Indian Journal of History of Science, **21**(1): 62—71 (1986)

COMPUTATIONAL ASPECTS OF THE ĀRYABHAṬA ALGORITHM

SUBHASH KAK

Department of Electrical and Computer Engineering
Louisiana State University
Baton Rouge, LA 70803

(Received 30 March 1985)

This paper investigates the Āryabhaṭa algorithm from the point of view of computational complexity. It is also shown that this algorithm is as efficient as the popularly used Chinese Remainder algorithm in solving a system of congruences.

INTRODUCTION

The solution to the problem of a system of congruences where the moduli are pairwise prime is normally obtained by the Chinese Remainder (CR) algorithm. This algorithm is of particular interest to computer and communication scientists because systems of congruences arise frequently in coding, cryptography, signal processing, and in computer design. The significance of an alternate efficient algorithm cannot be overstated especially since one may obtain an elegant implementation structure even if the complexity remained unchanged. An algorithm to solve congruences in a manner different to the CR method is presented in *Āryabhaṭīya*. Recently I have brought this method to the attention of computer scientists.[1] I believe the reason this algorithm has not been described earlier in computer literature is because history books often state it only in the context of the solution of the linear indeterminate equation $ax—by =c$ for x, y in positive integers, where a, b, c are given integers.

In *Āryabhaṭīya*, this method is called *kuṭṭaka* (the pulverizer). Even though I have sometimes called it the Āryabhaṭa algorithm, to conform to the convention of associating a person with a result, the traditional name is very appropriate. Considering that Āryabhaṭa's system was a modification of the earlier *Paitāmaha Siddhānta* it is likely that this method, like other results in his book, was already well known before him. Commentaries on this method were given by Bhāskara I (522 A.D.), Brahmagupta (628 A.D.), Mahāvīra (850 A.D.), Bhāskara II (1150 A.D.) and others.[2] This algorithm for the solution of a linear indeterminate equation appears to be the earliest recorded anywhere. Diophantos of Alexandria (250 A.D.) had described determinate and indeterminate problems but provided no methods of solutions; furthermore, he was only concerned with rational solutions.

The Algorithm

The Āryabhaṭa problem, in its simplest form, is: Find a number x less than $d_1 d_2 = n$ which, when divided by d_1 and d_2, leaves the residues x_1 and x_2, respectively, where $x_2 - x_1 = c$, and d_1 and d_2 are relatively prime. In other words, find x so that

$$x \bmod d_1 \equiv x_1 \qquad \text{(1a)}$$

$$x \bmod d_2 \equiv x_2 = c + x_1 \qquad \text{(1b)}$$

The pulverizer to solve this problem is given in A2. 32-33. There are several difficulties in translating these stanzas described in the literature.[3] One uses the commentary and the methods of the later mathematicians to help in the translation. The following is the translation by Clark based on Parameśvara's interpretation and of Brahmagupta's pulverizer :

> A2.32-33. Divide the divisor which gives the greatest *agra* (*agra:* remainder[4]) by the divisor which gives the smaller *agra*. The remainder is reciprocally divided (that is to say, the remainder becomes the divisor of the original divisor, and the remainder of this second division becomes the divisor of the second divisor, etc.). (The quotients are placed below each other in the so-called chain.) (The last remainder) is multiplied by an assumed number and added to the difference between the *agras*. Multiply the penultimate number by the number above it and add the number which is below it. (Continue this process to the top of the chain). Divide (the top number) by the divisor which gives the smaller *agra*. Multiply the remainder by the divisor which gives the greater *agra*. Add this product to the greater *agra*. The result is the number which will satisfy both divisors and both *agras*.

Clark quotes another translation by Ganguly that leads to a method differing somewhat in detail. Since our objective is to emphasize the essential method we express it in the following modern form :

Theorem : Let $d_2 > d_1$ and let

$$d_2 = a \; d_1 + r_1 \qquad , r_1 < d_1$$

$$d_1 = a_1 r_1 + r_2$$

$$r_1 = a_2 r_2 + r_3$$

$$r_k = a_{k+1} r_{k+1} + r_{k+2} \qquad \text{(2)}$$

and $r_{k+2} = 1$, then write the a's in a column, appending $c = x_2 - x_1$, and reduce this as shown :

$$
\begin{array}{cccccccc}
a & a & a & \cdot & \cdot & \cdot & \cdot & a' \\
a_1 & a_1 & a_1 & \cdot & \cdot & \cdot & \cdot & b' \\
a_2 & a_2 & a_2 & \cdot & \cdot & \cdot & \cdot & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
\cdot & \cdot & a_{k-1} & \cdot & \cdot & & & \\
\cdot & a_k & a_k a_{k+1}\, c + c & \cdot & & & & \\
a_{k+1} & a_{k+1}\, c & a_{k+1}\, c & & & & & \\
c & c & & & & & & \\
0 & & & & & & &
\end{array}
\qquad (3)
$$

where to obtain column $i+1$, we drop the last entry of column i, and replace the last but two entry by its product with the last but one entry, plus the entry being dropped.

Let $\quad (-1)^k \cdot a' \bmod d_2 \equiv a$, and

$$(-1)^k \cdot b' \bmod d_1 \equiv b, \qquad .. \qquad (4)$$

then

$$x = ad_1 + x_1$$
$$= bd_2 + x_2 \qquad .. \qquad (5)$$

This x is the least positive solution; other solutions will be $x +$ constant [l.c.m. (d_1, d_2)].

Proof : The proof of the theorem is elementary and it is stated in Datta and Singh.[5] We provide the outline of this proof below.

The operations in (2) represent division of d_2 by d_1, d_1 by the remainder in the previous step, and so on in sequence. The a's are the quotients obtained in this process. Since (1) can be rewritten as $x = ad_1 + x_1 = bd_2 + x_2$, therefore, the problem is transformed to the solution in terms of a and b of

$$ad_1 - bd_2 = c.$$

Use of the equations of (2) repeatedly in this equation until the last r_1, which is 1, sets up a sequence of equations where working backwards amounts to a reduction of the column of a's and c into the values a', b' which yield a, b.

Comment 1 *:* It should be noted that the Āryabhaṭa algorithm provides the solution to the class of problems defined by $x_2 - x_1 = c$, which is more general than the Chinese Remainder problem described first in *Sun Tzu Suan Ching* (Master Sun's Arithmetical

Manual) which, according to Needham,[6] was written between 280 A.D. and 473 A.D. The problem reads :

> We have a number of things, but do not know exactly how many. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?

Sun Tzu determined the 'use numbers' 70, 21 and 15, these are multiples of 5×7, 3×7 and 3×5, and have the remainder 1 when divided by 3, 5 and 7, respectively. The sum $2\times70+3\times21+2\times15=233$ is one answer, and by casting out a multiple of $3\times5\times7$ $(=105)$ as many times as possible (in this case, twice) the least answer, 23, is obtained. In the eighth century A.D. I-Hsing used the method for solving calendar problems, and in the thirteenth century A.D. Chhin Chiu-Shao gave a full explanation.

Sun Tzu's problem also occurs in identical words as Problem 5 of the 'supplementary problems' printed by Hoche in his edition of the 'Introduction to Arithmetic' of Nikomachos of Gerasa. According to Needham this problem occurs in only two or three of the nearly fifty extant manuscripts of Nikomachos. Three of the five 'supplementary problems' are ascribed to the monk Isaac Argyros (14th century A.D.), so it seems reasonable to assume that Problem 5 was also added by Argyros or his contemporaries.[7]

The stanza (A2. 31) immediately preceeding the pulverizer presumably represents the motivation for the method. It deals with an astronomical problem:

> 2:31. The two distances between two planets moving in opposite directions is divided by the sum of their daily motions. The two distances between two planets moving in the same direction is divided by the difference of their daily motions. The two results (in each case) will give the time of meeting of the two in the past and in the future.[8]
>
> This represents a concern different to that of Sun Tzu.

Brahmagupta in his *Siddhānta* describes a similar problem: "What number, divided by 6 has a remainder of 5, and by 5 a remainder of 4, and by 4 a remainder of 3, and by 3 a remainder of 2?" Brahmagupta and Bhāskara II showed how Āryabhaṭa's general method to solve linear indeterminate equations could be used to solve the problem. As mentioned before, Āryabhaṭa's algorithm can solve problems more general than the Chinese Remainder problem.

We note that Āryabhaṭa example is very different from that of Sun Tzu or Nikomachos. The main motivation to consider such problems in India was the cyclic cosmological system related to the Sāṅkhya School (700 B.C.). It appears, therefore, that the Indian tradition of solving congruence problems was independent of the Chinese and was perhaps older.

The recent demonstration[9] that the quotients can be combined in the forward direction (in contrast to the backward direction as described above) resulting in a faster procedure raises the question if Āryabhaṭa's stanzas admit the new interpretation. This question deserves a thorough investigation.

Some examples of the application of the algorithm are now described.

Example 1 : Solve for x when :

$x \bmod 63 \equiv x_1$
$x \bmod 100 \equiv x_2$,
and $x_2 - x_1 = 70$.

Solution :

```
63)100(1
   63
   --
   37) 63(1
       37
       --
       26)37(1
          26
          --
          11) 26(2
              22
              --
               4)11(2
                  8
                  -
                  3) 4(1
                     3
                     -
                     1
```

The sequence of quotients is 1, 1, 1, 2, 2, 1. We can now apply the Āryabhaṭa algorithm.

1	1	1	1	1	1	1890
1	1	1	1	1	1190	1190
1	1	1	1	700	700	
2	2	2	490	490		
2	2	210	210			
1	70	70				
70	70					
0						

Thus $a' = 1890$, $b' = 1190$

Now using (4) :

$$a = 1890 \bmod 100 = 90$$
$$b = 1190 \bmod 63 = 56.$$

Therefore,

$$x = 90.63 + x_1$$
$$= 56.100 + x_2.$$

Let $x_1 = 2$, $x_2 = 72$, then

$$x = 5672.$$

Example 2 : Solve for x when :

$$x \bmod 26 = 18$$
$$x \bmod 37 = 11$$

Solution : The sequence of quotients is 1, 2, 2, 1. The value of c is 11—18 = —7. We form the table (3) :

1	1	1	1	—70
2	2	2	—49	—49
2	2	—21	—21	
1	—7	—7		
—7	—7			
0				

Therefore,

$$a = -70 \bmod 37 = 4$$
$$b = -49 \bmod 26 = 3,$$

and

$$x = 4.26 + 18$$
$$= 3.37 + 11 = 122.$$

There is no need to introduce negative numbers in this example if one changed the order of the congruences; we have done so to show that the algorithm works irrespective of the sign of numbers.

Āryabhaṭa's algorithm was generally used to solve problems in astronomy. The following problem by Brahmagupta (born 598 A.D.) which appears in his *Brahma-sphuṭa-siddhānta* (628 A.D.) (The Revised System of Brahma) is an example:

Suppose that viewed from the earth the sun, moon, etc. have travelled for the following number of days after completing full revolutions since the beginning of the *Kalpa* (when the sun and the planets were collinear):

Sun	Moon	Mars	Mercury	Jupiter	Saturn
1000	41	315	1000	1000	1000

Given that the sun completes 3 revolutions in 1096 days, the moon 5 revolutions in 137 days, Mars 1 in 685 days, Mercury 13 in 1096 days, Jupiter 3 in 10960 days, Saturn 1 in 10960 days, find the number of days elapsed since the beginning of the *Kalpa*.

The solution to this problem can be easily seen to be 11960.

Comment 2: It can be easily established that in algorithm (3), the multiplication by c can be made at the very end in the last column. This reduces the computational effort considerably. We describe the modified Āryabhaṭa's algorithm:

Step 1 : Replace c by 1 in column 1 in (3).
Step 2 : Compute a' and b' by algorithm (3).
Step 3 : Replace a' and b' by ca' and cb' in (4). Compute x as in (5). .. (6)

Comment 3 : Āryabhaṭa's algorithm can be used repeatedly to solve for more than two congruences. Thus if one has three congruences A, B, C where the moduli are pairwise prime, solve A and B first and then use this solution with C to get the final answer.

Moduli not relatively prime

Āryabhaṭa's algorithm can solve simultaneous congruences with nonrelatively prime moduli (where a solution exists) if one can reduce the congruences to a linear indeterminate equation, where the common factors of the moduli can be divided out.

Example : Consider Brahmagupta's problem:

$x \equiv 5 \bmod 6$
$x \equiv 4 \bmod 5$
$x \equiv 3 \bmod 4$
$x \equiv 2 \bmod 3,$

where we want to solve for smallest x.

Solution : The moduli of the first and the second pair are relatively prime. Applying the Āryabhaṭa algorithm :

$x \equiv 29 \bmod 30$
$x \equiv 11 \bmod 12.$

We convert this into a linear indeterminate equation by :

$$x = 30a + 29 = 12b + 11$$
$$\text{or } 12b - 30a = 18,$$

which reduces to :

$$2b - 5a = 3.$$

Using Āryabhaṭa's algorithm, the least positive solution is :

$$x = 59.$$

Complexity of the Algorithm

We count the number of multiplication, division and addition operations in the Āryabhaṭa algorithm and compare that with those in the standard Chinese Remainder (CR) algorithm.

Āryabhaṭa Algorithm

Let N be the order of the moduli d_1 and d_2. Step (2) requires roughly $\log_2 N$ divisions. Step (3) requires about $\log_2 N$ multiplications and the same number of additions. Step (4) requires 2 divisions, while step (5) requires 1 division and 1 multiplication. This adds up to approximately

$$\begin{aligned}&3 + \log_2 N \text{ divisions}\\ &1 + \log_2 N \text{ multiplications, and}\\ &1 + \log_2 N \text{ additions.}\end{aligned} \qquad \ldots (7)$$

CR Algorithm

In this algorithm we first compute y_1, such that $d_2 y_1 \bmod d_1 = 1$, and $d_1 y_2 \bmod d_2 = 1$. Then

$$x = d_2 y_1 x_1 + d_1 y_2 x_2 \bmod d_1 d_2 = n. \qquad \ldots (8)$$

If $\phi(d_1)$ and $\phi(d_2)$ are known then y_1 and y_2 can be obtained in about $\log_2 \phi(d_1) \phi(d_2) \approx \log_2 N$ multiplications and divisions (where the size N is taken to be the same as n), by using Euler's generalization of Fermat's theorem. This complexity is of the same order as in Āryabhaṭa's algorithm.

If $\phi(d_1)$ are not known, one can use an extension of Euclid's algorithm for computing the greatest common divisor. The number of operations performed in this algorithm is roughly $2 \log_2 d_1$ multiplications, $\log_2 d_1$ divisions and $\log_2 d_1$ additions (see Knuth or Denning for details). The total number of operations, considering that we must obtain y_1 and y_2 and compute (8), is therefore

$$\begin{aligned}&1 + \log_2 N \text{ divisions}\\ &4 + 2\log_2 N \text{ multiplications, and}\\ &1 + \log_2 N \text{ additions.}\end{aligned} \qquad \ldots (9)$$

We conclude that the Āryabhaṭa and the CR algorithms have about the same complexity.

It appears that algorithmic ideas have pervaded Indian mathematics since the earliest times. The *śulvasūtra* rules on altar construction amount to arithmetic and algebraic procedures. The logic behind these procedures must have been well understood which would explain why irrational numbers resulting from the use of these procedures were readily accepted.[10] Some of the constructions require solution to simultaneous equations. The *Meru Prastara* is a procedure to find combinations that was described by Pingala in 200 B.C.[11] Algebra that appears in *Āryabhaṭiya* can be seen to be an extension of the algebra of the *śulvasūtras*.

Concluding Remarks

In the late nineteenth century considerable attention was given to the contributions of the ancient Indian mathematicians. That was the age when classical mathematics itself was being formalized, and historians found the Indian sources, in contrast to the greatest concern of the mathematics of the day, lacking in formalization and proof. Ancient Indian mathematics emphasized algorithms and computational techniques, which are constructive procedures. The nineteenth century historians did not consider computational issues and, therefore, many results derived using novel procedures were forgotten as mathematical curiosities.

The motivation for the development of clever algorithms by the ancient Indians was presumably the urge to algorithmize knowledge in the spirit of Pāṇinī. A corroboration of this hypothesis is provided by the recent work of C.-O. Selenius[12] who has shown that *chakravala* method of Jayadeva and Bhāksara II for solving the indeterminate equation of the multiplied square

$$x^2 - Dy^2 = 1 \qquad \text{.. (10)}$$

lead to a minimum number of steps; in other words, the *chakravala* method is an optimum algorithm. Selenius notes that "the method represents a best *approximation algorithm of minimal length* that, owing to *several minimization properties, with minimal effort* ("economization") and *avoiding large numbers,* always *automatically* (without trial processes) *produces the least solutions* to the equation, and thereby *the whole set of solutions*... It is accepted that the *chakravala* method here explained anticipated the European methods by more than a thousand years. But, as we have seen, no European performances in the whole field of algebra at a time much later than Bhâskara's, nay nearly up to our times, equalled the marvellous complexity and ingenuity of chakravala".

This shows that the efficiency of *kuṭṭaka* is no accident, and there must have been a deliberate search for powerful computing methods.

References and Notes

[1]Kak, S., The Aryabhata Algorithm, *Tech. Report*, L.S.U., 1985.

[2]Kak, S., Norton, D. and El-Amawy, A., An Efficient Implementation of the Aryabhata Algorithm, *20th Annual Conference on Information Sciences and Systems*, Princeton, N. J., March 1986.

[3]*See* Clark, W. E., *The Aryabhatiya of Aryabhata*, University of Chicago Press, Chicago, 1930; Srinivasiengar, C. N., *The History of Ancient Indian Mathematics*, The World Press, Calcutta, 1967; Shukla, K. S. and Sarma, K. V., *The Āryabhaṭiya of Āryabhaṭa*, Indian National Science Academy, New Delhi, 1976.

[4]"Agra denotes the remainders which constitute the provisional value of x, that is to say, values one of which will satisfy one condition, one of which will satisfy the second condition of the problem" (Clark, 1930).

[5]Datta, B. and Singh, A. N., *Source Book of Hindu Mathematics*, Asia Publishing House, Bombay, 1935.

[6]Needham, J., *Science and Civilization in China*, Vol. III, Cambridge University Press, Cambridge, 1959.

[7]———, *ibid.*

[8]Ref. 3, p. 41.

[9]*see* Ref. 2.

[10]This is in contrast to Greece where their discovery led to a crisis. For an exposition of several issues related to irrational numbers in Geometry *see* Sarasvati Amma, T. A., *Geometry in Ancient and Medieval India*, Motilal Banarasidas, Delhi, 1979.

[11]Also known as Pascal's triangle after Blaise Pascal (1623-1662).

[12]Selenius, C.-O., Rationale of the Chakravala Process of Jayadeva and Bhaskara II, *Historia Mathematica*, 2, 167-184, 1975; Selenius has also shown how Lagrange (1736-1813) is wrongly credited with a rediscovery of the chakravala method. The first correct interpretation of the chakravala method was presented by Selenius himself in 1959.