of p and q is-

Average= [Nf(N)]/2=[σ(N)-1-N]/2

and –

HalfDiff=sqrt{(Nf(N)/2)^2-N}=sqrt{[(σ(N)-1-N)/2]^2-N}

Thus we can always find the prime components of any semi-prime if either f(N) or σ(N) are known. Fortunately the values of the sigma function are recognized by most advanced mathematics programs such as MAPLE or Mathematica to at least forty digit Ns. So the factoring of any semi-prime up- to about forty digits can be gotten in a split second. Let us demonstrate the above method for the 24 digit long semi-prime-

N=640209797372372884407071

Here it takes only a split second using MAPLE to show that-

σ(N)= 640209797374004940164544

In this case the Average =816027878736 and the HalfDiff= 160286311025 . So we get -

p=Average-HalfDiff= 655741567711 and q=Average+HalfDiff= 976314189761 . Thus we have been able to factor the above 24 digit long semi-prime into two twelve digit primes with a minimum of effort compared to present less successful methods such as the elliptic curve techniques or generalized grid methods. If some new method for quickly finding values of sigma(N) or f(N) can be discovered, the present method of factoring semi-primes will make present day cybersecurity, relying on the use of public keys, obsolete.

We point out a few additional observations concerning the present semi-prime factoring technique. Here they are-

(1)-Neglecting the prime p or q of 2, the difference between q and p is always an even integer.

(2)-The sigma function σ(N) is an even function related to the number fraction via f(N)=[σ(N)-1-N]/N.

(3)-The numbers N, p and q all have the form 6n±1, where the integer n equals one or greater. So for N=77=6(13)-1, p=6(1)+1=7, and q=6(2)-1=11.

(4)-Without loss of generality, one has p<sqrt(N) and q=N/p>sqrt(N)

(5)-An approximation for f(N)≈2/sqrt(N) so that σ(N)≈ [I+2sqrt(N)+N].

(6)-The Fermat number 2^32+1 is a composite 641 x 6700417 as first shown by Euler and an almost trivial exercise today using the present approach.

U.H.Kurzweg
March 12, 2024
Gainesville, Florida