College of Natural and Computational Science

Department of Mathematics

congruence and system of linear congruence

Prepared by:Damaku Wakuma

Advisor:Mr. Yusuf Hussein (M.S.c)

A Project Submitted to the Department of Mathematics, Wolkite University in Partial Fulfillment of the Requirements of the Bachelor of Science Degree in Mathematics

January, 2021

Contents

Wolkite University

Department of Mathematics

The undersigned hereby certify that they have read and recommend to the Department of Mathematics for acceptance of a project entitled **Project topic** by Student name in partial fulfillment of the requirements for the degree of Bachelor of Science.

Dated: January, 2021

Advisor: _____

Advisor name

Examining committee: _____

_____

January, 2021

Acknowledgment

First of all,I am grateful to Jesus who makes all my planes succeed according to his good will and in whom all things all things are made possible.I wish to express my grateful thanks and deep appreciation to my adviser Mr. Yusuf Husen extremely useful comments during preparation of this final project. finally I would like to say thanks to all my family because always giving a special comment for me.

Abstract

This project deals about Congruence,properties of congruence, linear congruence, system of linear congruence and chinese remainder theorem .it contains two chapters.the first chapter is deals about defnition of congruence and its examples and properties of congruence the second chapter deals about system of linear congruence solvability of system of linear congruence and chinese remainder theoerem.and it contains many subsections under each chapter.

Notations

$a \equiv b(modm)$	a is congruent to b modulo m
$a \not\equiv b(modm)$	a is not congruent to b modulo m
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\equiv$	the symbol of congruence
$d = (a, m)$	d represent the greatest common
divisors of a and m	
CRS	complete residue system
gcd	greatest common divisor
Z	integers

Chapter 1

congruence

1.1 Introduction

Congruence is a refined statement of divisibility.Congruence provides us with algebraic machinery for the study of divisibility property of integers. In this chapter we shall discuss the theory of congruence.

1.2 Notion of congruence

Definition 1.2.1. .

Let m be a fixed integer. Then an integer a is said to be congruent to another integer b if m divides the difference of a and b. This is symbolically written as

$a \equiv b(modm)$..... *(1).*

We call m the modulus of the congruence

If $m \nmid (a-b)$, *We write* $a \not\equiv bmod(m)$, *and say that a and b are incongurent modulo m.*

Example 1.2.1. $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8(mod6)$ *But* $7 \not\equiv 4(mod6)$ *Because* $6 \nmid 7-4$ *That means* $6 \nmid 3$

Expression (1) is called the congruence, m is called the modulus of the congruence and b is called a residue of a with modm.

Example 1.2.2.

$37 \equiv 57(mod10)$,since $37 - 57 = -20$ is a multiple of 10 i. e $10 \mid 37 - 57$ $\exists -2 \in Z$ such that $-20 = -2 \cdot 10$

Example 1.2.3. $17 \equiv 5(mod6)$,*since* $6 \mid 17 - 5 = 6 \mid 12$

Definition 1.2.2. *If n is a positive integer,we say the integers a and b are congruent modulo of n,and write $a \equiv b(modn)$,if they have the same remainder on division by n*

Theorem 1.2.1. *$a \equiv b(modn)$ if and only if a and b have the same remainder with respect to n.*

***proof**: Let $a \equiv b(modn)$ let r_1 andr_2 be remainders of a and b respectively with respect to n. that means*

$a = mq_1 + r_1$, $0 \leq r_1 < m$ .....*(1) and*

$b = mq_2 + r_2$, $0 \leq r_2 < m$.....*(2) for some integers q_1 and q_2*

We have to show that $r_1 = r_2$

since $a \equiv b(modn)$,we have

$(mq_1 + r_1 \equiv (mq_2 + r_2)(modn)$

$\implies m \mid [(mq_1 + r_1) - (mq_2 + r_2)]$

$\implies m \mid [(m(q_1 - q_2) + (r_1 - r_2))]$

$\implies m \mid (r_1 - r_2)$

$r_1 - r_2 = 0$ *(because r_1 and r_2 are positive integers less than m).this gives that*

$r_1 = r_2$

conversely,let $r_1 = r_2$.then from (1) and (2) we have $a - b = m(q_1 - q_2)$

$\implies a \equiv b(modn)$

This completes the proof.

Example 1.2.4. 37 *and* 57 *are* $\equiv (mod10)$,*since both* 37 *and* 57 *have the same remainder of* 7 *when divided by* 10

1.3 Basic properties of congruences

Theorem 1.3.1. *let $n > 0$ and let $a, b, c, \in Z$*

a. $a \equiv a(modn)$ *.....reflexive*

b. if $a \equiv b(modn)$ *then* $b \equiv a(modn)$ *.....symmetry*

c. if $a \equiv b(modn)$ *and* $b \equiv c(modn)$*,then* $a \equiv c(modn)$*. .....transitive*

proof:

(a) $a - a = 0$ and $n \mid 0$,hence $a \equiv a(modn)$

(b) $a \equiv b(modn)$ means that $a - b = nk$ for some $k \in Z$.
Therefore,$b - a = -nk = n(-k)$;hence $b \equiv a(modn)$

(c) If $a \equiv b(modn)$ and $b \equiv c(modn)$,Then
$a - b = nk$ again
$b - c = nk'$
Adding these two equations yields,
$(a - b) + (b - c)$=nk+nk'
$= a - b + b - c = n(k + k')$
$= a - c = n(k + k')$
and also $a \equiv c(modn)$
Therefore congruence modulo of n is equivalence relation.

Theorem 1.3.2. *If* $a \equiv b(modn)$ *and* $c \equiv d(modn)$*, Then*

(d) $a + c \equiv b + d(modn)$

(e) $ac \equiv bd(modn)$

(f) $a + c \equiv b + c(modn)$

(g) $ac \equiv bc(modn)$

Proof:

(d) By the definition of congruence there are integers s and t such that $a - b = sn$ and $c - d = tn$.Therefore adding $b + d$ to both sides of the equation,
$a + c = b + d + n(s + t)$
Hence,$a + c \equiv b + d(modn)$

(e) using the fact that $-bc + bc = 0$ we have,
$ac - bd = ac + 0 - bd$
$= ac + (-bc + bc) - bd$
$= c(a - b) + b(c - d)$
$= c(sn) + b(tn)$
$= n(cs + bt)$
and so $n \mid (ac - bd)$.Hence $ac \equiv bd(modn)$

(f) If $a \equiv b(modn)$ then $n \mid a - b$.if we add and subtract we get $n \mid (a + c) - (b + c)$
$\implies a + c \equiv b + c(modn)$

(g) If $a \equiv b(modn)$ then $n \mid a - b$.thus,there exist an integer k such that $a - b = nk$
$\implies ac - bc = n(ck)$
$\implies n \mid ac - bc$
$\implies ac \equiv bc(modn)$

Theorem 1.3.3. *(cancellation law)*
If a,b and c are integers such that $ac \equiv bc(modm)$,$m > 0$ *is a fixed integers and* $d = (c, m)$ *then,*
$a \equiv b(mod\frac{m}{d})$

Proof: since $d = (c, m)$ there exist integers q_1 and q_2 such that $c = dq_1$, $m = dq_2$ and $(q_1, q_2) = 1$, Now we have $ac \equiv bc(modm)$
$\implies m \mid (ac - bc)$

$\implies m \mid c(a-b)$

$\implies m \mid dq_1(a-b)$, (because $c = dq_1$)

$\implies \frac{m}{d} \mid q_1(a-b)$, (because $q_2 = \frac{m}{d}$)

$q_2 \mid (a-b)$, (because $(q_1 q_2)) = 1$

$\implies a \equiv b(mod q_2)$

$a \equiv b(mod \frac{m}{d})$

Definition 1.3.1. *Let a and n be integers with $n > 0$.The congruence class of a modulo n denoted $[a]_n$,is the set of all integers that are congruent to modulo n,that means $[a]_n = \{z \in Z | a - z = kn\}$ for some $k \in Z$*

Example 1.3.1. *In congruence modulo 2 we have*

$[0]_2 = \{..., -4, -2, 0, 2, 4, ...\}$

$[1]_2 = \{..., -7, -5, -3, -1, 1, 3, 5, 7, ...\}$

Thus,the congruence classes of 0 and 1 are,respectively the sets of even and odd integers.

***Note**:we observe that the set of integers is divided into m different sets called congruent classes modulo m, each containing integers that are mutually congruent modulo m. See the following example:*

Example 1.3.2. *The Four congruence classes modulo two are given by by:*

$... \equiv -12 \equiv -4 \equiv 0 \equiv 6 \equiv 12 \equiv ...mod2$

$... \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv ...mod2$

$... \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv ...mod2$

$... \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv ...mod2$

Suppose that m is a positive integer. Given an integer a, by the division algorithm we have $a = bm + r$, where $0 \leq r \leq m-1$ We call r the least non negative residue of modulo m. we say that r is the result of reducing a modulo m.

Similarily, when we know that a is not divisible by m we call r the least positive residue of a modulo m.

Definition 1.3.2. *Let $n \in N$. A collection of n integers $S = \{a_1, a_2, a_3, ..., a_n\}$ is called a complete residue system modulo n or a CRS if every integer b is congruent modulo n to exactly one of the elements in S.*

Example 1.3.3. *The set* $\{10, 8, 2, 14, 21\}$ *forms a CRS modulo 5.*
Let $Z_N = \{0, 1, 2, ..., n-1\}$. *The set* Z_n *is the set of least positive residues modulo n.*

Definition 1.3.3. *Consider* Z_n. *We define addition and multiplication modulo n as follow:*

1 ***Addition:*** *If* $a, b \in Z_n$,*then* $a + b(modn)$ *is the least positive residue modulo n.*

2. ***Multiplication:****If* $a, b \in Z_n$,*then* $ab(modn)$ *is the least positive residue modulo n.*

3. ***Negative of a least residue:****If* $a \in Z_n$,*then* $-a = b$ *if* $a + b = 0$ *in* Z_n

1.3.1 Residue class

Given any integer a,the collection of all integers congruent to a modulo n is known as as the residue class,or congruence class,of a modulo n.

The word 'residue' means 'remainder'.
This term is used because the residue class of a modulo n is the class of those integers that have the same remainder on divison by as a does.

1.3.2 Least residue

The least residue of a modulo n is the remainder r that you obtain when you divide a by n. The integer r is one of the numbers,$0, 1, ..., n-1$,and it satisfies $a \equiv r(modn)$

Example 1.3.4. *Find the least residue of -33 modulo 7*
solution: *That means find the quotient and remainder when you divide -33 by 7. to do this, First notice that* $-5 < -33/7 < -4$, *so the quotient is -5,the remainder is then given by* $a - qn$ *since*$-33 = 7 * (-5) + 2$ *Hence the least residue is 2.*

Theorem 1.3.4. *For every a and p, p prime,*$a^p \equiv a(modp)$

Proof: when $p \mid a$ the statement obviously holds; for in this setting, $a^p \equiv a \equiv 0(modp)$ .if $p \nmid a$, then $gcd(a,p) = 1$ and $\phi p = p-1$, and we have $a^{p-1} \equiv 1(modp)$ when this congruence is multiplied by a, the conclusion $a^p \equiv a(modp)$ follows

Theorem 1.3.5. *If a,b,k and m are integers such that* $k > 0$,$m > 0$, *and* $a \equiv b(modm)$,*then*
$a^k \equiv b^k(modm)$

proof:

Because $a \equiv b(modm)$,we have $m \mid (a-b)$.since $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b_+... + ab^{k-2} + b^{k-1})$ We see that $(a-b) \mid (a^k - b^k)$
Therefore it follows that $m \mid (a^k - b^k)$

Example 1.3.5. $7 \equiv 2(mod5)$
$343 = 7^3 \equiv 2^3 \equiv 8(mod5)$

Theorem 1.3.6. *: If* $a \equiv b(modm_1)$,$a \equiv b(modm_2)$,...$a \equiv b(modm_k)$ *Where a, b* ,$m_1, m_2, ..., m_k$ *are integers with* $m_1, m_2, ..., m_k$ *positive, then*
$a \equiv b(mod)[m_1, m_2, ..., m_k]$
where $[m_1, m_2, ..., m_k]$ *is the least common multiple of* $m_1, m_2, ..., m_k$
an immediate and useful consequence of this theorem is the following result.

corollory .If $a \equiv b(modm_1)$,$a \equiv b(modm_2)$,...,$a \equiv b(modm_k)$ where a and b are integers and $m_1, m_2, ..., m_k$ are relatively prime positive integers,then $a \equiv b(modm_1m_2...m_k)$
Proof: Since $m_1, m_2, ..., m_k$ are pairwise relatively prime $[m_1, m_2, ..., m_k] = m_1m_2...m_k$
Hence, from theorem above $a \equiv b(modm_1m_2...m_k)$

1.4 Application of congruences

Congruences are helpful in carrying out certain types of computations

Example 1.4.1. *What is the remainder when* 4^{30} *is divided by 23?*
Solution*:since* $4^3 = 64 \equiv -5(mod23)$.
We have $4^6 \equiv (-5)^2 \equiv 2(mod23)$
Hence $4^{30} \equiv (2)^5 \equiv 9(mod23)$

Thus the remainder is 9

Congruences often arise in everyday life. For instance, clocks work either modulo 12 or 24 for hours, and modulo 60 for minutes and seconds. calendars work modulo 7 for days of the week and modulo 12 for months. Utility meters often operate modulo 1000, and odometers usually work modulo 100000. In working with congruences, it is often useful to translate them into equalities

Example 1.4.2. *prove that for any natural number n* $17^n-12^n-24^n+19^n$ *is divisible by 35*

***solution**:let* $N = 17^n-12^n-24^n+19^n$.*Now* $35 = lcm(5,7)$ *so to check that* $35 \mid N$*it is enough to show that* $5 \mid N$ *and* $7 \mid N$

***Remember**:*$N \equiv 0(modm)$ *means exactly the same thing as* $m \mid N$

-*Firstly,*$N = 17^n-12^n-24^n + 19^n$

$\equiv 2^n-2^n-4^n+4^n(mod5)$ *dividing all bases by 5 and putting their remainder*

$\equiv 0(mod5)$ *and hence* $5 \mid N$

-*Similarily,* $N = 17^n-12^n-24^n+19^n$

$\equiv 3^n-5^n-3^n+5^n(mod7)$

$\equiv 3^n-3^n-5^n+5^n(mod7)$

$\equiv 0(mod7)$

and hence $7 \mid N$ *Thus, since* $5 \mid N$ *and* $7 \mid N$ *we have* $35 = lcm(5,7)$ *divides* $N = 17^n-12^n-24^n+19^n$

Chapter 2

linear congruence

An expression of the form $ax \equiv b(modm)$,$a \not\equiv 0(modm)$.....(1) is called a linear congruence mod m.

An integer x_0 for which $ax_0 \equiv b(modm)$ is called a solution of linear congruence $ax \equiv b(modm)$

Now, $ax_0 \equiv b(modm) \implies m \mid (ax_0 - b)$

$\implies \exists$ an integer y_0 such that $ax_0 - b = my_0$

$\implies ax_0 - my_0 = b$

This shows that (x_0, y_0) is a solution of the linear Diophantine equation

$ax - my = b$.....(2)

Linear diophantine equation (2) has a solution if $d = (a, m)$ divides b.

If (x_0, y_0) is a particular solution of (2) then the general solution is given by

$x = x_0 + \frac{m}{d}t$, $y = y_0 + \frac{a}{d}t$ where t is any integer

Theorem 2.0.1. *The linear congruence $ax \equiv b(modm)$ has a solution if and only if $d \mid b$,where $d = (a, m)$*

proof:

We have observed that the linear congruence $ax \equiv b(modm)$ is equivalent to the linear Diophantine equation $ax - my = b$ which is solvable if and only if $d \mid b$.

if (x_0, y_0) is its solution then,

$x = x_0 + \frac{m}{d}t$, $y = y_0 + \frac{a}{d}t$ are the other solutions.

We consider the solution

x_0, $x_0 + \frac{m}{d}$, $x_0 + 2\frac{m}{d}$,...,...,$x_0 + \frac{d-1}{d}m$

Now we shall show that these solutions are mutually in congruent solutions of the linear congruences $ax \equiv b(modm)$

For if $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2(modm)$, $0 \leq t_1 < t_2 \leq d-1$, then we have

$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2(modm)$.....(1)

Now $\frac{m}{d}, m = \frac{m}{d}$ therefore (1) implies $t_1 = t_2(modd)$

$\implies d \mid (t_2 - t_1)$

But this is impossible as $0 < t_2 < t_1 < d$

Theorem 2.0.2. *Let $ax \equiv b(modm)$, $(a, m) = d$ and $d \mid b$.Then the given linear congruence has d incongruent solutions (modm).*

proof: We have already shown that $x_0 + \frac{m}{d}t$ is the solution of the given linear congruence. we have to show that they are exactly d incongruent solutions (modm).

By division algorithm we write,

$t = qd + r$, where $0 \leq r \leq d-1$

Therefore,

$x_0 + \frac{m}{d}t = x_0 + \frac{m}{d} \cdot (qd + r)$

$= x_0 + mq + \frac{m}{d}r$

$\equiv x_0 + \frac{m}{d}r(modm)$

Thes solutions are d in numbers thus,the given linear congruence has exactly d incongruent solutions (modm)

corollary: The linear congruence $ax \equiv b(modm)$ has a unique solution if and only if $(a, m) = 1$

Definition 2.0.1. *If a' is a solution of the congruence $ax \equiv 1(modm)$, then a' is called a multiplicative inverse of a modulo m.*

a has a multiplicative inverse modulo m if and only if a and m are relatively prime,and the inverse of a,if it exists,is unique.

2.1 solvability of a linear congruence $ax \equiv b(modm)$

2.1.1 solvability of linear congruence of one variable

The solvability of a linear congruence $ax \equiv b(modm)$ can be easily be described by the following:

i. If a and m are relatively prime then there is precisely one incongruent solution modulo m

ii. If the greatest common divisor of a and m does not divide b,then the linear congruence has no solution,and

iii. If the gcd of a and m does divide b, then there are exactly (a, m) distinct incongruent solutions modulo m.

Example 2.1.1. *solve the linear congruence* $18 \equiv 30(mod42)$

Solution: *Rewrite the given congruence interms of linear diophantine equation*

$18x - 42y = 30$

step1:Find $d = gcd(a, n) \implies$ *gcd(18,42)*

By using Euclidean Algorithm

$42 = 2 * 18 + 6$

$18 = 3 * 6 + 0$

Therfore,$d = gcd(18, 42) = 6$

step2.does $d \mid b \implies 6 \mid 30$*?yes ,since* $\exists\ 5 \in Z$ *such that* $30 = 5 * 6$

Hence,the linear congruence $18x \equiv 30(mod42)$ *has 6 incongruent solution.*

step3.find particular solution

To find the particular solution, express the gcd as a linear combination of of 18 and 42.

$6 = 42 - 2(18)$

$6 = -2 * 18 + 42$

$(6 = -2 * 18 + 42)5$

$30 = -10 * 18 + 5(42) \equiv 18x_0 - 42y_0 = 30$

$x_0 = -10$

step4.find the six incongruent solutions

$x = x_0 + \frac{n}{d}t, t \in Z$

$x = -10 + \frac{42}{6}t, t = 0, 1, 2, 3, 4, 5$

$x = -10 + 7t, t = 0, 1, 2, 3, 4, 5$

$x_0 = -10$ *but by adding 42 on it we get* $x_0 \equiv 32(mod 42)$

$x_1 = -3$ *again adding 42 on it we get* $x_1 \equiv 39(mod 42)$

$x_2 \equiv 4(mod 42)$

$x_3 \equiv 11 mod(42)$

$x_4 \equiv 18(mod 42)$

$x_5 \equiv 25(mod 42)$

Therfore,$x \equiv 4, 11, 18, 25, 32, 39(mod 42)$

Example 2.1.2. *Solve the linear congruence* $17x \equiv 9(mod 276)$

Solution*:rewrite the given congruence interms of linear Diophantine equation*

$17x - 276y = 9$

step1.find $d = gcd(276, 17)$

By using Euclidean Algorithm: $276 = 16 * 17 + 4$

$17 = 4 * 4 + 1$

$4 = 4 * 1 + 0 \implies d = 1$ *,since the last non zero remainder is the gcd of (276.17)*

step2.check that $1 \mid 9$*? yes, since* $\exists\ 9 \in Z$ *such that* $9 = 9 * 1$

Hence,the linear congruence $17x \equiv 9(mod 276)$ *has a unique solution*

step3.find a particular solution.

To find a particular solution express 1 that means $gcd(17, 276)$ *as a linear combination of 17 and 276*

$1 = 17 - 4 * 4$

$= 17 - 4(276 - 16 * 17)$

$= 17 - 4(276) + 64 * 17$

$= 65(17) - 4(276)$

$(1 = 65 * 17 - 4(276))9$

$9 = 585(17) - 36(276)$

$\therefore x_0 = 585$ *and* $y_0 = -36$

step4. The general solution is $x = x_0 + \frac{n}{d}t, t = d - 1, t = 0$

$x = 585 + 276t but\ t = 0$

$x = 585 + 276(0)$

$\therefore x \equiv 585(mod276)$

Example 2.1.3. *solve the linear congruence* $36x \equiv 8(mod102)$

Solution:*rewrite the linear congruence interms of linear diophantine equation*

$36x - 102y = 8$

By using Euclidean Algorithm

$102 = 2 * 36 + 30$

$36 = 1 * 30 + 6$

$30 = 5 * 6 + 0$

$\therefore d = 6$

step1.check that $d \mid b$*? this means* $6 \mid 8$*?No ,because* $6 \nmid 8$

$\therefore$ *The given linear congruence* $36x \equiv 8(mod102)$ *has no solution*

2.1.2 solvability of linear congruence of two variable

An expression $ax+by \equiv c(modn)$ has a solution if and only if gcd (a,b,n) divides c. The condition for solvability holds if either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$. Say $\gcd(a, n) = 1$ when the congruence is expressed as $ax \equiv c - by(modn)$

Example 2.1.4. *solve the congruence* $7x + 4y \equiv 5(mod12)$

Solution: $7x \equiv 5 - 4y(mod12)$

$7x \equiv 5 - 4(5(mod12)(mod12))$, *subistitute* $y \equiv 5(mod12)$ *gives,*

$7x \equiv -15(mod12)$

$-5x \equiv -15(mod12)$

$\therefore x \equiv 3(mod12)$ *and* $y \equiv 5(mod12)$ *is the solution of the given congruence*

2.2 System of linear congruence

The focus of our concern here is how to solve a system of two linear congruence in two variable with the same modulo

Theorem 2.2.1. *The system of linear congruence*

$ax + by \equiv r(modn)$

$cx + dy \equiv s(modn)$ *has a unique solution modulo n whenever gcd* $(ad - bc, n) = 1$

Example 2.2.1. *consider the system*

$7x + 3y \equiv 10(mod16)$

$2x + 5y \equiv 9(mod16)$

solution: *we have* $a = 7$, $b = 3$, $c = 2$, $d = 5$

$gcd(7 * 5 - 3 * 2, 16) = gcd(35 - 6, 16) = gcd(29, 16) = 1$ *since gcd* $(ad - bc, n) = gcd(29, 16) = 1$*,hence the system has a unique solution.it is solved by using the above theorem,multiplying the first congruence by 5,the second congruence by 3,and substracting, we arrive at:*

$35x + 15y \equiv 50(mod16)$

$6x + 15y \equiv 27(mod16)$

$\Longrightarrow 29x \equiv 23(mod16)$ *or dividing 29 and 23 by 16 the remainders are respectively 13 and 7 and we write as*

$13x \equiv 7(mod16)$ *and multiplying by 5 we obtain*

$65x \equiv 35(mod16)$

$x = 3(mod16)$ *by dividing 65 by 16 and 35 by 16 the remainders are respectively 1 and 3.*

$\therefore x \equiv 3(mod16)$ *is a unique solution and to obtain the value of y multiply the first system by -2 and the second by 7 and we arrive*

$-2(7x + 3y \equiv 10(mod16))$

$7(2x + 5y \equiv 9(mod16))$

$29y \equiv 43(mod16)$ *upon dividing 29 and 43 by 16 the remainders are respectively, 13 and 11.then*

$13y \equiv 11(mod16)$ *by multiplying by 5 we arrive at*

$65y \equiv 55(mod16)$ *dividing 65 and 55 by 16 the remainders are respectively 1 and 7.*

$\therefore y \equiv 7(mod16)$ *is a solution of the given congruence*

The unique solution of our system turns out to be

$\therefore x \equiv 3(mod16)$ *and* $y \equiv 7(mod16)$

Theorem 2.2.2. *The Chinese Remainder theorem*

let $m_1, m_2, m_3, ..., m_r$ *be pair wise relatively prime numbers such that* $(m_i, m_j) = 1$ *for* $i \neq j$*.Then the system of linear congruence*

$x \equiv a_1(modm_1)$

$x \equiv a_2(modm_2)$

$x \equiv a_3(modm_3)$

$\vdots$

$x \equiv a_r(modm_r)$

has a simultaneous solution which is unique modulo $m_1 \cdot m_2 m_3 ... m_r$

Proof: Let $m = m_1 \cdot m_2 \cdot m_3 ... m_r$ and let for each $k = 1, 2, 3, ...r$

$M_k = \frac{m}{m_k} = m_1 \cdot m_2 \cdot m_3 \cdot m_4 ... m_{k-1} \cdot m_{k+1} ... m_r$ Since m_i are relatively prime in pairs, we have $(M_k, m_k) = 1$

Therefore,it is possible to solve the linear congruence $M_k x \equiv 1(modm_k)$. It will have a unique solution,say x_k.Now,we shall show that

$\bar{x} = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + ..., a_r M_r x_r$ is a simultaneous solution of the given system. we have $M_i \equiv 0(modm_k)$ for $i \neq k$ as $m_k \mid M_i$

Therefore, $\bar{X} = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + ..., a_r M_r x_r \equiv a_k M_k x_k (modm_k)$.

Therefore, $\bar{X} \equiv a_{k1} \equiv a_k (modm_k)$

This shows that a solution to the given system of congruence exists.

uniqueness:-Suppose $\bar{X_1}$ and $\bar{X_2}$ are two solutions to the given system. then

$\bar{X_1} \equiv a_k \equiv X_2(\bar{m}odm_k)$, k=1,2,3,...r.

$\implies M_k \mid \bar{X_1} - \bar{X_2}$ for each k.

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

$m = m_1 m_2 m_3 m_4 ... m_r \mid \bar{X_1} - \bar{X_2}$

Therefore, $\bar{X_1} \equiv \bar{X_2}(modm)$ this proves the uniqueness.

Example 2.2.2. *Solve the system of linear congruence:*

$x \equiv 2(mod 5)$

$x \equiv 3(mod 13)$

***Solution**:*

Here $a_1 = 2$, $a_2 = 3$

$m_1 = 5$, $m_2 = 13$

$m = m_1 \cdot m_2$

since, $gcd(5, 13) = 1$ *therefore,5 and 13 are relatively prime*

$m = 5 \cdot 13 = 65$

$M_1 = \frac{m}{M_1} = \frac{65}{5} = 13$

$M_2 = \frac{m}{M_2} = 5$

$13x_1 \equiv 1(mod 5)$,$x_1 = 2(mod 2)$

$5x_2 \equiv 1(mod 13)$, $x_2 = 8(mod 13)$

$X = a_1 m_1 x_1 + a_2 m_2 x_2$

$= 2 \cdot 13 \cdot 2 + 3 \cdot 5 \cdot 8(mod 65)$

$= 172(mod 65)$

$x = 42(mod 65)$

Example 2.2.3. *Solve the system of linear congruence:*

$x \equiv 2(mod 3)$

$x \equiv 5(mod 4)$

$x \equiv -3(mod 7)$

***Solution**:*

Here, $a_1 = 2$, $a_2 = 5$, $a_3 = -3$

$m_1 = 3$, $m_2 = 4$, $m_3 = 7$

Since 3,4 and 7 all are relatively prime to one another i.e

$gcd(3, 4) = gcd(4, 7) = gcd(3, 7) = 1$

We have $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 7 = 84$ *and* $M_1 = \frac{84}{3} = 28$

$M_2 = \frac{84}{4} = 21$

$M_3 = \frac{84}{7} = 12$ *. Now we will calculate* x_i *for the linear congruence*

$M_i x_i \equiv 1(mod m_1)$ *where* x_i *is the multiplicative inverse of* M_i

Now, $M_1x_1 \equiv 1(modm_1)$ *where* x_1 *is the multiplicative inverse of* M_1

$28X_1 \equiv 1(mod3)$, $x_1 = 1$

$21x_2 \equiv 1(mod4)$, $x_2 = 1$

$12x_3 \equiv 1(mod7)$, $x_3 = 3$

$X = a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3$

$X = 2 \cdot 28 \cdot 1 + 5 \cdot 21 \cdot 1 + 5 \cdot 21 \cdot 1 + -3 \cdot 12 \cdot 3(mod84)$

$x = 56 + 105 - 108(mod84)$

$\therefore x \equiv 53(mod84)$

To verify $x = 53$ *is a solution of the linear congruence*

$53 \equiv 2(mod3)$ *since* $3 \mid 53 - 1$

$53 \equiv 5(mod4)$ *since* $4 \mid 53 - 5$

$53 \equiv -3(mod7)$ *since* $7 \mid 53 - (-3)$

Example 2.2.4. *solve the system of linear congruence:*

$x \equiv 1(mod2)$

$x \equiv 2(mod3)$

$x \equiv 3(mod5)$

$x \equiv 4(mod7)$

Solution: *Here,* $a_1 = 1$, $a_2 = 2$,$a_3 = 3$, $a_4 = 4$

$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$

since 2 ,3 5 and 7 are relatively prime to one another so we can find x

$m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$M_1 = \frac{m}{m_1} = \frac{210}{2} = 105$

$M_2 = \frac{m}{m_2} = \frac{210}{3} = 70$

$M_3 = \frac{m}{m_3} = \frac{210}{5} = 42$

$M_4 = \frac{m}{m_4} = \frac{210}{7} = 30$

$105x_1 \equiv 1(mod2)$,$x_1 = 1$

$70x_2 \equiv 1(mod3)$, $x_2 = 1$

$42x_3 \equiv 1(mod5)$, $x_3 = 3$

$30x_4 \equiv 1(mod7)$, $x_4 = 4$

By Chinese theorem:

$X = 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 4 \cdot 30 \cdot 4$

$= 105 + 140 + 378 + 480(mod 210)$

$= 1103 \equiv 53(mod 210)$

To verify $x = 53$ *is a solution of the linear congruence*

$53 \equiv 1(mod 2)$ *since* $2 \mid 53 - 1$

$53 \equiv 2(mod 3)$ *since* $3 \mid 53 - 2$

$53 \equiv 3(mod 5)$ *since* $5 \mid 53 - 3$

$53 \equiv 4(mod 7)$ *since* $7 \mid 53 - 4$

2.2.1 Solvability condition of a system of linear congruence

A system of linear congruences

$x \equiv a_1(mod m_1)$

$x \equiv a_2(mod m_2)$

$x \equiv a_3(mod m_3)$

$\vdots$

$x \equiv a_r(mod m_3)$ is solvable if and only if (m_i, m_j) divides $(a_i - a_j)$.

Example 2.2.5. *solve the system of linear congruence:*

$x \equiv 1 mod(5)$

$x \equiv 4 mod(9)$

$x \equiv 6 mod(7)$

solution: *Here* $a_1 = 1$ *,*$a_2 = 4$ *,*$a_3 = 6$

Since gcd 5,9 *and* 7 *all are relatively prime to one another i.e* $gcd(5, 9)$=$gcd(9, 7)$=$gcd(5, 7) =$ 1.

So we can find x.

We have $n = n_1 \cdot n_2 \cdot n_3 = 5 \cdot 9 \cdot 7 = 315$ *and*

$N_1 = n/5 = 63$

$N_2 = n/9 = 35$

$N_3 = n/7 = 45$

Now we will calculate x_i *for the linear congruence*

$N_i x_i \equiv 1(mod n_i)$ *where* x_i *is the multiplicative inverse of* N_i

Now $N_i x_i \equiv 1 mod(n_1)$ *where* x_i *is the multiplicative inverse of* N_1

$\implies 63x_1(mod5) = 1$

$\implies 3x_1(mod5) = 1$ *Since* $63 \equiv 3(mod5)$

$x_1 = 2$

Similarly ,$N_2X_2 = 1(mod9)$

$35x_2(mod9) = 1$

$x_2 = 8$

$N_2X_2 \equiv 1(mod9)$

again,$N_3X_3 \equiv 1(mod7)$

$45x_3(mod7) = 1$

$x_3 = 5$

$\therefore x = a_1N_1X_1 + a_2N_2X_2 + a_3N_3X_3$

$X = 1 \cdot 1 \cdot 2 + 4 \cdot 35 \cdot 5 + 6 \cdot 45 \cdot 5$

$x = 126 + 700 + 1350$

$x = 2176(mod315)$

Thus,we have the unique solution $x = 2176 \equiv 286(mod385)$

conclusion

This project discusses about congruence,linear congruence, application of congruence, system of linear congruence,solvability of system of liner congruence and Chinese remainder theorem.Generally,let m be a fixed integer.Then an integer a is congruent to b modulo m if $m \mid a - b$.this is symbolically written as :

$a \equiv b(modm)$.....(1)

Expression (1) is called the congruence, m is called the modulus of the congruence and b is called a residue of a with m.

• **cancellation law:** If a, b and c are integers such that $ac \equiv bc(modm)$, $m > 0$ is a fixed integer and $d = (c, m)$ then $a \equiv b(mod\frac{m}{d})$

• If a, b and c are integers such that

$ac \equiv bc(modm)$, $m > 0$ is a fixed integer and $d = (c, m) = 1$ then $a \equiv b(modm)$ if and only if a and b have the same remainder with respect to m.

• An expression of the form

$ax \equiv b(modm)$,$a \not\equiv 0(modm)$ is called a linear congruence mod m.

• The linear congruence

$ax \equiv b(modm)$ has a solution if and only if $d \mid b$, where $d = (a, m)$

• Let $a \equiv b(modm)$, $(a, m) = d$ and $d \mid b$.then the given linear congruence has exactly d incongruent solutions $(modm)$.

• The linear congruence $ax \equiv b(modm)$ has a unique solution if and only if $(a, m) = 1$

Bibliography

[1] .Yismaw Alemu Introduction to elementry theory of numbers Department of Mathematics,AAU.

[2] Number theory module of 2006 E.C

[3] Kenneth Rosen,Elementary number theory Copy right 1984 by Bell Telephone and Kenneth H,Rosen

[4] Stewart,tall D.Algebraic number theory Copy right 2002 by A K Petters, LTD

[5] Shanks D.Solved and unsolved problems second edition copy right 1962 by Daniel shanks

[6] Adler A;CouryJ.the theory of NumberCopy right 1995 by Jones and Bartlett.