Ch'in Chiu-shao and the Chinese Remainder Theorem* –

Lam Lay Yong
University of Singapore

Ch'in Chiu-shao[a]

Ch'in Chiu-shao was born about 1202 in Szechuan province and his work, the Shu-shu chiu-chang[b] (Mathematical Treatise in Nine Sections), was published in 1247. The thirteenth century was a period which marked the culminating point in the development of mathematics in China. It was also a period of political strife and decline when China was fighting for her very survival against the Mongols. Against this background of political unrest, mathematics flourished and Ch'in stood out as the first of four great mathematicians, all living in the same half-century. The other three were Chu Shih-chieh[c] (a wand ering teacher), Yang Hui[d] (a civil servant) and Li Yeh[e] (a recluse scholar).

What was a mathematician in those times? In the first place, the starting point of mathematics was at a very high level. Since the compilation of the Chiu-chang suan-shu[f] (Nine Chapters on the Mathematical Art) in the first century, this work had significant influence on Chinese mathematics up to and beyond the thirteenth century. A Chinese mathematician was primarily a technologist who was able to solve a variety of practical problems in the fields of chronology and astronomy, or in the fields of financial affairs, taxation, architecture, military problems and so forth, and this determined his social role. On the

---

*This is the text of a public lecture delivered on 25 April 1975.

other hand, mathematics of a very simple kind was one of the essential accomplishments of the post-Confucian gentleman on the same level as propriety, music, archery, charioteering and calligraphy.

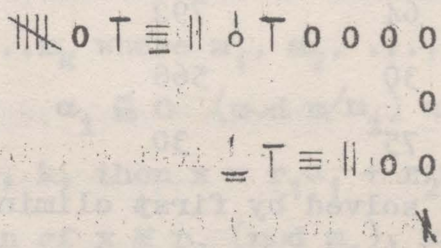
Ch'in Chiu-shao studied at the Board of Astronomy in Hangchow. This was rather exceptional, and perhaps explained why he dealt with calendrical problems and why the remainder problem was preserved. In relation to astronomy and calendrical science, mathematics, at that time, was considered the servant to the more important sciences of the heaven. Ch'in was never an official mathematician, though it was said that someone recommended him to the emperor on account of his knowledge of the calendrical science.

Ch'in, in George Sarton's judgement, was 'one of the greatest mathematicians of his race, of his time and indeed of all times'. In his youth, Ch'in was an army officer and was noted both for athletic and literary achievements. He later rose to the rank of Governor in two cities. He has often been described as of an intriguing and unprincipled character. In love affairs he had a reputation similar to Avicenna. Liu K'e-chuang[g], in a petition to the emperor, described him 'as violent as a tiger or a wolf, and as poisonous as a viper or a scorpion'.

The Shu-shu chiu-chang

The Shu-shu chiu-chang consists of nine sections, the first being the indeterminate analysis, where the remainder problem lies; the second section involves astronomical, calendrical and meteorological calculations and the third is on land measurement. The fourth section refers to surveying by the method of triangulation; while the fifth is on land tax and state service, and the sixth concerns problems on money and grains. The seventh and eighth sections deal with structural works and military matters respectively, and the last section is on barter and purchase.

Ch'in represented algebraic equations by placing calculating rods on the counting board so that the absolute term appeared on the top in a vertical column; immediately below it was the coefficient of the unknown quantity, followed by the coefficients of the increasing powers of the unknown quantity. For example, the equation $-x^4 + 763,200x^2 - 40,642,560,000 = 0$ is represented by calculating rods placed on a counting board as follows:



Originally, Ch'in used red and black counting rods to represent positive and negative quantities respectively, but in the text, negative quantities are denoted by an extra rod placed obliquely over the first figure of the number concerned.

The <u>Shu-shu chiu-chang</u> is the oldest existing Chinese mathematical text to contain the zero symbol. There are more than twenty problems in the book involving the setting up of numerical equations which include one of the tenth degree, namely,

$$x^{10} + 15x^8 + 76x^6 - 864x^4 - 11,664x^2 - 34,992 = 0.$$

The method employed for solving these equations is identical to that rediscovered by Paolo Ruffini about 1805 and W.G. Horner in 1819.

Formulae giving the areas of various types of geometrical figures are mentioned in the Shu-shu chiu-chang, although some of them are not very accurate. Problems involving series and progressions are also dealt with. Linear simultaneous equations are discussed with the numbers set up in vertical columns; for example, the system of equations

$$(1) \qquad 140x + 88y + 15z = 58,800$$

$$(2) \qquad 792x + 568y + 815z = 392,000$$

$$(3) \qquad 64x + 30y + 75z = 29,400$$

is set up on the counting board as follows.

29400	392000	58800
64	792	140
30	568	88
75	30	15 .

The equations are solved by first eliminating z in equations (1) and (3), and then in (2) and (3). From these, x and y are obtained, and finally z is found by substituting the values of x and y in (3). In a recent work, Ulrich Libbrecht shows that one of Ch'in's methods of solving a set of linear equations resembles Cramer's rule (eighteenth century).

The Chinese Remainder Theorem

The Chinese remainder theorem states that the system of linear congruences $x \equiv r_1 \pmod{m_1}$, $x \equiv r_2 \pmod{m_2}$, ..., $x \equiv r_k \pmod{m_k}$ such that $m_1, m_2, \ldots, m_k$ are coprime in pairs, has integral solutions x, and the solution is unique modulo $m_1 m_2 \ldots m_k$.

This theorem may be illustrated by a simple problem, which is the oldest existing remainder problem, from Sun Tzu suan-ching[h] (Sun Tzu's Mathematical Manual) (fourth century). The problem states: what is the number which when divided by 3 gives 2 as remainder, when divided by 5 gives 3 as remainder and when divided by 7 gives 2 as remainder? In modern notations,

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

The Sun Tzu suan-ching gives the solution as

$$x = 2\times70 + 3\times21 + 2\times15 - 2\times105 = 23.$$

This problem became known in Europe through Alexander Wylie's article 'Jottings on the science of Chinese arithmetic' in 1852. Sun Tzu's rule was pointed out by Matthiessen to be identical to Gauss's statement (1801):

If $m = m_1 m_2 \ldots m_k$ where $m_1, m_2, \ldots, m_k$ are coprime in pairs and if $\alpha_i \equiv 0 \pmod{m/m_i}$ and $\alpha_i \equiv 1 \pmod{m_i}$, $i = 1, 2, \ldots, k$, then $x = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_k\alpha_k$ is a solution of $x \equiv r_1 \pmod{m_1}$, $x \equiv r_2 \pmod{m_2}$, $\ldots$, $x \equiv r_k \pmod{m_k}$.

The remainder problem reaches its zenith in the work of Ch'in Chiu-Shao. There are ten remainder problems in his Shu-Shu Chiu-Chang. The text is largely obscure and no explanations are given for the steps taken. Below is one of Ch'in's problems, the statement and working of which are simplified by the use of modern notations.

1. $x \equiv r_1 \pmod{m_1}$	$x \equiv 10 \pmod{12}$
$\equiv r_2 \pmod{m_2}$	$\equiv 0 \pmod{11}$
$\equiv r_3 \pmod{m_3}$	$\equiv 0 \pmod{10}$
$\equiv r_4 \pmod{m_4}$	$\equiv 4 \pmod{9}$
$\equiv r_5 \pmod{m_5}$	$\equiv 6 \pmod{8}$
$\equiv r_6 \pmod{m_6}$	$\equiv 0 \pmod{7}$
$\equiv r_7 \pmod{m_7}$	$\equiv 4 \pmod{6}$

[Note that 12, 11, 10, 9, 8, 7, 6 are not coprime in pairs.]

2. $12 = 2^2 \times 3$ $\mu_1 = 1$ $x \equiv 10 \pmod{1}$

$11 = 11$ $\mu_2 = 11$ $\equiv 0 \pmod{11}$

$10 = 2 \times 5$ $\mu_3 = 5$ $\equiv 0 \pmod{5}$

$9 = 3^2$ $\mu_4 = 9$ $\equiv 4 \pmod{9}$

$8 = 2^3$ $\mu_5 = 8$ $\equiv 6 \pmod{8}$

$7 = 7$ $\mu_6 = 7$ $\equiv 0 \pmod{7}$

$6 = 2 \times 3$ $\mu_7 = 1$ $\equiv 4 \pmod{1}$

[Note that 1, 11, 5, 9, 8, 7, 1 are coprime in pairs and l.c.m. (12, 11, 10, 9, 8, 7, 6) = l.c.m. (1,11,5,9,8,7,1). This is a necessary condition for all of Ch'in's problems. The set of congruences in (2) is equivalent to the set of congruences in (1).]

3. $\theta = \mu_1\mu_2 \ldots \mu_7 = 11 \times 5 \times 9 \times 8 \times 7 = 27{,}720.$

4. $\theta/\mu_1 = M_1 = \mu_2\mu_3\mu_4 \ldots \mu_7 = 11 \times 5 \times 9 \times 8 \times 7 \times 1 = 27{,}720$

$\theta/\mu_2 = M_2 = \mu_1\mu_3\mu_4 \ldots \mu_7 = 1 \times 5 \times 9 \times 8 \times 7 \times 1 = 2{,}520$

$\theta/\mu_3 = M_3 = \mu_1\mu_2\mu_4 \ldots \mu_7 = 1 \times 11 \times 9 \times 8 \times 7 \times 1 = 5{,}544$

$\theta/\mu_4 = M_4 = \ldots \ldots = 1 \times 11 \times 5 \times 8 \times 7 \times 1 = 3{,}080$

$\theta/\mu_5 = M_5 = \ldots \ldots = 1 \times 11 \times 5 \times 9 \times 7 \times 1 = 3{,}465$

$\theta/\mu_6 = M_6 = \ldots \ldots = 1 \times 11 \times 5 \times 9 \times 8 \times 1 = 3{,}960$

$\theta/\mu_7 = M_7 = \ldots \ldots = 1 \times 11 \times 5 \times 9 \times 8 \times 7 = 27{,}720$

5. $N_1 = M_1 - p_1\mu_1 = 27{,}720 - 27{,}720 \times 1 = 0$

$N_2 = M_2 - p_2\mu_2 = 2{,}520 - 229 \times 11 = 1$

$N_3 = M_3 - p_3\mu_3 = 5{,}544 - 1{,}108 \times 5 = 4$

$N_4 = M_4 - p_4\mu_4 = 3{,}080 - 342 \times 9 = 2$

$N_5 = M_5 - p_5\mu_5 = 3{,}465 - 433 \times 8 = 1$

$N_6 = M_6 - p_6\mu_6 = 3{,}960 - 565 \times 7 = 5$

$N_7 = M_7 - p_7\mu_7 = 27{,}720 - 27{,}720 \times 1 = 0$

[Note that $p_i\mu_i$ is the largest possible multiple of μ_i such that N_i is the smallest non-negative integer.]

6. $a\times 0 \quad 1 \pmod{1}, \qquad a = 0$

$b\times 1 \quad 1 \pmod{11}, \qquad b = 1$

$c\times 4 \quad 1 \pmod{5}, \qquad c = 4$

$d\times 2 \quad 1 \pmod{9}, \qquad d = 5$

$e\times 1 \quad 1 \pmod{8}, \qquad e = 1$

$f\times 5 \quad 1 \pmod{7}, \qquad f = 3$

$g\times 0 \quad 1 \pmod{1}, \qquad g = 0$

7. $\alpha_1 = aM_1 = 0$

$\alpha_2 = bM_2 = 2{,}520$

$\alpha_3 = cM_3 = 22{,}176$

$\alpha_4 = dM_4 = 15{,}400$

$\alpha_5 = eM_5 = 3{,}465$

$\alpha_6 = fM_6 = 11{,}880$

$\alpha_7 = gM_7 = 0$

8. $\beta_1 = \alpha_1 r_1 = 0$

$\beta_2 = \alpha_2 r_2 = 0$

$\beta_3 = \alpha_3 r_3 = 0$

$\beta_4 = \alpha_4 r_4 = 61{,}600$

$\beta_5 = \alpha_5 r_5 = 20{,}790$

$\beta_6 = \alpha_6 r_6 = 0$

$\beta_7 = \alpha_7 r_7 = 0$

9. $x = 61{,}600 + 20{,}790 = 82{,}390$, or

$x = 82{,}390 - 2\times 27{,}720 = 26{,}950$.

In Europe, the first treatment of the remainder problem in which the moduli are not coprime in pairs was given by Lebesque in 1859. T.J. Stieltjes published a profound article on it in 1890. In order to establish the validity of Ch'in's method of solving the remainder problem, Kurt Mahler wrote a paper in 1957 in which he proved the general form of the Chinese remainder theorem based on Ch'in's method. This result states that the system of linear congruences $x \equiv r_i \pmod{m_i}$, $i = 1, 2, \ldots, k$, has integral solutions x if and only if g.c.d.(m_i, m_j) divides $(r_i - r_j)$ for all pairs i, j $(i \neq j)$.

In India, Brahmagupta (seventh century) and Bhaskara (twelfth century) employed the kuttaka method to investigate the remainder problem. In the Islamic world, Ibn al-Haitham also investigated this type of problem and he might have influenced Leonardo Pisano of Italy. After the thirteenth century, there was not much further development on the subject in China, India and the Islamic world, but from the fifteenth century onwards, there was a marked increase in European research, which reached its apogee in the studies of Lagrange, Euler and Gauss.

References

1. Ch'in Chiu-shao. Shu-shu chiu-chang (Mathematical Treatise in Nine Sections), 1247. T'sung-shu chi-ch'eng[i], Commercial Press, Shanghai, 1936.
2. Dickson, L.E. History of the Theory of Numbers. 3 vols., New York, 1934.
3. Ho Peng Yoke. 'Ch'in Chiu-shao'. In Dictionary of Scientific Biography (in press).
4. Libbrecht, U. Chinese Mathematics in the Thirteenth Century. The Shu-shu chiu-chang of Ch'in Chiu-shao. MIT Press, 1973.
5. Mahler, K. 'On the Chinese Remainder Theorem'. Mathematische Nachrichten 18 (1958), 120.
6. Needham, J. Science and Civilisation in China. 7 vols., Cambridge, 1954 - .

7. Sarton, G. Introduction to the History of Science. 3 vols., Baltimore, 1927 - 1947 (Carnegie Institution Publ. no. 376).

Glossary

a. 秦九韶 f. 李冶

b. 数書九章 g. 刘克莊

c. 朱世傑 h. 孫子算经

d. 楊輝 i. 叢書集成

e. 九章算術

— ** ** —

The advance of science is not comparable to the change of a city, where old edifices are pitilessly torn down to give place to new, but to the continuous evolution of zoologic types which develop ceaselessly and end by becoming unrecognizable to the common sight, but where an expert eye finds always traces of the prior work of past centuries.

\- Henri Poincaré.