Historical Development of the Chinese Remainder Theorem

SHEN KANGSHENG

Communicated by C. TRUESDELL

1. Source of the Problem

Congruences of first degree were necessary to calculate calendars in ancient China as early as the 2nd century B.C. Subsequently, in making the *Jingchu* [a] calendar (237 A.D.), the astronomers defined *shangyuan* [b][1] as the starting point of the calendar. If the Winter Solstice of a certain year occurred r_1 days after *shangyuan* and r_2 days after the new moon, then that year was N years after *shangyuan;* hence arose the system of congruences

$$aN \equiv r_1 \pmod{60} \equiv r_2 \pmod{b},$$

where a is the number of days in a tropical year and b the number of days in a lunar month.

2. *Sun Zi suanjing* [c] (Master Sun's Mathematical Manual)

Sun Zi suanjing (Problem 26, Volume 3) reads: "There are certain things whose number is unknown. A number is repeatedly divided by 3, the remainder is 2; divided by 5, the remainder is 3; and by 7, the remainder is 2. What will the number be?" The problem can be expressed as

$$x \equiv 2 \pmod{3} \equiv 3 \pmod{5} \equiv 2 \pmod{7}.$$

SUN ZI solved the problem as we do, giving

$$x \equiv 140 + 63 + 30 \equiv 233 \equiv 23 \pmod{105}.$$

---

[1] *Shangyuan* is a supposed moment that occurred simultaneously with the midnight of *jiazi* [v] (the first day of the 60 day cycle), the Winter Solstice and the new moon.

In speaking of the algorithm yielding these addends in the solution he continued: "In general, for

$$G_1 \equiv 0 \pmod 5 \equiv 0 \pmod 7 \equiv 1 \pmod 3, \text{ take } G_1 = 70,$$

$$G_2 \equiv 0 \pmod 3 \equiv 0 \pmod 7 \equiv 1 \pmod 5, \text{ take } G_2 = 21,$$

$$G_3 \equiv 0 \pmod 3 \equiv 0 \pmod 5 \equiv (1 \bmod 7), \text{ take } G_3 = 15.$$

Thus, in the present problem, if

$$G_1' \equiv 0 \pmod 5 \equiv 0 \pmod 7 \equiv 2 \pmod 3, \text{ so } G_1' = 70\times 2 = 140,$$

$$G_2' \equiv 0 \pmod 3 \equiv 0 \pmod 7 \equiv 3 \pmod 5, \text{ so } G_2' = 21\times 3 = 63,$$

$$G_3' \equiv 0 \pmod 3 \equiv 0 \pmod 5 \equiv 2 \pmod 7, \text{ and } G_3' = 15\times 2 = 30,$$

then the required $x \equiv G_1' + G_2' + G_3' \pmod{105}$."

SUN'S example is a special numerical one, which can be transformed to solve the general case:

$$x \equiv r_i \pmod{m_i} \quad (i = 1, 2, \ldots, n) \tag{1}$$

where m_i, m_j are relative primes, $1 \leqq i < j \leqq n$. If

$$\begin{aligned} &G_1 \equiv 0 \pmod{m_2} \equiv 0 \pmod{m_3} \ldots \equiv 0 \pmod{m_n} \equiv 1 \pmod{m_1}, \\ &G_2 \equiv 0 \pmod{m_1} \equiv 0 \pmod{m_3} \ldots \equiv 0 \pmod{m_n} \equiv 1 \pmod{m_2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &G_n \equiv 0 \pmod{m_1} \equiv 0 \pmod{m_2} \ldots \equiv 0 \pmod{m_{n-1}} \equiv 1 \pmod{m_n}, \end{aligned} \tag{2'}$$

then

$$x \equiv \sum_{i=1}^{n} G_i' \equiv \sum_{i=1}^{n} G_i r_i \left(\bmod \prod_{i=1}^{n} m_i\right). \tag{3'}$$

In the same way, if we get F_i from n congruences and let

$$M_i F_i = G_i \equiv 1 \pmod{m_i}, \tag{2}$$

then

$$x \equiv \sum_{i=1}^{n} G_i' \equiv \sum_{i=1}^{n} G_i r_i \equiv \sum_{i=1}^{n} M_i F_i r_i \pmod M, \tag{3}$$

where

$$M = \prod_{i=1}^{n} m_i,\ M_i = M/m_i.$$

This statement is called the SUN ZI Theorem, or the Chinese Remainder Theorem. Indeed, in imitation of the theorem, YANG HUI [d] in *Xu gu zhai qi suanfa* [e] (Continuation of ancient mathematics for elucidating the strange, 1275) had four similar problems, three of which concerned $n = 3$ and the fourth $n = 4$, *i.e.*

$$x \equiv 1 \pmod 2 \equiv 2 \pmod 5 \equiv 3 \pmod 7 \equiv 4 \pmod 9.$$

By applying formula (2), he estimated

$$G_1 = 315, \quad G_2 = 126, \quad G_3 = 540, \quad G_4 = 280.$$

Substituting these in formula (3) he got the final answer:

$$x \equiv 315\times 1 + 126\times 2 + 540\times 3 + 280\times 4 \equiv 3307 \equiv 157 \pmod{630}.$$

3. Kuttaka of India

3.1. The solution of the equation

$$ax + c = by \tag{4}$$

for x, y in positive integers (where a, b, c are given integers, $a > b$, and a, b are relatively prime) is called *Kuttaka* by Indian mathematicians. Literally, *Kuttaka* means a pulverizer, a name given on account of the process of continued division that was adopted for the solution. Legend has it that it was up to ARYABHATA (c. 476 A.D.) to determine the integer N which when divided by a leaves the remainder r_1, and when divided by b, leaves the remainder r_2; thus

$$N = ax + r_1 = by + r_2,$$

i.e.

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

Thus ARYABHATA discoverd a rule for the solution, which he expressed in two obscure stanzas of his *Aryabhatiya.*[2]

In modern symbolism by B. DATTA[3], the solution can be expressed as follows. Through continued division (Euclidean algorithm) a series of quotients and corresponding remainders are as follows:

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

the relations among them are

$$a = bq_1 + r_1,$$

$$b = r_1q_2 + r_2,$$

$$r_1 = r_2q_3 + r_3,$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$r_{n-2} = r_{n-1}q_n + r_n,$$

---

[2] ARYABHATA, *Aryabhatiya*, K. S. SHUKLA's English Translation, 1979, Delhi, pp. 74–84.

[3] B. DATTA & A. N. SINGH, *History of Hindu Mathematics*, 1938, Lahole, Vol. 2, pp. 95–99.

from which there is a series of reduction formulas:

$$y = q_1 x + y_1, \text{ where } by_1 = r_1 x + c,$$

$$x = q_2 y_1 + x_1, \text{ where } r_1 x_1 = r_2 y_1 - c,$$

$$y_1 = q_3 x_1 + y_2, \text{ where } r_2 y_2 = r_3 x_2 + c,$$

$$x_1 = q_4 y_2 + x_2, \text{ where } r_3 x_2 = r_4 y_2 - c,$$

.....

$$y_{m-1} = q_{2m-1} x_{m-1} + y_m, \text{ where } r_{2m-2} y_m = r_{2m-1} x_{m-1} + c,$$

$$x_{m-1} = q_{2m} y_m + x_m, \text{ where } r_{2m-1} x_m = r_{2m} y_m - c.$$

There are two cases to consider:
Case 1, $n = 2m - 1$.

$$y_{m-1} = q_{2m-1} x_{m-1} + y_m, \; r_{2m-2} y_m = r_{2m-1} x_{m-1} + c.$$

Let $x_{m-1} + t$, so that $y_m = (r_{2m-1} t + c)/r_{2m-2}$ is the integer q, and then from bottom to top by reduction formulas we obtain the required x and y.
Case 2, $n = 2m$.

$$x_{m-1} = q_{2m} y_m + x_m, \; r_{2m-1} x_m = r_{2m} y_m - c.$$

Let $y_m = t'$, so that $x_m = (r_{2m} t' - c)/r_{2m-1}$ is the integer q'. We then obtain x and y by using these reduction formulas from bottom to top.

3.2. We may note that Chapter IV of MAHAVIRA'S *Ganita Sara Sangraha* presents new points of view[4]:

1. Omit q_1, and when x is solved, y may be determined by substituting x in equation (4).
2. Continued division is carried up to $r_n = 1$.

MAHAVIRA'S idea is fascinating. Let us apply his suggestion to the equation

$$ax - 1 = by \tag{5}$$

and the series of quotients will be

$$q_{2m-1}, q_{2m-2}, \ldots, q_3, q_2.$$

When $r_{2m-1} = r_n = 1$, in Case 1 of *Kuttaka*, let $x_{m-1} = t = 1$, so that $y_m = 0$, and let $k_0 = y_m = 0$, $k_1 = x_{m-1} = 1$. With the reduction formula of *Kuttaka*, we have

$$k_2 = y_{m-1} = q_{2m-1} x_{m-1} + y_m = q_{2m-1} k_1 + k_0,$$

$$k_3 = x_{m-2} = q_{2m-2} y_{m-1} + x_{m-1} = q_{2m-2} k_2 + k_1, \ldots,$$

---

[4] C. N. SRIHIVASIENGAR, *The History of Ancient Indian Mathematics*, 1967, Calcutta, pp. 101–102.

and in general,

$$k_i = q_{2m+1-i}k_{i-1} + k_{i-2} = q_{n+2-i}k_{i-1} + k_{i-2};$$

thus

$$x = k_n = q_2k_{n-1} + k_{n-2}. \tag{6}$$

3.3. Moreover, Indian mathematicians did much work on *Kuttaka* and left us many problems, such as the following.

Example 1. Find the number that if divided by 8 is known to leave 5, that if divided by 9 leaves a remainder 4, and that if divided by 7 leaves a remainder 1 (*Aryabhatiya*, annotated by BHASKARA I. the 6th century).

Example 2. Suppose at a certain time since the *Kalpa*, the sun, the moon *etc.*, have travelled for the following number of days after completing their full revolutions:

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 revolution in 185 days, Mercury, 13 revolutions in 1096 days, Jupiter, 3 revolutions in 10960 days, Saturn, 1 revolution in 10960 days, find the number of days since the *Kalpa* (*Brahmagupta*, XVIII, sl 7–8, 628.)

Example 3. The dividends are sixteen numbers beginning with 35 and increasing successively by 3; the divisors are 32 and others increasing successively by 2; the remainders are 1 and others increasing successively by 3. What is the unknown multiplier? (MAHAVIRA, *Ganita Sara Sargraha*, IV, 138 1/3, c. 850.)

In general, in solving systems of equations

$$x = a_1x_1 + r_1 = a_2x_2 + r_2 = \ldots = a_nx_n + r_n,$$

Indian mathematicians started with the first two conditions,

$$x = a_1x_1 + r_1 = a_2x_2 + r_2.$$

By *Kuttaka* one can find the minimum value of x_1, say α; then the minimum value of x will be $a_1\alpha + r_1$ and hence the general solution will be

$$x = a_1(a_2t + \alpha) + r_1 = a_1a_2t + a_1\alpha + r_1$$

where t is an integer. If we supply the third condition, then

$$x = a_1a_2t + a_1\alpha + r_1 = a_3x_3 + r_3,$$

which can be solved in the same way. Proceeding in this way successively we will have a value satisfying all the conditions.[3]

4. The General *Dayan qiuyi* [f] Rule

Shu shu jiu zhang [g], written by QIN JIUSHAQ [h] in 1247, was the most important mathematical work in the Song [i] dynasty. At its very beginning there is the General *Dayan qiuyi* Rule, discussing extensively congruences of first degree in order to solve the nine problems in Chapter I and the third problem of Chapter II. These problems are set against various natural or social backgrounds, yet all of them are expressed by systems of congruences as far as mathematics is concerned[5]. Their moduli are of different types.

Example 1. Solve $x \equiv 1 \pmod{19} \equiv 14 \pmod{17}$
$\equiv 1 \pmod{12}$ (*Ssjz*[6], I, 9)

Example 2. Solve $x \equiv 0.32 \pmod{0.83}$
$\equiv 0.70 \pmod{1.10}$
$\equiv 0.30 \pmod{1.35}$ (*Ssjz*, I, 5)

Example 3. Solve $x \equiv 0 \pmod{365\ \ 4108/16900}$
$\equiv 11\ \ 7540/16900 \pmod{60}$
$\equiv 10\ \ 7264/16900 \pmod{29\ \ 8967/16900}$ (*Ssjz*, II, 3)

Example 4. Solve $x \equiv 0 \pmod{54} \equiv 0 \pmod{57}$
$\equiv 51 \pmod{75} \equiv 18 \pmod{72}$ (*Ssjz*, I, 3)

Example 5. Solve $x \equiv -60 \pmod{130} \equiv -30 \pmod{110}$
$\equiv -10 \pmod{120} \equiv -10 \pmod{60} \equiv 10 \pmod{25}$
$\equiv 10 \pmod{100} \equiv 10 \pmod{30} \equiv 10 \pmod{20}$ (*Ssjz*, I, 8)

The General *Dayan qiuyi* Rule is composed of four parts, as follows:

4.1. The classification of moduli

Yuanshu [j]—A set of natural numbers without a gcf (greatest common factor)[7].
Shoushu [k]—A set of decimals.
Tongshu [l]—A set of fractions.
Fushu [m]—A set of natural numbers having a gcf.

4.2. To convert moduli into *dingshu* [n].

4.2.1. To convert *shoushu* and *tongshu* into *yuanshu* QIN believed that

$$x \equiv \frac{b}{a} \left(\mathrm{mod}\, \frac{c}{a}\right),$$

---

[5] U. LIBBRECHT, *Chinese Mathematics in the Thirteenth Century*, 1973, MIT Press, pp. 384–412.

[6] We abbreviate *Shu shu jiu zhang* (Mathematical Treatise in Nine Chapters) as *Ssjz*.

[7] The greatest common factor of $a, b, \ldots, c$, we denote by $(a, b, \ldots c)$.

where a, b, c are natural numbers, was the same as the congruence

$$ax \equiv b \pmod{c}.$$

Therefore the system of congruences in Example 2 may be converted into

$$100x \equiv 32 \pmod{83} \equiv 70 \pmod{110} \equiv 30 \pmod{135},$$

and that in Example 3 into

$$\begin{aligned} 6172608x &\equiv 193440 \pmod{1014000} \\ &\equiv 163771 \pmod{499067}. \end{aligned}$$

4.2.2. To convert *yuanshu* into *dingshu*, QIN must have had an intimate knowledge of the Chinese Remainder Theorem and also the condition for solubility of the system of congruences. The moduli of nine problems in *Ssjz* are not relatively prime. If we solve them by the theorem directly, there would be a contradiction. Thus, with great care, QIN converted each modulus of the sets into *dingshu* μ_i so as to satisfy

$$(\mu_i, \mu_j) = 1, \tag{7.1}$$

$$\mu_i \mid m_i, \tag{7.2}$$

$$\prod_{i=1}^{n} \mu_i = M = \{m_1, m_2, \ldots, m_n\}^8. \tag{7.3}$$

As we know, QIN's treatment is correct and necessary. When we replace m_i by μ_i, the new system is the same as the original system (1) and so then the converted system may be solved by the theorem.

Ssjz formulated a program for converting *yuanshu* into *dingshu*. For a set of moduli $m_1, m_2, \ldots, m_n$ QIN gives:

Step 1. To find the gcf of m_{n-1}, m_n, *i.e.*, $(m_{n-1}, m_n) = d_1$: QIN considered m_{n-1}/d_1, m_n as *dingshu* of m_{n-1}, m_n, respectively, if $(m_{n-1}/d_1, m_n) = d_2 = 1$.

Step 2. Otherwise, *i.e.*, $d_2 > 1$, give $m_{n-1}, m_n/d_1$ as *dingshu* of m_{n-1}, m_n, if

$$(m_{n-1}, m_n/d_1) = d_2' = 1.$$

Step 3. Otherwise, *i.e.*, $d_2' > 1$, give m_{n-1}/d_2', $m_n d_2'/d_1$ as *dingshu* of m_{n-1}, m_n, if

$$(m_{n-1}/d_2', m_n d_2'/d_1) = d_3 = 1.$$

Step 4. Otherwise, *i.e.*, $d_3 > 1$, give $m_{n-1}/d_2' d_3$, $m_n d_2' d_3/d_1$ as *dingshu* of m_{n-1}, m_n, if

$$(m_{n-1}/d_2' d_3, m_n d_2' d_3/d_1) = d_4 = 1.$$

Likewise, give $\mu_{n-1}' = m_{n-1}/d_2' d_3 \ldots d_k$,

$$\mu_n' = m_n d_2' d_3 \ldots d_k/d_1$$

---

[8] lcm, the least common multiplier of $a, b, \ldots c$, we denote by $\{a, b, \ldots c\}$.

as *dingshu* of m_{n-1}, m_n, if

$$(\mu'_{n-1}, \mu'_n) = d_{k+1} = 1^9.$$

Similarly, operate on μ'_n with $m_{n-1}, m_{n-2}, m_{n-3}, \ldots, m_2, m_1$ and denote the results by

$$\mu'_1, \mu'_2, \ldots, \mu'_{n-2}, \mu'_{n-1}, \mu_n.$$

Again, operate on μ'_{n-1} with μ'_i $(i = n-2, n-3, \ldots, 2, 1)$ and denote the results by

$$\mu''_1, \mu''_2, \ldots, \mu''_{n-3}, \mu''_{n-2}, \mu_{n-1}, \mu_n.$$

Again, operate on μ''_{n-2} with μ''_i $(i = n-3, n-4, \ldots, 2, 1)$ and denote the results by

$$\mu'''_1, \mu'''_2, \ldots, \mu'''_{n-3}, \mu_{n-2}, \mu_{n-1}, \mu_n.$$

.....

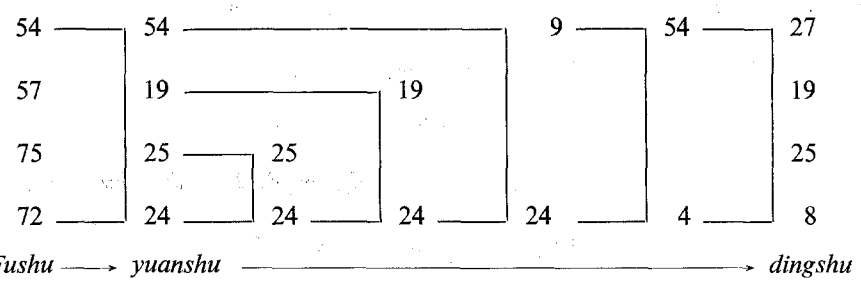
Finally, we have

$$\mu_1, \mu_2, \ldots, \mu_{n-1}, \mu_n.$$

These are the required *dingshu* of the moduli. It is obvious that conditions (7.1) to (7.3) are satisfied and system $x \equiv r_i \pmod{\mu_i}$ is the same as system (1).

4.2.3. To convert *fushu* into *yuanshu*, QIN considered a set of moduli $a, b, \ldots, c$, in which $a = a_1 d$, $b = b_1 d, \ldots, c = c_1 d$, where $d = (a, b, \ldots, c)$. If there is also a factor d in $a_1, b_1, \ldots$ or c_1 and the exponent of d, say, in a_1 is the highest, then the *dingshu* of the set $a, b, \ldots, c$ is equal to that of $a, b_1, \ldots, c_1$.

The set of moduli in Example 4 is *fushu*, for $(54, 57, 75, 72) = 3$, and the exponent of 3 in 54 is the highest, QIN converted first the *fushu* into 54, 19, 25, 24, and then converted them further into *dingshu* by the process in § 4.2.2. The numerical examples treated in *Ssjz* are as follows:

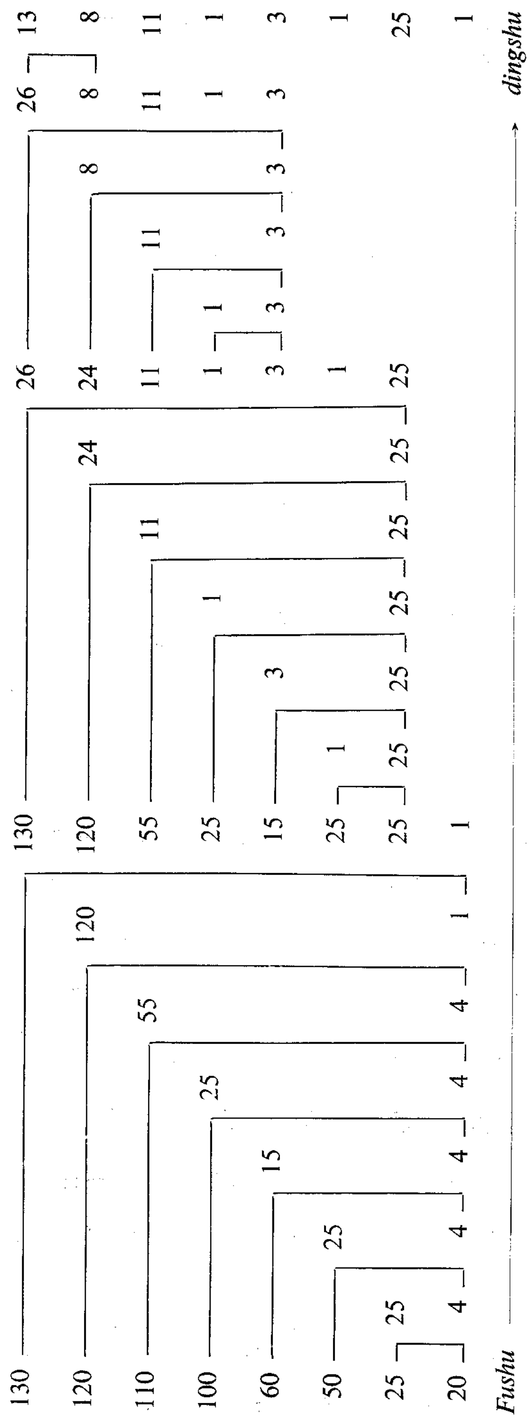


The original moduli are thus converted into *dingshu* 27, 19, 25, 8.

In fact it is unnecessary to convert *fushu* into *yuanshu* first. The moduli in Example 5 have a gcf, so that the set would be *fushu*, which QIN, however, converted directly by the process in § 4.2.2. (ruling out § 4.2.3.) into *dingshu* as follows:

---

[9] There is a k, certainly such that $d_{k+1} = 1$, for d_1 is definite, whereas $d_2 \geqq d_3 \geqq d_4 \geqq \ldots \geqq d_k$; see LI JIMIN, On *Dingshu* of *Ssjz*, *Qin Jiushao and Ssjz*, 1987, Beijing Normal University Press, pp. 220–234.


Fushu
dingshu

4.3. The *Dayan qiuyi Rule*. The moduli having been converted into *dingshu*, the system of congruences can be solved by the Chinese Remainder Theorem. It boils down to

$$ax \equiv 1 \pmod{b}. \tag{8}$$

QIN summed up the *Dayan qiuyi* Rule (Rule of finding unity) in this connection. The rule is a special algorithm designed to solve congruence (8), where $a < b$. Though the original text is brief and obscure, a careful study of the problems of *Ssjz* presents the rule as follows:

Step 1. Arrange a at the upper right, and b below. Set down *tian yuan* [o], the unity $(j_1 = 1)$, at the upper left.

Step 2. Divide the lower right number by the upper one $(b/a = q_2 + r_2/a)$, and then multiply the quotient by *tian yuan*. Put the result $(j_2 = q_2 j_1)$ at the left below.

Step 3. Divide the larger number (upper right number, a) by the smaller one (lower right number r_2, $a/r_2 = q_3 + r_3/r_2$). Multiply the quotient (q_3) by the lower left number and add the result to the upper left number $(j_3 = q_3 j_2 + j_1)$. Put the sum at the upper left.

Step 4. Repeat the same process

$j_4 = q_4 j_3 + j_2$ (put the sum at the lower left),

$j_4 = q_5 j_4 + j_3$ (put the sum at the upper left),

.....

Step n. It is necessary to set the final upper right number at unity (*i.e.* to find the remainder $r_n = 1$), where n is odd. Then the corresponding upper left number is *chenglü* [p], the solution of congruence (8), *i.e.*

$$j_n = q_n j_{n-1} + j_{n-2}, \quad j_0 = 0, \quad j_1 = 1. \tag{9}$$

QIN's idea may be expressed by the following diagrams:

Step 1		Step 2		Step 3		Step 4		...	Step n	
				q_3						q_n
j_1	a	j_1	a	j_3	r_3	j_3	r_3	...	j_n	$r_n = 1$
	b	j_2	r_2	j_2	r_2	j_4	r_4		j_{n-1}	r_{n-1}
		q_2				q_4				

Problem 3, in Chapter II of *Ssjz* has a numerical example (Figure 1) in calculating the *Kaixi* [q] calendar (1207–1251), which, in modern notation, is

$$377873x \equiv 1 \pmod{499067}.$$

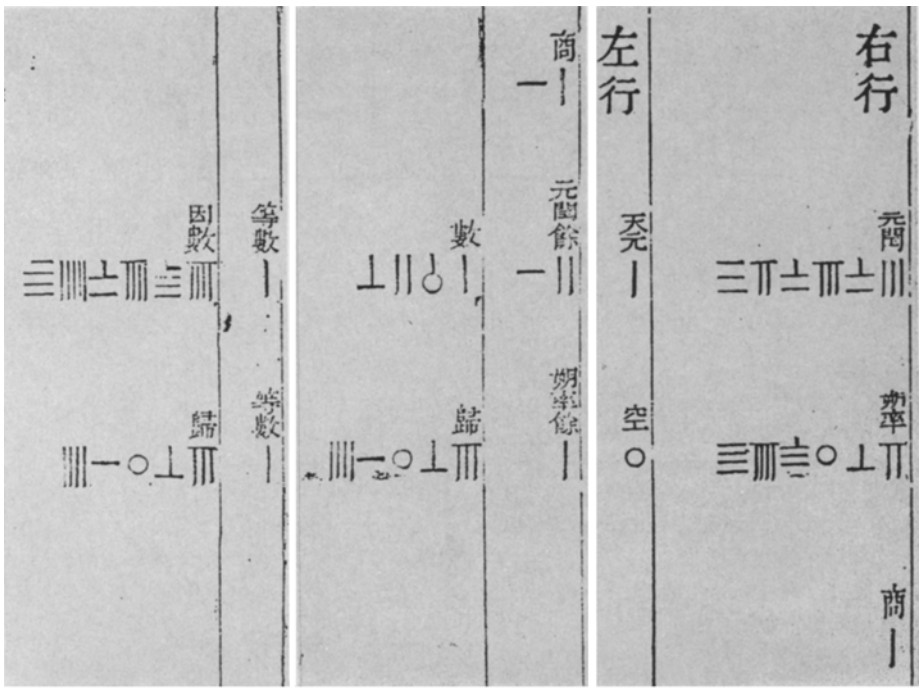


Fig. 1. Episode of Chapter II, *Ssjz*, the processes of solving $337873x \equiv 1 \pmod{499067}$

In Arabic figures the processes of the solution are:

Step 1		Step 2		Step 3		Step 4	
				q_3			
				3			
j_1	a	j_1	a	j_3	r_3	j_3	r_3
1	377873	1	377873	4	14291	4	14291
	b	j_2	r_2	j_2	r_2	j_4	r_4
	499067	1	121194	1	121194	33	6866
		q_2				q_4	
		1				8	

Step 5		Step 6		Step 7		Step 8	
q_5				q_7			
2				3			
j_5	r_5	j_5	r_5	j_7	r_7	j_7	r_7
70	559	70	559	2689	85	2689	85
j_4	r_4	j_6	r_6	j_6	r_6	j_8	r_8
33	6866	873	158	873	158	3562	73
		q_6				q_8	
		12				1	

Step 9		Step 10		Step 11	
q_9				q_{11}	
1				11	
j_9	r_9	j_9	r_9	j_{11}	r_{11}
6251	12	6251	12	457999	1
j_8	r_8	j_{10}	r_{10}	j_{10}	r_{10}
3562	73	41068	1	41068	1
		q_{10}			
		6			

Here QIN concluded: "*Chenglü* 457999 is the solution of the congruence."

4.4. To solve the System of Congruences.

When the moduli in system (1) are converted, one by one, into *dingshu*, the unknown F_i in congruence (2) is solved by the *Dayan qiuyi* rule. Substituting F_i in the general solution (3) we have the required

$$x \equiv \sum_{i=1}^{n} M_i F_i r_i \pmod{M}, \qquad M_i = M/m_i.$$

This is the rule in the 740-year-old *Ssjz*.

5. *Sho yuku jutu su* [r] of Japan

The Japanese mathematician SEKI TAKAKAZU [s], wrote *Kwatsuyo sampo* [t] (Essential Algorithm) in 1683, the second chapter of which, *Sho yuku jutu su*, deals with some algorithms corresponding to QIN'S work.

5.1. The Algorithm of Mutual Reduction. The algorithm gives a program for transforming two *yuanshu* m_1, m_2 into *dingshu* μ_1, μ_2.

Step 1. To find the gcf of m_1, m_2, i.e. $(m_1, m_2) = d_1$. SEKI considered m_1, m_2/d_1 as *dingshu* of m_1, m_2, if $d_2 = (m_1, m_2/d_1) = 1$.

Step 2. When $d_2 > 1$; m_1/d_2, $m_2\, d_2/d_1$ are *dingshu* of m_1, m_2, if $d_3 = (m_1/d_2, m_2\, d_2/d_1) = 1$.

Step 3. When $d_3 > 1$, $m_1/d_2 d_3$, $m_2\, d_2\, d_3/d_1$ are *dingshu* of m_1, m_2, if $(m_1/d_2\, d_3, m_2\, d_2\, d_3/d_1) = 1$.

.....

The process does not stop until the two numbers become relatively prime.

5.2. Algorithm of Seeking *dingshu* One by One. SEKI transforms *yuanshu* (more than 2) to *dingshu* with his algorithm of mutual reduction one by one. The program is just like QIN's.

5.3. The rule of "Unit Remainder" and the rule of "Cutting Tubes" are somewhat similar to QIN's General *Dayan qiuyi* Rule, suitable for a congruence or a system of congruences.

6. Relevant Treatises in Central Asia and Western Europe

6.1. In the Islamic scholar IBN AL-HAITHAM'S work (c. 1000 A.D.) there is a remainder problem, *i.e.* put in modern words, to solve

$$x \equiv 1 \pmod 2 \equiv 1 \pmod 3 \equiv 1 \pmod 4 \equiv 1 \pmod 5$$
$$\equiv 1 \pmod 6 \equiv 0 \pmod 7).$$

His answer, 721, is not the smallest solution.

There are several remainder problems in LEONARDO FIBONACCI'S *Liber Abaci* (1202). However, FIBONACCI did not give the slightest theoretical or general explanation of the method for solution of the remainder problem, and for this reason his whole treatment is on a level no higher than that of SUN ZI.[10]

In other Western works of the 14th–17th centuries appeared a few remainder problems with merely incomplete solutions. In the 18th century the great mathematicians L. EULER (1707–1783), J. L. LAGRANGE (1736–1813), and C. F. GAUSS (1777–1855) studied successively the remainder problems and they accomplished ample achievements.

6.2. EULER gave the general solution of congruence (8). If the quantities A, B, C, D, E, *etc.* depend on α, β, γ, δ, ε, *etc.* in the following way:

$$A = \alpha,\ B = \beta A + 1,\ C = \gamma B + A,$$
$$D = \delta C + B,\ E = \varepsilon D + C, \text{ etc.}$$

[10] LIBBRECHT, *Op. cit.* p. 240.

which may be simplified as

$$A = [\alpha],\ B = [\alpha, \beta],\ C = [\alpha, \beta, \gamma],\ D = [\alpha, \beta, \gamma, \delta] \text{ etc.}$$

Consider the indeterminate equation $ax = by \pm 1$ $(a > b)$. By the Euclidean algorithm he had

$$a = \alpha b + c, \quad b = \beta c + d, \quad c = \gamma d + e, \quad \text{etc.},$$

so that α, β, γ, *etc.*, c, d, e, *etc.*, constantly decrease until $m = \mu n + 1$. The result will be

$$a = [n, \mu, \ldots, \gamma, \beta, \alpha], \quad b = [n, \mu, \ldots, \gamma, \beta].$$

EULER took

$$x = [\mu, \ldots, \gamma, \beta], \quad y = [\mu, \ldots, \gamma, \beta, \alpha], \tag{10}$$

as the solution if $ax = by + 1$ if the number of terms $\alpha, \beta, \gamma, \ldots, \mu, n$ is even, and as the solution of $ax = by - 1$ if it is odd.[11]

6.3. LAGRANGE treated the same problem by the theory of continued fraction, b/a was converted into the continued fraction

$$\frac{a}{b} = \alpha + \frac{1}{\beta + \dfrac{1}{\gamma + \dfrac{1}{\delta + \cdots + \dfrac{1}{\mu + \dfrac{1}{n}}}}}. \tag{11}$$

Having deleted the last term $1/n$, he reconverted it into a common fraction. He considered the numerator and the denominator of the fraction as the answer to $ax = by + 1$ if the number of terms $\alpha, \beta, \gamma, \ldots, \mu, n$ is even and as the answer to $ax = by - 1$ if the number of terms $\alpha, \beta, \gamma, \ldots, n$ is odd.[12]

6.4. GAUSS published his *Disquisitiones Arithmeticae*[13] in 1801; the first two of its seven chapters are devoted to congruences. We sum up his relevant theorems as follows:

I, 16. A composite number can be resolved into prime factors in only one way.

II, 27. If $(a, b) = 1$, then

$$ax + t \equiv u \pmod{b} \tag{*}$$

is solvable. If $x = r$ satisfies

$$ax \equiv \pm 1 \pmod{b}, \tag{**}$$

then $x = \pm(u - t)\, r$ will satisfy (*).

---

[11] L. EULER, Solutio Problematis Arithmetici de Inveniendo Numero qui per Datos Numeros Divisus, Relinquat Data Residua; *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, 1734–1735, St. Petersburg.

[12] J. L. C. LAGRANGE, Sur la solution des Problèmes Indéterminées du Second Degré, *Histoire de l'Academie Royale des Sciences*, 1767, Berlin.

[13] C.F. GAUSS, *Disquisitiones Arithmeticae*, English Translation, Yale University Press, 1966.

Citing EULER's algorithm for solving (**), GAUSS gave his own investigations:

1. $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] \cdot [\beta, \gamma, \ldots, \lambda] - [\alpha, \beta, \gamma, \ldots, \lambda] \cdot [\beta, \gamma, \ldots, \lambda, \mu] = \pm 1$

where the upper sign is taken if the number of terms $\alpha, \beta, \gamma, \ldots, \lambda$ is even and the lower is taken if it is odd.

2. The order of the numbers can be inverted:

$$[\alpha, \beta, \gamma, \ldots, \lambda, \mu] = [\mu, \lambda, \ldots, \gamma, \beta, \alpha].$$

II, 28. Cites LAGRANGE's algorithm.

II, 29. Congruence (*) is solvable if $t \equiv u \pmod{\delta}$, where $\delta = (a, b)$. Congruence (*) is equivalent to $ex + k \equiv 0 \pmod{f}$, if $a = \delta e$, $b = \delta f$, $t - u = \delta k$.

II, 32. To solve $z \equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C}$, first solve $Ax + a \equiv b \pmod{B}$. If $(A, B) = \delta$, the complete solution will be

$$x \equiv v \pmod{B/\delta};$$

thus

$$z = Ax + a = A(v + Bk/\delta) + a \equiv c \pmod{C}.$$

If $(AB/\delta, C) = e$ and the solution of

$$z = ABx/\delta + Av + a \equiv c \pmod{C} \quad \text{is} \quad x = w \pmod{C/e},$$

the problem will be completely solved by the congruence

$$z = ABw/\delta + Av + a \pmod{ABC/\delta e}.$$

II, 33

$$z \equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C} \textit{ etc.}$$

is equivalent to $z \equiv r \pmod{ABC \textit{ etc.}}$ if A, B, C, *etc.* are relatively prime.

II, 34

$$z \equiv a \pmod{A} \equiv b \pmod{B} \textit{ etc.}$$

is equivalent to

$$z \equiv a \pmod{A'} \equiv a \pmod{A''} \equiv a \pmod{A'''} \text{ etc.}$$

$$\equiv b \pmod{B'} \equiv b \pmod{B''} \equiv b \pmod{B'''} \text{ etc.}$$

where $A = A'A''A'''$ etc., $B = B'B''B'''$, etc. Either $z \equiv a \pmod{A'}$ or $z \equiv b \pmod{B'}$ can be rejected if $A' = B'$. If however, $a \equiv b \pmod{A'}$ is not true, the problem has no solution. If B' is multiple of A', the former can be rejected.

When all the superfluous conditions have been rejected, all the remaining moduli A', A'', A''', etc., B', B'', B''', etc. will be relatively prime.

II, 36

$$z \equiv a \pmod{A} \equiv b \pmod{B} \equiv c \pmod{C} \equiv d \pmod{D} \text{ etc.}$$

where $A, B, C, D, \ldots$ are relatively prime. It is often preferable to use the following method. If we solve in the proper order

$$z \equiv 1 \pmod{A} \equiv 0 \pmod{BCD \text{ etc.}},$$
$$z \equiv 1 \pmod{B} \equiv 0 \pmod{ACD \text{ etc.}},$$
$$z \equiv 1 \pmod{C} \equiv 0 \pmod{ABD \text{ etc.}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

the least solution to the congruences will be, say, α, β, γ, etc. respectively. The general solution is

$$z = \alpha a + \beta b + \gamma c \text{ etc. } (\text{mod } ABC \text{ etc.}).$$

7. Conclusion

7.1. The cultural development of the world makes it fairly clear that remainder problems originated from calendar making.[14] Calculating *shangyuan*, the starting point of the calendar, ancient Chinese astronomers had to solve numerous systems of congruences, with data so vast as to make it impossible to obtain accurate answers without some special algorithm. Example 3 in Section 4 of this paper is a vivid sample. Similar examples appeared in medieval India; BRAHMAGUPTA's problem (see the example in Section 3) for finding the number of days since the *Kalpa* was also based on sound astronimical facts. Let us compare:

Period (days)	Sun	Moon	Mars	Mercury	Jupiter	Saturn
India, 8th c.	365.3	27.4	84.3	685	3653.3	10960
Recent Data	365.2	27.3	89	687	4333	10759

Moreover, GAUSS explained Proposition II, 36 of his *Disquisitiones Arithmeticae* in these words: "This usage arises in ... chronology when we determine what Julian year it is whose indiction, golden number, and solar cycle are given. Here $A = 15$, $B = 19$, $C = 28$; thus the value of α will be 6916, β 4200 and γ 4845. The number we seek will be the least residue of the number $6196a + 4200b + 4845c$, where a is the indiction, b the golden number, and c the solar cycle." Here $\alpha = 6916$, $\beta = 4200$, $\gamma = 4845$ are the solutions to the following congruences respectively:

$$G_1 \equiv 0 \pmod{19} \equiv 0 \pmod{28} \equiv 1 \pmod{15},$$
$$G_2 \equiv 0 \pmod{15} \equiv 0 \pmod{28} \equiv 1 \pmod{19},$$
$$G_3 \equiv 0 \pmod{15} \equiv 0 \pmod{19} \equiv 1 \pmod{28}.$$

[14] B. L. VAN DER WAERDEN, *Geometry and Algebra in Ancient Civilization*, Universität Zürich, 1983, pp. 113–132.

7.2. SUN ZI's remainder problem had no astronomical content, but it was undoubtedly born out of astronomy. The proposition is called the Chinese Remainder Theorem because of its antiquity, together with its correct solution through detailed deduction by which one can solve other similar problems. However, it was only in embryo, and thus incomplete. Its deficiencies are

1. The solution was obtained by trial and error, without a general rule for a congruence of type (8).

2. There was only a numerical example, without a general rule for a system of congruences of type (1).

3. The moduli were restricted to natural, relatively prime numbers. No general cases were given. However, in daily life we often come across moduli of natural composites, decimals and fractions as well.

4. There was no further study such as to prove the propositions, to discuss the consistency of congruences, to reject the superfluous congruences, *etc.*

By joint efforts both in the East and the West, these questions have finally been solved completely.

7.2.1. Out of objective needs, QIN extended the fields of moduli to numbers other than natural, relatively prime numbers. Such problems appeared also in the Indian literature. However, they considered the question as it stood, without further discussion. QIN discussed different kinds of moduli and finally they were all converted into *dingshu*, provided that the converted system of congruences were equivalent to the original one. This operation was so important that mathematicians always paid much attention to it. GAUSS also studied the operation in II, 34. In fact by the fundamental theorem, of arithmetic, I, 16, he converted each of the moduli into a product of prime factors, and then rejected all the superfluous congruences. But QIN had obtained the same results without the concept of prime numbers 550 years before him. Theoretically, neither solution had any defect, but we should compare the two programs of computation by the example given in II, 34. There GAUSS solved the following process:

$$\begin{cases} z \equiv 17 \pmod{504} \\ z \equiv -4 \pmod{35} \\ z \equiv 33 \pmod{16} \end{cases} \rightarrow \begin{cases} z \equiv 17 \pmod{9} \\ z \equiv 17 \pmod{8} \\ z \equiv 17 \pmod{7} \\ z \equiv -4 \pmod{5} \\ z \equiv -4 \pmod{7} \\ z \equiv 33 \pmod{16} \end{cases} \rightarrow \begin{cases} z \equiv 17 \pmod{9} \\ z \equiv -4 \pmod{5} \\ z \equiv -4 \pmod{7} \\ z \equiv 33 \pmod{16} \end{cases}$$

By QIN's rule converting *yuanshu* 504, 35, 16 into *dingshu* 9, 35, 16, we have simply:

$$\begin{array}{ccccc} 504 & & 63 & 9 & \begin{cases} z \equiv -17 \pmod{504} \\ z \equiv -4 \pmod{35} \\ a \equiv 16 \pmod{16} \end{cases} \rightarrow \begin{cases} z \equiv 17 \pmod{9} \\ z \equiv -4 \pmod{35} \\ z \equiv 16 \pmod{16} \end{cases} \\ 35 & 35 & 35 & 35 & \\ 16 & 16 & 16 & 16 & \end{array}$$

If the moduli are enormous, it is inconventient to decompose them into prime factors, whereas by mutual division one may easily get the required results.

SEKI's algorithm for converting *yuanshu* into *dingshu* is better than QIN's: Failing in step 1, *i.e.* $d_2 > 1$, QIN had to go to $d_2' = 1$, while SEKI's algorithm remains the same way whether $d_2 = 1$ or not. Let us compare by numerical examples.

To find *dingshu* between 72, 54, by QIN's algorithm

$(72, 54) = 18$, $(54, 72/18) = (54, 4) = 2 > 1$, and again $(54/18, 72) = (3, 72) = 3 > 1$, whereas $(3\times 3, 72/3) = (9, 24) = 3 > 1$, and again $(3\times 3\times 3, 72/3\times 3) = (27, 8) = 1$. Finally we have the *dingshu* 27 and 8.

By SEKI's algorithm simply

$(72, 54) = 18$, $(54, 72/18) = (54, 4) = 2$, and $(54/2, 4\times 2) = (27, 8) = 1$; *dingshu* 27, 8 are obtained more promptly.

7.2.2. ARYABHATA published his work about a century after SUN ZI *suanjing*. He gave a general rule for solving the indeterminate equation (4), equivalent to congruence (8). Though the statements of *Kuttaka* were rather obscure, it provided the first attempt to solve such problems in general. Over the subsequent centuries, Indian mathematicians tried unremittingly to write commentaries to elucidate ARYABHATA'S words.

If the positive sign is taken. EULER'S and GAUSS' (II, 27) indeterminate equation $ax = by \pm 1$ is equal to (5), discussed by MAHAVIRA. They are all equivalent to congruence (8).

The Chinese mathematician QIN JIUSHAO in *Ssjz* gave the *Dayan qiuyi* rule, a complete solution of congruence (8). The program of the algorithm is in perfect order:

$$\frac{a}{b} = q_1 + \frac{1}{q_2} + \cdots + \frac{1}{q_n} + \frac{1}{q_{n+1}}.$$

In any continued fraction

$$q_1 + \frac{1}{q_2} + \cdots + \frac{1}{q_m} = \frac{l_m}{j_m}.$$

$$l_m = q_m l_{m-1} + l_{m-2},\quad j_m = q_m j_{m-1} + j_{m-2};$$

$$l_1 = q_1,\quad j_0 = 0,\quad j_1 = 1,$$

and

$$l_m j_{m-1} - l_{m-1} j_m = (-1)^m.$$

Under the conditions restricted by QIN, *i.e.*,

$$(a, b) = 1,\ r_n = 1,\ \text{where } n \text{ is odd},$$

therefore $l_{n+1} j_n - l_n j_{n+1} = 1$, and $l_{n+1} = a$, $j_{n+1} = b$. j_n is obviously the answer to congruence (8). This fact was pointed out by GAUSS in his first investigation, II, 27, of EULER'S algorithm, *Disquisitiones Arithmeticae*.

Moreover, LAGRANGE's treatment is exactly the same as QIN's.[15] Let us compare them.

LAGRANGE's Notation (11) $\alpha, \beta, \gamma, \ldots, \mu, n$	QIN's Rule (9) $q_1, q_2, q_3, \ldots, q_n, q_{n+1}$
Reconvert $\alpha + \frac{1}{\beta} + \frac{1}{\gamma} + \cdots + \frac{1}{n}$ into a common fraction; its denominator is the solution of (5)	$q_1 + \frac{1}{q_2} + \frac{1}{q_3} + \cdots + \frac{1}{q_n} + \frac{1}{q_{n+1}} = \frac{a}{b}$; $j_n = q_n j_{n-1} + j_{n-2}$ is the solution of (8)

The cases with the negative sign in equation $ax = by \pm 1$ were also successfully solved by QIN; see Example 5, Section 4.

The indeterminate analysis of *Kuttaka* is surprisingly similar to QIN's rule. MAHAVIRA's new idea is fascinating. Solving equation (5) in MAHAVIRA's way, we discover that *Kuttaka* is equivalent to the *Dayuan qiuyi* Rule:

No.	MAHAVIRA's formula (6)		QIN's rule (9)	
	quotient	k	quotient	j_i
2	q_n	$k_2 = q_n k_1 + k_0$	q_2	$j_2 = q_2 j_1 + j_0$
3	q_{n-1}	$k_3 = q_{n-1} k_2 + k_1$	q_3	$j_3 = q_3 j_2 + j_1$
...	...	...	...	...
i	q_{n+2-i}	$k_i = q_{n+2-i} k_{i-1} + k_{i-2}$	q_i	$j_i = q_i j_{i-1} + j_{i-2}$
...	...	...	...	...
$n-1$	q_3	$k_{n-1} = q_3 k_{n-2} + k_{n-3}$	q_{n-1}	$j_{n-1} = q_{n-1} j_{n-2} + j_{n-3}$
n	q_2	$k_n = q_2 k_{n-1} + k_{n-2}$	q_n	$j_n = q_n j_{n-1} + j_{n-2}$

Let us prove $k_n = j_n$. First of all, $k_n = j_h k_{n-h+1} + j_{h-1} k_{n-h}$, where $2 \leqq h \leqq n = 2m - 1$. By mathematical induction if $h = 2$, it is true, for $k_n = j_2 k_{n-1} + j_1 k_{n-2} = q_2 k_{n-1} + k_{n-2}$. If $h = i$ is true, then $h = i + 1$ is also true, for

$$\begin{aligned} k_n &= j_i k_{n-i+1} + j_{i-1} k_{n-i} \\ &= j_i (q_{(n+2)-(n-i+1)} k_{n-i} + k_{n-i-1}) + j_{i-1} k_{n-1} \\ &= (j_i q_{i+1} + j_{i-1}) k_{n-i} + j_i k_{n-i-1} \\ &= j_{i+1} k_{n-i} + j_i k_{n-i-1}. \end{aligned}$$

Especially, if $h = n$, $k_n = j_n k_1 + j_{n-1} k_0 = j_n$. Q.E.D.

[15] Here n is odd and $r_n = 1$.

The *Dayan qiuyi* Rule has its advantages. To solve equation (5) by *Kuttaka* one would apply different formulas according as n is odd or even. However, by the *Dayan quiyi* Rule we can easily have the answer by unique algorithm whether n is odd or even.[16]

It is interesting that the order of the quotients in EULER's notation (10) is the same as that of MAHAVIRA's (6) and is the inverse of QIN's (5). This fact was mentioned by GAUSS in his second investigation, II, 27, of *Disquisitiones Arithmeticae*, concerning EULER's algorithm.

7.2.3. QIN gave a complete and systematic process for solving a system of congruences of first degree, just as in the *Disquisitiones Arithmeticae*, 1801. It should be mentioned that GAUSS' work in II, 36 is just like SUN ZI's formulas (2′) and (3′). Moreover, the proceedings given by GAUSS in II, 32 are exactly what Indian mathematicians used in medieval times; see Section 3.3.

7.2.4. At last GAUSS in his *Disquisitiones Arithmeticae* finished the relevant tasks:

The proof of Proposition (2′), (3′), given by SUN ZI; see II, 36.

The proof of equivalence of systems of congruences when the moduli are converted into *dingshu*; see II, 34.

The proof of the *Dayan qiuyi* Rule, by citation of EULER's and LAGRANGE's results, II, 27 and II, 28.

The condition for solvability of a congruence; see II, 27.

The condition for solvability of a system of congruences; see II, 34.

The solutions of a system of congruences remains unchanged after rejecting the superfluous congruences; see II, 34.

7.3. It is hard to judge the actual exchanges between nations over so long a historical period, 4th–18th centuries. Indian mathematicians, BRAHMAGUPTA and BHASKARA had been in Ujjain, where XUAN ZHANG [u] and other Chinese envoys lived for years, and intercultural overflows would have been inevitable. The complexity of transmission is an interesting problem which has to be discussed further.

As we know, Chinese mathematicians have exerted a great influence upon the Japanese since the 6th century, A.D. It is interesting that SEKI TAKAKAZU had not read QIN's book, which was not published until 1842. SEKI's achievement in the field of congruences was his independent work. However, SEKI is said[17] to have transcribed *Xu gu zha qi suanfa* in 1661, so no doubt his work was somewhat influenced by YANG HUI.

EULER, LAGRANGE and GAUSS presented their achievements in indeterminate analysis in the 18th century, published respectively by the Academy of St. Petersburg, the Academy of Berlin, and the Göttingen Society of Sciences. GAUSS introduced his new discoveries in Chapters I & II of his famous treatise. Obviously,

---

[16] $r_n = 1$, $r_{n+1} = r_{n-1} - q_{n+1}r_n = 0$, if n is even. Continue the algorithm, and let $r'_{n+1} = r_{n+1}$, whereas $r'_{n+1} = r_{n-1} - r_n(q_{n+1} + 1) = 1$; here $n + 1$ is odd.

[17] Japanese Academy of Sciences, *History of Japanese Mathematics*, 1979, Tokyo, p. 172, vol. II.

at that time Europeans considered their results in mathematics unique and very significant. They did not know that they had been completely solved in the East at least several hundred years earlier.

Acknowledgement. Mr. WANG ZIGUANG read the paper for clarity and correctness of English usage.

Glossary

a	景初	b	上元
c	孙子算经	d	杨辉
e	续古摘奇算法	f	大衍求一
g	数书九章	h	秦九韶
i	宋	j	元数
k	收数	l	通数
m	复数	n	定数
o	天元	p	乘率
q	开禧	r	诸约之术
s	关孝和	t	括要算法
u	玄奘	v	甲子

Department of Mathematics
Hangzshou University

(Received June 1, 1987)