MORE ON FACTORING SEMI-PRIMES

In the last few years I have spent some time examining prime numbers and their properties. Among some of my new results are the a **Prime Number Function F(N)** and the concept of **Number Fraction f(N)**. We can define these quantities as –

$$f(N)=\frac{\sigma(N)-N-1}{N} \quad and \quad F(N)=\frac{f(N^2)+1}{Nf(N^3)}$$

Here σ(N) is the divisor function of number theory. The interesting property of these functions is that when N is a prime then f(N)=0 and F(N)=1. For composite numbers f(N) is a positive fraction and F(N) will be less than one. One of the problems of major practical interest in number theory is how to rapidly factor large semi-primes N=pq, where p and q are prime numbers. This interest stems from the fact that encoded messages using public keys are vulnerable to decoding by adversaries if they can factor large semi-primes when they have a digit length of the order of 100. We want here to show how one might attempt to factor such large primes by a brute force approach using the above f(N) function.

Our starting point is to consider a large semi-prime given by-

N=pq with p<sqrt(N)<q

By the basic definition of f(N) we get-

$$f(N)=f(pq)=\frac{p+q}{N}=\frac{p^2+N}{pN}$$

This may be written as a quadratic in p which reads-

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

It has the solution-

$$p=K-\sqrt{K^2-N} \quad , \quad with \quad p<\sqrt{N}$$

Here K=Nf(N)/2={σ(N)-N-1}/2. The constant K will always be an integer. The second prime follows via q=N/p.

To show you how simple it is to factor a larger semi-primes by this brute force approach consider N=455839. This is a semi-prime often used to demonstrate Lenstra elliptic curve factorization. We

show here how the factorization can be accomplished with very little effort. One finds that K=680 so that-

$$p = 680 - \sqrt{462400 - 455839} = 599$$

The second factor is -

$$q = \frac{N}{p} = \frac{455839}{599} = 761$$

Another semi-prime easily factored is the Fermat number $2^{32}+1$=4294967297. Leonard Euler first factored this number several hundred years ago. His ability to do so is quite amazing considering he had no access to any sort of calculating machine except pencil and paper and a brilliant mind. Let us factor this Fermat number. We find K=3350529 so that-

$$p = 3350529 - \sqrt{3350529^2 - 4294967297} = 641$$

The second factor is-

$$q = \frac{N}{p} = \frac{2^{32}+1}{641} = 6700417$$

We could also get this last value for q by replacing the minus sign in the above p formula by a plus sign.

Let us next push my MAPLE math program to its limits by looking at the twelve digit semi-prime-

N= 589937256521 where we find K= 854589

Substituting into the p formula, we get-

$$p = 854589 - \sqrt{854589^2 - 589937256521} = 479909$$

and-

$$q = \frac{589937256521}{479909} = 1229269$$

That is-

$$89937256521 = 479909 \; x \; 1229269$$

Although my PC (using MAPLE) cannot rapidly calculate K for semi-primes in excess of 13 digit length or so, there is no reason to think that someone with a faster computer should not be able to factor larger semi-primes such as-

N= 85397342226735670654637567334028930584606539118838378 3

To construct this semi-prime I generated two primes based on the constants exp(1) and π. The primes are-

p=2718281828459045235360353 and q=3141592653589793238462643383 11

Although my PC cannot factor this N in any reasonable length of time, we can work things backwards to show that here-

$$K=\frac{1}{2p}\{p^2+N\}=\frac{(p+q)}{2}=157080991820403891445749849332$$

From this result one can conclude that-

σ(N)=N+1+2K=85397342226735670654637598750227294665384828268808 2448

and-

$$f(N)=\frac{\{\sigma(N)-N-1\}}{N}=\ 3141619836408077828914996986 64/\ N$$

See if any of you (with a more advanced computer system) can come up with the value of K for this last example without knowing the values of p or q beforehand. If you can do this, then in effect you have shown how to factor a 55 digit long semi-prime and are in a position to break many of the extant public keys. Note that if you take any two primes p and q you can write down N=pq, K(N), f(N), and σ(N) at once. Here is a small table-

p	q	N=pq	K=(p+q)/2	f(N)=(p+q)/N	σ(N)=Nf(N)+N+1
7	11	77	9	18/77	96
29	67	1541	45	90/1541	1632
127	439	55753	283	566/55753	56320
36701	76379	2810059789	56585	113170/N	2810172960

In view of the above, it seems very likely that security agencies such as NSA in this country and their counterparts in Russia and China can decode any intercepted electronic communication encrypted with the use of public keys less than about 100 digit length. It may therefore become necessary in the near future to dispense with encryption all together and rather communicate by stealth methods such as electronic versions of self-destructing microdots. Messages will always be secure if an adversary does not recognize a message has been sent or is being sent.

July 21, 2014
Gainesville, FL