FACTORIZING OF SEMI-PRIMES HAVING THE FORM N MOD(6)=1

In several earlier articles on this web page we have discussed factoring large semi-primes of the form \( N= pq \) where \( p=6n\pm1 \) and \( q=6m\pm1 \). We want here to look in greater detail at the case where \( N \mod(6)=1 \). This involves essentially two possibilities \( N=(6n+1)(6m+1) \) or \( N=(6n-1)(6m-1) \).

For these solution forms we get-

\[
6nm \pm (n+m) = (N-1)/6 = k
\]

We need to retain the plus or minus sign in front of \((n+m)\) since we don’t know beforehand which sign applies. We note that generally the term \( 6nm \gg (n+m) \). This allows one to re-write things as –

\[
nm = \frac{1}{36} \{(N-1) \mp [(\alpha + \frac{1}{\alpha})\sqrt{N} + 2]\}
\]

where \( \alpha \) is a small unknown number lying between 0 and 1. Also \( p=\alpha \sqrt{N} \) and \( q=(1/\alpha)\sqrt{N} \) so that \( pq=N \). For large \( N \) the second term becomes negligible compared to the first so we get the integer approximation–

\[
nm = [(N-1)/36 - H/6] \quad \text{where} \quad H = k \mod(6) = [(N-1)/6] \mod(6)
\]

It allows us to state that –

\[
nm = [(N-1)/36 - H/6] + \epsilon = A + \epsilon
\]

where the term within the square bracket is termed \( A \) and is the integer value closest to \((N-1)/36\). The small integer \( \epsilon \) will have a minus sign when \( N=(6n+1)(6m+1) \) and a plus sign when \( N=(6n-1)(6m-1) \).

Going back to the original above expansion for \( N \), we can eliminate \( m \) to get-

\[
\frac{n[k \mp n]}{(6n \pm 1)} = A + \epsilon
\]

This is equivalent to the following quadratic in \( n \)-

\[
n^2 + n \{6(A + \epsilon) - k\} + (A + \epsilon) = 0
\]
where both positive and negative values of $\varepsilon$ are allowed. For $n$ to be an integer, we require that the radical:

$$R = \sqrt{6(A + \varepsilon) - k^2} - 4(A + \varepsilon)$$

be a positive integer. This is possible for values of $\varepsilon$ in the two ranges where the parabola defined by the square of $R$ is positive. We demonstrate this clearly via the following graph:

For $N=(6n+1)(6m+1)$ we start our $R$ search with $-\varepsilon_0$, and we start the search when $N=(6n-1)(6n-1)$ using $+\varepsilon_0$. Here the $\varepsilon$s are located as indicated on the graph.

To find the integer $\varepsilon$ and its corresponding $R$ we use the search programs:

```plaintext
for $\varepsilon$ from $-(\varepsilon_0+b)$ to $-\varepsilon_0$ do {evalf(R)}od;
```

and:

```plaintext
for $\varepsilon$ from $\varepsilon_0$ to $(\varepsilon_0+b)$ do {evalf(R)}od;
```
since we don’t know beforehand which of the N mod(6)=1 forms we are dealing with.

Having found the correct $\varepsilon$ and $R$ we can then go into the quadratic for $n$ to get-

$$[n,m]=0.5\{(N-1)/6-6(A+\varepsilon)\pm R\}$$

From this will follow the prime components $[p,q]$.

Let us demonstrate the above outlined procedure for factoring three specific large semi-primes. The first of these will be-

$$N=2264221 \text{ where } k=(N-1)/6=377370 \text{ and } A=\left[(N-1)/36-k\text{mod}(6)/6\right]=62895$$

Ploting $R$ versus $\varepsilon$ shows that we should look for an integer $R$ solution for $k< -83$ or $k>83$. Just five trials starting with $\varepsilon=-84$ produce the answer $R=166$ at $\varepsilon=-88$. So we have-

$$[n,m]=0.5\{6(62895-88)-372370 \pm 166\}=[181,347]$$

Hence-

$$p=6(181)+1=1087 \quad \text{and} \quad q=6(347)+1=2083$$

Notice that in this case we never had to look for the alternative possibility of $\varepsilon_0>+83$.

As a second example consider the $N \mod(6)=1$ semi-prime-

$$N= 455839 \text{ where } k=75973 \text{ and } A=12662$$

Here a plot of $R^2$ versus $\varepsilon$ shows we should look at $\varepsilon>37$ and $\varepsilon<-37$. Doing so we find $R=27$ at $\varepsilon=+38$ using just one trial calculation. This in turn produces-

$$[n,m]=0.5\{6(A+38)-k^2\pm R\}=[100,127]$$

So we have the result-

$$p=6(100)-1=599 \quad \text{and} \quad q=6(127)-1=761$$

The speed with which this result was obtained is indeed impressive when compared to the alternate elliptic curve factorization method of Lenstra when applied to this same number.

As a last example we look at the nine digit long semi-prime satisfying $N \mod(6)=1$. It reads-
N = 468863683 with k = (N-1)/6 = 78143947 and A = (N-1)/36 - H/6 = 13023991

Here –

\[ R = \sqrt{6(A + \varepsilon) - k)^2 - 4(A + \varepsilon)} \]

First plotting \( R^2 \) in the range \(-1500 < \varepsilon < 1500\) we get the following parabola this time given values for the coordinates-

Doing an evaluation about \( \varepsilon = \pm 1200 \), we find the solution \( R = 1883 \) at \( \varepsilon = -1243 \). So substituting into the quadratic for \( n \) we have-

\[ [n,m] = [2788,4671] \]

This in turn allows us to write out the prime factors-

\[ p = 6n + 1 = 16729 \quad \text{and} \quad q = 6m + 1 = 28027 \]

Note that the fact that \( \varepsilon \) is here negative means that \( p \) and \( q \) have the definitions indicated.

We have shown in the above that we can factor any size semi-prime \( N = pq \) of the form \( N \mod(6) = 1 \). The procedure consists of first finding a quadratic for \( n \) or \( m \), then plotting the square of the radical \( R \) associated with this quadratic to see what values of \( \varepsilon \) one
should use in starting a search for integer $R$. Once $\varepsilon$ and $R$ have been found, the rest of the calculation for $[n,m]$ and $[pq]$ becomes trivial. We are unaware of any extant factorization method which can match the speed and simplicity of the present approach.

U.H. Kurzweg
May 6, 2018
Gainesville, Florida