Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

MA8551 ALGEBRA AND NUMBER THEORY

UNIT-IV

LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES

Equation with integer coefficient which are to be solved in integers are called Diophantine equations. This type of equation was first investigated by the Greek algebraist Diophantus of Alexandria in the third century AD.

For example the equations

$2x+3y=4$, $x^2+y^2=4$. $x^2+y^2=z^2$

are called Diophantine equations if we restrict their solution to be integers.

The Diophantine equation $2x+3y=4$ is linear where as the other two Diophantine equations are nonlinear.

The equation $2x+3y=4$ has (-1, 2) as a solution in fact it has infinitely many solution (2+3t, -2t) where t is an arbitrary integer.

Geometrically, such solution are points in the plane with integer coordinates and they are called lattice points.

LINEAR DIOPHANTINE EQUATION (LDE)

The linear Diophantine equations are the simplest class of Diophantine equations.

The general form of a linear Diophantine (LDE) in two variables x and y is

$$ax + by = c,$$

where a,b,c are integers.

Theorem

The linear Diophantine equation $ax + by= c$ is solvable if and only if $d|c$, where $d = (a, b)$. If x_0, y_0 is a particular solution of the linear Diophantine equation, then all its solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad y = y_0 - \left(\frac{a}{d}\right)t,$$

where t is any integer.

Proof

Assume the linear Diophantine equation $ax + by = c$ is a solvable

To prove $d|c$

If $x = \alpha$, $y = \beta$ is a solution, then

$$a\alpha + b\beta = c \qquad (1)$$

Since $d = (a, b)$, $d|a$ and $d|b$

$\Rightarrow$ $d \mid a\alpha + b\beta$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$\Rightarrow$ d|c

Conversely, assume d|c.

To prove the Diophantine equation ax + by = c is solvable

Since d|c, $\Rightarrow$ c = dm for some integer m.

Since d = (a, b) then there exist integers r and s such that

d = ra + sb

Multiplying by m, we get

dm =(ra)m + (sb)m

$\Rightarrow$ c = (ra)m + (sb)m

This shows that x_0 = rm and y_0=sm is a solution of the linear Diophantine equation ax + by = c.

So, it is solvable.

Next we shall prove that if (x_0, y_0) is a solution of ax + by = c, then

$x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$

is a solution for any integer t.

Now $ax + by = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right]$

$= (ax_0 + by_0) + \frac{ab}{d}t - \frac{ab}{d}t$

$= ax_0 + by_0$

$= c$ [$\because (x_0, y_0)$ is a solution of ax+by=c, we have $ax_0+by_0=c$]

$\therefore$ $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$ is a solution for any t.

Finally, we prove that every solution x', y' is of this form.

Since x_0, y_0 and x', y' are solutions of the linear Diophantine equation ax + by = c we have $ax_0 + by_0 = c$ and $ax' + by' = c$

$\therefore$ $ax_0 + by_0 = ax' + by' \Rightarrow a(x'-x_0) = b(y_0 - y')$ (2)

Dividing by d, we get

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y')$$

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

Hence $\frac{b}{d} | (x'-x_0) \Rightarrow x'-x_0 = \frac{b}{d}t$ for some integer t

$\Rightarrow$ $x' = x_0 + \left(\frac{b}{d}\right)t$

substituting in (2) we get

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$$a\left(\frac{b}{d}\right)t = b(y_0 - y')$$

$$\Rightarrow y_0 - y' = \left(\frac{a}{d}\right)t$$

$$\Rightarrow y' = y_0 - \left(\frac{a}{d}\right)t$$

Thus every solution is of the form

$x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$ t is an arbitrary integer.

This solution is called the general solution of $ax + by = c$.

Corollary If (a, b) = 1, then the linear Diophantine equations $ax + by = c$ is solvable and general solution is

$$x = x_0 + bt$$
$$y = y_0 - at$$

where x_0, y_0 is a particular solution and t is an arbitrary integer.

We can extend this result to equation with more than 2 variables.

Theorem

The linear Diophantine equation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ is solvable if and only if $(a_1, a_2, \ldots, a_n) | c$. When it is solvable, it has infinitely many solutions.

Problem

Determine if the linear Diophantine equation 12x + 18y = 30 is solvable. If so, find the solution.

Solution:-

Given LDE is $12x + 18y = 30$ (1)

Here $a = 12, b = 18, c = 30$

$\therefore$ $(a, b) = (12, 18) = 6$

So, $d = (a, b) = 6$

Since $6|30$, we have $d|c$

So, the LDE is solvable

Clearly $x_0 = 1$ and $y_0 = 1$ is a solution of (1)

$\therefore$ the general solution is given by

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, $t \in Z$

$\Rightarrow$ $x = 1 + \left(\frac{18}{6}\right)t$ and $y = 1 - \left(\frac{12}{6}\right)t$

$\Rightarrow$ $x = 1 + 3t$ and $y = 1 - 2t$, $t \in Z$.

Problem

Examine whether the LDE 12x + 16y = 18 is solvable. Write the general solution if solvable.

Solution:-

Given LDE is $12x + 16y = 18$ (1)

Here $a = 12$, $b = 16$, $c = 18$

$\therefore$ $(a, b) = (12, 16) = 4$

So, $d = (a, b) = 4$

Since $4 \nmid 18$, we have $d \nmid c$

So, the LDE is not solvable.

Problem

Obtain the general solution of 15x + 21y = 39.

Solution:-

Given LDE is $15x + 21y = 39$ (1)

Here $a = 15$, $b = 21$, $c = 39$

$\therefore$ $(a, b) = (15, 21) = 3$

So, $d = (a, b) = 3$

Since $3|39$, we have $d|c$

So, the LDE is solvable.

By inspection (or trial and error), we find one solution of (1) is

$x_0 = -3$ and $y_0 = 4$

$\therefore$ the general solution is given by

$x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, $t \in Z$

$\Rightarrow$ $x = -3 + \left(\frac{21}{3}\right)t$ and $y = 4 - \left(\frac{15}{3}\right)t$

$\Rightarrow$ $x = -3 + 7t$ and $y = 4 - 5t$, $t \in Z$.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Remark The solution (x_0, y_0) can be also found by using division algorithm systematically by first expressing gcd (a, b) as a linear combination of a and b

In the above problem $21 = 1(15) + 6$

$15 = 2(6) + 3$

$6 = 2(3) + 0$

$\therefore \quad (15, 21) = 3$

$= 15 - 2(6)$

$= 15 - 2(21-15) = 15 - 2(21) + 2(15)$

$= 3(15) - 2(21)$

$3(15) - 2(21) = 3$

Multiplying by 13, we get $39(15) - 26(21) = 39$

So, $x_0 = 39$ and $y_0 = -26$

So, the general solution is given by

$$x = x_0 + \left(\frac{b}{d}\right)s \quad \text{and} \quad y = y_0 - \left(\frac{a}{d}\right)s,\ s \in Z$$

$$\Rightarrow \quad x = 39 + \left(\frac{21}{3}\right)s \text{ and } \quad y = -26 - \left(\frac{15}{3}\right)s$$

$\Rightarrow \quad x = 39 + 7s \quad$ and $\quad y = -26 - 5s,\ s \in Z.$

We have found two sets of (apparently different) solution

$x = -3 + 7t \quad$ and $\quad y = 4 - 5t,\ t \in Z.$

and $\quad x = 39 + 7s \quad$ and $\quad y = -26 - 5s,\ s \in Z.$

For some t and s if $39 + 7s = -3 + 7t \Rightarrow 7t - 7s = 39 + 3$

$\Rightarrow 7(t - s) = 42 \Rightarrow t - s = 6 \Rightarrow s = t - 6$

$\therefore \quad x = 39 + 7(t-6) \quad$ and $\quad y = -26 - 5(t-6)$

$x = 39 + 7t - 42 \quad$ and $\quad y = -26 - 5t + 30$

$x = -3 + 7t \quad$ and $\quad y = 4 - 5t$

So, we find the two sets of solution are same through they appear to be different as t, s are arbitrary in Z

Problem

Find the general solution of the LDE 6x + 8y + 12z = 10.

Solution:-

Given the LDE is $6x + 8y + 12z = 10 \qquad (1)$

Here $a_1 = 6$, $a_2 = 8$, $a_3 = 12$ $c = 10$

$\therefore \quad (a_1, a_2, a_3) = (6, 8, 12) = 2$ and $c = 10$

$\therefore \quad d = (a_1, a_2, a_3) = (6, 8, 12) = 2$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Since 2|10, d|c

So, the given LDE is solvable.

Since 8y + 12z is linear combination of 8 and 12, it must be a multiple of (8, 12) = 4

$\therefore$ 8y + 12z = 4u (2)

$\therefore$ (1) $\Rightarrow$ 6x + 4u = 10 (3)

First we solve the LDE (3) in two variable x and u.

Here a = 6, b = 4, c = 10

$\therefore$ (a, b) = (6, 4) = 2

So, d = (a, b) = 2

Since 2|10, we have d|c

So, the LDE is solvable.

By inspection (or trial and error), we find one solution of (3) is

$x_0 = 1$ and $u_0 = 1$

$\therefore$ the general solution is given by

$x = x_0 + \left(\frac{b}{d}\right)t$ and $u = u_0 - \left(\frac{a}{d}\right)t, t \in Z$

$\Rightarrow$ $x = 1 + \left(\frac{4}{2}\right)t$ and $u = 1 - \left(\frac{6}{2}\right)t, t \in Z$

$\Rightarrow$ $x = 1 + 2t$ and $u = 1 - 3t, t \in Z$

Substituting for u in (2), we get

$8y + 12z = 4(1-3t)$

Since d = (8, 12) =4 and 4 = 2.8 + (-1)12 is a linear combination of 8 and 12

Multiplying by (1-3t), we get

$4(1-3t) = 2(1-3t).8 + (-1)(1-3t).12$

$= (2-6t).8 + (-1+3t).12$

$\therefore$ a solution of (2) is

$y_0 = 2-6t$ and $z_0 = -1+3t$

So, the general solution of (2) is

$y = y_0 + \left(\frac{b}{d}\right)t'$ and $z = z_0 - \left(\frac{a}{d}\right)t', t' \in Z$

$y = 2-6t + \left(\frac{12}{4}\right)t'$ and $z = -1+3t - \left(\frac{8}{4}\right)t', t' \in Z$

$y = 2 - 6t + 3t'$ and $z = -1 + 3t - 2t'$

Thus the general solution of (1) is

$X = 1 + 2t$ $y = 2 - 6t + 3t'$ and $z = -1 + 3t - 2t'$ for any integer t and t'.

Note that we reduced the 3 variable equation to a two variable equation and solved.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

This method can be extended to linear Diophantine equation with finite number of unknowns.

Problem

Determine if the LDE 2x + 2y + 3z = 6 is solvable? If so find the general solution.

Solution:-

Given LDE is $2x + 2y + 3z = 6$. (1)

Here $a_1 = 2, a_2 = 2, a_3 = 3$ $c = 6$

$\therefore$ $(a_1, a_2, a_3) = (2, 2, 3 = 1$and $c = 6$

$\therefore$ $d = (a_1, a_2, a_3) = (2, 2, 3) = 1$

Since $1|6$, $d|c$

So, the given LDE is solvable.

Since $2y + 3z$ is linear combination of 2 and 3, it must be a multiple of $(2, 3) = 1$

$\therefore$ $2y + 3z = u$ (2)

$\therefore$ (1) $\Rightarrow$ $2x + u = 6$ (3)

First we solve the LDE (3) in two variable x and u.

Here $a = 2, b = 1, c = 6$

$\therefore$ $(a, b) = (2, 1) = 1$

So, $d = (a, b) = = (2, 1) = 1$

Since $1|6$, we have $d|c$

So, the LDE is solvable.

By inspection (or trial and error), we find one solution of (3) is

$x_0 = 1$ and $u_0 = 4$

$\therefore$ the general solution is given by

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad u = u_0 - \left(\frac{a}{d}\right)t,\ t \in Z$$

$$\Rightarrow \quad x = 1 + \left(\frac{1}{1}\right)t \text{ and } \quad u = 4 - \left(\frac{2}{1}\right)t,\ t \in Z$$

$$\Rightarrow \quad x = 1 + t \text{ and } \quad u = 4 - 2t,\ t \in Z$$

Substituting for u in (2), we get

$2y + 3z = 4 - 2t$

Since $d = (2, 3) = 1$ and $1 = 2.2 + (-1)3$ is a linear combination of 2 and 3

Multiplying by (4-2t), we get

$4 - 2t = 2(4 - 2t).2 + (-1)(4 - 2t).3$

$= (8-4t).2 + (-4 + 2t).3$

$\therefore$ a solution of (2) is

$Y_0 = 8-4t$ and $z_0 = -4+2t$

So, the general solution of (2) is

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$y = y_0 + \left(\frac{b}{d}\right)t'$ and $z = z_0 - \left(\frac{a}{d}\right)t'$, $t' \in Z$

$y = 8 - 4t + \left(\frac{3}{1}\right)t'$ and $z = -4 + 2t - \left(\frac{2}{1}\right)t'$, $t' \in Z$

$y = 8 - 4t + 3t'$ and $z = -4 + 2t - 2t'$

Thus the general solution of (1) is

$x = 1 + t$ $y = 8 - 4t + 3t'$ and $z = -4 + 2t - 2t'$ for any integer t and t'.

Problem

Determine if the LDE 2x + 4y -5z = 11 is solvable. If solvable, find the general solution.

Solution:-

Given LDE is $2x + 4y - 5z = 11$. (1)

Here $a_1 = 2$, $a_2 = 4$, $a_3 = -5$, $c = 11$

$\therefore$ $(a_1, a_2, a_3) = (2, 4, -5 = 1$ and $c = 11$

$\therefore$ $d = (a_1, a_2, a_3) = (2, 4, -5) = 1$

Since $1|11$, $d|c$

So, the given LDE is solvable.

Since $4y - 5z$ is linear combination of 4 and -5, it must be a multiple of $(4, -5) = 1$

$\therefore$ $4y - 5z = u$ (2)

$\therefore$ (1) $\Rightarrow$ $2x + u = 11$ (3)

First we solve the LDE (3) in two variable x and u.

Here $a = 2$, $b = 1$, $c = 11$

$\therefore$ $(a, b) = (2, 1) = 1$

So, $d = (a, b) = = (2, 1) = 1$

Since $1|6$, we have $d|c$

So, the LDE is solvable.

By inspection (or trial and error), we find one solution of (3) is

$x_0 = 5$ and $u_0 = 1$

$\therefore$ the general solution is given by

$x = x_0 + \left(\frac{b}{d}\right)t$ and $u = u_0 - \left(\frac{a}{d}\right)t$, $t \in Z$

$\Rightarrow$ $x = 5 + \left(\frac{1}{1}\right)t$ and $u = 1 - \left(\frac{2}{1}\right)t$, $t \in Z$

$\Rightarrow$ $x = 5 + t$ and $u = 1 - 2t$, $t \in Z$

Substituting for u in (2), we get

$4y - 5z = 1 - 2t$

Since $d = (4, -5) = 1$ and $1 = (-1).4 + (-1)(-5)$is a linear combination of 4 and -5

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Multiplying by (1-2t), we get

$1 - 2t = (-1)(1 - 2t).4 + (-1)(1 - 2t).(-5)$

$= (-1 + 2t).4 + (-1 + 2t).(-5)$

$\therefore$ a solution of (2) is

$Y_0 = -1+2t$ and $z_0 = -1+2t$

So, the general solution of (2) is

$y = y_0 + \left(\frac{b}{d}\right)t'$ and $z = z_0 - \left(\frac{a}{d}\right)t'$, $t' \in Z$

$y = -1 + 2t + \left(\frac{-5}{1}\right)t'$ and $z = -1 + 2t - \left(\frac{4}{1}\right)t'$, $t' \in Z$

$y = -1 + 2t - 5t'$ and $z = -1 + 2t - 4t'$

Thus the general solution of (1) is

$x = 5 + t$ $y = -1 + 2t - 5t'$ and $z = -1 + 2t - 4t'$ for any integer t and t'.

CONGRUENCES

Congruence relation was introduced and developed by the German mathematician Karl Friedrich Gauss (1777-1855). Gauss is considered as one of the greatest mathematician of all time, known as the prince of mathematics.

When Gauss was in elementary school his teacher gave the class the problem of finding the sum of the first 100 natural numbers. In no time Gauss, at the age 7, had the answer. The teacher was surprised to see his answer.

He has considered the number in increasing order as

1, 2, 3, . . . 99, 100

and in the decreasing order 100, 99. 98, . . . 2, 1

and added them. Each sum as 101.

There are 100 terms and so the total sum is 100.101

Since each number is used twice, he divided it by 2.

So, the answer is $\frac{100.101}{2}$=5050.

This type of addition is now known as Gaussian addition.

It is used to find the sum of n terms of an A.P. a, a + d, a + 2d, . . .

Definition

Let m be a positive integer. An integer a is congruent to an integer b modulo m if m|a-b. Symbolically, we write $a \equiv b \pmod m$. m is the modulus of the congruence relation.

If a is not congruent to b modulo m, then we write $a \not\equiv b \pmod m$.

If a is not congruent to b mod m, we sat a is in congruent to b mod m.

We use the congruence in everyday life.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

For example we use:

(i) Congruence mod 12 to tell the time of the day (clock is numbered in this way)

(ii) Congruence mod 7 to tell day of the week.

(iii) Congruence mod 100,000 is used in odometers of automobiles.

Theorem

$a \equiv b \pmod m$ if and only if $a = b + km$ for some integer k.

Proof

Let $a \equiv b \pmod m$

Then $m|a-b \Rightarrow a - b = mk$, for some integer.

$\Rightarrow \quad a = b + mk$

Conversely, let $a = b + mk$

Then $a - b = km \Rightarrow m|a - b$

$\Rightarrow \quad a \equiv b \pmod m$.

Note

1. Through the result is very simple, the significant aspect about it is that it gives the relation between congruence and equality.
2. It follows that $a \equiv 0 \pmod m$ if and only if $m|a$. Thus $a \equiv b \pmod m$ and $m|a$ mean exactly the same thing.

Theorem Properties of congruence relations

1. Reflexive property: ie., $a \equiv a \pmod m \quad \forall a \in Z$
2. Symmetric property: If $a \equiv b \pmod m$, the $b \equiv a \pmod m$
3. Transitive property: If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$

Proof

1. Since $m|a-a = 0 \quad \forall a \in Z$
   $a \equiv a \pmod m \quad \forall a \in Z$
2. If $a \equiv b \pmod m$, then $m|a-b$
   $\Rightarrow \quad m| - (b - a)$
   $\Rightarrow \quad m| (b - a) \Rightarrow b \equiv a \pmod m$
3. If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $m| a - b$ and $m| b - c$
   $\therefore \quad m| (a-b) + (b-c) \Rightarrow m| a-c \Rightarrow a \equiv c \pmod m$

Theorem

$a \equiv b \pmod m$ if and only if a and b have the same remainder when divided my m.

Proof

Let $a \equiv b \pmod m$

Then $m \mid a - b$

$\Rightarrow$ $a - b = mk$ for some integer k.

$\Rightarrow$ $a = b + mk$

Now consider b and m. By division algorithm

$b = qm + r,\ 0 \le r < m$

Then $a = qm + r + mk$

$= (q+k)m + r,\ 0 \le r < m$

$\therefore$ a leaves remainder r on division by m.

Then a and b have the same remainder r when divided my m.

Conversely, Let a and b have the same remainder r, when divided by m.

$\therefore$ $a = qm + r$

and $b = q'm + r,\ 0 \le r < m$

$\therefore$ $a - b = (q-q')m \Rightarrow m \mid a - b$

$\Rightarrow$ $a \equiv b \pmod m$

Corollary

If $a \equiv r \pmod m$, where $0 \le r < m$, then r is the remainder when a is divided by m.

Theorem

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

(i) $a+c \equiv b+d \pmod m$

(ii) $a.c \equiv b.d \pmod m$

Proof

Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$\therefore$ $a = b + km$

and $c = d + k'm$

$\therefore$ $a+c = b+d + (k+k')m$

$\Rightarrow$ $a+c \equiv b+d \pmod m$

Hence (i) is proved

Now $ac = (b+km)(d+k'm)$

$= bd + (bk'+kd)m + kk'm^2$

$\Rightarrow$ $ac - bd = m(bk'+kd+kk'm)$

$\Rightarrow$ $m \mid ac - bd$

$\Rightarrow$ $a.c \equiv b.d \pmod m$

Hence (ii) is proved.

Corollary If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

(i) $a-c \equiv b-d \pmod m$

(ii) $a.c \equiv b.c \pmod m$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

(iii) $a^2 \equiv b^2 \pmod m$

More generally $a^r \equiv b^r \pmod m$ for any positive integer r.

Problem

Find the remainder when 1! + 2! + 3! + . . . + 100! is divided by 15

Solution

We have n! = 1.2.3.4. . . . (n-1) . n

5! = 1.2.3.4.5 is divided by 15 (but 4!= 1.2.3.4 is not divided by 15)

$\therefore$ 5! $\equiv$0(mod15)

All higher factorials are divided by 15

So, for r$\geq$5, r! $\equiv$0(mod15)

$\therefore$ 1! + 2! + 3! + . . . (n-1)! + n! $\equiv$ 1! + 2! + 3! + 4! + 0 + . . . + 0 + 0 (mod 15)

$\equiv$ 1+2+6+24(mod15)

$\equiv$ 1+2+30(mod15)

$\equiv$ 3 + 0(mod15)

$\equiv$ 3(mod15)

$\therefore$ when 1!+2!+3!+. . . +100! is divided by 15, the remainder is 3.

Problem

Find the remainder when 1!+2!+3!+ . . . +300! is divided by 13

Solution

For divisibility by 13, we consider mod13

For r$\geq$13, r! will contain 13 as a factor

$\therefore$ r! $\equiv$0(mod13)

$\therefore$ 1!+2!+3!+4!+5! . . . +12!+ . . +300! $\equiv$1!+2!+3!+ . . . +12!+ 0+0+. . +0(mod13)

$\equiv$1!+2!+3!+ . . . +12!(mod15)

$\equiv$1+2+6+24+120+. . . +12!(mod13)

But 2+24 =26 $\equiv$0(mod13)

5! = 120 $\equiv$3(mod13)

6!=5!.6=3.6=18(=1.13+5) $\equiv$5(mod13)

7!=6!.7=5.7=35(=2.13+9) $\equiv$9(mod13)

8!=7!.8=9.8=72(=5.13+7) $\equiv$7(mod13)

9!=8!.9=7.9=63(=4.13+11) $\equiv$11(mod13)

10!=9!.10=11.10=110(=8.13+6) $\equiv$6(mod13)

11!=10!.11=6.11=66(=5.13+1) $\equiv$1(mod13)

12!=11!.12=1.12=12(=0.13+12) $\equiv$12(mod13)

$\therefore$ 1!+2!+3!+4!+5! . . . +12!+ . . +300! $\equiv$1+6+0+3+5+9+7+11+6+1+12(mod13)

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$\equiv 61 \pmod{13}$ $(\because 61=4.13+9)$

$\equiv 9 \pmod{13}$

$\therefore$ the remainder is 9 when 1!+2!+3!+ . . . +300! is divided by 13.

Problem

Find the ones digit in the sum 1!+2!+3!+ . . . +100!, when expressed in decimal notation.

Solution

Required the digit in the unit's place of the number 1!+2!+3!+ . . . +100!

So, we find the remainder when it is divided by 10.

If $r \geq 5$, the r! has 10 as a factor

$\therefore$ $r! \equiv 0 \pmod{10}$

$\therefore$ $1! + 2! + 3! + \ldots + 100! \equiv 1! + 2! + 3! + 4! + 0 + \ldots + 0 \pmod{10}$

$\equiv 1 + 2 + 6 + 24 \pmod{10}$

$\equiv 1 + 2 + 30 \pmod{10}$

$\equiv 3 \pmod{10}$

$\therefore$ the digit in the unit place of 1!+2!+3!+ . . . +100! is 3.

Problem

Compute the remainder 3^{181} is divided by 17.

Solution

We have to find the remainder when 3^{181} is divided by 17.

We have $3^2 \equiv 9 \pmod{17}$

$3^4=81 \equiv 13 \pmod{17}$ $(81=4.17+13)$

$\equiv -4 \pmod{17}$ $(-4=13-17)$

$3^8 \equiv (-4)^2 \pmod{17}$

$\equiv 16 \pmod{17}$

$\equiv -1 \pmod{17}$ $(-1=16-17)$

$\therefore$ $3^{16} \equiv (-1)^2 \pmod{17} \equiv 1 \pmod{17}$

$\therefore$ $(3^{16})^9 \equiv 1^2 \pmod{17}$

$\Rightarrow$ $3^{144} \equiv 1^2 \pmod{17}$

$3^{181}=3^{144+32+4+1}=3^{144}.3^{32}.3^4.3$

But $(3^{16})^2 \equiv 1^2 \pmod{17}$

$3^{32} \equiv 1 \pmod{17}$

$\therefore$ $3^{181} \equiv 1.1.13.3 \pmod{17}$

$\equiv 39 \pmod{17}$

$3^{181} \equiv 5 \pmod{17}$ $(39=2.17+5)$

$\therefore$ the remainder when 3^{181} is divided by 17 is 3.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Problem

Compute the remainder when 3^{247} is divided by 25.

Solution

We have to find the remainder when 3^{247} is divided by 25.

We have $3^2 \equiv 9 \pmod{25}$

$3^4=81 \equiv 6 \pmod{25}$ $(81=3.25+6)$

$3^8 \equiv (6)^2 \pmod{25}$

$\equiv 36 \pmod{25}$

$\equiv 11 \pmod{25}$ $(36=1.25+11)$

$\therefore$ $3^{16} \equiv (11)^2 \pmod{25}$

$\equiv 121 \pmod{25}$

$\equiv 21 \pmod{25}$

$\therefore$ $(3^{16})^2 \equiv 21^2 \pmod{25}$

$\Rightarrow$ $3^{32} \equiv 441 \pmod{25}$

$\equiv 16 \pmod{25}$ $(441=17.25+16)$

$(3^{32})^2 \equiv 16^2 \pmod{25}$

$\Rightarrow$ $3^{64} \equiv 256 \pmod{25}$

$\equiv 6 \pmod{25}$ $(256=10.25+6)$

$(3^{64})^2 \equiv 6^2 \pmod{25}$

$\Rightarrow$ $3^{128} \equiv 11 \pmod{25}$

$3^{247}=3^{128+64+32+16+4+2+1}=3^{128}.3^{64}\ 3^{32}.3^{16}.3^{4}.3^{2}.3$

$\therefore$ $3^{247} \equiv 11.6.16.21.6.9.3 \pmod{25}$

$\Rightarrow$ $3^{247} \equiv 11.96.21.54.3 \pmod{25}$

$\equiv 11.(-4).(-4).4.3 \pmod{25}$

$\equiv 44.48 \pmod{25}$

$\equiv (-6).(-2) \pmod{25}$

$\equiv 12 \pmod{25}$

$\therefore$ the remainder is 12 when 3^{247} is divided by 25.

Home work

Find the remainder when 3^{247} is divided by 17 [Ans. 11]

[Hint $3^{247}=3^{240+6+1}$]

Problem

Find the remainder when 13^{218} is divided by 17.

Solution

We have to find the remainder when 13^{218} is divided by 17.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$13^2=169 \equiv -1(\text{mod}17)$

$\Rightarrow (13^2)^{109} \equiv (-1)^{109}(\text{mod}17)$

$13^{218} \equiv -1(\text{mod}17)$

$\equiv 16(\text{mod}17)$

$\therefore$ the remainder is 16 when 13^{218} is divided by 17.

Problem

Find the remainder when 193^{183} is divided by 19.

Solution

We have to find the remainder when 193^{183} is divided by 19.

We have $193 \equiv 3(\text{mod}19)$

$193^2 \equiv 9(\text{mod}19)$

$193^4 \equiv 81(\text{mod}19)=5(\text{mod}19)$ [81=4.19+5]

$\Rightarrow (193^4)^2 \equiv 5^2(\text{mod}19)$

$(193)^8 \equiv 25(\text{mod}19)$ [25=1.19+6]

$\equiv 6(\text{mod}19)$

$(193^8)^2 \equiv 6^2(\text{mod}19)$

$\Rightarrow 193^{16} \equiv 36(\text{mod}19)$ [36=1.19+17]

$\equiv 17(\text{mod}19)$

$\equiv -2(\text{mod}19)$

$(193^{16})^4 \equiv (-2)^4(\text{mod}19)$

$\Rightarrow 193^{64} \equiv 16(\text{mod}19)$

$\equiv -3(\text{mod}19)$

$(193^{64})^2 \equiv (-3)^2(\text{mod}19)$

$\Rightarrow 193^{128} \equiv 9(\text{mod}19)$

$193^{128}.193^{16} \equiv 9.(-2)(\text{mod}19)$

$\Rightarrow 193^{144} \equiv -18(\text{mod}19)$

$\equiv 1(\text{mod}19)$

$193^{144}.193^{16} \equiv 1.(-2)(\text{mod}19)$

$\Rightarrow 193^{160} \equiv -2(\text{mod}19)$

$193^{183} = 193^{160+16+4+2+1}$

$\Rightarrow =193^{160}.193^{16}.193^4.193^2.193^1$

$\Rightarrow 193^{183} \equiv (-2).(-2).5.9.3(\text{mod}19)$

$\equiv (4.5).(9.3)(\text{mod}19)$

$\equiv 20.27(\text{mod}19)$

$\equiv 1.8(\text{mod}19)$

$\therefore$ the remainder is 8 when 193^{183} is divided by 19.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Problem

Find the last two digits in the decimal value of 1776^{1776}.

Solution

The last two digits is the remainder when a number is divided by 100

$$1776 \equiv 76 \pmod{100}$$

We shall study the power of 76

$$76^2 = 5776 \equiv 76 \pmod{100}$$

$$76^3 = 76.76 \equiv 76 \pmod{100}$$

and so on. We find $76^n \equiv 76 \pmod{100} \ \forall n \geq 1$

$\therefore$ $1776^n \equiv 76 \pmod{100} \ \forall n \geq 1$

$\Rightarrow$ $1776^{1776} \equiv 76 \pmod{100}$

Hence last two digits in the decimal value of 1776^{1776} is 76.

Problem

Prove that $2^{2^5}+1$ is divisible by 641.

Solution

We observe that $640 \equiv -1 \pmod{641}$ $[640 = 64.10 = 2^6.2.5 = 2^7.5]$

$\Rightarrow$ $2^7.5 \equiv -1 \pmod{641}$

$\therefore$ $(2^7)^4.5^4 \equiv (-1)^4 \pmod{641}$

$2^{28}.5^4 \equiv 1 \pmod{641}$ (1)

But $5^4 = 625 \equiv -16 \pmod{641} \equiv -2^4 \pmod{641}$

(1) $\Rightarrow$ $2^{28}.(-2^4) \equiv 1 \pmod{641}$

$-2^{32} \equiv 1 \pmod{641}$

$\Rightarrow$ $2^{32} \equiv -1 \pmod{641}$

$\Rightarrow$ $2^{2^5} \equiv -1 \pmod{641}$

$\Rightarrow$ $2^{2^5}+1 \equiv 0 \pmod{641}$

Hence $2^{2^5}+1$ is divided by 641

Theorem

If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $a \equiv b \pmod{m_3}$, . . . , $a \equiv b \pmod{m_r}$.

Then $a \equiv b \pmod{[m_1, m_2, m_3, \ldots, m_r]}$

Proof

Given $a \equiv b \pmod{m_i}$, $i=1,2,3,\ldots,r$

Then $m_i | a-b$, $i=1,2,3,\ldots,r$

Since $m_1 | a-b$, $m_2 | a-b$, $m_3 | a-b$, … , $m_r | a-b$, then their lcm$[m_1,m_2,m_3,\ldots,m_r] | a-b$

$\Rightarrow$ $a \equiv b \pmod{[m_1,m_2,m_3,\ldots,m_r]}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Corollary

If $a \equiv b \pmod{m_i}$, $i=1,2,3,\ldots,r$ and $m_1, m_2, m_3, \ldots, m_r$ are pair wise relatively prime then $a \equiv b \pmod{m_1, m_2, m_3, \ldots, m_r}$

Note

The above result says that congruence's of two numbers with different moduli can be combined into single congruence.

Theorem

If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \left(\mod \frac{m}{d}\right)$.

Proof

Given $ac \equiv bc \pmod{m}$ and $(c, m) = d$.

$\Rightarrow$ $m \mid ac-bc$ $\Rightarrow$ $m \mid c(a-b)$ and $\left(\frac{c}{d}, \frac{m}{d}\right) = 1$

$\Rightarrow$ $c(a-b) = mk$ (1)

Dividing (1) by d, we get

$$\frac{c}{d}(a-b) = k\frac{m}{d}$$

Since $\frac{c}{d}$ and $\frac{m}{d}$ are relatively prime, we get $\frac{m}{d}$ divides (a-b)

$\Rightarrow$ $a \equiv b \left(\mod \frac{m}{d}\right)$.

Corollary

If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.

For example,

$14 \equiv 8 \pmod{6} \Rightarrow 7.2 \equiv 4.2 \pmod{6}$ and $(2, 6) = 2$

$\therefore$ $7 \equiv 4 \left(\mod \frac{6}{2} = 3\right)$.

INVERSE OF A MODULO M

Definition

When (a, m) = 1, there is unique least residue x such that $ax \equiv 1 \pmod{m}$. Then a is said to be invertible and x is called an inverse of a modulo m, denoted by a^{-1}.

$\therefore$ $a.a^{-1} \equiv 1 \pmod{m}$.

If $a = a^{-1}$, then a is said to be self-invertible.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Theorem

The unique solution of the linear congruence $ax \equiv b \pmod m$, where $(a, m) = 1$, is the least residue of $a^{-1}b \pmod m$

Proof

Given the linear congruence $ax \equiv b \pmod m$, where $(a, m) = 1$.

Since $(a, m) = 1$, then a has an inverse a^{-1} modulo m.

Multiplying by a^{-1} we get

$a^{-1}(ax) \equiv a^{-1} b \pmod m$

$\Rightarrow (a^{-1}a)x \equiv a^{-1} b \pmod m$

$\Rightarrow 1.x \equiv a^{-1} b \pmod m$

$\Rightarrow x \equiv a^{-1} b \pmod m$

$\therefore$ the solution is the least residue of $a^{-1}b \pmod m$

For example,

Since $2.3 \equiv 1 \pmod 5$

$\therefore$ 2 is invertible and 3 is inverse of 2 (mod 5)

i.e., $2^{-1} \equiv 3 \pmod 5$

Since $4.4 \equiv 1 \pmod 5$, the inverse of 4 is 4 (mod 5) and so 4 is self reciprocal.

LINEAR CONGRUENCE

Linear congruence is the simplest of congruence with variable. We will see that linear congruence and linear Diophantine equation are related.

Definition

A congruence of the form $ax \equiv b \pmod m$, where m is a positive integer and a,b are integers and x is variable, is called a linear congruence.

Theorem

The linear congruence $ax \equiv b \pmod m$ is solvable if and only if $d|b$, where $d = (a, m)$. If $d|b$, then it has d incongruent solutions.

Proof

Given the linear congruence

$ax \equiv b \pmod m$, where $m \in Z^+$ and $a,b \in Z$ (1)

$ax \equiv b \pmod m$ if and only if $m|ax-b$ (2)

i.e., if and only if $ax - b = my \Leftrightarrow ax - my = b$

which is a linear Diophantine equation.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Thus, the linear congruence $ax \equiv b \pmod m$ is solvable if and only if the linear congruence equation

$ax - my = b$ is solvable.

Then the linear Diophantine equation is solvable if $d|b$

When $d|b$, there are infinitely many solutions, which are given by

$x = x_0 + \left(\frac{-m}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, $t \in Z$

$x = x_0 + \left(\frac{m}{d}\right)(-t)$ and $y = y_0 + \left(\frac{a}{d}\right)(-t)$

$x = x_0 + \left(\frac{m}{d}\right)t'$ and $y = y_0 + \left(\frac{a}{d}\right)t'$, where $t' = -t \in Z$

When (x_0, y_0) is a particular solution of (2)

Hence the congruence $ax \equiv b \pmod m$ has infinitely many solution given by $x = x_0 + \left(\frac{m}{d}\right)t$, where x_0 is a particular solution if the congruence and t is an arbitrary integer.

When $d|b$, we shall now prove that there are only d incongruent solution.

Suppose $x_1 = x_0 + \left(\frac{m}{d}\right)t_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right)t_2$ are two solution of congruence.

Suppose $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \pmod m$, then $\left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \pmod m$.

Since $\left(\frac{m}{d}\right)|m$, we get $t_1 \equiv t_2 \pmod d$

Thus x_1 and x_2 are congruent iff $t_1 \equiv t_2 \pmod d$

$\therefore$ x_1 and x_2 are incongruent solution iff t_1, t_2 belong in different congruence classes mod d.

But we know that there are only d congruence classes modulo d.

So, the number of incongruent solution is d and they are given by

$$x = x_0 + \left(\frac{m}{d}\right)t, \ 0 \le t < d$$

This is the general solution of the congruence.

Problem

Determine whether the congruence $12x \equiv 48 \pmod{18}$ is solvable and also the solution if solvable.

Solution

Given the linear congruence equation is

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$12x \equiv 48 \pmod{18}$

$2 \mid 12, 18$
$3 \mid 6, 9$
$2, 3$

Here $a = 12,\ b = 48,\ m = 18$

$\therefore\ (a, m) = (12, 18) = 6$

$\Rightarrow\ d = (a, m) = 6$

Since $6 \mid 48$, we have $d \mid b$

$\therefore$ the equation is solvable.

Hence the general solution is

$$x = x_0 + \left(\frac{m}{d}\right)t,\ t \in Z$$

We find, when x=1

$12 \equiv 48 \pmod{18}$ $[\because 12 - 48 = -36]$

$\therefore\ x_0 = 1$ is particular solution

$$\therefore\quad x = 1 + \left(\frac{18}{6}\right)t,\ t \in Z$$

$$= 1 + 3t,\ t \in Z$$

The incongruence solution are $x = 1 + 3t$, where $0 \le t < 6$

Since (12, 18) = 6 and $6 \mid 48$, the congruence has six incongruent solution modulo 6

When t = 0,1,2,3,4,5 we get the incongruent solution 1,4,7,10,13,and 16.

Problem

Determine the number of incongruent solution of $48x \equiv 144 \pmod{84}$.

Solution

Given the congruence $48x \equiv 144 \pmod{84}$.

Here $a = 48\ \ b = 144\ \ m = 84$

Now $(a, m) = (48, 84) = 12$

$\Rightarrow\ d = (a, m) = 12$

$2 \mid 48, 84$
$2 \mid 24, 42$
$3 \mid 12, 21$
$4, 7$

Since $12 \mid 144 \Rightarrow d \mid b$ and so the congruence is solvable. It has 12 incongruence solutions.

Problem

Find the incongruent solutions of the linear congruence $28x \equiv 119 \pmod{91}$.

Proof

Given the linear congruence equation is

$28x \equiv 119 \pmod{91}$

$7 \mid 28, 91$
$4, 23$

Here $a = 28,\ b = 119,\ m = 91$

$\therefore\ (a, m) = (28, 91) = 7$

$\Rightarrow\ d = (a, m) = 7$

Since $7 \mid 119$, we have $d \mid b$

$\therefore$ the equation is solvable.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Hence the general solution is

$$x = x_0 + \left(\frac{m}{d}\right)t,\ t \in Z$$

We find, when x=1

$28 \equiv 119 \pmod{91}$ [$\because 28 - 119 = -91$]

$\therefore$ $x_0 = 1$ is particular solution

$$\therefore \quad x = 1 + \left(\frac{91}{7}\right)t,\ t \in Z$$

$$= 1 + 13t,\ t \in Z$$

The incongruence solution are $x = 1 + 23t$, where $0 \le t < 67$

Since (28, 91) = 7 and 7|91, the congruence has 7 incongruent solution modulo 7

When t = 0,1,2,3,4,5,6 we get the incongruent solution 1,14,27,40,53,66and 79 (mod 91).

Problem

Solve the linear Diophantine equation 63x – 23y =-7 using congruence.

Solution

Given LDE is 63x – 23y =-7. (1)

From this we get the congruence

$63x \equiv -7 \pmod{23}$ and $-23y \equiv -7 \pmod{63}$

We solve

$63x \equiv -7 \pmod{23}$

Since $63 \equiv -6 \pmod{23}$

We get $-6x \equiv -7 \pmod{23} \Rightarrow 6x \equiv 7 \pmod{23}$

Here $a = 6,\ b = 7,\ m = 23$

$\therefore$ $(a, m) = (6, 23) = 1$

$\Rightarrow$ $d = (a, m) = 1$

Since 1|7, we have d|b

$\therefore$ the equation is solvable.

Hence the general solution is

$$x = x_0 + \left(\frac{m}{d}\right)t,\ t \in Z$$

We find, when x=5

$30 \equiv 7 \pmod{23}$ [$\because 30 - 7 = 23$]

$\therefore$ $x_0 = 5$ is particular solution

$$\therefore \quad x = 5 + \left(\frac{23}{1}\right)t,\ t \in Z$$

$$= 5 + 23t,\ t \in Z$$

Now substituting for x in (1), we get

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$63(5 + 23t) - 23y = -7 \Rightarrow 23y = 63(5+23t) + 7$

$= 315 + 63.23t + 7$

$= 322 + 63.23t$

$y = 14 + 63t$

$\therefore$ the general solution of LDE is $x = 5 + 23t$, $y = 14 + 63t$, $t \in Z$.

Problem

Twenty three weary travelers entered the outskirts of a lush and beautiful forest. They found 63 equal heaps of plantains and seven single fruits, and divided them equally. Find the number of fruits in each heap.

Solution

Let x be the number of plantains in a heap.

Let y be the number of plantains received by traveler.

Then the total number of plantains is $63x + 7$

Each traveler received y plantains

$\therefore$ the total number of plantains received by the travelers = $23y$

$\therefore \quad 63x + 7 = 23y \Rightarrow 63x - 23y = -7 \quad (1)$

which is a Diophantine equation.

By above problem

General solution is $x = 5 + 23t$, $y = 14 + 63t$, $t \in Z$

When $t = 0 \Rightarrow x=5$ and $y=14$

When $t = 1 \Rightarrow x=28$ and $y=77$

Infinitely many solutions are there.

Note This problem is taken from the Indian mathematician.

Mahavira's book Ganita-Sara-Sangraha (AD 850)

This puzzle of mahavira yields the above Diophantine equation. Mahavira was born in Mysore. He was an astronomer and mathematician in the Court of King Amogavartana.

Problem

Use congruence to solve the LDE 15x + 21y = 39

Solution

Given LDE is $15x + 21y = 39$. (1)

From this we get the congruence

$15x \equiv 39 \pmod{21}$ and $21y \equiv 39 \pmod{15}$

We solve

$15x \equiv 39 \pmod{21}$

Course/Branch: BE/CSE	**Year / Semester** : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	**Subject Name** :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	**Unit Name:** LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Here $a = 15,\ b = 39,\ m = 21$

$\therefore$ $(a, m) = (15, 21) = 3$

$\Rightarrow$ $d = (a, m) = 3$

Since $3|39$, we have $d|b$

$\therefore$ the equation is solvable.

Hence the general solution is

$$x = x_0 + \left(\frac{m}{d}\right)t,\ t \in Z$$

We find, when $x=4$

$60 \equiv 39 \pmod{21}$ $[\because 60 - 39 = 21]$

$\therefore$ $x_0 = 4$ is particular solution

$\therefore$ $$x = 4 + \left(\frac{21}{3}\right)t,\ t \in Z$$

$$= 4 + 7t,\ t \in Z$$

Now substituting for x in (1), we get

$15(4 + 7t) + 21y = 39 \Rightarrow 21y = 39 - 15(4 + 7t)$

$= 39 - 60 - 105t$

$= -21 - 105t$

$y = -1 - 5t$

$\therefore$ the general solution of LDE is $x = 4 + 7t,\quad y = -1 - 5t, t \in Z.$

Problem

Using inverse find the incongruent solution of the linear congruence $5x \equiv 3 \pmod 6$.

Solution

Given linear congruence is

$5x \equiv 3 \pmod 6$ (1)

Here $a = 5,\ b = 3,\ m = 6$

$\therefore$ $(a, m) = (5, 6) = 1$

$\Rightarrow$ $d = (a, m) = 1$

Since $1|3$, we have $d|b$

$\therefore$ the equation is solvable.

We know $5.5 = 25 \equiv 1 \pmod 6$

$\therefore$ the inverse of 5 is 5

$5^{-1} \equiv 5 \pmod 6$

Multiplying (1) by 5^{-1}, then

$(5^{-1}.5)x \equiv 5^{-1}.3 \pmod 6$

$\Rightarrow$ $x \equiv 5.3 \pmod 6$ $[15=2.6 + 3]$

$x \equiv 3 \pmod 6$ is the solution

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Divisibility Test

As an application of theory of congruence we shall now find the criterion for a given integer to be divisible by another integer.

Let n be a positive integer in the decimal ststem.

Let $n = n_k n_{k-1} \ldots n_2 n_1 n_0$

Then $n = n_k 10^k + n_{k-1} 10^{k-1} + \ldots + n_2 10^2 + n_1 10^1 + n_0 10^0$ (1)

Using this expansion we shall now develop criterion for divisibility by

$2, 2^2, 2^3, \ldots$ and 3, 5, 9, 10, 11.

Divisibility Test for 10

We know $10 \equiv 0 \pmod{10}$

$\therefore$ the expression (1) reduces to $n = n_0 \pmod{10}$

so, n is divisible by 10 if the unit place n_0 is divisible by 10.

i.e., iff $n_0 = 0$

Thus an positive integer is divisible by 10 if its unit digit is 0.

Divisibility Test for 5

We know $10 \equiv 0 \pmod 5$, the expression (1) reduces to $n = n_0 \pmod 5$

$\therefore$ n is divisible by 5 iff the unit digit n_0 is divisible by 5.

But the only single digit numbers divisible by 5 are 0 and 5

$\therefore$ ***n is divisible by 5 if its unit digit is 0 or 5.***

Divisibility Test for 2, 2^2, 2^3, . . .

We know $10 \equiv 0 \pmod 2$ and $10^i \equiv 0 \pmod{2^i}$

$\therefore$ $n \equiv n_0 \pmod 2$

$\equiv n_1 n_0 \pmod{2^2}$

$\equiv n_2 n_1 n_0 \pmod{2^3}$

Thus **n is divisible by 2 if n_0 is divisible by 2**

n is divisible by 4 if $n_1 n_0$ is divisible by 4

n is divisible by 8 if $n_2 n_1 n_0$ is divisible by 8

For example,

We know 31432 is divisible by 2, since the last digit is divisible by 2

It is divisible by 4, since the last 2 digits 32 is divisible by 4.

It is divisible by 8, since the last 3 digits 432 is divisible by 8.

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Divisibility test for 3 and 9

We know $10 \equiv 1 \pmod 3$ and $10^i \equiv 0 \pmod 3$

$\therefore$ $n \equiv n_k + n_{k-1} + \ldots + n_2 + n_1 + n_0 \pmod 3$

So, n is divisible by 3, if the ***sum of the digits is divisible by 3***.

$\therefore$ $n \equiv n_k + n_{k-1} + \ldots + n_2 + n_1 + n_0 \pmod 9$

So, n is divisible by 9, if the ***sum of the digits is divisible by 9***.

For example

123456 is divisible by 3.

Since the sum of the digits 1+2+3+4+5+6=21 is divisible by 3

But this is not divisible by 9

Divisibility test for 11

We know $10 \equiv -1 \pmod{11}$ and $10^i \equiv (-1)^i \pmod{11}$

$\therefore$ $n = (-1)^k n_k + (-1)^{k-1} n_{k-1} + \ldots + n_2 - n_1 + n_0 \pmod{11}$

$n = (n_0 + n_2 + n_4 + \ldots) - (n_1 + n_3 + n_5 + \ldots) \pmod{11}$

$\therefore$ n is divisible by 11.

the sum ***of digits in the even places – sum of digits in odd places*** is divisible by 11.

For example

We have 243506076 is divisible by 11.

for, (7+6+5+4) – (6+0+0+3+2) = 22 – 11 = 11 which is divisible by 11.

SYSTEM OF LINEAR CONGRUENCES

When we consider a set of two or more linear congruences in the same number of variables, we call it ***a system of linear congruences***.

First we shall consider a system of linear congruences in one variable x with pair wise relatively prime moduli.

For example,

$$x \equiv 1 \pmod 3 \quad x \equiv 2 \pmod 5 \quad x \equiv 3 \pmod 7$$

is a system of linear congruences.

A solution of a linear system is a number that satisfies every congruence in the system

One method of solving a linear system is ***iteration***.

That is successive substitution for x until the last congruence is used.

Problem

Solve the system of congruences $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

Solution

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Given $x \equiv 1(\text{mod } 3)$ $x \equiv 2(\text{mod } 5)$ $x \equiv 3(\text{mod } 7)$

We solve this system by iteration.

We start with $x \equiv 1(\text{mod } 3)$

Here $a=1, b=1, m=3$

$(a, m) = (1, 3) = 1$

$\therefore$ $d = 1$ and so $d|b$

So, the equation has a solution $x = 1$

$\therefore$ the general solution is $x = x_0 + \left(\frac{m}{d}\right)t_1,\ t_1 \in Z$

$x = 1 + \left(\frac{3}{1}\right)t_1,$

$x = 1 + 3t_1,\ t_1 \in Z$ (1)

Substituting by (1) in $x \equiv 2(\text{mod } 5)$

$\therefore$ $1 + 3t_1 \equiv 2(\text{mod } 5)$

$\Rightarrow$ $3t_1 \equiv 1(\text{mod } 5)$

We find $t_1 = 2$ is clearly a solution, since $6 \equiv 1(\text{mod } 5)$

$\therefore$ $t_1 = 2(\text{mod } 5)$ is a particular solution

Here $a=3, b=1, m=5$

$(a, m) = (1, 5) = 1$

$\therefore$ $d = 1$ and so $d|b$

So, the equation has a solution $t_1 = 2$

$\therefore$ the general solution is $t_1 = x_0 + \left(\frac{m}{d}\right)t_2,\ t_2 \in Z$

$t_1 = 2 + \left(\frac{5}{1}\right)t_2,$

$= 2 + 5t_2,\ t_2 \in Z$

$\therefore$ $x = 1 + 3(2+5t_2) = 7 + 15t_2$ (2)

Substituting by (2) in $x \equiv 3(\text{mod } 7)$

$7 + 15t_2 \equiv 3(\text{mod } 7)$

$\Rightarrow$ $15t_2 \equiv -4(\text{mod } 7)$

$\Rightarrow$ $15t_2 \equiv 3(\text{mod } 7)$ [$\because$ $-4 \equiv 3(\text{mod } 7)$]

We find $t_2 = 3$ is clearly a solution, since $45 \equiv 3(\text{mod } 7)$

$\therefore$ $t_2 = 3(\text{mod } 7)$ is a particular solution

Here $a=15, b=3, m=7$

$(a, m) = (15, 7) = 1$

$\therefore$ $d = 1$ and so $d|b$

So, the equation has a solution $t_2 = 3$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$\therefore$ the general solution is $t_2 = x_0 + \left(\frac{m}{d}\right)t_3,\ t_2 \in Z$

$t_2 = 3 + \left(\frac{7}{1}\right)t_3,$

$= 3 + 7t_3,\ t_3 \in Z$

$\therefore$ $x = 7 + 15(3 + 7t_3) = 52 + 105t_3,\ t_3 \in Z$

$\therefore$ the general solution of the system is

$x = 52 + 105t,\ t \in Z$

The next theorem gives a systematic method of solving system of linear congruences single variable with pair wise relatively prime moduli. It is known as Chines Remainder theorem in handout of early contributions of Chinese mathematicians to the theory of congruences.

In the first centuary AD, the puzzle was posed by the Chinese mathematician Sun-Teu.

There are certain number of things when divided by 3, the remainder is 2.
when divided by 5, the remainder is 3
and when divided by 7, the remainder is 2.
What will be the number of things?
This puzzle is the earliest known example of the Chinese remainder theorem.

Theorem [Chinese Remainder Theorem][CRT]

The system of linear congruences $x \equiv a_1 (\text{mod } m_1)$, $x \equiv a_2 (\text{mod } m_2)$, . . . , $x \equiv a_1 (\text{mod } m_k)$, where $m_1, m_2, \ldots, m_k$ are pair wise relatively prime positive integers and $a_1, a_2, \ldots, a_k$ are given integers, has unique solution modulo $m_1.m_2.m_3.....m_k$.

Proof

First we prove the existences of the solution

Let $n = m_1.m_2.m_3. \ldots .m_k$

Let $n_i = \frac{n}{m_i}$, i = 1, 2, 3, . . .,k

Since $m_1, m_2, \ldots, m_k$, are relatively prime

$(n_i, m_i) = 1$, i = 1, 2, 3, . . .,k

Also $n_i \equiv 0 (\text{mod } m_j)$, $i \neq j$

1. First we construct a solution to the linear system.
   Since $(n_i, m_i) = 1$, we congruence $n_i y_i \equiv 1 (\text{mod } m_i)$ has a unique solution y_i (in fact y_i is the inverse of n_i modulo m_i), i = 1, 2, 3, . . .,k.
   Let $x = a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 + \ldots + a_kn_ky_k$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

Now we will show that x is a solution of he system of congruences.
Since $n_i \equiv 0 \pmod{m_k}$, $i \neq k$, all the terms except the k^{th} term in this sum are congruent to 0 modulo m_k.
Since $n_k y_k \equiv 1 \pmod{m_k}$, we see that $x = a_k n_k y_k \equiv a_k \pmod{m_k}$, for k = 1, 2, 3, . . . ,n.
Thus x satisfies every congruence in the system.
Hence x is a solution of the linear system.

2. Next to show that the solution is unique modulo $n = m_1.m_2.m_3. \ldots .m_k$
Let x_1, x_2 be two solutions of the system
To prove that $x_1 \equiv x_2 \pmod{n}$
Since $x_1 \equiv a_j \pmod{m_j}$ and $x_2 \equiv a_j \pmod{m_j}$, j = 1, 2, 3, . . . ,k
We have $x_1 - x_2 \equiv 0 \pmod{m_j}$
$\Rightarrow$ $m_j \mid x_1 - x_2$ for every j
Since $m_1, m_2, \ldots, m_k$ are pair wise relatively prime.
Lcm $[m_1, m_2, \ldots, m_k] = m_1.m_2.m_3. \ldots .m_k \mid x_1 - x_2$
$\Rightarrow$ $n \mid x_1 - x_2 \Rightarrow x_1 \equiv x_2 \pmod{n}$
Hence the solution is unique modulo $m_1 m_2 \ldots m_k$

Working rule: Let $n = m_1.m_2.m_3. \ldots .m_k$ and $n_i = \frac{n}{m_i}$

Step 1: Find the solution $y_1, y_2, \ldots, y_k$, where $n_i y_i \equiv 1 \pmod{m_i}$, i = 1, 2, 3, . . . ,k.
Step 2: $x = a_1 n_1 y_1 + a_2 n_2 y_2 + a_3 n_3 y_3 + \ldots + a_k n_k y_k$ is the solution of (mod n).

Problem
Solve the system $x \equiv 1 \pmod 3$ $x \equiv 2 \pmod 4$ $x \equiv 3 \pmod 5$.
Solution
Given system is $x \equiv 1 \pmod 3$ $x \equiv 2 \pmod 4$ $x \equiv 3 \pmod 5$.
Here $a_1 = 1, a_2 = 2, a_3 = 3$
$m_1 = 3, m_2 = 4, m_3 = 5$
We find m_1, m_2, m_3 are pair wise relatively prime
Let $n = m_1.m_2.m_3 = 3.4.5 = 60$
and

$$n_1 = \frac{n}{m_1} = \frac{3.4.5}{3} = 20$$

$$n_2 = \frac{n}{m_2} = \frac{3.4.5}{4} = 15$$

$$n_3 = \frac{n}{m_3} = \frac{3.4.5}{5} = 12$$

1. We find y_1, y_2, y_3 from the congruences
$n_1 y_1 \equiv 1 \pmod{m_1}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$n_2y_2 \equiv 1 \pmod{m_2}$

$n_3y_3 \equiv 1 \pmod{m_3}$

we have $n_1y_1 \equiv 1 \pmod{m_1}$

$\Rightarrow$ $20y_1 \equiv 1 \pmod 3$

Since $20.2 = 40 \equiv 1 \pmod 3$, we see $y_1 = 2$ is a solution.

we have $n_2y_2 \equiv 1 \pmod{m_2}$

$\Rightarrow$ $15y_2 \equiv 1 \pmod 4$

Since $15.3 = 45 \equiv 1 \pmod 4$, we see $y_2 = 3$ is a solution.

we have $n_3y_3 \equiv 1 \pmod{m_3}$

$\Rightarrow$ $12y_3 \equiv 1 \pmod 5$

Since $12.3 = 36 \equiv 1 \pmod 5$, we see $y_3 = 3$ is a solution.

2. The solution is $x = a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 \pmod n$

$x = 1.20.2 + 2.15.3 + 3.12.3 \pmod{60}$

$\therefore$ $x = 40 + 90 + 72 \pmod{60}$

$\Rightarrow$ $x = 238 \pmod{60}$

$\Rightarrow$ $x = 58 \pmod{60}$ [238 = 3.60 + 58]

$\therefore$ 58 is the unique solution (mod 60)

$\therefore$ the solution of the system is $x = 58 \pmod{60}$ and it is the unique solution.

[OR]

Let x be the number. When x is divided by 3, 4, 5 leaves the remainder 1,2,3 respectively.

$\therefore$ $x \equiv 1 \pmod 3 \Rightarrow x \equiv -2 \pmod 3$

$x \equiv 2 \pmod 4 \Rightarrow x \equiv -2 \pmod 4$

$x \equiv 3 \pmod 5 \Rightarrow x \equiv -2 \pmod 5$

But lcm of [3, 4, 5] =3.4.5 = 60

$\therefore$ $x \equiv -2 \pmod{60}$

$\equiv 58 \pmod 6$

$\therefore$ 58 is the least positive integer required.

Problem

Solve the system $x \equiv 3 \pmod 7$ $x \equiv 4 \pmod 9$ $x \equiv 8 \pmod{11}$.

[OR]

Find the least positive integer that leaves remainder 3 when divided by 7, 4 when divided by 9, and 8 when divided by 11.

Solution

Given system is $x \equiv 3 \pmod 7$ $x \equiv 4 \pmod 9$ $x \equiv 8 \pmod{11}$.

Here $a_1 = 3, a_2 = 4, a_3 = 8$

$m_1 = 7, m_2 = 9, m_3 = 11$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

We find m_1, m_2, m_3 are pair wise relatively prime

Let $n = m_1.m_2.m_3 = 7.9.8 = 693$

and $$n_1 = \frac{n}{m_1} = \frac{7.9.11}{7} = 99$$

$$n_2 = \frac{n}{m_2} = \frac{7.9.11}{9} = 77$$

$$n_3 = \frac{n}{m_3} = \frac{7.9.11}{11} = 63$$

1. We find y_1, y_2, y_3 from the congruences

   $n_1y_1 \equiv 1 \pmod{m_1}$

   $n_2y_2 \equiv 1 \pmod{m_2}$

   $n_3y_3 \equiv 1 \pmod{m_3}$

   we have $n_1y_1 \equiv 1 \pmod{m_1}$

   $\Rightarrow$ $99y_1 \equiv 1 \pmod 7$

   Since $99.1 = 99 \equiv 1 \pmod 3$, we see $y_1 = 1$ is a solution.

   we have $n_2y_2 \equiv 1 \pmod{m_2}$

   $\Rightarrow$ $77y_2 \equiv 1 \pmod 9$

   Since $77.2 = 154 \equiv 1 \pmod 9$, we see $y_2 = 2$ is a solution.

   we have $n_3y_3 \equiv 1 \pmod{m_3}$

   $\Rightarrow$ $72y_3 \equiv 1 \pmod{11}$

   Since $72.2 = 144 \equiv 1 \pmod{11}$, we see $y_3 = 2$ is a solution.

2. The solution is $x = a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 \pmod n$

   $x = 3.99.1 + 4.77.2 + 8.72.2 \pmod{693}$

   $\therefore$ $x = 297 + 616 + 3528 \pmod{693}$

   $\Rightarrow$ $x = 4441 \pmod{693}$

   $\Rightarrow$ $x = 283 \pmod{693}$ [4441 = 6.693+283]

   $\therefore$ 283 is the unique solution (mod 693)

   $\therefore$ the solution of the system is $x = 283 \pmod{693}$ and it is the unique solution.

Problem

Sun-Tsu's puzzle can be translated as system of congruences. If x is the number of things then $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 5$ $x \equiv 2 \pmod 7$.

Solution

Given system is $x \equiv 2 \pmod 3$ $x \equiv 3 \pmod 5$ $x \equiv 2 \pmod 7$.

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

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

We find m_1, m_2, m_3 are pair wise relatively prime

Let $n = m_1.m_2.m_3 = 3.5.7 = 105$

and $n_1 = \frac{n}{m_1} = \frac{3.5.7}{3} = 35$

$n_2 = \frac{n}{m_2} = \frac{3.5.7}{5} = 21$

$n_3 = \frac{n}{m_3} = \frac{3.5.7}{7} = 15$

1. We find y_1, y_2, y_3 from the congruences

   $n_1y_1 \equiv 1 \pmod{m_1}$

   $n_2y_2 \equiv 1 \pmod{m_2}$

   $n_3y_3 \equiv 1 \pmod{m_3}$

   we have $n_1y_1 \equiv 1 \pmod{m_1}$

   $\Rightarrow$ $35y_1 \equiv 1 \pmod 3$

   Since $35.2 = 70 \equiv 1 \pmod 3$, we see $y_1 = 2$ is a solution.

   we have $n_2y_2 \equiv 1 \pmod{m_2}$

   $\Rightarrow$ $21y_2 \equiv 1 \pmod 5$

   Since $21.1 = 21 \equiv 1 \pmod 5$, we see $y_2 = 1$ is a solution.

   we have $n_3y_3 \equiv 1 \pmod{m_3}$

   $\Rightarrow$ $15y_3 \equiv 1 \pmod 7$

   Since $15.1 = 15 \equiv 1 \pmod 7$, we see $y_3 = 1$ is a solution.

2. The solution is $x = a_1n_1y_1 + a_2n_2y_2 + a_3n_3y_3 \pmod n$

   $x = 2.35.2 + 3.21.1 + 2.15.1 \pmod{105}$

   $\therefore$ $x = 140 + 63 + 30 \pmod{105}$

   $\Rightarrow$ $x = 233 \pmod{105}$

   $\Rightarrow$ $x = 23 \pmod{60}$ [233 =2.105 + 23]

   $\therefore$ 23 is the unique solution (mod 105)

   $\therefore$ the solution of the system is $x = 23 \pmod{105}$ and it is the unique solution.

Problem

Find the least positive integer when divided by 3, 4, 5, 6 leaves the remainder 2,3,4,5 respectively.

Solution

Let x be the number. When x is divided by 3, 4, 5, 6 leaves the remainder 2,3,4,5 respectively.

$\therefore$ $x \equiv 2 \pmod 3 \Rightarrow x \equiv -1 \pmod 3$

$x \equiv 3 \pmod 4 \Rightarrow x \equiv -1 \pmod 4$

$x \equiv 4 \pmod 5 \Rightarrow x \equiv -1 \pmod 5$

$x \equiv 5 \pmod 6 \Rightarrow x \equiv -1 \pmod 6$

But lcm of [3, 4, 5, 6] =2.3.2.5 = 60

2	3, 4, 5, 6
3	3, 2, 5, 3
	1, 2, 5, 1

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$\therefore$ $x \equiv -1 \pmod{60}$

$\equiv 59 \pmod{6}$

$\therefore$ 59 is the least positive integer required.

2X2 Linear system

Definition

A system of linear congruence of the form

$ax + by \equiv e \pmod{m}$

$cx + dy \equiv f \pmod{m}$

is called 2X2 linear system, where a, b, c, d, e, f are integers and m is a positive integer.

A solution of the linear system is a pair $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$ that satisfies both the congruences.

The solution can be obtained by a formula similar to Cramer's rule and by elimination method.

Theorem

The linear system of congruences

$ax + by \equiv e \pmod{m}$ and $cx + dy \equiv f \pmod{m}$

has a unique solution if and only if $(\Delta, m) = 1$ where $\Delta = ad - bc \pmod{m}$.

Proof

Given the linear congruences

$ax + by \equiv e \pmod{m}$ (1)

$cx + dy \equiv f \pmod{m}$ (2)

Let $\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \equiv ad - bc \pmod{m}$

Suppose the system has a solution

$x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$

Then $ax_0 + by_0 \equiv e \pmod{m}$ (3)

$cx_0 + dy_0 \equiv f \pmod{m}$ (4)

(3)xd$\Rightarrow$ $adx_0 + bdy_0 \equiv ed \pmod{m}$

(4)xb$\Rightarrow$ $bcx_0 + bdy_0 \equiv bf \pmod{m}$

Subtracting $(ad - bc)x_0 \equiv (ed-bf) \pmod{m}$

$\Rightarrow$ $\Delta x_0 \equiv (ed-bf) \pmod{m}$

This is a linear congruence is x_0

We know x_0 has unique value iff $(\Delta, m) = 1$

[(4)xa$\Rightarrow$ $acx_0 + ady_0 \equiv af \pmod{m}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

(3)xc$\Rightarrow$ $acx_0 + bcy_0 \equiv ce \pmod m$

Subtracting $(ad - bc)y_0 \equiv (af-ce) \pmod m$

$\Rightarrow$ $\Delta y_0 \equiv (af-ce) \pmod m$]

Similarly y_0 has unique value iff $(\Delta, m) = 1$

Hence the system has unique solution modulo m iff $(\Delta, m) = 1$

The unique solution modulo m is given by

$x_0 \equiv \Delta^{-1}(ed-bf) \pmod m$

$\equiv \Delta^{-1}\begin{vmatrix} e & b \\ f & d \end{vmatrix} \pmod m$ where $\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$

$y_0 \equiv \Delta^{-1}(af - ce) \pmod m$

$\equiv \Delta^{-1}\begin{vmatrix} a & e \\ c & f \end{vmatrix} \pmod m$

Where $\Delta.\Delta^{-1} \equiv 1 \pmod m$

Thus $x \equiv x_0 \pmod m$, $y \equiv y_0 \pmod m$ is the unique solution of linear system.

Note

This method is similar to Cramer's rule. In x_0 the determinant $\begin{vmatrix} e & b \\ f & d \end{vmatrix}$ is obtained from Δ by the replacing x column by constant column and in y_0, $\begin{vmatrix} a & e \\ c & f \end{vmatrix}$ is obtained from Δ by the replacing y column by constant column

Problem

Solve the system of congruence

$$3x + 13y \equiv 8 \pmod{55}$$
$$5x + 21y \equiv 34 \pmod{55}$$

Solution

Given the linear system

$3x + 13y \equiv 8 \pmod{55}$

$5x + 21y \equiv 34 \pmod{55}$

Here a=3, b=13, c=5, d=21, e=8, f=34

Now $\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \equiv ad - bc \pmod m$

$\Delta = \begin{vmatrix} 3 & 13 \\ 5 & 21 \end{vmatrix} \equiv 3.21 - 5.13 \pmod{55}$

$\equiv 63 - 65 \pmod{55}$

$\equiv -2 \pmod{55}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$\equiv 53 \pmod{55}$

Here $\Delta = 53$ and $m = 55$

$\therefore$ $(\Delta, m) = (53, 55) = 1$

$\therefore$ the system has unique solution modulo 55

The solution is $x_0 \equiv \Delta^{-1}\begin{vmatrix} 8 & 13 \\ 34 & 21 \end{vmatrix} \pmod{55}$

$y_0 \equiv \Delta^{-1}\begin{vmatrix} 3 & 8 \\ 5 & 34 \end{vmatrix} \pmod{55}$

To find Δ^{-1}

Now $\Delta.\Delta^{-1} \equiv 1 \pmod{55} \Rightarrow 53.\Delta^{-1} \equiv 1 \pmod{55}$

$\Rightarrow$ $-2.\Delta^{-1} \equiv 1 \pmod{55}$ $[\because 53 \equiv -2 \pmod{55}]$

If $\Delta^{-1} = -28$ then $(-2)(-28) = 56 \equiv 1 \pmod{55}$

But $-28 \equiv 27 \pmod{55}$

$\therefore$ $\Delta^{-1} \equiv 27 \pmod{55}$

$\therefore$ $x_0 \equiv \Delta^{-1}(ed-bf) \pmod{m}$

$\equiv 27(8.21 - 34.13) \pmod{55}$

$\equiv 27(168 - 442) \pmod{55}$

$\equiv 27(-274) \pmod{55}$

$\equiv 27(1) \pmod{55}$ $[\because 274 \equiv -1 \pmod{55} \Rightarrow -274 \equiv 1 \pmod{55}]$

$\Rightarrow$ $x_0 \equiv 27 \pmod{55}$

and $y_0 \equiv \Delta^{-1}(af - ce) \pmod{m}$

$\equiv 27(3.34-5.8) \pmod{55}$

$\equiv 27(102-40) \pmod{55}$

$\equiv 27.62 \pmod{55}$

$\equiv 27.7 \pmod{55}$

$\equiv 189 \pmod{55}$

$\Rightarrow$ $y_0 \equiv 24 \pmod{55}$ [189 = 3.55+24]

Thus $x_0 \equiv 27 \pmod{55}$ and $y_0 \equiv 24 \pmod{55}$ is the unique solution of the given system.

Note The solution is also written as $x=27+55t$, $y=24+55t$, $t \in Z$

Problem

Solve the system of congruence

$$5x + 6y \equiv 8 \pmod{13}$$
$$6x - 7y \equiv 2 \pmod{13}$$

Solution

Given the linear system

$5x + 6y \equiv 8 \pmod{13}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : IV	Unit Name: LINEAR DIOPHANTINE EQUATIONS AND CONGRUENCES	Date	14-11-2017

LECTURE NOTES

$6x - 7y \equiv 2 \pmod{13}$

Here a=5, b=6, c=6, d=-7, e=10, f=2

Now $\Delta = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \equiv ad - bc \pmod m$

$\Delta = \begin{vmatrix} 5 & 6 \\ 6 & -7 \end{vmatrix} \equiv 5.(-7)-6.6 \pmod{13}$

$\equiv -35 - 36 \pmod{13}$

$\equiv -71 \pmod{13}$

$\equiv 7 \pmod{13}$ [$\because -71 \equiv 7 \pmod{13}$]

Here $\Delta = 7$ and $m = 13$

$\therefore (\Delta, m) = (7, 13) = 1$

$\therefore$ the system has unique solution modulo 13

The solution is $x_0 \equiv \Delta^{-1} \begin{vmatrix} e & b \\ f & d \end{vmatrix} \pmod m$

$\equiv \Delta^{-1} \begin{vmatrix} 10 & 6 \\ 2 & -7 \end{vmatrix} \pmod{13}$

$y_0 \equiv \Delta^{-1} \begin{vmatrix} a & e \\ c & f \end{vmatrix} \pmod m$

$\equiv \Delta^{-1} \begin{vmatrix} 5 & 10 \\ 6 & 2 \end{vmatrix} \pmod{13}$

To find Δ^{-1}

Now $\Delta.\Delta^{-1} \equiv 1 \pmod{13} \Rightarrow 7.\Delta^{-1} \equiv 1 \pmod{13}$

If $\Delta^{-1} = 2$ then $(2)(7) = 14 \equiv 1 \pmod{13}$

But $\Delta^{-1} \equiv 2 \pmod{13}$

$\therefore x_0 \equiv \Delta^{-1}(ed-bf) \pmod m$

$\equiv 2[10.(-7) - 6.2] \pmod{13}$

$\equiv 2(-70- 12) \pmod{13}$

$\equiv 2(-82) \pmod{13}$

$\equiv 2(-4) \pmod{13}$ [$\because -82=-6.13-4$]

$\equiv -8 \pmod{13}$

$\Rightarrow x_0 \equiv 5 \pmod{55}$

and $y_0 \equiv \Delta^{-1}(af - ce) \pmod m$

$\equiv 2 (5.2-6.10) \pmod{13}$

$\equiv 2(10-60) \pmod{13}$

$\equiv 2.(-50) \pmod{13}$

$\equiv 2.2 \pmod{13}$ [$\because 50 \equiv -2 \pmod{13} \Rightarrow -50 \equiv 2 \pmod{13}$]

$\Rightarrow y_0 \equiv 4 \pmod{13}$

Thus $x_0 \equiv 5 \pmod{13}$ and $y_0 \equiv 4 \pmod{13}$ is the unique solution of the given system.

Problem

Solve the system of congruence

$$3x + 4y \equiv 5 \pmod 7$$
$$4x + 5y \equiv 6 \pmod 7$$

by using elimination method.

Solution

Given the linear system of congruences

$3x + 4y \equiv 5 \pmod 7$ (1)

$4x + 5y \equiv 6 \pmod 7$ (2)

(1)x5 $15x + 20y \equiv 25 \pmod 7$

(2)x4 $16x + 20y \equiv 24 \pmod 7$

Subtracting we get $-x \equiv 1 \pmod 7$

$\Rightarrow$ $x \equiv -1 \pmod 7$

$\Rightarrow$ $x \equiv 6 \pmod 7$

Substituting in (1) we get

$3.6 + 4y \equiv 5 \pmod 7$

$\Rightarrow$ $18 + 4y \equiv 5 \pmod 7$

$\Rightarrow$ $4 + 4y \equiv 5 \pmod 7$ [18=2.7+4]

$\Rightarrow$ $4y \equiv 1 \pmod 7$

$\Rightarrow$ $y \equiv 2 \pmod 7$ [$\because 4.2=8 \equiv 1 \pmod 7$]

$\therefore$ the solution is $x \equiv 6 \pmod 7$ and $y \equiv 2 \pmod 7$

Home work

Solve the system of congruence

$$x + 3y \equiv 3 \pmod{11}$$
$$5x + y \equiv 6 \pmod{11}$$

by using elimination method

[Ans. $x \equiv 4 \pmod{11}$ and $y \equiv 7 \pmod{11}$