SOLVING THE DIOPHANTINE EQUATION (R+x)^2-y^2=N

INTRODUCTION:

In a recent earlier article on this Web Page we have shown a new way to factor semi-primes N=pq based on solving the Diophantine equation (R+x)^2-y^2=N, where R is the nearest integer above sqrt(N). We want in this article to re-derive this equation and then to find the integers [x,y] for several examples. Here y=(q-p)/2 is the half distance between q and p and x=[(p+q)/2]-R the average value of p and q minus the number R.

DERIVING THE DIOPHANTINE EQUATION:

Starting with the definitions of x and y we have-

$$q-p=2y \quad \text{and} \quad p+q=2(R+x)$$

Next eliminating q and then p, we get –

$$p=(R+x)-y \quad \text{and} \quad q=(R+x)+y$$

So we can write-

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

This is the desired Diophantine Equation with N and R known integer values.

Note that if one were to drop the integer requirement for this Diophantine Equation, then the last equation represents a hyperbola with a slope in the first quadrant of-

$$dy/dx=(R+x)/y=(R+x)/\mathrm{sqrt}(-N+(R+x)^2)$$

This slope becomes infinite at x=-R+sqrt(N) and has an asymptotic value of one as x approaches infinity.

We can rewrite the above Diophantine Equation as-

$$\mathrm{sqrt}(N+y^2)=R+x=n$$

, where both terms must equal the same integer n. Solving for x means-

$$x=-R+\mathrm{sqrt}(N+y^2)$$

So if we have y known, then the variable x is also known and visa versa. Typically y>x.

COMPUTER SOLUTION:

A computer solution of the above Diophantine Equation follows via the following simple one line program-

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

Here b and c are bounds chosen for the evaluation. When N is not very large the trials can begin with b=0 and run until the integer point [x,y] is reached. For Larger Ns one needs to consider starting the trials at large integer values for b in order to reduce the computation times. We will show how this is done below.

Let us begin a factorization for the relatively small six digit semi-prime N=455839, where R=676. Here we take b=0 and run things through c=5.The computer program produces the table-

x	Y
0	sqrt(1137)
1	sqrt(2490)
2	sqrt(3845)
3	sqrt(5202)
4	81
5	sqrt(7922)

From this table we have the integer solution [x,y]=[4,81]. So the factors are-

p=(676+4)-81=599 and q=(676+4)+81=761

In quad notation this N solution may be written as-

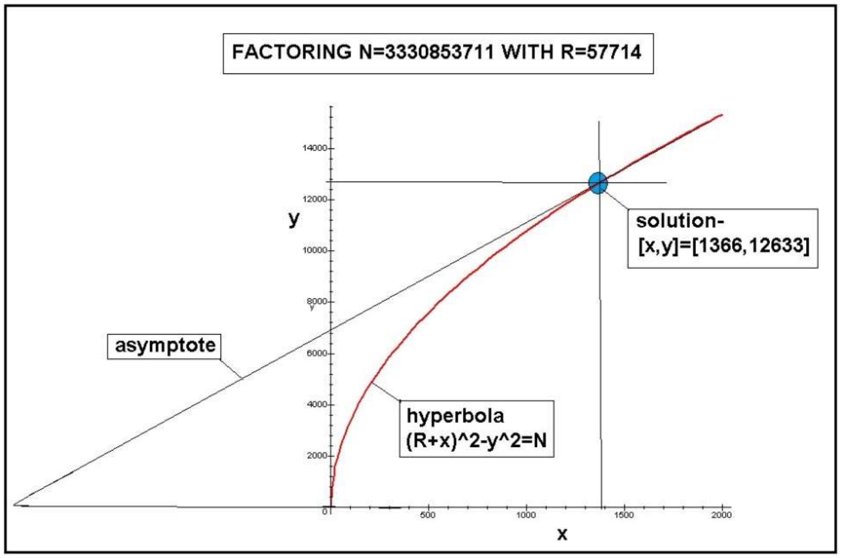
Q= [455839,676,81,4]

FIDING b FOR LARGER Ns:

When dealing with semi-primes of ten digits or larger one needs to start the n search trials at bs considerably above zero and possibly as close to [x,y] as possible. How can we find such bs? One way we have found is to study the shape of the corresponding hyperbola and pick a starting point slightly below the point where the hyperbola approaches its asymptote. We have found this approach seems to work in most cases with larger N. Let us try this method of picking b for the ten digit semi-prime N=3330853711, where R=57714. Here the corresponding hyperbola reads-

(57714+x)^2-y^2=3330853711

Its plot and the asymptote look as follows-



Placing b a little below the point where the asymptote and the hyperbola meet, we start with b=1300 and go to c=1400. After sixty six trials we arrive in a split second at [x,y]=[1366,12633]. So we have the factors-

p=(57714+1366)-12633=46447 and q=(57714)1266)+12633=71713

and the quad notation-

Q=[3330853711,57714,12633,1366] .

CONCLUDING REMARKS:

We have shown that large semi-primes N=pq can be factored by solving a new type of Diophantine Equation. With appropriate location of a starting point, a simple one line computer program can be used to find the point values x and y. From this one obtains the quad Q=[N,R,x,y] and the problem is solved as-

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

Detailed examples of factoring both a six and a ten digit long semi-prime are presented.

U.H.Kurzweg
May 26, 2023
Gainesville, Florida