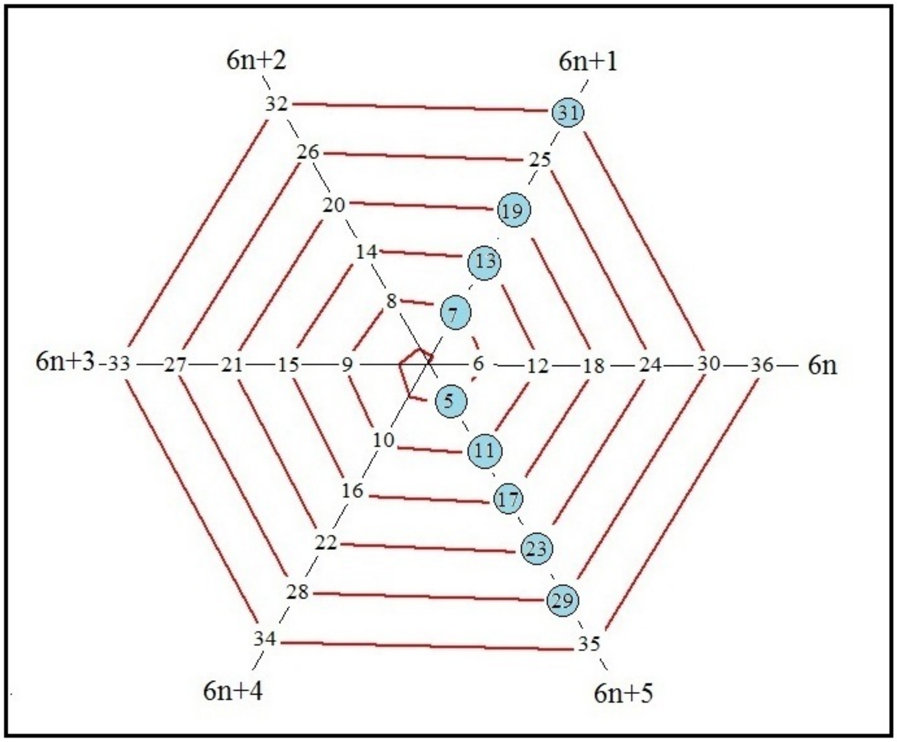
FACTORING OF SEMI-PRIMES USING DIOPHANTINE EQUATIONS

One of the remaining unsolved problems in number theory is how to find an algorithm which can efficiently factor large semi-primes N=pq, where p and q are prime numbers. We have been able to achieve some progress in recent years toward this goal by noting that all prime numbers greater than three and also semi-primes with both components greater than three must have the form $6n\pm1$. This last fact is beautifully demonstrated in the following hexagonal spiral integer graph which we came up with several years ago-



Here the prime numbers (shown in light blue) all lie along the two radial lines 6n+1 and 6n-1.(The radial line 6n-1 and 6n+5 are equivalentl). The gaps shown for 25=5x5 and 35 =5x7 in the graph represent semi-primes. What is clear is that both primes and semi-primes have the form $6n\pm1$. That is, a N mod(6) operation will always produce 1 or 5 for these numbers.

Let us now take a typicasl semi-prime N=6a+1, where a is a positive integer. This may be written, in view of the above, as-

$$6nm\pm(n+m)=(N-1)/6=a$$

with a, n, and m equal to integers. In this case N mod(6)=1 so that we have-p=6n±1 and q=6m±1

We begin our discussion by choosing p=6n+1 and q=6m+1. Upon setting –

x=nm   and y=n+m

we obtain the linear Diophantine Equation-

6x+y=(N-1)/6=a

This equation has the known closed form solutions-

x=s   and y=a-6s

, with s representing all positive and negative integers.

For larger n and m one notices the important fact that-

$$\frac{y}{6x}=\frac{(n+m)}{nm}<<1$$

This means that a first approximation for x will be the nearest integer value to (N-1)/36=a/6. We choose to designate this nearest integer value by 'b'. Then making the substitution x=b-z, since x should be slightly less than b, we get the alternate Diophantine form-

-6z+y=a-6b=c

The values of a, b and c are known since the semi-prime N is given. The integer solutions to this last equation are points lying along the straight line 6z=y-c. Only one of this infinite set of solutions will allow n and m to be a real integer. To find this special solution pair [n,m] we first note that x=nm and y=n+m is equivalent to-

$$n^2-ny+x=0$$

with the solution-

$$[n,m]=(\frac{1}{2})\{(c+6z)\pm\sqrt{(c+6z)^2-4(b-z)}\}$$

The only way n and m can be real is to have the radical in this equation satisfy-

$$\sqrt{(c+6z))^2-4(b-z)}=Positive\ Integer$$

And also satisfy the inequality- $\frac{[c+6z)]^2}{4(b-z)} \geq 1.$

The search for z will begin with the value of z where this last inequality is first satisfied.

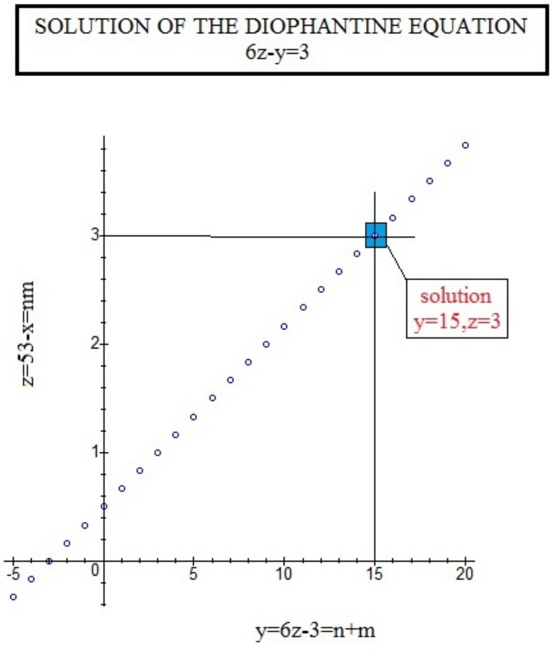
We begin our evaluation with the semi-prime N=1891 where N mod(6)=1, a=(1890)/6=315, the nearest integer to (N-1)/36 yields b=53, and c=a-6b=-3. It tells us to start the search at z=1 and go up to larger integer z. Doing so produces the integer solution of 5 for the radical at z=3. Thus we have-

$$[n,m]==(\frac{1}{2})\{15\pm 5\}=[10,5]$$

Hence we have factored N as-

$$1891=[6(10)+1][6(5)+1]=61 \text{ x } 31$$

Graphically we can demonstrate this result with the following point plot of the Diophantine solutions to 6z-y=3



We show there the infinite number of Diophantine solutions as small circles and the special solution of $z=3$ an $y=6z-3=15$ which yields $n=10$ and $m=5$.The big advantage of the present approach is that z will generally be a small integer so that the search will be relatively rapid.

To further show the enhanced capability of the present factoring algorithm, take next the larger semi-prime-

$$N= 7923367 \quad \text{where } N \bmod(6)=1,\ a= 1320561 ,\ b=220094, \text{ and } c=-3$$

Also by the above inequality we must have that $z>157$. So we use the search program-

```
for z form 157 to 200 do {z, sqrt((c+6*z)^2-4*(b-z))}od
```

It yields the integer radical value of 361 at $z=168$. It thus took just 11 simple computer evaluations to get our answer. The rest follows from-

$$[n,m]=0.5\{c+6(168)\pm361\}=[683, 322]$$

which produces the factored result-

$$7923367=[6(683)+1][6(322)+1]=4099 \times 1933$$

Up to this point we have only looked at the cases where $p=6n+1$ and $q=6m+1$. What about the case where N mod(6)=1 is represented by $p=6n-1$ and $q=6n-1$? The solution here will be identical with the above case except that n and m will both have negative signs and z changes sign. Such a case occurs for the prime number–

$$N=455839=[6(100)-1][6(127)-1]$$

which is often used in the literature to demonstrate the Lenstra Elliptic Curve factorization method. We get $a=(N-1)/6=75973$, $b=12662$, and $c=1$.This time z will be a negative number so we must change the sign of z on our lower limit inequality and also in our expression for [n,m]. Doing so we have that the search should start at $z=-37$ and run to still larger negative values. The solution procedure is straight forward and after just two trials yields the radical value of 27 at $z=-38$. It produces –

$$[n,m]=(0.5)\{-227\pm27\}=[-127,-100]$$

and yields $p=761$ and $q=599$. The speed with which this result was obtained is indeed impressive when compared with the much more involved Lenstra approach.

The one remaining case not yet discussed in this article occurs when N mod(6)=5. This time we have that-

$$N=[6n-1][6m+1]=36nm+6(n-m)-1$$

So we let x=nm, y=n-m, and a=(N+1)/6. All three variables are taken as integers. One obtains the Diophantine Equation-

$$6x+y=a \quad \text{with} \quad y/6x<<1$$

Chosing n>m, we see that 6x is slightly less than a. So letting b be the closest integer to a/6 we can define a new variable z=b-x. This produces the new Diophantine equation-

$$-6z+y=a-6b=c$$

This last equation is identical with that obtained for the N mod(6) case when p=6n+1 and q=6m+1 except that the definitions of a and b have changed slightly.

Let us try a specific N mod(6)=5 semi-prime case. We consider-

N= 814971 where N mod(6)=5, a=(N+1)/6= 139162, b= 23193, and c=4.

This time we find-

$$n=(\frac{1}{2})\{(4+6z)+\sqrt{(4+6z)^2+4(b-z)}\}$$

In this case one does not have a specific starting point for z to make the radical a positive integer. Thus we need to evaluate things about z=0 for both positive and negative integer values for z. Doing so we find that the radical has the integer value of 310 for z=9. It produces the result n=184 so that p=9(184)-1=1103. This leaves us with q=834971/1103=757=6(126)+1. Note that the m=126 value also follows from [310-4-6(9)]/2. The final factored result reads-

$$834971= 1103 \times 757$$

We have shown via the above examples that one may factor any large semi-prime by an algorithm based on a Diophantine Equation together with finding the integer value of a specified radical whose form depends on the value of N mod(6). It remains for someone to apply this method to semi-primes of the order of one hundred digit length where they are of importance in connection with public key cryptography. A comparison in factoring speed of this approach in comparison with the commonly used general number field sieve method would be very instructive.

U.H.Kurzweg
July 23, 2016