Innovative method to find primes of given semi-primes

Sachin Shinde

Software Test Engineer and Early Career Researcher
Pune, Maharashtra, India - 411045

Abstract *— Prime factorization has been very important since many years because of its experimental usages in various applications and the challenges associated with them. In digital technology many computer applications uses encrypted algorithms such as Rivest–Shamir–Adleman (RSA) for information security. The public and private keys of the encrypted code are represented using prime factors. A semi-prime being, a product of two prime numbers, has wide applications in RSA algorithms and pseudo number generators. The most common approach to split primes from semi-prime is* $\boldsymbol{K^2 - n = h^2}$*. In this research, we have found an unconventional and quicker way to split a given semi-prime. This article also reveals a specific series of numbers based on digital sum of a semi-prime. The paper also demonstrate how the series can be used to factor semi-prime that belongs to a particular SUM type.*

Keywords — *Prime numbers, Semi-prime, Prime factorization*

I. INTRODUCTION

A semi-prime is a product of two primes. We will consider a semi prime number 282943 and demonstrate how the existing method is used to split it into two primes. The approach uses $K^2 - n = h^2$ where $\sqrt{n}\ is \leq K$ and n is the given semi-prime. From this one can find h. To achieve the results, find the square root of given semi-prime and round it to nearest positive integer. The square root of 282943 is 531.9238. Thus $K = 532$.

$$K^2 - n = h^2$$
$$Thus, \quad 283024 - 282943 = h^2 = 81$$
$$K^2 - h^2 = n$$
$$532^2 - 81 = n$$
$$(532 - 9)(532 + 9) = n$$

Therefore, we know the prime numbers are $523\ and\ 541$.

II. FIND THE SUM TYPE

The research is based on the difference between two factored primes. The above semi-prime {282943 } shows that the sum of it's the digits are 10. $2 + 8 + 2 + 9 + 4 + 3 = 28\ and\ 2 + 8 = 10$.

Thus this semi prime can be classified as a SUM 10 type. One of the most significant outcomes of this study is that when there is a semi prime of SUM 10 or SUM 4 or SUM 7 types, the difference between the two primes is always going to be in the sequence of following series

$$6, 12, 18, 24, 30, 36\ and\ so\ on$$

III. USING THE SERIES

Now that we know when we have to use the series let's get into more details of how to use the above series.

$$With\ difference\ of\ 6\ \ it\ looks\ like\ this \qquad \left(\frac{6}{2}\right)^2 + 282943 = 282952$$
$$\sqrt{282952}\ \ does\ not\ give\ a\ positive\ integer$$
$$With\ difference\ of\ 12\ \ it\ looks\ like\ this \qquad \left(\frac{12}{2}\right)^2 + 282943 = 282979$$

$$\sqrt{282979}\ \ does\ not\ give\ a\ positive\ integer$$

$$With\ difference\ of\ 18\ \ it\ looks\ like\ this \qquad \left(\frac{18}{2}\right)^2 + 282943 = 283024$$

$$\sqrt{283024}\ \ gives\ a\ positive\ integer$$

It can be seen that in all above outputs 283024 is the only number whose square root gives a whole number. So it can be inferred that the difference between our prime factors is 18 .

Let's say $p\ and\ q$ are those prime factors. So if one prime is p other will be p +18.

$$p\ (p + 18) = 282943$$

$$p^2 + 18p + 81 = 282943 + 81$$

$$(p + 9)^2 = 283024$$

$$p + 9 = 532$$

$$p = 532 - 9$$

$$p = 523$$

$$q = p + 18$$

$$q = 523 + 18$$

$$q = 541$$

IV. SIMPLIFYING THE METHOD TO GET RESULTS MUCH QUICKER

A. SUM 10 Type Example

If we look at the same equation $K^2 -$ n $= h^2$ for a semi prime of 282943 we know that K equals 532. There is quicker way to apply the series for SUM 10 type. We just have to start adding and subtracting the square root from the series until we get a prime on each side.

Table 1. Prime factorization for SUM 10 type semi-prime of 282943

Step No	K= 532	
1	$subtracting\ 3\ \ from\ above\ 529\ \leftarrow$	$\rightarrow 535\ \ adding\ 3\ to\ above$
2	$subtracting\ 3\ \ from\ above\ \ 526\ \leftarrow$	$\rightarrow 538\ \ adding\ 3\ to\ above$
3	$subtracting\ 3\ \ from\ above\ 523\ \leftarrow$	$\rightarrow 541\ \ adding\ 3\ to\ above$

Table 1 Step no.3 gives the required answer. The two prime numbers are 523 and 541.

Let us take another example. Here we try to split a semi prime 24512077 into two primes. The digital sum of 24512077 is $2 + 4 + 5 + 1 + 2 + 0 + 7 + 7 = 28 = 2 + 8 = 10$. Therefore this is SUM 10 type and the difference between two primes is going to be in the sequence $6, 12, 18, 24, 30, 36\ and\ so\ on$ and root of n is 4950.96 so $K = 4951$.

Table 2. Prime factorization for SUM 10 type semi-prime of 24512077

Step No	K= 4951	
1	$subtracting\ 3\ \ from\ above\ 4948 \leftarrow$	$\rightarrow 4954\ adding\ 3\ to\ above$
2	$subtracting\ 3\ from\ above\ \ 4954 \leftarrow$	$\rightarrow 4957\ adding\ 3\ to\ above$
3	$subtracting\ 3\ \ from\ above\ 4942 \leftarrow$	$\rightarrow 4960\ adding\ 3\ to\ above$
4	$subtracting\ 3\ from\ above\ 4939 \leftarrow$	$\rightarrow 4963\ adding\ 3\ to\ above$
5	$subtracting\ 3\ \ from\ above\ 4936 \leftarrow$	$\rightarrow 4966\ adding\ 3\ to\ above$
6	$subtracting\ 3\ \ from\ above\ 4933 \leftarrow$	$\rightarrow 4969\ adding\ 3\ to\ above$

The resulting sixth step as shown in Table 2 renders product value of 24512077. So we have obtained two prime numbers from given semi prime $4933 * 4969 = 24512077$. Sometimes there exist certain small changes. For example value of k has been taken as 4951 and it resulted in required prime numbers. If the product of 4933 and 4969 does not equal to the given semi prime then the value of K can be taken as 4950 and the process can be repeated by adding/subtracting 3 from each side as illustrated above. To avoid this complication the proper method can be followed. Here value of K = 4951 does not play important role. Let us check for the difference $6, 12, 18, 24, 30, 36\ and\ so\ on$.

$$With\ difference\ of\ 6, \quad \left(\frac{6}{2}\right)^2 + 24512077 = 24512086$$
$$Square\ root\ of\ 24512086\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 12, \quad \left(\frac{12}{2}\right)^2 + 24512077 = 24512122$$
$$Square\ root\ of\ 24512122\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 18, \quad \left(\frac{18}{2}\right)^2 + 24512077 = 24512158$$
$$Square\ root\ of\ 24512158\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 24, \quad \left(\frac{24}{2}\right)^2 + 24512077 = 24512221$$
$$Square\ root\ of\ 24512221\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 30, \quad \left(\frac{30}{2}\right)^2 + 24512077 = 24512302$$
$$Square\ root\ of\ 24512302\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 36, \quad \left(\frac{36}{2}\right)^2 + 24512077 = 24512401$$
$$Square\ root\ of\ 24512401\ \ is\ a\ positive\ integer\ \ 4951$$

Thus the difference between two primes is 36. So if one prime is p and other is $p + 36$ then $p(p + 36) = 24512077$. $p^2 + 36p = 24512077$. Hence $p^2 + 36p + 324 = 24512401$. Solving this equation we get $(p + 18)^2 = 4951^2$. So $(p + 18) = 4951$ and $p = 4933$. This is one prime and other prime is $4933 + 36 = 4969$. Product of 4933 and 4969 is 24512077.

B. SUM 4 Type Example

906079 is a SUM 4 type semi-prime as $9 + 0 + 6 + 0 + 7 + 9 = 31 = 3 + 1 = 4$. Using the same series above, we can now check the difference.

$$With\ difference\ of\ 6, \quad \left(\frac{6}{2}\right)^2 + 906079 = 906088$$
$$Square\ root\ of\ 906088\ \ is\ not\ a\ positive\ integer$$

$$With\ difference\ of\ 12, \quad \left(\frac{12}{2}\right)^2 + 906079 = 906115$$
$$Square\ root\ of\ 906115\ is\ not\ a\ positive\ integer$$
$$With\ difference\ of\ 18, \quad \left(\frac{18}{2}\right)^2 + 906079 = 906160$$
$$Square\ root\ of\ 906160\ is\ not\ a\ positive\ integer$$
$$With\ difference\ of\ 24, \quad \left(\frac{24}{2}\right)^2 + 906079 = 906223$$
$$Square\ root\ of\ 906223\ is\ not\ a\ positive\ integer$$
$$With\ difference\ of\ 30, \quad \left(\frac{30}{2}\right)^2 + 906079 = 906304$$
$$Square\ root\ of\ 906304\ is\ a\ positive\ integer$$

Thus the difference between two primes is 30. So if one prime is p and other is $p + 30$ then $p(p + 30) = 906079$.

Hence $p^2 + 30p + 225 = 906079 + 225$

$(p + 15)^2 = 906304$. So $(p + 18) = 952$ and $p = 937$. This is one prime and other prime is $937 + 30 = 967$. Product of 937 and 967 is 906079 .

Alternatively, using the quicker method we derive $K = 951.88$ $so\ K \approx 952$

Table 3. Prime factorization for SUM 4 type semi-prime of 906079

Step No	K= 952	
1	$subtracting\ 3\ \ from\ above\ 949 \leftarrow$	$\rightarrow 955\ adding\ 3\ to\ above$
2	$subtracting\ 3\ from\ above\ \ 946 \leftarrow$	$\rightarrow 958\ adding\ 3\ to\ above$
3	$subtracting\ 3\ \ from\ above\ 943 \leftarrow$	$\rightarrow 961\ adding\ 3\ to\ above$
4	$subtracting\ 3\ from\ above\ 940 \leftarrow$	$\rightarrow 964\ adding\ 3\ to\ above$
5	$subtracting\ 3\ \ from\ above\ 937 \leftarrow$	$\rightarrow 967\ adding\ 3\ to\ above$

Therefore, Table 3 Step no. 5 gives the answer $937 * 967 = 906079$

V. CONCLUSIONS

In this paper, we proposed an unconventional method for semi-prime factorization that consist of identifying sum types and then using a series to derive primes. By exploiting the relationship between sum type and series identified, we provide a relatively simple, fast and scalable factorisation method that is much quicker than existing method. To find square root each time in this method is somewhat time consuming however we can further shorten it. It is generally observed that after adding $9, 36, 81, 144, 225$ & 324 we get a number and if the number ends with $2, 3, 7, 8$ we can affirm that they are not perfect squares. We have verified several semi-primes of SUM 10 and SUM4 types using this method and we confirm that the new approach gives accurate results. Our work in this paper forms the backbone in creating new research opportunities to investigate further into new possible SUM types and sequential series.

REFERENCES

[1] Stewart, Ian, Professor Stewart's Cabinet of Mathematical Curiosities

[2] Ishmukhametov, Shamil & Sharifullina, (2014). On distribution of semiprime numbers. Russian Mathematics. 58. 43-48. 10.3103/S1066369X14080052.

[3] du Sautoy, Marcus (2011). "What are the odds that your telephone number is prime?" The Number Mysteries: A Mathematical Odyssey through Everyday Life

[4] Dudley 1978, Section 2, Lemma 5, p. 15; Higgins, Peter M. (1998). Mathematics for the Curious. Oxford University Press. pp. 77–78. ISBN 978-0-19-150050-3

[5] Caldwell, Chris K. "The Top Twenty: Factorial". The Prime Pages. Retrieved 2017-01-03

[6] Riesel, Hans (1994). Prime Numbers and Computer Methods for Factorization (2nd ed.). Basel, Switzerland: Birkhäuser. p. 36. doi:10.1007/978-1-4612-0251-6. ISBN 978-0-8176-3743-9. MR 1292250.

[7] Caldwell, Chris K.; Xiong, Yeng (2012). "What is the smallest prime?" (PDF). Journal of Integer Sequences. 15 (9): Article 12.9.7. MR 3005530.

[8] Weisstein, Eric W. Semiprime: from Wolfram MathWorld

[9] Hua, L.K. (2009) [1965]. Additive Theory of Prime Numbers. Translations of Mathematical Monographs. 13. Providence, RI: American Mathematical Society. pp. 176–177.
[10] Goldston, D.A.; Graham, S.; Pintz, J.; Yildirim, C.Y. Small gaps between primes or almost primes. Trans. Am. Math. Soc. 2009, 361, 5285–5330
[11] Ambedkar, B.R.; Bedi, S.S. A New Factorization Method to Factorize RSA Public Key Encryption. Int. J. Comput. Sci. Issues (IJCSI) 2011, 8, 242–247
[12] Tiyaonse Chisanga Kabwe"Introducing a New Standard Formula for Finding Prime Numbers", International Journal of Mathematics Trends and Technology (IJMTT). V25(1):59-109 September 2015. ISSN:2231-5373. www.ijmttjournal.org. Published by Seventh Sense Research Group.
[13] McKee, J. Turning Euler's factoring method into a factoring algorithm. Bull. Lond. Math. Soc. 1996, 28, 351–355. [CrossRef]
[14] Kaddoura, I.; Abdul-Nabi, S. On formula to compute primes and the nth prime. Appl. Math. Sci. 2012, 6, 3751–3757
[15] Hiary, G.A. A Deterministic Algorithm for Integer Factorization. Math. Comput. 2016, 85, 2065–2069. [CrossRef]
[16] Neeraj Anant Pande"Maximum Spacing's between 2-PrimeFactors Numbers till 1 Trillion", International Journal of Mathematics Trends and Technology (IJMTT). V52(5):311-321 December 2017. ISSN:2231-5373. www.ijmttjournal.org. Published by Seventh Sense Research Group.