Indian Journal of History of Science, 19 (4) : 397—405 (1984)

KUṬṬAKA AND QIUYISHU

A. K. BAG
Indian National Science Academy, India
AND
K. S. SHEN
Hangzhou University, China

1. *Kuṭṭaka* IN INDIA

The solution of the equation

$$by-ax=c \qquad (*)$$

for x, y in positive integers, where a, b, c are given integers, $a>b$, $(a, b)=1$ is called in Indian mathematics as *kuṭṭaka*. *Kuṭṭaka* literally means pulverizer, and the name has been given on account of the process of continued division that is adopted for the solutions. It is said that the problem arose to Ārya Bhaṭa[1] (*c.* 476 A.D.) to determine an integer N which when divided by a leaves remainder r_1 and by b leaves remainder r_2, then

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

Ārya Bhaṭa discovered the Rule for the solution, but he has given his method in just two stanzas of his *Ārya Bhaṭīyam* in a language which is very difficult to interpret. In modern symbology, according to B. Datta, the solution can be expressed as follows:[2]

By continued division (Euclidean algorithm), a series of quotients and corresponding remainders are

$$q_1, q_2, \ldots, q_m; r_1, r_2, \ldots, r_m.$$

the relationships between them are:

$$a=bq_1+r_1$$
$$b=r_1q_2+r_2$$
$$r_1=r_2q_3+r_3$$
$$\ldots\ldots\ldots\ldots$$
$$r_{m-2}=r_{m-2}q_m+r_m$$

from which there are series of the following reduction formulas:

(1) $y = q_1 x + y_1$, where (1.1) $by_1 = r_1 x + c$;
(2) $x = q_2 y_1 + x_1$, where (2.1) $r_1 x_1 = r_2 y_1 - c$;
(3) $y_1 = q_3 x_1 + y_2$, where (3.3) $r_2 y_2 = r_3 x_1 + c$;
(4) $x_1 = q_4 y_2 + x_2$, where (4.1) $r_3 x_2 = r_4 y_2 - c$;

..., ..., ...,

$(2n-2)$ $x_{n-2} = q_{2n-2} y_{n-1} + x_{n-1}$,

where,
$(2n-2.1)$ $r_{2n-3} - x_{n-1} = r_{2n-2} y_{n-1} - c$;
$(2n-1)$ $y_{n-1} = q_{2n-1} x_{n-1} + y_n$,

where,
$(2n-1.1)$ $r_{2n-2} y_n = r_{2n-1} x_{n-1} + c$;
$(2n)$ $x_{n-1} = q_{2n} y_n + x_n$,

where,
$(2n \cdot 1)$ $r_{2n-1} x_n = r_{2n} y_n - c$.

In considering two cases we have:[3,4]

Case 1: $m = 2n-1$

$y_{n-1} = q_{2n-1} x_{n-1} + y_n$

$r_{2n-2} y_n = r_{2n-1} x_{n-1} + c$, since $(2n-1)$, $(2n-1.1)$

select $x_{n-1} = t$, so that $y_n = (r_{2n-1} t + c)/r_{2n-2}$

is an integer q, and then from the bottom to the top by reduction formulas and finally obtain the required x and y.

Case 2: $m = 2n$

$x_{n-1} = q_{2n} y_n + x_n$

$r_{2n-1} x_n = r_{2n} y_n - c$, since $(2n)$, $(2n.1)$

select $y_n = t'$, so that $x_n = (r_{2n} t' - c)/r_{2n-1}$

is an integer q', and then from bottom to top by using these reduction formulas to find out x and y.

In chapter 4, *Gaṇita Sāra Saṃgraha* (850) by Mahavira[5], he had a new idea:

(1) to omit q_1, when x is solved, y may be sought by substitute x in equation (*).
(2) Continued division is proceeded up to $r_m = 1$,

2. QIUYISHU* IN CHINA

Problem 26, volume 3, *Mathematical classic of Sun Zi*.**[6]
"There are certain things whose number is unknown. Repeatedly divided by 3 leaves remainder 2, by 5 leaves remainder 3, and by 7 the remainder is 2. What will be the number?"

The answer is 23.

The problem may be expressed in the system of congruences of first degree:

$$x \equiv 2 \pmod 3 \equiv 3 \pmod 5\ 2 \equiv \pmod 7,$$

of which we should find out F_1, F_2, F_3 to satisfy the following independent congruences:

$$F_1 \times 7 \times 5 \equiv 1 \pmod 3$$
$$F_2 \times 3 \times 7 \equiv 1 \pmod 5$$
$$F_3 \times 5 \times 3 \equiv 1 \pmod 7,$$

by mental arithmetic, we get

$$F_1 = 2,\ F_2 = 1,\ F_3 = 1,$$

and

$$x_2 \equiv 2 \times 2 \times 7 \times 5 + 3 \times 1 \times 3 \times 7 + 2 \times 1 \times 5 \times 3$$
$$= 140 + 63 + 30 = 233 \equiv 23 \pmod{3 \times 5 \times 7}.$$

Sun Zi solved the problem somewhat as we do,[7,8] he said: "Divided by 3, the remainder is 2, and so take 140. Divided by 5, the remainder is 3, and so take 63. Divided by 7, the remainder is 2, and so take 30. Adding them together we get 233. Therefrom subtract 210, and we obtain the answer."

Moreover, added Sun Zi:
"In general, take 70, when the remainder of the repeated divisions by 3 is 1; take 21, when the remainder of the repeated divisions by 5 is 1; and take 15, when the remainder of the repeated divisions by 7 is 1. When the sum of these numbers is above 106, subtract 105, before we get the answer."

Although Sun Zi's problem is only a special numerical one, it has its general sense. If we find out F_1, F_2, F_3 to satisfy the congruences:

$$F_1 m_2 m_3 \equiv 1 \pmod{m_1}$$
$$F_2 m_1 m_3 \equiv 1 \pmod{m_2}$$
$$F_3 m_1 m_2 \equiv 1 \pmod{m_3}$$

*Qiuyishu, literally means 'To make the remainder unity'.
**Sun Zi, Chinese mathematician, *c.* 400 A.D.

and the solution of the system of congruences

$$x \equiv r_1 \pmod{m_1} \equiv r_2 \pmod{m_2} \equiv r_3 \pmod{m_3}$$
$$(m_i, m_j) = 1;\ i, j = 1, 2, 3,\ i \neq j.$$

is

$$x \equiv r_1 F_1 m\, m_3 + r_2 F_2 m_1 m_3 + r_3 F_3 m_1 m_2 \pmod{m_1 m_2 m_3}.$$

It may be further generalized in two cases:

(1) To grow the number of congruences,

(2) m_i, m_j may not be prime with each other.

In ancient China people did much in both of these two cases. However, all the cases finally would meet a common question how to solve

$$ax \equiv 1 \pmod{b},\ (a, b) = 1 \qquad (**)$$

Qin Jiushao himself is a good example. For, in the nine problems, volume 1, 2 of his book *Nine Chapters Mathematics* (1247)[9] he not only increased the number of congruences up to 8, and let the modulus not all relatively prime. Qin had summed up a rule—Qiuyishu to solve the congruence (**).

500 years have passed since Qin invented the splendid rule, it is indeed the rule was almost forgotten in China during these days. Zhang Dunren (1754—1834) was the first who understood the rule. He wrote *Arithmetic of Qiuyishu* (1803). Huang Zhongxian wrote *General Solution of Qiuyishu*[10] to improve Zhang's work. For solving (**), Huang set a in the left column, b in the right. Subtract mutually again and again until the remainder in the left column turns to unity. Regard the final Jishu*, the answer of (**). Huang made 3 rules for seeking Jishu.

(1) Jishu of a is 1, that of b is 0. After the first subtraction, we get the remainder, and consider Jishu of r_1 is identical to that of a, i.e. 1.

(2) Then b as the minuend, the remainder r_1 as the subtrahend to subtract secondly. Consider the number of subtractions q_2 as Jishu of the second remainder r_2.

(3) Then r_1 as minuend, r_2 as subtrahend to subtract thirdly. Denote q_3 as the number of subtractions. Jishu 1 of r_1 plus the product of q_3 by Jishu of r_2, i.e. $1+q_2q_3$ is Jishu of r.

The rest may be deduced by analogy up to $r_m=1$, where m is odd. Huang's words may be represented by Table A as follows:

*Jishu, literally means 'Deposit number'.

TABLE A

m	Jishu			Jishu	m
	1	a	b	0	
1	1	$\frac{-bq_1}{r_1}$	$\frac{-r_1q_2}{r_2}$	q_2	2
3	$\frac{+q_2q_3}{1+q_2q_3}$	$\frac{-r_2q_3}{r_3}$	$\frac{-r_3q_4}{r_4}$	$\frac{+q_4(1+q_2q_3)}{q_4(1+q_2q_3)+q_3}$	4
		$\frac{-r_4q_5}{r_5}$	:		
		:	:		
		:			
		$\frac{}{r_m=1}$			

no matter how $a<b$, or $a>b$.

Huang's programming is correct, for in his processes of mutual subtraction, all the remainders are the difference between the multiple a and that of b.

TABLE B

$r_1=a-q_1b$	J_1a-I_1b
$r_2=(1+q_1q_2)\,b-q_2a$	I_2b-J_2a
$r_3=(1+q_2q_3)\,a-(q_1+q_3\,(1+q_1q_2))\,b$	J_3a-I_3b
$r_4=(1+q_1q_2+q_4\,(q_1+q_3\,(1+q_1q_2))\,b$ $-(q_2+q_4\,(1+q_1q_2))\,a$	I_4b-J_4q
:	:
:	:
:	:

In the processes of mutual subtraction there is a proposition:

$$r_{2m-1}=J_{2m-1}a-I_{2m-1}b,$$
$$r_{2m}=I_{2m}b-J_{2m}a,$$

where, I_m is integer, and Jishu J_m as Huang had concluded:

$$J_m=q_mJ_{m-1}+J_{m-2},\ J_0=0,\ J_1=1.$$

$(m=2, 3, 4, \ldots)$

Proof. (1) $m=2$, the proposition is true.

(2) if $m=k$. then

$$\begin{aligned} r_{2k+1}&=r_{2k-1}-q_{2k+1}r_{2k}\\ &=J_{2k-1}a-I_{2k-1}b\ q_{2k+1}(I_{2k}b-J_{2k}a)\\ &=(q_{2k+1}J_{2k}+J_{2k-1})\,a-(I_{2k-1}+q_{2k+1}I_{2k})\,b\\ &=J_{2k+1}a-I_{2k+1}b. \end{aligned}$$

In like manner to prove

$$r_{2m}=I_{2m}b-J_{2m}a \quad \text{Q.E.D.}$$

Therefore, the so-called Jishu J_m is nothing but the multiplier of a in the minuend of the difference (where m is odd). When we control the final remainder $r_m=1$ of left column, m is odd of course, thus

$$r_m=1=aJ_m-\text{multiple of } b,$$
$$\text{i.e., } aJ_m\equiv 1 \pmod b$$

J_m is the solution of (**) certainly.

Huang's rules for seeking Jishu J_m are rather complicated literally, but is simple in numerical calculation, so that he had solved the relevant problems from Sun Zi, Qin Jiusho, to scholars in Qing Dynasty (1644—1911).[11] It has its practical significance for to-day. For instance, to solve

$$65x\equiv 1 \pmod{83}$$

by aid of Huang's programming the answer is obtained very easily.

J_m			J_m
1	65	83	0
+3	$-3\times 18=54$	−65	+1
4	11	18	1
+5	−7	−11	+4
9	4	7	5
+14	−3	−4	+9
23	1	3	14

the answer is 23.

3. Parallelism between Kuttaka and Dayan Qiuyishu

It is evident that the meanings of solving indeterminate equation (*) and the congruence (**) are unanimous. It is glaring that the sources of indeterminate analysis all occurred in division with remainders both in India and in China. Furthermore, *Kuṭṭaka* means pulverizer, Dayan Qiuyishu uses mutual subtraction algorithm, i.e. both are by aid of the so-called Euclidean algorithm of the West.

The indeterminate analysis applied in both the mothods are two kinds of different programming but lead to surprisingly similar results.

The two points of Mahāvira's new idea are full of fascination. Let us apply his suggestion in solving equation

$$ax-1=by.$$

It is then equivalent to congruence (**), and then *Kuṭṭaka* and Dayan Qiuyishu would be completely identical. For by case 1, Ārya Bhaṭa's rule, we select $m=2n-1$, where $r_m=1$ and select again $x_{n-1}=t=1$, where $c=-1$.

$$y_n=q=t+c=0, \quad q=0$$

then we have Table C.

Table C

Programming I: *Kuṭṭaka*

Using formulas from (2n.1) to (1), Case 1, Ārya Bhaṭa's Rule
$\longleftarrow$
$q_2, q_3, \ldots, q_{2n-3}, q_{2n-2}, q_{2n-2}, 1, 0.$

Programming II: *Kuṭṭaka*

Using formulas from (2*n*.1) to (1) by *Kuṭṭaka*
$\longrightarrow$
$0, 1, q_{2n-1}, q_{2n-2}, q_{2n-3}, \ldots, q_3, q_2$

Programming III: Dayan Qiuyishu

Using Qin Jiushao's Rule, Dayan Qiuyishu
$J_m=q_mJ_{m-1}+J_{m-2}$, $(m=0, 1, 2\ldots, 2_{n-1}, J_1\equiv 1, J_0\equiv 0)$
$\longrightarrow$
$0, 1, q_2, q_3, \ldots q_{2n-3}, q_{2n-2}, q_{2n-1}.$

It is obvious that programming I and II are equivalent. That programming I and II are equivalent may be proved as follows. For *Kuṭṭaka*, programming II, we denote

$$K_m=2n+1-m\ K_{m-1}+K_{m-2},\ m=2n-1,\ 2n-2,\ \ldots,\ 3,\ 2$$

where $K_0=0$, $K_1=1$, and then the results by these two programmings would be:

$$\begin{aligned}
&K_0=0; && J_0=0\\
&K_1=1; && J_1=1\\
&K_2=q_{2n-1}; && J_2=q_2\\
&k_3=q_{2n-2}K_2+K_1; && J_3=q_3J_2+J_1=q_3q_2+1\\
&\qquad\cdots\cdots\\
&K_i=q_{2n+1-i}K_{i-1}+K_{i-2}; && J_i=q_iJ_{i-1}+J_{i-2}\\
&\qquad\cdots\cdots\\
&K_m=q_2K_{m-1}+K_{m-2}; && J_m=q_mJ_{m-1}+J_{m-2}.
\end{aligned}$$

Let us prove at first

$$K_m=J_m$$

for $K_m=J_jK_{m-j+1}+J_{j-1}K_{m-j}$, where $2\leqslant j\leqslant m=2n-1$.

By mathematical induction we have

(1) $j=2$, $K_m=q_2K_{m-1}+K_{m+2}=J_2K_{m-1}+J_1K_{m-2}$
(2) if $j=i$ is true, then $j=i+1$ is also true,

for

$$\begin{aligned}
K_m&=J_iK_{m-i+1}+J_{i-1}K_{m-i}\\
&=J_i(q_{(m+2)-(m-i+1)}\ K_{m-i}+K_{m-i-1})+J_{i-1}K_{m-i}\\
&=(J_iq_{i+1}+J_{i-1})\ K_{m-i}+J_i\ K_{m-i-1}\\
&=J_{i+1}\ K_{m-i}+J_i\ K_{m-i-1}.
\end{aligned}$$

Especially, $j=m$, we have

$$K_m=J_mK_1+J_{m-1}K_0=J_m.\qquad \text{Q.E.D.}$$

Both China and India are ancient nations in Asia, they all have thousands years of recorded history, and contact through religions, trade, travel and cultural exchanges and envoys of friendship. The Indian monk Kāśyapa-mātaṅga brought Buddhist Sūtra to Laoyang, Henan Province in 67 A.D., and the Chinese monks Fa Xian and Xuan Zhang went on a pilgrimage for Buddhist Scriptures in 399 and 627 A.D. respectively. These are the eminent examples. *Memoirs on Western Countries* (646) notes Xian Zhang's profound memoirs during his visiting trips. The Indian astronomer

Gautama Siddhartha had served in Chinese Royal Observatory of the Tang Dynasty for years, his work *Jiu Zhi Calendar* was translated from Sanskrit. The books written by both Chinese and Indians, handed down from ancient times, become indeed important historical as well as scientific records for all times.

Indian mathematicians, Brahmagupta and Bhāskara had been in Ujjain where Xian Zhang and other Chinese envoys were living there for a long time, and cultural overflows with each other would be inevitable. The parallelism in the development of mathematics between China and India has been the deep concern for years of international learning circles. This paper gives a comparatively thorough and objective comparison depending upon sound foundations of original mathematical literatures of both the nations. As for the true relationship of transmission it is a complex, hard but interesting problem which has to be further discussed.

References

[1]Ārya Bhaṭa, *Ārya Bhaṭīya*, critically Edited with English Translation and Notes by K. S. Shukla and K. V. Sarma, New Delhi, 1976.
[2]Datta, B. and Singh, A. N., *History of Hindu Mathematics*, Lahore, 1935.
[3]Bag, A. K., 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**, No. 1, pp. 1-16, 1977.
[4]——, *Mathematics in Ancient and Medieval India*, Varanasi, 1979.
[5]Srinivasiengar, C. N., *The History of Ancient Indian Mathematics*, Calcutta, 1967.
[6]Sun Zi, *A Mathematical Classic of Sun Zi*, Collated by Qian, B. C., Shanghai, 1964.
[7]Mikami, Y., *The Development of Mathematics, in China and in Japan*, Dresden, 1910.
[8]See Ref. 6.
[9]Qin Jiushao, *Nine Chapters of Mathematics*, Hangzhou, 1247.
[10]Huang, Z. X., *General Solution of Qiuyishu*, Changsha, 1874.
[11]Shen, K. S., Origin and Development of Mutual-subtraction Algorithm, *Studies in the History of Natural Sciences*, **2**, No. 3, pp. 193-207, 1982.