A QUICK WAY TO FACTOR LARGE SEMI-PRIMES

In several earlier articles found in both our MATHFUNC and RIC'S TECH BLOG pages we have discussed prime-numbers, the number fraction f(N), and a new prime-number function F(N)=[f(x^2)+1]/f(x^3). We want here to combine all this information to indicate a quick (but brute force) approach to factoring large semi-primes.

Our starting point is any semi-prime N=pq, where p and q are unknown primes. The number fraction for such numbers equals-

$$f(N) = \frac{\sigma(N) - (1+N)}{N} = \frac{(p+q)}{N}$$

We thus have two equations involving p and q. These are-

$$N = pq \quad and \quad Nf(N) = p+q$$

Eliminating q, we get the quadratic equation-

$$p^2 - p\{Nf(N)\} + N = 0$$

which has the solution-

$$p = \frac{1}{2}[Nf(N)] \pm \sqrt{[\frac{Nf(N)}{2}]^2 - N}$$

The factoring problem is thus reduced to quickly finding the value of Nf(N).

Let us demonstrate the procedure for several examples involving larger semi-primes. We begin with the eight digit semi-prime N=21428053. It produces an Nf(N) of 9334. From this we immediately have-

$$p = 4667 \pm \sqrt{352836} = 4073 \quad or \quad 5261$$

Thus one finds p= 4073 and q= 5261. Note here that both p and q are what we term Q primes since p=6(679)-1 and q=6(877)-1. That p and q have the same sign in the -1 appendage could have been anticipated from the fact that N mod(6)=1.

We next consider the ten digit number–

N=2^{32}+1=4294967297 for which we find Nf(N)= 6701058

so that-

$$p \text{ or } q = \frac{6701058}{2} \pm \sqrt{(\frac{6701058}{2})^2 - 4294967297} = 3350529 \pm 3349888$$

That is, p=641=6(107)-1 and q=6700417=6(1116736)+1. Note the opposite sign in the p and q appendages. This is consistent with the fact that N mod(6)=5. This semi-prime is of historical interest since it was the first Fermat Number F[n]=2^2^n+1 to be proven to be a composite. To date none of the Fermat numbers with n=5 or greater has been found to be prime although a definitive proof of this fact has not been given. A violation of the composite nature of Fermat Numbers above n=4 would be given if someone finds a zero value for the number fraction f(2^2^n+1) for any n≥5.

Consider next the even larger semi-prime-

N=52190007682269149553406649 3 for which we find Nf(N)= 49665335458974

It produces the result-

p=15098125637513 and q=34567209821461

To be able to obtain this last result in a split second on our home PC is quite amazing since the Nf(N) determination already involves looking for all factors of N.

Finally we study a semi-prime lying near the maximum size for which our PC (using the MAPLE math program) can determine Nf(N) in less than five seconds . The 30 digit long semi-prime under consideration is-

N=194920496263521028482429080527

for which our computer finds -

Nf(N)= 962570796312952

after less than a 2 second run. This result yields the prime factors-

p=289673451203483 and q=672897345109469

If one attempts to factor semi-primes in excess of 30 digit length, our computer will try to carry out the calculations required for determining Nf(N) but will be unable to reach an answer in a reasonable length of time. We tried an evaluation of Nf(N) for a 40 digit long semi-prime but were unable to find a result after a ten minute computer run on our home PC. Higher speed computers should be able to overcome this limitation. One can be almost certain that agencies such as the NSA (and foreign adversaries) are able to quickly break semi-primes of several hundred digit length and hence are able to read any encrypted messages involving the use of public keys when electronic transmissions over the internet, telephone lines, optic cable or microwaves are involved.

U.H.Kurzweg
Christmas 2013