LATEST ON FACTORING LARGE SEMI-PRIMES

We have shown in earlier articles found on our Tech Blog or Mathfunc web pages that any semi-prime N=pq, where the primes p and q are both five or greater, has the form N mod(6)=1 or N mod(6)=5. We want here to review our new procedure for quickly factoring such larger semi-primes.

Case 1: N mod(6)=1

For this case we can write N=(6n+1)(6m+1) to get-

6nm+(n+m)=(N-1)/6=A

Noting that 6nm>>(n+m) for large N, we can write this equation as the simultaneous expressions-

nm=B+k and (n+m)=H-6k

, where B =[A-A mod(6)]/6 =(A-H)/6. On eliminating m we get the quadratic in n-

$$n^2+n(6k-H)+(B+k)=0$$

which solves as-

$$[n,m]=\left(\frac{1}{2}\right)\left\{(H-6k)\pm\sqrt{(36k^2-4k(1+3H)-4B+H^2}\right\} \quad \textit{, where one}$$
$$\textit{recalls that } p=6n+1 \quad \textit{and} \quad q=6m+1$$

What one now needs to do is to find the value of the constant k so as to make the radical R equal to an integer. Once this has been done the rest of the problem becomes trivial. Since generally H<<4B and k<<B, we see that the value of k must be lie outside the strip -sqrt(B)/3 and +sqrt(B)/3. Starting a search near these points will generally produce a correct value for k and R without too much effort. One can also write-

$$36k^2-4k(1+3H)-4B+H^2-R^2=0$$

Solving this for k produces-

$$k=\frac{1}{18}\left\{(1+3H)\pm\sqrt{1+6H+36B+9R^2}\right\}$$

A requirement is that the last radical equal a positive integer and one where k is also an integer. Carrying out such a search yields k which can then be used to get [n,m].

Let us demonstrate things for the semi-prime N=455839 where N mod(6)=1 and A=75973, H=1 and B=12662. So we will find the integer values of n and m from-

$$[n,m]=\left(\frac{1}{2}\right)\left\{(1-6k)\pm\sqrt{36k^2-16k-50647}\right\}$$

Here k will lie outside the strip ±sqrt(50647)/36=37.51 So we conduct a search near k=-38 and k=38. A simple search yields R=27 for k=38. So we get-

[n,m]=0.5{-227±27}=[-100,-127]

The presence of the minus signs in the answer to n and m, means that the numbers we are dealing with have the form-

p=6(103)-1=599 and q=6(130)-1=779

This particular semi-prime is the one which has been used in the literature to demonstrate the Lenstra Elliptic Curve factorization method (see Trappe, W., Washington, L. C. (2006). *Introduction to Cryptography with Coding Theory*). The speed and simplicity which we were able to accomplish the factorization of this number by the present method far exceeds anything possible by the Lenstra approach.

Case 2: N mod(6)=5

For this second case we can write (6n-1)(6m+1)=N. This is equivalent to-

$$6nm+(n-m)=\frac{(N+1)}{6}=A$$

, where this time A differs slightly but importantly from the form used earlier where N mod(6) was equal to one. Noting that 6nm>>(n-m) for larger Ns, we can rewrite things as-

nm=B+k and n-m=H-6k

, where as before H=A mod(6) and B=[A-Amod(6)]/6. Solving for n and m we find-

$$[n,m]=\left(\frac{1}{2}\right)\left\{(H-6k)\pm\sqrt{36k^2+4k(1-3H)+H^2+4B}\right\}$$

This time the radical R suggests that all positive and negative ks must be considered in a search. This can become rather time consuming without some further simplification. We do know that when k=0 the radical will have the fractional value of 2sqrt(B) . Also we can write-

$$36k^2+4k(1-3H)+H^2+4B-R^2=0$$

If we look at this as a quadratic in k, we find-

$$k=\left(\frac{1}{18}\right)\left\{(3H-1)+\sqrt{1-6H-36B+9R^2}\right\}$$

Here the radical must be a positive integer so we start the search for R>2sqrt(B) to get a good starting value R in this last radical which can then be used to find a lower bound on k.

Let us demonstrate this procedure for the semi-prime N=3239 where N mod(6)=5. We have A=540, H=0, and B=90. The radical for R becomes sqrt(-3239+9R^2). Searching near R=2sqrt(90)=18.97, we find R=20 for k=1. So the solution becomes-

$$[n,m]=(1/2)[(-6\pm20),(6+20)]=[7,13]$$

It leavers us with the solution-

$$3239=[6(7)-1][6(13)+1]=41 \times 79$$

Wow! Again a very simple and straight forward factoring achieved with elementary mathematical methods.

There is no reason why the present approach for either N mod(6)=1 or N mod(60=5 semi-primes should not work for very much larger Ns in the range of fifty digit length such as used in cryptography. Let us demonstrate things for the very seven digit long semi-prime-

N=:=7828229 where N mod(6)=5

It has A=1304705, H=5, and B=217450. We can estimate R as 2sqrt(B)= 933. So we search the radical in R starting at 933 to get R=959 at k=38. So we have the solution-

$$[n,m]=0.5[(-223+\pm959),(223+959)]=[368,591]$$

It produces the final factoring of-

$$7828229=[6(368)-1][6(591+1]=2207 \times 3547$$

Note that this time the actual value of R differs with the actual value of 959 by 2.7% . As N gets still larger this departure will increase requiring more trials for the actual R.

Finally let us go back to a larger N mod(6)=1 semi-prime . Here we take N=10416979. We find A=1736163, H=3, and B=289360. We estimate k to lie outside the range ±sqrt(B)/3=179 . Doing a search with k outside the strip |179| we get R=397 for k=-190. Thus we have the solution-

$$[n,m]=\left(\frac{1}{2}\right)\{3+6(190)\pm 387\}=[265, 378]$$

So we have the factorization –

10416979=[6(265)+1][6(378)+1]=2269 x 4591

Again easy to obtain. The departure from the initial estimate for k=- 179 compared to the correct value k=-190 is about ½ percent. It is important to remember in the above solutions that-

$$|k|>\frac{\sqrt{B}}{3} \quad and \quad A=\frac{(N-1)}{6} \quad when \quad N\bmod(6)=1$$

$$R>2\sqrt{B} \quad and \quad A=\frac{(N+1)}{6} \quad when \quad N\bmod(6)=5$$

U.H.Kurzweg
May 29, 2017
Memorial Day