 FACTORING LARGE SEMI-PRIMES

We have shown in several earlier articles that all primes greater than three have the form 6n±1. These, so called Q Primes, can be conveniently displayed as numbers along two diagonal lines 6n+1 and 6n+5 crossing a hexagonal spiral as shown-

In terms of modular arithmetic, one can say that all Q Primes have the form P mod(6)=1 when P lies along the diagonal defined by 6n +1. Primes along the line 6n-1 have P mod(6)=5. You will note in the diagram that there are certain gaps in the primes along these two diagonals. These points represent the semi-primes 25=5x5, 35=5x7, 49=7x7, etc. Also they may locate numbers made of more than two prime products. What is clear is that there can be only two types of semi-primes. These are

\[ N = 6k+1 = (6n \pm 1) (6m \pm 1) \quad \text{and} \quad N = 6k-1 = 6n \pm 1 (6m \mp 1) \]

They are characterized as N mod(6)=1 or N mod(6)=5. Our purpose here is to show how to quickly factor large semi-primes using these facts.

CASE 1: N=6k+1
For this type of semi-prime we can write-

\[ N = 6k + 1 = (6n + 1)(6m + 1) = 36nm + 6(n + m) + 1 \]
so that \(6nm + (n + m) = (N - 1)/6 = k\)

or we can write-

\[ N = 6k + 1 = (6n - 1)(6m - 1) = 36nm - 6(n + m) + 1 \]
so that again \(6nm - (n + m) = (N - 1)/6 = k\)

From these equalities, we can state that when \(N \mod(6) = 1\), we have the Diophantine equation-

\[ 6nm \pm (n + m) = k \]

Now for large semi-primes one has \(6nm \gg (n + m)\). This suggests that \(nm\) equals to a first approximation the nearest integer to \(k/6\). We define this new integer as-

\[ A = \text{nearest integer to } k/6 = (N - 1)/36 \]

An improved value for \(nm\) can now be taken as-

\[ nm = A \mp \varepsilon \quad \text{where } \varepsilon \text{ is a small positive integer} \]

Next substituting into the above Diophantine equation produces the following two quadratic equations in \(n\)-

\[ n^2 + n\{6(A - \varepsilon) - k\} + (A - \varepsilon) = 0 \quad \text{for } p = 6n + 1 , \quad q = 6m + 1 \]

\[ n^2 + n\{k - 6(A + \varepsilon)\} + (A + \varepsilon) = 0 \quad \text{for } p = 6n - 1 , \quad q = 6m - 1 \]

Sine in these last two equations the terms \(n, A, k, \text{ and } \varepsilon\) are all integers, the term in the radical in the solution for \(n\) must be positive. Since \(6A - k\) is a quite small number and \(A \gg \varepsilon\) with \(N \gg 1\), we can say that-

\[ \varepsilon \geq \varepsilon_0 = \text{nearest whole number to } \sqrt{N}/18 \]

This fact suggests that in our search for \(n\), we introduce a new integer -

\[ \delta = \varepsilon - \varepsilon_0 \]

In terms of \(\delta\) the two quadratics in \(n\) become-
In these expressions $C = A - \varepsilon_0$ and $D = A + \varepsilon_0$.

Let us show how these generic forms allow for the factoring of an actual semi-prime of the form $6k + 1$. Consider the six digit long semi-prime -

$$N = 247243 = 6(41207) + 1 \text{ where } k = 41207, A = 6868, \text{ and } \varepsilon_0 = 28, C = 6840, \text{ and } D = 6896.$$

Since we don’t know which sign the one has in the definitions of $p$ and $q$ beforehand, we run a search using both quadratic equations in a computer search. We have a 50-50 chance of picking the right quadratic in the first guess in the first set of calculations. We did this using the $+1$ forms for $p$ and $q$. This produced the quadratic -

$$n^2 + n\{6(C - \delta) - k\} + (C - \delta) = 0$$

and

$$n^2 + n\{k - 6(D + \delta)\} + D + \delta = 0$$

, respectively.

The one line search program used was -

```markdown
for \(\delta\) from 0 to 10 do\{\(\delta,\) solve\(n^2-(167+6*\delta)*n+(6840-\delta)=0,n\})od;
```

After just one evaluation, it produced the result -

\[\{\delta,n,m\} = \{0,72,95\}\]

That is -

$$N = 247243 = [6(72)+1][6(95)+1] = 433 \times 571$$

There is no need to go on and try the second quadratic since an integer solution for $n$ and $m$ has already been found.

Another example of factoring a semi-prime of the form $N = 6k + 1$ is the number -

$$N = 455839 \text{ for which } N \mod(6) = 1$$

This time we use the second quadratic in $n$ first. It reads -

$$n^2 - (221 + 6\delta)n + (12699 + \delta) = 0$$
since here \( k=75973, \ A=12662, \) and \( e_0=37. \) This quadratic produces the integer solution triplet-

\[
\{\delta,n,m\}=\{1,100,127\}
\]

Thus, after just two evaluations starting with \( \delta=0, \) the number is factored as-

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

What is interesting about this last semi-prime is that it is often used in the literature to demonstrate the Lenstra Elliptic Curve factorization technique. The present approach is seen to be much simpler and faster.

**CASE 2: \( N=6k-1 \)**

Here we can write-

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

with the possibility of \( n \) and \( m \) being interchanged. A bit of manipulation allows us to write this as the Diophantine Equation-

\[
6nm+(m-n)=k \text{  with } k=(N+1)/6 \text{ an integer}
\]

Again one typically has \( 6nm \gg m-n, \) so that we can try –

\[
nm=A-\varepsilon \quad \text{where } A \text{ is the nearest integer to } k/6 \text{ and } \varepsilon \text{ a small integer}
\]

Substituting this form for \( nm \) into the Diophantine equation produces the quadratic in \( n \) of-

\[
n^2 + n[k - 6(A - \varepsilon)] - (A - \varepsilon) - 0
\]

This time the quadratic yields real \( \varepsilon \) for all values of \( n \) and so splitting of \( \varepsilon \) into an \( \varepsilon \) and \( \delta \) won’t work. However we can modify the term \( e_0=\text{nearest integer to } \sqrt{N}/18 \) to the modified form –

\[
e_i = f \frac{\sqrt{N}}{18}
\]

where \( f \) has a fractional value somewhere in the range \( 0<f<1. \) It still requires that \( e_i \) be an integer. Substituting things into the Diophantine equation produces the new quadratic-

\[
n^2 + n[(k - 6A) - (e_i - \delta)] - (A - e_i - \delta) - 0
\]
Let us a solution for the N mod(6)=5 number-

\[ N = 4680113 = 6(780019) - 1 \]

Here \( k = 780019 \), \( A = 130003 \), and \( \varepsilon_1 = \frac{\sqrt{N}}{18} = 120f \). It means evaluating the quadratic-

\[ n^2 + n[1 + 6(120f + \delta)] - (130003 - 120f - \delta) = 0 \]

If we choose \( f = 1/2 \), a search yields the integer triplet solution-

\( \{\delta, n, m\} = \{-12, 242, -537\} \)

So we have the factoring-

\[ N = 4680113 = (6(242) + 1)(6(537) - 1) = 1453 \times 3223. \]

It took some 18 operations about \( \delta = 0 \) to get the result. By varying \( f \) we would expect a larger and possibly also a smaller number of operations required to factor \( N \).

**CONCLUSION:**

We have found a way to factor larger semi-primes \( N = 6k \pm 1 = pq \) based on the fact that the product \( 6nm \) is typically much larger than \( (n+m) \), where \( n \) and \( m \) are unknown integers appearing in the definition of the primes \( p = 6n \pm 1 \) and \( q = 6m \pm 1 \). We have shown that factoring of \( N \)s in the six to ten digit long range is readily accomplished by the present method with very little effort. It would be worthwhile for someone with larger electronic computing power to extend this process to semi-primes in the 20 to 100 digit length range where such factoring becomes of interest in connection with public key cryptography. Our present computer limit allows us to not go much beyond a factoring of a ten digit semi-prime such as-

\[ 2265223549 = 38737 \times 58477 \quad \text{where} \quad \{\delta, n, m\} = \{56, 6456, 9746\} \]

U.H. Kurzweg
August 2015