The Chinese Remainder Theorem

(a) Suppose that the positive integers $m_1, m_2, \ldots, m_k$ are pairwise coprime; in other words $\text{hcf}(m_i, m_j)=1$ for all i, j where $i \neq j$, where hcf denotes the highest common factor. Then the set of congruences

$$x \equiv r_i \pmod{m_i} \quad \text{for } i = 1, 2, \ldots k \qquad (*)$$

has a unique common solution modulo M where $M = m_1 m_2 \ldots m_k$.

Set

$$M = m_1 M_1 = m_2 M_2 = \ldots = m_k M_k$$

Since M_i and m_i are coprime we can find integers $\mu_1, \mu_2, \ldots, \mu_k$ such that $M_1\mu_1 \equiv 1 \pmod{m_1}$, $\ldots$, $M_k\mu_k \equiv 1 \pmod{m_k}$ and the general solution of $(*)$ is

$$x \equiv M_1\mu_1 r_1 + M_2\mu_2 r_2 + \ldots + M_k\mu_k r_k \pmod{M} \qquad (**)$$

(b) More generally, a necessary and sufficient condition for the system of simultaneous congruences $(*)$ to be soluble is that

$$r_i - r_j \equiv 0 \pmod{\text{hcf}(m_i, m_j)}$$

for all pairs i, j with $i \neq j$.

(c) If condition (b) is satisfied, it is always possible to replace the original set $(*)$ of congruences by another equivalent set of simultaneous linear congruences

$$x \equiv r_i \pmod{m_i'}$$

the moduli of which are pairwise coprime. Then, for all i, $1 \leq i \leq k$, m_i' divides m_i and $\text{lcm}(m_1', \ldots, m_k') = \text{lcm}(m_1, \ldots, m_k)$, where lcm denotes the least common multiple.

A proof of (a) appears in almost every book on elementary number theory. (b) is dealt with, for example, in K. Malher, "On the Chinese Remainder Theorem," *Mathematische Nachrichten*, 1958, vol. 18, pp. 120–122 and in A. S. Fraenkel, "New Proof of the Generalized Chinese Remainder Theorem," *Proc. Am. Math. Soc.*, 1963, vol. 14, no. 4, pp. 790–791. A constructive proof of (c) akin to Qin Jiushao's original algorithm (i.e. relying only on the computation of hcfs and not on prime number decompositions) is contained in R. J. Stieltjes, *1918, Oeuvres Complètes*, Groningen: P. Noordhoff, vol. II, p. 280 ff. and p. 295 ff.

This is a special case of the Chinese remainder theorem. Stating that the system admits an infinity of solutions. Ibn al-Haytham proposes two methods of resolution. The first of these is

$$x = (p-1)! + 1$$

and the fact that it gives a solution of the above system is a consequence of Wilson's theorem, a theorem in fact established by Ibn al-Haytham[16] (Wilson's theorem asserts that

$$(p-1)! \equiv -1 \pmod{p}$$

for any prime p).

Finally, we note that Leonardo Fibonacci's *Liber Abaci* (1202) also contains Sunzi's problem, formulated with the same moduli and the same resolutory rule.[17]

We shall not continue the long enumeration of all the sources from the Middle Ages to the modern period which mention this problem; instead, we refer readers to the very detailed studies by Libbrecht (2), *1973*, p. 214 ff. and Tropfke (3), *1980*, p. 636.

Qin Jiushao's General *dayan* Rule *dayan zongshu shu*

The expression *dayan zongshu shu* (General *dayan* rule) is the name of the general rule for solving systems of simultaneous congruences which is to be found immediately after the statement of and answer to the first problem of chapter 1 of the *Shushu jiuzhang*.

Exactly as in the previous case, this rule is intended for solving problems similar to that of Sunzi (system of simultaneous congruences) but with a totally different degree of complexity and sophistication to that of Sunzi's problem. As, U. Libbrecht wrote:

> The only progress [with respect to Sunzi's rule] [...] was the *ta-yen* [*dayan*] rule of Ch'in-Chiu shao. We should not underestimate this revolutionary advance, because from this single remainder problem, we come at once to the general procedure for solving the remainder problem, even more advanced (from the algorithmical point of view) than Gauss's method, and there is not the slightest indication of gradual evolution.[18]

The nine artificial problems described by Qin Jiushao involve divination, the calendar, finances, military logistics, architecture and excavation work. These problems are factually very intricate.

The *dayan* rule is itself complex. This complexity relates partly to the length of the rule and partly to the nesting of the sub-rules which compose it.[19]

[16] Rashed (1), *1984*, pp. 227 ff.

[17] Libbrecht, op. cit., p. 236 ff.

[18] Libbrecht (1), *1972*, p. 183; Tropfke (3), *1980*.

[19] Partial translation of the rule in Libbrecht (2), *1973* pp. 328 ff.

Jean-Claude Martzloff

A HISTORY OF *Chinese Mathematics*

Springer