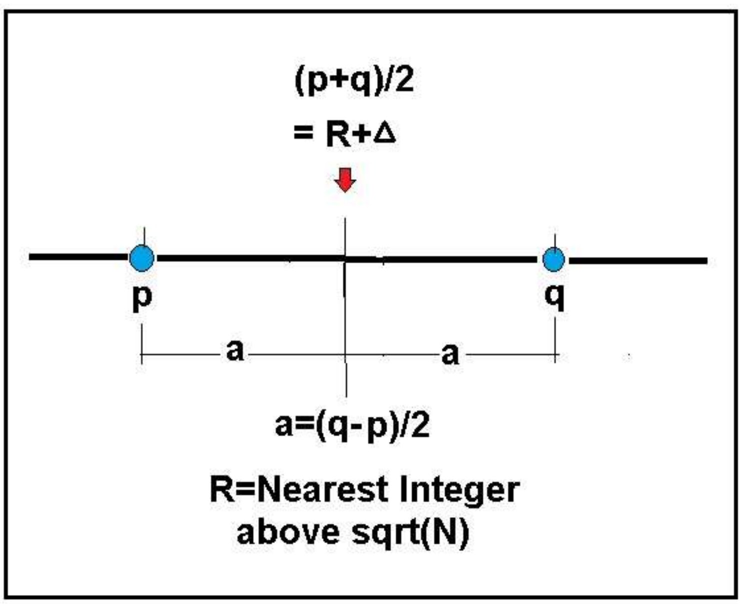
# LATEST ON FACTORING LARGE SEMI-PRIMES

## INTRODUCTION:

One of the incompletely solved problems in number theory is to find a way to quickly factor large semi-primes N=pq into their prime components. Numerous methods have been proposed but none have succeeded in factoring large one-hundred digit long values. We want here to introduce a new approach for factoring semi-primes based on the prime difference 2a=q-p and the departure from the mean 2Δ=(p+q) - 2R.

## CONSTRUCTING THE f(Δ,a) FUNCTION:

We begin by sketching the various components N,p,q,a,Δ involved in the new factoring approach. Here is the picture-




The mean value of (p +q)/2 equals R+Δ , with R being the next integer above sqrt(N). Also-

$$p=(R+\Delta)-a \qquad \text{and} \qquad q=(R+\Delta)+a$$

Taking the product of p and q , we get the new governing equation for factoring any semi-prime N=pq as-

$$a^2+N=(R+\Delta)^2$$

This is the important new equation relating Δ to 'a' and hence is the starting point for finding the factors p and q for any semi-prime. Note that the root of both sides of this equation must be equal to the same integer. Thus it must also be true that-

$$\mathrm{sqrt}(N+a^2) = R+\Delta \equiv \text{integer } n$$

**EVALUATION OF Δ AND a FOR SPECIFIC CASES:**

To find p and q we start with the simple one line computer search program-

```
for Δ from 0 to b do ({Δ, sqrt(-N+(R+Δ)^2)}) od;
```

, where b is chosen to be large enough to include the integer solution Δ. Running the program for a given N and hence also a given R, we get the integer values for both Δ and 'a' from which follow p and q.

Let us demonstrate this factoring for some specific cases starting with the simple semi-prime N=77 for which R=9. Here we carry out the search-

```
for Δ from 0 to 4 do ({Δ, sqrt(-77+(9+Δ)^2)})od;
```

After just one trial this produces Δ=0 and a=2. Thus we have p=9-2=7 and q=9+2=11.

Next we look at N=11303, where R=107. Here our search program produces Δ=1 and a=19. So we have the factors-

p=107+1-19=89 and q=107+1+19=127

For a third example consider the semi-prime N=455839 which has R=676. Here we find after four trials that Δ=4 and a=81. So the prime factors become-

p=(676+4)-81=599 and q=(676+4)+81=761

As a fourth specific example consider the seven digit long semi-prime-

N=7828229 where R=2798.

Doing a search for Δ we find Δ=79 and a=670. So we have -

p=(2798+79)-670=2207 and q=(2798+79)+670=3547

You will notice that the number of required search trials rapidly increases with increasing N so it would be a good idea for factoring larger semi-primes to start the search at some values of Δ greater than zero. To get some idea of what Δ to start the search with, one can look at the following table-

Integer Solutions of a=sqrt[-N+(R+Δ)^2]

| | | | | | |
|---|---|---|---|---|---|
| N=77 | R=9 | a=2 | Δ=0 | p=7 | q=11 |
| N=779 | R=28 | a=11 | Δ=2 | p=19 | q=41 |
| N=2701 | R=52 | a=18 | Δ=3 | p=37 | q=73 |
| N=11303 | R=107 | a=19 | Δ=1 | p=89 | q=127 |
| N=455839 | R=676 | a=81 | Δ=4 | p=599 | q=761 |
| N=7828229 | R=2798 | a=670 | Δ=79 | p=2207 | q=3547 |
| N=28787233 | R=5366 | a=2076 | Δ=387 | p=3677 | q=7929 |
| N=169331977 | R=13013 | a=6732 | Δ=1638 | p=7919 | q=21383 |
| N=3330853711 | R=57714 | a=12633 | Δ=1366 | p=46447 | q=71713 |

Here R is the nearest integer above sqrt(N) and

p=R+Δ-a and q=R+Δ+a

. All the numbers given there follow from –

a=sqrt([(R+Δ)^2-N]

, with R being the nearest integer above sqrt(N). Note that Δ<<a , n ≈ R, and R>> Δ.

Let us see from the table what a good starting point for the Δ search might be. Take the seven digit semi-prime N=2430101 where R=1559. From the table we have that –

$$81<a< 670 \quad \text{and} \quad 4<\Delta<79$$

So we could start the Δ search at about (4+79)/2 $\sim 41$. Doing this we get integer values at Δ=46 and a=382 after jus t five trials.

**CONCLUDING REMARKS:**

We have shown that large semi-primes can be evaluated using a new formula relating Δ to 'a'. Having found these values, one can then proceed to find-

$$p=(R+\Delta)-a \quad \text{and} \quad q=(R+\Delta)+a$$

To reduce the number of required trials for Δ, we can use an extended table to estimate a starting point for Δ greater than zero.

U.H.Kurzweg
May 13, 2023
Gainesville, Florida