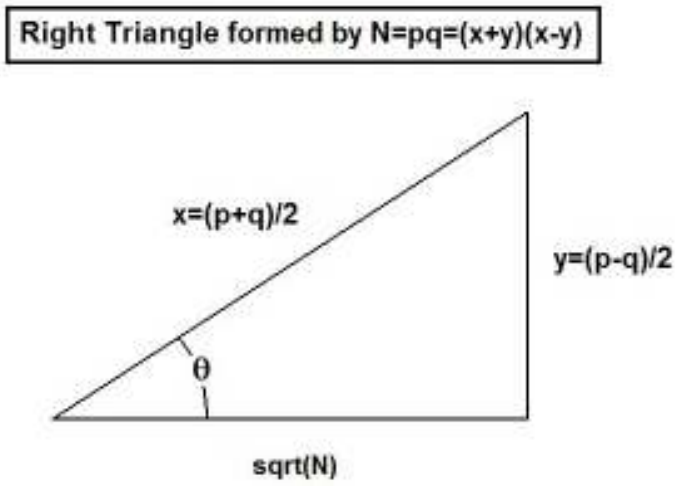
ANOTHER METHOD FOR FACTORING SEMI-PRIMES

There are many techniques for factoring semi-primes N=pq. Unfortunately they all become unwieldy when the number N approaches lengths of one hundred digits or more. We want here to introduce an alternate approach to factoring starting with the Diophantine equation-

$$y^2 = x^2 - N$$

where N is an odd integer , and x=(p+q)/2, and y=(p-q)/2 are integers. One of the first things one notices about this hyperbolic curve is that it has a corresponding right triangle as shown-



From the triangle we have that–

$$\tan(\theta) = \frac{(p-q)}{2\sqrt{N}} = \frac{(p^2 - N)}{2p\sqrt{N}}$$

This tangent function has a change in sign at p=sqrt(N). It allows one to introduce the related rational function-

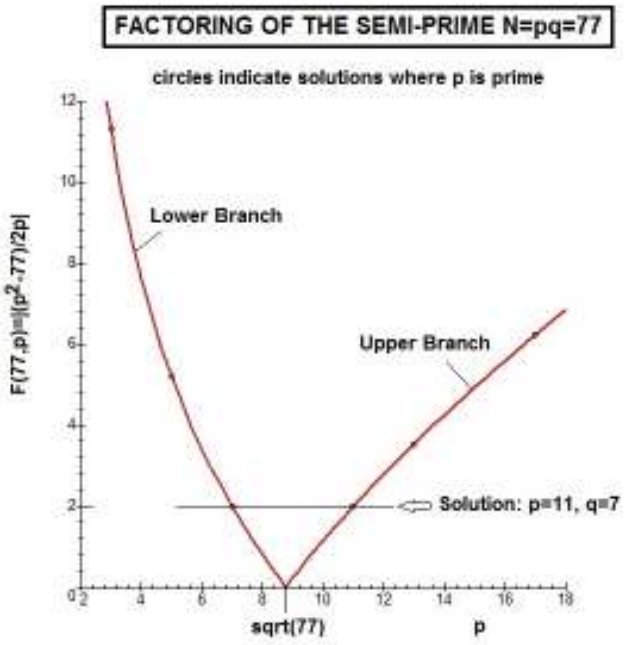
$$F(N,p) = \sqrt{N}\left|\tan(\theta\right| = \left|\frac{p^2 - N}{2p}\right|$$

where p represents any prime number above p=2. The function is always positive for all primes p and has two branches on opposite sides of sqrt(N). We designate the prime number closest to sqrt(N) as $p=p_0$. A table or point plot of F(N,p) can readily be

generated by using an electronic computer and a canned program such as MAPLE. Here is an example of the solution F(77, p) for p=3, 5, 7, 11, 13, 17. The prime p_0 is taken as 7 since it is the prime closest to sqrt(77)=8.77496.. . The generated table of rational values looks like this-

p	F(77, p)=|(p^2-77)/2p|
3	34/3
5	26/5
7	2
11	2
13	46/13
17	106/17

The corresponding point plot has this appearance-



What is very interesting about this result is that the factors p and q of N are given when F(77,p) takes on an integer value which is matched on both branches. You will also notice that all other solutions to F(N,p) versus p, where p is a prime but not a factor of N, take on non-integer values. Whenever the quantity F(N,p) is equal on the two branches, we find the distance between the branches equals 2F(N,p) so that F(N,p) represents the mean value of p and q. In the above case the solution is found to be p=11 and q=7 as shown in the graph. So that F(77,11)=(p-q)/2=2 This procedure , which differs from most other known factoring techniques for semi-primes,is related to the brute force approach of dividing N by different primes p until an integer value is reached. The above definition of tan(θ) makes the present approach possible and can often involve only a few divisions.

Typically one needs to evaluate F(N,p) along only one of the branches until an integer value for F(n,p) is encountered.

Let us look at some additional examples. Take N=713 where sqrt(N)=26.702.. Here the nearest prime is p_0=29 with other primes to the right being p=31, 37, 41, etc. Evaluating F(N,p) we find F(713,29)=6/29, and F(713,31)=4. So we have, after just two trials, the factor p=31 from which follows q=713/31=23. The evaluations become more difficult as N is increased. Take next the semi-prime N=455839 where sqrt(N)=675.158.. .This number is of interest since it has often been used to demonstrate the Lenstra Elliptic Curve factorization method . The primes in the neighborhood of sqrt(N) are-

p=ithprime(123+n) where 0<n<20

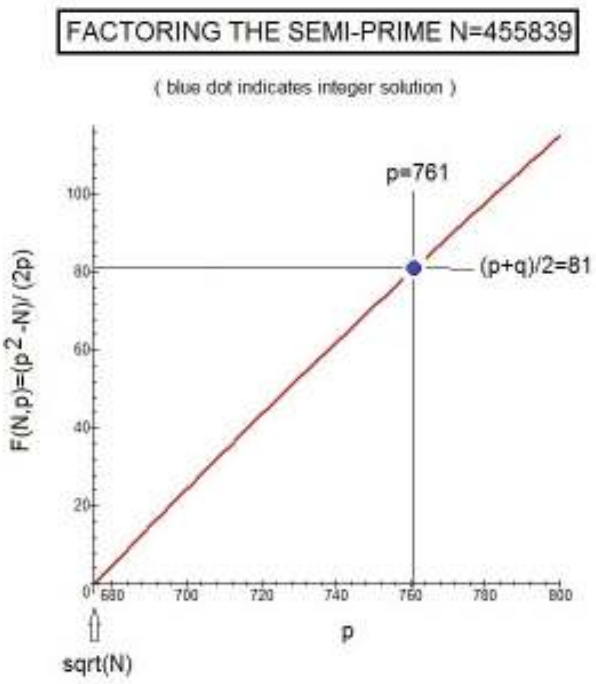
Here p_0= ithprime(123)=677 which is the prime closest to sqrt(N). Running the MAPLE program-

for n from 0 to 20 do {n,p,evalf(abs((p^2-N)/(2p)))}od;

produces the solution point [n, p, F(N,p)] =[12, 81,761] along the right branch after just 12 trials. Thus we have that N=pq factors as-

455839=599 x 761

The integer value for F(N,p) along both branches has the value of 81=(p-q)/2. We can also show this solution graphically by plotting F(455839,p) versus p for p>sqrt(N). The result looks as follows-



For an even larger semi-prime consider -

N=3493004741 where sqrt(N)=59101.64753…

Here p_o=ithprime(5976)=59107. This time, looking along the upper branch, we find an integer solution for F does not occur until p=79769. There the solution triplet reads-

[n, p, F(N,p)=[1836,79769,17970]

The number N is thus factored into-

p=79769 and q=N/p=43789

This time it took quite a bit more effort involving some 1836 divisions. The value of F(N,p) =17970 and matches F(N,q) as expected. To cut down on the number of required divisions one could start the divisions using qs near f { sqrt(N)} where f is some fraction in the range 0<f<1. Thus f=3/4 will produce the same answer after just a few divisions. Typically one should use a trial and error approach where F(N,x) is evaluated over a limited range of x near different values of f{sqrt(N)}q .

We have shown that semi-primes **N=pq** may be factored by noting that **$F(N,z)=|(z^2-N)/(2z)|$ is a positive integer only when z represents a prime factor p or q of N.** The technique works fine for semi-primes of twelve digit length or less but is likely to have problems when N approaches several hundred digits in length such as used in public key cryptography. Since F(N,p) can also be thought of as (p-q)/2 , the criterion makes good sense since the difference between two odd numbers(which is the case for all primes except 2) is even and hence always divides by two.

February 22, 2013

ps-Here is an additional table for factored semi-primes carried out with our MAPLE program-

N=pq	Sqrt(N)	F(N,p)=(p^2-N)/(2p)	p	q
29213	170.918	46	223	131
63787	252.560	27	281	227
108209	328.951	104	449	241
21830857	4672.350	792	5531	3947
947536544749	973414.888	203490	1197947	790967

One can cut down on the number of required divisions by noting that the endings of the Ns suggest the possible forms the odd ps can take when dividing into F(N,p). For example, the number N=29213=pq in the above table suggests we only need to try ps which are prime, end in 1 or 3 and are equal or greater than 171. Thus we try p=173, 181,191,193, 211, and 223. After six divisions we have our answer p=223 with F=46.