QUAD NUMBERS AND THE FACTORING OF SEMI-PRIMES

INTRODUCTION:

In an earlier article on this Web Page we showed that any semi-prime N=pq can be factored into its two prime components-

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

by solving the Diophantine Equation-

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

Here 2a=(q-p) equals the prime number difference and R is the nearest integer above sqrt(N). This result means that the factoring of any semi-prime N is uniquely determined by the following four component quad -

$$Q= [N, R, a, \Delta]$$

So, for instance Q=[2701, 52, 18, 3] means that it represents the semi-prime N=2701 and its prime components p=(52+3)-18=37 and q-(52+3)+18=73. We wish to show in this article more details on how the components of a quad Q are obtained .

FINDING a AND Δ AND HENCE Q:

To find a and Δ for any N we start with a given semi-prime N and then pick a new integer R lying directly above the non-integer sqrt(N). Having obtained N and R we next go to the one-line computer program-

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

Here b is an integer sufficiently large to include the integer value of Δ. The integer c is larger than the integer value f Δ. Running the program for some ten specific cases of N, we obtain 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=7829
N=76357301	R=8739	a=1082	Δ=66	p=7723	q=9887
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

We see from the table that the quad numbers satisfy

$$N > R > a > \Delta$$

and R, a, and Δ increase rapidly in value as N increases. There is no obvious relation for a and Δ as one changes from one semi-prime N to another. The best one can do is to start the search with b =0 and go to c=200 to see if an integer factor exists. If not repeat the search with b=200 and go to c=400.If the factors are found stop. If not repeat the search with trials 400 to 600. Eventually the integer values for a and Δ will be found. Let us demonstrate things for the semi-prime N=81811999, where R=9045. Here the first trial run from b=0 to c=200 already fields the integers a=999 for Δ=55. This produces the unique quad-

Q=[81811999, 9045, 999, 55]

, with the prime factors-

p =(9045+55)-999=8101 and q=(9045+55)+999=10099

As a second example consider factoring N=44526491 where R=6673. This time it takes three 200 point trials to finds Δ=581 at a=2345. So we have the quad-

Q=[44526491, 6673, 2345, 581]

with the prime factors-

$$p=(6673+581)-2345=4409 \quad \text{and} \quad q=(6673+581)+2345=10099$$

Sometimes one can skip the lower 200 point trials when N is large and neighboring Δs become large.

CONCLUDING REMARKS:

We have shown that any semi-prime can be factored into its two prime components by solving the formula-

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

for integer a and Δ for a known N and R. The resultant solution can be written into a compact form via a unique Quad Number-

$$Q=[N,R,a,\Delta]$$

One of the lowest of these quads is Q=[15,4,1,0] corresponding to N=15 with p=3 and q=5.

U.H.Kurzweg
May 18, 2023
Gainesville, Florida