Chinese Remainder Theorem and its Applications

A Dissertation for

MAT-651 Discipline Specific Dissertation

Credits: 16

Submitted in partial fulfilment of Masters Degree

M.Sc. in Mathematics

by

Miss. Prajakta Fatu Rawool

Seat Number : 22P0410026

ABC ID : 426-145-792-604

PRN : 201804273

Under the Supervision of

Dr. Kunhanandan

School of Physical & Applied Sciences

Goa University

Mathematics Discipline

GOA UNIVERSITY

APRIL 2024

Examined by: Seal of the School

DECLARATION BY STUDENT

I hereby declare that the data presented in this Dissertation report entitled, "Chinese Remainder Theorem and its Applications" is based on the results of investigations carried out by me in the Mathematics Discipline at the School of Physical and Applied Sciences Mathematics Department, Goa University under the Supervision of Dr. Kunhanandan and the same has not been submitted elsewhere for the award of a degree or diploma by me. Further, I understand that Goa University or its authorities will be not be responsible for the correctness of observations / experimental or other findings given in the dissertation. I hereby authorize the University/college authorities to upload this dissertation on the dissertation repository or anywhere else as the UGC regulations demand and make it available to any one as needed.

Signature: 

Student Name: Prajakta Fatu Rawool

Seat no: 22P0410026

Date: 10/05/2024

Place: GOA UNIVERSITY

COMPLETION CERTIFICATE

This is to certify that the dissertation report "Chinese Remainder Theorem and its Applications" is a bonafide work carried out by Miss. Prajakta Fatu Rawool under my supervision in partial fulfilment of the requirements for the award of the degree of Master of Science in Mathematics in the Discipline Mathematics at the School of Physical & Applied Sciences , Goa University.

Signarure : _____

Supervisor : Dr. Kunhanandan

Date: 10/05/2024

Signature of HoD of the Dept

Date: 10/05/2024

Place: Goa University

School Stamp

Contents

PREFACE

The topic assigned for the research report is: " Chinese Remainder Theorem and its Applications". The main purpose of this project is to study the different formulations of Chinese Remainder theorem which includes Polynomial form, Group theory form, Ring theory form, Chinese Remainder theorem for RNS to Binary conversion and fast algorithm of Chinese Remainder theorem. The Chinese Remainder theorem has applications in different fields of mathematics and also in real life problems. This study will deal with the applications in mathematics and some applications in real life such as in trading problems, in arrangement of things and also in secret sharing in the form of integers.

FIRST CHAPTER :

The first introductory chapter contains the history of Chinese Remainder theorem along with the statement of the theorem (CRT 1) in Number theory.

SECOND CHAPTER :

The second chapter gives the proof of CRT-1 and the second form of Chinese Remainder theorem (CRT-2) in Number theory along with its proof and their examples. It also contains some of the real life applications of Chinese remainder theorem.

THIRD CHAPTER :

The third chapter gives formulations of Chinese Remainder theorem in Polynomial form, Group theory form, and Ring theory form with examples.

FOURTH CHAPTER :

The fourth chapter is about Chinese Remainder theorem and RNS systems in which we will find reverse converter set for RNS to binary conversion.

FIFTH CHAPTER :

The fifth chapter contains a fast algorithm of Chinese Remainder theorem and its application to Fibonacci Numbers.

ACKNOWLEDGEMENT

I would like to express my gratitude to my Mentor, Dr. Kunhanandan, who was a continual source of inspiration. He pushed me to think imaginatively and urged me to do this homework without hesitation and his useful advice and suggestions were really helpful to me during the project's completion. His vast knowledge, extensive experience, and professional competence enabled me to successfully accomplish this project. This endeavour would not have been possible without his help and supervision. I would also like to thank our University library resources which provided me with the best books to refer throughout the project writing.

NOTATIONS AND ABBREVIATIONS

$\mathbb{Z}$	Set of all integers.
$\mathbb{N}$	Set of all Natural numbers.
$\equiv$	Congruence notation
$\cong$	isomorphism notation
(a,b)	Greatest common divisor of a,b
CRT	Chinese Remainder Theorem
RNS	Residue Number System

ABSTRACT

The Chinese Remainder Theorem (denoted by CRT) is an important theorem in Number theory. In mathematics, the Chinese Remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime. The Chinese Remainder theorem basically gives a rule for obtaining a simultaneous solution to a set of linear congruence system having coprime moduli.

With the continuous advancement in algebraic system, the theorem has evolved into different forms. This study was initiated to learn the various forms of CRT. The study began with first learning the basic CRT in Number theory and its proof followed by studying the different forms of CRT and their applications to various areas of mathematics and also to real life problems..

The conclusion of this study was that CRT has various form and they have various applications in real life problems which will surely help us in future.

Keywords: Chinese Remainder theorem, Euclidean division, algebraic system, congruence, coprime, moduli.

Chapter 1

INTRODUCTION

Chinese Remainder theorem (CRT) is an ancient and important theorem in Number Theory. The oldest remainder problem in the world was first discovered in a third century Chinese mathematical treatise entitled "Sun Zi Suanjing" (The Mathematical Classic of Sun Zi), of which the author was unknown. The remainder problem is stated below:

Problem: Now there are an unknown number of things. If we count by three, there is a remainder 2; if we count by five, there is a remainder 3; and if we count by seven, there is a remainder 2. Find the number of things.

Besides the above problem, the author of "Sun Zi Suanjing" also provided the answer and the methods as follows:

Method: If we count by threes and there is a remainder 2, put down 140.

If we count by fives and there is a remainder 3, put down 63.

If we count by sevens and there is a remainder 2, put down 30.

Add them to obtain 233 and subtract 210 to get the answer.

If we count by threes and there is a remainder 1, put down 70.

If we count by fives and there is a remainder 1, put down 21.

If we count by sevens and there is a remainder 1, put down 15.

When a number exceeds 106, the result is obtained by subtracting 105.

The remainder problem in "Sun Zi Suanjing" is popularly known as the Chinese Remainder Theorem (CRT), for the reason that it first appeared in a Chinese mathematical treatise. Sun Zi's work didn't contain proof nor a full algorithm. The complete theorem was first given by Qin Jiushao in 1247 in his mathematical text named "Mathematical Treatise in Nine Sections".

The Chinese Remainder theorem basically gives the necessary condition for multiple equations to have a simultaneous integer solution. Below is given the statement of the theorem:

Chinese Remainder Theorem (CRT-1)

Suppose $m = m_1 m_2 .....m_r$ and $m_1, m_2, ..., m_r$ are positive integers that are pairwise and mutually prime.

Then for any positive integer $a_1, a_2, ..., a_r$, congruence equation system:

$$\begin{cases} x \equiv a_1 (mod m_1) \\ x \equiv a_2 (mod m_2) \\ \vdots \\ x \equiv a_r (mod m_r) \end{cases}$$

has a solution x $=\sum_{k=1}^{r} a_k \ M_k M_k'$, where $M_k = \frac{m}{m_k}$, 1≤k≤r and M_k' (1≤k≤r) satisfy $M_k M_k' \equiv 1 (\text{mod } M_k)$.

We will see the detailed proof of the theorem (CRT-1) in Chapter 2.

The main aim behind studying this topic is to learn different forms of Chinese Remainder theorem in Number theory, Ring theory , Group theory, Polynomial form, new form with moduli sets and a fast algorithm of CRT-1. By studying these forms we can also see their applications in different areas of mathematics and also in real life problems.

In this study, chapter 2 will focus on the two forms of Chinese Remainder theorem in Number theory denoted by CRT-1 and CRT-2[1] and their examples and application to real life problems[2][3]. In chapter 3 you will see the Chinese Remainder theorem in different areas of mathematics namely; Polynomial form, group theory form and Ring theory form with examples[1]. Chapter 4 contains another modification of Chinese Remainder theorem so as to apply to Residue number System (RNS) and find a reverse converter set for RNS to convert it into binary[4]. Also some of its examples are given in this chapter. Next is the chapter 5 which deals with a Fast algorithm of Chinese Remainder theorem[5] which makes the calculation easy and thereby reducing the steps involved in finding the solutions to system of congruence equations with coprime moduli. Again in this chapter we will see how this fast algorithm can be applied to Fibonacci Numbers[5].

Chapter 2

CHINESE REMAINDER THEOREM IN NUMBER THEORY

In this chapter we will see the two forms of Chinese Remainder theorem in Number theory, ie. the one which we had stated earlier in chapter one, CRT-1 and second one is the modified form of CRT-1, denoted by CRT-2. Let us see them in sections below.

2.1 Chinese Remainder Theorem 1

In this section we will see the proof of CRT-1 stated in chapter (1). Before going for the proof, there are several terms, lemmas, and theorems that we need to know concerning the relatively prime integers which will be required in proving CRT-1.

Definition 2.1(a)

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(modn)$ if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.

Definition 2.1(b): Mutually prime Integers

Two integers a & b not both of which are zero are said to be mutually prime when gcd(a,b)=1.

Definition 2.1(c) : Divisibility

Let a,b $\in \mathbb{Z}$. We say that b divides a if $\exists$ c $\in \mathbb{Z}$ such that a = b.c . We denote b divides a by "$b|a$".

Theorem 2.1.1

Given a,b $\in \mathbb{Z}$ and a $\neq 0$ and b $\neq 0$, $\exists$ x,y $\in \mathbb{Z}$ such that gcd(a,b)=ax+by .

Proof: Consider the set S of all positive linear combinations of a and b:

$$S = \{au + bv | au + bv > 0; u, v \in \mathbb{Z}\}$$

For $a > 0$, taking $u = 1$ and $v = 0$: $au + bv = a > 0$.

For $a < 0$, taking $u = -1$ and $v = 0$; $au + bv = -a > 0$.

Hence $S \neq \phi$.

S contains positive integers, thus by applying Well-Ordering principle there exists integers, S must contain a smallest element d.

Thus from the definition of S, $\exists$ integers x and y for which d=ax+by.

We claim that d=(a,b).

Applying the Division Algorithm to a and b, we can obtain integers q and r such that a=qd+r, where $0 \leq r < d$.

Then r can be written in the form $r = a - qd = a - q(ax+by) = a(1-qx)+b(-qy)$

If $r > 0$, then this implies r $\in$ S, contradicting the fact that d is the least integer

in S (recall that $r < d$).

Therefore, r=0, and so a=qd, or equivalently $d|_a$.

By similar reasoning, $d|_b$, the effect of which is to make d a common divisor of a and b.

Now if c is an other arbitrary positive common divisor of the integers a and b,

ie. $c|a$, $c|b$

$\implies$ $c|ax + by$

ie. $c|d$

$\therefore$ By definition of greatest common divisor, d=(a,b). $\square$

Theorem 2.1.2: Euclid's lemma

If $a|bc$, with (a,b)=1, then $a|c$.

Proof: We have (a,b)=1 $\implies$ $\exists$ x,y $\in \mathbb{Z} \ni$ 1=ax+by

Now, c = c(1) = c(ax+by) = (ac)x+(bc)y

$\implies$ $a|ac$, $a|bc$

$a|(ac)x + (bc)y \implies a|c$. $\square$

Theorem 2.1.4

The linear congruence $ax \equiv b(mod n)$ has a solution iff $d|b$ where $d = gcd(a, n)$.

If $d|b$ then linear congruence $ax \equiv b(mod n)$ has d mutually incongruent solution modulo n.

Proof: Since ax $\equiv$ b (mod n).

$\therefore n|ax - b \implies$ ax-b=ny $\implies$ ax-ny=b for y $\in \mathbb{Z}$

Now this is a linear Diophantine equation and it can be solved iff $d|b$ where d=(a,n). Then by theorem (2.1.1) we are done. $\square$

Now let us see the proof of CRT-1 which we have stated earlier in chapter 1:

Chinese Remainder theorem 1 (CRT-1)

Suppose $m = m_1 m_2 .....m_r$ and $m_1, m_2, ..., m_r$ are positive integers that are pairwise and mutually prime. Then for any positive integer $a_1, a_2, ..., a_r$, congruence equation system:

$$\begin{cases} x \equiv a_1 (mod m_1) \\ x \equiv a_2 (mod m_2) \\ \vdots \\ x \equiv a_r (mod m_r) \end{cases} \tag{2.1}$$

has a solution x $=\sum_{k=1}^{r} a_k \; M_k M_k'$, where $M_k = \frac{m}{m_k}$, and M_k' satisfy

$M_k M_k' \equiv 1 (\text{mod } M_k)$, (1≤k≤r).

Proof:

Given $M_k = \frac{m}{m_k} = m_1 m_2 .....m_{k-1} m_{k+1} ....m_r$, 1≤k≤r

ie. M_k is the product of all the integers m_i (i=1,2,...,r) with the factor m_k deleted.

It is given that $(m_i, m_j)=1$; i≠j

This implies $(M_k, m_k)=1$ and M_k' and y_k satisfy $M_k M_k' + y_k m_k = 1$.

Thus $M_k M_k' \equiv 1 (mod m_k)$ since m_k divides $M_k M_k' - 1$

$\implies a_k M_k M_k' \equiv a_k (mod m_k)$; 1≤k≤r

By $m_i M_i = m_j M_j = $ m, $(m_i, m_j) = 1$ for i≠ j.

$\implies m_i — M_j$, i ≠ j.

$\implies \sum_{k=1}^{r} a_k M_k M_k' \equiv a_k M_k M_k' \equiv a_k (mod m_k)$

and this implies $\sum_{k=1}^{r} a_k M_k M_k' \equiv a_k (mod[m_1 m_2 .... m_r]) \equiv a_k (mod m)$

$x \equiv \sum_{k=1}^{r} a_k M_k M_k'$ (mod m) is the solution. □

Now let us see some examples based on CRT-1:

Example: Find the integer solutions of the equation $x^3 - 1 \equiv 0 (mod 15)$.

Solution: Since 15=5 X 3 and (3,5) = 1,

$x^3 - 1 \equiv 0 (mod 15)$ and $\begin{cases} x^3 - 1 \equiv 0 (mod 5) \\ x^3 - 1 \equiv 0 (mod 3) \end{cases}$ have the same solution.

$x^3 - 1 \equiv 0 (mod 5) \implies x^3 - 1 = 5k \implies x^3 = 5k+1$

$x^3 - 1 \equiv 0 (mod 3) \implies x^3 - 1 = 3k \implies x^3 = 3k+1$

So, $\begin{cases} x^3 - 1 \equiv 0 (mod 5) \\ x^3 - 1 \equiv 0 (mod 3) \end{cases}$ and $\begin{cases} x^3 \equiv 1 (mod 5) \\ x^3 \equiv 1 (mod 3) \end{cases}$ have the same solution.

Now $\begin{cases} x^3 \equiv 1 (mod 5) \\ x^3 \equiv 1 (mod 3) \end{cases}$ satisfies the preconditions of the theorem CRT-1, thus solving it we get;

a_1=1, a_2=1, m_1=5, m_2=3, m=$m_1 m_2$=15

M_1=3 , M_2=5

By $M_i M_i' \equiv 1 (mod m_i)$ we have;

$M_1 M_1' \equiv 1 (mod 5) \implies 3M_1' \equiv 1 (mod 5) \implies M_1' \equiv 3 (mod 5)$

$M_2 M_2' \equiv 1 (mod 3) \implies 5M_2' \equiv 1 (mod 3) \implies M_2' \equiv 1 (mod 3)$

$\therefore$ The solution is,

$x \equiv (a_1 M_1 M_1' + a_2 M_2 M_2')$ (mod m)

$x \equiv$ (1 X 3 X 3 + 1 X 5 X 1)(mod 15)

$x \equiv 14$ (mod 15)

$x \equiv 1 \pmod{15}$ is the required solution.

Example: Solve the system of linear congruence equation

$$\begin{cases} x \equiv 2(mod3) \\ x \equiv 3(mod5) \\ x \equiv 2(mod7) \end{cases}$$

Solution: a_1=2, a_2=3, a_3=2, m_1=3, m_2=5, m_3=7 and they are pairwise prime.

m=$m_1m_2m_3$=105 M_1=35 , M_2=21, M_3=15

By $M_iM_i' \equiv 1(modm_i)$ we have;

$M_1M_1' \equiv 1(mod3) \implies 35M_1' \equiv 1(mod3) \implies M_1' \equiv -1(mod3)$

$M_2M_2' \equiv 1(mod5) \implies 21M_2' \equiv 1(mod5) \implies M_2' \equiv 1(mod5)$

$M_3M_3' \equiv 1(mod7) \implies 15M_3' \equiv 1(mod7) \implies M_3' \equiv 1(mod7)$

$\therefore$ The solution is,

$x \equiv (a_1M_1M_1' + a_2M_2M_2' + a_3M_3M_3') \pmod{\text{m}}$

$x \equiv (2 \text{ X } 35 \text{ X } (-1) + 3 \text{ X } 21 \text{ X } 1 + 2 \text{ X } 15 \text{ X } 1) \pmod{105}$

$x \equiv -70 + 63 + 30 \pmod{105}$

$x \equiv 23 \pmod{105}$ is the required solution.

2.2 Chinese Remainder Theorem 2

Let us see the second form of CRT in Number Theory. The theorem is just a modified form of CRT-1 in which the solution of the congruence system comprise of the particular solutions which are obtained by rewriting the system of congruence equation as some Linear Diophantine equations. First let us see the what are these linear Diophantine equations and some of its results.

Definition 2.2(a): Linear Diophantine Equation

The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns: $ax+by = c$ where a, b, c are given integers and a, b are not both zero. A solution of this equation is a pair of integers x_0, y_0 that, when substituted into the equation, satisfy it; that is, $ax_0+by_0 = c$.

Theorem 2.2.1

The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$ where $d = gcd(a, b)$. If x_0,y_0 is any particular solutions of this equation then all other solutions are given by $x = x_0 + \frac{b}{d}t$, $y = y_0 + \frac{a}{d}t$ where t is any arbitrary constant.

Proof: Suppose $ax + by = c$ be a Linear Diophantine equation.

Then by definition of Linear Diophantine equation $\exists$ x_0, y_0 $\ni$ ax_0+by_0=c

d=(a,b) $\implies$ $d|a$, $d|b$

$\therefore$ By definition of divisibility, $\exists$ r,s $\in \mathbb{Z} \ni$ a=dr , b=ds ——(1)

Now we have,

c=ax+by

c=(dr)x+(ds)y

c=d(rx+sy)

$\implies$ $d|c$

Conversely if $d|c$

$\exists$ t $\in \mathbb{Z} \ni$ c=dt

Since d=(a,b) $\exists$ x_0, y_0 $\ni$ d=ax_0+by_0

Thus we get,

c = dt

c = (ax_0+by_0)t

c = a(tx_0)+b(ty_0)

Hence ax+by=c has a particular solution $x = x_0t$, $y = y_0t$.

Suppose that x_0,y_0 are particular solutions of given equation and x', y' are any other solutions then

ax_0+by_0=c=$ax' + by'$

ax_0+by_0=$ax' + by'$

b$(y_0 - y')$=a$(x' - x_0)$ ———(2)

Put (1) in (2)

d$r(x' - x_0)$=d$s(y_0 - y')$ $\implies$ r$(x' - x_0)$=s$(y_0 - y')$ ———(3)

$\implies$ $r|s(y_0 - y')$ $\implies$ $(\frac{a}{d})|(\frac{b}{d})(y_0 - y')$

Since (a,b)=d $\implies$ $(\frac{a}{d}, \frac{b}{d})$=1

Then we have, $(\frac{a}{d})|_{(y_0-y')}$

Again by definition of divisibility, $\exists$ t $\in \mathbb{Z} \ni (y_0 - y')$=t$(\frac{a}{d})$

$\implies$ $y' = y_0 - (\frac{a}{d})$t ———(4)

Now putting (4) in (3) we get,

t $(\frac{a}{d}) = (\frac{r}{s})$ $(x' - x_0)$

$(x' - x_0)$ = t $(\frac{as}{dr})$

$x' = x_0 + (\frac{b}{d})$t. $\square$

CRT-1 was stated for n relatively coprime moduli but now we will see the modified form of CRT-1 which is restricted to only 2 coprime moduli. Let us see what it looks like.

2.2.2 Chinese Remainder Theorem (CRT-2)

Suppose $m = m_1 m_2$ where $(m_1, m_2) = 1$ and $d_1 = (a_1, m_1)$ and $d_2 = (a_2, m_2)$ and $d_1|_{C_1}$ and $d_2|_{C_2}$.The congruence equations

$$\begin{cases} a_1 x \equiv c_1 (mod m_1) \\ a_2 x \equiv c_2 (mod m_2) \end{cases} \tag{2.2}$$

has a solution. The solution is x$\equiv M_1 M_1' q_1 + M_2 M_2' q_2 (mod m)$

where $q_1 = x_1 + \frac{m_1}{d_1} k_1$, $q_2 = x_2 + \frac{m_2}{d_2} k_2$; $(k_1, k_2 = 1, 2, ...)$, x_1,x_2 are particular solutions of congruence equation(2.2), $M_i M_i' \equiv 1 (mod m_i)$; i=1,2

Proof: Given $d_1|_{C_1}$ and $d_2|_{C_2}$

This implies by theorem(2.1.4) $a_1 x \equiv c_1 (mod m_1)$ and $a_2 x \equiv c_2 (mod m_2)$ have solutions

Also by theorem (2.1.4), since $d_1|_{C_1}$ then the linear congruence $a_1 x \equiv c_1 (mod m_1)$ will have d_1 mutually incongruent solution modulo m_1 and $d_2|_{C_2}$ then the linear congruence $a_2 x \equiv c_2 (mod m_2)$ will have d_2 mutually incongruent solution modulo m_2.

Also given that x_1, x_2 are particular solutions of system(2.2).

$\therefore$ By theorem (2.1.3) $q_1 = x_1 + \frac{m_1}{d_1} k_1$ and $q_2 = x_2 + \frac{m_2}{d_2} k_2$ are other solutions of a_1x$\equiv c_1 (mod m_1)$ and a_2x$\equiv c_2 (mod m_2)$ respectively.

Now since q_1 and q_2 satisfy the linear congruence equations in (2.2).

$\therefore$ system (2.2) and $\begin{cases} x \equiv q_1 (mod m_1) \\ x \equiv q_2 (mod m_2) \end{cases}$ ———(i)

have the same number of solutions.

Also note that equations (i) satisfies the preconditions for the CRT-1.

Hence by CRT-1 the solutions of equations (i) is

$x \equiv M_1 M_1' q_1 + M_2 M_2' q_2 (mod m)$

where $M_i M_i' \equiv 1 (mod mi)$; $i = 1, 2$ $\square$

Example: Solve the system of linear congruence equation

$$\begin{cases} 2x \equiv 1 (mod 3) \\ \\ 3x \equiv 2 (mod 4) \end{cases} \quad \text{———}(1)$$

Solution: m_1=3, m_2=4, and they are pairwise prime.

Since $(2, 3)|_1$ and $(3, 4)|_2$, the congruence equation system(1) have solutions and the number of solutions is d_1=(2,3)=1 , d_2=(3,4)=1.

So from CRT-2, we know that number of solutions of given system of congruence equation is $d = d_1 d_2 = 1$.

Now we have 2x ≡ 1 (mod 3) has a particular solution x ≡ 2 (mod 3),

and 3x ≡ 2 (mod 4) has a particular solution x ≡ 2 (mod 4)

ie. q_1=2, q_2=2

Also, $M_1 = \frac{m}{m_1} = \frac{12}{3} = 4$ and $M_2 = \frac{m}{m_2} = \frac{12}{4} = 3$

From $M_i M_i' \equiv 1 (mod m_i)$ we get;

$M_1' \equiv 1 (mod 3)$

$M_2' \equiv 3 (mod 4)$

Thus from theorem CRT-2 we have,

$x \equiv M_1 M_1' q_1 + M_2 M_2' q_2 (mod m)$

x ≡ (4 X 1 X 2 + 3 X 3 X 2) (mod 12)

x ≡ 26 (mod 12)

x ≡ 2 (mod 12)

is the required solution.

2.3 Chinese Remainder theorem in Real life

Chinese Remainder theorem has various applications in mathematics as well as in real life. In this section we will see some real life applications of Chinese Remainder theorem.

2.2.1 CRT in Trading

The CRT can be applied in trading so as to maximize returns. In trading, the retailers normally ask for reduction of prices of goods since they have to resell the commodities and make some profit out of it. Therefore they price the goods in groups. Most often, some goods are given free to the retailers. If in case there are more than one retailer who wish o purchase from the same wholesaler, in that case we can arrange their bid into some linear congruence and then apply CRT to determine the best bid so as to maximize profit. Let us see one example on how this is applied to such a problem in trading.

Problem: A wholesaler sells cartons of biscuits. Three retailers agree to buy the cartons in groups. Retailer one agrees to buy them at every three for $ 55.00 of which two will be left and added free to the retailer. Retailer two agrees to buy them at every seven for $ 125.00 of which four will be left and given him free. Retailer three agrees to buy it in tens for $ 175.00 of which six will be left and added free. Calculate the total number of cartons the wholesaler is having. Again, if the wholesaler agrees to sell to retailer one, he can sell six

times of such cartons in a month. If he agrees to sell for retailer two, he can sell ten times of such cartons in a month. If he agrees to sell for retailer three, he can sell sixteen times of such cartons in a month. To find which of these retailers the wholesaler should choose to make the maximum profit in a month and assuming the cost price of a carton of the biscuit is $ 15.00 with selling price of $ 20.00 per carton, we look for the profit on each retailer.

Solution:

Claim(i): To find total number of cartons of biscuits the wholesaler has.

Claim(ii): To find which of these retailers the wholesaler should choose to sell the cartons inorder to make the maximum profit in a month.

To estimate how many cartons are to be sold we use CRT(1):

We have

$x \equiv 2(mod3)$

$x \equiv 4(mod7)$

$x \equiv 6(mod10)$

$m_1 = 3$, $m_2 = 7$, $m_3 = 10$

$a_1 = 2$, $a_2 = 4$, $a_3 = 6$

$M = 210$, $M_1 = 70$,$M_2 = 30$, $M_3 = 21$

$70M_1' \equiv 1(mod3) \implies M_1' \equiv 1(mod3)$

$30M_2' \equiv 1(mod7) \implies M_2' \equiv 4(mod7)$

$21M_3' \equiv 1(mod10) \implies M_3' \equiv 1(mod10)$

$\therefore$ By CRT-1,

$x \equiv \sum_{i=1}^{3} a_i M_i Mi' \,(\mathrm{mod} M)$

$\implies x \equiv 746(mod210)$

ie. $x \equiv 116(mod 210)$

Hence there are total 116 cartons of biscuits.

Next to find which of these retailers the wholesaler should choose to make the maximum profit in a month.

For agreement with retailer one:

Total sales = $\frac{116}{3}$ = 38 with remainder 2

The selling price in a month = 38 x 6 x 55 = $ 12,540.00

Cost price =15 x 116 x 6 = $ 10,440.00

Profit = 12540.00 - 10440.00 = $ 2,100.00

Hence the profit is $ 2,100.00

For agreement with retailer two:

Total sales = $\frac{116}{7}$ = 16 with remainder of 4

The selling price in a month = 16 x 10 x 125 = $ 20,000.00

Cost price =116 x 15 x 10 = $ 17,400.00

Profit = 20000 - 17400.00 = 2,600.00

Hence the profit is $ 2,600.00

For agreement with retailer three:

Total sales = $\frac{116}{10}$ = 11 with remainder of 6

The selling price in a month = 16 x 11 x 175 = $ 30,500.00

Cost price =116 x 16 x 15 = $ 27,840.00

Profit = 30500 - 27840.00 = $ 2,960.00

Hence the profit is $ 2,960.00

Hence the wholesaler should agree to do business with retailer three so as to earn maximum profit for that month.

2.2.2 CRT in Information Retrieval or Leakage

Confidential information shared between people can be retrieved using CRT if one of them died unfortunately or one of them misplaced the information.

Problem: Consider a confidential message to be in the form of an integer, K = 1000 and shared into three distinct messages among three people in such a way that K can be retrieved by working together the secret messages of all three people but not by the participation of fewer people. We thus, choose the pairwise coprime say, p_i such that

$\sqrt[3]{K} < p_i < \sqrt{K}$

ie. $10 < p_i < 31.6$

We choose $p_1 = 11$, $p_2 = 13$, $p_3 = 17$.

Finding the residues of K modulo p_i we get

$x \equiv 10(mod 11)$

$x \equiv 12(mod 13)$ ———(1)

$x \equiv 14(mod 17)$

Solution: Suppose that we know the secret messages of all three people, ie. we are given system(1) and we have to find the confidential message K.Then we proceed as follows:

Now here 11,13,17 are pairwise coprime moduli and hence by using CRT-1 we can find the simultaneous solution of system(1)

$m_1 = 11$, $m_2 = 13$, $m_3 = 17$, $m = 2431$

$M_1 = \frac{2431}{11} = 221$, $M_2 = 187$, $M_3 = 143$

$M_i M_i' \equiv 1(mod m_i)$

$221M_1' \equiv 1(mod 11) \implies M_1' = 1$

$187M_2' \equiv 1(mod 13) \implies M_2' = 8$

$143M_3' \equiv 1(mod 17) \implies M_3' = 5$

Thus the system(1) satisfies the hypothesis of CRT-1 and thus we get

$x \equiv \sum_{i=1}^{3} a_i M_i Mi' \,(\mathrm{mod} m)$

$x \equiv 30172(mod 2431)$

ie. $x = 1000 = K$ which is the desired confidential message.

Now if one of the 3 people is perished, by the use of CRT the full message can be retrieved using the available secret messages of the remaining people.

$x \equiv 10(mod 11)$

$x \equiv 12(mod 13)$ ———(2)

Solving (2) using CRT,

$M_1 = 13$, $M_2 = 11$, $m = 143$

$13M_1' \equiv 1(mod 11) \implies M_1' = 6$

$11M_2' \equiv 1(mod 13) \implies M_2' = 6$

$\therefore x \equiv 1572(mod 143)$

$x \equiv 142(mod 143)$

To generate the required message we compute:

$x - 142 = 143i$ $(i = 1, 2, 3, ...)$; yielding x = 285, 428, 571, 714, 857, 1000,...

2.2.3 CRT in arrangement of things

CRT can also be applied to certain problems in real life which involves ar-

rangement of things in given number of ways. The problem stated below is an example of the same.

Problem: If a group of academic scholars in a conference can be fitted to 3 rows leaving 2 left, in 5 rows leaving 4 left and 7 rows leaving 6 left then find the total number of scholars who attended the conference.

Solution: We can translate this problem into the following system of congruences:

$x \equiv 2(mod3)$

$x \equiv 4(mod5)$

$x \equiv 6(mod7)$

Next, $m = m_1$ x m_2 x $m_3 = 3$ x 5 x 7 $= 105$

$M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

$35M_1' \equiv 1(mod3)$

$\implies M_1' \equiv 2(mod3)$

$21M_2' \equiv 1(mod5)$

$\implies M_2' \equiv 1(mod5)$

$15M_3' \equiv 1(mod7)$

$\implies M_3' \equiv 1(mod7)$

Then by CRT-1 we get,

$x \equiv 314(mod105)$

$x \equiv 104(mod105)$

Therefore, there were 104 scholars at the conference.

Chapter 3

FORMULATIONS OF CHINESE REMAINDER THEOREM

In this chapter we will see the forms of Chinese Remainder theorem such as in Polynomial form, Group theory form and Ring theory form. Also we will see some applications of each one of them so as to understand the theorems in a better way.

3.1 Polynomial form

In this section we will extend the notion of relatively prime integers to coprime polynomials. This will allow us to extend the Chinese Remainder theorem to Polynomials. Before that let's take a look at what are coprime polynomials.

Definition 3.1(a): Mutually prime polynomials

Two polynomials $f_1(x)$ and $f_2(x)$ are said to be mutually prime if there exists $u_j(x)$ and $v_j(x)$ such that $f_1(x)u_j(x) + f_2(x)v_j(x)$=1.

3.1.1 CRT in Polynomial form

If $\{f_i(x) : i = 1, 2, ..., n\}$ are pairwise coprime polynomials and $a_1(x), a_2(x), ..., a_n(x)$ are n polynomials, then there is a polynomial $g(x)$, $q_i(x)$ $(i = 1, 2, ..., n)$ such that $g(x) = f_i(x)q_i(x) + a_i(x)$ for each i

Proof: Firstly we will try to prove there exist polynomial $g_i(x)$ such that for arbitrary i

$g_i(x) = f_i(x)q_i(x) + 1$; $f_j(x)|g_i(x)$, $(i \neq j)$

This can be rewritten as $g_i(x) - 1 = f_i(x)q_i(x)$

Then by the definition of congruence we have, $g_i(x) \equiv 1 \pmod{f_i(x)}$

Now since $f_1(x)$ and $f_j(x)$ $(j \neq 1)$ are mutually prime $\exists$ $u_j(x)$ and $v_j(x)$ such that $f_1(x)u_j(x) + f_j(x)v_j(x) = 1$

Let $g_1(x) = f_2(x)v_2(x)...f_n(x)v_n(x)$

$= (1 - f_1(x)u_2(x))...(1 - f_1(x)u_n(x))$

So $g_1(x)$ fulfills the requirement.

In the same way $g_i(x)$ can be constructed.

Example: $f(x)$ is a polynomial with integer coefficients, for each positive integer m, write N_m=$\{x \in \mathbb{Z}|f(x) \equiv 0(modm)\}$.

Prove that when $m_1, m_2, ..., m_s$ are mutually prime,

$N_{m_1m_2.....m_s}$=$N_{m_1}N_{m_2}...N_{m_s}$

Solution: We only need to prove for $s = 2$.

Note $m = m_1m_2$

$P = \{0 \leq x < m|f(x) \equiv 0(modm)\}$ and

$P_i = \{0 \leq x < m_i|f(x) \equiv 0(modm_i)\}$ i=1,2

The above defined set P and P_i proves that there is a natural one-to-one cor-

respondence between P and $P_1 \mathrm{X} P_2$.

Take any $x \in P$, that is $0 \leq x < m$ and $m|f(x)$.

Note $x = q_i m_i + x_i$ where $0 \leq x_i < m_i$, q_i is an integer, $m_i|x - x_i$.

Notice that $x - x_i|_{f(x)-f(x_i)}$ then $m_i|f(x_i)$

ie. $x_i \in P_i$.

Hence $(x_1, x_2) \in (P_1 X P_2)$

In turn, take any $(y_1, y_2) \in (P_1 X P_2)$

ie. $m_1|f(y_1)$, $m_2|f(y_2)$.

Using the CRT $\exists!$ integer y, $0 \leq y < m_1 m_2 = m$ and satisfies

$y \equiv y_1 (mod m_1)$

$y \equiv y_2 (mod m_2)$

Since $m_i|_{y-y_i}$ and $y - y_i|_{f(y)-f(y_i)}$

Hence $m_i|f(y)$ ie. $m_1 m_2|f(y)$

ie. $m|f(y) \implies y \in P$

This proves $N_{m_1 m_2} = |P| = |P_1 X P_2| = N_{m_1} N_{m_2}$

Similarly the solution follows for $s > 2$.

3.2 Group theory form

This section deals with the details of Group theory followed by the CRT in group theory form. Let us take a look at some of the definitions and results we require to understand the theorem statement and proof.

Definition 3.2(a) : Group

A group $\langle G, * \rangle$ is a set G, closed under the binary operation $*$, such that the

following axioms are satisfied:

$\mathcal{G}_1$: For all $a, b, c \in G$, we have

$(a * b) * c = a * (b * c)$. Associativity of $*$

$\mathcal{G}_2$: There is an element $e \in G$ such that for all $x \in G$,

$e * x = x * e = x$. Identity element e of $*$

$\mathcal{G}_3$: Corresponding to each $a \in G$, there is an element $a' \in G$ such that

$a*a'=a'*a = e$. Inverse of a' of a

Definition 3.2(b): Subgroup

If a subset of H of a group G is closed under binary operation of G and if H with the induced operation from G is itself a group, then H is a subgroup of G.

Definition 3.2(c) : Coset

Let H be a subgroup of a finite group G. The partition of G into r cells, all having the same size as H. Then we have, r(order of H)=(order of G).
The cells in the partition will be called cosets of H.

Definition 3.2(d) : Left and Right Cosets

Let H be a subgroup of a group G. The subset $aH=\{ah : h \in H\}$ of G is the left coset of H containing a, while the subset $Ha=\{ha : h \in H\}$ is the right coset of H containing a.

Definition 3.2(e) : Normal subgroup

A subgroup H of a group G is normal if its left and right cosets coincide, ie. if $gH = Hg$, $\forall\ g \in G$. Equivalently, $H = gHg^{-1}$

Definition 3.2(f) : Quotient Group or Factor Group

When the subgroup H of G is normal, then the set of left (or right) cosets of H in G is itself a group called the factor group of G by H (or the quotient group of G by H).

It is denoted by $G/H = \{aH | a \in G\}$.

Definition 3.2(g) : External Direct Product

Let $G_1, G_2, ..., G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, ..., G_n$, written as $G_1 \oplus G_2 \oplus ... \oplus G_n$, is the set of all n-tuples for which the i^{th} component is an element of G_i and the operation is component-wise.

In symbols, $G_1 \oplus G_2 \oplus ... \oplus G_n = \{(g_1, g_2, ..., g_n) : g_i \in G_i\}$

where $(g_1, g_2, ..., g_n)(g'_1, g'_2, ..., g'_n)$ is defined to be $(g_1 g'_1, g_2 g'_2, ..., g_n g'_n)$.

It is understood that each product $g_i g'_i$ is performed with the operation of G_i.

Definition 3.2(h) : Isomorphism

An isomorphism ϕ from a group G to a group $\bar{G}$ is a one-to-one mapping (or function) from G onto $\bar{G}$ that preserves the group operation.

That is, $\phi(ab) = \phi(a)\ \phi(b)\ \forall a, b \in G$

3.2.1 First isomorphism theorem

Let ϕ be a group homomorphism from G to $\bar{G}$. Then the mapping from $G/Ker(\phi)$ to $\phi(G)$, given by $gKer(\phi) \to \phi(g)$, is an isomorphism.

In symbols, $G/Ker(\phi) \cong \phi(G)$.

3.2.2 Proposition:

For each $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$

Proof: Let $\mathbb{Z}_n = <x>$ where $x^n = 1$

Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined $\forall\ x \in \mathbb{Z}$ by

$\phi(m) = x^{m(modn)}$

Observe that ϕ is indeed a homomorphism from $\mathbb{Z}$ since

$\forall\ m_1, m_2 \in \mathbb{Z}$ we have

$\phi(m_1 + m_2) = x^{m_1+m_2(modn)} = x^{m_1(modn)}x^{m_2(modn)}$

ie. $\phi(m_1 + m_2) = \phi(m_1)\phi(m_2)$

Now observe that

$ker(\phi) = \{m \in \mathbb{Z} : x^{m(modn)} = 1\} = \{m \in \mathbb{Z} : n|m\} = n\mathbb{Z}$

So by the first isomorphism theorem we have that

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/ker(\phi) \cong \phi(G)$

But ϕ is surjective , since $\forall\ x^t \in \mathbb{Z} =< x >$, $1 \leq t \leq n$, we have that $\phi(t) = x^t$

So $\phi(\mathbb{Z}) = \mathbb{Z}_n$ and thus from above $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ $\square$

3.2.3 Theorem:

The group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ iff m and n are relatively prime.

Proof: Suppose $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic.

Let (a, b) be a generator o $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Then $order((a, b)) = mn$

Let $o_a =$ order of (a) and $o_b =$ order of (b)

$o_a/m \wedge o_b/n$

$\implies$ $o_a.o_b/lcm\ (m, n)$

$\implies$ $lcm\ (m, n)$ is a common multiple of o_a o_b

$\implies lcm(o_a, o_b) \leq lcm\ (m, n)$

$order((a, b)) = lcm\ (o_a, o_b)$

$lcm\ (m, n) = mn/(m, n)$

$\therefore gcd(m, n) = 1$

Conversely, suppose $gcd(m, n) = 1$

Let a and b be generator of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively.

$o_a = m$ and $o_b = n$

$order((a, b)) = lcm(o_a, o_b) = lcm(m, n) = \dfrac{mn}{gcd(m, n)} = mn$

$\implies \mathbb{Z}_m \oplus \mathbb{Z}_n = \langle (a, b) \rangle \wedge |\mathbb{Z}_m \oplus \mathbb{Z}_n| = mn$

$\implies \mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ □

3.2.4 Corollary:

The group $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_n}$ is cyclic and is isomorphic to $\mathbb{Z}_{m_1 m_2 ... m_n}$ iff m_i, $i = 1, 2, ..., n$ are such that gcd of any two of them is 1.

Proof: We will prove this by induction.

For k=2 already proved in previous theorem (3.2.3).

Assume for k=n-1.

ie. $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_{n-1}} \cong \mathbb{Z}_{m_1 m_2 ... m_{n-1}}$

To prove for k=n,

Now, $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_{n-1}} \oplus \mathbb{Z}_{m_n} = \mathbb{Z}_{m_1 m_2 ... m_{n-1}} \oplus \mathbb{Z}_{m_n}$

Since $m_1 m_2 ... m_{n-1}$ and m_n are coprime, then using theorem(3.2.3) we get;

$\mathbb{Z}_{m_1 m_2 ... m_{n-1}} \oplus \mathbb{Z}_{m_n} \cong \mathbb{Z}_{m_1 m_2 ... m_{n-1} m_n}$

ie. we get,

$\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_n} \cong \mathbb{Z}_{m_1 m_2 ... m_n}$. □

3.2.5 Theorem: CRT in Group theory:

Suppose $m = m_1 m_2 ... m_s$ and $m_1, m_2, ..., m_s$ are pairwise prime positive integers. Then $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/m_s\mathbb{Z}$

Proof : We know $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ for each $n \in \mathbb{N}$

So here we only need to prove that

(i) $\mathbb{Z}/m\mathbb{Z} \cong Z_m$ where m= $m_1.m_2....m_s$ and $m_i \in \mathbb{Z}$ for i=1,2,3,...,s

(ii) $\mathbb{Z}_{m_1 m_2 ... m_s} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus ... \oplus \mathbb{Z}_{m_s}$

To prove (i):

Since m= $m_1.m_2....m_s$ are positive integers, thus by Proposition 3.2.2

$\mathbb{Z}/(m_1.m_2....m_s)\mathbb{Z} \cong \mathbb{Z}_{m_1 m_2 ... m_s}$

To prove (ii)

Since m_i are pairwise prime for i=1,2,...,s from Theorem 3.2.3 and Corollary 3.2.4 we are done. □

Now let us see one example based on theorem (3.2.5):

Example: Find the solution of the congruence equation

$$\begin{cases} x \equiv 2(mod 3) \\ x \equiv 3(mod 5) \\ x \equiv 2(mod 7) \end{cases}$$

Solution: Note that 3,5,7 are pairwise prime positive integers and m=3×5×7=105.

This problem corresponds to the decomposition

$\mathbb{Z}/105\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$.

3.3 Ring theory form

In this section of the chapter we will see the Chinese Remainder theorem extended to the coprime monoid rings.

3.3(a) Definition: Ring

A ring $< R, +, . >$ is a set R together with two binary operations + and . , which we call addition and multiplication, defined on R such that the following axioms are satisfied:

$\mathcal{R}_1$: $< R, + >$ is an abelian group.

$\mathcal{R}_2$: Multiplication is associative.

$\mathcal{R}_3$: For all a,b,c $\in \mathbb{R}$, the left distributive law a.(b+c) = (a.b)+(a.c) and the right distributive law (a+b).c = (a.c)+(b.c) hold.

3.3(b) Definition: Homomorphism

For rings R and R', a map $\phi : R \to R'$ is a homomorphism if the following two conditions are satisfied for all a,b $\in R$:

(i) ϕ(a+b) = ϕ(a)+ϕ(b)

(ii) ϕ(ab) = ϕ(a) ϕ(b)

3.3(c) Definition: Isomorphism

An isomorphism $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one to one and onto R'. The rings R and R' are then isomorphic.

3.3(d) Definition:

A ring in which the multiplication is commutative is a commutative ring.

A ring with a multiplicative identity element is a ring with unity; the multiplicative identity element 1 is called unity.

3.3(e) Definition: Ideal

An additive subgroup N of a ring R satisfying the properties aN $\subseteq$ N and Nb $\subseteq$ N $\forall$ a,b $\in$ R is an ideal.

3.3(f) Definition:

Ideals A, B are coprime if A+B=(1)=R.

3.3(g) Definition: Monoid

A monoid is a semigroup that has an identity element for the binary operation.

3.3(h) Definition: A Monoid Ring

Let R be a ring and let G be a monoid. The monoid ring or monoid algebra of G over R, denoted by R[G] or RG, is the set of formal sums $\sum_{g\in G} r_g g$ where $r_g \in R$ for each $g \in G$ and $r_g = 0$ for all but finitely many g, equipped with coefficient-wise addition, and the multiplication in which the elements of R commute with the elements of G.

3.3(i) Definition: Unitary ring

A ring in which there is an identity element for multiplication is called unital ring, unitary ring or simply ring with identity. The identity element is generally

denoted by 1.

3.3.1 Lemma:

Suppose R is a unitary ring and I and J are ideals that are mutually prime to R, then $IJ + JI = I \cap J$.

In particular when R is unitary $IJ = I \cap J$.

Proof: First to prove that $IJ \subseteq I \cap J$ ie. to prove that ab $\in I \cap J$ $\forall a \in I$ and $\forall b \in J$

Now $b \in J \subseteq R$; since I is an ideal, $ab \in I$.

Also, $ba \in I \subseteq R$; since J is an ideal, $ab \in J$.

Thus $ab \in I \cap J$

ie. $IJ \subseteq I \cap J = J \cap I$

Since $I \cap J$ is closed for addition, $IJ + JI$ is a subset of $I \cap J$.

Since I and J are prime, $\exists$ i $\in$ I and j $\in$ J such that $i + j = 1$.

For arbitrary $k \in I \cap J$; $k = 1k = (i + j)k = ik + jk \in IJ + JI$.

Hence $I \cap J$ is a subset of $IJ + JI$.

Hence $IJ + JI = I \cap J$

When R is unitary ring $IJ = JI$, hence $IJ + JI = IJ$. $\square$

3.3.2 Lemma:

Suppose R is a commutative ring, and $A_1, ..., A_n$ $(n > 1)$ are pairwise prime ideals. Then $A_1, ..., A_{n-1}$ and A_n are mutually prime and $A_1...A_n = A_1 \cap ... \cap A_n$

Proof: For n=2, A_1, A_2 are prime ideals then by lemma(3.3.1), $A_1.A_1 = A_1 \cap A_2$

For $n > 3$, $A_1 \cap A_2 = A_1A_2$ and A_3 are prime.

Hence $A_1 \cap A_2 \cap A_3 = A_1A_2 \cap A_3 = A_1A_2A_3$

Continuing in the same way we get,

A_1,A_2,...,A_{n-1} and A_n are mutually prime and

$A_1.A_2....A_n = A_1 \cap A_2 \cap ... \cap A_n$. $\square$

Now let us see the Ring theory form of CRT for coprime ideals.

3.2.3 Theorem : CRT in Ring theory form

Suppose $A_1, A_2, ..., A_n$ are the ideals of pairwise coprime on a monoid R.

Then for arbitrary $a_1, a_2, ..., a_n \in R$ the set $\{x \in R : \forall i = 1, 2, ..., n, x \equiv a_i (mod A_i)\}$

is not empty, and is the residual class module $\cap_{i=1}^{n} A_i$.

Besides $R/(A_1 \cap ... \cap A_n) \cong R/A_1 \oplus ... \oplus R/A_n$.

Proof: If n=2, $A_1 + A_2 = R$, so there exist $a_i \in A_i$ such that $a_1 + a_2 = 1$

Let $y_1 = a_2$ and $y_2 = a_1$

Then $y_i \equiv 1 (mod A_i)$ and $y_i \equiv 0 (mod A_i)$, for $i \neq j$

Let $x = x_1 y_1 + x_2 y_2$

Then $x \equiv x_1 (mo A_1)$ and $x \equiv x_2 (mo A_2)$

Thus for n=2 we have proved.

Now suppose $n > 2$

Then $\forall j \geq 2$, $A_1 + A_j = R$, so $a_1^{(j)} + a_j = 1$ for some $a_1^{(j)} \in A_1$ and $a_j \in A_j$

Then $1 = \prod_{j=2}^{n} (a_1^{(j)} + a_j) \in A_1 + \prod_{j=2}^{n} A_j$

By the case for two ideals , there exist $y_1 \in R$ such that $y_1 \equiv 1 (mod A_1)$ and

$y_1 \equiv 0 (mod \prod_{j=2}^{n} A_j)$

This implies $y_1 \in \prod_{j=2}^{n} A_j$, and thus $y_1 \equiv 0 (mod A_j)$ for all $j \geq 2$

Repeat this process to obtain $y_2, ..., y_n$.

Let $x = \sum_{i=1}^{n} x_i y_i$.

Then $x \equiv x_i (mod A_i)$

Next to prove $R/(A_1 \cap ... \cap A_n) \cong R/A_1 \oplus ... \oplus R/A_n$.

Define a map:$x \to (x + A_1, ..., x + A_n)$.

This is a surjective map by CRT and the kernel is $\cap_{i=1}^{n} A_i$

Then using isomorphism theorem we get,

$R/(A_1 \cap ... \cap A_n) \cong R/A_1 \oplus ... \oplus R/A_n$ $\square$

Now let us see on example on theorem(3.2.3).

Example: In $\mathbb{Z}_{91}$, find the square root of $\bar{1}$

Solution: We know $\mathbb{Z}_{91} = \mathbb{Z}/(91)$.

Since 91=7×13 and 7 and 13 are prime.

$(91) = (7)(13) = (7) \cap (13)$.

Hence $\mathbb{Z}/(91) \cong \mathbb{Z}/(7) \oplus \mathbb{Z}/(13)$, where the isomorphic mapping is

$\phi : a + (91) \to (a + (7), a + (13))$.

Hence $(a + (91))^2 = 1 + (91)$

$\iff (a + (7), a + (13))^2 = (1 + (7), 1 + (13))$

$\iff (a + (7))^2 = 1 + (7)$ and $(a + (13))^2 = 1 + (13)$.

Since $\mathbb{Z}/(7)$,$\mathbb{Z}/(13)$ are fields, and in the unary polynomial ring F[x] on any field F, the n-degree polynomial f(x) has at most n roots on F, so $x^2 - 1$ has at least 2 roots in $\mathbb{Z}/(7)$ and $\mathbb{Z}/(13)$.

Obviously, 1+(7) and -1+(7) are two different square roots of 1+(7); 1+(13) and -1+(13) are two different square roots of 1+(13).

Hence $(a + (91))^2 = 1 + (91)$

$\iff a + (7) = \pm 1 + (7)$ and $a + (13) = \pm 1 + (13)$

$$\iff \begin{cases} a \equiv 1(mod 7) \\ a \equiv 1(mod 13) \end{cases} \text{ or } \begin{cases} a \equiv 1(mod 7) \\ a \equiv -1(mod 13) \end{cases} \text{ or } \begin{cases} a \equiv -1(mod 7) \\ a \equiv 1(mod 13) \end{cases} \text{ or}$$

$$\begin{cases} a \equiv -1(mod 7) \\ a \equiv -1(mod 13) \end{cases}$$

Now solving the two congruence equations:

$$\begin{cases} x \equiv 1(mod 7) \\ x \equiv 0(mod 13) \end{cases} \implies x = 78 + 91k,\ k \in \mathbb{Z};$$

$$\begin{cases} x \equiv 0(mod 7) \\ x \equiv 1(mod 13) \end{cases} \implies x = 14 + 91k,\ k \in \mathbb{Z}.$$

According to the theorem it can be concluded that the solution of

$$\begin{cases} a \equiv 1(mod 7) \\ a \equiv 1(mod 13) \end{cases} \text{ is } a = 1 \times 78 + 1 \times 14 + 91k = 1 + 91l,\ l \in \mathbb{Z}.$$

Similarly, it can be concluded that the solutions of the remaining three congruence equations are:

$a = 1 \times 78 + (-1) \times 14 + 91k = 64 + 91k,\ k \in \mathbb{Z};$

$a = (-1) \times 78 + 1 \times 14 + 91k = 27 + 91l,\ l \in \mathbb{Z};$

$a = (-1) \times 78 + (-1) \times 14 + 91k = -1 + 91l,\ l \in \mathbb{Z}.$

Hence in $\mathbb{Z}_{91}$, the square roots of $\bar{1}$ are $\bar{1}$, $\bar{64}$, $\bar{27}$, $\bar{-1}$.

Chapter 4

CHINESE REMAINDER THEOREM AND MODULI SETS

In this chapter we will study the new form of CRT which will help in converting RNS moduli set to binary system.

4.1 RNS and Moduli sets

RNS has applications in digital signal processing and digital image processing. For such applications of RNS we need to first convert it into binary system using a reverse converter set. In this section we will study the new CRT form which will help us in finding the reverse converter set for RNS. First let us see what is RNS in detail and then we will see what is the theorem which we can use for finding reverse converter set.

4.1(a) Definition: Moduli sets

Moduli sets are general set of relatively prime numbers.

4.1(b) Definition: Residue Number System (RNS)

The Residue Number System is a non-weighted number system representing integers by their values modulo several pairwise relatively coprime integers called the moduli.

4.1.1 Proposition:

If $a \equiv 1(mod m_1 m_2 ... m_n)$ then

$a \equiv 1(mod m_1)$, $a \equiv 1(mod m_2)$, ... , $a \equiv 1(mod m_n)$

Proof: We will prove this by induction on n.

To prove for $i = 2$,

we have $a \equiv 1(mod m_1 m_2) \implies m_1 m_2 | (a-1)$

$\implies a - 1 = (m_1 m_2)k$; $k \in \mathbb{Z}$

ie. $a - 1 = m_1(m_2 k) \implies a \equiv 1(mod m_1)$

Also $a - 1 = m_2(m_1 k) \implies a \equiv 1(mod m_2)$

Assume it holds for $i = n - 1$.

ie. if $a \equiv 1(mod m_1 m_2 ... m_{n-1})$ then

$a \equiv 1(mod m_1)$, $a \equiv 1(mod m_2)$, ... , $a \equiv 1(mod m_{n-1})$

To prove for $i = n$.

$a \equiv 1(mod m_1 m_2 ... m_{n-1} m_n)$

$\implies a - 1 = (m_1 m_2 ... m_{n-1} m_n)k$; $k \in \mathbb{Z}$

$a - 1 = (m_1 m_2 ... m_{n-1}) m_n k$

By using the case for $i = 2$ and by induction assumption we get,

$a \equiv 1(mod m_1)$, $a \equiv 1(mod m_2)$, ... , $a \equiv 1(mod m_{n-1})$, $a \equiv 1(mod m_n)$ $\square$

4.1.2 Proposition:

If $(m_1, m_2) = 1$ then there is a $k \in \mathbb{Z}$ such that $m_1 k \equiv 1(mod m_2)$

Proof: Given $(m_1, m_2) = 1$ then by theorem(2.1.1) we get,

$m_1 k_1 + m_2 k_2 = 1$; $k_1, k_2 \in \mathbb{Z}$

ie. $m_1 k_1 - 1 = m_2 k_2$

$\implies m_1 k_1 \equiv 1(mod m_2)$. $\square$

4.1.3 Proposition:

If $(m_1, m_2) = 1$ and $(m_1, m_3) = 1$ then $(m_1, m_2 m_3) = 1$

Proof: $(m_1, m_2) = 1 \implies 1|m_1$, $1|m_2$

$(m_1, m_3) = 1 \implies 1|m_1$, $1|m_3$

Now $1|m_2$ and $1|m_3$

$\implies 1|m_2 m_3$

Similarly, $1|m_1$ and $1|m_2 m_3$

$\implies (m_1, m_2 m_3) = 1$. $\square$

4.1.4 Theorem: New CRT for RNS conversion

Let $m_1, m_2, ..., m_n$ be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$.

Then the system of linear congruence

$$\begin{cases} x \equiv x_1(mod m_1) \\ x \equiv x_2(mod m_2) \\ \vdots \\ x \equiv x_n(mod m_n) \end{cases} \tag{4.1}$$

has a unique solution modulo $m_1 m_2 ... m_n$. The solution is

$$\bar{x} = [x_1 + k_1 m_1 (x_2 - x_1) + ... + k_{n-1} m_1 m_2 ... m_{n-1} (x_n - x_{n-1})] (mod m_1 m_2 ... m_n) \tag{4.2}$$

where $k_1, k_2, ..., k_{n-1}$ satisfy

$$\begin{cases} m_1 k_1 \equiv 1 (mod m_2 ... m_n) \\ m_1 m_2 k_2 \equiv 1 (mod m_3 ... m_n) \\ \vdots \\ m_1 m_2 ... m_{n-1} k_{n-1} \equiv 1 (mod m_n) \end{cases} \tag{4.3}$$

Proof: Since $(m_i, m_j) = 1$ for $i \neq j$ by proposition(4.1.2) and proposition(4.1.3)

$\exists$ k_i's satisfying system(4.3).

We only need to prove that $\bar{x}$ in (4.2) satisfies every congruence in (4.1).

Clearly, $\bar{x} \equiv x_1 (mod m_1)$

Next,

$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1)] (mod m_2)$

$\bar{x} \equiv x_1 (mod m_1) + k_1 m_1 (x_2 - x_1) (mod m_2)$

Since $m_1 k_1 \equiv 1 (mod m_2 ... m_n)$ —from Proposition(4.1.2).

$m_1 k_1 \equiv 1 (mod m_2)$ —from Proposition(4.1.1).

$\therefore \bar{x} \equiv x_1 (mod m_2) + (x_2 - x_1) (mod m_2)$

$\bar{x} \equiv x_2 (mod m_2)$

Similarly,

$\bar{x} \equiv [x_1 + k_1 m_1 (x_2 - x_1) + k_2 m_1 m_2 (x_3 - x_2)] (mod m_3)$

$\bar{x} \equiv x_1 (mod m_3) + k_1 m_1 (x_2 - x_1) (mod m_3) + k_2 m_1 m_2 (x_3 - x_2) (mod m_3)$

Again by proposition(4.1.1); $k_1 m_1 \equiv 1(mod m_3)$ and

$$k_2 m_1 m_2 \equiv 1(mod m_3)$$

$\therefore \bar{x} \equiv x_1(mod m_3) + (x_2 - x_1)(mod m_3) + (x_3 - x_2)(mod m_3)$

$\equiv x_3(mod m_3)$

Extending the above to the larger dimensions we get,

$\bar{x} \equiv [x_1 + k_1 m_1(x_2 - x_1) + ... + k_{n-1} m_1 m_2 ... m_{n-1}(x_n - x_{n-1})](mod m_n)$

$\bar{x} \equiv x_1(mod m_n) + k_1 m_1(x_2 - x_1)(mod m_n) + ... + k_{n-1} m_1 ... m_{n-1}(x_n - x_{n-1})(mod m_n)$

$\bar{x} \equiv x_1(mod m_n) + (x_2 - x_1)(mod m_n) + ... + (x_n - x_{n-1})(mod m_n)$

$\bar{x} \equiv x_n(mod m_n)$

To prove uniqueness of solution.

Suppose $\bar{x}'$ is any other integer that satisfies the congruence in (4.1). Then,

$\bar{x} \equiv \bar{x}' \ (mod m_i) \ ; \ i = 1, 2, ..., n$

$\implies m_i |_{\bar{x} - \bar{x}'} \ ; \ i = 1, 2, ..., n$

Now, $(m_i, m_j) = 1$ for $i \neq j$.

We know that if $a|c$, $b|c$ and (a,b)=1 then $ab|c$.

$\therefore m_1 m_2 ... m_n \mid \bar{x} - \bar{x}'$

ie. $m|\bar{x} - \bar{x}'$

$\implies \bar{x} \equiv \bar{x}' (mod m)$

Thus we have proved the uniqueness part. □

4.2 RNS to Binary Conversion

We now propose the moduli set $S_1 = \{3^n, 3^n + 1, 3^n + 2\}$ for $n \geq 1$ and check that it is relatively prime. Also we will find its reverse converter set (inverse

set) using CRT-1 from chapter 2 and then find its reverse converter set (inverse set) using New CRT for RNS conversion ie. theorem (4.1.4).

4.2.1 Theorem:

The set $S_1 = \{3^n, 3^n + 1, 3^n + 2\}$ is a relatively prime set.

Proof : We need to prove that

(i) $(3^n, 3^n + 1) = 1$

(ii) $(3^n + 1, 3^n + 2) = 1$

(iii) $(3^n, 3^n + 2) = 1$

Check that (i) is trivial since 3^n is odd number.

Also (ii) is trivial since $3^n + 1$ will be even and it follows.

To prove (iii)

Suppose $p|_{3^n}$ and $p|_{3^n+2}$ where p is any prime.

Then by the properties of divisibility p divides $(3^n + 2) - (3^n)$.

ie.$p|_{(3^n+2)-(3^n)}$

ie. $p|_2$

But 3^n is always odd and $p|_{3^n}$ implies p is an odd number.

Hence $p = 1$ which proves (iii).

4.2.2 Theorem:

For the set S_1 , the multiplicative inverse set based on the CRT-1 is

$I_1 = \{\frac{1}{2}3^n + 1, 3^n, \frac{1}{2}(3^n + 3)\}$

Proof: Let $m = (3^n)(3^n + 1)(3^n + 2)$

$M_1 = (3^n + 1)(3^n + 2)$, $M_2 = 3^n(3^n + 2)$, $M_3 = 3^n(3^n + 1)$

Let

$$\begin{cases} x \equiv x_1 (mod 3^n) \\ x \equiv x_2 (mod 3^n + 1) \\ \vdots \\ x \equiv x_3 (mod 3^n + 2) \end{cases} \tag{4.4}$$

By the CRT-1 we shall show that the congruences in (4.4) has unique solution modulo $m = (3^n)(3^n + 1)(3^n + 2)$

ie. $x \equiv [M_1 k_1 x_1 + M_2 k_2 x_2 + M_3 k_3 x_3](mod m)$

for $k_1 = \frac{1}{2}3^n + 1$, $k_2 = 3^n$, $k_3 = \frac{1}{2}3^n + 3$

Claim(i): $M_1 k_1 \equiv 1(mod 3^n)$

We have $M_1 k_1 = (3^n + 1)(3^n + 2)(\frac{1}{2}3^n + 1)$

$= \frac{1}{2}(3^{3n} + 3^{2n} + 2.3^{2n} + 2.3^n + 3^{2n} + 3^n + 2.3^n + 2)$

$M_1 k_1 = \frac{1}{2}[3^{3n} + 4.3^{2n} + 5.3^n + 2]$

$M_1 k_1 - 1 = 3^n(\frac{3^{2n}}{2} + 2.3^n + \frac{5}{2})$

Claim(ii): $M_2 k_2 \equiv 1(mod 3^n + 1)$

We have $M_2 k_2 = (3^n)(3^n + 2)(3^n)$

$= (3^{2n} + 2.3^n)3^n$

$M_2 k_2 - 1 = (3^n + 1)(3^{2n} + 3^n - 1)$

Claim(iii): $M_3 k_3 \equiv 1(mod 3^n + 2)$

We have $M_3 k_3 = (3^n)(3^n + 1)(\frac{1}{2})(3^n + 3)$

$= (\frac{1}{2})(3^{3n} + 4.3^{2n} + 3.3^n)$

$M_3 k_3 = (3^n + 2)(\frac{3^{2n}}{2} + 3^n + \frac{3}{2})$

$M_3 k_3 - 1 = (3^n + 2)(\frac{3^{2n}}{2} + 3^n - \frac{1}{2})$

4.2.3 Theorem:

For the set S_1 , the multiplicative inverse set based on the New CRT for RNS conversion is $I_2 = \{3^n + 1, \frac{1}{2}(3^n + 1)\}$.

Proof: Let $M_1 = (3^n + 1)$, $M_2 = (3^n + 2)$, $M_3 = 3^n$

Let $x \equiv x_1(mod 3^n)$

$x \equiv x_2(mod 3^n + 1)$

$x \equiv x_3(mod 3^n + 2)$

By the New CRT (theorem 4.1.4) we need to show that

$x \equiv [x_1 + k_1M_1(x_2 - x_1) + k_2M_1M_2(x_3 - x_2)](modM_1M_2M_3)$

for $k_1 = 3^n + 1$, $k_2 = \frac{1}{2}3^n + 1$

Claim(i): $M_1k_1 \equiv 1(modM_2M_3)$

We have $M_1k_1 = (3^n + 1)(3^n + 1)$

$= 3^{2n} + 2.3^n + 1$

$M_1k_1 - 1 = 3^n(3^n + 2)$

Claim(ii): $M_1M_2k_2 \equiv 1(modM_3)$

We have $M_1M_2k_2 = (3^n + 1)(3^n + 2)(\frac{1}{2})(3^n + 1)$

$= \frac{3^{3n}}{2} + 2.3^{2n} + (\frac{5}{2})3^n + 1$

$M_1M_2k_2 - 1 = 3^n(\frac{3^{2n}}{2} + 2.3^n + \frac{5}{2})$

Example: Consider a weighted number x=256 and the moduli set 3,4,5,7. Then

x ≡ 1 (mod 3)

x ≡ 0 (mod 4)

x ≡ 1 (mod 5)

x ≡ 4 (mod 7)

Solution: We have to first find k_1,k_2,k_3 satisfying

$3k_1 \equiv 1 \pmod{4.5.7} \implies 3k_1 \equiv 1 \pmod{140}$

$3.4k_2 \equiv 1 \pmod{5.7} \implies 12k_2 \equiv 1 \pmod{35}$

$3.4.5k_3 \equiv 1 \pmod{7} \implies 60k_3 \equiv 1 \pmod{7}$

Thus we obtain k_1=47 , k_2=3 , k_3=2 satisfying above congruences.

$\therefore$ By new CRT for RNS we get;

$x \equiv x_1+k_1m_1(x_2-x_1)+k_2m_1m_2(x_3-x_2)+k_3m_1m_2m_3(x_4-x_3)\ (mod m_1m_2m_3m_4)$

$x \equiv 1+(-141)+36+360 \pmod{420}$

$x \equiv 256 \pmod{420}$ is the required solution.

Chapter 5

FAST ALGORITHM OF CHINESE REMAINDER THEOREM AND FIBONACCI NUMBERS

This chapter deals with a fast algorithm of CRT which will be later applied to Fibonacci numbers in section[5.2].

5.1 Fast Algorithm of Chinese Remainder theorem

In this section we will see the Fast Algorithm of CRT in detail. Before that let us first study the lemma required to prove the theorem.

5.1.1 Lemma: The system of congruence

$$\begin{cases} x \equiv a_1 (mod m_1) \\ x \equiv a_2 (mod m_2) \\ \vdots \\ x \equiv a_k (mod m_k) \end{cases} \tag{5.1}$$

is equivalent to the following system of congruence:

$$\begin{cases} M_1 x \equiv a_1 M_1 (mod M) \\ M_2 x \equiv a_2 M_2 (mod M) \\ \vdots \\ M_{k-1} x \equiv a_{k-1} M_{k-1} (mod M) \\ (\sum_{i=1}^{k} b_i M_i) x \equiv \sum_{i=1}^{k} a_i b_i M_i (mod M) \end{cases} \tag{5.2}$$

where b_i is relatively prime to m_i for i=1,2,...,k

Proof: We show the necessity part.

Suppose x is a solution of system (5.1) then for $i = 1, 2, ..., k$,

$x - a_i = c_i m_i$; where c_i is an integer.

Multiplying the above equation with M_i for each i we get

$M_i x - M_i a_i = c_i m_i M_i = c_i M$ for $i = 1, 2, ..., k$

which is rewritten as the congruence

$M_i x \equiv M_i a_i (mod M)$ for $i = 1, 2, ..., k$ ——-(i)

The first $k - 1$ congruences in system (5.2) are identical with those of equation(i) for $i = 1, 2, ..., k - 1$

The last congruence of system(5.2) can be obtained as a linear combination of equation(i).

Conversely, we assume that x is a solution of the system of congruence (5.2).

Since M_i and m_i are coprime, equation(i) can be reduced to

$x \equiv a_i (mod m_i)$ for $i = 1, 2, ..., k - 1$

Now subtracting the linear combination of the first $k - 1$ congrunces in (5.2), we have $b_k M_k x \equiv a_k b_k M_k (mod M)$

Since M_k and b_k are relatively prime to m_k, we conclude that

$x \equiv a_k(modm_k)$. $\square$

5.1.2 Lemma:

Under the same assumptions as in basic CRT and lemma [1], M is relatively prime to $\sum_{i=1}^{k} b_i M_i$

Proof: Let d be the gcd ($\sum_{i=1}^{k} b_i M_i$, M) and let p be a prime factor of d.

Then p divides $\sum_{i=1}^{k} b_i M_i$ and $M = \prod_{i=1}^{k} m_i$

The divisibility of M by p implies that p divides only one of m_i ; say m_j,

since $(m_i, m_j) = 1$ for $i \neq j$

Then p divides all M_i but $M_j = \frac{M}{m_j}$

Together with the divisibility of $\sum_{i=1}^{k} b_i M_i$ by p, we derive that p divides $b_j M_j$ and consequently divides b_j.

Hence p divides the gcd(m_j, b_j) which is equal to 1.

Next let us see what is the fast algorithm of CRT.

5.1.3 A Fast Algorithm of CRT

let $m_1, m_2, ..., m_k$ be pairwise relatively prime positive integers. Then there exists unique integer $x(modM)$ satisfying the system of congruence

$$\begin{cases} x \equiv a_1(modm_1) \\ x \equiv a_2(modm_2) \\ \vdots \\ x \equiv a_k(modm_k) \end{cases} \tag{5.3}$$

where M=m_1 m_2 ... m_k

The system (5.3) is equivalent to the following single linear congruence

$(\sum_{i=1}^{k} b_i M_i)x \equiv \sum_{i=1}^{k} a_i b_i M_i (mod M)$

where b_i's are arbitrary integers coprime to m_i's respectively and $M_i = \frac{M}{m_i}$, $i = 1, 2, ..., k$.

Proof: By lemma(5.1.1) we know that the congruence system(5.3) is equivalent to system(5.2).

From lemma(5.1.2), the last congruence has a unique solution, say $x_0(mod M)$. Thus the system(5.2) has a unique solution x_0 which implies that x_0 is the unique solution of the congruence system(5.3) since basic CRT assures the existence of unique solution of the system(5.3) modulo M.

Hence proved.

5.2 Fibonacci Numbers

In this section of the chapter 5 we will see how the theorem (5.1.3) is applied to Fibonacci numbers in the form of a corollary. Before the application we need to look at the definitions and results which will be used in the proof of the corollary. Let us see what are these results.

5.2(a) Definition: Fibonacci Sequence

Fibonacci sequence is a sequence in which each number is the sum of the two preceding ones. Numbers that are part of the Fibonacci sequence are known as Fibonacci numbers. ie.1,1,2,3,5,8,12,21,34,55,89,144,233,377,... is called the Fibonacci sequence and its terms are the Fibonacci numbers.

5.2.1 Theorem:

For the Fibonacci sequence, $(u_n, u_{n+1}) = 1$ for every $n \geq 1$.

Proof: Suppose that integer $d > 1$ divides both u_n and u_{n+1}.

ie. $d|u_n - u_{n+1}$

ie. $d|u_{n-1}$

Now d divides u_n and $u_{n-1} \implies d|u_n - u_{n-1}$ ie. $d|u_{n-2}$

Working in this way, at the end we will get $d|u_1$ and $u_1 = 1$ which is certainly not divisible by $d > 1$.

5.2.2 Theorem:

For $m \geq 1, n \geq 1$, u_{mn} is divisible by u_m.

Proof: We prove this by induction on n.

The result is certainly true for $n = 1$.

For the induction hypothesis, let us assume that u_{mn} is divisible by u_m for $n = 1, 2, ..., k$.

Now to prove for $n = k + 1$.

$u_{m(k+1)} = u_{mk+k}$

Now by using $u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$ we get,

$u_{m(k+1)} = u_{mk-1}u_m + u_{mk}u_{m+1}$

Since u_m divides u_{mk}, thus RHS (and hence the LHS) of this expression must be divisible by u_m .

Similarly, u_m divides $u_{m(k+1)}$.

Thus we have proved.

5.2.3 Lemma:

If $m = qn + r$, then $(u_m, u_n) = (u_r, u_n)$.

Proof: We know $u_{m(k+1)} = u_{mk-1}u_m + u_{mk}u_{m+1}$.

Now, $(u_m, u_n) = (u_{qn+r}, u_n) = (u_{qn-1}u_r + u_{qn}u_{r+1}, u_n)$

From theorem (5.2.2) and from the fact that $(a + c, b) = (a, b)$, whenever $b|c$, gives $(u_{qn-1}u_r + u_{qn}u_{r+1}, u_n) = (u_{qn-1}u_r, u_n)$

We claim that $(u_{qn-1}, u_n) = 1$

Let $(u_{qn-1}, u_n) = d$.

Then $d|u_n$ and $u_n|u_{qn}$ imply that $d|u_{qn}$ and thus d is a common divisor of the successive Fibonacci numbers u_{qn-1} and u_{qn}.

Now since successive Fibonacci numbers are relatively prime thus we get $d = 1$.

Now we know that if (a,c)=1 then (a,bc)=(a,b), using this we get;

$(u_m, u_n) = (u_{qn-1}u_r, u_n) = (u_r, u_n)$.

5.2.4 Theorem:

The greatest common divisor of two Fibonacci numbers is again a Fibonacci number; specifically, $gcd(u_m, u_n) = u_d$ where $d = gcd(m, n)$.

Proof: Assume that $m \geq n$.

Applying the Euclidean Algorithm to m and n, we get the following system of equations:

$m = q_1 n + r_1 \ 0 < r_1 < n$

$n = q_2 r_1 + r_2 \ 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3 \ 0 < r_3 < r_2$

.

.

.

$r_{n-2} = q_n r_{n-1} + r_n \; 0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n + 0$

In accordance with the previous lemma 5.2.3,

$(u_m, u_n) = (u_{r_1}, u_n) = (u_{r_1}, u_{r_2}) = \mathring{u}\mathring{u}\mathring{u} = (u_{r_{n-1}}, u_{r_n})$

Because $r_n | r_{n-1}$, theorem 5.2.2 tells us that $u_{r_n} | u_{r_{n-1}}$, where $(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$. But r_n, being the last non-zero remainder in the Euclidean Algorithm for m and n, is equal to (m, n).

Thus we get, $(u_m, u_n) = u_{(m,n)}$.

Now let us see how the fast algorithm is applied to Fibonacci numbers which is stated below in the form of a corollary.

5.2.5 Corollary: (Application of Fast Algorithm)

Let u_{n-1}, u_n, u_{n+1} be three successive terms of the Fibonacci sequence. Then the system of congruence,

$$\begin{cases} x \equiv a (mod u_{n-1}) \\ x \equiv b (mod u_n) \\ x \equiv c (mod u_{n+1}) \end{cases}$$

has a unique solution,

$x \equiv (-1)^{n+1}[a u_n u_{n+1} - (b u_{n-1} u_{n+1} + c u_{n-1} u_n)] (mod u_{n-1} u_n u_{n+1})$.

Proof: It is known that $(u_m, u_n) = u_{(m,n)}$

Thus we have $(u_{n-1}, u_n) = (u_n, u_{n+1}) = u_1 = 1$ and $(u_{n-1}, u_{n+1}) = u_1$ or $u_2 = 1$

Now,

$u_n u_{n+1} x \equiv a u_n u_{n+1} (mod u_{n-1} u_n u_{n+1})$

$u_{n-1} u_{n+1} x \equiv b u_{n-1} u_{n+1} (mod u_{n-1} u_n u_{n+1})$

$u_{n-1}u_nx \equiv cu_{n-1}u_n(modu_{n-1}u_nu_{n+1})$

Then by theorem (5.1.3),

$[u_nu_{n+1}-u_{n-1}(u_{n+1}+u_n)]x \equiv au_nu_{n+1}-(bu_{n-1}u_{n+1}+cu_{n-1}u_n)(modu_{n-1}u_nu_{n+1})$

$\implies (u_nu_{n+1}-u_{n-1}u_{n+2})x \equiv au_nu_{n+1}-(bu_{n-1}u_{n+1}+cu_{n-1}u_n)(modu_{n-1}u_nu_{n+1})$

Now since $u_nu_{n+1} - u_{n-1}u_{n+2} = (-1)^{n-1}$

Thus we get

$(-1)^{n-1}x \equiv au_nu_{n+1} - (bu_{n-1}u_{n+1} + cu_{n-1}u_n)(modu_{n-1}u_nu_{n+1})$

Hence $x \equiv (-1)^{n+1}[au_nu_{n+1} - (bu_{n-1}u_{n+1} + cu_{n-1}u_n)](modu_{n-1}u_nu_{n+1})$.

ANALYSIS AND CONCLUSIONS

In this project we have shown expansion of Chinese Remainder theorem in other areas of mathematics ie. to coprime polynomials, monoid Rings and Groups. We have also shown some other forms of Chinese Remainder theorem namely, the CRT for finding reverse converter set for Converting RNS to Binary system and the Fast Algorithm that we have applied to Fibonacci numbers. Here we have shown their applications not only restricted to mathematics but also to some real life problems. Chinese Remainder theorem not only has these applications but it is also used in computer coding and digital signal processing through RNS and also in cryptography.

Chinese Remainder theorem might look like a small topic to study but if you start exploring its various applications its really an interesting topic to study and will surely help in future in coding and many other areas too.

Bibliography

[1] Q. Luo, Research and application of chinese remainder theorem, Theoretical and Natural Science 9 (2023) 45–53. doi:10.54254/2753-8818/9/20240711.

[2] E. Alhassan, J. Bunyan, G. Abe-I-kpeng, On some algebraic properties of the euclidean algorithm with applications to real life, Research Journal of Mathematics and Statistics 6 (2014) 49–55. doi:10.19026/rjms.6.5271.

[3] E. Alhassan, K. Tian, O. Abban, I. Ohiemi, M. Adjabui, G. Armah, S. Agyemang, On some algebraic properties of the chinese remainder theorem with applications to real life, Journal of Applied Mathematics and Computation 5 (2021) 219–224. doi:10.26855/jamc.2021.09.008.

[4] R. S, New chinese remainder theorem and moduli sets, MATHEMATICAL SCIENCES RESEARCH JOURNAL 4 (2015) 179–181.

[5] K. Nagasaka, P. Shiue, C. Ho, A fast algorithm of the chinese remainder theorem and its application to fibonacci numbers (01 1991). doi:10.1007/978-94-011-3586-$3_2$7.

[6] B. Fraleigh , J. (2013). "A first course in abstract algebra" (7th ed.). "Pearson Education India."

[7] Burton, D. M. (2011). "Elementary number theory." McGraw-Hill.

[8] Law Huong Ing “The History of the Chinese Remainder Theorem”,Mathematical Madley, volume 30, June 2003.