EVALUATION OF THE POINT FUNCTION Nf(N)

We have shown in several earlier articles appearing on this Web Page that semi-primes N=pq can be factored into their prime components p and q by solving the quadratic equation-

\[ [p,q]^2 - Nf(N)[p,q] + N = 0 \]

Here f(N) is the number fraction defined as-

\[ f(N) = \frac{\sigma(N) - N - 1}{N} = \text{Sum of all divisors of N not 1 or N}/N \]

, with \( \sigma(N) \) being the sigma function of number theory. The number fraction f(N) has the interesting property that it vanishes whenever N is a prime. Furthermore one finds for all semi-primes that-

\[ f(N) = \frac{(p+q)}{N} \]

Since we know that N=pq , we can eliminate q to find-

\[ p^2 - pNf(N) + N = 0 \]

If instead one eliminates p, one finds-

\[ q^2 - qNf(N) + N = 0 \]

So p and q are interchangeable and produce the above two roots \[ [p,q] \] of the original combined equation. In effect , this result says is that knowledge of the value of the point function Nf(N) is all that is required to find the two components of any semi-prime. That is, you need only to determine-

\[ Nf(N) = \sigma(N) - N - 1 \]

and the rest of the factoring becomes trivial. One is fortunate that the values of \( \sigma(N) \) are available in most computer mathematics programs such as MAPLE up to quite large values of N, since N has only two divisors for any semi-prime when 1 and N are neglected.

Let us demonstrate the procedure for the six-digit long semi-prime-

\[ N=455839 \text{ where N mod(6)=1 and } \sqrt{N}=675.158. \]
This number is of some interest from a historical viewpoint since it is often used to demonstrate the Lenstra elliptic curve method for factoring semi-primes. If we take \( p < q \)

One has at once that \( p = (\alpha)675.158 \) and \( q = (1/\alpha)675.158 \), with \( \alpha \) being an unknown constant \( 0 < \alpha < 1 \). Using the one line math program-

\[
N := 455839; \quad \text{evalf}(\sigma(N)-N-1);
\]

we have the integer result \( Nf(N) = 1360 \) instantaneously. So the quadratic-

\[
[p,q]^2 - [p,q]1360 + 455839 = 0
\]

produces the prime factors-

\[
p = 599 \quad \text{and} \quad q = 761
\]

The speed with which this result was obtained is far superior to the Lenstra elliptic curve approach.

As another example of factoring, take the ten digit long Fermat number-

\[
N = 2^{32}+1 = 4294967297 \quad \text{where} \quad N \mod(6) = 5
\]

This time our math program yields-

\[
Nf(N) = 6701058
\]

in a split second. Substituting this integer result into our quadratic equation produces at once the roots-

\[
p = 641 \quad \text{and} \quad q = 6700417
\]

Leonard Euler was the first person to show that this number, thought by Fermat to be a prime, is a composite. That he was able to actually factor the number in the pre-electronic computer days of 1736 is truly amazing. He probably tried the division \( N/(6n-1) \) from \( n=1 \) through \( 107 \) at which point he got the integer \( 4294967297 \).

We next go on to even larger semi-primes in the range of 10 to 22 digit length. This produces among many others the following five factored semi-primes \( N = pq \). Their values for \( Nf(N) \) and the corresponding prime components are given in the table-

<table>
<thead>
<tr>
<th>Semi-Prime, N</th>
<th>( Nf(N) = \sigma(N)-N-1 )</th>
<th>p</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td>1927988213</td>
<td>90486</td>
<td>34337</td>
<td>56149</td>
</tr>
<tr>
<td>194223678877</td>
<td>889058</td>
<td>386871</td>
<td>502687</td>
</tr>
<tr>
<td>225476696539</td>
<td>972020</td>
<td>382429</td>
<td>589591</td>
</tr>
<tr>
<td>32391050471337716069</td>
<td>2665418145510</td>
<td>12152389</td>
<td>2665405993121</td>
</tr>
</tbody>
</table>
The calculations for \( N_f(N) \) in all these cases were produced in a split second each making the factoring of any twenty-two digit or shorter semi-primes a trivial problem.

We next go on to an even larger semi-prime of 32 digit length. The simplest way to construct such an \( N \) is to start with two prime numbers of half this length taken from parts of an irrational number product calculation. The irrational number combination used is an open choice, so we carried out the following calculation to sixty places-

\[
evalf(\exp(2)\sqrt{7}, 60) = 19.5496048612755770334568473639150468670990109275999492109917
\]

Next taking the 16 digit long segment-

\[
p \approx 6048612755770334
\]

and adjusting the last two digits till a prime is found. This occurs for-

\[
p = 6048612755770331
\]

Likewise we approximate \( q \) by the segment-

\[
q \approx 3915046867099031
\]

Adjusting the last two digits produces the prime-

\[
q = 3915046867099033
\]

Hence we have the 32 digit long semi-prime-

\[
N = 23680602419773882820145180189923
\]

Running \( N_f(N) \) for this \( N \) we get the integer solution-

\[
N_f(N) = 9963659622869364
\]

in approximately 30 seconds of computer run-time. Substituting this value into our quadratic equation produces the above given values for the prime factors in a split second. What we notice is that the calculation times for \( N_f(N) \) are getting longer. One expects this to continue as \( N \) gets even larger. We demonstrate this fact by attempting to factor the following 42 digit long \( N \) using the \( N_f(N) \) approach. Here we start with-

\[
N = 179801603109022530754264862089925963662693
\]
again constructed not by a random number generator but rather using segments of a secret irrational number combination. The construction of the number took only a few seconds. This time an evaluation of $N_f(N)$ required 4.5 minutes on my home PC. The integer result for $N_f(N)$ reads:

$$N_f(N) = 881497382191045239866$$

From it we at once recover the two roots of the quadratic which are-

$$p = 320508075688772935219 \quad \text{and} \quad q = 560989306502272304647$$

Although it becomes impractical to try to factor even larger $N$s on our home PC because of the observed rapid increase in time required to find $N_f(N)$, I have no doubt that using one of the latest super-computers that semi-primes of 100 and larger digit length can be factored by the present approach. Such a factoring should be of interest to people involved in public key cryptography as it may make this form of secure message exchange obsolete.

U.H.Kurzweg
July 9, 2018
Gainesville, Florida