# SOLUTION OF A NON-LINEAR DIOPHANTINE EQUATION

In several earlier articles found on this web page we have shown that any semi-prime N=pq can be decomposed into its components-

p=(R+x)-y   and   y=(R+x)+y

, with x and y given by a solution of the non-linear Diophantine equation-

(N+y^2)=(x+R)^2

,where R is he next integer above sqrt(N). Thus the integer solution [x,y] in effect factorizes N=pq. We wish in this note to offer a general solution to the above Diophantine Equation.

We begin by noting that-

(x+R)^2-y^2=N

is just a standard hyperbola when the integer restrictions for x and y are relaxed. This hyperbola is centered at [x,y]=[-R,0] and has slope-

dy/dx=(x+R)/y=(x+R)/sqrt(-N+(x+R)^2)

So we have an infinite slope at the slightly negative value of -R+sqrt(N).

There will be just one point [x,y] along this parabola in the first quadrant at which [x,y] will equal integers. To find this point we use the one line computer program-

```
for x from b to c do({x,sqrt(-N+(R+x)^2)})od;
```

, where b lies slightly below x and c just above it. To get some idea of what value b might have we have constructed the following table using a brute force approach starting with b=0. It produces-

Integer Solutions of the Non-Linear Diophantine Equation

(N+y^2)=(R+x)^2

| N=pq | R | y=(q-p)/2 | x=(p+q)/2-R | n=R+x |
|---|---|---|---|---|
| 35 | 6 | 1 | 0 | 6 |
| 77 | 9 | 2 | 0 | 9 |
| 779 | 28 | 11 | 2 | 30 |
| 2701 | 52 | 18 | 3 | 55 |
| 11303 | 107 | 19 | 1 | 108 |
| 455839 | 676 | 81 | 4 | 680 |
| 7828229 | 2798 | 670 | 79 | 2877 |
| 28787233 | 5366 | 2076 | 387 | 5753 |
| 76357301 | 8739 | 1082 | 66 | 8805 |
| 169331977 | 13013 | 6732 | 1638 | 14651 |
| 3330853711 | 57714 | 12633 | 1366 | 59080 |
| 3574406403731 | 1890610 | 725225 | 134324 | 2024934 |

Here N is a semi-prime, R is the nearest integer above sqrt(N) and

p=R+x-y and q=R+x+y

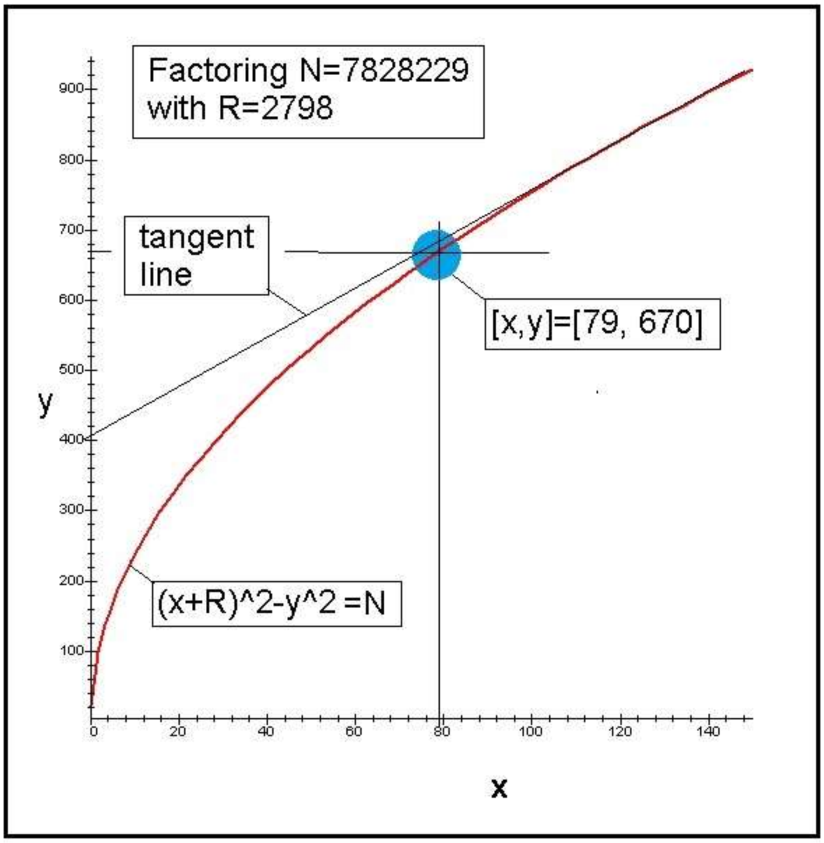
There are a few obvious points to note in this table. It is that N>R>y>x and that R and N are comparable in size. For the semi-prime N=7828229, where R=2798, we could choose b=75 and c=83. His produces-

Factoring N=7828229 with R=2798

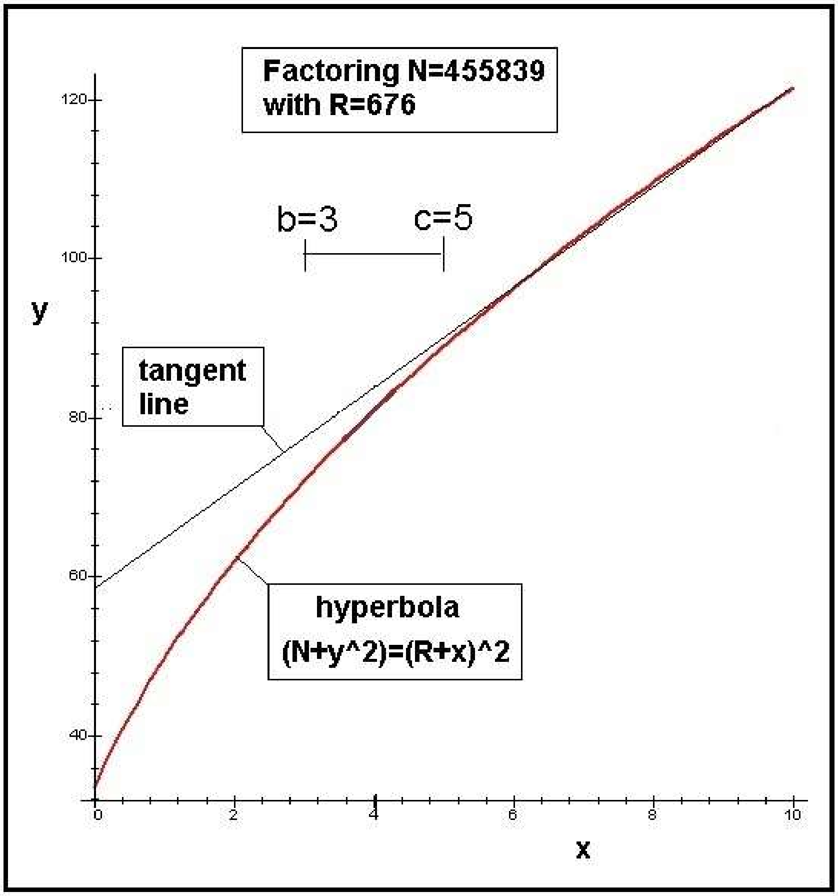
for x from 75 to 83 do ({x,sqrt(-N+(x+R)^2})od;

$\{75, 10\sqrt{4259}\}$
$\{76, \sqrt{431647}\}$
$\{77, 2\sqrt{109349}\}$
$\{78, \sqrt{443147}\}$
$\{79, 670\}$ ⟵ solution [x,y]
$\{80, \sqrt{454655}\}$
$\{81, 2\sqrt{115103}\}$
$\{82, \sqrt{466171}\}$
$\{83, 2\sqrt{117983}\}$

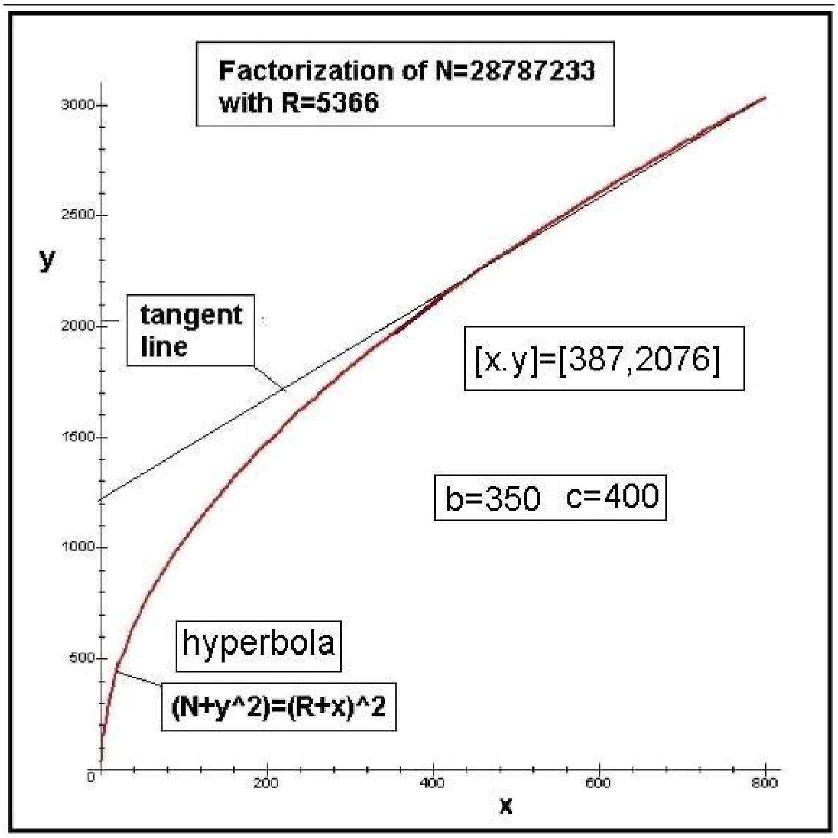
, with the desired integer solution [x,y]=[79, 670].This produces p=2207 and q=3547. The problem here is that x=79 was known from the above table and thus [x,y] are known to begin with. How could one estimate b by some other means? One way is to look at the hyperbola for this same N. Its curve looks as follows-




We have marked the [x,y] solution by the blue circle. It lies slightly below where the tangent line merges with the parabola, suggesting one could try b=75 and run things through c=85. This produces the solution [79,670] in five trials instead of the 79 trials it would take by starting the search at b=0. To confirm that this approach works consider another semi-prime N=455839 with R=676. Here we get the following hyperbolic graph together with its tangent line-




The graph suggests we start the [x,y] search with b=3 and go to c=5. After just two trials we arrive at the Diophantine solution [x,y]= [4,81]. Thus p=(676+4)-81=599 and q=(676+4)+81=761. As a third semi-prime to factor, consider N=28787233 with R=5366. This produces the graph-




It suggests we use b=350 as a starting point expecting [x,y] to occur below c=400. Running a search we find [x,y]=[387,2076]. So the prime components are p=(5366+387)-2076=3677 and q=(5366+387)+2076=7829.

We have shown how to factor any semi-prime N=pq regardless of its size by choosing a value of x=b in a computer search program, where b lies just below where a hyperbola and its tangent line meet. This Diophantine solution procedure is expected to work for an infinite number of additional cases requiring a relatively low number of computer trials.

U.H.Kurzweg
May 4, 2023
Gainesville, Florida