Prime Factoring Algorithm

If the number to be factored is N, find
$a_1^2 - N = k_1$ (where $a_1$ is the next integer > $(N)^{1/2}$ )

We now obtain a binary quadratic equation corresponding to N using the above information.
We do this as follows:

$(a_1 + 1)^2 - (N) = d_1$

$(a_1 + 2)^2 - (N) = d_2$

$(a_1 + 3)^2 - (N) = d_3$

so that we can find $(a_1 + n)^2 - (N) = d_n$ where $d_n$ is a square number.

Next using calculus of finite difference we obtain

$$\begin{array}{ccccc} d_1 & & d_2 & & d_3 \\ & d_4 & & d_5 & \\ & & d_6 & & \end{array}$$

where we subtract the number on the left from its neighbor on the right to obtain the next row.
And proceed to obtain the equation:

$$1/2(d_6)x^2 + (d_4-(1/2d_6))x + d_1 = y^2$$

since we want the equation on the LHS to be a square.
This is a Diophantine equation of the form $A x^2 + Bxy + C y^2 + Dx + Ey + F = 0$. While there are analytical methods to solve this type of equation they involve the use of factorization which we wish to avoid. Hence we will go by the rational point on conics route. Using
$A x^2 + Bxy + C y^2 + Dx + Ey + F = 0$
and the equation of the line given by

$y = y_1 + m(x-x_1)$

and considering the sum of roots we obtain the parametrization of x given by

$x = [( x_1 Cm^2 -(2C y_1+ E)m – (By_1 + Ax +D)] / ( Cm^2 + Bm + A)$ -(2)

In this case,

A = 1 C = -1 B = 0

so

$x = [( x_1 m^2 - ( E – 2y_1 )m – ( x + D )] / ( m^2 -1)$ - (2)

and similarly

$y = [( y_1 )m^2 – (2x_1 + D )m – y_1 ) / ( m^2 -1)$ - (3)

I will illustrate the process up to this stage with a numerical example where p and q are the 2 primes and N is their product.

For pq = N

137x 241 = 33017 ( $p \equiv q \equiv 1 \pmod 4$ , $N \equiv 1 \pmod 4$)

$\sqrt{33017} \approx 182$

$182^2 – 33017 = 107$

$183^2 – 33017 = 472$

$184^2 – 33017 = 839$

107 472 839

365 367

2

$x^2 + 364x + 107 = y^2$

I've solved this equation using the Generic Two Integer Variable Equation Solver found at the following website http://www.alpertron.com.ar/QUAD.HTM and obtained the following solutions

x = 16327 ,-16691 and y = 16508, -16508

and

x = 7, -371 and y = 52, -52

We can also find the larger set of values trivially as follows.

$x_0 = 16327$ $y_0 = 16508$

Since $(182 + 16327)^2 – (16508)^2 = 33017$

What we are interested in is the smaller set of values. The method used to find them involves factorization so we will have to use a different approach.

Now considering our equation $x^2 + 364x + 107 = y^2$ and the general Diophantine equation of the form $A x^2 + Bxy + C y^2 + Dx + Ey + F = 0$ we can find

A = 1 C = -1 B = 0 D = 364 E = 0

and parameterizing x and y using the technique of finding rational points on conics we get

$x_1 = ( x_0 m^2 + (E - 2 y_0 )m + (x_0 + D ))/(m^2 - 1)$

$x_1 = (16327m^2 – 33016m + 16691)/(m^2 – 1)$

$y_1 = ( (y_0-E) m^2 + (2 x_0 + D)m + y_0)/(m^2 - 1)$

$y_1 = (16508m^2 – 33018m + 16508)/(m^2 – 1)$

Where m is the gradient of the line passing through the rational point

Next we tabulate the values of $x_1, y_1$ for m of the form n/(n+1) and (n +1)/n.

| $m_1$ | $x_1$ | $y_1$ | $m_2$ | $x_2$ | $y_2$ |
|---|---|---|---|---|---|
| 2/1 | $\frac{15967}{3}$ | $\frac{16504}{3}$ | 1/2 | $-\frac{17059}{3}$ | $-\frac{16504}{3}$ |
| 3/2 | $\frac{15611}{5}$ | $\frac{16496}{5}$ | 2/3 | $-\frac{17431}{5}$ | $-\frac{16496}{5}$ |
| 4/3 | $\frac{15259}{7}$ | $\frac{16484}{7}$ | 3/4 | $-\frac{17807}{7}$ | $-\frac{16484}{7}$ |

| | | | | | |
|---|---|---|---|---|---|
| 68/67 | $\frac{1051}{135}$ | $\frac{7396}{135}$ | 67/68 | $-\frac{50191}{135}$ | $-\frac{7396}{135}$ |
| **69/68** | **959/137 = 7** | **7124/137 = 52** | **68/69** | **-50827/137 = -371** | **-7124/137 = -52** |
| 70/69 | $\frac{871}{139}$ | $\frac{6848}{139}$ | 69/70 | $-\frac{51467}{139}$ | $-\frac{6848}{139}$ |

| | | | | | |
|---|---|---|---|---|---|
| 90/89 | $-\frac{49}{179}$ | $\frac{488}{179}$ | 89/90 | $-\frac{65107}{179}$ | $-\frac{488}{179}$ |
| 91/90 | $-\frac{53}{181}$ | $\frac{128}{181}$ | 90/91 | $-\frac{65831}{181}$ | $-\frac{128}{181}$ |
| 92/91 | $-\frac{53}{183}$ | $-\frac{236}{183}$ | 91/92 | $-\frac{66559}{183}$ | $\frac{236}{183}$ |

| | | | | | |
|---|---|---|---|---|---|
| 120/119 | $\frac{1571}{239}$ | $-\frac{12052}{239}$ | 119/120 | $-\frac{88567}{239}$ | $\frac{12052}{239}$ |
| **121/120** | **1687/241 = 7** | **-12532/241 = -52** | **120/121** | **-89411/241 = -371** | **12532/241 = 52** |
| 122/121 | $\frac{1807}{243}$ | $-\frac{13016}{243}$ | 121/122 | $-\frac{90259}{243}$ | $\frac{13016}{243}$ |

| | | | | | |
|---|---|---|---|---|---|
| 180/179 | $\frac{15611}{359}$ | $-\frac{47932}{359}$ | 179/180 | $-\frac{146287}{359}$ | $\frac{47932}{359}$ |
| 181/180 | $\frac{15967}{361}$ | $-\frac{48652}{361}$ | 180/181 | $-\frac{147371}{361}$ | $\frac{48652}{361}$ |
| 182/181 | $\frac{16327}{363}$ | $-\frac{49376}{363}$ | 181/182 | $-\frac{148459}{363}$ | $\frac{49376}{363}$ |

The second and forth tables show the values of x and y when 2n + 1 corresponds to the prime factors we are trying to find as well as the values immediately adjacent to them. As we can observe they are the same as solutions to the equation $x^2 + 364x + 107 = y^2$. There are a few more observations that we can make :

1. The numerator of each column can be expressed as an arithmetic progression and the denominator in the form 2n +1.

2. Consider the $x_1$ and $x_2$.The values of x at the values of m corresponding to the two prime factors are the same integers. Similarly the value at of $y_1$ corresponding to one of the prime factors is the negative of that of the other prime factor and vice versa for $y_2$.Also these are the only times where a value is repeated. The values of m corresponding to the two prime factors are given by $m = (n_1+1)/n_1$ , $n_1/(n_1+1)$ and $(n_2+1)/n_2$ , $n_2/(n_2+1)$ where the sum of the numerator and denominator $2n_1+1$ and $2n_2+1$ are the two prime factors.

3. At $n = 90$ corresponding to $2n + 1 = 181$ for the numerator reaches a minimum value for $x_1$. After that the d of the arithmetic progression changes signs. To find the minimum value of $x_1$ and hence the location at which the transition occurs:

   We differentiate $x_1$ with respect to n after replacing m by (n+1)/n in this equation

$$x_1 = (x_0 m^2 + (E - 2 y_0)m + (x_0 + D))/(m^2 - 1)$$

Now let $p = 2n_1+1$ and $q= 2n_{2*}+1$ ( where $n_{2*} = n_2 + n$) using the information we obtain from tables 1 and 3 we are able to obtain at least three different equations in terms of $n_1$ and $n_2$. For example for $x_1$ in region from $n = 1$ to 90 we can express it as $[15967-((n_1-1)/2)(2(356) - 4(n_1-1))]/(2n_1+1)$.Also for the region from $n = 90$ to 180 where the transition of the common difference occurs we can express it as $[-53 – ((n_2-1+90)/2)(2(0) + 4(n_2-1))]/((2n_2 + 90) + 1)$. We can equate these two expressions since their value is equal at the points corresponding to p and q. We can obtain a similar expression for $x_2$ and $y_1$. Since we have three equations and only two unknowns we can easily solve for the unknowns and obtain the factors.
In this case the 3 equations that can be obtained are as follows

Corresponding to $x_1$ :

$(15967 – [(n_1 – 1)/2](2(356) - 4( n_1 - 2))/(2 n_1 + 1) =$

$(-53 - [(n_2– 1)/2](2(0) + 4( n_2 - 2))/(2(n_2 +89) +1$

Corresponding to $y_1$ :

$(-16504 – [(n_1 – 1)/2](2(8) - 4( n_1 - 2))/(2 n_1 + 1) =$

$-(-128 - [(n_2– 1)/2](2(364) + 4( n_2 - 2))/(2(n_2 +89) +1$

Corresponding to $x_2$ :

$(-17059 – [(n_1 – 1)/2](2(372) - 4( n_1 - 2))/(2 n_1 + 1) =$

$(-17059 - [(n_2+89– 1)/2](2(372) + 4( n_2+89– 2))/(2(n_2 +89) +1$