INTRODUCTION:

There are two types of semi-primes $N=pq$ whose components are both greater than three. These constitute what we have called the Q Primes in earlier notes. They are characterized by either:

$$N \mod(6)=1 \quad \text{or} \quad N \mod(6)=5$$

Examples of the first and second type are $N=50297791$ and $N=33414839$, respectively. We have already discussed the $N \mod(6) =1$ case in detail in a preceding note. This time we concentrate on factoring semi-primes of the form $N \mod(6)=5$ which means $N$ may be expanded as:

$$N=(6n-1)(6m+1)$$

As before we will try to obtain a universal curve of $N$ versus an adjustment parameter $k$. Once a certain radical $R$ has been evaluated the values of the prime components $p$ and $q$ follow.

DEVELOPING FORMULAS FOR $n$ AND $m$ WHEN $N \mod(6)=5$:

To find $n=(p+1)/6$ and $m=(q-1)/6$ we first expand things as:

$$6 nm-(m-n)=(N+1)/6=A$$

On setting $x=nm$ and $y=m-n$, we obtain the linear Diophantine equation:

$$6x-y=A$$

For large $N$ we have that $6x \approx A$ since generally $nm>>(m-n)$. Also, since $x$ and $y$ are integers we have to adjust $A$ by $A-A \mod(6)$. Calling $A \mod(6)=H$, we get the solution:

$$x=B+k \quad \text{and} \quad y=(-H+6k)$$

where $B=(A-H)/6$ and $k$ is an adjustment parameter small compared to $A$. We can now solve for either $n$ or $m$ by eliminating one or the other. First letting $m=(B+k)/n$, we get:

$$n^2 -(H - 6k)n - (B+k) = 0$$

Solving for $n$ we get:
Also one can solve for m by eliminating n to get-

\[ m = \left( \frac{1}{2} \right) \left\{ (-H + 6k) + \sqrt{(-H + 6k)^2 + 4(B + k)} \right\} \]

Subtracting n from m we find as expected that-

\[ y = m - n = -H + 6k \]

Also-

\[ x = nm = B + k \]

We call the radical appearing in the n and m solutions R. It is the finding of k which makes the radical an integer which is the most difficult part of the factoring procedure.

**EVALUATION OF R:**

The key to factoring N when \( N \mod 6 = 1 \) is to find the value of k which makes the above radical R an integer. Once this has been accomplished the rest of the factorization leading to the values of p and q becomes straightforward.

For smaller N this process of finding an integer value for R is quite easy using the program-

\[
\text{for } k \text{ from } 1 \text{ to } b \text{ do } \{k, \text{evalf(sqrt((-H+6k)^2+4*(B+k)))}\}\text{ od;}
\]

So, for example, if \( N = 731 \) we have \( H = 2 \) and \( B = 20 \). So the radical becomes \( R = \sqrt{36k^2 - 20k + 84} \). Its solution is \( R = 10 \) at \( k = 1 \). Hence we have-

\[ n = (2-6+10)/2 = 3 \quad \text{and} \quad m = (-2+6+10)/2 = 7 \]

, from which follow-

\[ p = 6(3) - 1 = 17 \quad \text{and} \quad q = 6(7) + 1 = 43 \]

For larger \( N \) a brute force approach of starting the search at \( k = 1 \) becomes impractical especially when dealing with semi-primes of fifty to a hundred digit length such as are encountered in public key cryptography. In these cases one needs to find a better starting point for k. After years of thought devoted to this task, it dawned on me about a year ago that one should be able to come up with a good estimate for a good starting value for k by looking at the reverse problem of generating a table and graph of precise values for N and
k for specified values of \(n\) and \(m\). This approach worked well for our earlier \(N \mod(6)=1\) factorization and is expected to also work here.

We begin with generating a graph of the points \([\log(N), \log(|k|)]\) using the simple MAPLE program:

\[
\begin{align*}
n := 3; & \quad m := 7; \quad \text{isprime}(6*n-1); \quad \text{isprime}(6*m-1); \quad p := 6*n-1; \quad q := 6*m+1; \quad N := p*q; \\
evalf(\log10(N)); & \\
A := (N+1)/6; & \quad H := A \mod(6); \quad B := (A-H)/6; \\
k := (1/36)*(N-1-6*H-(p-1)*(q-1)); & \quad \text{evalf}(\log10(k));
\end{align*}
\]

by varying \(n\) and \(m\). It produces the following graph-

As in our earlier study of semi-primes where \(N \mod(6)=1\), we find here a nearly straight line for the exact points shown as red circles. We can approximate the trend by the formula-

\[
\log(N) = 3.7 + 2 \log(|k|)
\]

This is equivalent to the universal Universal Curve-

\[
|k| = \sqrt{N}/[70.7745]
\]
The absolute value sign is kept on $k$ since $k > 0$ when $m > n$ and $k < 0$ when $n > m$. As in the earlier case on $N \mod(6) = 1$, we find again that $|k|$ goes as the square root of $N$. But in general the present $N \mod(6) = 5$ case produces a lower $|k|$ value for a given $N$.

To find the integer value of $R$ we now search the neighborhoods of $+k$ and $-k$. After enough trials the desired integer value for $R$ will be found. Once the integer values of $R$ and the corresponding $k$ have been determined, the rest of the problem becomes straightforward via use of the above $[n,m]$ equations.

**FACTORING OF SEVERAL DIFFERENT SEMI-PRIMES:**

We begin our specific evaluations with the eight digit semi-prime-

$$N = 207143 \quad \text{where} \quad N \mod(6) = 5$$

In this case $A = 34524$, $H = 0$, and $B = 5754$ and our search start will be $|k| = \frac{\sqrt{N}}{70.7745} = 6.43$. So we need to search about $k = 6$ and $k = -6$. The result of three evaluations about $k = 6$ using the program-

```plaintext
for k from 5 to 7 do (k, evalf(sqrt((6*k)^2+4*(5754+k)))}od;
```

produces-

{5, 154.7126369}  
{6, 156.} ←answer [k,R]  
{7, 157.5055555}

Hence we have the solution $R = 156$ when $k = 6$. The rest of the problem is straightforward yielding-

$$n = \frac{-36 + 156}{2} = 60 \quad \text{and} \quad m = \frac{36 + 156}{2} = 96$$

Hence- $p = 6(60) - 1 = 359$ and $q = 6(96) + 1 = 577$.

Note here that the actual required value of $k$ coincides exactly with that suggested by the Universal Curve when evaluated at the nearest integer. This will generally not be the case as $N$ gets larger. Still the present approach will still be much faster than any brute force search starting with $k = 1$.

As the next example we factor the semi-prime-

$$N = 64636973 \quad \text{where} \quad N \mod(6) = 5$$

The nearest integer to $|k| = \frac{\sqrt{N}}{70.7745} = 113.58$ is $k = 114$ or $-114$. Carrying out a search we obtain the integer value $R = 2771$ at $k = -117$. So just 3 integers away from the initial guess of $-114$. Solving for $n$ we get-
\[ n = \frac{1}{2} \{3 + 6(117) + 2771\} = 1738 \]

Likewise for \( m \) we get-

\[ m = \frac{1}{2} \{-3 - 6(117) + 2771\} = 1033 \]

These produce the results-

\[ p = 6(1738) - 1 = 10427 \quad \text{and} \quad q = 6(1033) + 1 = 6199 \]

Note that for this example we had a negative \( k \). This follows from the fact that here \( n > m \). It is of course something we did not know until after \( R \) was solved.

For our last example consider the ten digit long number-

\[ N = 9540703223 \quad \text{with} \quad N \mod(6) = 5 \]

Here \( A = 1590117204, H = 0, \) and \( B = 265019534 \). Our Universal Curve predicts we should expand around \(|k| = \sqrt{N}/707745 = 1380\). Doing so we find the correct \( k = 1490 \) which yields the integer value \( R = 33764 \). So we find-

\[ n = \frac{1}{2} \{-6(1470) + 33764\} = 12412 \]

This means \( p = 6(12412) - 1 = 74471 \) so that \( q = 9540703223/74471 = 128113 \)

It took us a total of \( 1490 - 1380 = 110 \) trials to get our answer. That is, is took some 13.5 times less effort than the use of a brute force search starting with \( k = 1 \).

**CONCLUDING REMARKS:**

From the present article and the preceding article on this web page we have succeeded in factoring all semi-primes of the \( Q \) type. That is for all semi-primes \( N = pq \) which are odd and have neither \( p \) or \( q \) be equal to three. The success of the method can be attributed to the use of two Universal Curves which allow a good starting value for \( k \) needed in a search which makes a certain radical \( R \) an integer. These Universal Curves are-

\[ |k| = \sqrt{N/10^{2.5}} \quad \text{for semi-primes where} \quad N \mod(6) = 1 \]

and-

\[ |k| = \sqrt{N}/70.7745 \quad \text{for semi-primes where} \quad N \mod(6) = 5 \]
Semi-primes up to 14 digits long can be readily evaluated by the present method on our home PC in just a few seconds. With the aide of supercomputers the rapid factoring of semi-primes of length 50 to 100 digits becomes a distinct possibility.

U.H.Kurzweg  
Feb.27. 2018  
Gainesville, Florida