(ii) let $b \in [a]$. Then $b \equiv a \pmod m$. Suppose $x \in [b]$.
This implies that $x \equiv b \pmod m$. So, using (iii) of Theorem 15,
we have $x \equiv a \pmod m$. So $x \in [a]$. Hence $[b] \subseteq [a]$
Now assume $x \in [a]$. Then $x \equiv a \pmod m$. Since $b \equiv a \pmod m$
we find that $a \equiv b \pmod m$. Hence $x \equiv a \pmod m$ and
$a \equiv b \pmod m$ together implies that $x \equiv b \pmod m$.
So, $x \in [b]$. So, $[a] \subseteq [b]$. So $[a] = [b]$

(iii) Let a, b be two integers. Suppose $[a] \cap [b] \neq \phi$
Let $x \in [a] \cap [b]$. So $x \in [a]$ and $x \in [b]$
$\Rightarrow$ $x \equiv a \pmod m$ and $x \equiv b \pmod m$
Now $x \equiv b \pmod m$ implies that $b \equiv x \pmod m$
So, $b \equiv x \pmod m$ and $x \equiv a \pmod m$ together
imply that $b \equiv a \pmod m$
So $b \in [a]$ Hence (ii) implies $[b] = [a]$

Consider the positive integer 6 and consider the congruence classes modulo 6. Now $8 \equiv 2 \pmod 6$ Hence $8 \in [2]$
This implies that $[8] = [2]$. Likewise $[1] = [7]$,
$[3] = [9]$, $[4] = [10]$ etc.

~~Theorem 19~~ ~~The number~~ For any positive integer m, let $\mathbb{Z}_m$ denote the congruence classes modulo m.

Theorem 20 The number of elements of $\mathbb{Z}_m$ is finite and this number is m.

Proof: Let k be any integer. By division algorithm there exist integers q and r such that $k = qm + r$ where $0 \leq r \leq m-1$

Hence m divides $k-r$. This implies $k \equiv r \pmod m$.

So, $[k] = [r]$. So, we find that for any integer k there exist an integer r, such that $0 \le r \le m-1$ and $[k] = [r]$

Hence the number of congruence class $[k]$ modulo m is less than or equal to m.

Now let $[r]$ and $[t]$ be two congruence classes, modulo m such That $0 \le r, t \le m-1$. Then

$$-(m-1) \le r-t \le (m-1)$$

Hence $[r] = [t]$ if and only if $r \equiv t \pmod m$, i.e., if and only if m divides $r-t$ i.e., if and only if $r-t = 0$ i.e., if and only if $r = t$.

It follows that $[0], [1], [2], \ldots, [m-1]$ are the m distinct congruence classes and congruence class $[k]$ equals to one of these. Hence the theorem.

Consider the positive integer 6. Here $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

where $[0] = \{\ldots, -12, -6, 0, 6, 12 \ldots\} = \{6k : k \in \mathbb{Z}\}$

$[1] = \{\ldots, -17, -11, -5, 1, 7, 13, \ldots\} = \{6k+1 : k \in \mathbb{Z}\}$

$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\} = \{6k+2 : k \in \mathbb{Z}\}$

$[3] = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\} = \{6k+3 : k \in \mathbb{Z}\}$

$[4] = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\} = \{6k+4 : k \in \mathbb{Z}\}$

$[5] = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\} = \{6k+5 : k \in \mathbb{Z}\}$

and $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5]$

We now define addition and multiplication of congruence classes $[a]$ and $[b]$ in $\mathbb{Z}_n$ for any positive integer n.

$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ Let $[a], [b] \in \mathbb{Z}_n$

Then $[a] + [b] = [a+b]$ if $a+b < n$

$= [a+b-n]$ if $a+b \ge n$

So, we demonstrate the addition of congruence classes in $\mathbb{Z}_6$ by the following table, which is known as addition table for $\mathbb{Z}_6$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

So, $[2]+[3] = [5]$

$[4]+[5]$

$= [(4+5)-6] = [3]$ etc.

We now define multiplication for two classes $[a], [b] \in \mathbb{Z}_n$ by

$[a].[b] = [ab]$ if $ab < n$

$[a].[b] = [ab - kn]$ if $ab \geq n$ and $ab = kn + r$, $0 \leq r \leq n-1$

We construct the multiplication table for $\mathbb{Z}_6$ as follows.

.	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Definition: An element $[b] \in \mathbb{Z}_n$ is called an inverse of an element $[a] \in \mathbb{Z}_n$ if $[a].[b] = [1]$ in $\mathbb{Z}_n$

Theorem 21 Let a and n be integers with $n \geq 2$. Then $[a]$ has an inverse in $\mathbb{Z}_n$ if and only if a and n are relatively prime.

Proof: Suppose a and n are relatively prime. Then $\gcd(a, n) = 1$

Hence there exist integers b and c such that $ab + nc = 1$

This implies $ab \equiv 1 \pmod{n}$ So, $[ab] = [1]$ in $\mathbb{Z}_n$

Hence $[ab] = [a][b] = [1]$ in $\mathbb{Z}_n$. Hence $[a].[b] = [1]$ in $\mathbb{Z}_n$

Conversely, if $[b]$ exists in $\mathbb{Z}_n$ such that $[a][b] = [1]$ in $\mathbb{Z}_n$, then $[ab] = [1]$, So, $ab \equiv 1 \pmod{n}$ This implies that $ab - 1 = nk$ for some integer k. Hence

$ab + n(-k) = 1$. So, $\gcd(a, n) = 1$.

Example 1 Find the inverse of $[15]$ in $\mathbb{Z}_{19}$

Solution: Because $\gcd(15, 19) = 1$, the inverse of $[15]$ exists in $\mathbb{Z}_{19}$ Now

$$19 = 15.1 + 4$$
$$15 = 4.3 + 3$$
$$4 = 3.1 + 1$$

Hence $1 = 4 - 3.1 = 4 - (15 - 4.3) = 4.4 - 15$

$$= (19 - 15.1)4 - 15$$
$$= 19.4 - 15.4 - 15$$
$$= 19.4 + 15(-5)$$

This implies that $[1] = [19][4] + [15][-5]$

$$= [0][4] + [15][14] \quad [14 \equiv -5 \pmod{19}]$$
$$= [15][14]$$

Hence the inverse of $[15]$ is $[14]$

Exercise 1. Find the inverse of $[7]$ in $\mathbb{Z}_{20}$

2. Find the inverse of $[9]$ in $\mathbb{Z}_{16}$

3. construct addition table and multiplication table for $\mathbb{Z}_5$ and $\mathbb{Z}_7$

Linear congruences Let m be a positive integer and a, b be two integers. If there exists an integer u such that $au \equiv b \pmod{m}$ Then we say that u satisfies the congruence $ax \equiv b \pmod{m}$ where x is an unknown.

Definition A congruence of the form

$$ax \equiv b \pmod{m} \quad \text{---} \quad (1)$$

where a, b are integers, m is a positive integer and x is an unknown integer, is called a linear congruence in one variable x. An integer x_0 is called a solution of (1) if $ax_0 \equiv b \pmod{m}$

Example: $2x \equiv 1 \pmod{5}$ is a linear congruence in one variable. Since $2.3 \equiv 1 \pmod{5}$ we find that 3 is a solution of this congruence. Now $8 \equiv 3 \pmod{5}$, we find that 8 is also a solution of $2x \equiv 1 \pmod{5}$. In fact, we can show that if x_0 is an integer such $x_0 \equiv 3 \pmod{5}$ i.e., x_0 is a member of class $[3]$ modulo 5, then x_0 is a solution of the congruence.

We state two theorems without proof:

Theorem 22 Let a, b and m be integers and $m > 0$ and $\gcd(a, m) = 1$ Then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution

Theorem 23 Let a, b and m be integers with $m > 0$. and $\gcd(a, m) = d$ Then $ax \equiv b \pmod{m}$ has no solution when d does not divide b; but if d divides b, there are exactly d solutions.

Now with the help of some worked out example we show how to find solutions for linear congruence in one variable,

Worked out examples : 1. Find all solutions of the congruence

$4x \equiv 6 \pmod 4$

Solution : Let $4x \equiv 6 \pmod 4$ . . . (1)

Here gcd $(4,4) = 4$ and 4 does not divide 6. Hence (1) has no solution.

2. Find all solutions of $3x \equiv 7 \pmod 4$

Solution : Let $3x \equiv 7 \pmod 4$ . . . (1)

Here gcd $(3,4) = 1$ Hence (1) has unique solution.

Now $3.(-1) + 4.1 = 1$ Hence $3(-7) + 4(7) = 7$. This shows that $3(-7) \equiv 7 \pmod 4$. This shows that (-7) is a solution of (1)

Now $-7 \equiv 1 \pmod 4$. So, the given has the solution

$x \equiv 1 \pmod 4$

3. Find all solutions of $7x \equiv 4 \pmod{18}$

Solution : Let $7x \equiv 4 \pmod{18}$ . . . (1)

Here gcd $(7, 18) = 1$ Hence (1) has a unique solution.

$$18 = 7.2 + 4$$
$$7 = 4.1 + 3$$
$$4 = 3.1 + 1$$

So, $1 = 4 - 3.1 = 4 - (7 - 4.1) = 4.2 - 7$

$$= (18 - 7.2).2 - 7$$

$$= 18.2 + 7(-5)$$

Hence $4 = 18.8 + 7(-20)$. This implies $7(-20) \equiv 4 \pmod{18}$. Hence $x_0 = -20$ is a solution of (1) Now $-20 \equiv 16 \pmod{18}$

So, the given congruence has the solution $x \equiv 16 \pmod{18}$

4. Solve the congruence $12x \equiv 9 \pmod{15}$

Solution: Since $\gcd(12, 15) = 3$ and 3 divides 9, the congruence

$$12x \equiv 9 \pmod{15} \quad \ldots (1)$$

has exactly three solutions.

Now $3 = 12(-1) + 15(1)$. Then $9 = 12(-3) + 15(3)$

Accordingly, we have $12(-3) \equiv 9 \pmod{15}$ and hence $x_0 \equiv -3$ is a solution of $12x \equiv 9 \pmod{15}$

So, the three solutions of the congruence (1) are given by

$$x \equiv \left(-3 + \left(\frac{15}{3}\right) i\right) \pmod{15}, \text{ where } i = 0, 1, 2$$

i.e., $x \equiv (-3 + 5i) \pmod{15}$, $i = 0, 1, 2$

So, the three solutions are $x \equiv -3 \pmod{15}$, $x \equiv 2 \pmod{15}$ and $x \equiv 7 \pmod{15}$

5. Solve the linear congruence $72x \equiv 18 \pmod{42}$

Solution: Since $\gcd(72, 42) = 6$ and 6 divides 18, the congruence

$$72x \equiv 18 \pmod{42} \quad \ldots (1)$$

has exactly six solutions.

We now find a solution of (1). To find a solution of (1), we may consider the following congruence and find a solution of it.

$$12x \equiv 3 \pmod{7} \quad \ldots (2)$$

Now $\gcd(12, 7) = 1$ and $12 = 7.1 + 5$, $7 = 1.5 + 2$, $5 = 2.2 + 1$

Hence $1 = 5 + 2(-2) = 5 + (7 - 5)(-2) = 7(-2) + 5.3$

$$= 7(-2) + (12 - 7.1)3 = 12.3 + 7(-5)$$

Accordingly $3 = 12.9 + 7(-15)$. Hence $12.9 \equiv 3 \pmod{7}$. So, we find that $x_0 = 9$ is a solution of (2). Hence $x_0 = 9$

is a solution of (1)

Therefore the six solutions of (1) are given by

$$x \equiv \left(9 + \frac{42}{6} i\right) \pmod{42} \quad i = 0, 1, 2, 3, 4, 5$$

i.e., $x \equiv (9 + 7i) \pmod{42} \quad i = 0, 1, 2, 3, 4, 5$

Exercise: 1. Find all the solutions of the following linear congruences:

(a) $5x \equiv 3 \pmod{19}$

(b) $12x \equiv 8 \pmod{42}$

(c) $5x \equiv 2 \pmod{26}$

(d) $6x \equiv 3 \pmod{9}$

(e) $36x \equiv 27 \pmod{45}$

Now we consider the solution of a system of linear congruences.

Theorem 24 (Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_k$ be positive integers such that $\gcd(m_i, m_j) = 1$, $i \neq j$. Then for any integers $a_1, a_2, \ldots, a_k$, the system of linear congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

has a solution. Furthermore, any two solutions of the system are congruent modulo $m_1 m_2 \cdots m_k$.

Proof: Let $M = m_1 m_2 \cdots m_k$ and $N_i = \frac{M}{m_i}$, where $i = 1, 2, 3, \ldots, k$

Since $\gcd(m_i, m_j) = 1$ for $i \neq j$, we find that $\gcd(N_i, m_i) = 1$

It is therefore possible to find the solution of the linear congruence $N_i x \equiv 1 \pmod{m_i}$; denote this unique solution by b_i. Now we propose to show that the integer $x_0 = a_1 b_1 N_1 + a_2 b_2 N_2 + \cdots + a_k b_k N_k$ is a solution of the given system of linear congruences.

We first observe that $N_i = \frac{M}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k \equiv 0 \pmod{m_j}$ for $j = 1, 2, \ldots, i-1, i+1, \ldots, k$. Hence

$$x_0 \equiv a_i b_i N_i \pmod{m_i} \quad \text{for } i = 1, 2, \ldots, k$$

But $N_i b_i \equiv 1 \pmod{m_i}$ and this implies $a_i b_i N_i \equiv a_i \pmod{m_i}$

Hence $x_0 \equiv a_i \pmod{m_i}$ $i = 1, 2, \ldots, k$. This shows that x_0 is a solution of the given system of congruences.

Next we shows that if $\bar{x}$ is a solution of the given system, then $\bar{x} \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$

Suppose $\bar{x} \equiv a_i \pmod{m_i}$ for $i = 1, 2, \ldots, k$

Then $\bar{x} \equiv x_0 \pmod{m_i}$ for $i = 1, 2, \ldots, k$ and so, m_i divides $\bar{x} - x_0$ for each $i = 1, 2, \ldots, k$ Since $\gcd(m_i, m_j) = 1$ for $i \neq j$. It follows that $m_1 m_2 \cdots m_k$ divides $\bar{x} - x_0$.

Thus we find that $\bar{x} \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$

This completes the proof.

Worked examples:

1. Solve the following system of congruence

$$x \equiv 2 \pmod 7$$
$$x \equiv 5 \pmod{19}$$
$$x \equiv 4 \pmod 5$$

Solution Let $M = 7.19.5$. Now consider the congruences

$$\frac{M}{7} x \equiv 1 \pmod 7$$
$$\frac{M}{19} x \equiv 1 \pmod{19}$$
$$\frac{M}{5} x \equiv 1 \pmod 5$$

That is,

$$95x \equiv 1 \pmod 7$$
$$35x \equiv 1 \pmod{19}$$
$$133x \equiv 1 \pmod 5$$

That is, $(91+4)x \equiv 1 \pmod 7$

$(38-3)x \equiv 1 \pmod{19}$

$(130+3)x \equiv 1 \pmod 5$

Now Consider the system of congruences

$$4x \equiv 1 \pmod 7 \quad \text{——} (1)$$
$$-3x \equiv 1 \pmod{19} \quad \text{——} (2)$$
$$3x \equiv 1 \pmod 5 \quad \text{——} (3)$$

Notice that $x = 2$ is a solution of (1), $x = 6$ is a solution of (2) and $x = 2$ is a solution of (3). Hence

$95x \equiv 1 \pmod 7$ is satisfied by $x = 2$

$35x \equiv 1 \pmod{19}$ is satisfied by $x = 6$

$133x \equiv 1 \pmod 5$ is satisfied by $x = 2$

Hence a solution of the given system of congruences is given by

$x_0 = 2 \cdot 2 \cdot 95 + 5 \cdot 6 \cdot 35 + 4 \cdot 2 \cdot 133 = 2494$

and the unique solution is given by

$$x \equiv 2494 \pmod{7 \cdot 19 \cdot 5}$$

i.e., $x \equiv 2494 \pmod{665}$

i.e., $x \equiv 499 \pmod{665}$

2. A certain integer between 1 and 1000 leaves the remainder 1, 2, 6 when divided by 9, 11, 13 respectively. Find the integer.

Solution: The required integer is a solution of the system of linear congruences

$$\left.\begin{aligned} x &\equiv 1 \pmod 9 \\ x &\equiv 2 \pmod{11} \\ x &\equiv 6 \pmod{13} \end{aligned}\right\} \quad \text{——} (1)$$

Let $M = 9 \cdot 11 \cdot 13$. Now consider the congruences

$$13 \cdot 11x \equiv 1 \pmod 9$$
$$13 \cdot 9x \equiv 1 \pmod{11}$$
$$9 \cdot 11x \equiv 1 \pmod{13}$$

That is,
$$143x \equiv 1 \pmod 9$$
$$117x \equiv 1 \pmod{11}$$
$$99x \equiv 1 \pmod{13}$$

That is,
$$(144-1)x \equiv 1 \pmod 9$$
$$(110+7)x \equiv 1 \pmod{11}$$
$$(91+8)x \equiv 1 \pmod{13}$$

Hence consider the system
$$-x \equiv 1 \pmod 9$$
$$7x \equiv 1 \pmod{11}$$
$$8x \equiv 1 \pmod{13}$$

Now $x = 8$ is a solution of $-x \equiv 1 \pmod 9$. Hence $x = 8$ is a solution of $143x \equiv 1 \pmod 9$

Similarly, $x = 8$ is a solution of $117x \equiv 1 \pmod{11}$ and $x = 5$ is a solution of $99x \equiv 1 \pmod{13}$

Hence a solution of the system (1) is given by

$$x_0 = 1 \cdot 8 \cdot 13 \cdot 11 + 2 \cdot 8 \cdot 9 \cdot 13 + 6 \cdot 5 \cdot 9 \cdot 11 = 5986$$

and the unique solution is given by $x \equiv 5986 \pmod{1287}$

i.e., $x \equiv 838 \pmod{1287}$

Hence the required integer is 838.

Exercises 1. Solve the following system of congruences

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 3 \pmod 5$$

2. Find the smallest integer greater than 23 That leaves the remainders 2, 3, 2 when divided by 3, 5, 7 respectively.