Applied Science Periodical **ISSN 0972-5504**
Volume - XXVII, No. 4, November 2025
Journal website: https://internationaljournalsiwan.com/applied-science.php
ORCID Link: https://orcid.org/0009-0008-5249-8441
International Impact Factor: **7.0** https://impactfactorservice.com/home/journal/2296
Google Scholar: https://scholar.google.com/citations?user=BRweiDcAAAAJ&hl=en
Refereed and Peer-Reviewed Quarterly Periodical

Application of Vedic Sutras - I (Elite Project - 2024)

by **Gaurav Kumar,** *B.Sc. (H) Mathematics II Year,*
Acharya Narendra Dev College, University of Delhi, India
Sarita Agarwal, *Assistant Professor,*
Department of Mathematics,
Acharya Narendra Dev College, University of Delhi, India

(Received: September 5, 2025; Accepted: October 3, 2025;
Published Online: November 29, 2025)

Abstract:

"Ekadhikena Purvena" is a Vedic sutra that translates to "by one more than the previous one." It is primarily used in multiplication, particularly when multiplying numbers close to powers of 10. The method simplifies calculations by focusing on the digits to the left of the base number and adding one to it, which can then be used to quickly find the product.

"Nikhilam Navatascharmam Dasatah" means "all from 9 and the last from 10." This sutra is applied to perform multiplication of numbers that are close to a base, such as 10, 100, or 1000. It involves subtracting each digit of the number from 9, except the last digit, which is subtracted from 10. This technique reduces the complexity of multiplication, especially when dealing with large numbers.

In this paper we have studied the application of Ekadhikena purvena and Nikhilam Navatascharmam Dasatah.

Introduction:

Vedic mathematics is part of four Vedas (books of wisdom).

It is part of Sthapatya-Veda (book on civil engineering and architecture), which is an upa-veda (supplement) of Atharva Veda.

It gives explanation of several mathematical terms including arithmetic, geometry (plane, co-ordinate), trigonometry, quadratic equations, factorization and even calculus.

His Holiness Jagadguru Shankaracharya Bharati Krishna Teerthaji Maharaja (1884-1960) comprised all this work together and gave its mathematical explanation while discussing it for various applications.

Swamiji constructed 16 sutras (formulae) and 16 Upa sutras (sub formulae) after extensive research in Atharva Veda.

Obviously, these formulae are not to be found in present text of Atharva Veda because these formulae were constructed by Swamiji himself.

The word "Vedic" is derived from the word "Veda" which means the store-house of all knowledge. Vedic mathematics is mainly based on 16 Sutras dealing with various branches of mathematics like arithmetic, algebra, geometry, etc.

These Sutras along with their brief meanings are enlisted below alphabetically.

1. (Anurupye) Shunyamanyat - If one is in ratio, the other is zero.
2. Chalana-Kalanabyham - Differences and Similarities.
3. Ekadhikina Purvena - By one more than the previous One.
4. Ekanyunena Purvena - By one less than the previous one.
5. Gunakasamuchyah - The factors of the sum is equal to the sum of the factors.

6. Gunitasamuchyah - The product of the sum is equal to the sum of the product.
7. Nikhilam Navatashcaramam Dashatah - All from 9 and last from 10.
8. Paraavartya Yojayet - Transpose and adjust.
9. Puranapuranabyham - By completion or noncompletion.
10. Sankalana- vyavakalanabhyam - By addition and by subtraction.
11. Shesanyankena Charamena - The remainders by the last digit.
12. Shunyam Saamyasamuccaye - When the sum is the same that sum is zero.
13. Sopaantyadvayamantyam - The ultimate and twice the penultimate.
14. Urdhva-tiryagbhyam - Vertically and crosswise.
15. Vyashtisamanstih - Part and Whole.
16. Yaavadunam - Whatever the extent of its deficiency.

Ekadhikena Purvena:
(एकाधिकेन पूर्वेण) [6, 8]

The Sutra (formula) Ekadhikena Purvena means: "By one more than the previous one". (पिछले से एक अधिक)

Applications:

I) Squares of numbers ending in 5:
(5 से समाप्त होने वाली संख्याओं का वर्ग)

Now we relate the sutra to the 'squaring of numbers ending in 5'. Consider example 25^2.

Here the number is 25. We have to find out the square of the number. For the number 25, the last digit is 5 and the 'previous' digit is 2. Hence, 'one more than the previous one', that is, $2 + 1 = 3$. The Sutra, in this context, gives the procedure to multiply the previous digit 2 by one more than itself, that is, by 3. It becomes the L.H.S (left hand side) of the result, that is, $2 \times 3 = 6$. The R.H.S (right hand side) of the result is 5^2, that is, 25.

Thus $25^2 = 2 \times 3/25 = 625$.

In the same way,

$35^2 = 3 \times (3 + 1)/25 = 3 \times 4/25 = 1225$.

$65^2 = 6 \times 7/25 = 4225$.

$105^2 = 10 \times 11/25 = 11025$.

$135^2 = 13 \times 14/25 = 18225$.

II) To finding product of two numbers whose sum of digit at unit place is 10 and rest the digit are same.

(दो संख्याओं का गुणनफल ज्ञात करना जिनके इकाई स्थान पर अंकों का योग 10 है और शेष अंक समान हैं)

Example: 52×58

In this example, we clearly see that sum of digits at unit place is 10 and the rest digits are same. The previous digit is 5. Hence, 'one more than the previous one', that is $5 + 1 = 6$. The sutra in this context, gives the procedure to multiply the same digit 5 by one more than itself, that is by 6. It becomes the L.H.S (left hand side) of the result, that is, $5 \times 6 = 30$. The R.H.S (right hand side) of the result is given by multiplying the unit digits numbers that is $2 \times 8 = 16$.

Thus $52 \times 58 = 5 \times 6/2 \times 8 = 3016$.

In the same way,

$77 \times 73 = 7 \times 8/7 \times 3 = 5621$.

$19 \times 11 = 1 \times 2/9 \times 1 = 2/09 = 209$.

$109 \times 101 = 10 \times 11/9 \times 1 = 110/09 = 11009$.

$121 \times 129 = 12 \times 13/1 \times 9 = 156/09 = 15609$.

III) Vulgar fractions whose denominators are numbers ending in nine.

(साधारण भिन्न जिनके हर नौ पर समाप्त होने वाली संख्याएँ हैं)

We now take examples of $1/a9$, where $a = 1, 2, ..., 9$. In the conversion of such vulgar fractions into recurring decimals, Ekadhika process can be effectively used both in division and multiplication.

a) Division Method: Value of 1/19.

The numbers of decimal places before repetition is the difference of numerator and denominator, i.e., 19 - 1 = 18 places.

For the denominator 19, the purva (previous) is 1.

Hence Ekadhikena purva (one more than the previous) is 1 + 1 = 2.

The sutra is applied in a different context. Now the method of division is as follows:

Step 1: Divide numerator 1 by 20.
i.e., 1/20 = 0.1/2 = $._1$0 (0 times, 1 remainder)

Step 2: Divide 10 by 2
i.e., 0.$0_0$5 (5 times, 0 remainder)

Step 3: Divide 5 by 2
i.e., 0.05$_1$2 (2 times, 1 remainder)

Step 4: Divide $_1$2 i.e., 12 by 2
i.e., 0.0526 (6 times, No remainder)

Step 5: Divide 6 by 2
i.e., 0.05263 (3 times, No remainder)

Step 6: Divide 3 by 2
i.e., 0.05263$_1$1(1 time, 1 remainder)

Step 7: Divide $_1$1 i.e., 11 by 2
i.e., 0.052631$_1$5 (5 times, 1 remainder)

Step 8: Divide $_1$5 i.e., 15 by 2
i.e., 0.0526315$_1$7 (7 times, 1 remainder)

Step 9: Divide $_1$7 i.e., 17 by 2
i.e., 0.05263157 $_1$8 (8 times, 1 remainder)

Step 10: Divide $_1$8 i.e., 18 by 2
i.e., 0.0526315789 (9 times, No remainder)

Step 11: Divide 9 by 2
i.e., 0.0526315789 $_1$4 (4 times, 1 remainder)

Step 12: Divide $_1$4 i.e., 14 by 2
i.e., 0.052631578947 (7 times, No remainder)

Step 13: Divide 7 by 2
i.e., 0.052631578947$_1$3 (3 times, 1 remainder)

Step 14: Divide $_1$3 i.e., 13 by 2
i.e., 0.0526315789473$_1$6 (6 times, 1 remainder)

Step 15: Divide $_1$6 i.e., 16 by 2
i.e., 0.052631578947368 (8 times, No remainder)

Step 16: Divide 8 by 2
i.e., 0.0526315789473684 (4 times, No remainder)

Step 17: Divide 4 by 2
i.e., 0.05263157894736842 (2 times, No remainder)

Step 18: Divide 2 by 2
i.e., 0.052631578947368421 (1 time, No remainder)

Now from Step 19, i.e., dividing 1 by 2, Step 2 to Step 18 repeats thus giving 1 / 19 = 0.052631578947368421.

b) Multiplication Method: Value of 1 / 19

First, we recognize the last digit of the denominator of the type 1 / *a*9. Here the last digit is 9.

For a fraction of the form in whose denominator 9 is the last digit, we take the case of 1 / 19 as follows:

For 1 / 19, 'previous' of 19 is 1. And one more than of it is 1 + 1 = 2.

Therefore 2 is the multiplier for the conversion. We write the last digit in the numerator as 1 and follow the steps leftwards.

Step 1: 1

Step 2: 21(multiply 1 by 2, put to left)

Step 3: 421(multiply 2 by 2, put to left)

Step 4: 8421(multiply 4 by 2, put to left)

Step 5: $_1$68421 (multiply 8 by 2 =16, 1 carried over, 6 put to left)

Step 6: $_1$368421 (6 × 2 =12 & +1 [Carry over]
= 13, 1 carried over, 3 put to left)

Step 7: 7368421 (3 × 2 = 6 +1 [Carry over]
= 7, put to left)

Step 8: $_1$47368421 (as in the same process)

Step 9: 947368421 (continue to step 18)

Step 10: $_1$8947368421

Step 11: $_1$78947368421

Step 12: $_1$578947368421

Step 13: $_1$1578947368421

Step 14: 31578947368421

Step 15: 631578947368421

Step 16: $_1$2631578947368421

Step 17: 52631578947368421

Step 18: 1052631578947368421

Now from step 18 onwards the same numbers and order towards left continue. Thus 1 / 19 = 0.052631578947368421.

Application of Ekadhikena Purvena in Calculus [10]:

Preliminary Ideas:

To understand the importance of this sutras, we should have the following basic concepts of Calculus.

Power Series: If the power series of a function $f(x)$ has a radius of convergence $R > 0$ and an interval of convergence $x_0 - R < x < x_0 + R$, then the series may be differentiated and integrated term-by-term i.e., once a function is written in power series, it can be differentiated and integrated quite easily, by treating every term separately. We pick up a constant of integration C, that is outside of the series here in the antiderivative of $f(x)$.

Power Rule of Antiderivative: If $n(\neq -1)$ is any real number, then

$$\int x^n \, dx = (x^{n+1}/n + 1) + C \tag{i}$$

where C is an arbitrary constant of integration, which is generally added after finding antiderivative. This exists due to the following derivative formula

$$d/dx(x^{n+1}/n + 1) = x^n$$

Here $n = -1$ will lead to division by zero, so it is excluded from the formula.

Antiderivative Using Vedic Sutra: The Vedic sutra 'Ekadhikena Purvena' gives the antiderivative of a function, which contains only powers of x. In finding integration, we use it which means "one more than the previous index to integrate the power term of the function and divide it by coefficient by the new index" i.e.,

$$\int x^n dx = x^{n+1}/n + 1 \tag{ii}$$

It is clear that for $n = -1$, division by zero occurs, which fails the sutra. Therefore we use the above rule for all real numbers except $n = -1$.

Example 1: Find the indefinite integral

$$\int x^7 dx$$

We have using the above rule

$$\int x^7 dx = x^{7+1}/7 + 1 = x^8/8$$

Here Ekadhika of index 7 is $7 + 1 = 8$ and the coefficient = 8. In it we may add a constant of integration.

Similarly, we can find the antiderivative using Vedic sutra as follows.

Example 2:

$$\int \cos x\, dx = \int (1 - x^2/2! + x^4/4! - x^6/6! + \cdots + x^{2n}/(2n)! + O[x]^{2n+2})\, dx$$

$$= x - x^3/2!3 + x^5/4!5 - x^7/6!7 + \cdots + x^{2n+1}(2n)!(2n+1) + O[x]^{2n+3} + K$$

$$= x - x^3/3! + x^5/5! - x^7/7! + \cdots + x^{2n+1}/(2n+1)! + O[x]^{2n+3} + K$$

$$= \sin x + K$$

where K is a constant of integration.

Example 3:

$$\int \sin x\, dx = \int (x - x^3/3! + x^5/5! - x^7/7! + \cdots + x^{2n+1}/(2n+1)! + O[x]^{2n+3})\, dx$$

$$= x^2/2 - x^4/3!4 + x^6/5!6 - x^8/7!8 + \cdots + x^{2n+2}/(2n+1)!(2n+2) + O[x]^{2n+4} + K$$

$$= -1 + x^2/2 - x^4/3!4 + x^6/5!6 - x^8/7!8 + \cdots + x^{2n+2}/(2n+1)!(2n+2) + O[x]^{2n+4} + (K+1)$$

$$= -(1 - x^2/2 + x^4/3!4 - x^6/5!6 + x^8/7!8 - \cdots + x^{2n+2}/(2n+1)!(2n+2) + O[x]^{2n+4} + (K+1)$$

$= -\cos x + C$, where $C = K + 1$ is a constant of integration.

Example 4:

$$\int \cos hx\, dx = \int \sum x^{2n}/(2n)!\, dx$$

$$= \sum \int x^{2n}/(2n)!\, dx$$

$$= \sum x^{2n+1}/(2n+1)(2n)!$$

$$= \sum x^{2n+1}/(2n+1)!$$

$$= \sin hx$$

Example 5:

$$\begin{aligned}\int \sin hx\, dx &= \int \sum x^{2n+1}/(2n+1)!\, dx \\ &= \sum \int x^{2n+1}/(2n+1)!\, dx \\ &= \sum x^{2n+2}/(2n+2)(2n+1)! \\ &= \sum x^{2(n+1)}/(2n+2)! \\ &= \sin hx + K\end{aligned}$$

Example 6:

$$\begin{aligned}\int e^x dx &= \int (1+x+x^2/2!+x^3/3!+x^4/4!+\cdots+x^n/n!+O[x]^{n+1}) \\ &= x+x^2/2!+x^3/3!+x^4/4!+\cdots+x^{n+1}/(n+1)!+O[x]^{n+2} \\ &= 1+x+x^2/2!+x^3/3!+x^4/4!+\cdots+x^{n+1}/(n+1)!+O[x]^{n+2}-1+K \\ &= 1+x+x^2/2!+x^3/3!+x^4/4!+\cdots+x^{n+1}/(n+1)!+O[x]^{n+2}+K \\ &= e^x+K\end{aligned}$$

Limitations:

The problem starts when after operations applied, the new series is not an expression of any known elementary functions.

Because every finite or infinite series is neither a series expansion of an elementary function nor an expression of closed form of elementary functions.

For example,

$$\begin{aligned}\int e^x/x\, dx &= \int 1/x(1+x+x^2/2!+x^3/3!+\cdots+x^k/k!+O[x]^{k+1})\, dx \\ &= \int (1/x+1+x+x/2!+x^2/3!+\cdots+x^{k-1}/k!+O[x]^k)\, dx \\ &= \mathrm{In}(x)+x+x^2/2!.2+x^3/3!.3+\cdots+x^k/k!.k+O[x]^{k+1}+K\end{aligned}$$

This series can't be denoted by an elementary function. That's why it is known as a nonelementary function or nonelementary integral.

Thus term-wise derivative and antiderivative terminate at this point. Modern techniques of integration also don't solve these problems.

Nikhilam Navatascaramam Dasatah:

All from nine and last from ten. [6, 9]

Applications:

1. Substraction: Subtracting a number from a power of 10 {like 10, 100, 1000…}

Example - 10^6-533928

533928
466072

Example - 10^5-4928

04928
95072

Example - 10^8-23456

00023456
99976544

2. Multiplying two number which are closed to the same power of 10:

Example: 9997 × 9898

Step 1) Identify the base of the number like (10000).

Step 2) Find deviation from base.

Step 3) Multiply the deviation on R.H.S. and subtract deviation from multiplier on L.H.S.

9997	3
× 9898	102
9895	0306

9997 × 9898 = 98950306

Example: 9992 × 9997

9992	8
× 9997	3
9989	0024

9992 × 9997 = 99890024

(Case-II): Both the number are higher than the base:

The method and rules are same with a little difference is the positive deviation. Instead of cross-subtract, we follow cross-add.

Example: 13 × 12

Base is 10

13	3
× 12	2
15	6

13 × 12 = 156

Example: 1275 × 1004

Base is 1000

1275	275
× 1004	004
1279	1100

1275 × 1004 = 1280100

In this example right hand side is greater than the base, hence, add 1 to left hand side.

Nikhilam Division:

Consider some two-digit numbers (dividends) and same divisor 9. Observe the following example.

i) 13 ÷ 9 The quotient (Q) is 1, Remainder (R) is 4.

Since

$$9)\ 13\ (1$$
$$\underline{9}$$
$$4$$

ii) $34 \div 9$, Q is 3, R is 7.

iii) $60 \div 9$, Q is 6, R is 6.

iv) $80 \div 9$, Q is 8, R is 8.

Now we have another type of representation for the above examples as given here under:

i) Split each dividend into a left-hand part for the quotient and right-hand part for the remainder by a slant line or slash.

ii) Eg. 13 as 1/3, 34 as 3/4, 80 as 8/0.

iii) Leave some space below such representation, draw a horizontal line

Eg. 1/3 3/4 8/0

iv) Put the first digit of the dividend as it is under the horizontal line. Put the same digit under the right-hand part for the remainder, add the two and place the sum i.e., sum of the digits of the numbers as the remainder.

1/3	3/4	8/0
1	3	8
1/4	3/7	8/8

Now the problem is over. i.e.,

$13 \div 9$ gives $Q = 1$, $R = 4$

$34 \div 9$ gives $Q = 3$, $R = 7$

$80 \div 9$ gives $Q = 8$, $R = 8$

Proceeding for some more of the two digit number division by 9, we get

a) $21 \div 9$ as

9) 2/1 i.e $Q = 2, R = 3$
2
2/3

b) $43 \div 9$ as

9) 4/3 i.e $Q = 4, R = 7$
4
4/7

The examples given so far convey that in the division of two digit numbers by 9, we can mechanically take the first digit down for the quotient-column and that, by adding the quotient to the second digit, we can get the remainder.

Dividing any number by a number close to and less than power of 10:

Example: 698/92

Base = 100

Deviation = 8

Last digit x deviation = $6 \times 8 = 48$

6/98
+48
146

$Q = 6 + 1 = 7$

Step 1) Multiply deviation and add with remaining

Step 2) Remainder 146 > 92

So, 146 - 92 = 54

$R = 54$

Multiplication of two numbers using integer modulo *n*:

Proposition[3]: Let $a, b, n \in N$ be three positive integers such that

$a \equiv (a - n) \pmod{n}$ and $b \equiv (b - n) \pmod{n}$. Then there exist integers $x, y \in N$, $x < n$ and $y < n$, such that

$x \equiv (a - n)(b - n) (\text{mod } n)$ and $y \equiv ((a - n) + (b - n)) (\text{mod } n)$ and the multiplication of a and b is given by, $ab = ny + x$.

Proof: For any $a, b, n \in N$ be three integers such that $a < b < n$. Then,

$$a \equiv a' \ (\text{mod } n)$$

and

$$b \equiv b' \ (\text{mod } n).$$

Where, $a' = a - n$ & $b' = b - n$ that gives,

$$a = a' + n \ \& \ b = b' + n \qquad \text{(i)}$$

For some $k \in N$ we can write,

$$a \times b \equiv a' \times b' \ (\text{mod } n)$$

$$a \times b = nk + a'b' \qquad \text{(ii)}$$

From (i)

$$(a' + n)(b' + n) = nk + a'b'$$

$$nk = (a' + n)(b' + n) - a'b'$$

$$nk = a'b' + nb' + a'n + n^2 - a'b'$$

$$nk = n(a' + b' + n)$$

$$k = (a' + b' + n) \qquad \text{(iii)}$$

$$a \times b = n(n + a' + b') + a'b' \qquad \text{from (ii)}$$

Which is statement of the proposition and exactly same as the general form of Nikhilam Sutra.

By substituting for a' and b', we can write

$$a \times b = n(a + b - n) + (a - n)(b - n) \qquad \text{(iv)}$$

Example: In decimal number system, to find 993×998

choose integer $n = 1000$ and substitute in (iv),

$$993 \times 998 = 1000(993 + 998 - 1000) + (993 - 1000)(998 - 1000)$$
$$= 1000(993 - 2) + (-7)(-2)$$
$$= 991{,}000 + 14$$
$$= 991{,}014$$

Example: In binary number system,

To find $(1101)_2 \times (1010)_2$ choose integer $n = (1000)_2$ and substitute in (iv),

$$(1101)_2 \times (1010)_2 = (1000)\,[1101 + 1010 - 1000] + (1101 - 1000)\,(1010 - 1000)$$
$$= (1000)\,[1111] + (101)(10)$$
$$= 1111000 + 1010$$
$$= (10000010)_2$$

The above example shows that chosen integer n, need not be greater than the multiplier and multiplicand in case of binary multiplication.

Multiplication of three integers:

Let any $a, b, c, n \in N$ be four integers such that $a < b < c < n$. Then, $a \equiv a'(\text{mod } n)$, $b \equiv b'(\text{mod } n)$ and $c \equiv c'(\text{mod } n)$. Where, $a' = a - n$, $b' = b - n$ and $c' = c - n$ that gives,

$$a = a' + n,\ b = b' + n \text{ and } c = c' + n \qquad \text{(i)}$$

For some $k \in N$ we can write,

$$a \times b \times c \equiv a' \times b' \times c' \ (\text{mod } n)$$
$$a \times b \times c = nk + a'b'c' \qquad \text{(ii)}$$

Further, substitute $a = (a' + n)$, $b = (b' + n)$ and $c = (c' + n)$ into (ii) to find k,

$$nk = a \times b \times c - a'b'c'$$
$$nk = (a' + n)(b' + n)(c' + n) - a'b'c' \quad \text{from (i)}$$
$$k = n(a + b + c - 2n) + (a - n)(b - n) + (b - n)(c - n) + (c - n)(a - n)$$

Substituting for k in eq. (ii),

$$a \times b \times c = n[n(a + b + c - 2n) + (a - n)(b - n) + (b - n)(c - n) + (c - n)(a - n)] + (a - n)(b - n)(c - n)$$

$$= n[n(a + b + c - 2n) + (b - n)\{(c - n) + (a - n)\}] + n(c - n)(a - n) + (a - n)(b - n)(c - n)$$

$$= n[n(a + b + c - 2n) + (b - n)(a + c - 2n)] + (c - n)(a - n)[n + b - n]$$

$$a \times b \times c = n[n(a + b + c - 2n) + (b - n)(a + c - 2n)] + b(c - n)(a - n) \quad \text{(iii)}$$

Example: $96 \times 97 \times 98$

$a = 96$, $b = 97$, $c = 98$.

Choose base $n = 100$ and substitute for a, b, c and n into (iii),

$$96 \times 97 \times 98 = 100[100(96 + 97 + 98 - 200) + (97 - 100)(96 + 98 - 200)] + 97(98 - 100)(96 - 100)$$

$$= 100[9100 + (-3)(-6)] + 97(-2)(-4)$$

$$= 100[9118] + 776$$

$$= 912, 576.$$

Multiplication of four integers:

Let any $a, b, c, d, n \in N$ be five integers such that $a < b < c < d < n$. Then, $a \equiv a' (\text{mod } n)$, $b \equiv b' (\text{mod } n)$, $c \equiv c' (\text{mod } n)$ and $d \equiv d' (\text{mod } n)$. Where, $a' = a - n$, $b' = b - n$, $c' = c - n$ and $d' = d - n$ that gives,

$$a = a' + n, b = b' + n, c = c' + n \text{ and } d = d' + n \quad \text{(i)}$$

For some $k \in N$ we can write,

$$a \times b \times c \times d \equiv a' \times b' \times c' \times d' (\text{mod } n)$$

$$a \times b \times c \times d = nk + a'b'c'd' \quad \text{(ii)}$$

Further, substitute for a, b, c, d into (ii) to find k,

$$nk = a \times b \times c \times d - a'b'c'd'$$

$$nk = (a' + n)(b' + n)(c' + n)(d' + n) - a'b'c'd'$$

$$k = (n(a + b - n) + (a - n)(b - n))(c + d - n) + (c - n)(d - n)(a + b - n)$$

Substituting for k into (ii),

$$a \times b \times c = n[(n(a + b - n) + (a - n)(b - n))(c + d - n) + (c - n)(d - n)(a + b - n)] + (a - n)(b - n)(c - n)(d - n)$$

$$a \times b \times c \times d = [n(a + b - n) + (a - n)(b - n)] \times [n(c + d - n) + (c - n)(d - n)] \quad \text{(iii)}$$

Example: $101 \times 102 \times 103 \times 104$

$a = 101$, $b = 102$, $c = 103$, $d = 104$.

Choose base $n = 100$ and substitute for a, b, c, d and n into (iii),

$$\begin{aligned} 101 \times 102 \times 103 \times 104 &= [100(101 + 102 - 100) + (101 - 100)(102 - 100)] \\ &\quad \times [100(103 + 104 - 100) + (103 - 100)(104 - 100)] \\ &= [100(103) + (1)(2)] \times [100(107) + (3)(4)] \\ &= [10302 \times 10712] \end{aligned}$$

Now, we choose a base $n = 10{,}000$ and apply multiplication for two integers,

$$\begin{aligned} 10302 \times 10712 &= 10{,}000[10302 + 10712 - 10000] \\ &\quad + (10302 - 10000)\,(10712 - 10000) \\ &= 10{,}000[11014] + (302)(712) \end{aligned}$$

For 302×712,

choose two bases $m = 300$ and $n = 600$ so that

$k = n/m = 2$.

substitute in below eq. (iii),

$$302 \times 712 = 300[2(302 - 300) + 712] + (302 - 300)(712 - 600)$$
$$= 215{,}024$$
$$101 \times 102 \times 103 \times 104 = [10302] \times [10712]$$
$$= 10{,}000[11014] + (302)(712)$$
$$= 110{,}140{,}000 + 215024$$
$$= 110{,}355{,}024$$

Multiplication of two numbers near different bases:

Let $a, b, m, n \in N$ be four integers such that $a < b$, $a < m$, $b < m$, such that $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{n}$.

Where, $a' = a - m$ & $b' = b - n$ that gives, $a = a' + m$ & $b = b' + n$. Choose m & n such that there exist an integer k, to get $k = n/m$, which gives, $n = mk$.

For some $k' \in N$ we can write,

$$a \times b \equiv a' \times b' \pmod{mn}$$
$$a \times b = (mn)k' + a'b' \quad \text{(i)}$$

Further, substitute $a = (a' + m)$ and $b = (b' + n)$ in eq. (i) to find k,

$$(mn)k' = (a' + m)(b' + n) - a'b'$$
$$mnk' = a'b' + mb' + a'n + mn - a'b'$$
$$mnk' = (na' + mb' + mn) \quad \text{(ii)}$$

From (i),

$$a \times b = (na' + mb' + mn) + a'b'$$
$$= (n(a - m) + m(b - n) + mn) + (a - m)(b - n)$$
$$a \times b = (na + mb - mn)(a - m)(b - n)$$

Now put $n = mk$ in the above eq.

$$a \times b = (mka + mb - m^2k) + (a - m)(b - mk)$$
$$= m[k(a - m) + b] + (a - m)(b - km) \quad \text{(iii)}$$

Example: 96 × 99998

Let $a = 96$, $b = 99998$ and the integer $m = 100$, $n = 100000$.

Then $k = n/m = 100000/100 = 1000$ and substitute in (iii),

$$\begin{aligned} 96 \times 99998 &= 100[1000(96 - 100) + 99998] \\ &\quad + (96 - 100)(99998 - 100000) \\ &= 100[1000(-4) + 99998] + (-4)(-2) \\ &= 100[-4000 + 99998] + 8 = 9{,}599{,}808 \end{aligned}$$

Application of Vedic Mathematics to Cryptography [2]:

The application of Vedic mathematics to cryptography holds promise in several areas, leveraging the efficiency and elegance of Vedic techniques to enhance cryptographic algorithms and protocols. The following are some potential applications-

Speed Optimization: Vedic mathematics offers techniques for fast arithmetic operations such as multiplication, division, and exponentiation.

These techniques based on sutras like "Nikhilam Navatashcaramam Dashatah" (All from 9 and the last from 10), enable rapid computation of mathematical operations, which can significantly improve the performance of cryptographic algorithms requiring intensive mathematical calculations.

For example, in elliptic curve cryptography (ECC), where scalar multiplication operations are fundamental, Vedic multiplication techniques could expedite the computation process, leading to faster encryption and decryption.

An Efficient Elliptic Curve Cryptography Arithmetic using Nikhilam Multiplication [1]:

Cryptography is a technique of making a message secure or secret. Sensitive information can store or transmite across secure or insecure networks with secure or secret message transmission method. So that an unauthorised person can't access the secret message.

One of the best public key cryptographic methods to secure message is Elliptic Curve Cryptography. In this cryptographic method, major time-consuming operations are (1) Point Addition and (2) Point Doubling.

Use of Nikhilam Multiplication in ECC Scalar Multiplication:

The point multiplication in ECC is basically includes Point doubling and Point addition operations.

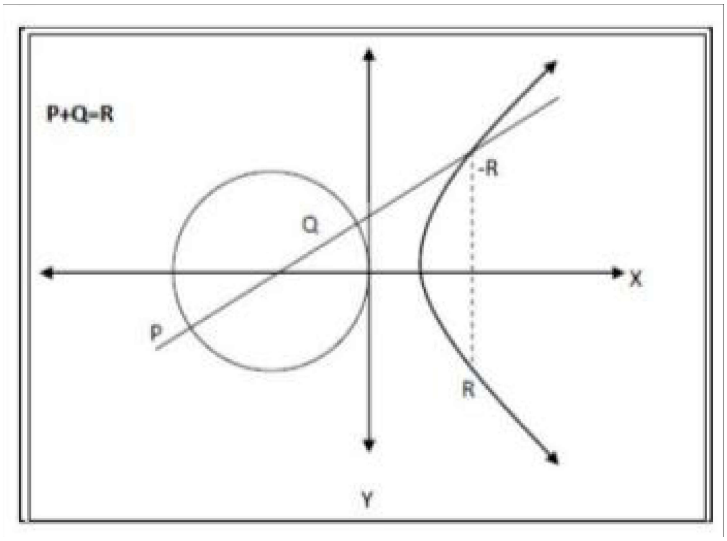
These operations need scalar (integer) multiplication of large magnitude. In standard multiplication and Karatsuba multiplication method n^2 and $n^{\log_2 3}$operations required to multiply two n digits numbers. Whereas the Nikhilam method requires less multiplication operational steps.

The use of Nikhlam method of multiplication in ECC scalar multiplication will increase the overall speed of Elliptic Curve Cryptography operation.

The use of scalar multiplication in ECC arithmetic point addition and point doubling-

(1) Point addition:

Point addition is defined as taking two points along a curve E and computing where a line through them intersects the curve. The negative of the intersection point is used as the result of the addition.



Point addition operation is denoted as $P + Q = R$

or $(Xp, Yp) + (Xq, Yq) = (Xr, Yr)$.

This can be algebraically calculated by:

$$\lambda = (Yq - Yp)/(Xq - Xp)$$

$$Xr = \lambda^2 - Xp - Xq$$

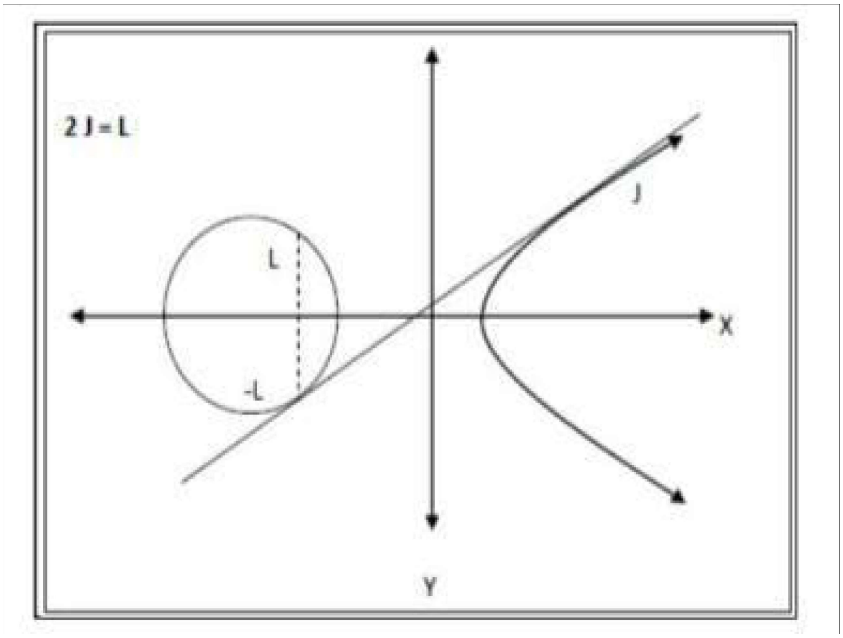
$$Yr = \lambda(Xp - Xr) - Yq$$

Note that we assume the elliptic field is given by

$$X^3 + aX + b$$

(2) Point Doubling:

Point doubling is similar to point addition, except one takes the tangent of a single point and finds the intersection with the tangent line.



The point doubling operation is denoted as $2J = L$

or $(Xp, Yp) + (Xp, Yp) = (Xr, Yr)$.

This can be algebraically calculated by:

$$\lambda = (3X^2p + a)/2Yp$$

$$Xr = \lambda^2 - 2Xp$$

$$Yr = \lambda(Xp - Xr) - Yq$$

Where a is the multiplication factor of X in the elliptic field given by $X^3 + aX + b$

Example: $p = (3, 10)$ and $q = (9, 7)$ in $E_{23}(1, 1)$. Find R? [7]

Solution: Here, $p \neq q$

$$X_p = 3,\ Y_p = 10,\ X_q = 9,\ Y_q = 7$$

$$a = 1,\ b = 1 \text{ and } C = 23.$$

So, $\lambda = [(Yq - Yp)/(Xq - Xp)] \bmod C$

$= [(7 - 10)/(9 - 3)] \bmod 23$

$= (-3/6) \bmod 23$

$= (-1/2) \bmod 23$

$= (-2^{-1}) \bmod 23$

$\Rightarrow$ $23 = 2(11) + 1$

$\Rightarrow$ $23 - 2(11) = 1$

$\Rightarrow$ $[23 - 2(11)] \bmod 23 = 1 \bmod 23$

$\Rightarrow$ $2(-11) = 1 \bmod 23$

$\Rightarrow$ $(-11) = (2)^{-1} \bmod 23$

Inverse of 2 is -11

$= [-(-11)] \bmod 23$

$= 11$

$Xr = (\lambda^2 - Xp - Xq) \bmod c$

$= (11^2 - 3 - 9) \bmod 23$

11		1	
11		1	(by Nikhilam sutra)
12	|	1	

$11^2 = 121$

$Xr = 109 \bmod 23$

$Xr = 17.$

$Yr = [\lambda(Xp - Xr) - Yq] \bmod c$

$= [11(3 - 17) - 10] \bmod 23$

$= [11(-14) - 10] \bmod 23$

	14	4	
	11	1	(by Nikhilam suta)
15	| 4		

$14 \times 11 = 154$

$Yr = (-154 - 10) \bmod 23$

$= (-164) \bmod 23$

$= 20 \bmod 23$

$Yr = 20$

$R = (17, 20).$

Acknowledgement:

We are highly appreciative of our Principal Prof. Ravi Toteja for selecting our paper for the ELITE fellowship.

References:

1. https://www.researchgate.net/publication/320934348_An_Efficient_Elliptic_Curve_Cryptography_Arithmetic_Using_Nikhilam_Multiplication?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6ImxvZ2luIiwicGFnZSI6InNlYXJjaCIsInBvc2l0aW9uIjoicGFnZUhlYWRlciJ9fQ

2. https://engrxiv.org/preprint/view/3583
3. Vedic Mathematics by Jagadguru Swami Sri Bharati Krishna Tirthaji Maharaj.
4. Vedic Mathematics Made easy.
5. http://www.vedamu.org/veda/1795$vedic_mathematics_methods.pdf
6. https://youtube/3AmkQjdiW7o?si=duQzKfvs6Yb53tee
7. https://www.youtube.com/live/vY6kh-fjUkc?si=t-4Hz68nVvDuaHfN
8. https://www.youtube.com/live/2paxjWaTGec?si=-FTnGOzeUn0wO4r7
9. Rohit Ranjan Lal; Dharmendra Kumar Yadav : Volume 13, Number 3, September 3, 2023.