A FURTHER NOTE ON FACTORING SEMI-PRIMES

In an earlier note we have shown that a semi-primes $N=pq$ may be broken up into its two components $p$ and $q$ by expanding the semi-prime $N$ as-

$$N=(6n+1)(6m+1) \quad \text{or} \quad N=(6n+1)(6n-1)$$

depending upon $N \mod(6)$ being equal to 1 or 5, respectively. Such an expansion leads to two functions –

$$F(k,N)=[36k-(N+1)]^2-4N \quad \text{and} \quad G(k,N)=[36k-(N-1)]^2+4N$$

which need to be evaluated by varying $k$ until either $\sqrt{F}$ or $\sqrt{G}$ assume an integer value. Once this integer value has been found then $p$ and $q$ follow immediately. The question which arises is –with what value of $k$ does one start the search?. As a first estimate one can try an integer value for $k$ closest to $N/36$. This should be a pretty good starting point for $N>>1$ in view of the original expansions of $N$ given above. To see how one can improve on this starting point we can look at the following figure-

\[ \text{BREAKUP OF A SEMI-PRIME } N=pq \]

It shows that $p$ is a number below $\sqrt{N}$ and $q$ a number above $\sqrt{N}$ . The factors of $N$ thus take the form $p=\alpha \sqrt{N}$ and $q=(1/\alpha) \sqrt{N}$ since $pq=N$. The constant $\alpha$ lies somewhere in the range $0<\alpha<1$. Using the original expansions for $N$, we therefore have the improved initial starting points-

$$k_0 \approx \frac{1}{36} \left\{ N + 1 - \left( \frac{\alpha^2 + 1}{\alpha} \right) \sqrt{N} \right\} \quad \text{for} \quad N \mod(6) = 1$$

and-

$$k_0 \approx \frac{1}{36} \left\{ N - 1 + \left( \frac{\alpha^2 - 1}{\alpha} \right) \sqrt{N} \right\} \quad \text{for} \quad N \mod(6) = 5$$
The problem with these estimates is that one does not know the value of $\alpha$ beforehand. If $p$ and $q$ are close to $\sqrt{N}$ each then $\alpha=1$ but if $p=\sqrt{N}/2$ then $\alpha=1/2$. The choice of $\alpha=1/2$ will probably yield one of the better values for $k_0$. In any case, after having chosen an $\alpha$ one makes the substitution $k=\text{(nearest integer to } k_0) + x$ and then constructs the new function $F(x,N)$ or $G(x,N)$ depending on the $N \mod(6)$ value. Next one applies the computer command-

\[
\text{for } x \text{ from } -\beta \text{ to } +\beta \text{ do } \{x,\sqrt{F} \text{ or } \sqrt{G}\}\} \text{od;}
\]

and stops where the roots of $F$ or $G$ equal an integer. Having found this value, the rest is just simple bookkeeping to recover the values of $p$ and $q$.

Let us demonstrate the factoring for the semi-prime $N=490339$. This has $N \mod(6)=5$ and $\sqrt{N}=700.313\ldots$. Let us take $\alpha=1/2$. Then $G$ becomes-

\[
G=(36k-490338)^2-4(490339)
\]

and-

\[
k_0=[N-1.5\sqrt{N}-1]/36=13594.09805\ldots
\]

So we replace $k$ by $13594+x$. This produces the function-

\[
G(x,N):= (-954+36x)^2+1961756
\]

Doing a computer search about $x=0$ then produces the integer result $\sqrt{G}=2016$ at $x=-11$. So we have $k=nm=13594-11=13583$ and-

\[
p,q = \frac{1}{2} \left\{ \sqrt{G} \mp \sqrt{G^2 - 4N} \right\} = 0.5\{2016 \mp \sqrt{2016^2 - 4(490339)}\} = 283 \text{ and } 1733
\]

So it took only eleven operations to find integer $\sqrt{Q}$. Had we chosen $\alpha=1$ it would have taken thirty operations before an integer value for $\sqrt{G}$ would have been found. This points out the importance of having a value of $\alpha$ near $p/\sqrt{N}$ and suggest one might speed up the operations by trying several different $\alpha$s in $0<\alpha<1$ and evaluate things over the limited range of $-b<x<b$ in each case. With a value of $\alpha$ close to $p/\sqrt{N}$ one is guaranteed that an integer $\sqrt{G}$ will be found using only a small number of $x$ trials.

Let us next look at a six digit $N \mod(6)=1$ semi-prime. The number under consideration is-

\[
N=7362451 \text{ which has } \sqrt{N}=2713.38\ldots
\]

Here we need to find the $k$ which yields an integer value for $\sqrt{F}$ where-

\[
F=[36k-(N+1)]^2+4N
\]
Choosing $\alpha=1/2$, we get $k_0=\left\lfloor (N+1-(5/2)\sqrt{N})/36 \right\rfloor = 204324.1262...$. So $k$ becomes $204324+x$ and $F$ assumes the form:

$$F = (-6788 + 36x)^2 - 29449804$$

Searching about $x=0$ produces the integer solution $\sqrt{F}=2190$ at $x=26$. We would have found fewer required operations had one chosen $\alpha=0.7$, where just two operations would have been needed. Indeed the following table gives one a summary of the number of operations ($x$ trials) required versus $\alpha$ for $N=7362451$:

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$k_0$</th>
<th>$x$</th>
<th>$k=k_0+x$</th>
<th>$\sqrt{F}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>204362</td>
<td>-12</td>
<td>204350</td>
<td>2190</td>
</tr>
<tr>
<td>0.9</td>
<td>204361</td>
<td>-11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.8</td>
<td>204358</td>
<td>-8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.7</td>
<td>204352</td>
<td>-2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.6</td>
<td>204342</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.5</td>
<td>204324</td>
<td>26</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The values for $p$ and $q$ follow from $[\sqrt{F+4N}\pm\sqrt{F}]/2$ and yields $p=1831$ and $q=4021$. Notice from this table that there is one point $k_0=204350$ where $x=0$ produces the desired solution. It falls at $\alpha=0.675$ as can be seen in the following graph.

Again, since we don’t know the value of $\alpha$ to begin with, probably the best starting point for $k$ corresponds to $\alpha=0.5$. Alternatively, since $k_0$ does not vary much in moving $\alpha$ from 1 to 0.5, one could take the average value of $k_0$ at $\alpha=1$ and $\alpha=0.5$. That is, try $k_0=(204362+204324)/2=20443$. With this value we would get $x=7$ and so just seven trials to get our desired answer when factoring $N=7362451$. 
As a third semi-prime consider $N=24623267$. Here $N \mod(6)=5$, so we should use 
$G=[36k-(N-1)]^2+4N$ and $k_0=\{N-1+[(\alpha^2-1)/\alpha]\ \sqrt{N}\}/36$. Trying $\alpha=1$ where $k_0 \approx 683980$ one finds that \sqrt{G}=10308 at $x=77$. So the number factors into-

$$6547, 3761)24623267(410308()24623267(421421, 2$$

The optimum approach for this last example would have been $\alpha=0.758$. But this of course was not known until $p$ had been found.

With the above examples we have shown that the present method of factoring semi-primes can be very efficient especially when one allows for the use several different values of $\alpha$ in the range $0<\alpha<1$. When one chooses a value of $\alpha$ lying close to $p/\sqrt{N}$ it will require only a few $x$ trials to find where either $\sqrt{F}$ or $\sqrt{G}$ is an integer.

U.H.Kurzweg
September 2013