In several earlier articles we have shown a way to quickly factor large semi-primes $N=pq$, where $p$ and $q$ are its prime components. The method depends on the fact that when both $p$ and $q$ are greater than 3 all $N$s, $p$s, and $q$s have their mod(6) operation equal to 1 or 5 without exception. Furthermore the form of the $p$ and $q$ can only have the forms-

$$p=6n+1 \quad \text{and} \quad q=6m+1 \quad \text{or} \quad p=6n-1 \quad \text{and} \quad q=6m-1 \quad \text{when} \quad N \mod(6)=1$$

and-

$$p=6n-1 \quad \text{and} \quad q=6m+1 \quad \text{or} \quad p=6n+1 \quad \text{and} \quad q=6m-1 \quad \text{when} \quad N \mod(6)=5$$

Our purpose here is to derive and further simplify the basic formulas for factoring large semi-primes.

**CASE 1, $N \mod(6)=1$**:  

Here we begin with $(6n+1)(6m+1)=N$ which can be written at once as a Diophantine Equation with solutions-

$$x=nm=B+\varepsilon \quad \text{and} \quad y=n+m=\delta-6\varepsilon$$

Here $\delta=k-6B$ is a small integer, $B\gg\varepsilon$, $k=(N-1)/6$, and $B$ is the nearest integer to $k/6$. We can eliminate $m$ from these last two equations to obtain a quadratic in $n$ which solves as-

$$[n, m] = \left(\frac{1}{2}\right)\{(\delta - 6\varepsilon) \pm R\}$$

with-

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

This last radical needs to be solved for an integer value by varying the unknown integer parameter $\varepsilon$ which is smaller than $B$ but can still have a large value when $N$ is large. To efficiently find the value of $\varepsilon$ we generate an estimate $\varepsilon_0$ which lies close to $\varepsilon$. This is done by noting that $p=\alpha \sqrt{N}$ and $q=\sqrt{N}/\alpha$ when $p<q$. It means that-

$$p + q = (\alpha + 1/\alpha)\sqrt{N} = 6(n + m) + 2 = 6(\delta - 6\varepsilon) + 2$$

But $n+m\gg2$ and $\delta\ll6\varepsilon$, so we get the approximate result-
\[ \varepsilon_o = -\left(\alpha + \frac{1}{\alpha}\right) \sqrt{\frac{N}{36}} \]

As will be seen in a graph shown later in this article the value of \( \varepsilon_o \) between 0.1<\( \alpha \)<1 will be about \( \varepsilon_o = \sqrt{N}/18 \). If \( p << \sqrt{N} \), then the term \( 1/\alpha \) can make \( \varepsilon_o \) quite a bit larger than this.

The basic operation in the factoring process is now to carry out a search to find a positive integer value for \( R \) by varying integer \( \varepsilon \) about \( \varepsilon_o \). The one line computer program for doing this is-

\[
\text{for } d \text{ from } \varepsilon_o-20 \text{ to } \varepsilon_o+20 \text{ do } \{d,R\}\text{od;}
\]

In this evaluation \( \varepsilon_o \) is set to the nearest integer and the range on \( d \) can be reduced or extended depending on the size of \( \varepsilon_o \). Once \( R \) has been found the rest of the problem is straightforward.

The second possibility for an \( N \mod(6)=1 \) semi-prime is to have \( N=(6n-1)(6m-1) \). Keeping the definitions of \( x=nm \) and \( y=n+m \) this produced the same \( R \), \( k \), \( B \) and \( \delta \) as in the earlier product but the sign of \( y \) changes. So we find-

\[
[n,m] = \left(\frac{1}{2}\right)\{(6\varepsilon - \delta) \pm R\}
\]

This time –

\[ \varepsilon_o = +\left(\alpha + \frac{1}{\alpha}\right) \sqrt{\frac{N}{36}} \]

So that the magnitude of \( \varepsilon_o \) stays the same but the sign has changed.

Let us now demonstrate how easy a semi-prime of the form \( N \mod(6)=1 \) can be factored. For this purpose we choose the semi-prime

\[ N= 455839 \quad \text{where} \quad N \mod(6)=1 \]

This number is often used to demonstrate the factoring ability of the Lenstra Elliptic Curve Technique. We find \( k=75973 \), \( B=12662 \), \( \delta=1 \) and \( \varepsilon_o=\pm37.508 \) when \( (\alpha+1/\alpha)=2 \). The \( \pm \) in \( \varepsilon_o \) is required since we don’t know yet which of the two possible forms \( p \) and \( q \) take. Evaluating \( R \) for \( \varepsilon \)s around -38 and +38 yields the integer result of \( R=27 \) at \( \varepsilon=38 \). So the guess for \( \varepsilon \) was right on. The positive sign on \( \varepsilon \) tells us that \( p=6n-1 \) and \( q=6m-1 \). Plugging into the \([n,m]\) solution yields-

\[ [n,m]=(1/2)\{6(38)-1\pm27\}=[100,127] \]
This means-

\[ 455839 = [6(100)-1]x[6(127)-1] = 599 \times 761 \]

The ease with which this factoring was achieved is far superior to application of the Lenstra Method for the same number.

**CASE2, N \text{ mod}(6)=5:**

For case two we start with \( N=(6n-1)(6m+1) \) which can be recast into a Diophantine Equation which has the integer solutions-

\[ x = nm = B + \varepsilon \quad \text{and} \quad y = n-m = \delta - 6\varepsilon \]

Here the definitions of the constants have changed a little now reading \( k=(N+1)/6 \) with \( y=n-m \), \( B \) being the nearest integer to \( k/6 \) and \( \delta=k-6B \). Eliminating \( m \) produces the quadratic equation-

\[ n^2 - n(\delta - 6\varepsilon) - (B + \varepsilon) = 0 \]

This solves as-

\[ [n,m] = \left( \frac{1}{2} \right) \{ (\delta - 6\varepsilon) \pm \sqrt{(\delta - 6\varepsilon)^2 + 4(B + \varepsilon)} \} \]

As a result we have a new \( R \) given as-

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

This differs from the earlier \( R \) in having the sign before 4 be positive. Everything else stays the same using the new definitions. The estimate for \( \varepsilon_0 \) can be established as follows-

\[ p - q = (\alpha - \frac{1}{\alpha})\sqrt{N} = 6y - 2 = 6\delta - 36\varepsilon - 2 \]

Noting that \( 36\varepsilon >> 2(1+3\delta) \), we can write the approximation for \( \varepsilon \) as-

\[ \varepsilon_0 = -(\alpha - \frac{1}{\alpha}) \frac{\sqrt{N}}{36} \]
Note the sign change from the earlier version of $\varepsilon_0$. The integer value of $R$ can now be found by searching for integer $R$ by searching about $\varepsilon_0$. Once this is done the rest of the problem is straightforward leading to the values of the factors $p$ and $q$.

The remaining possibility for $N \mod(6)=5$ is to have $p=6n+1$ and $q=6m-1$. This means essentially switching $n$ and $m$ so that $y=m-n$. It produces the solutions-

$$[-m,n] = \left(\frac{1}{2}\right)\{(\delta - 6\varepsilon) \pm R\}$$

with $R$ retaining its value from the $p=6n-1$ and $q=6m+1$ case. The estimate $\varepsilon_0$ becomes-

$$\varepsilon_0 = +\left(\alpha - \frac{1}{\alpha}\right) \frac{\sqrt{N}}{36}$$

and so equals the negative of the $\varepsilon_0$ obtained for the $p=6n-1$ and $q=6m+1$ case.

We can plot the quantity $36 \varepsilon_0 / \sqrt{N}$ versus the parameter $\alpha$ to get the following graph for all four $p,q$ combinations. It looks as follows for $0.1<\alpha<1$-

**ESTIMATED VALUE OF EPSILON**

FOR $N \mod(6)=1$ (red) AND $N \mod(6)=5$ (blue)

It is noted for the $N \mod(6)=5$ case that the absolute value of $\varepsilon_0$ increases approximately linearly from zero at $\alpha=0$ to $2$ at $\alpha=0.4$. After that it increases more rapidly. It is clear that a good guess for $\alpha$ produces a good estimate for $\varepsilon$ and thus minimizes the number of
trails needed in the search for integer R. Typically one wants to start with a value of \( \alpha = 0.7 \) and search about \( \varepsilon_0 \) in a band of about 0.1 \( \varepsilon_0 \) width. If no integer values for R are found then go on to a lower value of \( \alpha = 0.5 \) and repeat the search. Eventually a value of \( \alpha \) will be found where an integer solution to R results.

We are now ready to factor a semi-prime where \( N \mod(6)=5 \). One such number is-

\[ N=1651797 \quad \text{for which} \quad \sqrt{N}=4063.963213 \ldots \]

Here we find \( k=(N+1)/6=2752633, \ B=458772, \ \delta=k-6B=1, \ \text{and} \ \varepsilon_0 = \pm 82 \) if we take \( \alpha = 0.7 \). Carrying out a search about +82 yields the integer solution \( R = 1433 \) at \( \varepsilon = 78 \). This is only four divisions away from \( \varepsilon_0 = 82 \) telling us that the guess \( \alpha = 0.7 \) was a good guess and that \( p \) and \( q \) have the forms \( p=6n+1 \) and \( q=6m-1 \). We now find-

\[ [-m,n]=(1/2)\{ -467 \pm 1433 \} = [-950,488] \]

This means we have the factors-

\[ 1651797=\{ 6(483)-1 \}\{ 6(950)+1 \}=2897x5701 \]

**CONCLUDING REMARKS:**

The present factorization method for \( N \) works quickly and accurately for semi-primes up to about twelve digit length using my home PC and the math program MAPLE. However, as the digits in \( N \) grow further it becomes more difficult to know which \( \alpha \) to guess in order to have \( \varepsilon_0 \) lie close to the actual value \( \varepsilon \) so that the number of evaluations for finding integer R can be minimized. Also it becomes increasingly difficult to apply the present method when \( \alpha \) lies in the range \( 0<\alpha<0.1 \) since, as the above graph shows, the values of \( 36 \varepsilon_0/\sqrt{N} \) then become quite large. What is noted is that for a given \( \alpha \) the value of \( \varepsilon \) which leads to an integer solution for R increases as the square root of N. Thus a hundred digit long semi-prime \( N \) would be expected to require an integer value of \( \varepsilon \) in the fifty digit range to make R an integer. For an \( N \mod(6)=1 \) semi-prime a rough guess for \( \varepsilon \) is an integer value near \( \sqrt{N}/18 \).

U.H.Kurzweg

December 11, 2016