SEMI-PRIMES AND THEIR FACTORS

Semi-primes are defined as N=pq, where p and q are its prime components. Without loss of generality one knows that-

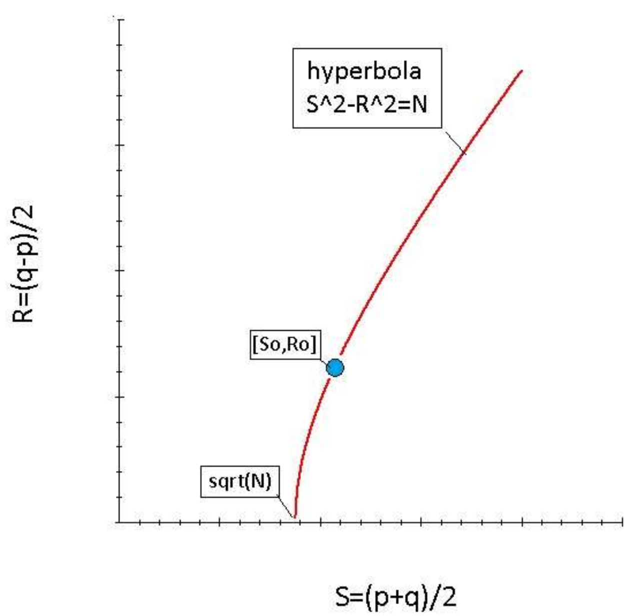
$$p< \mathrm{sqrt}(N)< q$$

Such numbers are very easy to construct via simple multiplication but are notoriously difficult to factor when the number of digits in N becomes large. It is this property which makes semi-primes play a significant role as public keys in cryptography. We wish in this note to further look at properties of N=pq.

We begin by defining the average value of p and q as S=(p+q)/2. Also we define the half difference between q and p as R=(q-p)/2. These new definitions allow us to write the semi-prime as-

$$S^2-R^2=N$$

Both S and R must be integers.This formula represents essentially one quarter of a hyperbola in the range $0<S<\infty$ and $0<R<\infty$. Here is its graph-



Note that there is only one point $[S_0,R_0]$ along this hyperbola where S and R both have finite integer values. For the simple case of N=77 we find $[S_0,R_0]=[9,2]$ meaning that p=7 and q=11.Using the definition of S, one can also write-

$$S=[\sigma(N)-N-1]/2$$

, where σ(N) is the sigma function of number theory. It [σ(N)] represents essentially the sum of all divisors of N. One is fortunate in that sigma(N) of up to about 40 digit length is given directly by most advanced computer programs.

Let us demonstrate the factoring of the Fermat number N=2^32+1=4294967297, where sqrt(N)=65536.00001. Here our MAPLE program yields in a split second that-

$$\sigma(N)=4301668356$$

From this we have S=3350529 and R=3349888. Combining, we get the factors-

$$p=S-R=641 \quad \text{and} \quad q=S+R=6700417$$

Pushing things to the limit of our home laptop, I next look at the forty digit long semi-prime-

$$N=3092054054324908237309972173911256672979$$

I constructed this number using an earlier discussed method found on our MATHFUNC page. Using this approach, we find the prime numbers-

p=exp(2)sqrt(23)/sin(Pi/3)-27= 40918739810545118939

and-

q=exp(3)cosh(2)+32=75565720465517824361

When multiplied together they yield the 40 digit long semi-prime given above.

Next we pretend that we don't know yet the values of p and q, and proceed to use our PC to evaluate –

S=sigma(N)-N-1= 58242230138031471650

It took just one minute to generate sigma(N) for this result. With S in hand, one next finds-

R=sqrt(S^2-N)= 17323490327486352711

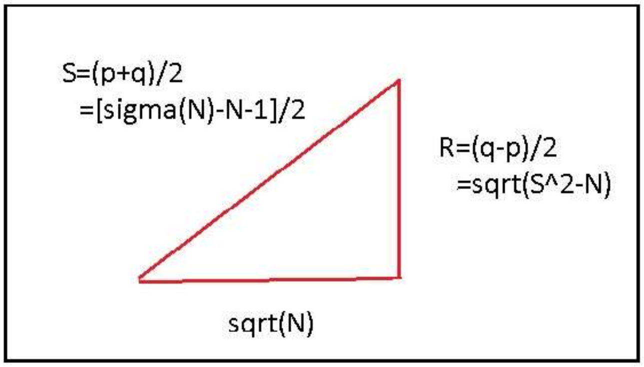
Combining we have the prime factors-

p=S-R= 40918739810545118939 and q=S+R=75565720465517824361

It is amazing how fast this factoring approach works for all semi-primes forty digit length or less. When going to sill larger digit Ns, the time to generate S rises dramatically and thus falls out of the range obtainable with one's PC. However with supercomputers one should be able to factor semi-primes as high as 100 digit length, thus making public key cryptography vulnerable. It is clear that the best approach for factoring still larger semi-primes is to find an improved method for generating sigma(N) . If such a method is found it will be much faster than presently employed generalized grid or elliptic curve approaches.

Going back to the above graph for S^2-R^2=N, we see that S, R, and sqrt(N) form a right triangle with S being the hypotenuse. The triangle looks as follows-

THE SEMI-PRIME TRIANGLE



For N=77 we have sqrt(77)=8.774964… , R=2, and S=9. That is, R^2+N=S^2. The tangent of the lower left vertex equals sqrt[(S^2/N)-1].

As already mentioned, finding sigma(N) values for semi-primes much above forty digit length becomes time prohibitive using one's home PC. There is, however, no difficulty in finding σ(N) once p and q are known. We there have-

$$\sigma(N)=1+p+q+pq$$

For N=77 this produces σ=96, while for N=3092054054324908237309972173911256672979 we find-

$$\sigma(N)=2S+1+N=3092054054324908237426456634187319616280$$

Note that for the second larger N we find N and σ(N) match each other for the first twenty digits or so. This follows from the fact that pq>>1+p+q.

U.H.Kurzweg
July 1, 2021
Gainesville, Florida