American Research Journal of Mathematics **Original Article**
ISSN 2378-704X **Volume 1, Issue3, June-2015**

Linear Indeterminate Analysis: Theory and Applications

Vinod Mishra[1]

Department of Mathematics
SantLongowal Institute of Engineering and Technology
Longowal (Punjab), India

Abstract: Recent years the theory of first degree or linear indeterminate analysis initiated by Āryabhaṭa I (b.476 AD) are widely appreciated and used in modern sciences on accounts of its varied applications in the field of mathematics, astronomy, coding theory, cryptography, information systems, computer design and signal processing. This paper intends to present the progress in the areas of linear indeterminate analysis from fourth century BCE to modern times. Examples and applications of significance have been presented with a view of mathematical learning.

Keywords: Linear indeterminate analysis; Pulverizer; Āryabhaṭa remainder theorem; Chinese remainder theorem

I. INTRODUCTION

The indeterminate (generally called Diophantine) equations are those algebraic equations in whichi) the values of *n* unknowns $x_1, x_2, ..., x_n$ involved are all positive integers, and ii) for *n* unknowns number of equations are $n+1.$ In particular for two unknowns there will be only one equation.

The most general form of linear equations in $x > 0, y > 0$ are given by $Ax + By + C = 0,$ where $A > 0$ and B, C are either positive or negative. Under these conditions, we have just two forms of equations, viz.

$$ax - by = \pm c \tag{1}$$

and

$$ax + by = c \tag{2}$$

In these equations a and b are relatively prime, that is, $\gcd(a,b) = 1$. If a and b have common factor, then so must have c. Such equations in ancient Indian mathematics have been designated by the term*kuṭṭaka, kuṭṭa, kuṭṭākāra, kuṭṭikāra*(pulveriser). *Kuṭṭ* means to break or pulverize into pieces by means continued division. The terms*a* is called dividend (*bhājya*), *b* devisor (*hara*), *c* interpolator (*kṣepa*, *kṣepaka*) (+*c* additive, -*c* subtractive), *x* multiplier (*guṇaka, guṇakāra, guṇa*) and*y* quotient (*phala, labdhi*).

Any solution of (1) is said to be optimal if $0 < x < b, 0 < y < a$ and of (2) if either $|x| < b or |y| < a$ or both.

Notice that (1) always possesses infinite number of solutions whereas (2) has finite number of solutions or sometimes no solution. The solution of (2) has been given by Brahmagupta by converting it into the type

$$ax - by = c.$$

Transmission and Foreign Contribution [AKB & SK]

The problems appear in the *Śulbasūtras* (200-800 BCE) in the form of simultaneous equations and are due to *altar* construction. ĀryabhaṭaI (b. 476AD), the first Hindu algebraist, is credited for devising excellent method for solution of (1) which later resembled Euler (1764) method of continued fraction.

Continued fraction is a process of converting a fraction into a continued division and most likely originated due to finding rational approximation to $\sqrt{N}$. Euclid (300 BCE) of Greek is credited to have made the earliest step in the

[1] *Corresponding Author: vinodmishra.2011@rediffmail.com*

theory of continued fraction and applying to determine the gcd of two lines to the gcd of two numbers. Indians made systematic use of the theory of continued fraction in the works of Āryabhaṭa I onwards.

Regarding Greek contribution, Nicomachus of Geresa (first century AD) gave an example on the problem of remainders involving linear indeterminate analysis. The answer was provided without a method.

Diophantus of Alexandria (250AD) discussed the problems of second and higher degree indeterminate equations but did not consider the first degree indeterminate equations. Further, he provided no method of solutions and was only concerned with rational solutions.

According to Kaye, primarily notions of Greek geometry, which is responsible for the evolution of the rule, is not found common among Indian works as it has been traced in Greek works.

The basis for Chinese contribution is placed in the following problem leading to simultaneous equations found in the *Sun-Tzu Suan Ching* (Master Sun's Arithmetical Manual, fl 280-473 BCE according to Needhm): "We have a number of things, but do not know how many. If we count them by threes we have two left over. If we count by fives we have three left over. If we count them by sevenths we have two left over. How many things are there?" [SK]. The solution was provided without a method.

The application of equation $by = ax \pm c$ was first found in a calendrical work, *Ta-Yen Li Shu* (Book of the Ta Yen Calendar) of I-Hsing (687-727 AD) with a method Ta-Yen-Shu which is similar to the Indian method of *kuṭṭaka*. I-Hsing visited India in 673AD, became a Tantric-Buddhist monk and learnt Sanskrit. According to Bag [AKB], it is quite probable that I–Hsing acquired the technique of solving indeterminate problems from Indian scholars and it was through his effort the knowledge was carried to China. It was five century later when Chhih Chiu-Shao (c. 1247 AD) gave full explanation to the method in his *Shu Shu Chiu Chang*.

According to Smith, Hindu treatment of indeterminate equations of first degree was original and not influenced by Chinese or Greek writers.

Integral solutions of some indeterminate equations based on trial are found in the work *Kitab al-taraifI'lhisab* (Book of Rare things in the Art of Calculation) of Arabic scholar AbuKamilal-Misri(c. 850-930 AD).

The problem of remainder is found in the works of Islamic Ibn al-Haitam (c.1000 AD) and Italian Leonardo Pisano (Fibonnaci) (c. 1202 AD). Through the knowledge of work of Pisano, Rigiomontanus (1836-1876) proposed a problem similar to that of Āryabhaṭa I. In the eighteenth century, the legends L. Euler, L.J. Langrage and C.F. Gauss strengthened the remainder problems

II. METHODS FOR SOLVING $ax \pm c = by$

2.1. First Method (Āryabhaṭa I)

To find the number (*N*), which when divided by a given number *a* will leave a remainder r_1 and when divided by another number *b* will leave a remainder r_2.

Symbolically we express: $N = ax + r_1 = by + r_2, i.e.\ N = r_1 (\text{mod } a) = r_2 (\text{mod } b).$

Āryabhaṭa I keeps $c = r_1 - r_2$ always positive. Consequently, this leads to the form:

$$y = \frac{ax + c}{b} \text{ or} \tag{3}$$

$$x = \frac{by - c}{a} \tag{4}$$

Āryabhaṭīya II,v.32-33[D-S] states:

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

Suppose $a > b$, we get [PSb]

$$a = bq_0 + r_1$$
$$b = r_1q_1 + r_2$$
$$r_1 = r_2q_2 + r_3$$
$$r_2 = r_3q_3 + r_4$$
$$- - - - -$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$
$$r_{n-1} = r_nq_n + r_{n+1},$$
$$0 \le r_1 < b, 0 \le r_{i+1} < r_i$$

Now substituting the values in (3) and (4), we find

1) $y = q_0x + y_1$ 1.1) $by_1 = r_1x + c$

2) $x = q_1y_1 + x_1$ 1.2) $r_1x_1 = r_2y_1 - c$

3) $y_1 = q_2x_1 + y_2$ 1.3) $r_2y_2 = r_3x_1 + c$

4) $x_1 = q_3y_2 + x_2$ 1.4) $r_3x_2 = r_4y_2 - c$

……..

2n-1) $y_{n-1} = q_{2n-2}x_{n-1} + y_n$ 1.2n-1) $r_{2n-2}y_n = r_{2n-1}x_{n-1} + c$

2n) $x_{n-1} = q_{2n-1}y_n + x_n$ 1.2n) $r_{2n-1}x_n = r_{2n}y_n - c$

2n+1) $y_n = q_{2n-1}x_n + y_{n+1}$ 1.2n+1) $r_{2n}y_{n+1} = r_{2n+1}x_n + c$

[If $a < b, q_0 = 0, r_1 = a.$]

Case 1(Āryabhaṭa I's Algorithm). Suppose that mutual division of dividend and divisor is stopped after having obtained an even or odd number of quotients.

Subcase 1.1. If the number of partial quotients (excluding q_0) obtained be even, the reduced form of the original equation is (1.2n+1), i.e. $r_{2n}y_{n+1} = r_{2n+1}x_n + c.$

Giving a suitable integral value *t* to x_n, we make

$$y_{n+1} = \frac{r_{2n+1}t + c}{r_{2n}} = t_1, \text{ an integer}$$

We now obtain an integral value for y_n by $(2n+1)$. The values of *x* and *y* will now be calculated as proceeding before.

Subcase 1.2. If the number of partial quotients (excluding q_0) be odd, the reduced form of the original equation is (1.2n), i.e. $r_{2n-1}x_n = r_{2n}y_n - c.$

Putting a suitable integer t' for y_n, we have

$$x_n = \frac{r_{2n}t' - c}{r_{2n-1}} = t_1', \text{ an integer}$$

Now proceeding as before we obtain the values of *x* and *y*.

Case2 (Improved Āryabhaṭa I's Algorithm) [IAA]. First suppose that the mutual division is continued until the zero remainder is obtained. Since *a,b* are co-prime, the last one remainder is unity.

Subcase 2.1. Let the number of partial quotients (excluding q_0) be even. Therefore, we have $r_{2n} = 1, r_{2n+1} = 0, q_{2n} = r_{2n-1}$ and so from (1.2n+1), $y_{n+1} = c$ and from (2n+1), $y_n = q_{2n}x_n + c.$

Giving a suitable integral value *t*to x_n, we get an integral value for y_n. Proceeding backwards step by step we ultimately obtain the values of *x* and *y* in positive integers.

Subcase 2.2. If the number of partial quotients (excluding q_0) be odd, then $r_{2n-1} = 1, r_{2n} = 0, q_{2n-1} = r_{2n-2}$. The equations (2n+1) and (1.2n+1) will be absent and so from (1.2n), $x_n = -c$ and from (2n), $x_{n-1} = q_{2n-1}y_n - c.$

Giving an arbitrary integral value t' to y_n, we obtain an integral value for x_{n-1}. Then proceeding backwards as before we calculate the values of *x* and *y* in positive integers.

Let the number of partial quotients *n* (excluding q_0) be even or odd. *Valli*, the column of partial quotients, starts from the last term at the bottom and proceeds upward. The solution $\bar{x}, \bar{y}$ is obtained. The least solution $(\alpha, \beta)$is obtained from abrading or scraping off as such $\bar{x} = bl + \alpha, \bar{y} = am + \beta, 0 < \alpha < b, 0 < \beta < a.$

Table1. *Case 1*

Remainders	*Valli* (column of q_i)	*Guṇa* (x),*Labdhi* (y)
r_1	q_0	$q_0\alpha_1 + \alpha_2 = \alpha_0 = \bar{y}$
r_2	q_1	$q_1\alpha_2 + \alpha_3 = \alpha_2 = \bar{x}$
r_3	q_2	$q_1\alpha_3 + \alpha_4 = \alpha_2$
…	…	…
…	…	…
r_{n-1}	q_{n-2}	$q_{n-2}\alpha_{n-1} + \alpha_n = \alpha_{n-2}$
r_n	q_{n-1}	$q_{n-1}\alpha_n + t = \alpha_{n-1}$
r_{n+1}	q_n	$q_n t + t_1 = \alpha_n$
	t	x
	t_1	x

Table2. *Case 2* $(t = c, t_1 = 0)$

Remainders	*Valli* (column of q_i)	*Guṇa* (*x*),*Labdhi* (*y*)
r_1	q_0	$q_0\alpha_1 + \alpha_2 = \alpha_0 = \bar{y}$
r_2	q_1	$q_1\alpha_2 + \alpha_3 = \alpha_1 = \bar{x}$
r_3	q_2	$q_1\alpha_3 + \alpha_4 = \alpha_2$
…	…	…
…	…	…
r_{n-1}	q_{n-2}	$q_{n-2}\alpha_{n-1} + \alpha_n = \alpha_{n-2}$
r_n	q_{n-1}	$q_{n-1}q_nc + c = \alpha_{n-1}$
r_{n+1}	q_n	$q_nc = \alpha_n$
	c	x
	0	x

Evidently, the solution follows the recurrence relation $q_i\alpha_{i+1} + \alpha_{i+2} = \alpha_i$

General Solution

Let $x = \alpha, y = \beta$ be the least solution of

$$ax \pm c = by. \tag{5}$$

Then

$$a\alpha \pm c = b\beta. \tag{6}$$

Subtracting (6) from (5), we write

$$\frac{x-\alpha}{b} = \frac{y-\beta}{a} = m, \text{ say}$$

This implies $x = \alpha + bm = \alpha(\text{mod } b), y = \beta + am = \beta(\text{mod } a), m = 0,1,2,.....$ are the general solution of (5). Clearly, the solutions *x* and *y*are the infinite arithmetic progression (A.P.) with first term $\alpha,$common difference *b* for *x*, and first term β , common difference *a* for*y*.

Aliter. The solution can also be obtained from (6) as $a(\alpha + bm) \pm cb = (\beta + am).$

Also from (6)

$$a(b-\alpha) \mp c = b(a-\beta). \tag{7}$$

Thus it $x = \alpha, y = \beta$ is a solution of (5), then $x = b-\alpha, y = a-\beta$ will be the solution of $ax \mp c = by.$

Remark. Sometimes it is also possible to find the least solution by trial.

Labdhi and *guṇa*are obtained according to the following table:

Table3.

Valli (excluding q_0)	*Kṣepa*(*c*)	*Labdhi* (*y*)	*Guṇa*(*x*)
even or odd	negative or positive	β	α
even or odd	positive or negative	$a-\beta$	$b-\alpha$

Here it is important to note that the values of *x* and *y* are sometimes not the corresponding values. The corresponding values *x* or *y* can be obtained by putting in the given equation.

Remark. In case there is only one partial quotient, say *k* of (2), i.e. $a = kb + 1,$ the method as prescribed before fails.

Table4.

Valli	x,y
k	$kc' = \bar{x}$
$c' = \lvert c \rvert$	$c' = \bar{y}$
0	

If *kṣepa* is positive, then $x = b - \alpha, y = a - \beta.$

If *kṣepa* is negative, then $x = \alpha, y = \beta.$

Here (α, β) is the smallest positive solution.

Example1. Consider the problem $63y = 100x + 70.$

Table5.

S.N.	Remainders	*Valli* (q_i)	*x,y*
0		1	$1 \times 1190 + 700 = 1890 = \alpha_0 = \bar{y}$
1	37	1	$1 \times 700 + 490 = 1190 = \alpha_1 = \bar{x}$
2	26	1	$1 \times 210 + 490 = 700 = \alpha_2$
3	11	2	$2 \times 210 + 70 = 490 = \alpha_3$
4	4	2	$2 \times 70 + 70 = 210 = \alpha_4$
5	3	1	$1 \times 70 = 70 = \alpha_5$
	1	$c = 70$	x
		0	x

Divide $\bar{x}$ by 100 getting remainder 90. $x' = 56 + 63t.$ Also divide $\bar{y}$ by 63 getting remainder 56. $y' = 90 + 100t.$ The least solution is $(\alpha, \beta) = (56, 90)$ after verification.

Example2. Consider the problem $63y = 100x - 70.$

The least solution is $(b - \alpha, a - \beta) = (63 - 56, 100 - 90),$ i.e. (7, 10) after verification.

AfterĀryabhaṭa I the method for $ax - by = \pm c$ was followed by Bhāskara I (600 AD), Brahmagupta (628 AD), Govindasvāmi (c.850 AD), Prthudakasvāmi (c. 850 AD) and Śripati (1039 AD). Āryabhaṭa II (950 AD) continued the mutual division till the remainder became 1. Mahāvira(850 AD) and Bhāskara II (b. 1150 AD) simply adopted the method of Āryabhaṭa I and extended to (1).

Later scholars involved are: Devraja, NārāyaṇaPaṇdita, Jyesthadeva, Kamlākara and Putuman Somayaji.

Improvement upon IAA

Some of the remainders are taken to be as least and may be negative, in such casesfew of the partial quotients may turn out to be negative. This subsequently improves the speed of improved ĀryabhaṭaI's Algorithm.

Example3. Consider $63y = 100x \pm 70.$

Table5

S.N.	Remainders	*Valli*	x,y
0		1	$1\times1190 + 700 = 1890 = \alpha_0 = \bar{y}$
1	37	2	$2\times700 - 210 = 1190 = \alpha_1 = \bar{x}$
2	-11	-3	$(-3)(-3)\times70 + 70 = 700 = \alpha_2$
3	4	-3	$(-3)\times70 = -210 = \alpha_3$
4	1	$c = 70$	
		0	

Solutions are the same as Examples 1 and 2 but with one step faster.

2.2. Second Method (Simple Continued Fraction) [TSB]

Let $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, ..., \frac{P_n}{Q_n}$ be the successive convergent of $\frac{a}{b}$, then

$$\frac{a}{b} = q_0 + \frac{1}{q_1 +}\frac{1}{q_2 +}..... \frac{1}{q_n +}\frac{1}{q_n}.... = \frac{P_n}{Q_n}, \text{ if } r_{n+1} = 0.$$

Here

$$\frac{P_0}{Q_0} = q_0\,,\ \frac{P_1}{Q_1} = q_0 + \frac{1}{q_1} = \frac{q_0q_1 + 1}{q_1},\ \frac{P_2}{Q_2} = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = \frac{q_0(q_1q_2 + 1) + q_2}{q_1q_2 + 1}, ..., \frac{P_n}{Q_n} = \frac{a}{b}.$$

Clearly we have the following recurrence relations:

$$P_n = q_nP_{n-1} + P_{n-2}, n > 2$$

$$Q_n = q_nQ_{n-1} + Q_{n-2}, n > 2$$

where

$$P_0 = a_0, Q_0 = 1$$

$$P_1 = a_0a_1 + 1, Q_1 = a_1$$

$$\begin{aligned} P_nQ_{n-1} - P_{n-1}Q_n &= (q_nP_{n-1} - P_{n-2})Q_{n-1} - P_{n-1}(q_nQ_{n-1} - Q_{n-2}) = -(P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1}) \\ &= (-)(-)(P_{n-2}Q_{n-3} - P_{n-3}Q_{n-2}) = ... = (-1)^{n-1}(P_1Q_0 - P_oQ_1) \\ &= (-1)^{n-1}(q_0q_1 + 1 - q_0q_1) = (-1)^{n-1}, n = 1,2,... \end{aligned}$$

Evidently, $P_nQ_{n-1} - Q_nP_{n-1} = \pm1$ according as *n* (number of partial quotients excluding Q_0) is even or odd, that is, $aQ_{n-1} - bP_{n-1} = \pm1.$ Let $Q_{n-1} = x_0', P_{n-1} = y_0'$, we have $ax_0' - by_0' = \pm1$ which further gives (1), where $x' = cx_0', y' = cy_0'.$ Moreover, we obtain $x = x' + bm, y = y' + am,$ *m* an integer. Putting suitable value of *m* will give the least solution $(\alpha, \beta).$

Example 4. Let $13y = 60x + 3.$

Continued fraction

$$\frac{60}{13} = 4 + \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{2} = \frac{13}{8}.$$

$ax_0' - by_0' = 60.8 - 13.37 = -1$ implies $x' = 3.8 = 24, y' = 3.37 = 111.$

The general solutions are: $x = 24 + 3t, y = 111 + 60t.$ For $t = -1, x = 11, y - 51$ is the smallest solution.

2.3. Some Specific Forms and Applications

Rule[*Līlāvatī* (LV)263] When the Constant is Zero [P-N-S]

If the constant (*c*) is zero or divisible by the divisor (*b*), a multiplier is zero and the (corresponding) quotient is the constant divided by divisor. That is, one solution is $x = 0$ and other $y = c/b$.

Rule (LV 265) When Constant is 1 [P-N-S]

First solve $\frac{ax \pm 1}{b} = y$ and get a solution $(x_{0,} y_0)$. Then a solution of $\frac{ax \pm c}{b} = y$ is: *x* is the remainder in $\frac{cx_0}{b}$ and *y* is the remainder in $\frac{cy_0}{a}$.

Example5 [**LV 251**][P-N-S]. O friend, one hundred is multiplied by an integer; 90 is added to or subtracted from the product; the results are exactly divisible by 63. If you are efficient in pulverization, tell me the multiplier correctly.

That is, if $100x \pm 90$ is divisible by 63, find x.

The solutions are: $x = 18 + 63t, y = 30 + 100t$ for 90 additives and $x = 45 + 63t, y = 70 + 100t$ for 90 subtractive, where *t* is an integer.

The same example is contained in *Bījagaṇita*(BG) Ch. 14, v.61 of Bhāskara II.

Example6[BG Ch. 14, v.143] [TBH p. 142-144]. Find a number *x* such that if *m* is the quotient and *p* is the remainder when 9*x* is divided by 10 and *n* is the quotient and *q* is the remainder when 7*x* is divided by 10. Given $m + n + p + q = 26.$

Here $9x = 30m + p$ and $7x = 30n + q.$ Adding $16x = 29k + 26,$ where $k = m + n.$ The least solutions are: $x = 29 - 2 = 27, y = 16 - 2 = 14.$ The general solutions are: $x = 27 + 29t, y = 14 + 16t.$ Further $k + p + q = 26$ implies $k = 14.$ Finally, $m = 8, n = 6, p = 3, q - 9.$

Example 7 [BG Ch. 14, v.144] [TBH p. 144-145]. Find a number *x* such that if a, b, c are the remainders when $3x, 7x$ and $9x$ are divided by 30, then 11 is the remainder when $a + b + c$ is divided by 30.

Here $9x = 30m + a,\ 7x = 30m + b,\ 9x = 30n + c$ and $a + b + c = 30q + 11.$ Adding $16x = 30k + 11$ by letting $m + n + p + q = k.$ Also $a + b + c = 30q + 11.$ The solution is: $x = 29 + 30t.$ Finally, $a = 27, b = 23, c = 21.$

Pulverizers with the Same Divisor [P-N-S]

If an (unknown) integer is multiplied by two integers (separately) and the products divided by a (given) leave two remainders then (to find the unknown) assume the sum of multipliers as dividend and sum of the remainders as negative constant of a proper pulverizer, which is the union of two pulverizers.

That is, if $\frac{ax}{b} = y + \frac{c}{b}$, i.e. $ax - c = by$ and $\frac{a'x}{b} = y' + \frac{c'}{b}$, i.e. $a'x - c' = by',$ then

$$(a+a')x-(c+c')=b(y+y').$$

Example8 [LV267][P-N-S]

If the product of an (unknown) integer and 5 is divided by 63 then the remainder is 7. If the same integer is multiplied by 10 and divided by 3 then the remainder is 14. Tell that integer.

The united pulverizer is $5x-7=21y.\ x=14,35,56,\ldots\ldots$

Example9[Krishna Daivajna Commentary on BG].Given the fractional part 11/19 of seconds, find the integral parts of seconds, minutes, degrees, signs and the fractional part of revolutions (1 sign=30 degree)

Suppose that the fractional part $x/19$ of minutes is to convert into seconds so that

$$\frac{x}{19}.60=y+\frac{11}{19},i.e.\ \frac{16x-11}{19}=y.$$

[*y* is integral part of seconds. (10, 31) is the least solution.]

Thus we recover the integral part 31 of seconds and we see that $x/19=10/19$ must be the fractional part of minutes involved. Now repeat the above argument. Suppose that the fractional part $x'/19$ of degree is to convert into minutes so that

$$\frac{x'}{19}.60=y'+\frac{10}{19},i.e.\ \frac{16x'-10}{19}=y'.$$

(16, 50) is the least solution.

Similarly, we find (17, 26) and (3, 1) the least solution of $\frac{13x''-16}{19}=y''$ and $\frac{12x''-17}{19}=y'''$ respectively.

Hence complete answer is: $1\,sign,26^{\circ},50',31\frac{11''}{19}\,or\,\frac{3}{19}\,revolutions$

Application: Vīrasena (*Dhavalāṭika*, c.816) Equation [M-Sa]

'The diameter multiplied by 16, increased by 16, divided by 113, and (again) combined with thrice the diameter is (the circumference) more accurate than the accurate one'.

$c=3d+(16d+16)/113$ (8) [Dimensionless]

Equivalently,

$$p=\frac{355}{113}+\frac{16}{113d},\ p=c/d \qquad (9)$$

(9) ismonotonically decreasing.

From (8)

$$113c=355d+16$$

Solving

$$c=352+355t;d=112+113t,\ where\,t=0,1,2,\ldots.$$

Pie corresponding to $t=0,i.e.\,d=112$ is 22/7

Pie corresponding to $t=176,i.e.\,d=20000$ is 62832/20000

Pie corresponding to $t = \infty, i.e.\, d = \infty$ is 355/113

Inequalities for Pie

Various significant values of Pie including series representation exist in India [M-Sb]. Takao Hayashi's [M-Sa] argument that there was no attempt in India to find the range for Pie is not worthwhile as we established inequality $355/113 < \pi < 22/7$ (from Vīrasena's verse) comparable to $223/71 < \pi < 22/7$ (Archemedes, fl. 287-212 BCE). Using remark of Vīrasena and taking ĀryabhaṭaI's value for pie 62832/20000 in consideration, Mishra and Singh [M-Sa] established

$$355/113 < \pi < 62832/20000\,, i.e.\ 3.1415929... < \pi < 3.1416.$$

III. EQUATIONS WITH NEGATIVE DIVIDEND: $ax + by = c$

Equation $ax + by = c$ possesses only a finite number of solutions. Even sometimes equation of this type may not have a solution. Distinction is that for Form (1), for both cases *c* and –*c*, common difference is positive for both *x* and *y* whereas for above form, this is positive for one variable and negative for the other variable.

3.1. First Method (Nārāyaṇa) [PSb]

If $x = \alpha, y = \beta$ be a solution of (5), then $x = -\alpha, y = \beta$ or $x = \alpha, y = -\beta$ will be a solution of $by = -ax + c.$

3.2. Second Method [TBH]

Write (2) in the *kuṭṭaka* form $\dfrac{-ax + c}{b} = y.$

Ignore the negative sign of dividend (-*a*) and proceed to construct *valli* etc. as before for solution of (1). After scraping off we get values of x' and $y'.$ Now if

i) *Valli* $n = odd, \alpha = b - x', \beta = y'$

ii) *Valli* $n = even, \alpha = x', \beta = a - y'$

Here it is important to note that they are not the corresponding values in general, infact they are the smallest possible positive values of *x* and *y*. They are corresponding values exactly when there is one and only one solution. Substituting in the equation we get their greatest values. Now as *x* and *y* are in arithmetic progressions. So one of them is increasing while the other decreasing, since the sum $ax + by$ must remain constant.

3.3. Third Method (Brahmagupta) [TBH]

1) Convert $y = \dfrac{-ax + c}{b}$ into $y = \dfrac{ax - c}{b}$ and proceed to construct *valli* etc as before for the solution of (1).

2) Quotient when dividing *labdhi* and *guṇa*by a and b respectively, must be the same and we obtain $x', y'.$ Meaning is: $\bar{x} = bl + x', \bar{y} = al + y'.$ *l*-quotient

   We get *x,y* . Write it as (u, v) and verify in (2).

3) $x = u - b, y = a - v$ and verify in (3). u, v may be negative.

4) Values for *x* and *y* are both in A.P., when *x* increases, *y* decreases and vice-versa, since the sum $ax + by$ is constant. Finally, take only the positive solutions $x = \alpha + bm, y = \beta - am, m = 0,1,2,\ldots,(N-1).$.

3.4. Fourth Method (Simple Continued Fraction) [TBH]

Express *a/b* as Simple Continued Fraction with even (i.e. *n* =odd) number of convergents (by continuing process of mutual division till remainder becomes zero). If not then make it even by breaking last quotient. Make use of penultimate convergent P_{n-1}/Q_{n-1} in $aQ_{n-1}-bP_{n-1}=1.$ Let $Q_{n-1}=x_0', P_{n-1}=y_0',$ we have $ax_0'-by_0'=1$ which further gives (2), where $x'=cx_0', y'=cy_0'.$ further, we obtain $x=x'-bm, y=am-y',$ *m* an integer. Putting suitable value of *m* we give the least solution $(\alpha,\beta).$ Now since $x>0, y>0$ and so we get the values of *m* lying in $\frac{y'}{a}<m<\frac{x'}{b}.$ This implies $r+s<m<R+S,$ where $0\le m<1, 0<S\le 1.$ Thus we get the number of solutions, $N=R-r.$

Exampl10 [TBH, p. 26]. Let $11x+29y=1067.$

Continued fraction

$$\frac{11}{29}=0+\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}=\frac{3}{8}.$$

$ax_0'-by_0'=11.8-29.3=1$ implies $x'=8536, y'=3201.$

The general solutions are $x=8536-29t, y=11t-3201.$

$\frac{3201}{11}<m<\frac{8536}{29}, i.e. 291<m<294+\frac{10}{29}.$ The number of solutions is $N=294-291=3.$

We write $x=29(294-t)+10, y=11(t-291).$ For $t=292,293,294,$ the solutions are (66, 11), (39,22) and (10,33).

3.5. Fifth Method (Taylor) [TBH]

Off *a* and *b* choose smaller one, say *a*. Divide *b* and *c* by a to obtain remainders r_b and r_c respectively.

1) Write down the natural numbers from 1 to $(a-1).$
2) Multiply these by $r_b.$
3) Divide these numbers by a and write down only the remainders. Count the place of remainder $r_c,$ called the rank of $r_c=r,$ say. It will give $y=r.$ Substituting in the given equation (3) will yield the corresponding value *x*.
4) Here we note that second and third steps become very laborious when *a* and *b* are large. These steps are equivalent to the following: We require the smallest number $1\le x\le a-1$ such that $r_b x$ leaves remainder r_c when divided by *a*, i.e. $r_b x=an+r_c.$ From where we find integer *x* by trial corresponding to the least positive integer *n*. Substituting in the given equation (3), we get corresponding *y*.

3.6. Method for Obtaining Integral Solutions [M-S]

Consider $c\le a+b$ in (2). Let the solutions be $x=\alpha+bm, y=\beta-am, m=0,\pm1,\pm2,\ldots,\pm(N-1).$ (α,β) is the least solution of (2). We set the pair as:

$x_1=\alpha, x_2,\ldots., x_N=x_{\max}.$

$y_N=y_{\max}, y_{N-1},\ldots., y_2, y_1=\beta.$

The *N* solutions are: $(x_1,y_N),(x_2,y_{N-1}),\ldots\ldots., (x_N,y_1).$ Further (x,y) is optimal solution if either or both of

$$|x| < b, |y| < a. \tag{10}$$

Similarly for (α, β). Moreover, there exist two integers $L \le 0 \le M$ such that the solution (x, y) satisfies (10) when $m = L, L+1, \ldots, M$ but fails to satisfy either of them when $m < L or m > M$. Thus after obtaining (α, β) calculate $|x| + |y|$ for $m \ge 0$ until (x, y) satisfies neither of (10). Similarly proceed for negative values of *m.* Thereafter find all the values of $|x| + |y|$, the smallest one will be the optimal solution.

Write (2) as $x = \frac{c - bp}{a}$ and $y = \frac{c - ap}{b}$. Once a zero remainder is obtained we stop and (α, β) is obtained. If the zero remainder is observed in the first step then $\alpha = \frac{c - bp}{a}$ and $\beta = p$; otherwise $\alpha = p$ and $\beta = \frac{c - bp}{a}$.

Remark: If one solution is positive other has to be negative.

In his example of $3x + 10y = 8,$ Mauch and Shi [M-S] find the two solutions (6,-1) and (-4, 2) with later as optimal solution.

Exampl 11. Let $7x + 8y = 106.$

Table6.

p	$x = \frac{106 - 8p}{7}$	quotient	remainder	$y = \frac{106 - 7p}{8}$	quotient	remainder	(α, β)
0	106/8	13	2	106/7	15	1	No
1	99/8	12	3	98/7	14	0	Yes $(14,1)$

Table7.

p	(x, y)	$\|x\| + \|y\|$	Relation (10) satisfied or not
0	$(14,1)$	15	Yes
1	$(22,-6)$	28	No, stop increasing value of p
-1	$(6,8)$	14	Yes
-2	$(-2,15)$	17	Yes, but solution does not exist
-3	$(-10,22)$	32	No, stop decreasing value of p

Out of two solutions (14, 1) and (6, 8) with former as optimal solution.

Application: Magic Squares with Entries in A.P.[PSa]

Let *n* be the total number of cells in the magic square (MS) and *N* its order. The MS is called double even, single even or odd accordingly $n = 4m + 2, 4m + 1 or 4m + 3.$

Square constant *S* is defined by

$$S = \frac{T}{N} = \frac{n(2a + (n-1)d)}{2N}.$$

S may be even (=2*m*) or odd (=2*m*+1).

No. of steps=*N*=No. of cells in a row (*caraṇa*) of MS= Order of MS= $\sqrt{n}$.

For $a=1,d=1,\ T=\frac{n}{2}\left[2a+(n-1)d\right]=na+\frac{n(n-1)}{2}d=na+sd$, where sum of all natural numbers $s=\frac{n(n-1)}{2}$. This means the first term *a* and common difference *d* of the A.P. are to be solved using pulverizer (*kuṭṭaka*) for generating equation $-sd+T=na.$

Example12 (GK Ch. XIV). O learned, if you have pride in mathematics, tell the integral first term (=1) and common difference (=1) of magic squares (whose) total number of cells are 16, 36 and 9 and (whose) totals are 400, 1296 and 180, in order.

Accordingly, the pulverisers are: $2a+15d=50,\ 2a+35d=72$ and $a+4d=20.$

The least solutions are respectively (25, 0), (1, 2) and (20, 0).

IV. General Problems Of Remainders

To find a number *N* which when divided by given positive numbers $a_1,a_2,a_3.....,\ a_n$ leaves the remainders (positive numbers) $r_1,r_2,r_3.....,\ r_n$ respectively. That is, to solve the $(n-1)$ simultaneous equations:

$$N=a_1x_1+r_1=a_2x_2+r_2=.....=a_nx_n+r_n \tag{11}$$

Here it is important that a common solution certainly exists if $a_i's$ are pairwise co-prime or GCM of $a_i,\ a_j$ divides r_i-r_j for all i,j such that $1\le i\le j\le n.$ Also if *m* is the least positive value of *N* then the general value is $N=m+dt,$ where d is the LCM of $a_1,a_2,a_3.....,\ a_n$ and *t* any non-negative integer.

The solution of (11) was known to Āryabhaṭa I,Bhāskara I, Brahmagupta, Mahāvīra, Bhāskara II and Nārāyaṇa

4.1. $n=3.$

In this case we have three methods for $N=a_1x_1+r_1=a_2x_2+r_2=a_3x_3+r_3.$

First method (Sun-Tsu) [TBH and UL]**.** Use of intermediary variable (here x_2)

Solving first equation formed from variables x_1,x_2 by *kuṭṭaka,* we get solutions in A.P. form as

$$\begin{aligned}x_1&=x_{1\min}+a_2p\\ x_2&=x_{2\min}+a_1p,p\ge 0\end{aligned} \tag{12a}$$

Solving second equation formed from variables x_2,x_3 by *kuṭṭaka,* we get solutions in A.P. form as:

$$\begin{aligned}x_2&=x'_{2\min}+d'_2q\\ x_3&=x_{3\min}+d_3q,q\ge 0\end{aligned} \tag{12b}$$

For common solutions of two equations, we take values common to the above two series of values for x_2 and then take the corresponding values of x_1 and $x_3.$ This gives the general solution

$$x_1=a_2a_3t+x_{1\min},x_2=a_1a_3t+x_{2\min},x_3=a_1a_2t+x_{3\min} \tag{12c}$$

and

$$N=a_1x_1+r_1=a_1\left(a_2a_3t+x_1\min\right)+r,i.e.N=N_{\min}+dt,t\ge 0, \tag{12d}$$

where $N_{\min} = a_1 x_{1\min} + r_1, d = a_1 a_2 a_3.$

Example 13(Sun Tsu). $N = 3x + 2 = 5y + 3 = 7z + 2.$

*kuṭṭaka*I gives $x = 2, y = 1.$ The General solutions are: $x = 2 + 5p, y = 1 + 3p.$

*kuṭṭaka*II gives $y = 4, z = 3.$ The General solutions are: $y = 4 + 7q, z = 3 + 5q.$

Corresponding to $y = 4,$ we have $x = 7, z = 3.$

Hence $x = 7 + 35t, y = 4 + 21t, z = 3 + 15t.$

Second Method (Brahmagupta)[TBH]

Form I. Get upto

$$x_1 = x_1' + a_2 p$$
$$x_2 = x_2' + a_1 p, p \geq 0$$

Now

$$N_{\min} = a_1 (x_{1\min} + a_2 p) + r_1 = a_1 a_2 p + (a_1 x_{1\min} + r_1).$$

Equating with third equality, we obtain second equation in *p* and $x_3.$

$$a_1 a_2 p + (a_1 x_{1\min} + r_1) = a_3 x_3 + r_3. \tag{13}$$

This gives

$x_3 = x_{3\min} + a_1 a_2 q, q \geq 0$ and

$$N_{\min} = a_3 (x_{3\min} + a_1 a_2 q) + r_3 = a_1 a_2 a_3 q + a_1 a_2 p + a_1 x_{1\min} + r_1.$$

Here $x_{3\min}$ is the smallest value of x_3 satisfying this equation so that $N_{\min} = a_3 x_{3\min} + r_3.$ $x_{1\min}$ and $x_{2\min}$ can be easily obtained from $N_{\min} = a_1 x_{1\min} + r_1, N_{\min} = a_2 x_{2\min} + r_2.$

Proceeding in this way successively we find

$$N = a_3 (x_{3\min} + a_1 a_2 q) + r_3 = a_1 a_2 a_3 .... a_n q + a_1 a_2 .... a_{n-1} \alpha_{n-1} + ... + a_1 \alpha_1 + r_1.$$

Similar method is prescribed by Mahāvīra (*Gaṇitasārsaṅgraha*) and Nārāyaṇa (*Gaṇitakaumudī*).Nārāyaṇaoffers extended version of the above rule.

Example 14 [GK] [PSb]**.** Tell the numbers which when divided by 3,5 and 7, leave the remainders 1,3 and 5, (in order)

$N = 3x + 1 = 5y + 3 = 7z + 5.$

*kuṭṭaka*I gives $x = 4, y = 2.$ Using (13), $15p + 8 = 7z.$ This gives $p = 6, z = 14.$

Now $N_{\min} = 7.14 + 5 = 103$ implies $103 = 3x + 1 = 5y + 3,$ yielding $x = 34, y = 20.$

Hence $x = 34 + 35p, y = 20 + 21p, z = 14 + 15p.$

Form II. Let $a_1 < a_2.$ Then first equality can be written as

$$a_1 X + r_1 - r_2 = (a_2 - a_1) x_2, X = x_1 - x_2.$$

Let

$$X = X' + (a_2 - a_1)p$$
$$x_2 = x_2' + a_1 p, p \geq 0 \quad (14)$$
$$N_{1\min} = a_2 x_2' + r_2$$

be the solution of above first equation.

Now proceed as in Form I.

Form III. Get upto (11) of Form1or (14) of Form II.

Substituting x_2 in the second inequality, we get second *kuṭṭaka* $a_1 a_2 p + N_{1\min} - r_3 = a_3 x_3$.

Let R,S be the respective remainders when $N_{1\min}$ and $a_1 a_2$ are divided by C. Thus obtaining $N_{1\min} = cr + R, a_1 a_2 = cs + S$ and substituting in the second equation, we have

$Sp + R - r_3 = cq$, where $q = x_3 - sp - r$.

Now $N_{\min} = a_2 x_{2\min} + r_2 = a_2 (a_1 p_{\min} + x_2') + r_2$, from FormI

$= a_1 a_2 p_{\min} + N_{1\min}$.

4.2. $n = 4$.

First Method (Brahmagupta)[TBH]

Consider $N = a_1 x_1 + r_1 = a_2 x_2 + r_2$. Proceed upto (11) so that $N_1 = a_1 a_2 m + N_{1\min}, m \geq 0$. Changing $N_1 \to N_2$ and let $N_2 = a_1 a_2 m + N_{1\min} = a_3 x_3 + r_3$.

$N_{2\min} = a_3 x_3' + r_3$. $N_2 = a_1 a_2 a_3 n + N_{2\min}, n \geq 0$.

Changing $N_2 \to N$ and letting $N_2 = a_1 a_2 a_3 n + N_{2\min} = a_4 x_4 + r_4$, $N_{\min} = a_4 x_{4\min}' + r_4$.

General solution obtained is:

$x_1 = a_2 a_3 a_4 t + x_{1\min}, x_2 = a_1 a_3 a_4 t + x_{2\min}, x_3 = a_1 a_2 a_4 t + x_{3\min}, x_4 = a_1 a_2 a_3 t + N_{4\min}$.

$N = a_1 a_2 a_3 a_4 t + N_{\min}$.

Second Method (Splitting up)[TBH]

Splitting the equations into two sets

$$N_1 = a_1 x_1 + r_1 = a_2 x_2 + r_2. \quad (15)$$

$$N_2 = a_3 x_3 + r_3 = a_4 x_4 + r_4. \quad (16)$$

Solving (15), $N_1 = a_1 a_2 m + N_{1\min}, m \geq 0$.

Solving (16), $N_2 = a_3 a_4 n + N_{2\min}, n \geq 0$.

Equating N_1, N_2 for common solution $(N = N_1 = N_2)$, we obtain *kuṭṭaka* in *m,n*. So we find

$N_{\min} = a_1 a_2 m_{\min}' + N_{1\min}$.

From given equation we easily obtain $x_{1\min}, x_{2\min}, x_{3\min}, x_{4\min}$. General solution is governed by (15).

4.3. $n = 5.$

Consider two sets

$$N_1 = a_1x_1 + r_1 = a_2x_2 + r_2 = a_3x_3 + r_3. \quad (17)$$

$$N_2 = a_4x_4 + r_4 = a_5x_5 + r_5. \quad (18)$$

Solve for N_1, N_2 as above and equate for common solutions.

Let $n = 6.$ Consider two sets

$$N_1 = a_1x_1 + r_1 = a_2x_2 + r_2 = a_3x_3 + r_3. \quad (19)$$

$$N_2 = a_4x_4 + r_4 = a_5x_5 + r_5 = a_6x_6 + r_6. \quad (20)$$

Solve for N_1, N_2 as above and equate for common solutions.

4.5. In the similar way solution for $n = 7,8,\ldots.$ **can be obtained.**

V. PROBLEMS OF SAMSLISTAKUṭṭAKA (CONSTANT PULVERIZER)

5.1. Part I. First Method

To solve simultaneous equations

$$b_1y_1 = a_1x_1 \pm c_1 \quad (21)$$

$$b_2y_2 = a_2x_2 \pm c_2 \quad (22)$$

$$b_3y_3 = a_3x_3 \pm c_3 \quad (23)$$

Here LCM of the coefficients of x_1, x_2, x_3 is L. Hence system is equivalent to

$$Lx = b_1L_1y_1 \mp L_1C_1 = b_2L_2y_2 \mp L_2C_2 = b_3L_3y_3 \mp L_3C_3, \text{ where } L = a_1L_1 = a_2L_2 = a_3L_3. \quad (24)$$

First solve $N_1 = b_1L_1y_1 \mp L_1C_1 = b_2L_2y_2 \mp L_2C_2$ so that $N_1 = Mp + N_{1\min}$, M is the LCM of b_1L_1 and b_2L_2.

Now consider $N = Mp + N_{1\min} = b_3L_3y_3 \mp L_3C_3.$ This implies $N_{\min} = Lx$ which gives $x_{\min}$. Other values $y_{1\min}, y_{2\min}, y_{3\min}$ are obtained from (24).

Second Method

Eq. (21) implies

$$x = b_1p + x' \quad (25)$$

Substituting this in (22) gives

$$p = b_2q + p' \quad (26)$$

Now substituting (26) in (25) we get equation in *x,q*. Substituting the values of *x* of this equation in (23) we get another equation in $y_3, q.$ This implies

$$q = b_3r + q' \quad (27)$$

Hence from (23) and (27) we obtain *x* and thereby $x_{\min}$.

5.2. Part II.

Sum of the dividends, $a = a_1 + a_2 + a_3$.

Sum of the remainders, $c = c_1 + c_2 + c_3$.

Suppose $b_1 = b_2 = b_3 = b$. Adding (21), (22) and (23), $by = ax \pm c$ which gives $x = x_{\min}$ and $y = y_{\min}$. Now substituting *x* in the above equations we obtain y_1, y_2, y_3.

Third Method (Nārāyaṇa**)**[PSb]

If $N = a_1x_1 + r = a_2x_2 + r = ... = a_nx_n + r$, then $N = r$ with LCM of $a_1, a_2, a_2, ..., a_n$ as additive.

VI. Modern Development and Applications

In the nineteenth and twentieth century's there have been considerable attentions to ancient Indian mathematics with a point of view of translation from Sanskrit texts, mathematical interpretation and formulation and comparison with other counter parts. However, study of computational efficiencies of algorithms as of today was lacking, ignored or forgotten. In concern of Āryabhaṭa I's algorithm of linear indeterminate equation requires approximately $5 + 3\log_2 N$ operations of addition, multiplication and division where *N* is the order of moduli. In Chinese remainder and Garner's algorithms complexities involved are of the same order or module or more. The two algorithms are of immense interest as these are applied to solve system of congruence's concerned with theory of coding, cryptography, signal processing, computer design. These are used to find modular inverses $a^{-1} \bmod b$ and $b^{-1} \bmod a$.

Rao and Yang [R-Y] applied improved ĀryabhaṭaI's algorithm (IAA) for $by = ax + c$ and extended to*t* moduli and named it as Āryabhaṭa remainder theorem (ART). This paper also contains extended Euclidean algorithm (EEA) and Chinese remainder theorem (CRT). CRT has further been compared with Garners algorithm. Later on ART was extended by Chang, Yeh and Yang [C-Y-Y] and Liu, Chang and Chang [L-C-C] to *t* moduli which led to generalized Āryabhaṭaremainder theorem (GART). Liu and Chang [L-C] applied GART to describe new data based encryption scheme whereby entire content of a record (confidential data) is converted into cipher text. Only authorized users can then use their decryption key to recover the cipher text to original field values of the record by GART.Priyanka et al.[P-N-K-R-C]applied CRT and ART based water making scheme in discrete cosine transform domain while CRT based scheme is concluded to be more resistant to different types of attacks and improved security feature. ART based algorithm is applicable to any kind of moduli and computation is cost effective than CRT based algorithm. Koo, Change and Yu [K-C-Y] applied ART to dynamic multicast management system.

References

[1] [AKB]AK Bag, the Method of Integral Solution of Indeterminate Equations of the Type: $By = Ax \pm C$ in Ancient and Medieval India, *Indian Journal of History of Science* 12 (1977), 1-16.

[2] [AKD]AK Dutta, Mathematics in Ancient India: Diophantine Equations: The Kuṭṭaka, *Resonance* 7 (2002) 4-19.

[3] [D-S]B Datta and AN Singh, *History of Hindu Mathematics*, Two Parts, Asia Publishing House, Bombay, 1962.

[4] [CBB]CB Boyer, *A History of Mathematics* (revised by Uta C. Merzbach), John Wiley & Sons, New York, 1989.

[5] [S-S]KS Shukla and KV Sarma, *Āryabhaṭīya of Āryabhaṭa*, Indian National Science Academy, New Delhi, 1976.

[6] [P-N-S]KS Patwardhan, SA Naimpally and SL Singh, *Līlāvati of Bhāskarācārya: A Treatise on Mathematics of Vedic Tradition*, MotilalBanarsidass, 2001.

[7] [PSa]Parmanand Singh, The *Gaṇitakaumudīof* NārāyaṇaPaṇdita (translation with notes), *GaṇitaBhāratī* 20 (1998), 25 – 82.

[8] [PSb]Parmanand Singh, the *Gaṇitakaumudī of* NārāyaṇaPaṇdita (translation with notes), *GaṇitaBhāratī* 22 (2000), 19 – 85.

[9] [PKM]PK Majumdar, A Rational of Brahmagupta's Method of Solving $ax + c = by$, *Indian Journal of History of Science* 16 (1981), 111-117.

[10] [RSS]RS Sharma, *Brahmasphutasiddhānta*, Vol. I, Indian Institute of Astronomical and Sanskrit Research, New Delhi, 1966.

[11] [M-Sa]Vinod Mishra and S.L. Singh, First Degree Indeterminate Analysis in Ancient India and its Application by Virasena, *Indian Journal of History of Science* 32(1997), 127-133.

[12] [M-Sb]Vinod Mishra and S.L. Singh, Values of π from Antiquity to Ramanujan, *SugakushiKenkyu*, No. 157, 1998, 12-25.

[13] [CZ]Changjiang Zhu, Integral Solutions to Linear Indeterminate Equation, 2011, arxiv.org

[14] [AK]Agathe Keller, Bhāskara I's Versified Solutions of a Linear Indeterminate Equation, *Indian Journal of History of Science*, 49.2 (2014) 97-126

[15] [UL]Ulrich Libbrecht, Chinese Mathematic in the Thirteenth Century, Ch.5 The Chinese Remainder Theorem: A Monograph, pp. 213-283, Dover, 2005

[16] [M-S]Elizabeth Mauch and Yixun Shi, Application of Linear Diophantine Equations in Teaching Mathematical Thinking, *Mathematics and Computer Education*, 240-247.

[17] [L-C]Yanjun Liu and Chin-Chen Chang, A Database Encryption Scheme Based on the Generalized Āryabhaṭa Remainder Theorem, *Journal of Information Hiding and Multimedia Signal Processing* 5(2014), 603-613.

[18] [R-Y]TRN Rao and Chung-Huang Yang, ĀryabhaṭaRemainder Theorem: Relevance to Public- Key Crypto-Algorithms, *Circuit, Systems and Signal Processing* 25(2006), 1-15.

[19] [KCY]Tung-Ming Koo, Hung-Chang Chang and Ting-Ching Yu, A Refined Research on the Dynamic Multicast Management Scheme, *International Journal of Digital Content Technology and its Applications* 6(2012), 41-49.

[20] [TBH]TB Hardikar, Indeterminate Analysis, Pune, 1991.

[21] [SK] SubashKak, Computational Aspects of the Āryabhaṭa Algorithm, *Indian Journal of History of Science* 21 (1986), 62-71.

[22] [P-N-K-R-C]V Priyanka, MNireesha, VVenu Kumar, N Venkat Ram, ASN Chakravarthy, CRT and ART based Watermaking Scheme in DCT Domain, *International Journal of Engineering and Advanced Technology* 1 (2012), 87-90.