RSRE
MEMORANDUM No. 3650

ROYAL SIGNALS & RADAR ESTABLISHMENT

THE CHINESE REMAINDER THEOREM AND MULTI-PRF RADARS

Author: J Clarke

PROCUREMENT EXECUTIVE,
MINISTRY OF DEFENCE,
RSRE MALVERN,
WORCS

ROYAL SIGNALS AND RADAR ESTABLISHMENT

Memorandum 3650

Title: THE CHINESE REMAINDER THEOREM AND MULTI-PRF RADARS

Author: J Clarke

Date: February 1984

SUMMARY

The Chinese remainder theorem is often discussed in connection with processing for multi-PRF radars. So, as a reference, the theorem is quoted here, a proof given and its application explained.

RSRE MEMORANDUM NO 3650

THE CHINESE REMAINDER THEOREM AND MULTI-PRF RADARS

J Clarke

CONTENTS

1 INTRODUCTION

The Chinese remainder theorem is often discussed in connection with processing for multi-PRF radars. However the theorem itself and its proof are usually only to be found buried deep inside a textbook on number theory, and so it is time-consuming for a radar engineer to uncover the relevant text, become familiar with the nomenclature of number theory and gain an insight into the theorem. So, as a reference, the theorem is quoted in this paper and a proof from first principles is given such that no prior knowledge of number theory is required. The application of the method of the Chinese remainder theorem is then explained and finally an example presented on the processing of radar detections in a multi-PRF radar.

Throughout the mathematical part of this paper any reference to a number is assumed to refer to an integer.

More advanced aspects of the application of the method, such as error detection, are not discussed.

2 THE CHINESE REMAINDER THEOREM

The theorem as quoted by Niven and Zuckerman[1] is:

"Let $m_1, m_2, \ldots\ldots, m_s$ denote s positive integers that are relatively prime in pairs, and let $a_1, a_2, \ldots\ldots, a_s$ denote any s integers. Then the congruences $x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots\ldots, s$ have common solutions. Any two solutions are congruent modulo $m_1 m_2 \ldots\ldots m_s$."

The terms "congruence" and "modulo" (abbreviation "mod") denote a convention that means if an integral number of m is added to (or subtracted from) x and a number y results, then

$$x \equiv y \pmod{m}$$

or alternatively

$$x - y \equiv 0 \pmod{m}$$

Some numerical examples of this are $7 \equiv 2 \pmod{5}$, $12 \equiv 0 \pmod{6}$, $7 \equiv 15 \pmod{4}$ and $86 \equiv 2 \pmod{3}$.

The term "relatively prime" means that the highest common denominator is 1.

3 PROOF OF THEOREM

Let $m = \prod_{i=1}^{i=s} m_i$

From this definition of m and the constraint that m_i are relatively prime in pairs, then it is true that m/m_j is an integer that is relatively prime to m_j. But for any two relatively prime numbers a third number, b, can always be found such that the following congruence holds (this is proved in Appendix 1).

$$\left(\frac{m}{m_j}\right) b_j \equiv 1 \pmod{m_j} \tag{3.1}$$

The definition of m also means that for $i \neq j$,

$$\left(\frac{m}{m_j}\right) b \equiv 0 \pmod{m_i} \tag{3.2}$$

for any b, because m_i is a factor of m/m_j.

Now define x_o according to this equation

$$x_o = \sum_{j=1}^{j=s} \frac{m}{m_j} b_j a_j$$

where the b_j are defined in Eq 3.1 and a_j are those referred to in the theorem. The number x_o is now examined with respect to modulo m_i.

$$x_o \equiv \left\{ \sum_{j=1}^{j=s} \frac{m}{m_j} b_j a_j \right\} \pmod{m_i}$$

Using the congruence 3.2, this simplifies to,

$$x_o \equiv \left\{ \frac{m}{m_i} b_i \; a_i \right\} \pmod{m_i}$$

But considering the summation of "a" of the congruence 3.1

$$\left(\frac{m}{m_i} \right) b_i \; a_i \equiv a_i \pmod{m_i}$$

and so the congruence for x_o simplifies to,

$$x_o \equiv a_i \pmod{m_i}$$

Thus there is a common solution (namely x_o) to the equations, and the first part of the theorem is proved.

Now to prove that the solutions are congruent modulo m, consider x_1 and x_2 to be any two solutions.

$$x_1 \equiv a_i \pmod{m_i}$$

$$x_2 \equiv a_i \pmod{m_i}$$

and so

$$x_1 - a_i \equiv 0 \pmod{m_i}$$

$$x_2 - a_i \equiv 0 \pmod{m_i}$$

Now if any two numbers are exactly divisible by m_i, then sums and differences are also exactly divisible by m_i. So,

$$x_1 - x_2 \equiv 0 \pmod{m_1}$$

This is true for all m_i, so $(x_1 - x_2)$ is a common multiple of any, and all, of $m_1, m_2, \ldots\ldots m_s$. But since the m_i are relatively prime, they have no factors in common. Hence $(x_1 - x_2)$ must be a common multiple of m. Thus the second part of the theorem is proved, that the solutions are congruent modulo m.

4 APPLICATION

The usefulness of the theorem is not as an existence theorem for a number that leaves a certain set of remainders for a certain set of divisors, but by use of the method of proof to find that number. The proof shows that the number is x_o where

$$x_o = \sum_{j=1}^{j=s} \frac{m}{m_j} b_j a_j$$

If we denote $k_j = \frac{m}{m_j} b_j$

then,

$$x_o = \sum_{j=1}^{j=s} k_j a_j$$

The solution may thus be computed directly from the remainders a_j by use of the constants k_j. The value obtained x_o may not be the solution closest to zero, but this solution can be found by reducing x_o modulo m.

To find the k_j the constants b_j are required; these are the solutions to

$$\left(\frac{m}{m_j}\right) b_j \equiv 1 \pmod{m_j}$$

These congruences are not difficult to solve, as can be seen in the following example. Find a number which when divided by 4 has a remainder 3 and when divided by 7 leaves a remainder 2. The method can be applied directly because 4 and 7 are relatively prime (it does not matter that 4 is not prime), here $m_1 = 4$ and $m_2 = 7$. So the b_j obey the following congruences

$$\frac{28}{4} \cdot b_1 \equiv 1 \pmod{4}$$

and $$\frac{28}{7} \cdot b_2 \equiv 1 \pmod{7}$$

These are equal to

$$7\, b_1 \equiv 1 \pmod{4}$$

$$4\, b_2 \equiv 1 \pmod{7}$$

By inspection, the solutions to these congruences are $b_1 = 3$ and $b_2 = 2$. Thus using the formula $k_j = \left(\frac{m}{m_j}\right).b_j$, the constants are $k_1 = 21$ and $k_2 = 8$.

So the solution for the number is

$$x_o = k_1 a_1 + k_2 a_2$$

$$= 21.3 + 8.2$$

$$= 79$$

Other solutions are congruent 28 to 79, so the least positive solution is 23 and other solutions are 51, 107, -5 etc.

5 EXAMPLE

The application of the method of the Chinese remainder theorem to multi-PRF radars will not be laboured here, but a brief example will now be presented as an illustration.

A high PRF radar transmits a pulse of length 10 μsec on each PRF and the following reception period is divided into 8 equal gates occupying a total of 80 μsec on PRF1, 9 gates occupying 90 μsec on PRF2 and 10 occupying 100 μsec on PRF 3. When the radar is directed on a certain bearing, a target is detected in gate 2 on PRF1, gate 3 on PRF2 and in gate 6 on PRF3. What is the true time delay to the target?

Let 10 μsec be equal to one unit.

Then on PRF1 the transmission repeats every 9 units, 10 units for PRF2, and 11 units for PRF3. Also let the target delay be N units.

Thus the problem is defined by

$$N \equiv 2 \pmod 9$$

$$N \equiv 3 \pmod{10}$$

$$N \equiv 6 \pmod{11}$$

Since 9, 10, 11 are relatively prime the method of the Chinese remainder theorem can be applied directly.

First the b_j are calculated.

For $m_1 = 9$, b_1 is defined by

$$\frac{990}{9} b_1 \equiv 1 \pmod 9$$

$$\therefore \quad 110\, b_1 \equiv 1 \pmod 9$$

Clearly $90\, b_1$ can be subtracted

$$\therefore \quad 20\, b_1 \equiv 1 \pmod 9$$

and similarly $18\, b_1$ can be subtracted

$$\therefore \quad 2\, b_1 \equiv 1 \pmod 9$$

by inspection $b_1 = 5$

Similarly $b_2 = 9$, $b_3 = 6$

Using the formula $k_j = \left(\frac{m}{m_j}\right) . b_j$ the constants are,

$$k_1 = 550$$

$$k_2 = 891$$

$$k_3 = 540$$

and so the solution is given by

$$N = \sum k_j a_j$$

$$= 2.550 + 3.891 + 6.540$$

$$= 7013$$

This is only one solution, and other solutions are N(mod m) ie N(mod 990) the solution of most interest is

$$N - 7.990$$

$$= 83$$

This is most likely to be the answer required.

So the true time delay of the target is 830 μsec.

(Other solutions are integral numbers of 9.9 msec longer than 830 μsec.)

REFERENCES

1 Niven, I and Zuckerman, H S, "An introduction to the theory of numbers", Wiley, 1966.

APPENDIX 1

EXISTENCE THEOREM FOR SOLUTION TO $cx \equiv 1 \pmod{m}$

This theorem applies when c and m are relatively prime, then some integer x can be found for which the above congruence holds.

Consider the variable e where

$$e = cx + my$$

and let x and y range over all values. Then e will range over positive values, negative values and zero. Let ℓ be the least positive value and this is obtained for x_o, y_o.

$$\therefore \quad \ell = cx_o + my_o$$

Now ℓ divides exactly into c, because if it did not

$$c = 1.q + r \qquad (\text{and } 0 < r < \ell)$$

(q is the quotient and r the remainder)

$$\therefore \quad r = c - q.\ell$$

$$= c - q\,(cx_o + my_o)$$

$$= c\,(1 - qx_o) + m\,(-qy_o)$$

Thus r would be in the set (cx + my) which contradicts the fact that ℓ is the least positive value.

Similarly ℓ divides exactly into m.

But only 1 can divide into both c and m.

$$\therefore \quad \ell = 1$$

$$\therefore \quad cx_o + my_o = 1$$

Now the congruence $1 \equiv 1 \pmod{m}$ always holds

$$\therefore \quad cx_o + my_o \equiv 1 \pmod{m}$$

$$\therefore \quad cx_o \equiv 1 \pmod{m}$$

Thus the congruence $cx \equiv 1 \pmod{m}$ does have a solution (namely x_o).

DOCUMENT CONTROL SHEET

Overall security classification of sheet ..... UNCLASSIFIED .....

(As far as possible this sheet should contain only unclassified information. If it is necessary to enter classified information, the box concerned must be marked to indicate the classification eg (R) (C) or (S))

1. DRIC Reference (if known)	2. Originator's Reference	3. Agency Reference	4. Report Security Classification
	MEMORANDUM 3650		U/C

5. Originator's Code (if known)	6. Originator (Corporate Author) Name and Location
	ROYAL SIGNALS AND RADAR ESTABLISHMENT

5a. Sponsoring Agency's Code (if known)	6a. Sponsoring Agency (Contract Authority) Name and Location

7. Title

THE CHINESE REMAINDER THEOREM AND MULTI-PRF RADARS

7a. Title in Foreign Language (in the case of translations)

7b. Presented at (for conference papers) Title, place and date of conference

8. Author 1 Surname, initials	9(a) Author 2	9(b) Authors 3,4...	10. Date	pp. ref.
CLARKE, J				

11. Contract Number	12. Period	13. Project	14. Other Reference

15. Distribution statement

UNLIMITED

Descriptors (or keywords)

continue on separate piece of paper

Abstract

The Chinese remainder theorem is often discussed in connection with processing for multi-PRF radars. So, as a reference, the theorem is quoted here, a proof given and its application explained.

SD0/AH