FACTORYING SEMI-PRIMES OF THE FORM (6n+1)(6m+1) and (6n-1)(6m+1)

In several earlier articles we have shown how to factor large semi-primes. We expand on those results by looking at the two types of generic semi-primes whose solutions also apply to the remaining two forms (6n-1)(6m-1) and (6n+1)(6m-1).

**CASE 1: N=(6n+1)(6m+1)**

Here N mod(6)=1. Examples among the infinite number of such semi-primes include-

- 247=13 x 19
- 2449=31 x 79
- 71989=193 x 373
- 984194977=21481 x 45817

In generic form these primes can be written as-

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

, where k is a positive integer. Letting \(x=nm\) and \(y=n+m\) produces the linear Diophantine equation-

\[6x+y=k\]

, where \(x\) and \(y\) are positive integers with the property that \(x>>y\) for larger semi-primes since \(nm>>(n+m)\). It suggests we try a solution of the form-

\[x=(k-H)/6-\varepsilon=B-\varepsilon\]  \hspace{1cm} \text{(1)}

Here \(H=k\mod(6)\) and \(B=(k-H)/6>>\varepsilon\). With these substitutions we have that the solution of the Diophantine Equation is –

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

, where \(B\) and \(H\) are known but the parameter \(\varepsilon\) is to be determined. Eliminating \(m\) from these results allows us to write-

\[ [p, q] = (1 + 3H + 18\varepsilon) \pm 3\sqrt{(H + 6\varepsilon)^2 - 4(B - \varepsilon)} \]

Here the term outside of the radical \(R=\sqrt{(H+6\varepsilon)^2-4(B-\varepsilon)}\) represents the mean value-

\[M=(p+q)/2=1+3H+18\varepsilon\]
provided that \( \epsilon > 0 \). The mean value can also be written as:

\[
M = \frac{[\alpha + \frac{1}{\alpha}]}{2} \sqrt{N}
\]

where \( p = \alpha \sqrt{N} \) and \( q = \sqrt{N}/\alpha \), with \( \alpha \) an unknown value lying between 0 and 1. For the solution \([p,q]\) to yield real values it is necessary that the \( \epsilon \) in the radical \( R \) must have at least the value \( \epsilon = \sqrt{B}/3 \). A better estimate for \( \epsilon \) follows from the identity:

\[
\epsilon_0 = \frac{1}{18} \left\{ \frac{(1+\alpha^2)}{2\alpha} \sqrt{N} - 1 - 3H \right\}
\]

with a guess for \( \alpha \). By looking at \( \alpha = 1 \) we can infer that:

\[
\epsilon_0 > \frac{1}{18} \left\{ \sqrt{N} - 1 - 3H \right\}
\]

for any smaller \( \alpha \).

Let us demonstrate the above factoring technique using the semi-prime \( N=17202763 \). Here \( \sqrt{N}=4147.621367 \), \( k:=2867127 \), \( H=3 \), and \( B=477854 \). We thus know that:

\[
\epsilon_0 > \frac{1}{18} \left\{ -10 + 4147.62 \right\} = 229.867
\]

For any \( \alpha \) in \([0,1]\) we have –

\[
\epsilon_0 = \frac{1}{18} \left\{ \frac{(1+\alpha^2)}{2\alpha} 4147.62 - 10 \right\}
\]

so that at \( \alpha = 0.6 \) we have the somewhat larger value of \( \epsilon_0 = 260.59 \). We average these two values to start a search of \( R \) using \( \epsilon_0 = 245 \). This produces with relatively little effort the result \( R = 263 \) at \( \epsilon = 234 \). From it follows:

\[
[p,q] = 10 + 18\epsilon \pm 3\sqrt{(3 + 6\epsilon)^2 - 4(477854 - \epsilon)}
\]

So that one achieves the factorization:

\[
[p,q] = 10 + 18*234 \pm 3*(263) = [3433, 5011]
\]
The speed with which this factoring was accomplished, compared with more sophisticated and involved techniques such as elliptic curve factorization or generalized sieve methods, is impressive. The mean value turns out to be $M = (3433 + 5011) / 2 = 4222$ and the exact value of $\alpha = 3433 / 4147.621367 = 0.8277$.

You will note that the $\alpha = 1$ limit says $(p+q)/2 = \sqrt{N}$. Hence we arrive at the previously unknown inequality:

$$(p+q) > 2 \sqrt{N}$$

for semi-primes. This inequality will also continue to hold for $N \mod(6) = 5$ semi-primes. For this last case the inequality reads:

$$(3433 + 5011) = 8444 > 2(4147.621367) = 8295.242$$

**CASE2: $N = (6n-1)(6m+1)$**

Here we have $N \mod(6) = 5$. Specific examples are–

- $209 = 11 \times 19$
- $146771 = 317 \times 463$
- $2603987 = 929 \times 2803$

This time the generic form reads-

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

That is, we again have the linear Diophantine equation-

$$6x + y = k$$

but the variables now are $x = nm$, $y = n-m$, and $k = (N+1)/k$. Again we note that for large semi-primes $6x > y$. Thus we have the solutions-

$$x = B - \varepsilon \quad \text{and} \quad y = H + 6\varepsilon$$

where $B = (k-H)/6 \gg \varepsilon$ and $H = k \mod(6)$. These are essentially the same solutions found earlier for the $N \mod(6) = 1$ case except now $k = (N+1)/6$ and $y = n-m$. Eliminating $m$ or $n$ from these solutions allows us to write-
\[ p = -1 + 3H + 18\varepsilon + 3\sqrt{(H + 6\varepsilon)^2 + 4(B - \varepsilon)} \]

and

\[ q = 1 - 3H - 18\varepsilon + 3\sqrt{(H + 6\varepsilon)^2 + 4(B - \varepsilon)} \]

Note that for this semi-prime the solutions for \( p \) and \( q \) have the same radical \( Q \) but there is no cut-off for the \( \varepsilon \) since the sign in front of 4 is positive. The mean value here becomes:

\[ M = \frac{(p + q)}{2} = \frac{(1 + \alpha^2)}{2\alpha} \sqrt{N} = 3Q \quad \text{where} \quad Q = \sqrt{(H + 6\varepsilon)^2 + 4(B - \varepsilon)} \]

We can write down the value \( Q_0 \) for a given \( \alpha \) from this last equation for \( M \). The lowest value occurs at \( \alpha=1 \) and equals \( Q_0=\sqrt{N}/3 \). For smaller \( \alpha \) values this value will increase. We typically choose the averaged \( Q_0 \) from the \( \alpha=1 \) and \( \alpha=0.6 \) cases to start the evaluation of the following quadratic in \( \varepsilon \):

\[ (H+6\varepsilon)^2 + 4(B-\varepsilon) = Q_0^2 \]

This produces two starting values for \( \varepsilon \) which are used in a search for integer \( Q \).

Let us apply the factoring technique for an \( N \equiv 5 \pmod{6} \) case by looking at:

\[ N=146771 \]

where \( \sqrt{N}=383.107 \), \( k=24462 \), \( H=0 \), and \( B=4077 \). So the mean value of \( p \) and \( q \) for \( \alpha=1 \) yields the estimate \( Q_0=\sqrt{N}/3=127.702 \). The value of \( Q_0 \) for \( \alpha=0.6 \) corresponds to a larger value \( Q_0=144.729 \). So we evaluate the quadratic in \( \varepsilon \) using \( Q_0=136 \). The solutions are:

\[ \varepsilon = -7.740 \quad \text{and} \quad \varepsilon = 7.851 \]

Searching \( Q \) then produces \( Q=130 \) at \( \varepsilon=-4 \). From this result it follows that:

\[ p = -1 - 4(18) + 3(130) = 317 \quad \text{with} \quad q = N/p = 463 \]

That is:

\[ 146771 = 317 \times 463 \]

Note that negative values of \( \varepsilon \) can arise in the factoring process for both \( N \equiv 1 \pmod{6} \) and \( N \equiv 5 \pmod{6} \) cases. The earlier mentioned inequality involving the mean again holds. We have:

\[ 780 > 2(383.107) = 766.214 \]
The exact value for $\alpha$ is $317/383.107=0.827$.

**FACTORING OF THE SEMI-PRIME N=455839:**

A semi-prime often used in the literature to demonstrate the Lenstra Elliptic Curve factorization method is N=455839. We show here that the present factorization procedure yields the correct result with a minimum of effort. Here we have-

\[ N=455839, \sqrt{N}=675.158, k=(N-1)/6=76473, H=N \mod(6)=1, \text{ and } B=(k-H)/6=12662. \]

A trial value for $\varepsilon$ at $\alpha=1$ is $\varepsilon_0=\pm\sqrt{B}/3=\pm37.51$. Without looking further for a better $\varepsilon_0$ one can carry out a search near -38 and near 38 since $\varepsilon_0$ is relatively small. This search yields the radical value of $R=27$ for $\varepsilon=-38$. The result produces the factors-

\[ [p,q]=(1+3+18(-38)\pm3(27)=[-599,-761] \]

The minus signs here indicate that $N=(6n-1)(6m-1)$ which still has $N \mod(6)=1$. The factored semi-prime is-

\[ 455839=599 \times 761 \]

The value of $\alpha=599/675.158=0.887$. Again the present factoring method is seen to be much simpler than other more complicated techniques such as the generalized sieve and elliptic curve approaches. We point out that the larger the semi-prime becomes the more values of $\alpha$ need to be tested to get a good starting point for $\varepsilon$. Remember that both $\alpha$ and $\varepsilon$ are unknown at the beginning of the calculations.

U.H.Kurzweg  
August 15, 2017  
Gainesville, Florida