

**NEW FORM OF CHINESE REMAINDER THEOREM WHEN
THE RESTRICTIONS ARE OF GENERALISED FORM**

By

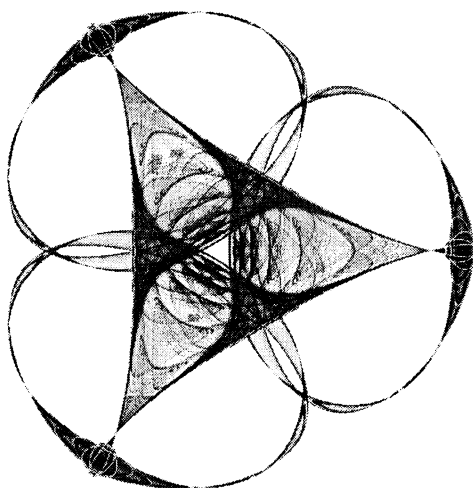
Anand Singh

and

H.S. Dhami

IMA Preprint Series # 1685

(February 2000)



INSTITUTE FOR MATHEMATICS AND ITS APPLICATIONS

UNIVERSITY OF MINNESOTA

514 Vincent Hall

206 Church Street S.E.

Minneapolis, Minnesota 55455-0436

Phone: 612/624-6066 Fax: 612/626-7370

URL: <http://www.ima.umn.edu>

NEW FORM OF CHINESE REMAINDER THEOREM WHEN THE RESTRICTIONS ARE OF GENERALISED FORM

ANAND SINGH & H.S. DHAMI

Department of mathematics, Govt. M.B.P.G. College, Haldwani & Almora Campus Almora.

KEY WORDS : Linear congruences / Relatively Prime / Modulo / Incongruent.

ABSTRACT

In the present paper an attempt has been made to discuss the Chinese remainder theorem in case of linear congruences having more than one incongruent solutions and Chinese remainder theorem have been proved by a new method.

1. Introduction

The kind of Problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the first century A.D. Sun-Tsu asked : Find a number which leave remainder 3,5,4, when divided by 5,7,11 respectively (such mathematics puzzles are by no means confined to a single cultural Sphere : Indeed, the same problem occurs in the *introductio Arithmeticae* of the Greek mathematician. Nicomachus, Circa 100 A.D). In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the Chinese remainder theorem.

2. General Formulation

The proof of Chinese remainder theorem has been obtained by taking linear congruences which have single incongruent solutions under the restriction $\text{g.c.d.}(n_i, m_j) = 1$ for $i \neq j$. The proof of which has been given by verification method. Adopting generalized approach $\text{g.c.d.}(a_i, m_i) = d_i$ and taking linear congruences having d_i incongruent solutions of type.

$$a_i x \equiv b_i \pmod{m_i} ; \text{g.c.d.}(a_i, m_i) = d_i \text{ and } d_i / b_i \quad \dots\dots\dots (2.1)$$

where $i = 1, 2, \dots\dots\dots, n$

equation (2.1) reduces to the form

$$\lambda_i x \equiv \mu_i \pmod{n_i} \quad \dots\dots\dots (2.2)$$

where $\lambda_i = a_i / d_i$

$$\mu_i = b_i / d_i$$

and $n_i = m_i / d_i$

equation (2.2) can be written in the form

$$x \equiv \bar{\lambda}_i \mu_i \pmod{n_i} \quad \dots\dots\dots (2.3)$$

equation (2.1) shall have $\prod_{i=1}^n (d_i)$ incongruent solutions.

Let $c_i \equiv \bar{\lambda}_i \mu_i \pmod{n_i} \quad \dots\dots\dots (2.4)$

In such a manner that d_i incongruent solutions of equation (2.1) shall be

$$C_i \equiv \lambda_i \mu_i + (\lambda - 1) n_i \pmod{m_i} \quad \dots\dots\dots (2.5)$$

for $\lambda = 1, 2, 3, \dots, d_i$.

3. PROOF OF THE THEOREM

Consider system of equations defined by (2.1) further conversion in equation (2.3) having single incongruent solutions.

Putting

$$x = k_i n_i + c_i \quad \dots\dots\dots (3.1)$$

in the equation

$$x \equiv c_j \pmod{n_j} \quad \dots\dots\dots (3.2)$$

we shall have

$$k_i n_i + c_i \equiv c_j \pmod{n_j} \quad \dots\dots\dots (3.3)$$

so that

$$k_i = \bar{n}_i (c_j - c_i) + \mu n_j \quad \dots\dots\dots (3.4)$$

Substituting of this value of k_i to (3.1) give rise to a solutions of general type

$$x = c_n \pmod{\prod_{i=1}^n (n_i)} \dots\dots\dots (3.5)$$

This is first incongruent solution of system of equations defined by (2.1). Other incongruent solutions are given by the following congruence

$$x = c_n + \alpha \prod_{i=1}^n n_i \pmod{\left(\prod_{i=1}^n m_i \right)} \dots\dots\dots (3.6)$$

Where α varies from 1 to $\prod_{i=1}^n (d_i)$

This approach has the advantage of producing direct proof of the theorem in the following manner.

In equation (3.6) if $d_i = 1$ then $m_i = n_i$ yields the proof of chinese remainder theorem

$$x = c_n \pmod{M} \dots\dots\dots (3.7)$$

Where $M = m_1 m_2 \dots\dots\dots m_n$

4. Examples Dealing with Generalized cases Discussed in the Theorem :-

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, 2, \dots, n.$$

when $(a_i, m_i) = d_i$ and $d_i \mid b_i$

Consider the following set of linear congruence

$$\left. \begin{aligned} 2x &\equiv 4 \pmod{6} \\ 5x &\equiv 15 \pmod{25} \\ 7x &\equiv 28 \pmod{49} \\ 11x &\equiv 55 \pmod{121} \end{aligned} \right\} \dots\dots\dots (4.1)$$

reducing each of congruences in the form (3.2) we get

$$x \equiv 2 \pmod{3} \dots\dots\dots (4.2)$$

$$x \equiv 3 \pmod{5} \dots\dots\dots (4.3)$$

$$x \equiv 4 \pmod{7} \dots\dots\dots (4.4)$$

$$x \equiv 5 \pmod{11} \dots\dots\dots (4.5)$$

Putting $x = 3k + 2$ in equation (4.3)

we get

$$k \equiv 2 \pmod{5} \dots\dots\dots (4.6)$$

or $k = 5k_1 + 2$

Substituting value of k yield

$$x = 15k_1 + 8 \dots\dots\dots (4.7)$$

repeating this process for equation (4.4) and (4.5)

we finally get.

$$x \equiv 368 \pmod{1155} \dots\dots\dots (4.8)$$

equation (4.8) gives solutions for (4.2) to (4.5) and first incongruent solution to equation (4.1) shall be

$$x \equiv 368 \pmod{6 \times 25 \times 49 \times 121} \dots\dots\dots (4.9)$$

other incongruent solutions of (4.1) are given by

$$x = 368 + 1155t \pmod{6 \times 25 \times 49 \times 121} \dots\dots\dots (4.10)$$

where $t = 0, 1, 2, \dots\dots, 770$.

REFERENCES

1. Burton, David, 1985. The History of Mathematics. An Introduction, Boston, Allyn and Bacon.
2. Hardy, G.H. and Wright, E. M. 1975. An Introduction to the theory of numbers, 5th ed. London, oxford University Press.