J. Mountain Res. P-ISSN: 0974-3030, E-ISSN: 2582-5011 DOI: https://doi.org/10.51220/jmr.v20-i1.25
Vol. 20(1), (2025), 241-249

An Improved ĀryabhaṬa Algorithm and Its Application in Cryptography

Gaurav Agrawal[1*]**• Omkar Lal Shrivastava**[2] **• Nidhi Handa**[1]

[1]*Department of Mathematics and Statistics, Gurukula Kangri (Deemed to be University), Haridwar, Uttarakhand, India-249404*
[2]*Department of Mathematics, Government Kamladevi Rathi Girls Postgraduate College, Rajnandgaon, Chhattisgarh, India-491441*

[*]Corresponding Author Email Id: agr.gaurav96@gmail.com

Received: 14.01.2025; Revised: 02.06.2025; Accepted: 13.06.2025

Abstract: In this article, we have discussed the Āryabhaṭa algorithm, traditionally used for solving linear indeterminate equations in Indian mathematics. An improved version of Āryabhaṭa algorithm has been developed, which decreases the number of steps in order to find all integer solutions to such equations. The algorithm also provides multiplicative inverses of different integers under some modulo, which is a very useful tool in cryptography, signal processing, coding, and computer design.

2020 Mathematical Sciences Classification: 01A32, 11A55, 11D45, 35L10.

Keywords: Āryabhaṭa Algorithm • Diophantine Equation • Linear Congruence • Multiplicative Inverse.

Introduction

A linear indeterminate equation is an equation in two variables with integer coefficients when the solution is found in integers (or sometimes rational numbers). This problem was first discussed by Diophantus (c. 250 AD) (a Greek mathematician from Alexandria), who was interested only in finding the rational roots of such equations (Clark 1930). The equation

$$ax - by = c \tag{1.1}$$

is a linear indeterminate equation. Here, *a, b* and *c* are positive integers, *x* and *y* are integer roots of the equation. Equation (1.1) played an important role in the calculation of Ahargaṇa (the number of days that elapsed from a given epoch) from the mean longitudes of planets and lunar eclipses in Indian astronomy (Gupta 1974, 1986; Kak 2003, 2004, 2005; Shukla 1976). In modern times, it is useful in serious fields, including cryptography.

Āryabhaṭa (499 AD) was the first Indian mathematician who drew attention to solving these equations for integer roots. The Āryabhaṭa method for solving linear indeterminate equations are traditionally knows as Kuṭṭaka or pulverizer method. Bhāskara I (c.598 AD), Brahmagupta (628 AD), and others did various refinements to solve linear indeterminate equations (Ayyangar 1926; Dutta 2002; Datta and Singh 2004; Joseph 2010). Kak (1986) nicely elaborated on computational aspects of the Kuṭṭaka method, such as solving for pairs of linear congruences under different moduli and designated as Āryabhaṭa algorithm. Bag (1977, 2017) discussed the solution of the indeterminate equation purposed by Āryabhaṭa in terms of continued fractions, suggesting that the Āryabhaṭa algorithm is similar to the general method of continued fractions, which was later discovered by the European scholars Bombelli and Cataldi (2018) in 1598. Rao and Young (2006) published an analysis of the Āryabhaṭa algorithm to find the multiplicative inverse of a group modulo a prime as well as the solution to multiple congruences, which has various applications in cryptography, signal processing, coding, and computer design.

1.0 Objectives of the Study

This article presents a brief introduction to the Āryabhaṭa algorithm. In addition, it aims to improve Āryabhaṭa algorithm for solving linear indeterminate equations. In particular, the study aims to develop an iteration formula for this algorithm (taking into account negative numbers) for solving linear indeterminate equations. The algorithm presented here differs from the traditional commentaries but seems consistent with the original (cryptic) description. Additionally, a few algorithmic applications are shown, and a couple of examples are used to validate the results.

Methodology

The methodology employed in this study consists of the analytical reconstruction and enhancement of the classical Āryabhaṭa algorithm for solving linear indeterminate equations. Initially, the traditional Kuṭṭaka (pulverizer) method was explicated through historical and mathematical analysis, referencing original Sanskrit formulations and their modern interpretations. Subsequently, an improved algorithm was developed using a recursive structure, incorporating the nearest integer function to optimize successive divisions and account for negative remainders. To validate the effectiveness of both the traditional and improved algorithms, a series of Diophantine equations and congruence relations were systematically solved. The results obtained were tabulated and compared in terms of computational steps required. Particular focus was given to demonstrating the algorithm's efficiency in calculating modular inverses—a key operation in modern cryptography. Examples were chosen to illustrate not only correctness but also the reduction in complexity and execution steps.

2 Āryabhaṭa

Āryabhaṭa (b. 476–550 AD) was born in Kusumpura (near Patna), a pioneer mathematician and astronomer known for his systematic collection and systematisation of knowledge. His contributions to mathematics were significant and laid the foundation for many subsequent developments in Indian mathematics. He authored the famous text *Āryabhaṭīya*: an algebraic treaty on mathematics and astronomy (Gupta 1977; Hayashi 2003; Shukla 1976).

2.1 The Āryabhaṭa Problem

Problem 2.1. *Suppose a number N which being divided by given two integers (a,b) will leave two given remainders (r_1,r_2).*

$$N = ax + r_1 = by + r_2 \quad \text{or} \quad ax - by = c\,,$$
$$c = r_2 - r_1 . .$$

another form of given pair of residues as suggested by Kak (1986).

$$X(\operatorname{mod} m_i) = x_i \text{ for } i = 1,2\,.$$

The primary purpose is to find positive integer solutions to the above equations.

2.2 The Āryabhaṭa Algorithm

Āryabhaṭa discussed the solution of the above problems in cryptic verses 32 and 33 (Gaṇita Section) of Āryabhatīya. The translation of these verses by Datta and Singh (2004) follows the interpretation of Bhāskara I.

अधिकाग्रभागहारं छिन्द्यादूनाग्रभागहारेण ।
शेषपरस्परभक्तं मतिगुणमग्रान्तरे क्षिप्तम् ॥
अध उपरिगुणितमन्त्ययुगूनाग्रच्छेदभाजिते शेषम् ।
अधिकाग्रच्छेदगुणं द्विच्छेदाग्रमधिकाग्रयुतम् ॥

2.2.1 Translation

"Divide the divisor corresponding to the greater remainder by the divisor corresponding to the smaller remainder. The remainder (and the divisor corresponding to the smaller remainder) being mutually divided, the last residue should be multiplied by such an optional integer that the product being added (in case the number of quotients of the mutual division is even) or subtracted (in case the number of quotients is odd) by the difference

DOI: https://doi.org/10.51220/jmr.v20-i1.25

of the remainders will be exactly divisible by the penultimate remainder. Place the quotients of the mutual division successively, one below the other, in a column; below them is the optional multiplier, and underneath it is the quotient just obtained. Any number below (i.e., the penultimate) is multiplied by the one just above it and then added to the one just below it. Divide the last number (obtained by doing so repeatedly) by the divisor corresponding to the smaller remainder; then multiply the remainder by the divisor corresponding to the smaller remainder and add the greater remainder. The result will be the number corresponding to the two divisors."

Following the above translation, the algorithm starts with successive divisions of greater integer to the smaller integers. The successive quotients and remainders will obtain using the recursive formula:

$$q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \text{ and } r_i = r_{i-2} - r_{i-1}q_i, \quad 1 \le i \le n, \tag{2.1}$$

assuming $b = r_{-1}$ and $a = r_0\ (b > a)$.

The work consists of some steps, represented by the Table 2.1 given below. Now we explain the work further below.

Table 2.1: Numerical Values

i	***q_i***	***a_i***
1	q_1	a_1
2	q_2	a_2
3	q_3	a_3
.	.	.
.	.	.
n	q_n	a_n
n+1	q_{n+1}	a_{n+1}
n+2	q_{n+2}	a_{n+2}

Here are features of this table in detail:

1. Column 2 contains the quotients obtained by equation (2.1). The last two elements (q_{n+1} and q_{n+2}) are obtained by using formula $q_{n+1}r_n \pm c = q_{n+2} \cdot r_{n-1}$ taken in order, where positive and negative sign is taken according as the quotients (omitting the first one) obtained are even or odd.
2. The element of column 3 will be obtained using the recursive formula
$$a_n = q_n a_{n+1} + a_{n+2}, \tag{2.2}$$
3. Let $\bar{a}$ and $\bar{b}$ are fundamental solution of the above equation, then
$$\bar{a} = a_1 (\bmod b) \text{ and } \bar{b} = a_2 (\bmod a). \tag{2.3}$$
4. The general solution of the given equation is
$$a_n = \bar{a} + bn \text{ and } b_n = \bar{b} + an,\ n \in □_0. \tag{2.4}$$

Remark 2.1. *The quotients are obtained by dividing the divisor of the greater remainder by the divisor of the smaller remainder, and the process is repeated in a similar way until all the quotients are not obtained. This process is called Kuṭṭaka in Indian mathematics, and traditionally known as the Euclid division algorithm. Euclid* (325-265 BC) *gives his method to obtain the G.C.D of numbers a and b, which occurs in the Elements of Euclid* [Thomas (1956)], *but Euclid did not suggest anything about the solutions of the linear Diophantine equation.*

The rational and the genesis of the algorithm can be illustrated by taking some examples, given below:

Example 2.1. *Solve* $23x - 63y = 7$.

Solution. Comparing $ax - by = c$, we have $a = 23, b = 63$ and $c = 7$.

Performing successive division of *b* by *a* and using (2.1), we get

$$q_1 = \left\lfloor \frac{63}{23} \right\rfloor = 2 \text{ and } r_1 = 63 - 2 \cdot 23 = 17,$$

$$q_2 = \left\lfloor \frac{23}{17} \right\rfloor = 1 \text{ and } r_2 = 23 - 1 \cdot 17 = 6,$$

$$q_3 = \left\lfloor \frac{17}{6} \right\rfloor = 2 \text{ and } r_3 = 17 - 2 \cdot 6 = 5,$$

$$q_4 = \left\lfloor \frac{6}{5} \right\rfloor = 1 \text{ and } r_4 = 6 - 1 \cdot 5 = 1.$$

The column of quotients is $\begin{pmatrix}2\\1\\2\\1\end{pmatrix}$.

The number of quotients, omitting the first one, is 3, which is odd. Hence, we choose a multiplier such that on multiplication by the last remainder, 1, and subtracting 7 from the product, the result is divisible by the penultimate remainder, 5. If the number of quotients after omitting the first one is even, then adding 7 is required instead of subtracting. So, we have $1\times12-7=5\times1$. Now, we formed the following Table 2.2 using the properties defined in Section 2.2.

Table 2.2: Numerical Values

i	***q_i***	***a_i***
1	2	140
2	1	51
3	2	38
4	1	13
5	12	12
6	1	1

Explanation: Start with last two elements: $a_6=q_6=1$ and $a_5=q_5=12$. The value obtained using the recursive formulas (2.2) is $a_4=q_4a_5+a_6=1\cdot12+1=13$. In the similar way, the values $a_3=38, a_2=51$ and $a_1=140$ are obtained. Hence, first positive solution using equation (2.3) is $\bar{a}=140(\operatorname{mod}63)=14$ and $\bar{b}=51(\operatorname{mod}23)=5$. The general solution is $a_n=14+63n$ and $b_n=5+23n,\ n\in\mathbb{N}_0$, obtained by using (2.4).

Example 2.2. *Solve* $23x-63y=1$.

Solution. Comparing with $ax-by=1$, we have
$a=23,\ b=63$ and $c=1$.

The column of quotients is $\begin{pmatrix}2\\1\\2\\1\end{pmatrix}$.

The number of quotients, omitting the first one, is 3, which is odd. Hence, we choose a multiplier such that on multiplication by the last remainder, 1, and subtracting 1 from the product, the result is divisible by the penultimate remainder, 5. So, we have $1\times6-1=5\times1$. Now, we formed the following Table 2.3 using the properties defined in Section 2.2.

Table 2.3: Numerical Values

i	***q_i***	***a_i***
1	2	74
2	1	27
3	2	20
4	1	7
5	6	6
6	1	1

Explanation. Start with last two elements: $a_6=q_6=1$ and $a_5=q_5=6$. The value obtained using the recursive formula (2.2) is $a_4=q_4a_5+a_6=1\cdot6+1=7$. Similarly, the values $a_3=20, a_2=27$ and $a_1=74$ are obtained. Hence, first positive solution using equation (2.3) is $\bar{a}=74(\operatorname{mod}63)=11$ and $\bar{b}=27(\operatorname{mod}23)=4$. The general solution is $a_n=11+63n$ and $b_n=4+23n,\ n\in\mathbb{N}_0$, obtained by using (2.4).

3 Improved Āryabhaṭa Algorithm

The Āryabhaṭa algorithm starts with successive divisions of greater integer to the smaller integers to obtained quotient. We assigned nearest integer function to find successive quotients considering negative remainders in account. The successive quotients and remainders will obtain using the modified recursive formula.

DOI: https://doi.org/10.51220/jmr.v20-i1.25

$$q_i = nint\left(\frac{r_{i-2}}{r_{i-1}}\right) \text{ and } r_i = r_{i-2} - r_{i-1}q_i,$$

$$1 \le i \le n. \qquad (3.1)$$

assuming $b = r_{-1}$ and $a = r_0\,(b > a)$. where '$nint$(x)' is defined as follows:

$$\forall\, x \in R : nint(\text{x}) = \begin{cases} \left\lfloor x + \frac{1}{2} \right\rfloor & : x \notin 2\mathbb{Z} + \frac{1}{2} \\ x - \frac{1}{2} & : x \in 2\mathbb{Z} + \frac{1}{2} \end{cases},$$

where $\lfloor . \rfloor$ is the floor function. Next, we shall follow steps 1-4 mentioned in Section 2.2.

The rational and the genesis of the algorithm can be illustrated by taking some examples, given below.

Example 3.1 *Solve* $23x - 63y = 7$.

Solution: Comparing with $ax - by = c$, we have

$a = 23, b = 63$ and $c = 7$.

Performing successive division of b by a and using (2.1), we get

$$q_1 = nint\left(\frac{63}{23}\right) = 3,, \; r_1 = 63 - 23 \cdot 3 = -6,$$

$$q_1 = nint\left(\frac{23}{-6}\right) = -4, \; r_2 = 23 - (-6)(-4) = -1$$

.

The column of quotients is $\begin{pmatrix} 3 \\ -4 \end{pmatrix}$.

The number of quotients, omitting the first one, is 1, which is odd. Hence, we choose a multiplier such that on multiplication by the last remainder, -1, and subtracting 7 from the product, the result is divisible by the penultimate remainder, -6. So, we have $-1 \times 5 - 7 = -6 \times 2$. Now, we formed the following Table 3.1 using the properties defined in Section 2.2.

Table 3.1: Numerical Values

i	***q_i***	***a_i***
1	3	-49
2	-4	-18
3	5	5
4	2	2

Explanation. Start with last two elements: $a_4 = q_4 = 2$ and $a_3 = q_3 = 5$. The value obtained using the recursive formula (2.2) is $a_2 = q_2 a_3 + a_4 = -4 \cdot 5 + 2 = -18$. In the similar way, the value $a_1 = -49$ is obtained. Hence, first positive solution using equation (2.3) is $\bar{a} = -49 (\bmod 63) = 14$ and $\bar{b} = -18 (\bmod 23) = 5$. The general solution is $a_n = 14 + 63n$ and $b_n = 5 + 23n,\; n \in \mathbb{N}_0$, obtained by using (2.4).

Example 3.2 Solve $23x - 63y = 1$.

Solution: Comparing with $ax - by = c$, we have

$a = 23,\; b = 63$ and $c = 1$.

The column of quotients is $\begin{pmatrix} 3 \\ -4 \end{pmatrix}$.

The number of quotients, omitting the first one, is 1, which is odd. Hence, we choose a multiplier such that on multiplication by the last remainder, -1, and subtracting 1 from the product, the result is divisible by the penultimate remainder, -6. So, we have $-1 \times 5 - 1 = -6 \times 1$. Now, we formed the following Table 3.2 using the properties defined in Section 2.2.

Table 3.2

i	***q_i***	***a_i***
1	3	-52
2	-4	-19
3	5	5
4	1	2

Explanation. Start with last two elements: $a_4 = q_4 = 1$ and $a_3 = q_3 = 5$. The value obtained using the recursive formula (2.2) is $a_2 = q_2 a_3 + a_4 = -4 \cdot 5 + 1 = -19$. In the similar way, the value $a_1 = -52$ is obtained. Hence, first positive solution using equation

(2.3) is $\bar{a} = -52 (\bmod 63) = 14$ and $\bar{b} = -19 (\bmod 23) = 5$. The general solution is $a_n = 11 + 63n$ and $b_n = 4 + 23n,\ n \in \mathbb{N}_0$, obtained by using (2.4).

It is clear that the answers are obtained in least number of steps after applying the nearest integer function mentioned above for successive division.

Conjecture 3.1 *The Āryabhaṭa algorithm provides integer solutions to linear indeterminate equations in least number of steps using the concept of least absolute remainder.*

4 Āryabhaṭa Algorithm for System of Linear Congruences

The text Āryabhaṭīya also contains problems that relate to more than two congruence relations. This involves the Āryabhaṭa algorithm previously discussed and explained in Section 2.2 [Datta and Singh (2004); Mishra (2015)]. The problem mentioned by Āryabhaṭa can be explained as follows in modern terms and notations.

Problem 4.1. *Find a number N which being severally divided by $(a_1, a_2, a_3, \ldots, a_n)$ leaves remainder $(r_1, r_2, r_3, \ldots, r_n)$.*

$$N = a_1x_1 + r_1 = a_2x_2 + r_2 = a_3x_3 + r_3 = \ldots = a_nx_n + r_n$$
.

another form

$$X(\bmod m_i) \equiv x_i \text{ for } 1 \le i \le n.$$

where $gcd(m_i, m_j) = 1 \ \forall \ i \ne j$ and $x_i > x_j \ \forall \ i = j - 1$.

The purpose is to find integer solutions of the above equations.

4.1 Algorithm

1. The method will start from taking first two modular relations $X(\bmod m_1) \equiv x_1$ and $X(\bmod m_2) \equiv x_2$.
2. As mentioned before the pair represents a linear Diophantine equation of the form $ax - by = c$. This equation solved using the Āryabhaṭa algorithm explained in section 2.
3. Let the minimum value of N is obtained at value $x_1 = \alpha_1$ such that $N = a_1\alpha_1 + r_1$ so that the general solution is $N = a_1(a_2t + \alpha_1) + r_1 = a_1a_2t + a_1\alpha_1 + r_1$, where t is an integer. The equation obtained can be explained as, the number N is when divided by a_1a_2 leaves remainder $a_1\alpha_1 + r_1$.
4. To solve further next modular relation with be taken with this new equation obtained.
5. The process is continued with successive reductions of equations, final solution is obtained for value of *N*.

Mahāvīra (c. 850), Āryabhaṭa II (c. 950), Śripati (c. 1039) and Bhāskara II (b. 1114) described similar methods for solving simultaneous linear Diophantine equations-samslista Kuṭṭaka (conjecture pulverizer) [Datta and Singh (2004)]. The following problem is present in the text of Bhāskara I on *Āryabhaṭīya* of Āryabhaṭa.

Example 4.1. *Find a number which is divided by 8 leaves (5 as remainder), divided by 9 leaves (4 as remainder), and divided by 9 leaves (1 as remainder)* [Datta and Singh (2004)].

Solution. The problem can be written in modern notation as

$$N = 8x + 5 = 9y + 4 = 7z + 1$$

Taking first two conditions, this forms a linear Diophantine equation. The minimum value found by using Āryabhaṭa algorithm is $N = 13$.

The new equation formed according to method explained above,

$$N = 72t + 13 = 7z + 1$$

The process is repeated in similar way to obtained least value of N satisfying all the given conditions, which is found to be 85.

Conjecture 4.1. *The Āryabhaṭa algorithm solves the system of n linear indeterminate equations in n-1 steps.*

Results and Discussion

5 Application to Cryptography

An equation of the form $ax \equiv b(\bmod m)$ is called a linear congruence of modulo *m*, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b(\bmod m)$, by the definition of the linear congruence the equation converts into $ax_0 - by_0 = c$ which is a linear Diophantine equation. Thus, finding all integer that will satisfy the linear congruence $ax \equiv b(\bmod m)$ is identical with that of obtaining all solution of linear Diophantine equation $ax_0 - by_0 = c$ [Rao (2006)]. Kak (1986) shows that the Āryabhaṭa problem represent a pair of linear congruence. The solutions obtained in this problem has various application in context of modular relation. Some of them are discussed in this section.

5.1 Multiplicative Inverse

The multiplicative inverse of an integer number *a* under modulo *m* is calculated by using the modular relation; $ax \equiv 1(\bmod m)$, where *a* and *m* are coprime integers. For instance, if $3 \cdot 5 \equiv 1(\bmod 7)$, then $3^{-1}(\bmod 7) \equiv 5$.

Consider the special case when $c = 1$ of linear indeterminate equation $ax - by = c$, we have

$ax - by = 1$,

this implies that

$$x = a^{-1}\left(\bmod b\right) \text{ and } y = -b^{-1}\left(\bmod a\right).$$

Example 5.1. *Find* $63^{-1}(\bmod 23)$ *and* $23^{-1}(\bmod 63)$.

Solution. Let $x \equiv 63^{-1}(\bmod 23)$, then we convert this relation into the linear indeterminate equation. The Āryabhaṭa algorithm gives the solution of corresponding linear indeterminate equation $23 \cdot 11 - 63 \cdot 4 = 1$ (see example 3.2). The relevance of the solution is that $63^{-1}(\bmod 23) = -4(\bmod 23) = 19$ and $23^{-1}(\bmod 63) = 11$. Thus, we obtained $a^{-1}(\bmod b)$ and $b^{-1}(\bmod a)$ both by this method.

Example 5.2. *Find* $137^{-1}(\bmod 60)$ *and* $60^{-1}(\bmod 137)$.

Solution. Let $x \equiv 137^{-1}(\bmod 60)$ then we convert this relation into the linear indeterminate equation. The Āryabhaṭa algorithm gives the solution of corresponding linear indeterminate equation $60 \cdot 16 - 137 \cdot 7 = 1$. The relevance of the solution is that $137^{-1}(\bmod 60) \equiv -7(\bmod 60) = 53$ and $60^{-1}(\bmod 137) \equiv 16$. Thus, we obtained $a^{-1}(\bmod b)$ and $b^{-1}(\bmod a)$ both by this method.

5.2 Linear Diophantine Equation

In *RSA* encryption, the equation $ed \equiv 1\left(\bmod \phi\left(n\right)\right)$ involves a linear Diophantine equation, where $\phi\left(n\right)$ is Euler's totient function. This equation $ed \equiv 1\left(\bmod \phi\left(n\right)\right)$ can be expressed as $ed - k\phi\left(n\right) = 1$, where *k* is an integer. The private key *d* can be found by using Āryabhaṭa algorithm which is useful in decryption of message in cryptography. This can be expressed as

$d = e^{-1}\left(\bmod \phi\left(n\right)\right)$.

6 Concluding Remarks

Āryabhaṭa was a great ancient Indian mathematician and Astronomer, whose contribution in solving indeterminate equations have extensive influence around the world. The Āryabhaṭa algorithm is considered to be one of the most significant topical contributions of Indians. The simplicity of algorithm lies in the fact that it lessens large time taking computing operations into several modular arithmetic with less iterations. The linear Diophantine equation $ed - k\phi(n) = 1$ is crucial in *RSA* for determining the private key exponent *d.* The Āryabhaṭa algorithm can be employed to find solution to this equation providing a method to compute the private key from the public key component. This may be utilized by the computer scientists in developing crypto algorithms. Although the algorithm basically provides solutions to the linear indeterminate equations, it also plays an important role in the solution of the much more difficult second-order indeterminate equations.

References

Ayyangar AAK (1926) The Mathematics of Aryabhata. Quarterly Journal of Mythic Society. 16: 158-179.

Bag AK (1977) The method of integral solution of indeterminate equation of the type: $BY = AX \pm C$ in ancient and medieval India, Indian Journal of History of Science. 12(1): 1-16.

Bag AK (2017) Some Features of the Solutions of Kuṭṭaka and Vargaprakṛti. Indian Journal of History of Science. 52(1): 1-16.

Caianiello E (2018) Indeterminate linear problems from Asia to Europe. Lettera Matematica 6: 233–243. https://doi.org/10.1007/s40329-018-0242-4

Clark WE (1930) The Aryabhatiya of Aryabhata: An Ancient Indian Work on Mathematics and Astronomy. The University of Chicago Press, Chicago.

Datta B and Singh AN (reprinted 2004) History of Hindu Mathematics I-II. Bharatiya Kala Prakashan, Delhi, India.

Dutta AK (2002) Mathematics in Ancient India: Diophantine equations: The Kuṭṭaka. Resonance 7 (10): 6-22.

Gupta RC (1974) Solution of the Astronomical Triangle as Found in the Tantrasaṅgraha (AD 1500). Indian Journal of History Science 9(1): 86-99.

Gupta RC (1977) On Some Mathematical Rules from the Āryabhaṭīya. Indian Journal of History Science 12(2): 200-206.

Gupta RC (1986) Some equalisation problems from the Bakhshālī manuscript. Indian Journal of History Science 21(1): 51-61.

Hayashi T (2003) Indian Mathematics. In: Guinnes, Ivor and Baltimore MD (Ed.) Companion Encyclopaedia of the History and Philosophy of Mathematical Sciences 1. The John Hopkins University Press. pp. 118-130. ISBN0: 8018-7396-7.

Joseph GG (2010) The Crest of the Peacock: Non-European Roots of Mathematics. Princeton University Press, Princeton, NJ.

Kak S (1986) Computational aspects of the Āryabhaṭa algorithm. Indian Journal of History Science 21(1): 62–71.

Kak S (2003) Indian Physics: Outline of Early History. arXiv: physics/0310001.

Kak S (2004) The golden mean and the physics of aesthetics, arXiv: physics/0411195.

Kak S (2005) Aristotle and Gautama on logic and physics. arXiv: physics/0505172.

Mishra V (2015) Linear Indeterminate Analysis: Theory and Applications. American Research Journal of Mathematics 1(3): 16-33.

Rao TRN and Yang C-H (2006) Aryabhata remainder theorem: relevance to public-key crypto-algorithms. Circuits, Systems, and Signal Processing. 25: 1-15.

Shukla KS (1976) Āryabhatīya of Āryabhaṭa, with the commentary of Bhāskara I and

Someśvara 2. Indian National Science Academy, New-Delhi.

Srinivasiengar CN (1967) The History of Ancient Indian Mathematics. World Press, Calcutta.

Sriram MS (2005) Algorithms in Indian Mathematics. In Emch GG et al. (Eds.) Contributions to the History of Indian mathematics. Hindustan Book Agency, New Delhi. pp. 153-164.

Thomas LH (1956) Elements of Euclid (Translation and commentaries). Dover Publications.