NEW PROOF OF THE GENERALIZED CHINESE REMAINDER THEOREM

AVIEZRI S. FRAENKEL

THEOREM. *A necessary and sufficient condition that the system of congruences* $x \equiv r_i \pmod{m_i}$, $i=1, 2, \cdots, s$ *be solvable is that* $r_i - r_j \equiv 0 \pmod{(m_i, m_j)}$, $1 \leqq i < j \leqq s$. *Any two solutions are congruent* mod $[m_1, m_2, \cdots, m_s]$.

PROOF.[1] The necessity is clear. For proving the sufficiency, let $M_0 = 1$, $M_i = [m_1, m_2, \cdots, m_i]$, $i \geqq 1$. Every integer N in the range $0 \leqq N < M_s$ is uniquely representable in the form $N = a_1 M_0 + a_2 M_1 + \cdots + a_s M_{s-1}$, $0 \leqq a_i < M_i / M_{i-1}$.

The congruence $a_1 M_0 \equiv r_1 \pmod{m_1}$ has a solution a_1 with $0 \leqq a_1 < m_1$. Assume that a_i has already been found as a solution of $a_1 M_0 + a_2 M_1 + \cdots + a_i M_{i-1} \equiv r_i \pmod{m_i}$, for all $i < n$. The congruence $a_1 M_0 + a_2 M_1 \cdots + a_n M_{n-1} \equiv r_n \pmod{m_n}$ is solvable for a_n if and only if[2] $c_n - r_n \equiv 0 \pmod{(M_{n-1}, m_n)}$, where $c_n = a_1 M_0 + a_2 M_1 + \cdots + a_{n-1} M_{n-2}$. Now $c_n \equiv r_i \pmod{m_i}$, and hence

$$c_n - r_n \equiv 0 \ (\mathrm{mod}(m_i, m_n)), \qquad i = 1, 2, \cdots, n-1,$$

by the hypothesis. Thus

$$c_n - r_n \equiv 0 \ (\mathrm{mod}[(m_1, m_n), (m_2, m_n), \cdots, (m_{n-1}, m_n)]).$$

Since[3] $[(m_1, m_n), (m_2, m_n), \cdots, (m_{n-1}, m_n)] = (M_{n-1}, m_n)$, an integer a_n with $0 \leqq a_n < M_n / M_{n-1}$ is uniquely determined, and thus N is determined.[4] If N_1 is any integer satisfying $N_1 \equiv r_i \pmod{m_i}$, $i = 1, 2, \cdots, s$, then $N_1 \equiv N \pmod{M_s}$, and the proof is complete.

NOTE. The necessity part was already established by the priest Yih-hing in the eighth century. Stieltjes proved both the necessity and sufficiency of the condition. For these and related references, see [**2**, pp. 57–64]. An existence proof is given in [**4**, Theorem 3–12, p. 34]. The solution which is produced in the conventional proof of the Chinese Remainder Theorem (i.e., the case $(m_i, m_j) = 1$ for $i \neq j$), is only an equivalence class; it is not known a priori in which interval of two consecutive multiples of M_s the solution will be found. The

Received by the editors June 16, 1962.

[1] References are given in the footnotes for the sake of the nonspecialist reader.

[2] See e.g. [**4**, Theorem 3–10, p. 32].

[3] See e.g. [**4**, problem 2, p. 23].

[4] The upper bound for a_n follows from the identity

$$m_n/(M_{n-1}, m_n) = [M_{n-1}, m_n]/M_{n-1} = M_n/M_{n-1}.$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

feature of the present proof is that a solution N is produced which is always in the range $0 \leqq N < M_t$. This is important in some applications, for example, in modular computation [**4**], which is a Chinese Remainder problem. Another application concerning the sieve problem [**1**; **3**] seems possible.

References

1. D. G. Cantor, G. Estrin, A. S. Fraenkel and R. Turn, *A very high-speed digital number sieve*, Math. Comp. **16** (1962), 141–154.

2. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, pp. 57–64.

3. D. H. Lehmer, *The sieve problem for all-purpose computers*, Math. Comp. **7** (1953), 6–14.

4. W. J. LeVeque, *Topics in number theory*, Vol. 1, Addison-Wesley, Reading, Mass., 1956.

5. H. B. Mann, *On modular computation*, Math. Comp. **15** (1961), 190–192.

University of Oregon and
Weizmann Institute of Science, Rehovot, Israel

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use