Revista Brasileira de História da Matemática - Vol. 15 nº. 30 - pág. 83-94
Publicação Oficial da Sociedade Brasileira de História da Matemática
ISSN 1519-955X

THE LINEAR INDETERMINATE EQUATION - A BRIEF HISTORICAL ACCOUNT

Kedar N Shukla
PRERANA CGHS Ltd., Sector-56, Gurgaon-122011 – India

(aceito para publicação em fevereiro de 2015)

Abstract

The paper presents in brief the contribution of Aryabhata in developing general solution of indeterminate equation of the type ax + c = by, where a, b, c are the integers. Also the contributions of Bhaskara and Brahmagupta in developing the solution of the indeterminate equations are discussed. Finally an example of Paramesvara is illustrated to solve coupled linear indeterminate equations which may be adopted to find the multiplicative inverse in a group that is of interest in cryptology, signal processing, coding and computer design.

Keywords Indeterminate equation; Chinese remainder theorem; Aryabhata; Kuttaka; Brahmagupta; Bhaskara.

[A EQUAÇÃO LINEAR INDETERMINADA – UMA BREVE CONSIDERAÇÃO HISTÓRICA]

Resumo

O artigo apresenta sucintamente a contribuição de Aryabhata no desenvolvimento da solução geral da equação indeterminada do tipo ax + c = by, em que a, b e c são inteiros. Também são discutidas as contribuições de Bhaskara e Brahmagupta ao desenvolvimento da solução de equações indeterminadas. Finalmente, um exemplo de Paramesvara serve de ilustração para resolver equações lineares indeterminadas acopladas que podem ser adotadas para encontrar o inverso multiplicativo em um grupo, de interesse em criptologia, processamento de sinais, codificação e projetos de computadores.

Palavras-chave: Equação indeterminada; teorema chinês do resíduo; Aryabhata; Kuttaka; Brahmagupta; Bhaskara.

Introduction

A problem of great interest to Indian mathematicians since ancient times has been to find integer solutions to the equations of the form ax+ by = c; a, b and c are integers a topic that is commonly known as Diophantine equations, proposed by the third century Alexandria mathematician Diaphanos. Although the problem has its roots in Vedic literature determining the planetary positions, it brought the attention of a 5^{th} century renowned mathematician and astronomer of India, Aryabhata. Aryabhata (476-550) developed a general method to solve an indeterminate equation. He called the method as **"**kuttaka**"** (pulverizer) which is now referred as Aryabhata**'s** algorithm. The kuttaka means a process of breaking into small pieces, and thus it involves a recursive algorithm for writing the original factors in terms of smaller numbers. The Euclidean algorithm, which occurs in the Elements of Euclid, (1956), gives a method to compute the greatest common divisor of two numbers by a sequence of reductions to smaller numbers. Although Euclid (325-265BC) did not suggest that the method could be used to solve linear indeterminate equations, it is commonly recognized that if the algorithm in Euclid is applied in reverse order, then in fact it yields Aryabhata**'**s kuttaka method. The method is also referred as the extended Euclidean algorithm ignoring the contribution of Aryabhata. Lehmer (1919) applied the Euclid method in determining the general solution of the indeterminate equation. There was also a mention of the Chinese Remainder Theorem (CRT) in a third century book by Sun Tzu, see Ulrich (1973).Although Sun Tzu's work contains neither a proof nor a solution; what amounts to a CRT algorithm was already given in Aryabhatiya as special cases. In fact, the CRT algorithm was developed in a general form by a Sanskrit scholar I-Tsing in AD727 who visited India in AD673 and brought the method of kuttaka from India for calculations used in making the Chinese calendars. Voladarsky (1977) described that the Indians, beginning with Aryabhata tried to solve the indeterminate equations in positive integers which was a stronger proposition as compared to Greeks. The mathematics of Aryabhatiya is mostly algorithmic without any proof but that does not necessarily mean that the author was ignorant about it. It was a matter of style of exposition as observed by Hayashi (2003). Keller (2006) recently wrote a literal translation of Bhaskara's commentary of Aryabhatiya with introduction.

Aryabhata presented a general solution of the linear indeterminate equations which may be adopted to find the multiplicative inverse in a group that is of interest in cryptology, signal processing, coding and computer design. Kak (2006) has nicely elaborated the computational aspect of Aryabhata algorithm which has recently generated interest among the cryptographic community. Rao and Yang (1986) have applied the algorithm to solve congruencies and have shown that the algorithm is better suited in some cases as compared to the CRT. The annual RSA conference in 2006 has chosen the topic on Aryabhata algorithm as one of its themes for discussion, see Kak (2006). The RSA algorithm was based on the factorization of a large number, which is stated as below:

Find a number, $x < d_1.d_2=n$, which when divided by d_1 and d_2 leaves the residues x_1 and x_2, where $x_1-x_2 = c$ and d_1 and d_2 are relatively prime!

The problem is stated in mathematical form, by Eqs (1-2) as below:

$$x \bmod d_1 = x_1, \qquad (1)$$
$$x \bmod d_2 = x_2 = c + x_1 \qquad (2)$$

Aryabhata's Method

Aryabhata discussed the solution of the problem in the following verses-32-33 of his book-Aryabhatiya (section- Ganita), as follows:

अधिकाग्रभागहारम च्छिन्द्यादूनाग्रभागहारेण,।
शेषपरस्परभक्तम मतिगुणमग्रान्तरेछिप्तम्.।।
अधउपरिगुणितमन्त्ययुगूनाग्रच्छेद भाजितेशेषम्। ,
अधिकाग्रच्छेदगुणम द्विच्छेदाग्रमधिकाग्रयुतम्.।।.

The English transliteration of these verses is given by Shukla (1976) as follows:

adhikāgrabhāghāram chindyāt ūnāgrabhāgahārena ।
śeṣaparasparasparabhaktam matigunam agrāntare ksiptam ।।
adhauparigunitam antyayuk nāgracchedabhajite śesṣam ।
a dhikāgracchedagunam dvicchdāgram adhikāgrayutam ।।

A valuable contribution of Prof. Walter Eugen Clark in deciphering the ancient Indian work on Mathematics and Astronomy is presented in the English translation with notes on the Aryabhatiya of Aryabhata, see Clark (1930). Further Ayangar (1926) elaborated the mathematics of Aryabhata; a translation of these two verses by him is quoted as below:

> *"Divide the divisor corresponding to the greater remainder (*अधिकाग्र *) by the divisor corresponding to smaller remainder by the other divisor and continue the process with the remainders. Write out the successive quotients in a vertical line, one underneath the other. Chose a suitable integer (called* मति*) which when multiplied by the final remainder and added to the difference between the given residues may yield an integral quotient and beneath it place the aforesaid integral quotient. Multiply the lower by the upper and add the last and continue this process till the operations cannot be further pursued. Divide (if possible) the figure thus obtained by the first divisor and multiply the remainder by the second*

(divisor). The product added to the corresponding residue is the required result".

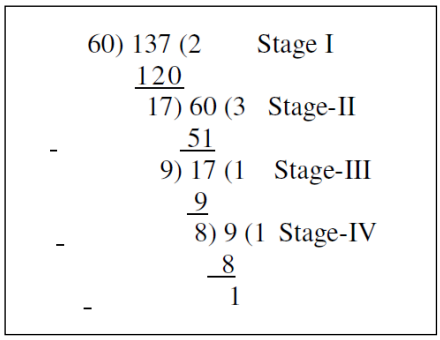
The rational and the genesis of the method can be illustrated by an example as below: Find a number, P which when divided by 60 gives a remainder1 while by 137 gives a remainder 11!

The problem reduces to finding an integer solution of the indeterminate equation,

$$137x+10=60y \quad (3)$$

The method that immediately suggests itself is to express x of Eq. (3) in terms of y, i.e., x= (60 y-10)/137. Since (60y-10)/137 should be an integer, put t = (60y-10)/137, so that y=2t + (17t+10)/60.Again (17t+10)/60 should be an integer, let it be expressed as s = (17t+10)/60, so that t = 3s + (9s -10)/17. Further by putting an integer R= (9s-10)/17, we have, s= R+ (8R+10)/9 and if we set R = 1, the term (8R+10) is readily divisible by 9. Thus the assumed number R is 1.

As above the divisor137 gives a greater remainder 11 as compared to the divisor 60, we divide 137 by 60 and proceed as below:



The process of division can be stopped at stage-III with the chosen number R=1. Aryabhata's algorithm is therefore nothing more than a method of detached coefficients for carrying out the backward process of evaluating successively x, y and P. The successive column of reduction of the Aryabhata's array is given in Table 1 as follows:

Table 1: Aryabhata's Array

2	10×2+3=23=y
3	3×3+1=10=x
1	1×1+2=3
1	1
2	

This gives a solution, x=10, y=23 and P=137*10+11=1381. If the process of the division is continued further to the stage IV, the chosen number, R is determined as

$$1*R-10=8 \rightarrow R=18.$$

The extended Aryabhata's array is given in Table 2 as below:

Table 2: Extended Aryabhata's Array

2	130×2+37=297=a
3	3×37+19=130=b
1	1×19+18=37
1	1×18+1= 19
18	18
1	

Noting that 297 mod 137=23 and 130 mod 60=10, we get a=10 and b=23 as simple solution of the indeterminate equation, The required number x= 137×10+11= 60×23+1=1381 and the number is doubly divided (द्विच्छेदाग्र in the terminology of Aryabhata) by the modulus d_1, d_2 where d_1=60 and d_2 =137, see Ayangar (1926).

It may also be noted that the remainder 10 was added at the stage III while it is subtracted at the stage IV, i.e. the remainder is subtracted at the even stage and added at the odd stage, a rule provided by the latter mathematicians (Bhaskaracharya I (AD 600-680),

Brahmagupta (AD 597-680) and Paramesvara (AD 1370-1460)) after Aryabhata while writing commentary on the Aryabhatiya, see Datta and Singh (1962) as

समेषु क्षिप्तं विषमेषु सोध्यम
(Sameshu kshiptam vishameshu sodhyam)

Bag (1977) also discussed the solution of indeterminate equation proposed by Aryabhata in terms of continued fraction.

Bhaskaracharya I, (hereafter is referred as Bhaskara) extended the method of Aryabhata and he suggested that it was not necessary to find a multiplier and a quotient as was done in Aryabhata**'**s method. The constant in the equation and 0 should be added to the table, instead. Bhaskara algorithm can be put as follows:

Table 3: Bhaskara's Array

137=60*2+17	2
60=17*3+9	3
17=9*1+8	1
9=8*1+1	1
modulus	Q

Step for formation of Table 4 is as follows:

(I) The number of rows of the table is the number of quotient +2.
(II) Column 1 of Rows 6, 5, 4, 3 will contain the column Q of the above table,
(III) Column 1 of Row 2 will contain the constant (=10) and that of Row 1 will contain 0.
(IV) The algorithm is as followed,
(V) Set (R1, C2) = 0, (R2, C2) = 10
(VI) (R3, C2) = (R2, C2)*(R3, C1)+ (R1, C2),
(R3, C2) = 10*1+0 =10;
(VII) (R4, C2) = (R3, C2)*(R4, C1) + (R2, C2)
(R4, C2) = 10*1+10=20;
(VIII) (R5, C2) = (R4, C2)*(R5, C1) + (R3, C2),
(R5, C2) = 20*3 + 10 = 70
(IX) (R6, C2) = (R5, C2)*(R6, C1) + (R4, C2)
(R6, C2) = 70*2 +20 =160

The above results can be generalized as

(Rn, C2) = (Rn-1, C2)* (Rn, C1) + (Rn-2, C2)

The above result can be expressed in Table 4 as

Table 4: Bhaskara's solution procedure

R6	2	160
R5	3	70
R4	1	20
R3	1	10
R2	10	10
R1	0	0
	C1	C2

Thus the solution is

$$x=70 \text{ and } y=160$$

The Panchsiddhantika by Varahmihir occupies an important position in Indian astronomical literature. It developed important innovations in planetary computations by using simplifying hypothesis. For example, an algorithm of calculating solar mean latitude is presented in eighth chapter of the book as follows:

> *"Multiply the ahargana* (total number of days in an epoch) *by 150, deduct 65 and divide by 54787, the fractional part of the dividend represents the mean latitude of the sun".*

Sudhakar Dvivedi (see Thibaut and Dvivedi (1899)) in his Sanskrit commentary of Panchsiddhantika presented the above algorithm in an indeterminate equation,

$$150\,x + 65 = 54787y \quad (4)$$

He divided the Eq. (4) throughout by 65 and employed the kuttaka for the solution of the reduced equation as $\begin{Bmatrix} 73 \\ 2663 \end{Bmatrix}$, which on multiplication by 65 yields the exact solution. He also considered the simultaneous indeterminate equation for planetary computations.

Simultaneous Indeterminate Equations

Brahmagupta considered simultaneous linear indeterminate equations. In a

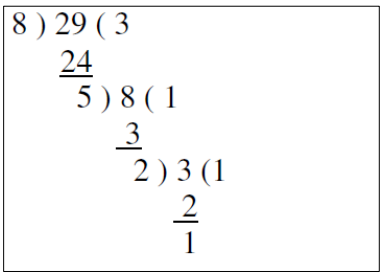
commentary on Aryabhatiya, see Clark (1930), Parmesvara considered the following example

$$8x \bmod 29 = 4;\ 17x \bmod 45 = 7,$$

The problem is equivalent of finding a solution of the simultaneous linear indeterminate equations,

$$8x-29y,\ 17x-45z= 7, \quad (5)$$

The integers y and z are the quotients of the division. Following the procedure described by Aryabhata's algorithm,



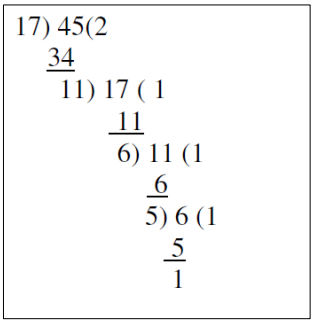
The chosen number is considered such that when multiplied by *1 (*last remainder of the reciprocal division) and added/ subtracted by 4 will be exactly divisible by 2.The assumed number is taken to be 6 because (6- 4) /2=1. Hence the Aryabhata's array (Table 5) becomes

Table 5: 73 mod 29 = 15 Aryabhata's array (Paramesvara)

3		73
1		20
1		13
1	7	
6	6	
1		

The remainder 15 is the agra value, a solution of x satisfying the equation.

Similarly proceeding for the second equation,



Assuming another number such that when multiplied by 1(last remainder of the reciprocal division) and added / substracted by 7 will be exactly divisible by 5. The number is assumed to be 3 because *(3 +7)/ 5= 2.* Hence the Aryabhata's array becomes

Table 6: Aryabhata's array (Parmesvara)

2						34
1					13	
1				8		
1			5			
3		3				
2						

Here 45 mod 34 = 11, a value of x satisfying the equation. The numbers 15 and 11 are the agras described in the beginning of the rule. The corresponding divisors are 29 and 4 and the difference between the agras (remainders) is *15 – 11 =4*. To find a value of *x* satisfying both the equations,

```
29) 45 (1
     29
      16) 29 (1
          16
          13) 16 (1
              13
                3) 13 (4
                   12
                    1
```

Chose another number such that when multiplied by 1 (last remainder of the reciprocal division) and added/ subtracted by 4 will be exactly divisible by 3.The assumed number is taken to be 2 because (3+ 4) /3=2. Hence the Aryabhata's array becomes,

Table 7: Aryabhata's final arrays (Parmesvara)

1					34
1					
				22	
1			12		
4		10			
2	2				
2					

Thus the remainder is 34 mod 45 = 34 and the smallest number is 34 x 29+15=1001satisfying both the equations.

Chinese Remainder Theorem

According to CRT, given a set of simultaneous congruencies for i= 1, 2**…** r;

$$X= a_i(\text{mod } m_i)$$

and for which there exists a relatively prime, m_i the solution of congruencies is as follows:

$$X = a_1 b_1 (M/m_1) + a_2 b_2 (M/m_2 + \ldots\ldots + ar\, br\, (M/mr)\, (\text{mod } M), \qquad (6)$$

where, M= m1.m_2.m_3**…..**m r and bi (M/m_i) =1 mod (mi).

For the solution of Eq. (6) one follows CRT. In CRT, one computes a modular arithmetic with a large number to adjust the final result which is time computing operation. On the contrary, in the Aryabhata**'s** arrays, one divides the large time computing operations into several modular arithmetic with smaller number in each of the iterations. Thus the Aryabhata**'s** Remainder theorem is more suitable than CRT, see Hang and Yang (2009).The simplicity of Aryabhata**'s** method of solving the indeterminate equations is of paramount importance. The historians of mathematics have already recognized his brilliance and the cryptology communities are reassessing the method, in particular the factorization of large numbers for the development of RSA algorithm.

Conclusion

Aryabhata was a great Indian mathematician and Astronomer of the ancient world whose contribution in solving indeterminate equations had enormous influence around the globe. The simplicity of kuttaka method lies in the fact that it divides the large time computing operations into several modular arithmetic with smaller number in each of the iterations which may be utilized by the computer scientists in developing crypto algorithm.

References

AYANGAR, A.A. K, 1926, The Mathematics of Aryabhata, Quarterly Journal of Mythic Society, Vol.16, pp 158-179.

BAG, A. K., 1977, The method of Integral Solution of Indeterminate Equations of the type by=ax +/- c in Ancient Medieval India, Indian Journal of History of Science, Vol.12, pp. 1-16.

CLARK, W. E., 1930, The Aryabhatiya of Aryabhata : Translation with notes, The University of Chicago Press, Chicago, Illinois.

DATTA, B. and Singh, A. N. ,1962, History of Hindu Mathematics, a source book, Parts 1 and 2, Asia Publishing House, Bombay.

Elements of Euclid (Translation and commentaries by Heath, Thomas, L.), Dover Publications, 1956.

HANG, Chin-Chen and YANG, Jen –Ho, 2009, A parallel algorithm base don Aryabhatta remainder Theorem for Residue number System, International Journal of Innovative Computing, Information and Control, Vol. 5(7), pp. 2053 - 2060.

HAYASHI, T, 2003, Indian Mathematics in "Companion Encyclopedia of the History and Philosophy of Mathematical Sciences, Vol. 1, pp.118-130" by Grattem Guinnes, Ivor, Baltimore, MD, The John Hopkins University Press, ISBN0 :8018-7396-7.

KAK, S., 1986, Computational Aspects of Aryabhata Algorithm, Indian Journal of History of Sciences, 21 (1), pp. 62-71.

KAK, S. *Aryabhata's Mathematics*, RSA Conference, San Jose, Feb. 2006, pp.13-17.
KELLER, Agathe. *Expounding the Mathematical Seeds*, Vol.1: A Translation of Bhaskara I on the Mathematical Chapter of Aryabhatiya, Birkhauser, 2006. ISBN:3764372915
LEHMER, D. N. *The general solution of the indeterminate equation Ax + By + Cz +...= r*, Proceedings of the National Academy of Sciences-PNAS, 1919. Vol (4), pp 111-114.
RAO, T. R. N. and Yang, C.H. *Aryabhata Remainder Theorem: Relevance to Crypto algorithms, Circuits, System and Signal Processing*, 2006. Vol. 25, Pp.1-15.
SHUKLA, K. S. *Aryabhata: Aryabhatiya with commentary of Bhaskara I and Someavara*, Critically edited with Introduction and Appendices by Kripa Shankar Shukla, Indian National Science Academy, 1976. (E-Text by Danielle Feller, 2001)
THIBAUT, G. and Dvivedi Sudhakar, *The Panchasiddhantika of Varahmihir*,The Medical Hall Press, Banaras, 1899.
URICH, Librect, *Chinese Mathematics in the Thirteenth Century*, Dover, 1973. www.math.harvard.edu/knill/crt/lib/librecht14.pdf
VOLODARSKY, , *Mathematical Achievements of Aryabhata*, Indian Journal of History of Sciences, 1977, Vol.12 (2) pp. 167-72.

Kedar N Shukla
PRERANA CGHS Ltd., Sector-56, Gurgaon-122011 - India

E-mail: kn_shukla@rediffmail.com