New Fastest Method to Find p & q of Given n.

Olvine Dsouza
Contact- olvind@ymail.com

Abstract

Where z is the product of two multiplied prime numbers, that is p and q. If the p and q as prime numbers having larger digits like 10, 50, 500 and more digits, then it is easier to multiply those two large numbers(p × q) to get z, but it is harder, more time consuming and can be a non- trivial solutions to reverse it back and find factors of z.

Introducing a new method of finding p and q of given z .

This method gives the fast result in finding either p or q of given z.

Where p × q = z

This method works in the principle of reduction in the value of z so as to minimize the calculation time and effort.

e.g we

z = 1384129, m = 1296 substitue it at below formula -

$$\frac{z}{m} = r$$

1384129 / 1296 = 1068.00 (ignore the decimals)

r = 1068 ......reduce value of z is used for further calculation.

This reduce the time and effort of calculation.

Steps to Solve Problems -

1) Reducing value of z -

Reducing value of z, where z is the product of multiple of p and q.

This method requires to reduce the value of z to any small digits so it will be easier for us to calculate z.

So if the z is of 1000 digits, then we can bring it down to 100 digits or lesser. So working to find solution become much easier.

To do this we will follow and use the method of -- 6 raised to power n, where 6 is the base and n is the powers. Raised to the power of n is equal to the multiplication of a, n times: a n = a × a × ... × a ... an

E.g., 6^3 = 216

Where base is 6 one can follow such calculations.

E.g., 6^2 = 6 × 6 , 6^3 = 6 × 6 × 6 and so on…

2) Finding Fixed Assumptions -

Using the above 6^3 = m we can find fixed fixed assumptions, which is required to use in the given formulas to find solutions. For finding list such assumptions, follow below method.

To Find Fixed Assumptions-

E.g, we want to find required 6^n = m for z = 1384129

Dividing the number of digits by 2,

1384129 has 7 digits, divide 7 / 2 = 3

So, our required 6^n = m, where m can be up to 3 to 4 digits.

and, 6^n = m will be.

6^3 = 216 …. is 3 digits integer.

6^3 = 1296 ……. is 4 digits integer.

So for any 7 digits z we must always take up to 3 to 4 digits assumptions.

Note –

One can go on finding required m by approximating m value depending in how larger digits of z by following above shown calculated method.

While doing calculation of ‘ Iterative Method For Getting Close Approximation', instead of calcualting all asumptions, one must follow the last larger assumption first, in order to reduce the multiple of operations and time of calculations. If we doesnt get the result from last last asumption, then only use the second last or the first asumption

E.g.

$6^2 = 36$ …. integer having 2 digits.

$6^3 = 216$ …. integer having 3 digits.

$6^4 = 1296$ …. integer having 4 digits.

Addjustmet of assumptions -

while calculating one can also adjust assumptions bt increasing it value by simply adding 6

e.g.

we got $6^2 = 36$ to use for calculation while solving problem. and find that we need to adjust by adding 6 as many times. So one can do it and use it for calculating. Check below example at -

3) Below is The List of Some Assumption One Can Use it While Finding Solutions.

-

10000 as five digits value of z requires $6^n = m$, where m can be 3 to 4 digits.

100000 as six digits value of z requires $6^n = m$, where m can be 3 to 4 digits.

1000000 as seven digits value of z requires $6^n = m$, where m can be 4 to 5 digits.

10000000 as eight digits value of z requires $6^n = m$, where m can be 4 to 5 digits.

100000000 as nine digits value of z requires $6^n = m$, where m can be 5 to 6 digits.

1000000000 as ten digits value of z requires $6^n = m$, where m can be 5 to 6 digits.

10000000000 as eleven digits value of z requires $6^n = m$, where m can be 6 to 7 digits.

100000000000 as twelve digits value of z requires $6^n = m$, where m can be 6 to 7 digits.

1000000000000 as thirteen digits value of z requires $6^n = m$, where m can be 7 to 8 digits.

.

.

.

10000.... as hundred digits value of z requires 6^{n} = m, where m can be 50 to 60 digits.

10000.... as hundred and one digits value of z requires 6^{n} = m, where m can be 50 to 60 digits.

10000.... as hundred and three digits value of z requires 6^{n} = m, where m can be up to 52 to 63 digits.

10000.... as hundred and three digits value of z requires 6^{n} = m, where m can be up to 52 to 63 digits.

Note - Always increase the gap between two asumptions as shown at above list.

e.g., For z = 10000 having five digits value. we can take 3 to 4 digits with 0 gap.

Same way for, z = 10000... having hundred digits value. we can take 50 to 60 digits having 10 gap .

This way increase gaps at every intervals as shown below -

1 to 10 digits - 0 gap.

10 to 99 digits - 10 gap.

100 to 999 digits - 20 gap.

and so on...

To find the value of 6^{n} = m, use below formula -

Check how many digits z has, then divide it by 2 to get required digits.

e.g.

use formula - total number of digits of z / 2

To find z = 10000, z has 5 digits therefore, 5/ 2 = 2.5

$6^2 = 36$ …. integer having 2 digits.

$6^3 = 216$ …. integer having 3 digits.

Close Approximation Adjustment-

While solving the problem, as we use the formula (r × 6 / g) +5, we alway get close approximation of final answer and those close approximate difference need to adjusted by subtracting as s - 1, s - 2; s - 3, s - 4 ….. s - n, and adding as s + 1, s + 2; s + 3, s + 4 ….. s + n, simultaneously, so on until we get the final answer. Check examples of any below solved problems at - Using Iterative Method For Getting Close Approximation's.

Using Simple Formula z / m = r -

$$\frac{z}{m} = r$$

Where, z is the product of p and q, m is from 6^n = m.

Guessing Positive Integers.

This step is required while we do final calculations as shown at below examples. Guess positive integers starting from 1, 2, 3, 4, 5…. and use it in the formula.

r / g = s

Where, r is from z / m = r, g is the guessing positive integers.(check the below examples for better understanding on how it works).

Examples Solutions -

First Example –

To find p and q of z

Where, z = 1384129

1^{st} Step – Find required 6^n = m.

Here as we can see the z = 1384129 is having a seven digits of integers.

Therefore, check above at '1.1 - Reduction value of z,' it states

1000000 as seven digits z requires 6^n = m, where m can be up to 3 to 4 digits.

So, we will take two assumptions having 2 and 4 digit integer.

6^3 = 216 …… 3 digit integer.
6^4 = 1296 …….. 4 digit integer.

2nd Step – Dividing z by m to get r and calculation by guessing.

Note - Alway start calcuation by following the last 6^n = m as first. We do this in order to reduce the calculation timing.
By taking the second 6^n = m,
6^4 = 1296
z = 1384129, m = 1296 substitue it at below formula -

$$\frac{z}{m} = r$$

1384129 / 1296 = 1068.00 (ignore the decimals)
r = 1068

Using Iterative Method For Getting Close Approximation's -

We can start by guessing g as starting from 2,3, 4, 5, 6, 7, 8, 9, 10... and use it at below formula to find final results.

Formula -

$$\frac{r \times 6}{g} + 5$$

(1068 × 6 / 2) +5 = 3209
(1068 × 6 / 3) +5 = 2141
(1068 × 6 / 4) +5 = 1607
(1068 × 6 / 5) +5 = 1286.6
(1068 × 6 / 6) +5 = 1073

.

.

.

.

1068 × 6 / 13) +5 = 497.923..

Ignore the decimals and we get 497

Let s = 497

We get very close approximation final answer only at 13th step.

The close approximate difference s need to adjusted by subtracting as s - 1, s - 2; s - 3, s - 4 ….. s - n, and adding as s + 1, s + 2; s + 3, s + 4 ….. s + n, simultaneously, so on until we get the final answer.

Here below, we have just done subtraction operation for presentation. One must do boith side operations to figure out the final anwer.

497 – 1 = 496

497 – 2 = 495

497 – 3 = 494

.

.

497 – 6 = 491

497 – 6 = 491, 1384129 is divisible 491

So, p = 491

Therefore, 2819 × 491 = 1384129

Second Example –

To find p and q of z

Where, z = 49949

1st Step Calculation to Find 6^3 = m -

Dividing the number of digits by 2,
49949 has 5 digits, divide 5 / 2 = 2.5
So, our required 6^n = m, where m can be roughly from 2 to 4 digits.
and, 6^n = m, will be.
6^2 = 36 …… 2 digit integer.
6^3 = 216 …… 3 digit integer.

Also at above '**List of Assumption' we find,**

Therefore we can take value depending as stated above at '1.1 - Reduction value of z'.
So we will take value of,
10000 as five digits value of z requires 6^n = m, where m can be up to 2 to 4 digits
So, we will take two assumptions having 2 and 3 digit integer.

6^2 = 36 …… 2 digit integer.
6^3 = 216 …… 3 digit integer.

2nd Step – Dividing z by m to get r and calculation by guessing.
Note - Alway start calcuation by following the last 6^n = m as first. We do this in order to reduce the calculation timing.
By taking the second 6^n = m,
6^3 = 216
z = 1384129, m = 216 substitue it at below formula -

$$\frac{z}{m} = r$$

49949 / 216 = 231.24537(ignore the decimals)
r = 231

Using Iterative Method For Getting Close Approximation's -

We can start by guessing g as starting from 2,3, 4, 5, 6, 7, 8, 9, 10… and use it at below formula to find final results.

Formula -

$$\frac{r \times 6}{g} + 5$$

(231 × 6 / 2) +5 = 698

(231 × 6 / 3) +5 = 467

(231 × 6 / 4) +5 = 351.5

.

.

.

.

(231 × 6 / 5) +5 = 282.2

Ignore the decimals and we get 282

Now let s = 282

Notice that we came to **very close approximation final answer only at 6th step having 236.**

The close approximate difference need to adjusted by subtracting as s - 1, s - 2; s - 3, s - 4 ….. s - n, and adding as s + 1, s + 2; s + 3, s + 4 ….. s + n, simultaneously, so on until we get the final answer.

Here below, we have just done subtraction operation for presentation. One must do boith side operations to figure out the final anwer.

282 – 1 = 281

282 – 2 = 280

282 – 3 = 279

.

.

282 – 31 = 251

236 - 31 = 251 ..... here at this step we found our required answer by adding 31

So, p = 251

Therefore, 251 × 199 = 49949

<u>Third Example –</u>

To find p and q of z

Where, z = 10345259

<u>1st Step Calculation to Find 6^3 = m -</u>

Dividing the number of digits by 2,

10345259 has 8 digits, divide 8 / 2 = 4

So, our required 6^n = m, where m can be up to 4 to 5 digits.

and, 6^n = m will be.

6^4 = 1296 ……. is 4 digits integer.

6^5 = 7776 ……. is 5 digits integer.

Also at above '**List of Assumption' we find,**

Here z = 10345259 has a eight digits of integers.

Therefore we can take value depending as stated above at '1.1 - Reduction value of z,'.

10000000 as eight digits value of z requires 6^n = m, where m can be up to 3 to 5 digits.

So we take,

$6^4 = 1296$ ……. is 4 digits integer.

$6^5 = 7776$ ……. is 5 digits integer

2^{nd} Step – Dividing z by m to get r and calculation by guessing.

Note - Alway start calcuation by following the last $6^n = m$ as first. We do this in order to reduce the calculation timing.

By taking the second $6^n = m$,

$6^3 =$

z = 10345259, m = 7776 substitue it at below formula -

$$\frac{z}{m} = r$$

10345259 / 7776 = 1330.4088(ignore the decimals)

r = 1330

<u>Using Iterative Method For Getting Close Approximation -</u>

We can start by guessing g as starting from 2,3, 4, 5, 6, 7, 8, 9, 10… and use it at below formula to find final results.

Formula -

$$\frac{r \times 6}{g} + 5$$

$(1330 \times 6 / 2) + 5 = 3995$

$(1330 \times 6 / 3) + 5 = 2665$

$(1330 \times 6 / 4) + 5 = 2000$

Notice above that we came to **very close approximation final answer only at 4^{th} step having 2000** those close approximate difference need to adjusted by subtracting as s - 1, s - 2; s - 3, s - 4 ….. s - n, and adding as s + 1, s + 2; s + 3, s + 4 ….. s + n, simultaneously, so on until we get the final answer.

Here below, we have just done subtraction operation for presentation. One must do boith side operations to figure out the final anwer, as stated at close approximation adjustment.

2000 + 1 = 2001 is our required answer.

2000 + 2 = 2002

2000 + 3 = 2003

.

.

.

2000 + 87 = 2087 ......here at this step we found our required answer by adding 87

So, p = 2087

Therefore, 2087 × 4957 = 10345259

Fourth Example –

To find p and q of z , z is having 120 digits

Where, z =
227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479

1st Step Calculation to Find 6^3 = m -

Dividing the number of digits by 2,
227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479

z has 120 digits, divide 120 / 2 = 60

So, our required 6^{n} = m, where m can be up to 60 to 70 digits.

and, 6^{n} = m will be.

6^{60} = 4.8873677980689E+46 ……. is a approx 50 to 60 digits integer.

6^{70} = 2.9552044145477E+54 ……. is a approx 50 to 70 digits integer.

2nd Step – Dividing z by m to get r and calculation by guessing.

Note - Alway start calcuation by following the last 6^{n} = m as first from above 6^{n}. We do this in order to reduce the calculation timing.

Here we take the second 6^{n} = m,

6^{70} = 2.9552044145477E+54

z = 227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479 , m = 2.9552044145477E+54 substitue it at below formula -

$$\frac{z}{m} = r$$

227010481295437363334259960947493668895875336466084780038173258247009162675779735389791151574049166747880487470296548479 / 2.9552044145477E+54 = 76,817,184,008,633,722,774,593,578,751,959,987,365,336,566,320,548,931,971,244,886,008

So, r = 76,817,184,008,633,722,774,593,578,751,959,987,365,336,566,320,548,931,971,244,886,008

Using Iterative Method For Getting Close Approximation & Final Answer-

We can start by guessing g as starting from 2,3, 4, 5, 6, 7, 8, 9, 10… and use it at below formula to find final results.

Formula -

$$\frac{r \times 6}{g} + 5$$

(76817184008633722774593578751959987365336566320548931971244886008 × 6 / 2) +5 =
230,451,552,025,901,168,323,780,736,255,879,962,096,009,698,961,646,795,913,734,658,029

(76817184008633722774593578751959987365336566320548931971244886008 × 6 / 3) +5 =
153,634,368,017,267,445,549,187,157,503,919,974,730,673,132,641,097,863,942,489,772,021

.

.

(76817184008633722774593578751959987365336566320548931971244886008 × 6 / 1407705) +5 =
327414553512136659774286141280850692575517880467351889655481

Let s =
327414553512136659774286141280850692575517880467351889655481

Notice above that we came to **very close approximation final answer at** 1407705 th **step having**

327414553512136659774286141280850692575517880467351889655481 as the answer.

Those close approximate difference need to adjusted by subtracting as s - 1, s - 2; s - 3, s - 4 ….. s - n, and adding as s + 1, s + 2; s + 3, s + 4 ….. s + n, simultaneously, so on until we get the final answer.

Here below, we have just done adding operation to directly show the difference, that we needed to do adjustment. One must do both side operations to figure out the final anwer, as stated at close approximation adjustment.

Actual answer -

327414555693498015751146303749141488063642403240171463406883

Answer which we got - -

327414553512136659774286141280850692575517880467351889655481

327414555693498015751146303749141488063642403240171463406883 -

327414553512136659774286141280850692575517880467351889655481 =

2,181,361,355,976,860,162,468,290,795,488,124,522,772,819,573,751,402 (this are the integers which we need to adjust to come up with the final answer).

Using the explained method, for this problem of 120 digit z, the calculation timing to come up with final answer was about half and hr with just simple computer and some proper guessing work.

Reference -

https://en.wikipedia.org/wiki/Shor%27s_algorithm

https://en.wikipedia.org/wiki/Integer_factorization