On the Chinese Remainder Theorem

To Prof. H. L. SCHMID

Von KURT MAHLER in Manchester

(Eingegangen am 20. 8. 1957)

Textbooks on elementary number theory discuss, under the name of Chinese Remainder Theorem, the well-known method für solving systems of linear congruences

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

when the moduli m_i are relatively prime in pairs. This method (naturally not in the modern notation) occurs in the Sun Tzu Suan Ching of the 4th century A. D. and the Chang Chiu-Chien Suan Ching (ca. 475 A. D.). It was used particularly by the astronomer-monk I-Hsing (682—727). The reader is referred to Dickson's History of the Theory of Numbers, and especially to the third volume of „Science and Civilisation in China" by Needham and Wang, which will appear shortly and contain the mathematical sections.

Chinese texts treat also the more general case when the moduli m_i are not prime in pairs. It is not quite easy to understand these very short passages because, as usual, only problems and short rules how to solve them are given, while there is no proof or any clear statement of conditions on the r_i or m_i. I am trying in this note to reproduce what I believe is the mathematical content of this old Chinese method. This method is entirely different from that in Gauss's Disquisitiones Arithmeticae, and I cannot remember finding it in Western books.

1. The general form of the Chinese Remainder Theorem states:

Theorem. *The system of linear congruences*

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

has integral solutions x if and only if

(2) $$(m_i, m_j) \mid r_i - r_j \text{ for all pairs } i, j \text{ with } i \neq j.$$

That the condition (2) is necessary is obvious. For put

$$d_{ij} = (m_i, m_j), \text{ so that } d_{ij} \mid m_i,\ d_{ij} \mid m_j.$$

Then

$$x \equiv r_i \pmod{d_{ij}} \quad \text{and} \quad x \equiv r_j \pmod{d_{ij}},$$

hence

$$0 = x - x \equiv r_i - r_j \pmod{d_{ij}}.$$

It is rather more difficult to show that condition (2) is also sufficient. The Chinese contribution consists here in the following result, where *Lcm* denotes the Least Common Multiple.

Lemma 1. *Let the condition* (2) *be satisfied, and let* $\mu_1, \ldots, \mu_k$ *be integers such that*

$$(3) \qquad \mu_i \mid m_i \qquad (i = 1, 2, \ldots, k),$$

$$(4) \qquad Lcm(\mu_1, \ldots, \mu_k) = Lcm(m_1, \ldots, m_k).$$

Then every solution x *of*

$$(5) \qquad x \equiv r_i \pmod{\mu_i} \qquad (i = 1, 2, \ldots, k)$$

also satisfies the congruences (1).

Proof. Denote by $p_1, \ldots, p_t$ the distinct prime factors of $m_1, \ldots, m_k$, by

$$(6) \qquad m_i = p_1^{a_{i1}} \ldots p_t^{a_{it}} \qquad (i = 1, 2, \ldots, k)$$

the prime factorizations of the moduli m_i, and by

$$(7) \qquad \mu_i = p_1^{\alpha_{i1}} \ldots p_t^{\alpha_{it}} \qquad (i = 1, 2, \ldots, k)$$

those of the moduli μ_i. The exponents $a_{i\tau}$ and $\alpha_{i\tau}$ are thus non-negative integers. By the hypotheses (3) and (4),

$$(8) \qquad 0 \leqq \alpha_{i\tau} \leqq a_{i\tau} \qquad (i = 1, 2, \ldots, k;\ \tau = 1, 2, \ldots, t),$$

and

$$(9) \qquad \max_{i=1,2,\ldots,k} a_{i\tau} = \max_{i=1,2,\ldots,k} \alpha_{i\tau} \qquad (\tau = 1, 2, \ldots, t).$$

Put therefore

$$(10) \qquad a_\tau = \max_{i=1,2,\ldots,k} a_{i\tau} = \max_{i=1,2,\ldots,k} \alpha_{i\tau} \qquad (\tau = 1, 2, \ldots, t).$$

Then

$$(11) \qquad Lcm(\mu_1, \ldots, \mu_k) = Lcm(m_1, \ldots, m_k) = p_1^{a_1} \cdots p_t^{a_t}.$$

Further denote by i_τ for each $\tau = 1, 2, \ldots, t$ a suffix $1, 2, \ldots, k$ such that

$$(12) \qquad \alpha_{i_\tau \tau} = a_\tau \quad \text{and hence also } a_{i_\tau \tau} = a_\tau$$

because of (8) and (10).

The two systems of k congruences (1) and (5) are equivalent to the two systems of kt congruences

$$(13) \qquad x \equiv r_i \pmod{p_\tau^{a_{i\tau}}} \qquad (i = 1, 2, \ldots, k;\ \tau = 1, 2, \ldots, t)$$

and

(14) $$x \equiv r_i \,(\mathrm{mod}\, p_\tau^{\alpha_{i\tau}}) \qquad (i = 1, 2, \ldots, k;\ \tau = 1, 2, \ldots, t),$$

respectively. The assertion is therefore proved if it can be shown that each of the t systems of k congruences

(15) $$x \equiv r_i \,(\mathrm{mod}\, p_\tau^{a_{i\tau}}) \qquad (i = 1, 2, \ldots, k;\ \tau \text{ fixed})$$

and

(16) $$x \equiv r_i \,(\mathrm{mod}\, p_\tau^{\alpha_{i\tau}}) \qquad (i = 1, 2, \ldots, k;\ \tau \text{ fixed})$$

is equivalent to one and the same single congruence

(17) $$x \equiv r_{i_\tau} (\mathrm{mod}\, p_\tau^{a_\tau}).$$

This can be done as follows. First, the congruence (17) is that element of both systems (15) and (16) which belongs to the suffix $i = i_\tau$, and hence both (15) and (16) imply (17).

Secondly, let x be any solution of (17). Then

$$x \equiv r_{i_\tau} (\mathrm{mod}\, p_\tau^{a_{i_\tau \tau}}),$$

so that

$$x \equiv r_i + (r_{i_\tau} - r_i) \,(\mathrm{mod}\, p_\tau^{a_{i_\tau \tau}}), \ \equiv r_i \,(\mathrm{mod}\, p_\tau^{a_{i\tau}}) \qquad (i = 1, 2, \ldots, k),$$

because

$$a_{i\tau} \leqq a_{i_\tau \tau} \text{ and } p_\tau^{a_{i\tau}} = (p_\tau^{a_{i\tau}},\ p_\tau^{a_{i_\tau \tau}}) \mid r_{i_\tau} - r_i$$

from the hypothesis. Hence (17) implies (15), and by the same reasoning it also implies (16). This concludes the proof.

2. Lemma 2. *The moduli* $\mu_1, \ldots, \mu_k$ *of Lemma* 1 *may be chosen such that*

(18) $$(\mu_i, \mu_j) = 1 \quad \textit{if} \quad i \neq j.$$

Proof. Select for each $\tau = 1, 2, \ldots, t$ a suffix j_τ such that

(19) $$a_{j_\tau \tau} = a_\tau.$$

Further put

(20) $$\alpha_{i\tau} = \begin{cases} a_\tau & \text{if} \quad i = j_\tau \\ 0 & \text{if} \quad i \neq j_\tau \end{cases} \qquad (\tau = 1, 2, \ldots, t)$$

and define $\mu_1, \ldots, \mu_k$ by (7). Then these moduli satisfy all the conditions (3), (4), and (18).

3. The Theorem follows now at once from Lemmas 1 and 2 and from the classical case of the Chinese Remainder Theorem when (18) holds. It becomes also clear that in the general case the solutions x of (1) lie in a unique residue class modulo $Lcm\,(m_1, \ldots, m_k)$.