UNIT-5

Congruences

Definition:

If a and b are integers and m is a positive integers, then a is said to be Congruent to b modulo m, if a-b is a multiple of m or $m/(a-b)$. This is denoted as $a \equiv b \pmod{m}$

m is called the modulus of the congruence b is called a residue of a (mod m)

If a is not congruent to b modulo 'm', it is denoted by $a \not\equiv b \pmod{m}$, We say that a and b are incongruent mod m.

Note:

If $a \equiv b \pmod{m}$, then $a = b + km$, for some integer k.

Examples:

1. $19 \equiv 7 \pmod{12}$

Soln:

$19 - 7$ ÷ by 12

Properties of Congruence:

1. When $a \equiv b \pmod m$, then $a \pmod m = b \pmod m$ and conversely.

Proof:

$a \equiv b \pmod m$ (multiple → divisible by)

$\therefore a-b$ is a multiple of m

$\therefore$ when a and b are divided by m, they leave the same remainder

(ie) $a \pmod m = b \pmod m$

Converse

When $a \pmod m = b \pmod m = r$

$a = q_1 m + r$ and $b = q_2 m + r$.

$\therefore a-b = (q_1 - q_2)m$

$=$ a multiple of m

(ie) $a \equiv b \pmod m$

2. The Congrueme relation is an equivalence relation.

Proof:

Sime $a \equiv a \pmod m$ as $a-a=0$ is divisible by m, the congrueme relation is reflexive.

When $a \equiv b \pmod m$, (ie) $a-b$ is divisible by m, clearly $b-a$ is also divisible by m

(ie) $b \equiv a \pmod{m}$.

Hence the Congruence relation is Symmetric.

When $a \equiv b \pmod{m}$, $a-b$ is divisible of m

when $b \equiv c \pmod{m}$, $b-c$ is divisible of m

(ie) ~~$a \equiv c \pmod{m}$~~

(ie) Now, $a-c = (a-b)+(b-c)$ is also divisible of m.

(ie) $a \equiv c \pmod{m}$

$\therefore$ The Congruence relation is transitive

3. If $a \equiv b \pmod{m}$ and c is any integer, then

(i) $a \pm c \equiv (b \pm c) \pmod{m}$

(ii) $ac \equiv (bc) \pmod{m}$

Proof:

(i) Since $a \equiv b \pmod{m}$, $a-b$ is a multiple of m.

Now $(a \pm c) - (b \pm c) = a-b$ is a multiple of m

$\therefore a \pm c \equiv (b \pm c) \pmod{m}$.

(ii) Since $a \equiv b \pmod{m}$, $a-b$ is a multiple of m

$\therefore (a-b)c = ac-bc$ is also a multiple of m

$\therefore ac \equiv (bc) \pmod{m}$.

Note: The converse of property 3(ii) is not true always. (ie) If $ac \equiv (bc) \bmod m$, then a need not be congruent to b modulo m always.

4. If a, b, c, d are integers and m is a positive integer such that $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

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

(ii) $ac \equiv (bd) \pmod m$

(iii) $a^n \equiv b^n \pmod m$, where n is a positive integer.

Proof:

(i) Since $a \equiv b \pmod m$, $(a-b)$ is a multiple of m and similarly $(c-d)$ is a multiple of m

$\therefore (a-b) \pm (c-d)$ is also multiple of m

(ie) $(a \pm c) - (b \pm d)$ is also a multiple of m

(ie) $a \pm c \equiv (b \pm d) \pmod m$

(ii) Since $(a-b)$ is a multiple of m, $(a-b)c$ is also a multiple of m.

Sine $(c-d)$ is a multiple of m, $(c-d)b$ is also a multiple of m.

$\therefore (a-b)c + (c-d)b$ is also a multiple of m

(ie) $ac - bd$ is a multiple of m.

(ii) $ac \equiv (bd) \pmod{m}$ ——(1)

(iii) In (1), put $c=a$ and $d=b$.

Then we get

$$a^2 \equiv b^2 \pmod{m}$$

Also, $a \equiv b \pmod{m}$

Using property (ii) in ② and ③, we get

$$a^3 \equiv b^3 \pmod{m}$$

Proceeding like this, we get

$a^n \equiv b^n \pmod{m}$, where n is a positive integer.

Theorem: 1

Cancellation law

If $ac \equiv bc \pmod{m}$ and if $d = (m, c)$ then

$$a \equiv b \pmod{\frac{m}{d}}$$

In otherwords, a common factor c can be cancelled provided the modulus is divided by $d = (m, c)$. In particular, a common factor which is relatively prime to the modulus can always be cancelled.

Proof: Sine $ac \equiv bc \pmod{m}$ we have

$$m \mid c(a-b) \quad \text{so} \quad \frac{m}{d} \Big/ \frac{c(a-b)}{d}$$

But $(m/d, c/d) = 1$,

hence $m/d \mid (a-b)$

Theorem! 2

Assume $a \equiv b \pmod{m}$. If d/m and d/a then d/b.

Proof! It suffices to assume that $d > 0$.

If d/m then $a \equiv b \pmod{m}$ implies

$a \equiv b \pmod{d}$.

But if d/a then $a \equiv 0 \pmod{d}$

So $b \equiv 0 \pmod{d}$.

Theorem! 3

If $a \equiv b \pmod{m}$ then $(a, m) = (b, m)$.

In other words, numbers which are congruent mod m have the same gcd with m.

Proof! Let $d = (a, m)$ and $e = (b, m)$.

Then d/m and d/a so d/b;

hence d/e.

Similarly, e/m, e/b so e/a; hence e/d.

Therefore $d = e$.

Theorem: 4

If $a \equiv b \pmod{m}$ and if $0 \leq |b-a| < m$, then $a = b$.

Proof: Since $m \mid (a-b)$ we have $m \leq |a-b|$ unless $a-b = 0$.

Theorem: 5

We have $a \equiv b \pmod{m}$ if and only if a and b give the same remainder when divided by m.

Proof: Write $a = mq+r$, $b = mQ+R$, where $0 \leq r < m$ and $0 \leq R < m$.

Then $a-b \equiv r-R \pmod{m}$ and

$0 \leq |r-R| < m$.

Now, using theorem (5)

Eg: Residue class modulo m – All congruence classes of integers modulo 5

$[0]_5 = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\}$

$= \{x \in \mathbb{Z} \mid x \text{ is divisible by } 5 \text{ or } x = 5k \text{ for some integer } k\}$

$= \{\ldots -10, -5, 0, 5, 10 \ldots\}$

$[1]_5 = \{x \in \mathbb{Z} / x \equiv 1 \pmod 5\}$

$= \{x \in \mathbb{Z} / x-1 = 5k\} = \{\ldots -9, -4, 1, 6, 11 \ldots\}$

$[2]_5 = \{\ldots -8, -3, 2, 7, 12 \ldots\}$, $[4]_5 = \{\ldots -6, -1, 4, 9, 14 \ldots\}$

$[3]_5 = \{\ldots -7, -2, 3, 8, 13 \ldots\}$ $[5]_5 = \{\ldots -5, 0, 5, 10, 15 \ldots\}$

∴ 5 distinct congruence classes of integer modulo 5 $[0], [1], [2], [3], [4]$

Residue classes and Complete residue systems

Defn:

Consider a fixed modulus $m > 0$. We denote by $\hat{a}$ the set of all integers x such that $x = a \pmod m$ and we call $\hat{a}$ the residue class a modulo m.

Thus, $\hat{a}$ consists of all integers of the form $a + mq$, where $q = 0, \pm 1, \pm 2 \cdots$

Note: (OR) **Defn: of Residue classes modulo 'm'**

Let 'r' be an integer then residue class of r under mod m is

$$[r] = \{x : x \in z \text{ and } x \equiv r \pmod m\}$$

$$Z_m = \{[0]_m, [1]_m, [2]_m, \ldots [m-1]_m\}$$ are $\frac{x}{m}$ $\frac{r}{m}$

m distinct congruent classes

Eg: Residue class modulo 4.

$$[r] = \{x : x \in z \text{ and } x \equiv r \pmod 4\}$$

$[0] = \{0, 4, 8, 12 \ldots\}$

$[1] = \{1, 5, 9, 13 \ldots\}$

$[2] = \{2, 6, 10, 14, 18 \ldots\}$

$[3] = \{3, 7, 11, 15 \ldots\}$,

$Z_4 = \{[0], [1], [2], [3]\}$

$13 \equiv 18 \pmod 5$

$5\overline{)13}$ (2, 10, 3) $\quad 5\overline{)18}$ (3, 15, 3)

Theorem:

For a given modulus m we have:

(a) $\hat{a} = \hat{b}$ if and only if $a \equiv b \pmod{m}$

(b) Two integers x and y in the same residue class if and only if $x \equiv y \pmod{m}$

(c) The m residue classes $\hat{1}, \hat{2} \ldots \hat{m}$ are disjoint and their union is the set of all integers.

Proof:

Parts (a) and (b) follow at once from the definition.

To prove (c) we note that the numbers $0, 1, 2 \ldots m-1$ are incongruent modulo m (by Thm 1. 4)

Hence by part (b) the residue classes

$$\hat{0}, \hat{1}, \hat{2} \ldots \hat{m-1}$$

are disjoint. But every integer x must be in exactly one of these classes because $x = qm + r$ where $0 \leq r < m$, so $x \equiv r \pmod{m}$ and hence $x \in \hat{r}$. Since $\hat{0} = \hat{m}$ this proves (c)

Complete residue system:

A set of m representatives, one from each of the residue classes $\hat{1}, \hat{2} \ldots \hat{m}$ is called a complete residue system modulo m

Eg

Any set consisting of m integers, incongruent mod m, is a complete residue system mod m. for example,

$\{1, 2 \ldots m\}$; $\{0, 1, 2 \ldots m-1\}$;

$\{1, m+2, 2m+3, 3m+4 \ldots m^2\}$.

Theorem: Assume $(k, m) = 1$. If $\{a_1 \ldots a_m\}$ is a complete residue system modulo m, so is $\{ka_1 \ldots ka_m\}$

Proof: If $ka_i \equiv ka_j \pmod{m}$ then $a_i \equiv a_j \pmod{m}$

Since $(k, m) = 1$.

Therefore no two elements in the set $\{ka_1, \ldots ka_m\}$ are congruent modulo m.

Since there are m elements in this set it forms a complete residue system.

Linear Congruence:

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

Any value of x which satisfies $ax \equiv b \pmod{m}$ is called a solution of the congruence.

Any value of x which is a solution of the congruence $ax \equiv 1 \pmod{m}$ is called an inverse of a modulo m.

Example: 1

The linear congruence $2x \equiv 3 \pmod{4}$ has no solutions, since $2x - 3$ is odd for every x and therefore cannot be divisible by 4.

Example: 2

The quadratic congruence $x^2 \equiv 1 \pmod{8}$ has exactly four solutions given by $x \equiv 1, 3, 5, 7 \pmod{8}$.

Theorem: 1

If a and m are relatively prime, then the congruence $ax \equiv 1 \pmod{m}$ has a unique solution or the inverse of 'a modulo m' is unique.

Proof:

Since a and m are relatively prime,

$\gcd(a, m) = 1$.

∴ There exist integers n_1 and n_2 such that

$n_1 a + n_2 m = 1$.

$\therefore n_1 a + n_2 m = 1 \pmod{m}$ $(\because n_1 a + n_2 m - 1 = 0)$

But $n_2 m \equiv 0 \pmod{m}$

$n_1 a \equiv 1 \pmod{m}$ ——— (1)

(ie) a solution of $ax \equiv 1 \pmod{m}$ exists, namely $x = n_1$,

Let us assume that $x = n_3$ is another solution of the congruence.

Then $n_3 a \equiv 1 \pmod{m}$ ——— (2)

From (1) and (2), we have

$n_1 a - n_3 a \equiv 0 \pmod{m}$

(ie) $n_1 a \equiv n_3 a \pmod{m}$

$\therefore n_1 \equiv n_3 \pmod{m}$ ($\because$ a & m are relatively prime)

Thus, the solution of $ax \equiv 1 \pmod{m}$ is unique modulo m.

Note: 1. If $\gcd(a, m) \neq 1$, then the congruence $ax \equiv 1 \pmod{m}$ has no solution.

2. Using the above theorem, we can find the solution of $ax \equiv b \pmod{m}$ as explained in the following example, in which we solve

$4x \equiv 3 \pmod{7}$

First we note that $\gcd(4, 7) = 1$, by Euclid's (theorem) algorithm or otherwise

Now let us find the solution of the linear congruence $4x \equiv 1 \pmod{7}$

The solution is obtained by finding m and n such that $4m + 7n = 1$

Obviously, $m = 2$ and $n = -1$ (Euclid's algorithm)

$\therefore 4 \times 2 + 7 \times (-1) = 1$

and so $4 \times 6 + 7 \times (-3) = 3$

$\therefore x = 6$ is the solution of the given congruence. It is usually given in the modular form $x \equiv 6 \pmod{7}$.

This means that $x = \ldots -8, -1, 6, 13, 20 \ldots$ satisfy the given congruence.

Theorem: 2 Assume $(a, m) = d$. Then the linear congruence

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

has solutions if and only if $d \mid b$.

Proof: If a solution exists then $d \mid b$ since $d \mid m$ and $d \mid a$.

Conversely, if $d \mid b$ the congruence

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

has a solution since $(a/d, m/d) = 1$ and this solution is also a solution of (1).

Theorem: 3

Assume $(a, m) = d$, and suppose that $d \mid b$. Then the linear congruence

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

has exactly d solutions modulo m. These are given by

$$t, \; t + \frac{m}{d}, \; t + 2\frac{m}{d} \; \ldots \; t + (d-1)\frac{m}{d}, \quad \text{---} (2)$$

where t is the unique solution modulo m/d, of the linear congruence

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \quad \text{---} (3)$$

Proof:

Every solution of (3) is also a solution of (1). Conversely, every solution of (1) satisfies (3). Now the d numbers listed in (2) are solutions of (3) hence of (1).

No two of these are congruent modulo m. Since the relations

$$t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m}, \quad \text{with } 0 \le r < d,\ 0 \le s < d$$

imply

$$r\frac{m}{d} = s\frac{m}{d} \pmod{m},$$

and hence $r \equiv s \pmod{d}$

But $0 \le |r-s| < d$ so $r = s$.

It remains to show that (1) has no solns. except those listed in (2).

If y is a soln. of (1) then $ay \equiv at \pmod{m}$ so $y \equiv t \pmod{m/d}$.

Hence $y = t + km/d$ for some k.

But $k \equiv r \pmod{d}$ for some r satisfying $0 \le r < d$. Therefore,

$$k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m} \quad \text{so} \quad y \equiv t + r\frac{m}{d} \pmod{m}$$

Therefore y is congruent modulo m to one of the numbers in (2).

This completes the proof.

Reduced Residue Theorem:

Definition:

By a reduced residue system modulo m we mean any set of $\phi(m)$ integers, incongruent modulo m, each of which is relatively prime to m.

Note: $\phi(m)$ denotes Euler's Totient.

Theorem:

If $\{a_1, a_2 \cdots a_{\phi(m)}\}$ is a reduced system modulo m and if $(k, m) = 1$, then $\{ka_1, ka_2 \cdots ka_{\phi(m)}\}$ is also a reduced residue system modulo m.

Proof: No two of the numbers ka_i are congruent modulo m.

Also, since $(a_i, m) = (k, m) = 1$ we have $(ka_i, m) = 1$ so each ka_i is relatively prime to m.

Defn! Reduced residue system

The set of integers $a, a_2 \cdots a_k$ is called a reduced residue system modulo m (written as RRS (mod m)) if

(i) $(a_i, m) = 1$ $\forall$ $i = 1, 2 \cdots k$,

(ii) $a_i \not\equiv a_j \pmod m$ $\forall$ $i \neq j$ and

(iii) If n is an integer relatively prime to m then $n \equiv a_i \pmod m$ for a unique i, $1 \leq i \leq k$.

Example! 1

The set of integers $\{1, 5, 7, 11\}$ is a Reduced residue system (mod 12). For (i) and (ii) hold clearly. Let m be any integer such that $(m, 12) = 1$.

By division algorithm,

$$m = 12q + r \qquad 0 \leq r < 12$$

Observe that, $(r, 12) = 1$.

Thus r can be either 1 or 5 or 7 or 11.

$\Rightarrow m \equiv r \pmod{12}$

Complete Residue System:

A collection of m integers $a_1, a_2 \ldots a_m$ is said to form a complete set of residues (or) Complete Residue System (CRS) modulo m if every integer is congruent modulo m to one and only one of the a_k

(ie) for every integer y, there is unique a_i such that $y \equiv a_i \pmod{m}$ for $i = 1, 2 \ldots m$

Eg: $m = 5$ we have $\{0, 1, 2, 3, 4\}$ is a CRS modulo 5

Further all possible CRS mod 5 are formed by taking only one element from each of the follg.

$\{5z+0 ; z \in Z\}, \{5z+1 : z \in Z\}, \{5z+2 : z \in Z\}, \{5z+3 : z \in Z\}, \{5z+4 ; z \in Z\}$

$z=0 \Rightarrow \{0, 1, 2, 3, 4\}$
$z=1 \Rightarrow \{5, 6, 7, 8, 9\}$
$z=-2 \Rightarrow \{-10, -9, -8, -7, -6\}$

here infinitely many CRS modulo 5

$\ldots -24, -19, -14, -9, -4, 1, 6, 11 \ldots$

Residue Class:

Residue class of 1 modulo 5 is $\{5z+1 : z \in Z\}$

...

Residue Class: For a fixed integer a, $m > 0$ the set of integers x satisfying $x \equiv a \pmod{m}$ is an arithmetic Progression.

$\ldots a-3m, a-2m, a-m, a, a+m, a+2m \ldots$

Also, since $(a_i, m) = (k, m) = 1$ we have $(ka_i, m) = 1$ so each ka_i is relatively prime to m.

Theorem: Euler - Fermat Theorem

Assume $(a, m) = 1$. Then we have $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof:

Let $\{b_1, b_2 \dots b_{\phi(m)}\}$ be a reduced residue system modulo m. Then $\{ab_1, ab_2 \dots ab_{\phi(m)}\}$ is also a reduced residue system.

Hence the product of all the integers in the first set is congruent to the product of those in the second set.

Therefore;

$$b_1 \dots b_{\phi(m)} \equiv a^{\phi(m)} b_1 \dots b_{\phi(m)} \pmod{m}$$

Each b_i is relatively prime to m so we can cancel each b_i to obtain the theorem.

Corollary: If a prime p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$

Proof:

This is a Cor/. for next theorem since $\phi(p) = p - 1$

Theorem: Little Fermat theorem:

For any integer a and any prime p we have $a^p \equiv a \pmod{p}$.

Proof:

If $p \nmid a$ this is above Corl.

If p/a then both a^p and a are congruent to $0 \bmod p$.

Theorem:

If $(a, m) = 1$ the solution (unique mod m) of the linear congruence

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

is given by

$$x \equiv b a^{\phi(m)-1} \pmod{m} \quad \text{---} \quad (2)$$

Proof:

The sol. x given by eqn. (2) satisfies eqn. (1) because of the Euler Fermat Theorem.

The solution is unique ~~and~~ mod m since $(a, m) = 1$.

Example: 1

Solve the congruence $5x \equiv 3 \pmod{24}$

Solution:

Since $(5,24) = 1$ there is a unique solution.

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

$x \equiv 3 \cdot 5^{\phi(24)-1} \pmod{24}$

$\equiv 3 \cdot 5^7 \pmod{24}$

$a = 5$, $b = 3$, $m = 24$

$\phi(6) \Rightarrow (6,1) = 1$, $(6,5) = 1$, $(6,5) = 1$, $(6,7) = 1$, $\phi(6) = \{1,5,5,7\}$

Since $\phi(24) = \phi(3)\phi(8) = 2 \cdot 4$

Modulo 24 we have $5^2 \equiv 1$ and

$5^4 \equiv 5^6 \equiv 1$, $5^7 \equiv 5$, so $x \equiv 15 \pmod{24}$

$\phi(3) \Rightarrow (3,1) = 1$, 3,

Example: 2

Solve the congruence $25x \equiv 15 \pmod{120}$

Solution: Since $d = (25, 120) = 5$ and $d \mid 15$ the congruence has exactly five solutions modulo 120. To find them we divide by 5 and solve the congruence $5x \equiv 3 \pmod{24}$

Using theorem, $x = 15 + 24k$, $k = 0,1,2,3,4$ (or)

$x = 15, 39, 63, 87, 111 \pmod{120}$.

$5 \overline{)24}$ (4, 24, 4)

$(5,24) \Rightarrow$ $24 = 5 \times 4 + 4$

$5 = 4 \times 1 + 1$

$4 = 1 \times 4 + 0$

$1 = 5 - 4 \times 1$

$= 5 \cdot (24 - 5 \times 4)$

$= 5 \times 1 - 24 + 5 \times 4$

$1 = 5 \times 5 - 24$

Polynomial Congruences modulo p

Lagranges Theorem

Given a prime p, let $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial of degree n with integer co-efficients such that $c_n \not\equiv 0 \pmod p$

Then the polynomial congruence

$$f(x) \equiv 0 \pmod p. \quad \text{——} (1)$$

has at most n solutions.

Proof:

We use induction on n, the degree of f.

When $n=1$ the congruence is linear:

$$f(x) = c_1 x + c_0 \equiv \pmod p; \quad c_1 \not\equiv 0 \pmod p$$

$$(c_1, p) = 1 \qquad \Rightarrow p \nmid c_1 \Rightarrow (a, p) = 1$$

$\Rightarrow$ Linear congruence $c_1 x \equiv -c_0 \pmod p$ has a unique solution

Assume that the theorem is true for polynomials of degree $n-1$.

Assume also that the congruence (1) has $n+1$ incongruent solutions modulo p, say

$$x_0, x_1 \ldots x_n$$

Where $f(x_k) \equiv 0 \pmod p$ for each $k = 0, 1, \ldots, n$

We shall obtain a contradiction.

We have the algebraic identity,

$$f(x) - f(x_0) = \sum_{r=1}^{n} c_r (x^r - x_0^r) = (x - x_0) g(x)$$

Where $g(x)$ is a polynomial of degree $n-1$ with integer co-efficients and with leading co-efficient c_n. Thus we have

$$f(x_k) - f(x_0) = (x_k - x_0) g(x_k) \equiv 0 \pmod{p}$$

Since $f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}$.

But $x_k - x_0 \not\equiv 0 \pmod{p}$ if $k \neq 0$

So we must have $g(x_k) \equiv 0 \pmod{p}$ for each $k \neq 0$.

By this means that the congruence $g(x) \equiv 0 \pmod{p}$ has n incongruent solutions modulo p, contradicting our induction hypothesis.

This completes the proof.

Theorem:

For any prime p all the co-efficients of the polynomial $f(x) = (x-1)(x-2)\ldots(x-p+1) - x^{p-1} + 1$ are divisible by p.

Proof:

Let $g(x) = (x-1)(x-2)\cdots(x-p+1)$

The roots of g are the numbers $1, 2 \cdots p-1$, hence they satisfy the congruence

$$g(x) \equiv 0 \pmod{p}$$

By the Euler Fermat theorem,

these numbers also satisfy the congruence $h(x) \equiv 0 \pmod{p}$, where

$$h(x) = x^{p-1} - 1$$

The difference $f(x) = g(x) - h(x)$ has degree $p-2$ but the ~~difference~~ congruence $f(x) \equiv 0 \pmod{p}$ has $p-1$ solutions $1, 2 \cdots p-1$.

Therefore, by the theorem,

"If $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ is a polynomial of degree n with integer co-efficients, and if the congruence $f(x) \equiv 0 \pmod{p}$ has more than n solutions, where p is prime, then every co-efficient of f is divisibly by p."

∴ each co-efficient of $f(x)$ is divisible by p.

Simultaneous linear congruences:

The Chinese Remainder Theorem

When $m_1, m_2 \ldots m_k$ are pairwise relatively prime positive integers, the system of congruences

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

where $a_1, a_2 \ldots a_k$ are given integers, has a unique solution modulo m, where $m = m_1 \cdot m_2 \ldots m_k$.

Proof:

Let $M_i = \frac{m}{m_i}$ for $i = 1, 2, 3 \ldots k$

(ie) M_i is the product of moduli expect m_i.

Since m_i and m_j have no common factor other than 1, where $i \neq j$, we have

$$\gcd(m_i, M_i) = 1.$$

Hence by known theorem, the congruence $M_i x \equiv 1 \pmod{m_i}$ has a unique solution.

Let it be x_i, $i = 1, 2 \ldots k$

$$\therefore M_i x_i \equiv 1 \pmod{m_i}$$

$\therefore$ $a_i M_i x_i \equiv a_i \pmod{m_i}$, for $i = 1, 2 \ldots k$ — ①

Now $M_1 \equiv 0 \pmod{m_i}$, if $i \neq 1$

$\therefore a_1 M_1 x_1 \equiv 0 \pmod{m_i}$

Similarly $a_2 M_2 x_2 \equiv 0 \pmod{m_i}$

$\cdots\cdots\cdots$

$a_{i-1} M_{i-1} x_{i-1} \equiv 0 \pmod{m_i}$

$a_{i+1} M_{i+1} x_{i+1} \equiv 0 \pmod{m_i}$

$\cdots\cdots\cdots$

$a_k M_k x_k \equiv 0 \pmod{m_i}$ — ②

From ① and ② we get

$$a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k \equiv a_i \pmod{m_i}$$

(ii) $x = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k$ is a solution of the congruence

$$x \equiv a_i \pmod{m_i}; \quad i = 1, 2 \ldots k.$$

(iii) $x = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k$

Satisfies every congruence in the system.

But it is easy to show that the system has only one solution mod M.

In fact, if x and y are two solns. of the system we have $x \equiv y \pmod{m_k}$ for each k and since the m_k are relatively prime in pairs, also have $x \equiv y \pmod{M}$

Hence proved.

Example:

Let us consider the congruences $x \equiv 2 \pmod 3$ $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 7$.

Now $m = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$

$\therefore M_1 = 35$; $M_2 = 21$; $M_3 = 15$

Now the solution of $35x \equiv 1 \pmod 3$ is -1, the solution of $21x \equiv 1 \pmod 5$ is 1 and the soution of $15x \equiv 1 \pmod 7$ is 1.

(ie) Steps: (i) $M = m_1 m_2 m_3$

(ii) $M_1 = M/m_1$, $M_2 = M/m_2$ ....

(iii) $M_1^{-1} \bmod m_1$ ....

(iv) $x = (a_1 \times m_1 \times M_1^{-1} + a_2 \times m_2 \times M_2^{-1} + \dots)$

Step:1 $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

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

Step:2 $M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 7$

$= 105$

Step:3

$M_1 = M/m_1 = 105/3 = 35$

$M_2 = M/m_2 = 105/5 = 21$

$M_3 = M/m_3 = 105/7 = 15$

Step: 4

$M_1^{-1} \bmod m_1 = (35)^{-1} \bmod 3$

$= 35 \bmod 3$

$= 2$

$35 \div 3 = 11.6667$

$11 \times 3 = 33$

$35 - 33 = 2$

$M_2^{-1} \bmod m_2 = (21)^{-1} \bmod 5$

$= (21)^3 \bmod 5$

$= 9261 \bmod 5$

$= 1$

$\because a^{P-2}$

$a^{5-2} = 3$

$\frac{9261}{5} = 1852$

$1852 \times 5 = 9260$

$9261 - 9260 = 1$

$M_3^{-1} \bmod m_3 = (15)^{-1} \bmod 7$

$= 15^5 \bmod 7$

$= 759375 \bmod 7$

$= 1$

$\frac{759375}{7} = 108482$

$108482 \times 7 = 759374$

$x = (a_1 m_1 m_1^{-1} + a_2 m_2 m_2^{-1} + \ldots)$

$= (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) \pmod{105}$

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

$= 233 \bmod 105.$

$= 23$ //

$\frac{233}{105} = 2$

$2 \times 105 = 110$

$233 - 110 = 23$

① Solve the congruence $6x \equiv 5 \pmod 9$

Soln! Since $\gcd(6,9) \neq 1$, no solution exists for the congruence $6x \equiv 1 \pmod 9$

Hence no solution exists for $6x \equiv 5 \pmod{19}$

② Solve the congruence $9x \equiv 12 \pmod{21}$

Soln! We note that $\gcd(9, 21) = 3$

Also 3 divides 12.

$\frac{9x}{3} = \frac{12}{3} \pmod{\frac{21}{3}}$ i.e. $3x \equiv 4 \pmod 7$

∴ The equation has 3 incongruent solutions

Dividing the congruent relation, we get

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

Since $\gcd(3,7) = 1$, (1) has a unique soln. modulo 7

To solve Gnl. ② $3x \equiv 1 \pmod 7$.

Since $1 \times 7 - 2 \times 3 = 1$ $\quad 3m + 7n = 1$

$4 \times 7 - 8 \times 3 = 4$

(ie) $3 \times (-8) \equiv 4 \pmod 7$

(or) $3 \times 6 \equiv 4 \pmod 7$

[∵ $\gcd(3,7) = 1$,

$7 = 3 \times 2 + 1$ gcd

$3 = 1 \times 3 + 0$

$1 = 1 \times 7 - 3 \times 2$

$1 = ma + nb$

$m = 1$ & $n = -2$

$\gcd(4,7)$

$\Rightarrow 7 = 1 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0$

$1 = 1 \times 4 - 1 \times 3$

$= 1 \times 4 - 1 \times (1 \times 7 - 1 \times 4)$

$= 1 \times 4 - 1 \times 7 + 1 \times 4$

$= 2 \times 4 - 1 \times 7$

$m = 2$, $n = -1$

The solution of eqn ① is $x \equiv 6 \pmod 7$

But we want to find the solution of

$9x \equiv 12 \pmod{21}$

The required solutions are 6, 6+7, 6+(2×7)

(ie) $x = 6, 13, 20 \pmod{21}$

3. Find the smallest positive integer which leaves the remainder 1, 2, 3, 4 when divided by the prime nos 2, 3, 5, 11 respl.

Soln

$x \equiv 1 \pmod 2$
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod{11}$

$a_1 = 1, a_2 = 2, a_3 = 4, a_4 = 4$
$m_1 = 2, m_2 = 3, m_3 = 5$
$m_4 = 11$

Now, $m = m_1 m_2 m_3 m_4 = 2 \times 3 \times 5 \times 11 = 330$

$M_1 = \frac{m}{m_1} = 165$; $M_2 = \frac{m}{m_2} = 110$

$M_3 = \frac{m}{m_3} = 66$; $M_4 = \frac{m}{m_4} = 30$

$M_1^{-1} \bmod m_1 = (165)^{-1} \bmod 2$
$= 165 \bmod 2$
$= 1$

$M_2^{-1} \bmod m_2 = (110)^{-1} \bmod 3$
$= (110)^2 \bmod 3$
$= 12100 \bmod 3$
$= 1$

$a^{p-2} =$

82.5
$165 \div 2 = 165$
$165 \times 1 = 165$
$82 \times 2 = 164$

$a^{p-2} = a^{3-1} = a^2$

$12100 \div 3 = 4033.33$
$4033 \times 3 = 12099$

$M_3^{-1} \bmod m_3 = (66)^{-1} \bmod 5$

$= (66)^3 \bmod 5$

$= 287496 \bmod 5$

$= 1$

$a^{p-2} = a^{5-2} = 3$

$\frac{287496}{5} = 57499.2$

57499×5

287495

$M_4^{-1} \bmod m_4 = (30)^{-1} \bmod 11$

$= (30)^9 \bmod 11$

$= 1$

$a^{p-2} = a^{11-2} = 9$

1.78936×10^{12}

$\times 11$

$= 1.9683 \times 10^{13}$

The solutions of the above congruences are resp/. $1, -1, 1, -4$.

∴ The required soln/. of the system of congruences is

$x = [1 \times 165 \times 1 + 2 \times 110 \times (-1) + 3 \times 66 \times 1 + 4 \times 30 \times (-4)] \pmod{330}$

$= -337 \pmod{330}$

or $x = 323 \pmod{330}$

The required least positive integer $= 323$.