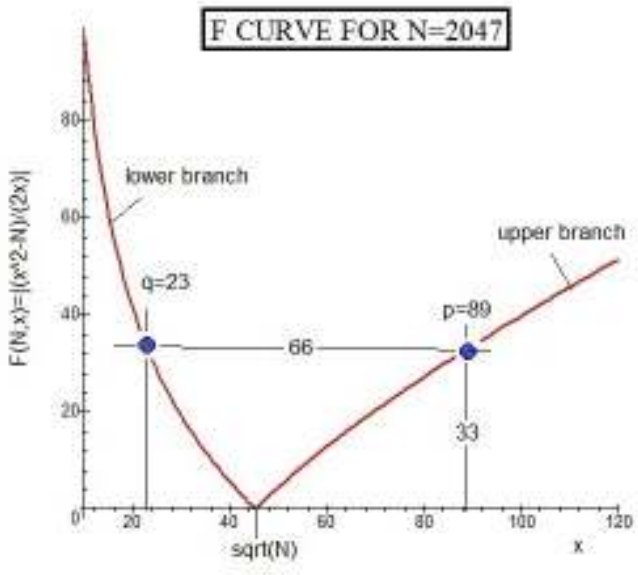
MORE ON THE EQUATION F(N,x)=|(x^2-N)/(2x)|

In a previous note we have shown that the semi-prime N=pq can be factored by finding that value of x for which F(N,x)=|(x^2-N)/(2x)|equals an integer. A demonstration of this point is found in the following graph of F(N,x) for the semi-prime number N=2047-



One sees that the function F(N,x), where F(N,p) and F(N,q) represent half the difference between the prime factors p and q, consists of two branches with q<sqrt(N)<p where F(N,q)=F(N,p). To factor N it is necessary to search along only one branch since the other value follows immediately from N/[integer(x)]. It appears that it will take fewer trial xs to find q along the lower branch than to discover p along the upper branch. For the special case of N=2047 it took six trial xs (43, 41, 37, 31, 29, 23) to find q and ten trials (47, 53, 59, 61, 67, 71, 73, 79, 83, 89) to find p. Thus, for the remainder of this note, we will concentrate only on the lower branch. There we have –

$$F(n,x)=(N-x^2)/(2x) \text{ with } 1<x<\sqrt{N}$$

The function always will have the negative slope-

$$dF(N,x)/dx=-(1/2)(1+N/x^2)$$

and its second derivative reads-

$$d^2F(N,x)/dx^2=N/x^3$$

We thus can define the lower branch by the second order differential expression-

$x^2F''-2F=x$ subject to $F[N,\sqrt{N}]=0$ and $dF[(N,\sqrt{N})]/dx=-1$

One is only interested in that value of F for which it equals an integer for a given integer trial function x. The tangent curve to F(N,x) at $x=x_0$ equals-

$$F(N,x)=F(N,x_0)-(1/2)(1+N/x_0^2)(x-x_0)$$

Note that, unlike for elliptic curves, this tangent curve does not intercept the F(N,x) curve at any other point.

We next look at the details of how one finds the one point along the F(N,x) curve for which x=q and F(N,q) is an integer. Since all factors of N are prime numbers which are odd (2 excepted), we need to consider only those values of x for which $x=x_0+2n+1$ with x_0 being an an arbitrarily chosen even number lying in the range $1<x_0<\sqrt{N}$ with n representing integers .

Consider the six digit long semi-prime N=510953 where sqrt(N)=714.805.. . Choosing $x_o=500$, we try the odd number values x=501+2n using the one line MAPLE command-

```
for n from 0 to 100 do {n, (-(501+2*n)^2+N)/(2*(501+2*n))}od;
```

It produces the integer value of F(N,q)=56 at n=80 so that q=501+2(80)=661 and p=N/q=773. Thus we have-

$$510953=661 \times 773$$

When we look at larger semi-primes , such as the twelve digit long number N= 230172046031 where sqrt(N)= 479762.4892, the number of required divisions jumps considerably. One can cut down on the number of required divisions by realizing that the only allowed xs are those which are prime numbers in the first place. Thus, if one has a large number of stored primes such as our MAPLE program which lists the first 50,000 primes , we can eliminate most of the odd number xs since they are not primes. For N=230172046031 we can use the program-

```
for n from 1800 to 2000 do
{n,evalf(-(ithprime(30000+n))^2+N)/(2*ithprime(30000+n))}od;
```

Here we have chosen for x_0 the ithprime(30000)=350377 and run n over the range - $0<n<2000$. The first integer value of F(N,x) occurs when n=2000 and yields x=q=376127 and F(N,q)= 117913. So we have the factored semi-prime-

$$230172004031=376127 \times 611953$$

When factoring even larger semi-primes the ithprime route will no longer be available since the primes above the fifty thousands are typically not stored in computer mathematics programs. This forces one back to using the $x=x_0+2n+1$ trial values. From the fundamental theorem for primes we know that there are approximately 2sqrt(N)/ln(N) primes lying below the integer closest to sqrt(N) and the total number of odd numbers in the same range is about (1/2)sqrt(N). Thus not having enough stored ithprimes will increase the number of required divisions by a factor of about (1/4)ln(N) for x in the range 1<x<sqrt(N). For a twelve digit number N this means an increase in divisions by a factor of about 7. For a hundred digit long semi-prime the number of divisions would increase by a factor of 58. Clearly for those wishing to factor a 100 digit long semi-prime, it would be of great advantage to have a stored table of the first 10^49 primes or so. If such a table could be constructed then the task of factoring hundred digit long semi-primes would be reduced to simply dividing N by each of the 10^49 stored primes until an integer value is reached. One could then dispense with other techniques such as we have discussed here and in earlier notes or other approaches found in the literature. For example, the Fermat Number 2^32+1=4294967297 where sqrt(N)=65536.00001 lies just at the limit of our computer stored ithprimes, so we can try-

for n from 1 to 200 do{n, ithprime(n), (2^32+1)/ithprime(n)}od;

and this yields the integer values-

{116, 6700417, 641}

which says that after 116 divisions, we have q=641 and p=6700417.

March 2013