



MADURAI KAMARAJ UNIVERSITY

(University with Potential for Excellence)

DISTANCE EDUCATION



B.Sc. (Mathematics)

THIRD YEAR

UNIT: 6 - 10 (Volume -2)

Paper - V II

**DIFFERENTIAL EQUATIONS,
LAPLACE TRANSFORMS AND
NUMBER SYSTEM**

Recognised by D.E.C.

www.mkudde.org

\$ 88



MADURAI KAMARAJ UNIVERSITY

(University with Potential for Excellence)

DISTANCE EDUCATION



B.Sc. (Mathematics)

THIRD YEAR

UNIT: 6 - 10 (Volume -2)

Paper - V II

**DIFFERENTIAL EQUATIONS,
LAPLACE TRANSFORMS AND
NUMBER SYSTEM**

Recognised by D.E.C.

www.mkudde.org

S 88

© All Copyrights reserved



MADURAI KAMARAJ UNIVERSITY
(University with Potential for Excellence)
DISTANCE EDUCATION



B.Sc. (Mathematics)

THIRD YEAR

UNIT: 8 - 10 (Volume - 2)

Paper - V II

DIFFERENTIAL EQUATIONS,
LAPLACE TRANSFORMS AND
NUMBER SYSTEM

Recognised by D.E.C.

www.mkude.org

288

Printed at Gokul Agencies
Copies-1000 Year: 2014 Reprint

© All Copyrights reserved

B.Sc., Mathematics

Third Year

DIFFERENTIAL EQUATIONS,

LAPLACE TRANSFORMS AND

NUMBER SYSTEM

Major Paper - VII

Dear Student,

We welcome you as a Student of the Third year B.Sc degree Course in Mathematics.

This major paper – VII deals with Differential Equations, Laplace Transforms and Number system. The learning material for this paper will be supplemented by Contact seminars.

Learning through the Distance Education mode, as you are all aware, involves self – learning and self – assessment and in this regard you are expected to put in disciplined and dedicated effort.

On our part, we assume of our guidance and support.

With best wishes.

SYLLABUS

III YEAR – MAJOR – PAPER VII

DIFFERENTIAL EQUATIONS, LAPLACE TRANSFORMS AND NUMBER SYSTEM

UNIT – 6:

Solving ordinary differential equations with constant coefficients and variable coefficients – Simultaneous linear differential equations using Laplace Transforms

UNIT – 7:

Theory of numbers – Prime and composite number – The sieve of Eratosthenes – Divisors of a given number – simple problems

UNIT – 8:

Euler's function – Integral part of a real number – Simple problems – Numbers in Arithmetic progression – Fermat's theorem – Simple problems – Product of consecutive integers is divisible by $r!$

UNIT – 9:

Congruences – Criteria of divisibility of a number – Simple problems – Numbers in Arithmetic progression – Fermat's theorem – Simple problems.

UNIT – 10:

Generalization of Fermat's theorem – Wilson's theorem – Lagrange's theorem – Simple problems

Text Books:

1. Calculus volume III by T.K. Manicavachagom Pillay and S. Narayanan

Publications: S. Viswanathan.

2. Algebra Volume II: T.K. Manicavachagam Pillai and S. Narayanan.

Publications: S. Viswanathan.

CONTENTS

UNIT NO.	SCHEME OF LESSONS	PAGE NO.
Unit – 6	LAPLACE TRANSFORMS	1
6.1	Solving ordinary differential equations with constant coefficients	1
6.2	Solving ordinary differential equations with variable coefficients	10
6.3	Simultaneous linear differential equations	21
	NUMBER SYSTEM	
UNIT – 7	THEORY OF NUMBERS	34
7.0	Introduction	34
7.1	Prime and Composite numbers	34
7.2	The sieve of Erathosthenes	34
7.3	Divisors of a given number N	39
UNIT – 8	EULER'S FUNTION $\phi(N)$	43
8.1	Euler's Function $\phi(N)$	43
8.2	Integral part of a real number	49
8.3	The highest power of a prime p contained in n!	50

UNIT NO.	SCHEME OF LESSONS	PAGE NO.
8.4	The product of r consecutive integers is divisible by $r!$	52
UNIT – 9	CONGRUENCES	57
9.1	Congruences	57
9.2	Criteria of divisibility of a number	60
9.3	Numbers in arithmetical progression	67
9.4	Fermat's Theorem	72
UNIT – 10	GENERALIZATION OF FERMAT'S THEOREM	83
10.1	Generalization of Fermat's Theorem	83
10.2	Wilson's Theorem	85
10.3	Lagrange's Theorem	86

UNIT – 6

LAPLACE TRANSFORMS

6.1 Solving Differential Equations with constant coefficients using Laplace Transforms

Example: 1

Solve $\frac{d^2 y}{dt^2} + 4\frac{dy}{dt} - 5y = 5$ given that $y = 0$, $\frac{dy}{dt} = 2$ when $t = 0$.

Solution:

Given differential equation can be written as

$$y''(t) + 4y'(t) - 5y(t) = 5$$

Taking Laplace Transforms on both sides,

$$L[y''(t)] + 4L[y'(t)] - 5L[y(t)] = L[5]$$

$$s^2 L[y(t)] - sy(0) - y'(0) + 4\{sL[y(t)] - y(0)\} - 5L[y(t)] = L[5]$$

(1)

[$\therefore$ using formula]

$$\text{Given } y(0) = 0, \quad y'(0) = 2$$

(2)

Let us denote $L[y(t)] = \bar{y}$ (for convenience)

(3)

Substituting (2) and (3) in (1) we get,

Space for Hints

$$s^2 \bar{y} - 2 + 4(s\bar{y}) - 5\bar{y} = 5 \cdot \frac{1}{s}$$

$$s^2 \bar{y} + 4(s\bar{y}) - 5\bar{y} = 5 \cdot \frac{1}{s} + 2$$

$$\text{i.e.,} \quad (s^2 + 4s - 5)\bar{y} = \frac{5}{s} + 2$$

$$\bar{y} = \frac{\frac{5}{s} + 2}{(s^2 + 4s - 5)} = \frac{5 + 2s}{s(s^2 + 4s - 5)}$$

$$\text{Now,} \quad \frac{2s + 5}{s(s^2 + 4s - 5)} = \frac{A}{s} + \frac{Bs + C}{s^2 + 4s - 5}$$

$$2s + 5 = A(s^2 + 4s - 5) + (Bs + C)s$$

$$\text{Putting } s = 0, \quad -5A = 5 \quad A = -1$$

$$\text{Equating coefficient of } s^2, A + B = 0 \quad \text{i.e.,} \quad B = -A$$

$$\text{i.e.,} \quad B = 1$$

$$\text{Equating coefficient of } s, 4A + C = 2 \quad \text{i.e.,} \quad C = 2 - 4A$$

$$= 2 + 4$$

$$\text{i.e.,} \quad C = 6$$

$$\frac{2s + 5}{s(s^2 + 4s - 5)} = \frac{-1}{s} + \frac{s + 6}{s^2 + 4s - 5}$$

$$\text{i.e.,} \quad \bar{y} = \frac{-1}{s} + \frac{s + 6}{s^2 + 4s - 5}$$

$$\text{i.e.,} \quad L[y(t)] = \frac{-1}{s} + \frac{s + 6}{s^2 + 4s - 5}$$

$$y(t) = L^{-1} \left[\frac{-1}{s} + \frac{s+6}{s^2+4s-5} \right]$$

$$= L^{-1} \left[\frac{-1}{s} \right] + L^{-1} \left[\frac{s+6}{s^2+4s-5} \right]$$

$$= -1 + L^{-1} \left[\frac{s+2+4}{(s+2)^2-9} \right]$$

$$= -1 + L^{-1} \left[\frac{s+2}{(s+2)^2-3^2} \right] + 4L^{-1} \left[\frac{1}{(s+2)^2-3^2} \right]$$

$$= -1 + e^{-2t} L^{-1} \left[\frac{s}{s^2-3^2} \right] + 4e^{-2t} L^{-1} \left[\frac{1}{s^2-3^2} \right]$$

$$= -1 + e^{-2t} \cosh 3t + 4e^{-2t} \frac{\sinh 3t}{3}$$

Example: 2

Solve $y''-3y'+2y=e^{2t}$, $y(0)=-3$, $y'(0)=5$.

Solution:

Given $y''-3y'+2y=e^{2t}$

Taking Laplace Transforms on both sides,

$$L[y'']-3L[y']+2L[y]=L[e^{2t}]$$

$$s^2L[y(t)]-sy(0)-y'(0)-3\{sL[y(t)]-y(0)\}+2L[y(t)]$$

$$= L[e^{2t}] \quad (A)$$

Substituting $y(0)=-3$, $y'(0)=5$ in (A) and putting

$L[y(t)] = \bar{y}$, we get,

Space for Hints

$$s^2 \bar{y} + 3s - 5 - -3[s\bar{y} + +3] + 2\bar{y} = \frac{1}{s-2}$$

i.e.,

$$\bar{y}(s^2 - 3s + 2) + 3s - 14 = \frac{1}{s-2}$$

$$\bar{y}(s^2 - 3s + 2) = \frac{1}{s-2} - 3s + 14$$

$$= \frac{1 - 3s(s-2) + 14(s-2)}{s-2}$$

$$= \frac{-3s^2 + 20s - 27}{s-2}$$

$$\therefore \bar{y} = \frac{-3s^2 + 20s - 27}{(s-2)(s^2 - 3s + 2)}$$

i.e.,

$$L[y(t)] = \frac{-3s^2 + 20s - 27}{(s-2)(s-1)(s-2)}$$

$$y(t) = L^{-1} \left[\frac{-3s^2 + 20s - 27}{(s-1)(s-2)^2} \right]$$

$$\text{Now, } \frac{-3s^2 + 20s - 27}{(s-1)(s-2)^2} = \frac{A}{s-1} + \frac{B}{s-2} + \frac{C}{(s-2)^2}$$

$$\text{i.e., } -3s^2 + 20s - 27 = A(s-2)^2 + B(s-1)(s-2) + C(s-1)$$

$$\text{Putting } s = 1, \quad A = -10$$

$$\text{Putting } s = 2, \quad C = 1$$

$$\text{Equating coefficient of } s^2, \quad A + B = -3$$

$$-10 + B = -3$$

$$B = 7$$

$$\therefore \frac{-3s^2 + 20s - 27}{(s-1)(s-2)^2} = \frac{-10}{s-1} + \frac{7}{s-2} + \frac{1}{(s-2)^2}$$

$$\mathcal{L}^{-1}\left[\frac{-3s^2 + 20s - 27}{(s-1)(s-2)^2}\right] = -10\mathcal{L}^{-1}\left[\frac{1}{s-1}\right] + 7\mathcal{L}^{-1}\left[\frac{1}{s-2}\right] + \mathcal{L}^{-1}\left[\frac{1}{(s-2)^2}\right]$$

$$= -10e^t + 7e^{2t} + e^{2t}\mathcal{L}^{-1}\left[\frac{1}{s^2}\right]$$

$$= -10e^t + 7e^{2t} + t.e^{2t}$$

Example: 3

Solve $y'' + 2y' - 3y = \sin t$ given, $y = 0, y'(0) = 0$ when $t = 0$.

Solution:

$$\text{Given } y''(t) + 2y'(t) - 3y(t) = \sin t$$

Taking Laplace Transforms on both sides we get,

$$\mathcal{L}[y''(t)] + \mathcal{L}[2y'(t)] - \mathcal{L}[3y(t)] = \mathcal{L}[\sin t]$$

$$s^2\mathcal{L}[y(t)] - sy(0) - y'(0) + 2\{s\mathcal{L}[y(t)] - y(0)\} - 3\mathcal{L}[y(t)] = \frac{1}{s^2 + 1}$$

Putting $y(0) = 0, y'(0) = 0$ and $\mathcal{L}[y(t)] = \bar{y}$, we get,

$$s^2\bar{y} + 2s\bar{y} - 3\bar{y} = \frac{1}{s^2 + 1}$$

$$\bar{y}(s^2 + 2s - 3) = \frac{1}{s^2 + 1}$$

$$\bar{y} = \frac{1}{(s^2 + 2s - 3)(s^2 + 1)}$$

Space for Hints

$$L[y(t)] = \left[\frac{1}{(s-1)(s+3)(s^2+1)} \right]$$

$$\text{i.e., } y(t) = L^{-1} \left[\frac{1}{(s-1)(s+3)(s^2+1)} \right] \quad (1)$$

$$\text{Now, } \frac{1}{(s-1)(s+3)(s^2+1)}$$

$$= \frac{A}{s-1} + \frac{B}{s+3} + \frac{Cs+D}{s^2+1}$$

$$1 = A(s+3)(s^2+1) + B(s-1)(s^2+1) + (Cs+D)(s-1)(s+3)$$

$$\text{Putting } s = 1, \quad 8A = 1 \quad \Rightarrow \quad A = \frac{1}{8}$$

$$\text{Putting } s = -3 \quad -40B = 1 \quad \Rightarrow \quad B = \frac{-1}{40}$$

$$\text{Equating coefficient of } s^3, \quad A + B + C = 0$$

$$C = -A - B$$

$$= -\frac{1}{8} + \frac{1}{40} = \frac{-1}{10}$$

$$C = \frac{-1}{10}$$

Equating constant coefficients,

$$3A - B - 3D = 1$$

$$\frac{3}{8} + \frac{1}{40} - 3D = 1$$

$$3D = \frac{3}{8} + \frac{1}{40} - 1$$

$$= \frac{15 + 1 - 40}{40}$$

$$= \frac{-24}{40} = \frac{-3}{5}$$

$$D = \frac{-1}{5}$$

$$\therefore \frac{1}{(s-1)(s+3)(s^2+1)} = \frac{\frac{1}{8}}{s-1} + \frac{\frac{-1}{40}}{s+3} + \frac{\frac{-1}{10}s - \frac{1}{5}}{s^2+1}$$

$$L^{-1} \left[\frac{1}{(s-1)(s+3)(s^2+1)} \right]$$

$$= \frac{1}{8} L^{-1} \left[\frac{1}{s-1} \right] - \frac{1}{40} L^{-1} \left[\frac{1}{s+3} \right] - \frac{1}{10} L^{-1} \left[\frac{s+2}{s^2+1} \right]$$

$$= \frac{1}{8} e^t - \frac{1}{40} e^{-3t} - \frac{1}{10} \left\{ L^{-1} \left[\frac{s}{s^2+1} \right] + L^{-1} \left[\frac{2}{s^2+1} \right] \right\}$$

$$= \frac{1}{8} e^t - \frac{1}{40} e^{-3t} - \frac{1}{10} [\cos t + 2 \sin t]$$

Example: 4

Solve $y''' - 3y'' + 3y' - y = t^2 e^t$, $y(0) = 1$, $y'(0) = 0$, $y''(0) = -2$

Solution:

Taking Laplace Transforms on both sides, we get,

$$L[y'''](t) - 3L[y''(t)] + 3L[y'(t)] - L[y(t)] = L[t^2 e^t]$$

Space for Hints

$$[s^3 L(y(t)) - s^2 y(0) - sy'(0) - y''(0)] - 3\{s^2 L[y(t)] - sy(0) - y'(0)\}$$

$$+ 3\{sL(y(t)) - y(0)\} - L[y(t)] = \frac{2}{(s-1)^3}$$

Putting $L[y(t)] = \bar{y}$, $y(0) = 1$, $y'(0) = 0$, $y''(0) = -2$, we get

$$(s^3 \bar{y} - s^2 + 2) - 3(s^2 \bar{y} - s) + 3(s\bar{y} - 1) - \bar{y} = \frac{2}{(s-1)^3}$$

$$\bar{y}(s^3 - 3s^2 + 3s - 1) - s^2 + 3s - 1 = \frac{2}{(s-1)^3}$$

$$\bar{y}(s-1)^3 = \frac{2}{(s-1)^3} + s^2 - 3s + 1$$

$$\bar{y} = \frac{2}{(s-1)^6} + \frac{s^2 - 3s + 1}{(s-1)^3}$$

$$= \frac{2}{(s-1)^6} + \frac{(s-1)^2}{(s-1)^3} - \frac{s}{(s-1)^3}$$

$$= \frac{2}{(s-1)^6} + \frac{1}{s-1} - \frac{s-1+1}{(s-1)^3}$$

$$L[y(t)] = \frac{2}{(s-1)^6} + \frac{1}{s-1} - \frac{1}{(s-1)^2} - \frac{1}{(s-1)^3}$$

$$y(t) = L^{-1} \left[\frac{2}{(s-1)^6} + \frac{1}{s-1} - \frac{1}{(s-1)^2} - \frac{1}{(s-1)^3} \right]$$

$$= \frac{t^5 e^t}{60} + e^t - te^t - \frac{t^2 e^t}{2}$$

Example: 5

Show the solution of the differential equation

$$\frac{d^2 y}{dt^2} + 4y = A \sin kt \text{ which is such that } y = 0 \text{ and } \frac{dy}{dt} = 0 \text{ when } t = 0$$

is

$$y = A \frac{\sin kt - \frac{k}{2} \sin 2t}{4 - k^2} \text{ if } k \neq 2.$$

$$\text{If } k = 2, \text{ show that } y = \frac{A(\sin 2t - 2t \cos 2t)}{8}$$

Solution:

$$y'' + 4y = A \sin kt$$

$$L(y'') + 4L(y) = AL(\sin kt)$$

$$s^2 \bar{y} - sy(0) - y'(0) + 4\bar{y} = A \frac{k}{s^2 + k^2}, \text{ where } L(y) = \bar{y}.$$

Since $y(0) = 0, y'(0) = 0$, we have

$$(s^2 + 4)\bar{y} = A \frac{k}{s^2 + k^2}.$$

$$\therefore \bar{y} = A \frac{k}{(s^2 + 4)(s^2 + k^2)}$$

$$\therefore y = AkL^{-1} \frac{1}{(s^2 + 4)(s^2 + k^2)}$$

Case: i

If $k \neq 2$,

$$y = AkL^{-1} \left(\frac{\frac{1}{s^2 + 4} - \frac{1}{s^2 + k^2}}{(k^2 - 4)} \right)$$

$$= \frac{Ak}{k^2 - 4} \left\{ L^{-1} \frac{1}{s^2 + 4} - L^{-1} \frac{1}{s^2 + k^2} \right\}$$

$$= \frac{Ak}{k^2 - 4} \left\{ \frac{\sin 2t}{2} - \frac{\sin kt}{k} \right\}$$

$$= \frac{A}{4 - k^2} \left(\sin kt - \frac{k}{2} \sin 2t \right)$$

Case: ii

$k = 2$, Then

$$\bar{y} = 2AL^{-1} \left\{ \frac{1}{(s^2 + 4)(s^2 + 4)} \right\}$$

$$= 2AL^{-1} \left\{ \frac{1}{(s^2 + 2^2)^2} \right\}$$

$$= 2A \cdot \frac{1}{2(2)^3} (\sin 2t - 2t \cos 2t)$$

$$= \frac{A}{8} (\sin 2t - 2t \cos 2t).$$

6.2 Solving ordinary differential equations with variable coefficients using Laplace Transforms

Introduction

We have shown that

$$L\{tf(t)\} = -\frac{d}{ds} L\{f(t)\}$$

$$\text{And } L\{t^2 f(t)\} = (-1)^2 \frac{d^2}{ds^2} L\{f(t)\}.$$

These results are used to solve equations containing variable

coefficients.

Space for Hints

Example: 1

Solve the equation

$$t \frac{d^2 y}{dt^2} - (2+t) \frac{dy}{dt} + 3y = t-1 \text{ when } y(0) = 0.$$

Solution

Taking Laplace transforms on both sides, we have

$$L(ty'') - L\{(2+t)y'\} + 3L(y) = L(t-1) \quad \text{i.e.,}$$

$$-\frac{d}{ds} \{s^2 L(y) - sy(0) - y'(0)\} - 2\{sL(y) - y(0)\} + \frac{d}{ds} \{sL(y) - y(0)\} + 3L(y) = \frac{1}{s^2} - \frac{1}{s}$$

Let $L(y)$ be $\bar{y}$.

Putting $y(0) = 0$,

$$-\frac{d}{ds} \{s^2 \bar{y} - y'(0)\} - 2(s\bar{y}) + \frac{d}{ds} (s\bar{y}) + 3\bar{y} = \frac{1-s}{s^2}$$

$$\text{i.e., } -s^2 \frac{d\bar{y}}{ds} - 2s\bar{y} - 2s\bar{y} + s \frac{d\bar{y}}{ds} + \bar{y} + 3\bar{y} = \frac{1-s}{s^2}$$

$$\text{i.e., } -(s^2 - s) \frac{d\bar{y}}{ds} - 4(s-1)\bar{y} = -\frac{s-1}{s^2}$$

$$\text{i.e., } \frac{d\bar{y}}{ds} + \frac{4\bar{y}}{s} = \frac{1}{s^3}$$

$$\text{Solving this equation, } \bar{y} = \frac{1}{2} \cdot \frac{1}{s^2} + \frac{c}{s^4}.$$

$$= \frac{t}{2} + \frac{ct^3}{6}.$$

Hence $y = \frac{t}{2} + At^3$, where A is an arbitrary constant.

Space for Hints

Example: 2

Solve the equation.

$$\frac{d^2y}{dt^2} + t \frac{dy}{dt} - y = 0 \text{ if } y(0) = 0 \text{ and } y'(0) = 1.$$

Solution

Taking Laplace transforms on both sides, we have

$$L(y'') + L(ty') - L(y) = 0$$

$$\text{i.e., } s^2L(y) - sy(0) - y'(0) - \frac{d}{ds}\{sL(y) - y(0)\} - L(y) = 0$$

$$y(0) = 0, y'(0) = 1.$$

$$\text{Putting } L(y) = \bar{y}, \text{ we get } s^2\bar{y} - 1 - \frac{d}{ds}(s\bar{y}) - \bar{y} = 0$$

$$\text{i.e., } s^2\bar{y} - 1 - s \frac{d\bar{y}}{ds} - \bar{y} = 0$$

$$\text{i.e., } s \frac{d\bar{y}}{ds} - (s^2 - 2)\bar{y} + 1 = 0$$

$$\text{Solving this equation } \bar{y}s^2e^{-s^2/2} = e^{-s^2/2} + c.$$

$$\therefore \bar{y} = \frac{1}{s^2} + c \frac{e^{s^2/2}}{s^2}.$$

$\bar{y}$ is a Laplace transform.

$$\therefore \lim_{s \rightarrow \infty} \bar{y} = 0, \therefore c = 0.$$

$$\text{Hence } \bar{y} = \frac{1}{s^2}$$

Taking inverse transform $y = t$.

Note:

Certain equations involving integrals can also be solved by Laplace transform

Example: 3

Determine y which satisfies the equation

$$\frac{dy}{dt} + 3y + 2 \int_0^t y dt = t \text{ for which } y(0) = 0.$$

Taking Laplace transforms on both sides, we get

$$L(y') + 3L(y) + 2L\left(\int_0^t y dt\right) = L(t)$$

$$\text{i.e., } sL(y) - y(0) + 3L(y) + \frac{2}{s}L(y) = \frac{1}{s^2}$$

Putting $L(y) = \bar{y}$ and substituting $y(0) = 0$, we have

$$s\bar{y} + 3\bar{y} + \frac{2}{s}\bar{y} = \frac{1}{s^2}$$

$$\text{i.e., } \bar{y}\left(s + 3 + \frac{2}{s}\right) = \frac{1}{s^2}$$

$$\text{i.e., } \bar{y}\left(s + 3 + \frac{2}{s}\right) = \frac{1}{s^2}$$

$$\therefore \bar{y} = \frac{1}{s(s+1)(s+2)}$$

Space for Hints

Space for Hints

$$\therefore \bar{y} = \frac{1}{s(s+1)(s+2)}$$

$$\therefore \bar{y} = L^{-1} \left\{ \frac{1}{s(s+1)(s+2)} \right\}$$

$$y = L^{-1} \left\{ \frac{1}{2} \cdot \frac{1}{s} - \frac{1}{s+1} + \frac{1}{2} \cdot \frac{1}{s+2} \right\}$$

$$= \frac{1}{2} L^{-1} \left(\frac{1}{s} \right) - L^{-1} \left(\frac{1}{s+1} \right) + \frac{1}{2} L^{-1} \left(\frac{1}{s+2} \right)$$

$$= \frac{1}{2} - e^{-t} + \frac{1}{2} e^{-2t}$$

Example: 4

Find y which satisfies the equation

$$\frac{dy}{dt} + 4y + 5 \int_0^t y dt = e^{-t}, \text{ when } y(0) = 0.$$

Solution:

Given equation is

$$y'(t) + 4y(t) + 5 \int_0^t y(t) dt = e^{-t}$$

Taking Laplace Transforms on both sides, we get,

$$L[y'(t) + 4L[y(t)] + 5L[\int_0^t y(t) dt] = L[e^{-t}]$$

$$sL[y(t)] - y(0) + 4L[y(t)] + 5 \cdot \frac{1}{s} L[y(t)] = \frac{1}{s+1}$$

$$\left[\because L \left\{ \int_0^t y(t) dt \right\} = \frac{1}{s} L[y(t)] \right]$$

Putting $L[y(t)] = \bar{y}$, $y(0) = 0$, we get,

$$s\bar{y} + 4\bar{y} + \frac{5}{s}\bar{y} = \frac{1}{s+1}$$

$$\bar{y}\left(s + 4 + \frac{5}{s}\right) = \frac{1}{s+1}$$

$$\bar{y}\left(\frac{s^2 + 4s + 5}{s}\right) = \frac{1}{s+1}$$

$$\bar{y} = \frac{s}{(s+1)(s^2 + 4s + 5)}$$

$$L[y(t)] = \frac{s}{(s+1)(s^2 + 4s + 5)}$$

$$y(t) = L^{-1}\left[\frac{s}{(s+1)(s^2 + 4s + 5)}\right]$$

$$\frac{s}{(s+1)(s^2 + 4s + 5)} = \frac{A}{s+1} + \frac{Bs + C}{s^2 + 4s + 5}$$

$$s = A(s^2 + 4s + 5) + (s+1)(Bs + C)$$

$$\text{Putting } s = -1, \quad 2A = -1 \quad \Rightarrow \quad A = -\frac{1}{2}$$

$$\text{Putting } s = 0, \quad 5A + C = 0 \quad \Rightarrow \quad C = \frac{5}{2}$$

$$\text{Equating coeff. of } s^2, A + B = 0 \quad \Rightarrow \quad B = \frac{1}{2}$$

$$\frac{s}{(s+1)(s^2 + 4s + 5)} = \frac{-\frac{1}{2}}{s+1} + \frac{\frac{1}{2}s + \frac{5}{2}}{s^2 + 4s + 5}$$

Space for Hints

$$\begin{aligned}\therefore L^{-1}\left[\frac{s}{(s+1)(s^2+4s+5)}\right] \\&= -\frac{1}{2}L^{-1}\left[\frac{1}{s+1}\right] + \frac{1}{2}L^{-1}\left[\frac{s+5}{(s+2)^2+1}\right] \\&= -\frac{1}{2}e^{-t} + \frac{1}{2}L^{-1}\left[\frac{s+2+3}{(s+2)^2+1}\right] \\&= -\frac{1}{2}e^{-t} + \frac{1}{2}\left\{L^{-1}\left[\frac{s+2}{(s+2)^2+1}\right] + L^{-1}\left[\frac{3}{(s+2)^2+1}\right]\right\} \\&= -\frac{1}{2}e^{-t} + \frac{1}{2}e^{-2t}\cos t + \frac{3}{2}e^{-2t}\sin t\end{aligned}$$

Example: 5

Determine y which satisfies the equation

$$\frac{dy}{dt} + 2y + \int_0^t y dt = 2 \cos t, y(0) = 1.$$

Solution:

Given equation can be written as

$$y'(t) + 2y(t) + \int_0^t y(t) dt = 2 \cos t$$

Taking Laplace Transforms on both sides, we get,

$$L[y'(t)] + 2L[y(t)] + L\left[\int_0^t y(t) dt\right] = L[2 \cos t]$$

$$\Rightarrow sL[y(t) - y(0)] + 2L[y(t)] + \frac{1}{s}L[y(t)] = 2 \cdot \frac{s}{s^2 + 1}$$

Putting $L[y(t)] = \bar{y}$, $y(0) = 1$, we get,

$$s\bar{y} - 1 + 2\bar{y} + \frac{1}{s}\bar{y} = 2 \cdot \frac{s}{s^2 + 1}$$

$$\bar{y}\left(s + 2 + \frac{1}{s}\right) = \frac{2s}{s^2 + 1} + 1 = \frac{s^2 + 2s + 1}{s^2 + 1}$$

$$\bar{y} = \frac{s(s^2 + 2s + 1)}{(s^2 + 1)(s^2 + 2s + 1)}$$

$$L[y(t)] = \frac{s}{s^2 + 1}$$

$$y(t) = L^{-1}\left[\frac{s}{s^2 + 1}\right] = \cos t$$

Example: 6

Solve $\frac{dy}{dt} + 3y + 2 \int_0^t y dt = t$ for which $y(0) = 0$.

Solution:

Given equation can be written as

$$y'(t) + 3y(t) + 2 \int_0^t y(t) dt = t$$

Taking Laplace Transforms on both sides, we get,

$$L[y'(t)] + 3L[y(t)] + 2L\left[\int_0^t y(t) dt\right] = L[t]$$

$$sL[y(t)] - y(0) + 3L[y(t)] + 2\frac{1}{s}L[y(t)] = \frac{1}{s^2}$$

Putting $L[y(t)] = \bar{y}$ and $y(0) = 0$, we get,

Space for Hints

$$s\bar{y} + 3\bar{y} + 2 \cdot \frac{1}{s} \bar{y} = \frac{1}{s^2}$$

$$\bar{y} \left(s + 3 + \frac{2}{s} \right) = \frac{1}{s^2}$$

$$\bar{y} \left(\frac{s^2 + 3s + 2}{s} \right) = \frac{1}{s^2}$$

$$\bar{y} = \frac{1}{s(s^2 + 3s + 2)}$$

$$L[y(t)] = \frac{1}{s(s^2 + 3s + 2)}$$

$$y(t) = L^{-1} \left[\frac{1}{s(s^2 + 3s + 2)} \right]$$

Now,
$$\frac{1}{s(s^2 + 3s + 2)} = \frac{A}{s} + \frac{Bs + C}{s^2 + 3s + 2}$$

$$1 = A(s^2 + 3s + 2) + (Bs + C)s$$

Put $s = 0$,

$$2A = 1,$$

$$A = \frac{1}{2}$$

Equating Coeff. of s^2 ,

$$A + B = 0$$

$$\Rightarrow B = -\frac{1}{2}$$

Equating Coeff. of s ,

$$3A + C = 0$$

$$\Rightarrow C = -3A$$

i.e., $C = -\frac{3}{2}$

$$\therefore \frac{1}{s(s^2 + 3s + 2)} = \frac{\frac{1}{2}}{s} + \frac{-\frac{1}{2}s - \frac{3}{2}}{s^2 + 3s + 2}$$

$$\begin{aligned}
 \mathcal{L}^{-1}\left[\frac{1}{s(s^2 + 3s + 2)}\right] &= \frac{1}{2}\mathcal{L}^{-1}\left[\frac{1}{s}\right] - \frac{1}{2}\mathcal{L}^{-1}\left[\frac{s+3}{s^2 + 3s + 2}\right] \\
 &= \frac{1}{2} - \frac{1}{2}\mathcal{L}^{-1}\left[\frac{s + \frac{3}{2} + \frac{3}{2}}{\left(s + \frac{3}{2}\right)^2 - \frac{1}{4}}\right] \\
 &= \frac{1}{2} - \frac{1}{2}\mathcal{L}^{-1}\left[\frac{s + \frac{3}{2}}{\left(s + \frac{3}{2}\right)^2 - \left(\frac{1}{2}\right)^2}\right] - \frac{1}{2}\mathcal{L}^{-1}\left[\frac{\frac{3}{2}}{\left(s + \frac{3}{2}\right)^2 - \left(\frac{1}{2}\right)^2}\right] \\
 &= \frac{1}{2} - \frac{1}{2}e^{\frac{-3}{2}t}\mathcal{L}^{-1}\left[\frac{s}{s^2 - \left(\frac{1}{2}\right)^2}\right] - \frac{3}{2}e^{\frac{-3}{2}t}\mathcal{L}^{-1}\left[\frac{\frac{1}{2}}{s^2 - \left(\frac{1}{2}\right)^2}\right] \\
 &= \frac{1}{2} - \frac{1}{2}e^{\frac{-3}{2}t}\cosh\left(\frac{t}{2}\right) - \frac{3}{2}e^{\frac{-3}{2}t}\sinh\frac{1}{2}t
 \end{aligned}$$

Example: 7

Solve by Laplace transform method

$$\frac{dy}{dt} - 2y + \int_0^t y(t)dt = 0 \text{ given that } y(0) = 1.$$

Solution:

$$y' - 2y + \int_0^t y(t)dt = 0$$

$$\mathcal{L}(y') - 2\mathcal{L}(y) + \mathcal{L}\left[\int_0^t y(t)dt\right] = 0$$

Space for Hints

$$sL(y) - y(0) - 2L(y) + \frac{1}{s}L(y) = 0$$

$$sL(y) - 1 - 2L(y) + \frac{1}{s}L(y) = 0$$

$$L(y) \left(s - 2 + \frac{1}{s} \right) = 1$$

$$L(y) \left(\frac{s^2 - 2s + 1}{s} \right) = 1$$

$$L(y) = \frac{s}{s^2 - 2s + 1}$$

$$y = L^{-1} \left(\frac{s}{(s-1)^2} \right)$$

$$= L^{-1} \left(\frac{s-1+1}{(s-1)^2} \right)$$

$$= L^{-1} \left(\frac{1}{s-1} + \frac{1}{(s-1)^2} \right)$$

$$= e^t \left[L^{-1} \left(\frac{1}{s} + \frac{1}{s^2} \right) \right]$$

$$y = e^t [1 + t]$$

Example: 8

Using Laplace transform solve the equation

$$x + \int_0^t x dt = 1 - e^{-t}$$

Solution:

$$x + \int_0^t x dt = 1 - e^{-t}$$

$$L(x) + L\left[\int_0^t x dt\right] = L(1) - L(e^{-t})$$

$$L(x) + \frac{1}{s}L(x) = \frac{1}{s} - \frac{1}{s+1} = \frac{1}{s(s+1)}$$

$$L(x)\left(1 + \frac{1}{s}\right) = \frac{1}{s(s+1)}$$

$$L(x)\left(\frac{s+1}{s}\right) = \frac{1}{s(s+1)}$$

$$L(x) = \frac{1}{(s+1)^2}$$

$$x = L^{-1}\left(\frac{1}{(s+1)^2}\right)$$

$$x = te^{-t}$$

6.3 Simultaneous Linear Differential Equations

Example: 1

$$\text{Solve } \frac{dx}{dt} - 2x + 3y = 0; \frac{dy}{dt} - y + 2x = 0 \text{ with } x(0) = 8, y(0) = 3$$

Solution:

The given differential equation can be written as

$$x' - 2x + 3y = 0$$

$$y' - y + 2x = 0$$

Taking Laplace Transforms we get,

$$\begin{aligned} L[x'(t)] - 2L[x] + 3L[y] &= 0 \\ L[y'(t)] - 2L[y] + 2L[x] &= 0 \\ \frac{L[y'(t)] - 2L[y] + 2L[x]}{sL[x] - x[0] - 2L[x] + 3L[y]} &= 0 \\ sL[y] - y[0] - L[y] + 2L[x] &= 0 \end{aligned}$$

Putting $L[x] = \bar{x}$, $L[y] = \bar{y}$, $x[0] = 8$, $y[0] = 3$, we get

$$s\bar{x} - 8 - 2\bar{x} + 3\bar{y} = 0$$

$$s\bar{y} - 3 - \bar{y} + 2\bar{x} = 0$$

$$(s-2)\bar{x} + 3\bar{y} = 8 \quad (1)$$

$$2\bar{x} + (s-1)\bar{y} = 3 \quad (2)$$

Solving (1) and (2) we get,

$$\begin{aligned} \bar{x} &= \frac{\begin{vmatrix} 8 & 3 \\ 3 & s-1 \end{vmatrix}}{\begin{vmatrix} s-2 & 3 \\ 2 & s-1 \end{vmatrix}} = \frac{8s-17}{s^2-3s-4} = \frac{8s-17}{(s+1)(s-4)} \\ &= \frac{8s-17}{(s+1)(s-4)} \quad (3) \end{aligned}$$

$$\bar{y} = \frac{\begin{vmatrix} s-2 & 8 \\ 2 & 3 \end{vmatrix}}{\begin{vmatrix} s-2 & 3 \\ 2 & s-1 \end{vmatrix}} = \frac{3s-22}{s^2-3s-4} = \frac{3s-22}{(s+1)(s-4)} \quad (4)$$

From (3) we get,

$$L[x(t)] = \frac{8s-17}{(s+1)(s-4)} = \frac{5}{s+1} + \frac{3}{s-4}$$

$$x(t) = L^{-1} \left[\frac{5}{s+1} + \frac{3}{s-4} \right]$$

$$= 5e^{-t} + 3e^{4t}$$

From (4) we get

$$L[y(t)] = \frac{3s - 22}{(s+1)(s-4)} = \frac{5}{s+1} - \frac{2}{s-4}$$

$$y(t) = L^{-1}\left[\frac{5}{s+1} - \frac{2}{s-4}\right]$$

$$= 5e^{-t} - 2e^{4t}$$

$$\therefore x = 5e^{-t} + 3e^{4t}$$

$$y = 5e^{-t} - 2e^{4t}$$

Note:

If the simultaneous equations are

$$a_1x + b_1y = c_1$$

$$a_2x + b_2y = c_2$$

Then, after solving, we get,

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} \quad y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}$$

Example: 2

Solve $\frac{dx}{dt} + y = \sin t$; $\frac{dy}{dt} + x = \cos t$ with $x = 2$ and $y = 0$

when $t = 0$.

Space for Hints

Solution:

The given differential equation can be written as

$$x'(t) + y(t) = \sin t$$

$$y'(t) + x(t) = \cos t$$

Taking Laplace Transforms on both sides we get,

$$L[x'(t)] + L[y(t)] = L[\sin t]$$

$$L[y'(t) + L[x(t)] = L[\cos t]$$

$$sL[x(t)] - x(0) + L[y(t)] = \frac{1}{s^2 + 1}$$

$$sL[y(t)] - y(0) + L[x(t)] = \frac{s}{s^2 + 1}$$

Putting $x(0) = 2, y(0) = 0$ and $L[x(t)] = \bar{x}, L[y(t)] = \bar{y}$, we get

$$s\bar{x} - 2 + \bar{y} = \frac{1}{s^2 + 1}$$

$$s\bar{y} + \bar{x} = \frac{s}{s^2 + 1}$$

$$s\bar{x} + \bar{y} = \frac{1}{s^2 + 1} + 2 \quad (1)$$

$$\bar{x} + s\bar{y} = \frac{s}{s^2 + 1} \quad (2)$$

Solving (1) and (2) simultaneously we get

Example: 3

$$\bar{x} = \frac{\begin{vmatrix} \frac{1}{s^2+1} + 2 & 1 \\ s & s \end{vmatrix}}{\begin{vmatrix} s & 1 \\ 1 & s \end{vmatrix}}$$

$$= \frac{s \left(2 + \frac{1}{s^2+1} \right) - \frac{s}{s^2+1}}{s^2-1}$$

$$= \frac{s[2(s^2+1)+1]-s}{(s^2+1)(s^2-1)}$$

$$= \frac{s(2s^2+2)}{(s^2+1)(s+1)(s-1)} = \frac{2s}{s^2-1}$$

$$L[x(t)] = 2 \frac{s}{s^2-1}$$

$$x(t) = 2L^{-1} \left[\frac{s}{s^2-1} \right]$$

$$x(t) = 2 \cosh t$$

$$\bar{y} = \frac{\begin{vmatrix} s & \frac{1}{s^2+1} + 2 \\ 1 & \frac{s}{s^2+1} \end{vmatrix}}{\begin{vmatrix} s & 1 \\ 1 & s \end{vmatrix}}$$

$$= \frac{\frac{s^2}{s^2+1} - \frac{1}{s^2+1} - 2}{s^2-1}$$

$$= \frac{s^2-1-2(s^2+1)}{(s^2+1)(s^2-1)} = \frac{-3-s^2}{(s^2+1)(s^2-1)}$$

Solving (1) and (2) simultaneously we get

$$= \frac{s^2 + 3}{(s^2 + 1)(1 - s^2)}$$

i.e., $L[y(t)] = \frac{s^2 + 3}{(s^2 + 1)(1 - s^2)}$

$$y(t) = L^{-1} \left[\frac{s^2 + 3}{(s^2 + 1)(1 - s^2)} \right] = \frac{s^2 + 3}{(s^2 + 1)(1 + s)(1 - s)}$$

$$= \frac{A}{1 + s} + \frac{B}{1 - s} + \frac{Cs + D}{s^2 + 1}$$

$$s^2 + 3 = A(1 - s)(s^2 + 1) + B(1 + s)(s^2 + 1) + (Cs + D)(1 + s)(1 - s)$$

Putting $s = 1$, $4B = 4, \Rightarrow B = 1$

Putting $s = -1$, $4A = 4, \Rightarrow A = 1$

Putting $s = 0$, $A + B + D = 3 \Rightarrow D = 1$

Equating coeff. of s^3 , $-A + B - C = 0 \Rightarrow C = 0$

$$\therefore \frac{s^2 + 3}{(s^2 + 1)(1 + s)(1 - s)} = \frac{1}{s + 1} + \frac{1}{1 - s} + \frac{1}{s^2 + 1}$$

$$\therefore L^{-1} \left[\frac{s^2 + 3}{(s^2 + 1)(1 + s)(1 - s)} \right] = L^{-1} \left[\frac{1}{s + 1} + \frac{1}{1 - s} + \frac{1}{s^2 + 1} \right]$$

$$= L^{-1} \left[\frac{1}{s + 1} - \frac{1}{s - 1} + \frac{1}{s^2 + 1} \right]$$

$$= e^{-t} - e^t + \sin t$$

$$\therefore x = 2 \cosh t$$

$$y = \sin t + e^{-t} - e^t$$

Example: 3

Solve $\frac{dx}{dt} - \frac{dy}{dt} - 2x + 2y = 1 - 2t$; $\frac{d^2x}{dt^2} + 2\frac{dy}{dt} + x = 0$ with

$x = 0, y = 0, \frac{dx}{dt} = 0$ when $t = 0$.

Solution:

The given equation can be written as

$$x' - y' - 2x + 2y = 1 - 2t$$

$$x'' + 2y' + x = 0$$

Taking Laplace Transforms, we get

$$L[x'] - L[y'] - 2L[x] + 2L[y] = L[1 - 2t]$$

$$L[x''] + L[2y'] + L[x] = 0$$

$$sL[x] - x(0) - sL[y] - y(0) - 2L[x] + 2L[y] = \frac{1}{s} - \frac{2}{s^2}$$

$$s^2L[x] - sx(0) - x'(0) + 2sL[y] - 2y(0) + L[x] = 0$$

Putting $L(x) = \bar{x}$, $L(y) = \bar{y}$ and $x(0) = 0, y(0) = 0, x'(0) = 0$,
we get

$$s\bar{x} - s\bar{y} - 2\bar{x} + 2\bar{y} = \frac{1}{s} - \frac{2}{s^2}$$

$$s^2\bar{x} + 2s\bar{y} + \bar{x} = 0$$

$$\bar{x}(s-2) - \bar{y}(s-2) = \frac{s-2}{s^2} \quad (1)$$

$$\bar{x}(s^2+1) + \bar{y}2s = 0 \quad (2)$$

Solving (1) and (2) simultaneously we get,

Space for Hints

$$\bar{x} = \frac{\begin{vmatrix} \frac{s-2}{s^2} & -(s-2) \\ 0 & 2s \end{vmatrix}}{\begin{vmatrix} s-2 & -(s-2) \\ s^2+1 & 2s \end{vmatrix}}$$

$$= \frac{2(s-2)}{2s(s-2) + (s-2)(s^2+1)}$$

$$= \frac{2(s-2)}{s} \cdot \frac{1}{(s-2)(2s+s^2+1)}$$

$$= \frac{2}{s(s+1)^2}$$

$$\text{i.e., } L[x(t)] = \frac{2}{s(s+1)^2}$$

$$x(t) = L^{-1} \left[\frac{2}{(s(s+1)^2)} \right]$$

$$= 2L^{-1} \left[\frac{1}{s} - \frac{1}{s+1} - \frac{1}{(s+1)^2} \right]$$

[After separating into partial fractions]

$$= 2[1 - e^{-t} - e^{-t}.t]$$

$$\bar{y} = \frac{\begin{vmatrix} s-2 & \frac{s-2}{s^2} \\ s^2+1 & 0 \end{vmatrix}}{\begin{vmatrix} s-2 & -(s-2) \\ s^2+1 & 2s \end{vmatrix}}$$

$$= \frac{-\left(\frac{s-2}{s^2}\right)(s^2+1)}{2s(s-2) + (s-2)(s^2+1)}$$

$$= -\frac{s^2 + 1}{s^2(2s + s^2 + 1)}$$

$$L[y(t)] = -\frac{s^2 + 1}{s^2(s + 1)^2}$$

$$y(t) = -L^{-1}\left[\frac{s^2 + 1}{s^2(s + 1)^2}\right]$$

$$= -\int_0^t L^{-1}\left[\frac{s^2 + 1}{s(s + 1)^2}\right] dt \quad (3)$$

To find $L^{-1}\left[\frac{s^2 + 1}{s(s + 1)^2}\right]$

Now, $\frac{s^2 + 1}{s(s + 1)^2} = \frac{A}{s} + \frac{B}{s + 1} + \frac{C}{(s + 1)^2}$

$$s^2 + 1 = A(s + 1)^2 + Bs(s + 1) + Cs$$

Putting $s = -1$, $-C = 2$, $\Rightarrow C = -2$

Putting $s = 0$, $A = 1$

Equating coeff. of s^2 , $A + B = 1 \Rightarrow B = 0$

$$\frac{s^2 + 1}{s(s + 1)^2} = \frac{1}{s} - \frac{2}{(s + 1)^2}$$

$$L^{-1}\left[\frac{s^2 + 1}{s(s + 1)^2}\right] = L^{-1}\left[\frac{1}{s}\right] - 2L^{-1}\left[\frac{1}{(s + 1)^2}\right]$$

$$= 1 - 2e^{-t}.t$$

(4)

Substituting (4) in (3) we get,

$$y(t) = -\int_0^t (1 - 2e^{-t}.t) dt$$

$$= -[t - 2\{t(-e^{-t}) - 1(e^{-t})\}]_0^t$$

$$= -[t + 2te^{-t} + 2e^{-t} - 2]$$

$$= -t(1 + 2e^{-t}) + 2(1 - e^{-t})$$

$$\therefore x = 2[1 - e^{-t} - e^{-t}t]$$

Example: 4

Solve the simultaneous equations.

$$3\frac{dx}{dt} + \frac{dy}{dt} + 2x = 1 \quad (1)$$

$$\frac{dx}{dt} + 4\frac{dy}{dt} + 3y = 0 \quad (2)$$

Given $x = 0 = y$ at $t = 0$.

Solution:

Applying Laplace transforms to both the equations, (1) becomes

$$3L(x') + L(y') + 2L(x) = L(1)$$

$$\text{i.e., } 3(s\bar{x} - x(0)) + s\bar{y} - y(0) + 2\bar{x} = \frac{1}{s}$$

$$\text{where } \bar{x} = L(x), \quad \bar{y} = L(y).$$

Since $x(0) = 0$, $y(0) = 0$, we have

$$3s\bar{x} + s\bar{y} + 2\bar{x} = \frac{1}{s}$$

$$\text{i.e., } (3s + 2)\bar{x} + s\bar{y} = \frac{1}{s}$$

Equation (2) becomes

$$L(x') + 4L(y') + 3L(y) = 0$$

$$\text{i.e., } s\bar{x} - x(0) + 4\{s\bar{y} - y(0)\} + 3\bar{y} = 0$$

$$\text{i.e., } s\bar{x} + (4s + 3)\bar{y} = 0$$

Solving (3) and (4), we get

$$\bar{x} = \frac{4s + 3}{s(s + 1)(11s + 6)}$$

$$\bar{y} = -\frac{1}{(11s + 6)(s + 1)}$$

$$\therefore x = L^{-1}\left\{\frac{4s + 3}{s(s + 1)(11s + 6)}\right\}$$

$$= L^{-1}\left\{\frac{1}{s} - \frac{1}{s + 1} - \frac{33}{11s + 6}\right\}$$

$$= \frac{1}{2}L^{-1}\left(\frac{1}{s}\right) - \frac{1}{5}L^{-1}\left(\frac{1}{s + 1}\right) - \frac{33}{10}L^{-1}\left(\frac{1}{11s + 6}\right)$$

$$= \frac{1}{2} - \frac{1}{5}e^{-t} - \frac{3}{10}e^{-\frac{6t}{11}}$$

$$y = L^{-1}\left\{\frac{-1}{(11s + 6)(s + 1)}\right\}$$

$$= L^{-1}\left\{\frac{1}{5} \cdot \frac{1}{s + 1} - \frac{11}{5} \cdot \frac{1}{11s + 6}\right\}$$

$$= \frac{1}{5} L^{-1} \left(\frac{1}{s+1} \right) - \frac{11}{5} \cdot \frac{1}{11} L^{-1} \left(\frac{1}{s + \frac{6}{11}} \right)$$

$$= \frac{1}{5} e^{-t} - \frac{1}{5} e^{-\frac{6t}{11}}$$

Example: 5

Solve the simultaneous equations.

$$\frac{dx}{dt} - \frac{dy}{dt} - 2x + 2y = 1 - 2t \quad (1)$$

$$\frac{d^2x}{dt^2} + 2 \frac{dy}{dt} + x = 0 \quad (2)$$

With the conditions $x = 0, y = 0, \frac{dx}{dt} = 0$ when $t = 0$.

Solution:

Applying Laplace transforms to both the equations, equation (1) becomes

$$L(x') - L(y') - 2L(x) + 2L(y) = L(1) - L(2t)$$

$$\text{i.e., } s\bar{x} - x(0) - s\bar{y} + y(0) - 2\bar{x} + 2\bar{y} = \frac{1}{s} - \frac{2}{s^2}$$

$$\text{i.e., } s\bar{x} - s\bar{y} - 2\bar{x} + 2\bar{y} = \frac{1}{s} - \frac{2}{s^2}$$

$$\text{i.e., } (s-2)\bar{x} - (s-2)\bar{y} = \frac{s-2}{s^2}$$

$$\bar{x} - \bar{y} = \frac{1}{s^2}$$

$$(3)$$

Equation (2) becomes

$$L(x'') + 2L(y') + L(x) = 0$$

$$\text{i.e., } s^2 \bar{x} - sx(0) - x'(0) + 2s\bar{y} - 2y(0) + \bar{x} = 0$$

$$\text{i.e., } s^2 \bar{x} + 2s\bar{y} + \bar{x} = 0$$

$$\text{i.e., } (s^2 + 1)\bar{x} + 2s\bar{y} = 0 \quad (4)$$

Solving equations (3) and (4) for $\bar{x}$ and $\bar{y}$, we get

$$\bar{x} = \frac{2}{s(s+1)^2}, \bar{y} = -\frac{s^2 + 1}{s^2(s+1)^2}$$

$$\therefore x = L^{-1} \left[\frac{2}{s(s+1)^2} \right]$$

$$= 2L^{-1} \left[\frac{1}{s} - \frac{1}{s+1} - \frac{1}{(s+1)^2} \right]$$

$$= 2 \left\{ L^{-1} \left(\frac{1}{s} \right) - L^{-1} \left(\frac{1}{s+1} \right) - L^{-1} \left[\frac{1}{(s+1)^2} \right] \right\}$$

$$= 2(1 - e^{-t} - te^{-t}).$$

$$y = -L^{-1} \left\{ \frac{s^2 + 1}{s^2(s+1)^2} \right\}$$

$$= - \int_0^t L^{-1} \left\{ \frac{s^2 + 1}{s(s+1)^2} \right\} dt$$

$$= - \int_0^t L^{-1} \left\{ \frac{1}{s} - \frac{2}{(s+1)^2} \right\} dt$$

$$= - \int_0^t (1 - 2te^{-t}) dt$$

$$= 2 - t - 2(t+1)e^{-t}$$

THEORY OF NUMBERS**7.0 Introduction**

Number theory is the part of mathematics that seeks to investigate the properties of integers, more specifically the properties of positive integers. One gets the benefit of an over all – view of much of contemporary mathematics, for almost any field of Mathematics is connected with it. Also, it is an art enjoyable and pleasing to everybody.

7.1 Prime and Composite Numbers:**Definition: 7.1.1**

Prime number is an integer greater than one which has no divisors except itself and unity. Thus, 2, 3, 5, 7, 11, 13, 17, 19,..... are prime numbers.

Definition: 7.1.2

Composite numbers which can be expressed as the product of two smaller integers. (i.e.,) A natural number which is neither a unit nor a prime is called a composite number.

Examples of composite numbers are 4, 12, 18, 15,.....

Two numbers which have no common divisor other than one are said to be prime to one another. Thus 12 and 17, 32 and 63, 28 and 45 are prime to one another.

7.2 The Sieve of Eratosthenes:

Prime numbers were a subject of great interest from early days. Eratosthenes who lived about 200 B.C. devised a simple method to

find the primes below a given number.

The method consists in writing down all the integers up to the given number in their natural succession and then striking out all the multiples of 2, then the multiples of 3, then those of 5 and so on.

If we want to determine the primes less than 500, it is not necessary to go beyond multiples of 23. This scheme with a little modification is used even today for the construction of tables of prime numbers.

The Sieve of Eratosthenes for prime less than 100 is given below.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

The prime numbers below 100 are 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 and 97.

7.1 Theorem

The number of primes is infinite.

Proof:

Let the number of prime be finite, say n , and let those primes be $p_1, p_2, p_3, \dots, p_n$. Then all the other numbers are composite and therefore should be exactly divisible by atleast one of the prime numbers $p_1, p_2, p_3, \dots, p_n$. Let us consider the number

$$A = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$$

When this number is divided by p_1 or by p_2 , or by $p_3, \dots$ or by p_n the remainder is 1. Hence the number A is not exactly divisible by any of the prime numbers $p_1, p_2, \dots, p_n$.

(i.e.,) A is a prime number which is contrary to our assumption.

Hence our assumption that the number of primes, is finite, is wrong.

Hence the number of primes is infinite.

Remark:

The previous article gives us a method of constructing an infinite sequence of primes. We know that 2 and 3 are primes.

Hence $2 \times 3 + 1$ (i.e.,) 7 is a prime

$2 \times 3 \times 5 + 1$ (i.e.,) 31 is a prime

$2 \times 3 \times 5 \times 7 + 1$ (i.e.,) 211 is a prime

By this method it is not possible to find all the primes. So attempts have been made to find some simple arithmetical formulae that give only primes even through they may not give all of them.

The following are some formulae which give prime numbers for certain value of n :

- 1) $n^2 + n + 41$ is a prime number if $n < 40$.
- 2) $n^2 + n + 17$ is a prime number if $n < 16$.
- 3) $2n^2 + 29$ is a prime number if $n < 29$.
- 4) $n^2 - 79n + 1601$ is a prime number if $n < 80$.
- 5) $2^{2^n} + 1$ is a prime number if $n < 5$.

7.2.1 Prime Number Theorem:

The number of prime numbers less than or equal to a number N is usually denoted by $\pi(N)$. Thus

$$\pi(1) = 1; \pi(2) = 2; \pi(3) = 3; \pi(4) = 3; \pi(5) = 4; \pi(6) = 4; \dots$$

The distribution of prime numbers is very irregular and no exact formula has been discovered for $\pi(N)$, but it has been shown

$$\text{that } \lim_{N \rightarrow \infty} \frac{\pi(N)}{N / \log N} = 1.$$

This result is known as 'Prime Number Theorem'.

Remark:

Every composite number can be resolved into prime factors and this can be done only in one way.

Let N be the composite number. Since the number is composite, it has a factor other than N and 1. Let it be a and the quotient when N is divided by a be b .

$$\text{Then } N = ab.$$

If a and b are not primes, we can find the divisors of a and b and express a and b in the form $a = cd$ and $b = ef$.

$$\therefore N = cdef.$$

Here a and b are less than N .

c and d are less than a .

e and f are less than b .

$\therefore c, d, e$ and f are less than N .

Proceeding in this way we must come finally to factors which are prime numbers since the factors diminish at every stage.

Hence N can be expressed in the form $N = pqr\dots$ where $p, q, r, \dots$ are all prime numbers, not necessarily different.

$\therefore N$ can be expressed as $N = p^a q^b r^c \dots$ where $p, q, r, \dots$ are all primes and $a, b, c, \dots$ integers.

Let N be resolved into prime factors in another way and let that be $P^A Q^B R^C \dots$ where $P, Q, R, \dots$ are all primes and $A, B, C, \dots$ integers.

$$\therefore N = p^a q^b r^c \dots = P^A Q^B R^C \dots$$

Since the prime P is a divisor of the product $p^a q^b r^c \dots$ it is a divisor of one of the factors $p, q, r, \dots$.

Since $p, q, r, \dots$ are all primes p must be equal to one of them.

Similarly each one of $P, Q, R, \dots$ is equal to one of $p, q, r, \dots$.

$$\therefore p^a q^b r^c \dots = p^A q^B r^C \dots$$

If $A \neq a$, then let A be equal to $a + k$.

Since A and a are integers k is also an integer.

$$\therefore p^a q^b r^c \dots = p^{a+k} q^B r^C \dots$$

$$\therefore q^b r^c \dots = p^k q^B r^C \dots$$

p is a factor of the expression in the right side of the equation.

$\therefore p$ is a factor of the expression in the left side but this is impossible since the expression in the left side is prime to p .

$$\therefore k = 0. \text{ Hence } A = a.$$

$$\text{Similarly } B = b, C = c, \dots$$

Hence the factorization of a composite number into product of primes is unique.

7.3 Divisors of a Given Number N:

N can be expressed as the product of primes and let N be $p^a q^b r^c \dots$, where $p, q, r, \dots$ are primes.

Let n be the number of divisors.

The divisors of N are the terms in the expansion of

$$(1 + p + p^2 + \dots + p^a)(1 + q + q^2 + \dots + q^b)(1 + r + r^2 + \dots + r^c) \dots$$

Hence the number of terms in the product will be the number of divisors and we can easily see that the number of divisors is $(a+1)(b+1)(c+1) \dots$. The divisors include 1 and the number N itself. The sum of all the divisors is the sum of all the terms in the continued product.

$$\therefore S = \frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{b+1} - 1}{q - 1} \cdot \frac{r^{c+1} - 1}{r - 1} \dots$$

Example: 1

Find the number and sum of all the divisors of 360.

Solution:

$$360 = 2^3 \cdot 3^2 \cdot 5^1$$

$$\text{The number of divisors} = (3+1)(2+1)(1+1) = 24$$

$$\text{Sum of the divisors} = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1}$$

$$= \frac{15}{1} \cdot \frac{26}{2} \cdot \frac{24}{4}$$

$$= 1170$$

Example: 2

Find the smallest number with 18 divisors.

Solution:

Let the number be N which is equal to $p^a q^b r^c \dots$ where p, q, r are primes and $a, b, c, \dots$ are integers.

Since we have to find the smallest numbers $p, q, r, \dots$ must be as small as possible and a, b, c should be in the descending order of magnitude.

$$\therefore N = 2^a 3^b 5^c \dots$$

$$\text{Number of divisors} = (a+1)(b+1)(c+1) \dots$$

$$\therefore 18 = (a+1)(b+1)(c+1) \dots$$

$$\text{But } 18 = 2 \times 3 \times 3$$

$\therefore$ We can take $c+1=2, b+1=3, a+1=3$

(i.e.,) $c=1, b=2, a=2$

$$\therefore N = 2^2 3^2 5^1 = 180$$

Example: 3

Find the product of all the divisors of N .

Solution:

Let N be expressed in the form $p^a q^b r^c \dots$

The number of divisors is $(a+1)(b+1)(c+1) \dots$

If x is a divisor of N , then $\frac{N}{x}$ is also a divisor of N .

$\therefore$ All the divisor of N can be grouped into pairs whose product is N .

$\therefore (a+1)(b+1)(c+1) \dots$ divisors can be grouped into

$\frac{1}{2}(a+1)(b+1)(c+1) \dots$ pairs, the product of each pair being N .

$\therefore$ Product of the divisors $= N^{\frac{1}{2}(a+1)(b+1)(c+1) \dots}$

Exercises:

1. Find the number of divisors of 480 excluding 1 and 480.
2. Find the number of divisors of (i) 840 (ii) 1458 (iii) 288, excluding the number itself.
3. Verify that (i) 220 and 284, (ii) 17296 and 18416 are amicable numbers' (i.e.,) each is the sum of the divisors of the other (including 1 but excluding the number itself).

Space for Hints

4. Show that the number of divisors of an integer is odd if and only if this integer is a square.
5. If N has n divisors including itself and 1, prove that their continued product is $\sqrt{N^n}$.
6. Find the smallest number (i) with 24 divisors, (ii) with 10 divisors.
7. Show that if $2^n - 1$ is a prime, then $2^{n-1}(2^n - 1)$ is a perfect number and find the three least numbers given by the formula.
(N is a perfect number if the sum of all its divisors excluding N is N).
8. Prove that the sum of reciprocals of the divisors of the perfect number $2^{n-1}(2^n - 1)$ is 2.

UNIT – 8

EULER'S FUNCTION $\phi(N)$ 8.1 Euler's Function $\phi(N)$

8.1.1 Introduction

The number of positive integers less than N and prime to it is denoted by $\phi(N)$. From the definition we get $\phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2$. Even though $\phi(1)$ has no meaning as per this definition, we define it equal to 1.

Value of $\phi(N)$:

We have shown that N can be expressed as $N = p^a q^b r^c \dots$ where $p, q, r, \dots$ are all primes and $a, b, c, \dots$ integers. An integer will be prime to N iff it is not divisible by any of the primes $p, q, r, \dots$. Therefore $\phi(N)$ is the number of integers in the series $1, 2, 3, \dots, N$ which are not divisible by any of these primes. If we can find the numbers which are divisible by these primes in the series $1, 2, \dots, N$, we can get $\phi(N)$ by subtracting the numbers of such numbers from N . Numbers which are divisible by p in the series $1, 2, \dots, N$ are $p, 2p, 3p, \dots, N/p$ and therefore there are N/p numbers which are divisible by p .

So also there are $\frac{N}{q}$ numbers which are divisible by q .

Similarly there are $\frac{N}{r}$ numbers which are divisible by r .

Space for Hints

” ” ” ”

” ” ” ”

” $\frac{N}{pq}$ ” by pq

” $\frac{N}{qr}$ ” by qr

” $\frac{N}{pqr}$ ” by pqr

and so on.

Consider the series $= \sum \frac{N}{p} - \sum \frac{N}{pq} + \sum \frac{N}{pqr} \dots$ (1)

Consider any integer not greater than N.

Suppose that it is divisible by exactly k of the primes p, q, r,.....

This number occurs kC_1 times in $\sum \frac{N}{p}$

” kC_2 times in $\sum \frac{N}{pq}$

” kC_3 times in $\sum \frac{N}{pqr}$

and so on.

Therefore the number of times it is counted in the expression (1) is $kC_1 - kC_2 + kC_3, \dots$ which is equal to $1 - (1 - 1)^k$ (i.e.,) 1.

Every integer (excluding unity) not greater than N and not prime to it is counted exactly once in (1). In evaluating $\phi(N)$ we count 1 also.

Therefore

$$\phi(N) = N - \sum \frac{N}{p} + \sum \frac{N}{pq} - \sum \frac{N}{pqr} + \dots$$

$$= N \left(1 - \sum \frac{1}{p} + \sum \frac{1}{pq} - \sum \frac{1}{pqr} + \dots \right)$$

$$= N \left(1 - \frac{1}{p} \right) \left(1 - \frac{1}{q} \right) \left(1 - \frac{1}{r} \right) \dots$$

Corollary: 1

If $N = ab$ where a and b are prime to one another, then $\phi(N) = \phi(a) \cdot \phi(b)$.

Let $a = p_1^{a_1} \cdot p_2^{a_2} \dots p_k^{a_k}$ and $b = q_1^{b_1} \cdot q_2^{b_2} \dots q_r^{b_r}$, where $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_r$ are primes.

Since a and b are prime to one another $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_r$ are different.

$$\phi(a) = a \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \dots \left(1 - \frac{1}{p_k} \right)$$

$$\phi(b) = b \left(1 - \frac{1}{q_1} \right) \left(1 - \frac{1}{q_2} \right) \dots \left(1 - \frac{1}{q_r} \right)$$

$$N = ab = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \cdot q_1^{b_1} \cdot q_2^{b_2} \dots q_r^{b_r}$$

Therefore

Space for Hints

$$\begin{aligned}\phi(N) &= N \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_r}\right) \\ &= ab \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_r}\right) \\ &= \phi(a) \cdot \phi(b)\end{aligned}$$

Corollary: 2

If $a, b, c, d, \dots, k$ are prime to one another,
 $\phi(abcd \dots k) = \phi(a) \cdot \phi(b) \dots \phi(k)$.

Corollary: 3

If p is prime, then $\phi(p^r) = p^r \left(1 - \frac{1}{p}\right)$

Example: 1

Find the number of integers less than n and prime to it when
 $n = 729$ and 720

Solution:

We have $729 = 3^6$

$$\therefore \phi(729) = 729 \left(1 - \frac{1}{3}\right) = 486$$

$$720 = 2^4 \cdot 3^2 \cdot 5$$

$$\begin{aligned}\therefore \phi(720) &= 720 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\ &= 192\end{aligned}$$

Example: 2

Prove that the sum of the integers less than N and prime to it including unity is $\frac{1}{2}N\phi(N)$.

Solution:

Let x be one of the integers less than N and prime to it. Then $N - x$ is also prime to it.

$\therefore$ All the number less than N , prime to it can be grouped into pairs whose sum is N .

$\therefore \phi(N)$ can be grouped into $\frac{\phi(N)}{2}$ pairs the sum of each pair being N .

$$\therefore \text{Sum of the numbers} = \frac{N\phi(N)}{2}.$$

Example: 3

If $d_1, d_2, d_3, \dots, d_r$ (including 1 and N) are the divisors of N , then show that $\phi(d_1) + \phi(d_2) + \dots + \phi(d_r) = N$

Solution:

Let $N = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ where $p_1, p_2, \dots, p_n$ are primes and $a_1, a_2, a_3, \dots$ are integers.

Every divisor is of the form $p_1^x p_2^y p_3^z, \dots$ where $x, y, z, \dots$ take integral values from 0 to $a_1, 0$ to $a_2, 0$ to $a_3, \dots$ respectively. We know that,

$$\phi(p_1^x \cdot p_2^y \cdot p_3^z \dots) = \phi(p_1^x) \phi(p_2^y) \phi(p_3^z) \dots$$

Hence $\phi(d_1), \phi(d_2), \phi(d_3), \dots, \phi(d_r)$ are the terms in the expansion of

$$[1 + \phi(p_1) + \phi(p_1^2) + \dots + \phi(p_1^{a_1})]$$

$$x[1 + \phi(p_2) + \phi(p_2^2) + \dots + \phi(p_2^{a_2})]$$

$$x \dots \dots \dots$$

$$x[1 + \phi(p_n) + \phi(p_n^2) + \dots + \phi(p_n^{a_n})] \quad (1)$$

$$\therefore \phi(d_1) + \phi(d_2) + \dots + \phi(d_r)$$

= Continued product of the expression (1)

$$\begin{aligned} 1 + \phi(p_1) + \phi(p_1^2) + \dots + \phi(p_1^{a_1}) &= 1 + p_1 \left(1 - \frac{1}{p_1}\right) + p_1^2 \left(1 - \frac{1}{p_1}\right) + \dots + p_1^{a_1} \left(1 - \frac{1}{p_1}\right) \\ &= 1 + p_1 - 1 + p_1^2 - p_1 + p_1^3 - p_1^2 + \dots + p_1^{a_1} - p_1^{a_1-1} \\ &= p_1^{a_1} \end{aligned}$$

Similarly,

$$1 + \phi(p_2) + \phi(p_2^2) + \dots + \phi(p_2^{a_2}) = p_2^{a_2} \text{ and so on.}$$

$$\therefore \phi(d_1) + \phi(d_2) + \dots + \phi(d_r) = p_1^{a_1} \cdot p_2^{a_2} \dots p_n^{a_n} = N$$

Exercises:

1. How many numbers including unity are less than 210 and prime to it?
2. Find the sum of the positive integers including unity which are less than 600 and prime to it.
3. How many numbers are there less than 500 which are not divisible by 2, 3 or 5?

4. If a is prime to N , show that the number of terms of the arithmetical progression $x, x + a, x + 2a, \dots, x + (n - 1)a$ which are prime to N is $\phi(N)$.

5. Show that if N be any number and $a, b, c, \dots$ be its different prime factors, then the sum of all the numbers less than N and prime to N is

$\frac{N^2}{2} \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \left(1 - \frac{1}{c}\right) \dots$ and the sum of the squares of all such numbers is

$$\frac{N^3}{3} \left(1 - \frac{1}{a}\right) \left(1 - \frac{1}{b}\right) \left(1 - \frac{1}{c}\right) \dots + \frac{N}{6} (1 - a)(1 - b)(1 - c) \dots$$

6. Show that the arithmetic mean of all numbers less than N and prime to it (including unity) is $N/2$.

8.2 Integral Part of a Real Number:

The integral part of a number x is denoted by the symbol $[x]$.

For example,

$$\left[4\frac{2}{3}\right] = 4; [6] = 6, \left[\frac{2}{5}\right] = 0, [\sqrt{2}] = 1, [-\sqrt{2}] = -2$$

The “fractional part” is considered to be positive.

From the definition, the following properties are easily deduced.

$$(1) [x] \leq x < [x] + 1$$

$$(2) [x + a] = [x] + a \text{ if } a \text{ is an integer}$$

$$(3) [x + y] \geq [x] + [y]$$

8.3 The Highest Power of a Prime p Contained in $N!$:

$$n! = 1.2.3.....n$$

If $n < p$, there is no number in $n!$ which is divisible by p .

If $n \geq p$, then $n!$ contains numbers which are divisible by p .

The factors in $n!$ which will be divisible by p are $p, 2p, 3p, \dots, \left[\frac{n}{p} \right] p$.

Hence the highest power of p in $n!$ is the highest power of p in the product.

$$(i.e.,) \text{ in } p^{\left[\frac{n}{p} \right]} . 1.2.3..... \left[\frac{n}{p} \right]$$

But in $1.2.3..... \left[\frac{n}{p} \right]$ the prime p is a factor in the numbers $p, 2p,$

$$3p..... \left[\frac{n}{p^2} \right] p$$

$\therefore$ Power of p in the product $1.2.3..... \left[\frac{n}{p} \right]$ is the power of p in

$$\text{the product } p.2p.3p..... \left[\frac{n}{p^2} \right] p$$

$$(i.e.,) p^{\left[\frac{n}{p^2} \right]} . 1.2.3..... \left[\frac{n}{p^2} \right]$$

Hence the highest power of p in $n!$ is the highest power of p in

$$\text{the product } p^{\left[\frac{n}{p} \right]} . p^{\left[\frac{n}{p^2} \right]} . 1.2.3..... \left[\frac{n}{p^2} \right]$$

(i.e.,) in $p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right]} \cdot 1.2.3 \dots \left[\frac{n}{p^2}\right]$

In the same way we find the highest power of p in $n!$ is the highest power of p in the product $p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right]} \cdot 1.2.3 \dots \left[\frac{n}{p^3}\right]$

(i.e.,) in the product $p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \left[\frac{n}{p^4}\right]} \cdot 1.2.3 \dots \left[\frac{n}{p^4}\right]$

$\left[\frac{n}{p}\right], \left[\frac{n}{p^2}\right], \left[\frac{n}{p^3}\right] \dots$ from a decreasing sequence and hence

there exists a positive integer k where $\left[\frac{n}{p^k}\right] = 0$.

Hence if we continue this process we will get the highest power of

$$p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots + \left[\frac{n}{p^{k-1}}\right] \text{ where } \left[\frac{n}{p^k}\right] = 0$$

Example: 1

Find the highest power of 3 dividing 1000!

Solution:

$$\left[\frac{1000}{3}\right] = 333$$

$$\left[\frac{1000}{3^2}\right] = \left[\frac{333}{3}\right] = 111$$

$$\left[\frac{1000}{3^3}\right] = \left[\frac{111}{3}\right] = 37$$

$$\left[\frac{1000}{3^4} \right] = \left[\frac{37}{3} \right] = 12$$

$$\left[\frac{1000}{3^5} \right] = \left[\frac{12}{3} \right] = 4$$

$$\left[\frac{1000}{3^6} \right] = \left[\frac{4}{3} \right] = 1$$

The highest power of 3 in 1000! is $333 + 111 + 37 + 12 + 4 + 1 = 498$

The 3^{498} is the highest power of 3 dividing 1000!

Example: 2

With how many zeros does 79! end?

Solution:

Let us find the highest power of 2 and 5 in 79!

$$\left[\frac{79}{2} \right] = 39, \quad \left[\frac{79}{2^2} \right] = 19, \quad \left[\frac{79}{2^3} \right] = 9,$$

$$\left[\frac{79}{2^4} \right] = 4, \quad \left[\frac{79}{2^5} \right] = 2, \quad \left[\frac{79}{2^6} \right] = 1$$

Thus 2^{74} is the highest power of 2 in 79!, $\left[\frac{79}{5} \right] = 15, \left[\frac{79}{5^2} \right] = 3.$

Thus 5^{18} is the highest power of 5 in 79!

$\therefore$ The highest power of 10 in 79! is 18.

$\therefore$ 79! will end in 18 zeros.

8.4 The Product of r Consecutive Integers is Divisible by r!:

Let $n+1, n+2, \dots, n+r$ be the consecutive integers.

Product of these integers $= (n+1)(n+2)\dots\dots(n+r)$

$$= \frac{(n+r)!}{n!}$$

We have to prove that $= \frac{(n+r)!}{n!}$ is divisible by $r!$

Example:

(i.e.,) $\frac{(n+r)!}{n!r!}$ is an integer.

(i.e.,) We have to show that the highest power of a prime p occurring in $(n+r)!$ is greater than the highest power of p in $n!r!$.

The highest power of any prime p occurring in $(n+r)!, n!, r!$ are respectively.

$$\left[\frac{n+r}{p} \right] + \left[\frac{n+r}{p^2} \right] + \dots\dots$$

$$\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \dots\dots$$

$$\left[\frac{r}{p} \right] + \left[\frac{r}{p^2} \right] + \dots\dots$$

$\therefore$ Highest power of p occurring in $n!r!$ is

$$\left[\frac{n}{p} \right] + \left[\frac{r}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{r}{p^2} \right] + \dots\dots$$

We know that $[x+y] \geq [x] + [y]$

$$(i.e.,) \left[\frac{x+y}{p^k} \right] \geq \left[\frac{x}{p^k} \right] + \left[\frac{y}{p^k} \right]$$

By putting $x = n, y = r, k = 1, 2, \dots\dots$

We get

$$\left[\frac{n+r}{p} \right] \geq \left[\frac{n}{p} \right] + \left[\frac{r}{p} \right]$$

$$\left[\frac{n+r}{p^2} \right] \geq \left[\frac{n}{p^2} \right] + \left[\frac{r}{p^2} \right]$$

.....

.....

$$\therefore \left[\frac{n+r}{p} \right] + \left[\frac{n+r}{p^2} \right] + \dots \geq \left[\frac{n}{p} \right] + \left[\frac{r}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{r}{p^2} \right] + \dots$$

(i.e.,) the prime p enters in the numerator $(n+r)!$ in powers not lower than in the denominators $n!r!$.

$\therefore$ The numerator is divisible by the denominator.

$\therefore (n+1)(1+2)\dots(n+r)$ is divisible by $r!$.

Corollary: 1

$\frac{n!}{a!b!c!}$ is an integer when $a+b+c+\dots=n$.

Corollary: 2

If n is a prime, nc_r is divisible by n .

$$nc_r = \frac{n(n-1)(n-2)\dots(n-r+1)}{r!}$$

The numerator is a product of r consecutive integers.

$\therefore$ It is divisible by $r!$

n is prime to r .

$\therefore$ It is prime to $r!$

$\therefore (n-1)(n-2)\dots(n-r+1)$ is divisible by $r!$

$\therefore nc_r = n \times \text{an integer since } nc_r = \frac{n(n-1)\dots(n-r+1)}{r!}$

$\therefore nc_r$ is divisible by n .

Example:

Show that $n(n+1)(2n+1)$ is divisible by 6.

Proof:

$$\begin{aligned} n(n+1)(2n+1) &= n(n+1)(2n+4-3) \\ &= 2n(n+1)(n+2) - 3n(n+1) \end{aligned}$$

$n(n+1)$ is divisible by 2.

$n(n+1)(n+2)$ is divisible by $3!$ (i.e.,) 6.

Hence the expression is divisible by 6.

Note:

$n(n+1)(2n+1)$ is a multiple of 6.

This is usually written as $n(n+1)(2n+1) = M(6)$.

Exercises:

- Find the highest powers of 2, 5, 7, 11, 13 contained in 1000!
- With how many zeros does (i) $61!$ (ii) $257!$ and (iii) $82!$ end?
- If n is any odd number, show that $n(n^2-1)$ is divisible by 24.

Space for Hints

4. Show that $n(n^2 - 1)(29n^2 + 4) = M(120)$
5. Show that $n^5 - n = M(30)$
6. Show that $n(n - 1)(n + 25)(n + 50) = M(24)$
7. Show that the greatest power of n in $(n^r - 1)!$ is $\frac{n^r - nr + r - 1}{n - 1}$.
8. Show that if n is odd
 - (i) $(n^2 + 3)(n^2 + 7) = M(32)$.
 - (ii) $n^4 + 4n^2 + 11 = M(16)$.
9. Show that if n is a positive integer $(n + 1)(n + 2) \dots (n + n)$ is divisible by 2^n .
10. If n be an odd prime, show that $(a + 1)^n - (a^n + 1) = M(2n)$
11. If $n = 2^a + 2^b + 2^c + \dots + m$ terms where $a < b < c < \dots$ show that the greatest power of that must divide $n!$ is $(n - m)$.
12. Show that if n be prime greater than 3.
$$n(n^2 - 1)(n^2 - 4)(n^2 - 9) = M(2^7 \cdot 3^2 \cdot 5 \cdot 7)$$

Answers:

1. 994; 249; 164; 98; 81
2. (i) 14; (ii) 63; (iii) 19.

UNIT - 9

CONGRUENCES

9.1 Congruences

9.1.1 Introduction

Two integers a and b are called congruent with respect to the modulus m if an integer k exists such that $a - b = km$.

k may be positive, zero or negative. The congruence is denoted by

$$a \equiv b \pmod{m} \text{ (or) } a - b \equiv 0 \pmod{m}.$$

For example, $18 \equiv 4 \pmod{7}$

$$13 \equiv 28 \pmod{5}$$

$$14 - 4 \equiv 0 \pmod{5}$$

If two numbers are congruent with respect to the modulus m , each is called a **residue** of the other to the modulus m .

Every residue of a to the modulus is of the form $a + km$ where k may be positive or negative.

Congruences with the same moduli possess many properties of equalities.

Some of them are given below.

1. If $a \equiv b \pmod{m}$ and $a_1 \equiv b_1 \pmod{m}$ and if q, r are integers, then $qa + ra_1 \equiv qb + rb_1 \pmod{m}$

$$a \equiv b \pmod{m} \quad \therefore \quad a - b = km$$

Space for Hints

$$a_1 \equiv b_1 \pmod{m} \therefore a_1 - b_1 = k_1 m$$

$$qa + ra_1 = q(b + km) + r(b_1 + k_1 m)$$

$$= qb + rb_1 + m(qk + rk_1)$$

$$= qb + rb_1 + M(m)$$

$$\therefore qa + ra_1 \equiv qb + rb_1 \pmod{m}$$

Corollary:

$$\text{If } a \equiv b \pmod{m}; a_1 \equiv b_1 \pmod{m}$$

$$a + a_1 \equiv b + b_1 \pmod{m}$$

$$a - a_1 \equiv b - b_1 \pmod{m}$$

In general if $a \equiv b \pmod{m}$,

$$a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m},$$

$$\text{then } a + a_1 + a_2 + \dots = b + b_1 + b_2 + \dots \pmod{m}.$$

$$2. \text{ If } a \equiv b \pmod{m}; a_1 \equiv b_1 \pmod{m}, \text{ then } aa_1 \equiv bb_1 \pmod{m}$$

$$a = b \pmod{m}$$

$$a = b + km$$

$$a_1 \equiv b_1 \pmod{m}$$

$$\therefore a_1 = b_1 + k_1 m$$

$$aa_1 = (b + km)(b_1 + k_1 m)$$

$$= bb_1 + m(kb_1 + k_1 b + kk_1 m)$$

$$\therefore aa_1 \equiv bb_1 \pmod{m}$$

Corollary: 1

If $a \equiv b \pmod{m}$, $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$ then

$$aa_1a_2..... \equiv bb_1b_2..... \pmod{m}.$$

Corollary: 2

If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$

Corollary: 3

If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$, if $f(x)$ is a polynomial in x .

3. These result show that congruences may be manipulated as regards addition, subtraction and multiplication with integral numbers, just like equations. As regards division a modification is necessary.

If $ax \equiv bx \pmod{m}$ and if h is H.C.F. of x , m then

$$a \equiv b \pmod{\left(\frac{m}{h}\right)}.$$

$x = ph, m = qh$ where p, q are co - prime.

$$ax \equiv bx \pmod{m}$$

$$\therefore ax - bx = km$$

$$\text{(i.e.,)} \quad aph - bph = kqh$$

$$\text{(i.e.,)} \quad a - b = k \cdot \frac{q}{p}$$

q is prime to p .

$\therefore a - b$ has q as a factor.

$$a - b = M(q) = M\left(\frac{m}{h}\right)$$

$$\therefore a \equiv b \pmod{\left(\frac{m}{h}\right)}$$

Corollary:

If $h = 1$, $a \equiv b \pmod{m}$

Thus the rule of cancellation holds for congruences on the condition that the cancelled factor is relatively prime to the modulus.

4. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $a \equiv b \pmod{m_3}$, ..., $a \equiv b \pmod{m_n}$, then $a \equiv b \pmod{m}$, where m is the least multiple of $m_1, m_2, \dots, m_n$.

$$a \equiv b \pmod{m_1}$$

$$\therefore a - b = \text{a multiple of } m_1$$

$$\text{Similarly } a - b = \text{a multiple of } m_2$$

$$a - b = \text{a multiple of } m_3$$

...

$$a - b = \text{a multiple of } m_n$$

To satisfy these equations $a - b = \text{a multiple of } m$ where m is the least common multiple of $m_1, m_2, \dots, m_n$.

$$\therefore a \equiv b \pmod{m}.$$

9.2 Criteria of Divisibility of Number

We can derive the criteria of divisibility of a number by 3, 9, 11 from the properties of congruences.

Let N be the number and let the digits in the units, tens, hundreds,... place be $a, b, c, d, \dots$

$$\text{Then } N = a + 10b + 100c + 1000d + \dots$$

$$1) \quad 10 \equiv 1 \pmod{3}$$

$$100 \equiv 1 \pmod{3}$$

$$1000 \equiv 1 \pmod{3}$$

.....

$$\therefore N = a + b + c + d + \dots \pmod{3}$$

$\therefore N$ is divisible by 3 iff the sum of its digits is divisible by 3.

$$2) \quad 10 \equiv 1 \pmod{9}$$

$$100 \equiv 1 \pmod{9}$$

$$1000 \equiv 1 \pmod{9}$$

.....

$$\therefore N = a + b + c + d + \dots \pmod{9}$$

Hence the number N is divisible by 9 iff the sum of its digit is divisible by 9.

$$3) \quad \text{We have } 10 \equiv -1 \pmod{11}$$

$$100 \equiv 1 \pmod{11}$$

$$1000 \equiv -1 \pmod{11}$$

.....

$$\therefore N = a - b + c - d + \dots \pmod{11}$$

Hence N is divisible by 11 iff the alternate sum $a - b + c - d + \dots$ of the digits is divisible by 11 or if $a - b + c - d + \dots = 0$ (i.e.,) $a + c + \dots = b + d + \dots$ (i.e.,) the sum of the odd digits is equal to sum of the even digits.

Corollary:

Since congruent numbers leave the same remainder when divided by the modulus, the preceding congruences can be used in finding remainders in divisions by 3, 9, 11.

Example: 1

Find a number having the remainders 5, 4, 3, 2 when divided by 6, 5, 4, 3 respectively.

Solution:

Let N be that number.

$$N \equiv 5 \pmod{6} \text{ (i.e.,) } N \equiv -1 \pmod{6}$$

$$N \equiv 4 \pmod{5} \text{ (i.e.,) } N \equiv -1 \pmod{5}$$

$$N \equiv 3 \pmod{4} \text{ (i.e.,) } N \equiv -1 \pmod{4}$$

$$N \equiv 2 \pmod{3} \text{ (i.e.,) } N \equiv -1 \pmod{3}$$

$$\therefore N \equiv -1 \pmod{\text{L.C.M. of } (6, 5, 4, 3)}$$

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

$\therefore$ The least value of N is 59.

N can take any value $-1 + 60k$ where k is a positive integer.

Example: 2

Find the remainder when 9^{10} is divided by 11.

Solution:

We have $9^2 \equiv 4 \pmod{11}$ (1)

$\therefore 9^8 \equiv 256 \pmod{11}$

Also $256 \equiv 3 \pmod{11}$

$\therefore 9 \equiv 3^8 \pmod{11}$ (2)

From (1) & (2) $9^{10} \equiv 4.3 \pmod{11}$

$$9^{10} \equiv 1 \pmod{11}$$

Hence the remainder is 1.

Example: 3

Show that $13^{2n+1} + 9^{2n+1}$ is divisible by 22.

Solution:

$$13^{2n+1} \equiv 13.(13)^{2n} = 13.(169)^n$$

$$\equiv 13.(22 \times 7 + 15)^n$$

$$\equiv 13.(15)^n \pmod{22}$$

$$9^{2n+1} = 9.81^n = 9(3 \times 22 + 15)^n$$

$$= 9.15^n \pmod{22}$$

$$\therefore 13^{2n+1} + 9^{2n+1} \equiv [13.15^n + 9.15^n] \pmod{22}$$

$$\equiv 22.15^n \pmod{22}$$

$$\equiv 0(\text{mod } 22).$$

$\therefore 13^{2n+1} + 92^{n+1}$ is divisible by 22.

Example: 4

Find the remainder when 2^{1000} is divisible by 17.

Solution:

$$2^4 = 16$$

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

$$(2^4)^{250} \equiv (-1)^{250} (\text{mod } 17)$$

$$\equiv 1 (\text{mod } 17)$$

$\therefore$ The remainder when 2^{1000} is divided by 17 is 1.

Example: 5

Find the remainder obtained by dividing 2^{46} by 47.

$$2^5 \equiv 32$$

$$\equiv -15 (\text{mod } 47)$$

$$2^{10} \equiv (-15)^2 (\text{mod } 47)$$

$$\equiv 225 (\text{mod } 47)$$

$$\equiv -10 (\text{mod } 47)$$

$$2^{20} \equiv (-10)^2 (\text{mod } 47)$$

$$\equiv 100 (\text{mod } 47)$$

$$\equiv 6 (\text{mod } 47)$$

$$2^{40} \equiv 36 \pmod{47}$$

$$\equiv -11 \pmod{47}$$

$$2^{45} \equiv 2^{40} \cdot 2^5$$

$$\equiv -11 \cdot -15 \pmod{47}$$

$$\equiv 165 \pmod{47}$$

$$\equiv 24 \pmod{47}$$

$$2 \times 2^{45} \equiv 48 \pmod{47}$$

$$\equiv 1 \pmod{47}$$

$\therefore$ The remainder is 1.

Example: 6

If p is a prime number and $p > 0$, then

$$(a + b)^p \equiv (a^p + b^p) \pmod{p}.$$

Solution:

$$(a + b)^p = a^p + pC_1 a^{p-1} b + \dots + pC_{p-1} a b^{p-1} + b^p$$

Now,
$$pC_r = \frac{p!}{r!(p-r)!} = \frac{p(p-1)!}{r!(p-r)!} \text{ is an integer.}$$

Since $r < p$ and p is prime, $r!$ and $(p-r)!$ do not divide p .

Hence $\frac{(p-1)!}{r!(p-r)!}$ is an integer.

$\therefore p$ divides pC_r

$$(a + b)^p = a^p + p^k + b^p \text{ where } k \in \mathbb{Z}$$

$$\therefore (a + b)^p \equiv (a^p + b^p) \pmod{p}$$

Example: 7

A natural number n is divisible by 3 iff the sum of its digits is divisible by 3.

Solution:

Let $a, b, c, d, \dots$ be the digits in the units, tens, hundreds, thousands, $\dots$ places.

Then $n = a + 10b + 100c + 1000d + \dots$

Now $1 \equiv 1 \pmod{3} \quad \therefore a \equiv a \pmod{3}$

$10 \equiv 1 \pmod{3} \quad \therefore 10b \equiv b \pmod{3}$

$100 \equiv 1 \pmod{3} \quad \therefore 100c \equiv c \pmod{3}$

$1000 \equiv 1 \pmod{3} \quad \therefore 1000d \equiv d \pmod{3}$

$\dots \dots \dots$

$n \equiv (a + b + c + d + \dots) \pmod{3}$

$\therefore n$ is divisible by 3 iff $a + b + c + d$ is divisible by 3.

Exercises:

1. a. Find the least two positive integers having the remainders 2, 3, 2 when divided by 3, 5, 7 respectively.
- b. Find the least positive number which when divided by 7, 8, 9 will leave remainders 1, 2, 3 respectively. Find the general formula for such numbers.
2. Find a multiple of 7 which has remainder 1 when divided by 2, 3, 4, 5 or 6.
3. Prove that $3^{4n+2} + 5^{2n+1}$ is divisible by 14.

4. Show that $3^{2n+1} + 2^{n+2}$ is divisible by 7.
5. Show that $7^{2n+1} + 1 = M(8)$
6. Show that $19^{2n} - 1 = M(360)$
7. Show that $23^{2n} - 1 = M(528)$
8. Show that $17^{2n} - 1 = M(288)$
9. Show that $3^{2n+4} - 2^{2n} = M(5)$
10. Show that $3^{2n-1} + 2^{n+1}$ is divisible by 7.

Answers:

1. (a) 128, 233 (b) $498; (504)k - 6$.
2. 301

9.3 Numbers in Arithmetical Progression:

If $x, x + a, x + 2a, \dots, x + (n - 1)a$, n terms of an arithmetical progression, are divided by n , where n is prime to a , the remainders are numbers $0, 1, 2, \dots, n - 1$ taken in certain order.

Let us assume that $x + pa$ and $x + qa$ when divided by n leave equal remainder r .

$$\text{Then } x + pa = k_1 n + r$$

$$x + qa = k_2 n + r$$

$$\therefore (p - q)a = (k_1 - k_2)n$$

$(p - q)$ is less than n .

$\therefore a$ is divisible by n which is contrary to the hypothesis that n is prime to a .

The remainders are all different and as each is less than n , they must be the numbers $0, 1, 2, \dots, n - 1$, taken in some order or other.

Corollary: 1

One of the numbers $x, x + a, \dots, x + (n-1)a$ is divisible by n .

Corollary: 2

If the progression is continued beyond the n^{th} term, the remainders recur in the same order.

Corollary: 3

If p is prime to a , then when $a, 2a, 3a, \dots, (p-1)a$ are divided by p , the remainders are $1, 2, \dots, (p-1)$ in some order or other.

Example:

Show that every integer which is a perfect cube is of the form $7p$ or $7p \pm 1$.

Proof:

An integer, N when it is divided by 7 has one of the remainders $0, 1, 2, 3, 4, 5, 6$. Every integer has one of the forms.

$$7m, 7m + 1, 7m + 2, 7m + 3, 7m + 4, 7m + 5, 7m + 6.$$

$$\text{(i.e.,)} \quad 7m, 7m + 1, 7m + 2, 7m + 3, 7m - 3, 7m - 2, 7m - 1$$

$$\text{(i.e.,)} \quad 7m, 7m \pm 1, 7m \pm 2, 7m \pm 3$$

$$(7m \pm r)^3 = (7m)^3 \pm 3(7m)^2 r + 3(7m)r^2 \pm r^3$$

$$= M(7) \pm r^3$$

Hence in the four possible cases we have

$$N^3 = (7m)^3 = M(7)$$

$$N^3 = (7m \pm 1)^3 = M(7) \pm 1$$

$$N^3 = (7m \pm 2)^3 = M(7) \pm 8 = M(7) \pm 1$$

$$N^3 = (7m \pm 3)^3 = M(7) \pm 27 = M(7) \pm 28 \mp 1 \\ = M(7) \pm 1$$

If every case therefore the cube has one or other of the form
 $7p$ or $7p \pm 1$

Theorem: 9.1

If x be congruent with r with respect to the modulus m ,
 $f(x)$ will be congruent with $f(r)$ with respect to modulus m where
 $f(x)$ is a polynomial in x .

Proof:

Let $f(x)$ be $p_0 + p_1x + p_2x^2 + \dots + p_nx^n$

x is congruent with r with respect to modulus m .

$\therefore x$ is of the form $qm + r$

By the binomial expansion, we have

$$\begin{aligned} & (qm + r)^n \\ &= (qm)^n + nC_1(qm)^{n-1}r + \dots + nC_{n-1}(qm)r^{n-1} + r^n \\ &= (q^n m^{n-1} + nC_1 q^{n-1} m^{n-2} r + \dots + nC_{n-1} q r^{n-1})m + r^n \\ &= M(m) + r^n \end{aligned}$$

Similarly,

$$(qm + r)^{n-1} = M(m) + r^{n-1} \text{ and so on.}$$

Hence

$$\text{if } x = qm + r$$

$$f(x) = f(qm + r)$$

$$= p_0 + p_1(qm + r) + p_2(qm + r)^2 + \dots + p_n(qm + r)^n$$

$$= p_0 + p_1r + p_2r^2 + \dots + p_nr^n + M(m)$$

$$= f(r) + M(m)$$

Hence $f(x)$ is congruent with $f(r)$ with respect to modulus m .

Corollary:

Since all integers are congruent (with respect to modulus m) with one or other of the series $0, 1, 2, \dots, m-1$, it follows that to test the divisibility of $f(x)$ by m for all integral values of x we need only test the divisibility by m of $f(0), f(1), f(2), \dots, f(m-1)$.

Example: 1

Show that $x^5 - x$ is divisible by 30.

Solution:

$$f(x) = x^5 - x = x(x^4 - 1)$$

$$f(0) = 0$$

$$f(1) = 0$$

$$f(2) = 2 \times 15 = 30$$

$$f(3) = 3 \times 80 = 240$$

$$f(4) = 4 \times 255 = 1020$$

$$f(5) = 5 \times 624 = 3120$$

$f(0), f(1), f(2), f(3), f(4)$ are divisible by 5.

$\therefore f(x)$ is divisible by 5.

$f(0), f(1), f(2), f(3), f(4), f(5)$ are divisible by 6.

$\therefore f(x)$ is divisible by 6.

$\therefore f(x)$ is divisible by both 5 and 6.

(i.e.,) $f(x)$ is divisible by 30.

Example: 2

If x, y, z be three consecutive integers, show that

$(\sum x)^3 - 3\sum x^3$ is divisible by 108.

Proof:

Since x, y, z are consecutive integers $y = x + 1, z = x + 2$

$$(\sum x)^3 - 3\sum x^3 = (3x + 3)^3 - 3\{x^3 + (x + 1)^3 + (x + 2)^3\}$$

$$= 18x^3 + 54x^2 + 36x$$

$$= 18x(x + 1)(x + 2)$$

Let $f(x)$ be $x(x + 1)(x + 2)$

$$f(0) = 0$$

$$f(1) = 6$$

$$f(2) = 24$$

Space for Hints

$f(0), f(1)$ are divisible by 2.

$\therefore f(x)$ is divisible by 2.

$f(0), f(1), f(2)$ are divisible by 3.

$\therefore f(x)$ is divisible by 3.

$\therefore f(x)$ is divisible by 6.

$\therefore \left(\sum x\right)^3 - 3\sum x^3$ is divisible by 108.

Exercises:

1. Show that every square is of the form $3m$ or $3m+1$
2. Show that every square is of the form $5m$ or $5m \pm 1$
3. Show that every cube is of the form $9m$ (or) $9m \pm 1$
4. Show that every fourth power is of the form $5m$ (or) $5m+1$
5. Show that 2^{2x+1} is divisible by 3.
6. Show that in order that $x^4 + 1$ may be divisible by 17, x should be of the form $17m \pm 2$ (or) $17m \pm 8$.
7. If n is a prime number greater than 3. Show that $n^2 - 1$ is divisible by 24.
8. If n is a prime number greater than 7, show that $n^6 - 1$ is divisible by 504. [Show that $n^6 - 1$ is divisible by 7, 8 and 9].

9.4 Fermat's Theorem:

Statement:

If p is a prime and a is any number prime to p then $a^{p-1} - 1$ is divisible by p .

Proof:

We have proved that if n is a prime number, then nc_r is divisible by n .

$$(a+1)^p = a^p + pC_1 \cdot a^{p-1} + pC_2 \cdot a^{p-2} + \dots + pC_r \cdot a^{p-r} + \dots + pC_{p-1} \cdot a + 1$$

(i.e.,)

$$(a+1)^p - (a^p + 1) = pC_1 \cdot a^{p-1} + pC_2 \cdot a^{p-2} + \dots + pC_r \cdot a^{p-r} + \dots + pC_{p-1} \cdot a$$

Since p is prime $pC_1, pC_2, \dots, pC_{p-1}$ are divisible by p .

$$\therefore (a+1)^p - (a^p + 1) = \text{a multiple of } p$$

$$\therefore (a+1)^p \equiv (a^p + 1) \pmod{p}$$

Since this result is true for all values of a , replacing a by $a-1, a-2, a-3, \dots, 3, 2, 1$ in succession we get

$$a^p \equiv [(a-1)^p + 1] \pmod{p} \quad (1)$$

$$(a-1)^p \equiv [(a-2)^p + 1] \pmod{p} \quad (2)$$

$$(a-2)^p \equiv [(a-3)^p + 1] \pmod{p} \quad (3)$$

$$\dots \dots \dots$$

$$3^p \equiv [2^p + 1] \pmod{p} \quad (a-2)$$

$$2^p \equiv [1^p + 1] \pmod{p} \quad (a-1)$$

Adding all the equations (1), (2), (3).... $(a-1)$ we get

$$a^p + (a-1)^p + (a-2)^p + \dots + 3^p + 2^p \equiv [(a-1)^p + 1 + (a-2)^p + 1 + (a-3)^p + 1 + \dots + 2^p + 1 + 1^p + 1] \pmod{p}$$

Since we are adding $a-1$ equations, we have

$$a^p + (a-1)^p + (a-2)^p + \dots + 3^p + 2^p \equiv [(a-1)^p + (a-2)^p + \dots + 2^p + 1^p + a-1]$$

(mod p)

$$\text{(i.e.,)} \quad a^p \equiv [1 + (a - 1)] \pmod{p}$$

$$\text{(i.e.,)} \quad a^p \equiv a \pmod{p}$$

$$\text{(i.e.,)} \quad a^p - a \text{ is divisible by } p$$

$$\text{(i.e.,)} \quad a(a^{p-1} - 1) \text{ is divisible by } p.$$

Since a is prime to p, $a^{p-1} - 1$ is divisible by p.

II Method:

$$(x + y)^p = x^p + pC_1 x^{p-1} y + pC_2 x^{p-2} y^2 + \dots + pC_{p-1} x y^{p-1} + y^p$$

$pC_1, pC_2, \dots, pC_{p-1}$ are divisible by p.

$$\therefore (x + y)^p \equiv (x^p + y^p) \pmod{p}$$

$$(x + y + z)^p \equiv (x + y)^p + pC_1 (x + y)^{p-1} z + \dots + z^p$$

$$\equiv [(x + y)^p + z^p] \pmod{p}$$

$$\equiv (x^p + y^p + z^p) \pmod{p}$$

So in general

$$(x + y + z + \dots + w)^p \equiv (x^p + y^p + z^p + \dots + w^p) \pmod{p}$$

Where $x, y, z, \dots, w$ are any integers.

Let there be a integers $x, y, z, \dots, w$.

Put each equal to 1.

$$\text{Then } (1 + 1 + \dots \text{a terms})^p = (1^p + 1^p + \dots 1^p) \pmod{p}$$

$$\therefore a^p \equiv a \pmod{p}$$

(i.e.,) $a^p - a$ is divisible by p .

$\therefore a^{p-1} - 1$ is divisible by p .

III Method:

When $a, 2a, 3a, \dots, (p-1)a$ are divided by p , the remainders are $1, 2, \dots, p-1$ in certain order since p is prime to a .

$$a \equiv r_1 \pmod{p}$$

$$2a \equiv r_2 \pmod{p}$$

$$3a \equiv r_3 \pmod{p}$$

$$\dots\dots\dots$$

$$\dots\dots\dots$$

$$(p-1)a \equiv r_{p-1} \pmod{p}$$

Here $r_1, r_2, r_3, \dots, r_{p-1}$ are $1, 2, 3, \dots, p-1$ in a certain order.

$$\therefore a.2a.3a\dots(p-1)a \equiv r_1 r_2 r_3 \dots r_{p-1} \pmod{p}$$

$$(i.e.,) \quad (p-1)! a^{p-1} \equiv 1.2.3\dots(p-1) \pmod{p}$$

$$(i.e.,) \quad (p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$$

$$(i.e.,) \quad (p-1)! a^{p-1} - (p-1)! \equiv 0 \pmod{p}$$

$\therefore (p-1)! (a^{p-1} - 1)$ is divisible by p .

But $(p-1)!$ is not divisible by p , since p is prime.

$\therefore a^{p-1} - 1$ is divisible by p .

Corollary: 1

$a^p - a$ is divisible by p if p is prime and a is prime to p .

Corollary: 2

If p is an odd prime and a is prime to p , then $a^{\frac{1}{2}(p-1)} \pm 1$ is divisible by p .

$$a^{p-1} - 1 = \left\{ a^{\frac{1}{2}(p-1)} - 1 \right\} \left\{ a^{\frac{1}{2}(p-1)} + 1 \right\}$$

$a^{p-1} - 1$ is divisible by p .

$a^{\frac{1}{2}(p-1)} - 1$ or $a^{\frac{1}{2}(p-1)} + 1$ is divisible by p .

(i.e.,) $a^{\frac{1}{2}(p-1) \pm 1} \pm 1$ is divisible by p .

Example: 1

Show that if x and y are both prime to the prime number n , then $x^{n-1} - y^{n-1}$ is divisible by n . Deduce that $x^{12} - y^{12}$ is divisible by 1365.

Solution:

$x^{n-1} - 1 \equiv 0 \pmod{n}$ since x is prime to n and n is prime.

Similarly $y^{n-1} - 1 \equiv 0 \pmod{n}$

Subtracting we get $x^{n-1} - y^{n-1} \equiv 0 \pmod{n}$

$$x^{12} - y^{12} = x^{13-1} - y^{13-1}$$

$$\equiv 0 \pmod{13}$$

$$\therefore x^{12} - y^{12} = (x^6 - y^6)(x^6 + y^6)$$

But $x^6 - y^6 \equiv 0 \pmod{7}$

$x^6 - y^6$ is divisible by 7.

(i.e.,) $x^{12} - y^{12}$ is divisible by 7.

$$x^{12} - y^{12} = (x^4 - y^4)(x^8 + x^4y^4 + y^8)$$

By $x^4 - y^4 \equiv 0 \pmod{5}$

$\therefore x^{12} - y^{12}$ is divisible by 5.

$$x^{12} - y^{12} = (x^2 - y^2)(x^4 + x^2y^2 + y^4)(x^6 + y^6)$$

But $x^2 - y^2 \equiv 0 \pmod{3}$

$\therefore x^{12} - y^{12}$ is divisible by 3.

$\therefore x^{12} - y^{12}$ is divisible by 13, 7, 5 and 3.

(i.e.,) it is divisible by $13 \times 7 \times 5 \times 3$

(i.e.,) by 1365

Example: 2

Show that the 8th power of any number is of the form $17m$ or $17m \pm 1$.

Solution:

Let the number be N .

N may be prime to 17 or may not be prime to 17.

If N is not prime to 17, it must be a multiple of 17, since 17 is a prime number.

In that case N is a multiple of 17.

$\therefore N^8$ is of the form $17m$.

If N is prime to 17 ,

$N^{17-1} - 1$ is divisible by 17 .

(i.e.,) N^{16-1} is divisible by 17 .

(i.e.,) $(N^8 + 1)(N^8 - 1)$ is divisible by 17 .

$\therefore N^8 + 1$ or $N^8 - 1$ is divisible by 17 .

$\therefore N^8 + 1$ or $N^8 - 1$ is a multiple of 17 .

$\therefore N^8 + 1 = 17m$ (or) $N^8 - 1 = 17m$

(i.e.,) $N^8 = 17m \pm 1$

Hence N^8 is one of the forms $17m$ (or) $17m \pm 1$.

Another Method:

Since 17 is a prime number.

$$a^{17} \equiv a \pmod{17}$$

$$\therefore \frac{17}{a^{17} - a}$$

$$\therefore \frac{17}{a(a^8 - 1)(a^8 + 1)}$$

$$\therefore \frac{17}{a} \text{ (or) } \frac{17}{a^8 - 1} \text{ (or) } \frac{17}{a^8 + 1}$$

Hence a^8 is of the form $17m$ (or) $17m \pm 1$.

Example: 3

Prove that the 5th power of any integer N has the same units digit as N .

Solution:

By Fermat's theorem, $N^5 - N$ is divisible by 5.

$$\therefore N^5 - N = M(5)$$

$$\text{(i.e.,)} \quad N(N^4 - 1) = M(5)$$

$$\text{(i.e.,)} \quad N(N^2 + 1)(N + 1)(N - 1) = M(5)$$

Since N is any integer, either N or $N - 1$ is divisible by 2.

$$\therefore N^5 - N = \text{a multiple of } 10.$$

$$\text{(i.e.,)} \quad N^5 = M(10) + N$$

N can be put in the form $10p + q$ where $q < 10$

$$\therefore N^5 = M(10) + 10p + q$$

$$= M(10) + q$$

$\therefore N^5$ has the same units digit q as that of N .

Example: 4

Find the remainder when 2^{460} is divided by 47.

Solution:

$$2^{46} \equiv 1 \pmod{47} \text{ (Fermat's Theorem)}$$

$$\therefore (2^{46})^{10} \equiv 1^{10} \pmod{47}$$

$$\therefore 2^{460} \equiv 1 \pmod{47}$$

Hence the remainder is 1.

Example: 5

Find the remainder when 2^{1000} is divided by 13.

Solution:

$$2^{12} \equiv 1 \pmod{13} \text{ (Fermat's Theorem)}$$

$$\therefore (2^{12})^{83} \equiv 1 \pmod{13}$$

$$\therefore (2^{996}) \equiv 1 \pmod{13}$$

Also, $2^4 \equiv 3 \pmod{13}$

$$\therefore 2^{1000} \equiv 3 \pmod{13}$$

Hence the remainder is 3.

Example: 6

If a and b are prime to n , show that $\frac{n}{(a^{n-1} - b^{n-1})}$

Solution:

Since $(a, n) = 1$, by Fermat's theorem

$$a^{n-1} \equiv 1 \pmod{n}$$

Similarly $b^{n-1} \equiv 1 \pmod{n}$

Hence $a^{n-1} - b^{n-1} \equiv 0 \pmod{n}$

$$\therefore \frac{n}{(a^{n-1} - b^{n-1})}$$

Exercises:

1. Show that $n^5 - n$ is divisible by 30.
2. Show that $n^7 - n$ is divisible by 42.
3. Show that $n^{13} - n$ is divisible by 2730.
4. Show that if n is any prime number greater than 19, then $n^{18} - 1$ is divisible by 9576.
5. Show that the 4th power of any number is of the form $5m$ (or) $5m + 1$.
6. Show that the 12th power of any number is of the form $13m$ (or) $13m + 1$.
7. Show that the 9th power of any number is one of the forms $19m$ or $19m \pm 1$.
8. Show that if n be a prime number

$$1^{n-1} + 2^{n-1} + 3^{n-1} + \dots + (n-1)^{n-1} + 1 = M(n)$$
9. Show that if m and n are primes, then $m^{n-1} + n^{m-1} - 1 \equiv 0 \pmod{mn}$
10. Show that if m , n and p are prime, then

$$(np)^{m-1} + (pm)^{n-1} + (mn)^{p-1} - 1 \equiv 0 \pmod{mnp}$$
11. If n be prime and $x > 1$ show that

$$x^{n-2} + x^{n-3} + x^{n-4} + \dots + x + 1 \equiv 0 \pmod{n}$$
12. If n be an odd prime, show that

$$1 + 2(n+1) + 2^2(n+1)^2 + \dots + 2^{n-2}(n+1)^{n-2} \equiv 0 \pmod{n}$$
13. If n be odd, show that $1^n + 2^n + \dots + (n-1)^n \equiv 0 \pmod{n}$
14. If n is of the form $4m + 1$, show that a^n ends with the same digit as a for all values of a .

[Hint:

$$f(m) = a(a^{4m} - 1), f(0) = 0; f(1) = a(a^4 - 1); f(2) = a(a^8 - 1); f(3) = a(a^{12} - 1);$$

$$f(4) = a(a^{16} - 1)$$

$a(a^4 - 1)$ is a factor of $f(0), f(1), f(2), f(3), f(4)$. $a^4 - 1$ is divisible by 5.

$a(a^4 - 1) = a(a + 1)(a - 1)(a^2 + 1)$ is so divisible by 2.

$\therefore a(a^4 - 1)$ is divisible by 10.

$\therefore f(m)$ is dividid by 10].

UNIT – 10

GENERALIZATION OF FERMAT'S THEOREM

10.1 Generalization of Fermat's Theorem

Statement:

If n is any number and a is prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof:

Let $a_1, a_2, \dots, a_{\phi(n)}$ be the $\phi(n)$ integers less than n and prime to it.

Consider the products $aa_1, aa_2, \dots, aa_{\phi(n)}$

Let k be the remainder when aa_r is divided by n .

Then $aa_r = M(n) + k$ (1)

Since a and a_r are prime to n and k is also prime to n .

Hence the remainder is prime to n .

Suppose the product aa_s gives the same remainder k when it is divided by n .

Then $aa_s = M(n) + k$ (2)

From (1)&(2), we get $a(a_r - a_s) = M(n)$

(i.e.) $a(a_r - a_s)$ is a multiple of n which cannot be the case

since $a_r - a_s < n$ and a is prime to n .

$\therefore aa_r$ and aa_s will not give the same remainder when they are divided by n . Hence when the products $aa_1, aa_2, \dots, aa_{\phi(n)}$ are divided by n the remainders $k_1, k_2, \dots, k_n$ are all different and prime to n .

$\therefore$ They are $a_1, a_2, \dots, a_{\phi(n)}$ is some order.

$$aa_1 \equiv k_1 \pmod{n}$$

$$aa_2 \equiv k_2 \pmod{n}$$

$$\dots\dots\dots$$

$$\dots\dots\dots$$

$$aa_{\phi(n)} \equiv k_{\phi(n)} \pmod{n}.$$

$$\therefore aa_1, aa_2, \dots, aa_{\phi(n)} \equiv k_1 k_2 \dots k_{\phi(n)} \pmod{n}$$

$$(ie) a^{\phi(n)} a_1 a_2 \dots a_{\phi(n)} \equiv a_1 a_2 \dots a_{\phi(n)} \pmod{n}$$

Dividing by $a_1, a_2, \dots, a_{\phi(n)}$ which is prime to n .

we get

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Corollary:

If n is a prime number, then $\phi(n) = n - 1$. Then this theorem reduces to Fermat's theorem.

Exercises:

1. If $\alpha, \beta, \gamma, \dots$ be primes and $N = \alpha\beta\gamma, \dots$ then show that

$$\sum \left(\frac{N}{\alpha} \right)^{\alpha-1} \equiv 1 \pmod{\alpha\beta\gamma, \dots}$$

2. Show that $16^{99} \equiv 1 \pmod{437}$

[Hint $16^{99} = 2^{4 \times 99}$ and $\phi(437) = 437 \left(1 - \frac{1}{19}\right) \left(1 - \frac{1}{23}\right)$ and

use extension of Fermat's theorem]

3. Show that $x^{pq-q} \equiv 1 \pmod{pq}$ if x is prime to p , p is prime and $q = p^n$

4. Find the remainder obtained in dividing 2^{460} by 47.

5. When $p+1$ and $2p+1$ are both prime numbers, show that $x^{2p} - 1$ is divisible by $8(p+1)(2p+1)$ where x is prime to 2, $p+1$ and $2p+1$.

10.2 Wilson's Theorem:

Statement:

If P is a prime number, then $(p-1)! + 1$ is divisible by p .

Proof:

If a is any number of the series $1, 2, \dots, (p-1)$ where p is a prime then when $a, 2a, 3a, \dots, (p-1)a$ are divided by p the remainders are $1, 2, 3, \dots, p-1$ in some order or other.

Hence there is only one number say, a_1 among the number $1, 2, \dots, p-1$ such that when aa_1 is divided by p , the remainder is 1.

$$\therefore aa_1 \equiv 1 \pmod{p}$$

Such two numbers are called associate residues.

Suppose $a = a_1$ then $a^2 \equiv 1 \pmod{p}$

$$\text{(i.e.,)} \quad a^2 - 1 \equiv 0 \pmod{p}$$

$$\text{(i.e.,)} \quad (a+1)(a-1) \equiv 0 \pmod{p}$$

$\therefore$ Either $a + 1$ is divisible by p (or) $a = 1$.

Since a is less than p , $a + 1 = p$ (or) $a = 1$.

(i.e.,) $a = p - 1$ (or) 1 .

Hence numbers which are identical with their associate residues are 1 and $p - 1$. Excluding these 2 numbers 1 and $p - 1$, the remaining numbers $2, 3, 4, \dots, p - 2$ can be grouped into $\frac{p-3}{2}$ pairs of associate residues such that the product of each pair is congruent with 1 .

$$\therefore 2 \cdot 3 \cdot \dots \cdot (p - 2) \equiv 1 \pmod{p} \quad (1)$$

$$\text{We also have } 1 \cdot (p - 1) \equiv -1 \pmod{p} \quad (2)$$

Multiplying (1) & (2) we get,

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p - 2) \cdot (p - 1) \equiv -1 \pmod{p}$$

$$\text{(i.e.,)} \quad (p - 1)! + 1 \equiv 0 \pmod{p}$$

(i.e.,) $(p - 1)! + 1$ is divisible by p .

10.3 Lagrange's Theorem

Statement:

If $(x + 1)(x + 2) \dots (x + p - 1) = x^{p-1} + A_1 x^{p-2} + \dots + A_{p-2} x + A_{p-1}$ and p be prime, then $A_1, A_2, \dots, A_{p-2}$ are all divisible by p .

Proof:

Changing x into $x + 1 \dots$ we get

$$(x + 2)(x + 3) \dots (x + p) (x + 1)^{p-1} + A_1 (x + 1)^{p-2} + \dots + A_{p-2} (x + 1) + A_{p-1}.$$

$$\therefore (x + 1)(x + 2)(x + 3) \dots (x + p)$$

$$= (x+1)\{x+1\}^{p-1} + A_1(x+1)^{p-2} + \dots + A_{p-2}(x+1) + A_{p-1}\}$$

$$= (x+1)^p + A_1(x+1)^{p-1} + \dots + A_{p-2}(x+1)^2 + A_{p-1}(x+1)$$

$$\therefore (x+p)\{x^{p-1} + A_1x^{p-2} + A_2x^{p-3} + \dots + A_{p-2}x + A_{p-1}\}$$

$$= (x+1)^p + A_1(x+1)^{p-1} + \dots + A_{p-2}(x+1)^2 + A_{p-1}(x+1)$$

(i.e.,)

$$x^p + A_1x^{p-1} + A_2x^{p-2} + \dots + A_{p-2}x^2 + A_{p-1}x + p.x^{p-1} + A_1px^{p-2} + \dots + A_{p-2}p.x + pA_{p-1}$$

$$= (x+1)^p + A_1(x+1)^{p-1} + \dots + A_{p-2}(x+1)^2 + A_{p-1}(x+1)$$

$\therefore$

$$\{(x+1)^p - x^p\} + A_1\{(x+1)^{p-1} - x^{p-1}\} + A_2\{(x+1)^{p-2} - x^{p-2}\} + \dots + A_{p-1}\{(x+1) - x\}$$

$$= px^{p-1} + A_1px^{p-2} + \dots + A_{p-2}x + A_{p-1}$$

Equating the coefficient of $x^{p-2}, x^{p-3}, \dots$, we get

$$pA_1 = pC_2 + (p-1)C_1A_1$$

$$pA_2 = pC_3 + (p-1)C_2 + A_1(p-2)C_1A_2$$

$$pA_3 = pC_4 + (p-1)C_3A_1 + (p-2)C_2A_2 + (p-3)C_1A_3$$

$$\dots\dots\dots$$

$$\dots\dots\dots$$

$$pA_{p-1} = 1 + A_1 + A_2 + \dots + A_{p-2} + A_{p-1}$$

Since $(p-1)C_1, (p-2)C_2, (p-3)C_3, \dots$ are not divisible by

p , if p is prime, we get by successive steps that

$A_1, A_2, A_3, \dots, A_{p-2}$ are all divisible by p .

Corollary: 1

$$(x+1)(x+2)\dots(x+p-1) = x^{p-1} + A_1 x^{p-2} + \dots + A_{p-2} x + A_{p-1}$$

Put $x = 0$, we get $A_{p-1} = (p-1)!$

Put $x = 1$, we get $2, 3, \dots, p = 1 + A_1 + \dots + A_{p-2} + A_{p-1}$

$$\therefore A_{p-1} + 1 = p! - (A_1 + \dots + A_{p-2})$$

$$\text{(i.e.,)} \quad (p-1)! + 1 = p! - (A_1 + \dots + A_{p-2})$$

The left side is divisible by p .

$\therefore (p-1)! + 1$ is divisible by p .

This is Wilson's Theorem.

Corollary: 2

$$\begin{aligned} x(x+1)(x+2)\dots(x+p-1) &= x(x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + \dots + A_{p-2} x + A_{p-1}) \\ &= x^p + A_1 x^{p-1} + A_2 x^{p-2} + \dots + A_{p-2} x^2 + A_{p-1} x \end{aligned}$$

$$= (x^p - x) + A_1 x^{p-1} + A_2 x^{p-2} + \dots + A_{p-2} x^2 + (A_{p-1} + 1)x$$

$$\begin{aligned} x^p - x &= x(x+1)(x+2)\dots(x+p-1) - \{A_1 x^{p-1} + A_2 x^{p-2} + \dots \\ &\quad + A_{p-2} x^2\} - (A_{p-1} + 1)x \end{aligned}$$

$x(x+1)(x+2)\dots(x+p-1)$ being the product of p consecutive integers, must be divisible by p . Also if p be prime $A_{p-1} + 1, A_1, A_2, \dots, A_{p-2}$ are divisible by p .

$\therefore x^p - x$ is divisible by p if p be prime.

This is Fermat's theorem.

Corollary: 3

If p is a prime greater than 3, then A_{p-2} is a multiple of p^2 .

If the lagrange's theorem substitute the values of p and $-2p$ instead of x

We get

$$(p+1)(p+2)\dots(2p-1) = A_{p-1} + A_{p-2}p + \dots + p^{p-1} \quad (1)$$

$$(-2p+1)(-2p+2)\dots(-2p+p-1) = (-2p)^{p-1} + A_1(-2p)^{p-2} + \dots + A_{p-2}(-2p) + A_{p-1}$$

$$\text{(i.e.,)} \quad (2p-1)(2p-2)\dots(p+2)(p+1)(-1)^{p-1}$$

$$= (-1)^{p-1} \{ (2p)^{p-1} - A_1(2p)^{p-2} + \dots + A_{p-1} \}$$

Since there are p terms on the right side and p is odd.

$$\therefore (p+1)(p+2)\dots(2p-1) = A_{p-1} - 2pA_{p-2} + \dots + (2p)^{p-1} \quad (2)$$

Subtracting (2) from (1) we get

$$0 = 3p.A_{p-2} - 3p^2.A_{p-3} + \text{a multiple of } p^4.$$

Since $A_{p-1}, A_{p-2}, A_{p-3}, \dots$ are divisible by p .

$$\therefore 3p A_{p-2} = 3p^2 A_{p-3} - M(p^4)$$

$$\therefore A_{p-2} = pA_{p-3} - \frac{1}{3}M(p^3)$$

A_{p-3} is a multiple of p and $p > 3$.

A_{p-2} is a multiple of p^2 .

Corollary: 4

$(p-1)! \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right)$ is a multiple of p^2 .

In cor. 3 we have learnt that $A_{p-2} = M(p^2)$

$$\begin{aligned} A_{p-2} &= \text{Coeff. of } x \text{ in } (x+1)(x+2)\dots(x+p-1) \\ &= (2.3\dots p-1) + (1.3.4\dots p-1) + \dots (1+2\dots p-2) \\ &= (p-1)! \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right) \end{aligned}$$

Hence the result.

Example: 1

Show that $(18)!+1$ is divisible by 437

Solution:

19 is a prime number.

$\therefore (19-1)!+1$ is divisible by 19.

(i.e.,) $(18)!+1$ is divisible by 19.

23 is a prime number.

$\therefore (22)!+1$ is divisible by 23.

$$\text{(i.e.,)} \quad 22.21.20.19(18)!+1 = M(23)$$

$$\text{(i.e.,)} \quad (23-1)(23-2)(23-3)(23-4)(18)!+1 = M(23)$$

$$\text{(i.e.,)} \quad \{M(23) + 1.2.3.4\} (18)!+1 = M(23)$$

$$\text{(i.e.,)} \quad \{M(23) + 1\} (18)!+1 = M(23)$$

$$(i.e.,) \quad \{M(23) + 1\} (18)! + 1 = M(23)$$

$$(i.e.,) \quad \{M(23) (18)! + (18)!\} + 1 = M(23)$$

$\therefore (18)! + 1$ is divisible by 23.

$\therefore (18)! + 1$ is divisible by 19×23

(i.e.,) $(18)! + 1$ is divisible by 437.

Example: 2

If p is a prime number and $p = 4m + 1$ where m is a positive integer, prove that $\{(2m)!\}^2 + 1$ is divisible by p .

Solution:

Since p is a prime number,

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad (4m+1-1)! + 1 = 0 \pmod{p}$$

$$(i.e.,) \quad (4m)! + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad (2m)!(2m+1)(2m+2)\dots(4m) + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad (2m)!\{p-2m\}(p-2m-1)\dots(p-1) + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad (2m)!\{M(p) + (2m)!\} + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad M(p) + \{(2m)!\}^2 + 1 \equiv 0 \pmod{p}$$

$$\therefore \{(2m)!\}^2 + 1 \equiv 0 \pmod{p}$$

Example: 3

If $M = 1.3.5\dots(p-2)$ where p is an odd prime, show that

$$M^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Solution:

Since p is a prime number.

$$\therefore (p-1)! + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad 1.2.3.....(p-1) + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad 1.3.5...(p-2)p-2).2.4.6...(p-1) + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad 1.3.5...(p-2)\{p-p-2)(p-p-4)...(p-1)\} + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad 1.3.5...(p-2) \{M(p) + (-1)(p-1)/2(p-2)(p-4)...3.1\} + 1 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad 1.3.5...(p-2)M(p) + (-1)(p-1)/2 \cdot 1^2.3^2.5^2...(p-2)^2 + 1 \equiv 0 \pmod{p}$$

$$\therefore \quad (-1)(p-1)/2 \cdot 1^2.3^2.5^2...(p-2)^2 + 1 \equiv 0 \pmod{p}$$

Multiplying throughout by (-1)

We get,

$$(-1)^{p-1} \cdot 1^2.3^2.5^2...(p-2)^2 + (-1)(p-1)/2 \equiv 0 \pmod{p}$$

p is an odd prime

$\therefore p-1$ is even

$$\therefore \quad M^2 + (-1)(p-1)/2 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad M^2 - (-1)(p+1)/2 \equiv 0 \pmod{p}$$

$$(i.e.,) \quad M^2 \equiv (-1)(p+1)/2 \pmod{p}$$

Example: 4

Show that if n is a prime number and $r < n$, $(n-r)!(r-1)! + (-1)^{r-1} \equiv 0 \pmod{n}$

Deduce that $\left\{ \left[\frac{1}{2}(n-1) \right]! \right\}^2 + (-1)(n-1)/2 \equiv 0 \pmod{n}$

Solution:

n is a prime number

By Wilson's Theorem, $(n-1)! + 1 \equiv 0 \pmod{n}$

(i.e.,) $(n-r)!(n-r+1)(n-r+2)\dots(n-1) + 1 \equiv 0 \pmod{n}$

(i.e.,) $(n-r)!(n-r-1)(n-r-2)\dots(n-1) + 1 \equiv 0 \pmod{n}$

(i.e.,) $(n-r)\{M(n) - (-1)^{r-1}(r-1)!\} + 1 \equiv 0 \pmod{n}$

Where $M(n)$ is a multiple of n .

(i.e.,) $M(n)(n-r)! - (-1)^{r-1}(n-r)!(r-1)! + 1 \equiv 0 \pmod{n}$

$\therefore (-1)^{r-1}(n-r)!(r-1)! + 1 \equiv 0 \pmod{n}$

Multiplying throughout by $(-1)^{r+1}$, we get

$(-1)^{2r}(n-r)!(r-1)! + (-1)^{r+1} \equiv 0 \pmod{n}$

(i.e.,) $(n-r)!(r-1)! + (-1)^{r+1} \equiv 0 \pmod{n}$

Put $r = \frac{n+1}{2}$ in the above result.

We get, $\left(n - \frac{n+1}{2} \right) \left(\frac{n+1}{2} - 1 \right)! + (-1)(n-1)/2 \equiv 0 \pmod{n}$

(i.e.,) $\left(\frac{n-1}{2} \right) \left(\frac{n-1}{2} \right)! + (-1)(n-1)/2 \equiv 0 \pmod{n}$

(i.e.,) $\left\{ \left(\frac{n-1}{2} \right)! \right\}^2 + (-1)(n-1)/2 \equiv 0 \pmod{n}$

Example: 5

Show that $28!+233 \equiv 0 \pmod{899}$

Solution:

$$899 = 29 \cdot 31$$

Now $28! + 1 \equiv 0 \pmod{29}$ (Wilson's Theorem)

$$\therefore 28! + 1 + 29(8) \equiv 0 \pmod{29}$$

$$\therefore 28! + 233 \equiv 0 \pmod{29} \quad (1)$$

Now $30! + 1 \equiv 0 \pmod{31}$ (Wilson's Theorem)

$$\therefore 30 \cdot 29 \cdot 28! + 1 \equiv 0 \pmod{31}$$

$$\therefore (31-1)(31-2)28! + 1 + 31 \equiv 0 \pmod{31}$$

$$\therefore (-1)(-2)28! + 32 \equiv 0 \pmod{31}$$

$$\therefore 28! + 16 \equiv 0 \pmod{31} \text{ (since } (2, 31) = 1)$$

$$\therefore 28! + 16 + 7 \cdot 31 \equiv 0 \pmod{31}$$

$$28! + 233 \equiv 0 \pmod{31} \quad (2)$$

From (1) & (2) we get $28! + 233 \equiv 0 \pmod{899}$

Since $(31, 29) = 1$.

Example: 6

Show that $7^{2n} + 16n - 1 \equiv 0 \pmod{64}$

Solution:

$$\begin{aligned}
 7^{2n} + 16n - 1 &= (1-8)^{2n} + 16n - 1 \\
 &= (1 - 2nc_1 \cdot 8 + 2nc_2 \cdot 8^2 - \dots + 8^{2n}) + 16n - 1 \\
 &= 1 - 16n + (\text{a multiple of } 64) + 16n - 1 \\
 &= \text{a multiple of } 64.
 \end{aligned}$$

$$\text{Hence } 7^{2n} + 16n - 1 \equiv 0 \pmod{64}.$$

Example: 7

Show that $3^{2n+2} + 2^{n+1} \equiv 0 \pmod{7}$

Solution:

The result is true for $n = 1$

Let it be true when $n = m$. Then

$$3^{2m+1} + 2^{m+2} \equiv 0 \pmod{7}$$

$$\begin{aligned}
 \text{Now, } 3^{2(m+1)+1} + 2^{(m+1)+2} &= 9 \cdot 3^{2m+1} + 2 \cdot 2^{m+2} \\
 &= 2[3^{2m+1} + 2^{m+2}] + 7 \cdot 3^{2m+1} \\
 &= \text{a multiple of } 7.
 \end{aligned}$$

Hence the result follows by induction.

Example: 8

Prove that for any integer n , $n^5 - n$ is divisible by 30.

Solution:

$$n^5 - n = n(n^4 - 1) = (n-1)n(n+1)(n^2 + 1)$$

Space for Hints

Now $n-1, n, n+1$ are three consecutive integers and hence the product. $(n-1)(n+1)n$ is divisible by 6.

Therefore $n^5 - n$ is divisible by 6 (1)

Also by Fermat's theorem, $n^4 - 1 \equiv 0 \pmod{5}$

Hence $n^4 - 1$ is divisible by 5.

$\therefore n^5 - n$ is divisible by 5 (2)

Now, since 5 and 6 are relatively prime, $n^5 - n$ is divisible by 30.

Exercises:

1. If p is a prime number, show that $2(p-3)!+1$ is divisible by p .
2. Prove that $712!+1 \equiv 0 \pmod{719}$
3. Show that (1) $28!+233$ is divisible by 899, (2) $28! \equiv 666 \pmod{899}$
4. Show that $18! - 22 \equiv M(46)$
5. Show that any prime of the form $4n+1$ is a divisor of a number of the form $1+k^2$.
6. If p is a prime of the form $4m-1$, show that $\{(2m-1)!\}^2 - 1 \equiv 0 \pmod{p}$.
7. If p is an odd prime, show that $\left(1, 2, 3, \dots, \frac{p-1}{2}\right)^2 + (-1)^{p-1/2} \equiv 0 \pmod{p}$.

[Hint: If p is an odd prime

$$\frac{p+1}{2} = p - \frac{p-1}{2} \equiv -\frac{p-1}{2} \pmod{p}$$

$$\frac{p+3}{2} = p - \frac{p-3}{2} \equiv \frac{p-3}{2} \pmod{p}$$

.....

$$p-1 = p-1 = -1 \pmod{p}$$

$$\therefore \frac{p+1}{2} \frac{p+3}{2} \dots (p-1) \equiv (-1)(p-1)/2 \cdot 1 \cdot 2 \cdot 3 \dots, \pmod{p}$$

$$(p-1)!+1 \equiv 0 \pmod{p}.$$

$$(\text{i.e.,}) 1 \cdot 2 \cdot 3 \dots, \frac{p-1}{2}, \frac{p+1}{2}, \frac{p+3}{2} \dots (p-1)+1 \equiv 0 \pmod{p}].$$

