EVALUATING THE EQUATION SQRT[(x+R)^2-N]=INTEGER

Several years ago we found that any semi-prime N=pq has its prime components given by-

$$[p,q]=(x+R)\mp sqrt[(x+R)^2-N]$$

, where the radical-

F(x)=sqrt[(x+R)^2-N]=sqrt((x^2+2xR+(R^2-N] must be an integer.

Once F(x) has been found the prime components become-

p=x+R-F(x) and q=(k+R)+F(x) .

We wish in this note to examine the properties of the Diophantine Equation F(x)=int .

The first thing we notice is that the dominant term in the second square root is 2xR and not x^2 or (R^2-N). R is typically much larger than x. So we can set x=aR with a guess for 'a' in the range $0 < a \ll 1$. A graph of F(x) will give a clue as to which 'a' to choose as a search starting point.

To find the exact values of x and F(x) we apply the following computer search procedure-

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

For smaller semi-primes we can set 'a' to zero and run things for 'c' trials.

Let us use this computer approach for several different semi-primes. We begin with the semi-prime-

N= 3431 where R=59

Starting the search with 'a'=0, we get the first three terms to read-

x	F(x)
0	sqrt(50)
1	13
2	sqrt(290)

So we get an integer F(x)= 13 at x=1. This means –

p=1+59-13=47 and q=1+59+13=73.

Next take the six digit long semi-prime –

N=455839 for which R=676 .

Using just five trials, starting with x=0, we get-

x=4 producing F(x)=sqrt[(4+676)^2-N]=81

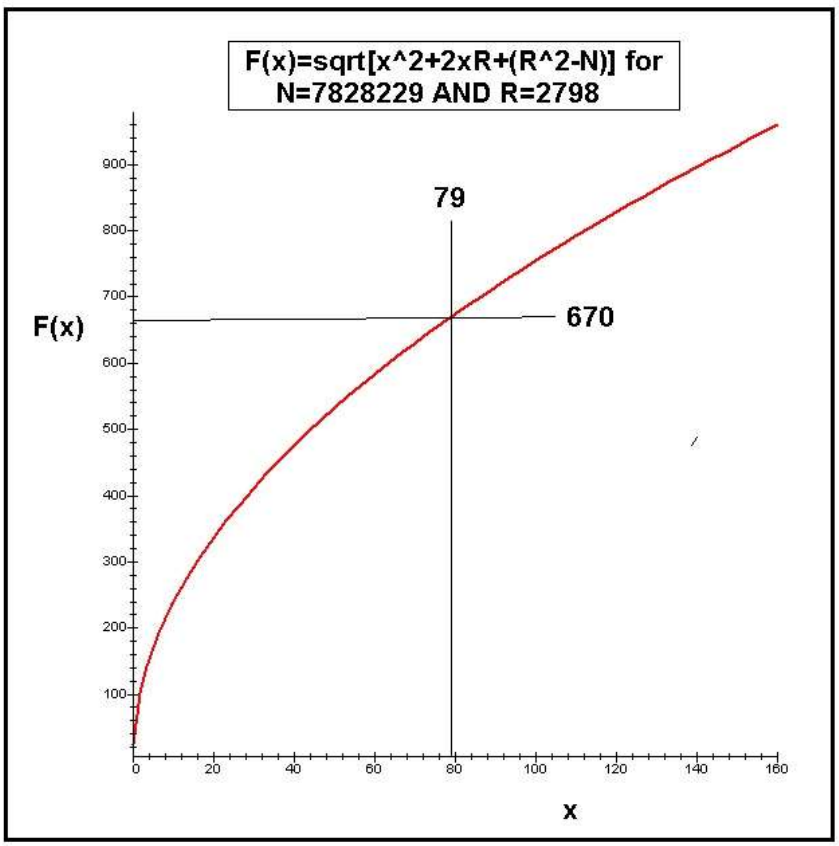
So the prime components become-

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

As a third case consider the seven digit long semi-prime-

N=7828229 where R=2798

Its F(x) plot in the range 0<x<160 has the parabolic like shape shown-

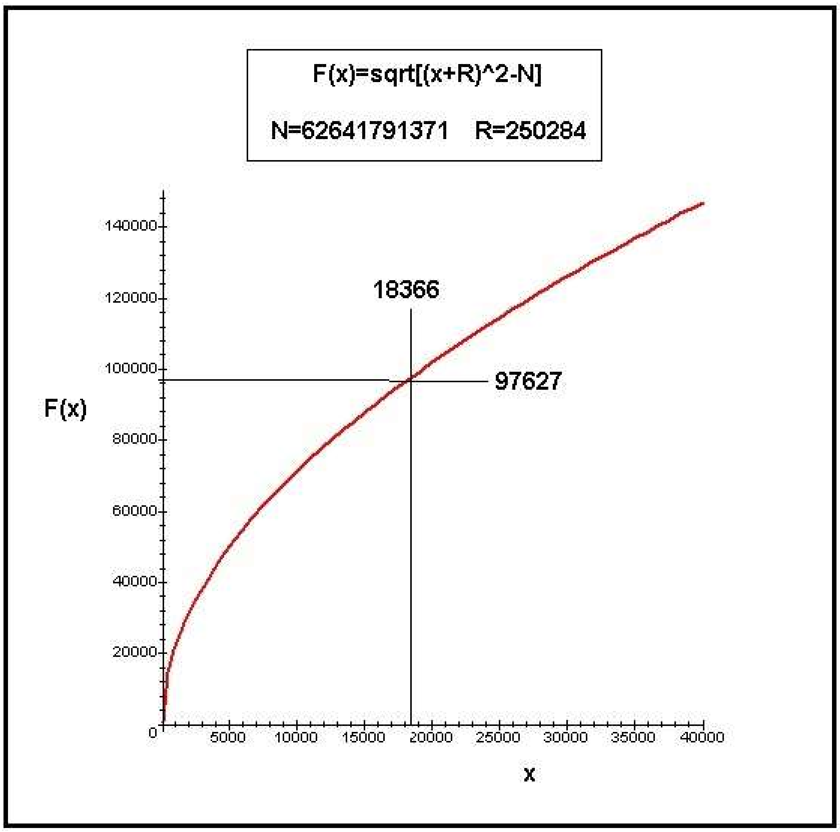


Our computer program, run over the range x=0 to x=160, shows that the integer solution is here x=79 with F(x)=670. We see this occurs along the F(x) curve just slightly to the left of where F(x) becomes asymptotic. This suggest one can carry out future searches with still larger Ns by looking at an x just slightly to the left of the asymptotic form of F(x).

Let us demonstrate the procedure for the eleven digit long semi-prime-

N=62641791371 where R=250284

The F(x) curve drawn over the range 0<x<40,000 looks as follows-



So carrying out a computer search near x=18000 produces the integer solution [x,F(x)=[18366, 97627]. From it we have the prime factors-

p=x+R-97627=171023 and q=x+R+97627=366277

Taking the product of p and q returns the original semi-prime N.

What is clear from the above examples is that the number of trials increases dramatically as N gets larger if one starts the search at $x=0$. In that situation one should try a larger $x= aRs$ as a starting point and run things out to c. The starting point value of x is suggested by looking at the parabolic shaped $F(x)$ curve slightly to the left of its asymptote for the specified N under consideration.

U.H.Kurzweg
November 16, 2023
Gainesville, Florida