We have shown in several recent notes that any prime greater than 3 has the form 6n+1 or 6n-1. Thus –

\[ p = 47352919 = 6(7892153)+1 \quad \text{and} \quad q = 83419463 = 6(13903244)-1 \]

are prime numbers and their product represents the semi-prime-

\[ N = pq = 3950155074462497 \]

One of the major research efforts in recent years has been to find faster ways to factor semi-primes of the above type into its p and q components for cases were the number N has lengths exceeding 100 digits or so. If anyone succeeds in doing this quickly, it will mean the end of communicating with encrypted messages using public keys.

We want here to suggest a new way to factor larger semi-primes. Being limited by our computer power we will concentrate on just two semi-primes of six and seven digit length, respectively. The first of these semi-primes will be-

\[ N = pq = 118837 \]

which has \( N \mod(6) = 1 \). This means that this number breaks up into-

\[ N = (6n+1)(6m+1) = 36nm + 6(n+m) + 1 \]

Since \( N \mod(6) = 1 \) could also mean \( (6n-1)(6m-1) \), it is possible that n and m are both negative integers. This fact will come out in the end of the calculations. Starting with plus n and m, we have-

\[ \frac{(N-1)}{6} = 19806 = T = 6nm + (m + n) \]

Here typically \( 6nm > (m+n) \). Solving for m we get-

\[ m = \frac{T - n}{1 + 6n} \]

Both \( m = (q+1)/6 \) and \( n = (p+1)/6 \) are unknown large numbers. Letting \( nm = k \) and eliminating m, we obtain the quadratic equation-

\[ n^2 + n[6k-(N-1)/6] + k = 0 \]

This quadratic equation in n has the solution-
\[ n = \frac{1}{12} \left\{ (N - 1) - 36k \pm \sqrt{[(N - 1) - 36k]^2 - 144k} \right\} \]

From this the factors \( p \) and \( q \) follow as-

\[ p = 1 + \frac{1}{2} \left\{ (N - 1) - 36k \pm \sqrt{[(N - 1) - 36k]^2 - 144k} \right\} = \frac{N}{q} \]

Let us assume that \( p \) is positive but smaller than \( q \) and have a value \( p = \alpha \sqrt{N} \), where \( 0 < \alpha < 1 \). Then \( q \) will have the value \( q = \sqrt{N}/\alpha \). For most cases involving large semi-primes the value of \( \alpha \) will lie somewhere above 1/4 but less than 1.

The problem of factoring \( N \) has thus been essentially reduced to finding that value of \( k \) for which the radical in the above \( n \) and \( p \) solutions equals a perfect square. For \( N = 118837 \) this means-

\[ \sqrt{(118836 - 36k)^2 - 144k} = \text{Integer} \]

It is easy to carry out \( v \) calculations starting out with \( k = 1 \) using the one line MAPLE program

```
for k from 1 to v do {k, sqrt((N-1-36k)^2-144*k)} od;
```

One has to go all the way to \( v = k = 3275 \) in order to find the integer value of 636 for the radical. This produces the integer factor-

\[ p = 1 + (1/2) \{118836 - 36(3275) - 636\} = 151 = N/q \]

Note here that \( \alpha = p/\sqrt{N} = 151/344.727.. = 0.438 \). This is of course not known until after \( p \) has been found.

It is clear that the above approach is one using a brute force evaluation requiring a total of 3275 operations when starting with \( k = 1 \). One asks at once if there is not a more efficient way of finding a solution for the factors \( p \) and \( q \) requiring less effort. The answer is in the affirmative as we will now show. First we work things backwards by estimating the approximate value of \( k \) near the point where the radical become equal to an integer. This is done by replacing the number \( n \) as follows-

\[ n = \frac{(p - 1)}{6} \geq \frac{(\alpha \sqrt{N} - 1)}{6} \]

knowing only that \( \alpha \) lies somewhere in \( 0 < \alpha < 1 \). Substituting this estimate into the above equation for \( p \) produces (after a little manipulation) the approximation-
which can now be used as a starting point for an evaluation of the radical in the above formulas for \( n \) and \( p \). The idea is to evaluate the \( ko \) equation after making a guess for \( \alpha \). As will be shown this guess is not very sensitive to changes in the value of \( ko \) since most of the weight of the approximation rests with the large \( (N+1)/36 \) portion. Once the \( ko \) has been determined we round it off to the nearest integer above the usual fractional value and then make the substitution into the radical to be evaluated. This produces for \( N=1188937 \) the estimate \( ko=3281.9 \) if we assume \( \alpha=1 \). Rounding things off then produces the new running integer-

\[
k = 3282 + \lambda
\]

and our radical assumes the simple new form-

\[
12\sqrt{9\lambda^2 - 342\lambda - 33}
\]

Which produces an integer solution of 636 for \( \lambda=-7 \). That is, it took only seven divisions starting with \( \lambda=0 \) to obtain our desired result.

You may ask what effect does a change in \( \alpha \) have on the speed of this new approach. The answer is relatively little. If, for instance, we take rather \( \alpha=1/2 \) for the initial guess the rounded \( ko \) becomes 3278 and so is only three units away from 3275. This result is even better than what we obtained with the \( \alpha=1 \) guess. Indeed by going to \( \alpha=p/\sqrt{N}=0.438 \) the value for an integer solution of the radical will be possible with just one operation (\( \lambda=0 \)). To see the actual evaluations one has to carry out to factor any semi-prime go to the appendix at the bottom of this page. There we consider the number \( N=455839 \) which is often used in the literature to demonstrate the Lenstra elliptic curve factorization method. The present approach makes the problem almost trivial.

In the event that \( N \ mod(6)=5 \) we use the expansion-

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

This produces the result-

\[
p = 1 + \frac{1}{2} \left\{ 36k - (N + 1) \pm \sqrt{\left[ (N + 1) - 36k \right]^2 + 144} \right\}
\]

This form differs only in some sign changes from the formula for \( p \) when \( N \ mod(6)=1 \). Consider now the 7 digit long semi-prime \( N=1349261 \) which has \( N \ mod(6)=5 \). The first
thing we do here is to find an estimate for the value of k which makes the radical an integer. Working backwards, we this time find-

\[ ko = \frac{1}{36} \left\{ (N - 1) - \frac{(1 - \alpha^2)}{\alpha} \sqrt{N} \right\} \]

Now making a guess of \( \alpha = 0.6 \) for \( N = 1349261 \), suggests searching near \( k = 37446 \). Doing so shows that \( \lambda = 70 \) makes the radical have an integer value of 2670 and produces-

\[ p = 677 \quad \text{and} \quad q = N/p = 1993 \]

It took some 70 operations starting with \( \lambda = 1 \) to produce our answer. Had we guessed a lower or higher value for \( \alpha \), the number of divisions required would have been higher since the actual \( \alpha \) value is here \( \alpha = 677/1161.57.. = 0.5828 \) and so close to our original guess. In this case it would actually have been even simpler if we had interchanged \( n \) and \( m \) so that things read \( N = (6n - 1)(6m + 1) \).

What is clear from the above results is that the formulas for \( p \) both for \( N \mod(6) = 1 \) and \( N \mod(6) = 5 \) semi-primes will continue to hold for any semi-prime \( N \). What is new here is that one now has a way to start with a good choice for \( ko \) to produce an integer value for the radical. By trying a spectrum of different \( ko \)s generated by different guesses for \( \alpha \), the search process can be made to quickly zero in on the value of \( ko \) closest to the actual integer value by running searches in a relatively narrow range about different \( ko \)s until one is found were it takes only a few operations to obtain an integer value for the radical.

Just to show that we can handle even larger semi-primes by the present approach we look at the 16 digit long semi-prime \( N = 3950155074462497 \) given at the beginning of this note. If we choose \( \alpha = 3/4 \) we obtain \( ko = 10972652882774 \). The actual value of \( k = nm \) is here \( k = 13903244 \times 7892153 = 10972652884432 \). Thus the number of required evaluations would involve just 21,558 operations starting with \( \lambda = 1 \) to find the integer value of the radical. This looks like a formidable task but is really not when using high speed electronic computers. I expect that this approach may prove useful in breaking large public keys in the near future.

APPENDIX:
U.H.Kurzweg  
Gainesville, Florida  
October 14, 2013

```
N:=455839;  N mod(6);  ROOT:=evalf(sqrt(N));
        N := 455839
        l
        ROOT := 675.1584999
a:=0.9;  ko:=evalf((N+1-(1+a^2)*sqrt(N)/a)/36);
        a := 0.9
        ko := 12625.50503

unassign('b');  k:=12625+b;  for b from 74 to 76 do {b, sqrt((N-1-36*k)^2-144*k)}od;
        recognizing radical is imaginary till b=75
        k := 12625 + b
        {74, 6.1/1955}
        {75, 162}
        {76, 6.3485}

p:=1+(1/2)*(N-1-36*(12625+75)+162);  q:=N/p;
        solution k=12625+75 for which the radical equals 162
        p := 599
        q := 761
        minus signs indicate form of p=6m-1 and q=6n-1
```