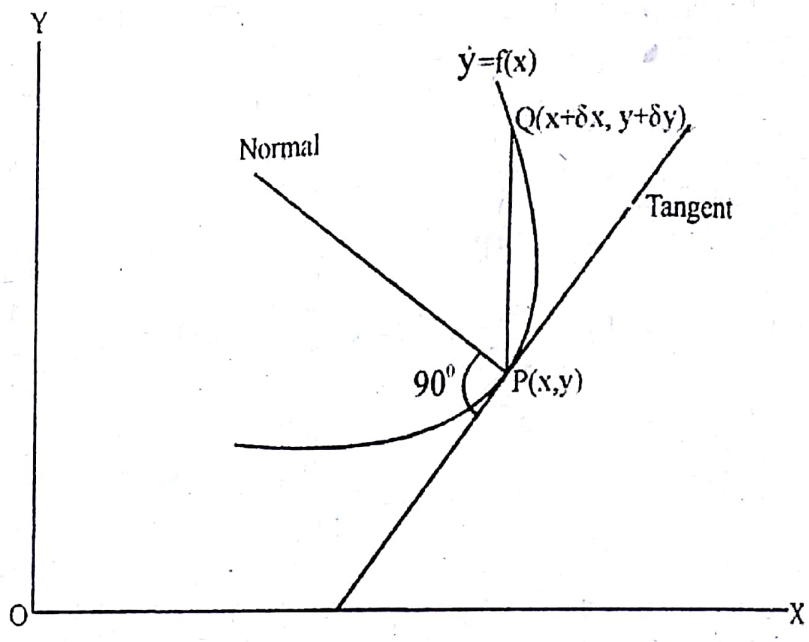
3

Tangents and Normals

3.1 Definition.

Tangent : Let P(x,y) and Q(x + δx, y+δy) be two neighbouring points on any curve y = f(x). The chord PQ, in the limiting position, when Q approaches P along the curve, is called tangent to the curve at point P.



Normal : The line perpendicular to tangent at P is called normal to the curve at point P.

3.2 Equation of tangent.

Let P(x,y) and Q(x + δx, y + δy) be two neighbouring points of the curve y = f(x). Then the equation of chord PQ is

$$Y - y = \frac{(y+\delta y)-y}{(x+\delta x)-x}(X-x)$$ (X, Y are current coordinates)

or $$Y - y = \frac{\delta y}{\delta x}(X-x).$$

Now as $Q \to P$, $\frac{\delta y}{\delta x} \to \frac{dy}{dx}$, and chord PQ becomes tangent to the curve at P(x,y).

Hence equation of tangent at P(x,y) is $Y - y = \frac{dy}{dx}(X-x)$.

3.3 Equation of normal.

Let the gradient of the normal at P be m. Then

$$m \cdot \frac{dy}{dx} = -1 \quad \text{or} \quad m = -\frac{dx}{dy}$$

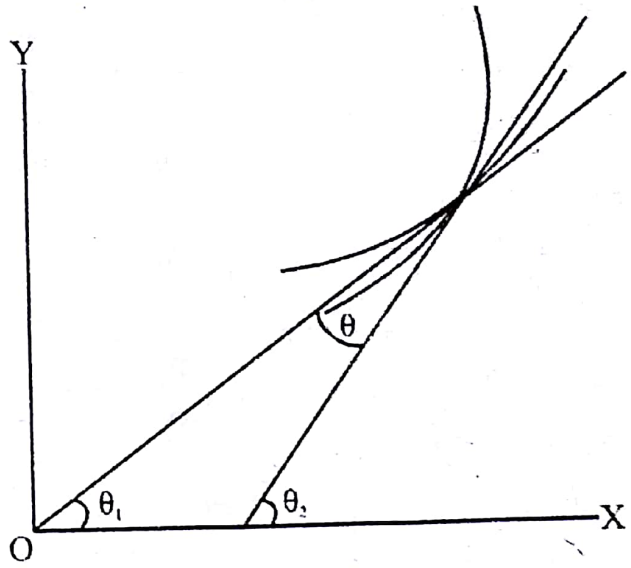
Hence the equation of the normal to the curve at P(x, y) is

$$Y - y = -\frac{dx}{dy}(X - x), \quad \text{or} \quad \frac{dy}{dx}(Y - y) + (X - x) = 0.$$

3.4 Angle of intersection of two curves.

The angle of intersection of two curves is the angle between the tangents at their common point of intersection. If m_1 and m_2 be the gradients of the tangents to the curve at their common point of intersection and if θ be the angle between them, we have

$$\tan\theta = \frac{m_1 - m_2}{1 + m_1 m_2}.$$

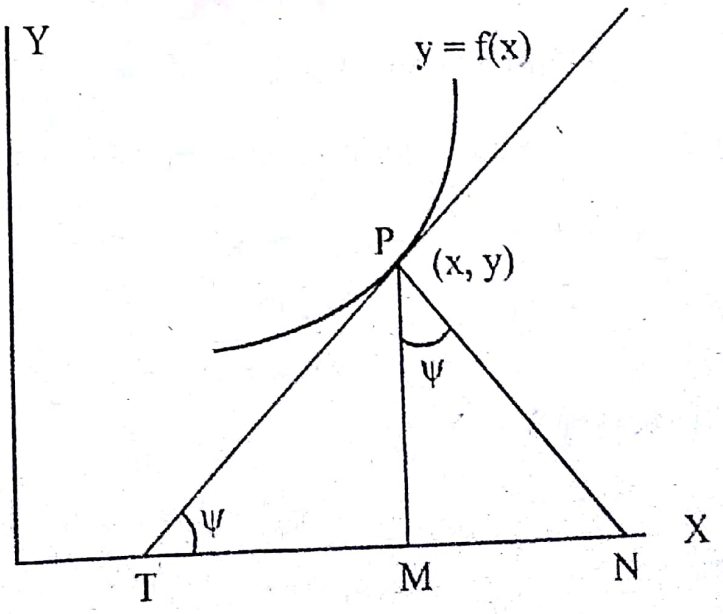


3.5 Cartesian Subtangent and subnormal.

Let the tangent and normal at any point P on a curve meet the x-axis in T and N respectively Let PM be the ordinate of P. Then TM is called subtangent and MN is called subnormal.

If the tangent at P makes an angle ψ with x-axis,

we have $\tan\psi = \frac{dy}{dx}$.



$\therefore$ Subtangent = TM = PM cot ψ

$$= \frac{y}{\tan\psi} = \frac{y}{\frac{dy}{dx}} = y\frac{dx}{dy},$$

and subnormal = MN = PM tan $\psi = y\frac{dy}{dx}$.

Length of tangent = PT

$$= PM \operatorname{cosec} \psi$$

$$= y\sqrt{1+\cot^2\psi}$$

$$= y\frac{\sqrt{1+\tan^2\psi}}{\tan\psi}$$

$$= y\frac{\sqrt{1+\left(\frac{dy}{dx}\right)^2}}{\frac{dy}{dx}}.$$

Length of Normal = PN

$$= PM \sec \psi$$

$$= y\sqrt{1+\tan^2\psi}$$

$$= y\sqrt{1+\left(\frac{dy}{dx}\right)^2}.$$

Example 1. Prove that the condition that the curves $ax^2 + by^2 = 1$ and $a'x^2 + b'y^2 = 1$ should intersect orthogonally is that $\frac{1}{a} - \frac{1}{b} = \frac{1}{a'} - \frac{1}{b'}$

Solution. Let the given curves

$$ax^2 + by^2 = 1 \quad \text{.....(i)}$$

and

$$a'x^2 + b'y^2 = 1 \quad \text{.....(ii)}$$

intersect at point $P(x_1, y_1)$.

Then $ax_1^2 + by_1^2 = 1$,

and $a'x_1^2 + b'y_1^2 = 1$.

or $$-\frac{1}{a}+\frac{1}{a'}=\frac{1}{b'}-\frac{1}{b}$$

or $$\frac{1}{a'}-\frac{1}{b'}=\frac{1}{a}-\frac{1}{b},$$

Example 2. If the normal to the curve $x^{2/3}+y^{2/3}=a^{2/3}$ makes angle ϕ with the axis of x, show that its equation is $y\cos\phi - x\sin\phi = a\cos 2\phi$. *(Avadh, 1991, '96)*

Solution. The given curve is $x^{2/3}+y^{2/3}=a^{2/3}$.

Its parametric equations may be taken as

$$x = a\sin^3\phi, \qquad y = a\cos^3\phi.$$

Then $$\frac{dx}{d\phi} = 3a\sin^2\phi\cos\phi, \qquad \frac{dy}{d\phi} = 3a\cos^2\phi(-\sin\phi)$$

$$\therefore \quad \frac{dy}{dx} = \frac{\frac{dy}{d\phi}}{\frac{dx}{d\phi}} = \frac{3a\cos^2\phi(-\sin\phi)}{3a\sin^2\phi\cos\phi}$$

$$= -\cot\phi.$$

Equation of normal at point $P(x, y)$ is

$$Y-y=-\frac{dx}{dy}(X-x).$$

Hence gradient of normal is $-\frac{1}{\frac{dy}{dx}} = \tan\phi$.

Therefore equation of normal at $P(x, y)$ of the curve is

$$y-a\cos^3\phi=\tan\phi(x-a\sin^3\phi)$$

or $$y\cos\phi - a\cos^4\phi = x\sin\phi - a\sin^4\phi$$

or $$y\cos\phi - x\sin\phi = a(\cos^4\phi-\sin^4\phi)$$

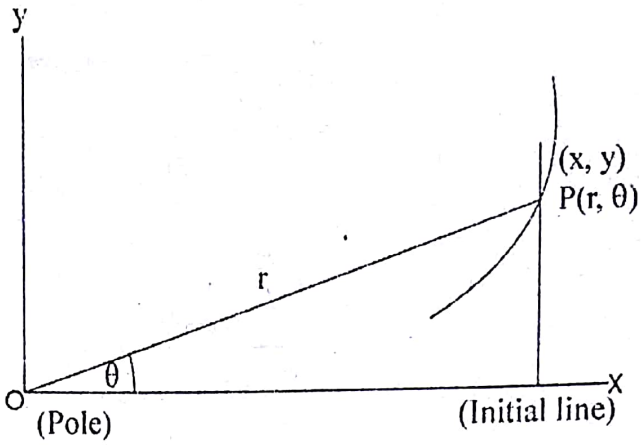
$$= a(\cos^2\phi+\sin^2\phi)(\cos^2\phi-\sin^2\phi)$$

$$= a\cos 2\phi.$$

3.6 Polar Coordinate

We may specify the position of a point P on a plane by knowing the distance r from a fixed point O and inclination of OP to a fixed straight line OX.

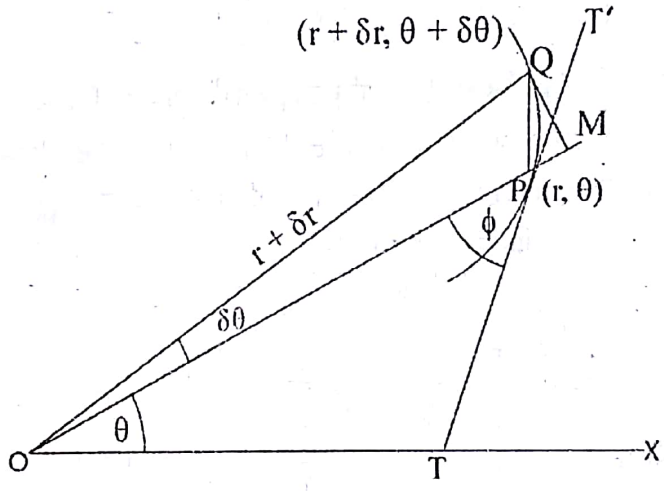
The fixed point O is called the pole, the line OX is called the initial line, r is called the radius vector, and θ is called the vectorial angle of point P. We call r, θ the polar coordinates of P. If Cartesian coordinates be P be (x, y), we have



$x = r\cos\theta, \qquad y = r\sin\theta.$

$x^2 + y^2 = r^2, \qquad \tan\theta = y/x.$

3.6.1 Angle between radius vector and tangent : Let $P(r, \theta)$ be a given point on the curve $r = f(\theta)$ and $Q(r + \delta r, \theta + \delta\theta)$ be other point of the curve in the neighbourhood of P. Let ϕ be the angle between the radius vector OP and tangent produced. Draw QM perpendicular to OP produced. As $\delta\theta \to 0$, $Q \to P$, also chord PQ $\to$ tangent' PT' and $\angle QPM \to \phi$.



Hence $\tan\phi = \underset{\delta\theta\to 0}{\text{Lim}} \tan\angle QPM$

$$= \underset{\delta\theta\to 0}{\text{Lim}} \frac{QM}{PM}$$

$$= \underset{\delta\theta\to 0}{\text{Lim}} \frac{(r+\delta r)\sin\delta\theta}{(r+\delta r)\cos\delta\theta - r}$$

$$= \underset{\delta\theta\to 0}{\text{Lim}} \frac{(r+\delta r)\sin\delta\theta}{\delta r\cos\delta\theta - r(1-\cos\delta\theta)}$$

$$= \underset{\delta\theta\to 0}{\text{Lim}} \frac{(r+\delta r)\dfrac{\sin\delta\theta}{\delta\theta}}{\left(\dfrac{\delta r}{\delta\theta}\right)\cos\delta\theta - \dfrac{r2\sin^2\dfrac{\delta\theta}{2}}{\delta\theta}}$$

$$= \lim_{\delta\theta\to 0} \frac{(r+\delta r)\dfrac{\sin\delta\theta}{\delta\theta}}{\left(\dfrac{\delta r}{\delta\theta}\right)\cos\delta\theta - r\dfrac{\dfrac{\sin\delta\theta}{2}}{\dfrac{\delta\theta}{2}}\sin\dfrac{\delta\theta}{2}}$$

$$= \frac{(r+0)\cdot 1}{\dfrac{dr}{d\theta}\cdot 1 - r\cdot 1\cdot \sin 0}$$

$$= \frac{r}{\dfrac{dr}{d\theta}} \qquad \text{using } \lim_{\delta\theta\to 0}\frac{\delta r}{\delta\theta} = \frac{dr}{d\theta},$$

and $$\lim_{\delta\theta\to 0}\frac{\dfrac{\sin\delta\theta}{2}}{\dfrac{\delta\theta}{2}} = 1.$$

$$\therefore \quad \tan\phi = r\frac{d\theta}{dr}.$$

3.6.2 Length of perpendicular from pole on the tangent :

Let $r = f(\theta)$ be given curve. Draw OT perpendicular to the tangent at any point P (r, θ) of the curve $r = f(\theta)$. Let OT = p

Now in triangle OPT,

$$p = r\sin\phi \qquad \text{.....(i)}$$

$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2\sin^2\phi}$$

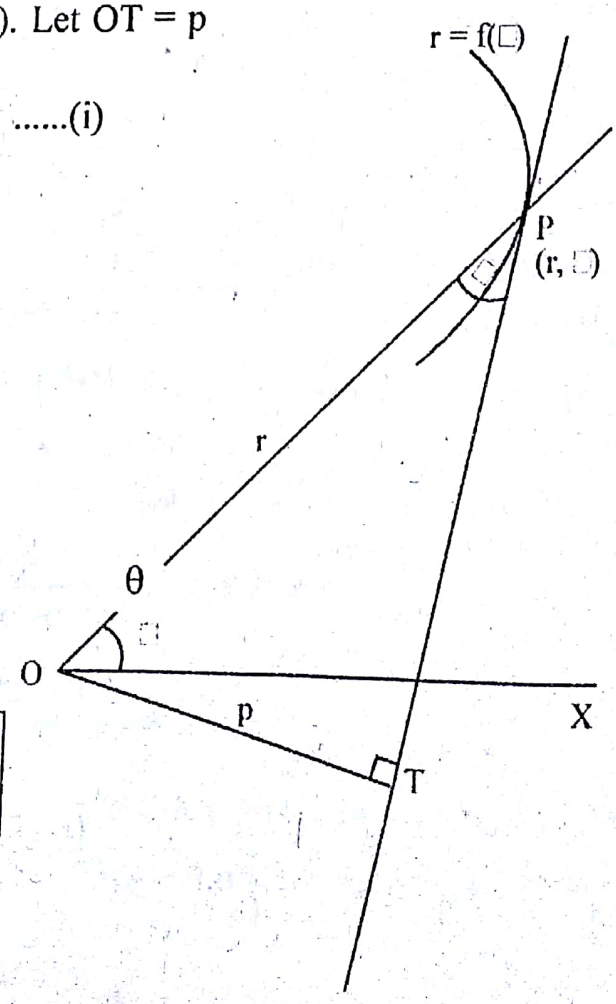
$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2}\operatorname{cosec}^2\phi$$

$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2}(1+\cot^2\phi)$$

$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2}\left(1+\frac{1}{\tan^2\phi}\right)$$

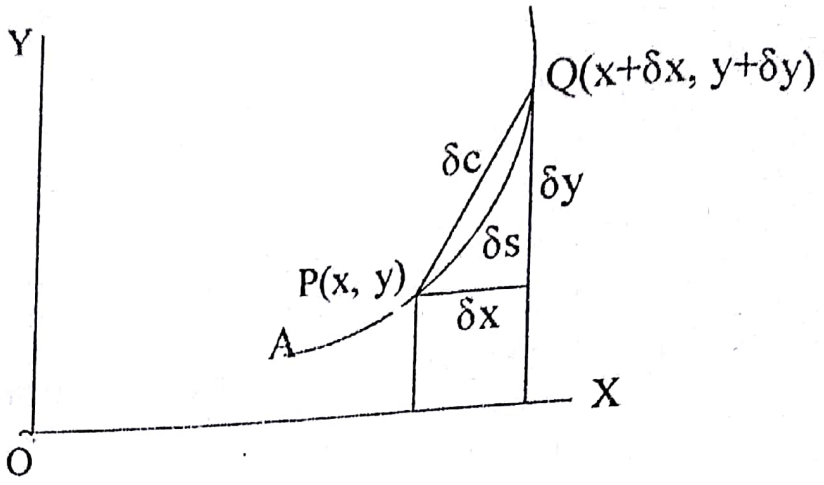
$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2}\left[1+\left(\frac{1}{r}\frac{dr}{d\theta}\right)^2\right]$$

$$\Rightarrow \quad \frac{1}{p^2} = \frac{1}{r^2} + \frac{1}{r^4}\left(\frac{dr}{d\theta}\right)^2$$



3.8 Differential Co-efficient of the length of arc.

(1) Cartesian form : Suppose A be a fixed point on the curve $y = f(x)$. Let P(x, y) be arbitrary point on the curve such that arc AP = Q. Let $Q(x + \delta x\ y + \delta y)$ be another point on the curve such that arc $AQ = s + \delta s$.



Let us assume that $Q \to P$.

Then $$\lim_{\delta x \to 0} \frac{\text{chord PQ}}{\text{arc PQ}} = 1$$

or $$\lim_{\delta x \to 0} \frac{\partial c}{\partial x} \frac{\partial x}{\partial s} = 1$$

or $$\lim_{\delta x \to 0} \frac{\sqrt{(\delta x)^2 + (\delta y)^2}}{\delta x} = \lim_{\delta x \to 0} \frac{\delta s}{\delta x}$$

or $$\lim_{\delta x \to 0} \sqrt{1 + \left(\frac{\delta y}{\delta x}\right)^2} = \frac{ds}{dx}$$

or $$\frac{ds}{dx} = \sqrt{1 + \left(\frac{dy}{dx}\right)^2}$$

When equations of the curve are in parametric form, say $x = x(t)$, $y = y(t)$, we have

$$\frac{ds}{dt} = \frac{ds}{dx} \frac{dx}{dt}$$

$$= \frac{dx}{dt} \sqrt{1 + \left(\frac{dy}{dx}\right)^2}$$

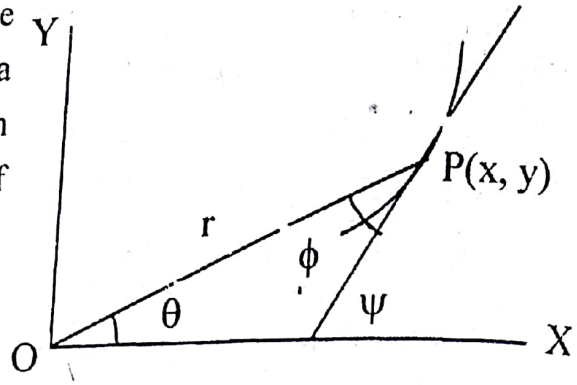
$$= \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}.$$

Eliminating θ between (i) and (ii) we get pedal equation of the curve.

Angle of intersection of polar curves : Let $r = f_1(\theta)$ and $r = f_2(\theta)$ be two curves intersecting at P. Let ϕ_1 and ϕ_2 be the angles which tangents to the curves at P make with radius vector OP. Then angle of intersection of two curves is $\phi_1 - \phi_2$.

Example 3. If ϕ be the angle between the tangent to a curve and the radius vector drawn from the origin to the point of contact, prove that

$$\tan \phi = \frac{\left(x\frac{dy}{dx} - y\right)}{\left(x + y\frac{dy}{dx}\right)}.$$



Solution.

From figure

$$\psi = \theta + \phi.$$

Also $$\frac{y}{x} = \frac{r\sin\theta}{r\cos\theta} = \tan\theta$$

and $$\frac{dy}{dx} = \tan\psi.$$

Since $\phi = \psi - \theta$,

therefore $$\tan\phi = \tan(\psi - \theta)$$

$$= \frac{\tan\psi - \tan\theta}{1 + \tan\psi\tan\theta}$$

$$= \frac{\left(\frac{dy}{dx}\right) - \left(\frac{y}{x}\right)}{1 + \left(\frac{dy}{dx}\right)\left(\frac{y}{x}\right)}$$

$$= \frac{\left(x\frac{dy}{dx} - y\right)}{\left(x + y\frac{dy}{dx}\right)}.$$

For example 214 and 216, hence 2 is a common divisor of 4 and 6.

Definition (4.2). Greatest common divisor (g.c.d). (2010, 12)
A non-zero integer d is called a **greatest common divisor** (g.c.d.) of two integers m and n iff .

(i) It is positive.

(ii) It is a common divisor of m and n, i.e. $d \mid m$ and $d \mid n$ and

(iii) It is divisible by all other common divisors of m and n, i.e. if $c \mid m$ and $c \mid n$ then $c \mid d$.

In symbols, $d = (m,n)$.

For example. 6. is the greatest common divisor of 12 and 30 because (1) 6 is positive

(ii) 6 | 12 and 6 | 30

and

(iii) the common divisors ± 2, ± 3 and ± 6 of 12 and 30 also divide 6.

Thus 6 = (12, 30).

Note 4.1. (i). If either m or n is zero, then the non–zero integer is the g.c.d.

(ii) If m and n both are zero, then we define zero to be the g.c.d.

Theorem 4.1. Euclidean algorithm. Any two non-zero integers m and n have a greatest common divisor space d such that

$d = am + bn$, where $a, b \in Z$. *(GKP 2004, 2006, 2012)*

Proof. Let m and n are two given non-zero integers. Let us construct an infinite set A which is given by

$$A = \{xm + yn : x, y \in Z\}.$$

Let B be a set of all the positive elements of A, i.e.

$$B = \{xm + yn > 0 : x, y \in Z\} \subset A.$$

Let d be the least (smallest) element of B. Then

$d \in B \Rightarrow d > 0$ and $d = am + bn$ for $x = a$ and $y = b$. .....(1).

Claim 1. We claim that $d \mid m$ and $d \mid n$, i.e. d is a common divisor of m and n.

Since m is a non-zero integer and d >0, therefore by division algorithm, there exist two unique integers q and r such that

$m = dq + r$, where $0 \leq r < d$ .....(2).

$\therefore$ $r = m - dq$

$= m - (am+bn)\, q$ ($\because d = am+bn$)

$= (1-aq)\, m + (-bq)\, n$ .....(3).

Thus, r is of the form xm + yn. If $0 < r < d$, then $r \in B$ which contradicts the fact that d is the least element of B. Hence $0 < r < d$ is not true.

Therefore, $r = 0$, Putting $r = 0$ in 2, we have $m = dq$.

$\therefore \quad d \mid m$.

Further, since n is a non-zero integer and $d > 0$. Therefore, applying division algorithm we can similarly prove that $d \mid n$ also.

Thus, d is a common divisor of m and n. Hence our claim 1 is true.

Claim 2. We claim that if $c \mid m$ and $c \mid n$ then $c \mid d$.

Now $c \mid m$ and $c \mid n \Rightarrow c \mid am$ and $c \mid bn$

$\Rightarrow c \mid (am + bn)$ by Example 2.1 (iv)

$\Rightarrow c \mid d$, by (1).

Thus any divisor of m and n also divides d.

Hence our claim 2 is true.

The relation 1, claim 1 and claim 2 collectively satisfy the definition 4.2. Hence d is the greatest common divisor of m and n, i.e. $d = (m,n)$.

Note 4.2. The integers a and b are not unique because d can be rewritten as :

$$\begin{aligned} d &= am + bn + mnp - mnp, \text{ where } p \in Z \text{ and } p \neq 0 \\ &= (a+np)m + (b-mp)n \\ &= Am + Bn \quad \text{where } A = (a + np) \neq a \\ &\qquad \text{and} \quad B = (b - mp) \neq b. \end{aligned}$$

Definition (4.3) . Two non-zero integers m and n are said to be relatively prime (or co-prime to each other) iff their greatest common divisor is 1, i.e.$(m,n) = 1$.

For example, 2 and 3 are relatively prime; 5 and 7 are relatively prime; 11 and 13 are relatively prime.

Theorem 4.2 . Show that :

(i) $k(m,n) = (km, kn)$, $k > 0$.

(ii) $(m,n) = d$, $m \mid b$, $n \mid b \Rightarrow mn \mid bd$.

(iii) $(m,n) = d$, $m = xd$, $n = yd \Rightarrow (x,y) = 1$.

(iv) $(m,n) = 1$, $(p,n) = 1 \Rightarrow (mp,n) = 1$.

(v) $(m,n) = 1$, $n \mid pm \Rightarrow n \mid p$.

(vi) $(m,n) = 1 \Rightarrow (m^k,n) = 1$, $k > 0$.

Proof. (i). Let $(m,n) = d$ .....(1).

Therefore, by Euclidean algorithm, $\exists$ two integers a and b such that

$d = am + bn$ .....(2).

Multiplying 2 by $k > 0$, we have

$kd = a(km) + b(kn)$

$\therefore (km, kn) = kd = k(m,n)$. .....(3).

by (1)

Hence every common divisor of m and n is also a divisor or r_k.

The relation $(k+1) \Rightarrow r_k | r_{k-1}$.

In the light of (k+1), the relation $k \Rightarrow r_k | r_{k-2}$.

Thus, continuing retrogressively we find that r_k divides r_1, n and m.

The above interpretations reveal that r_k satisfies the Definition 4.2. Hence $(m,n) = (n,r_1) = r_k$, the last non-vanishing remainder in this process known as **Euclid's algorithm**.

Example 4.1. Find the g.c.d of 2772 and 273 and express it in the form a· 2772 +b· 273 in two ways, where a and b are integers.

Solution .

$$273)2772(10$$
$$\underline{273}$$
$$42)273(6$$
$$\underline{252}$$
$$21)42(2$$
$$\underline{42}$$
$$\times$$

(GKP. 1988)

Here, the last non-vanishing remainder is 21.

Therefore, in view of Theorem 4.3, the g.c.d of 2772 and 273 is 21.

Now we can write

$2772 = 10 \times 273 + 42$ .....(1).

$273 = 6 \times 42 + 21$ .....(2).

$42 = 2 \times 21$ .....(3).

From 2, we have

$$21 = 273 - 6 \times 42$$
$$= 273 - 6.(2772 - 10 \times 273) \text{ from 1}$$
$$= 273 - 6.2772 + 60 \times 273$$
$$= -6.2772 + 61 \times 273 \quad ..(4)$$

where $a = -6$ and $b = 61$.

In the light of note 4.2, we can also express the g.c.d 21 in the form :

$$21 = (-6+273) \times 2772 + (61 - 2772) \times 273$$
$$= 267 \times 2777 + (-2711) \times 273 \quad ..(5).$$

where $A = 267$ and $B = -2711$.

Example 4.2. Find the g.c.d of 4078 and 814 and express it in the form a 4078 + b 814 in two ways, where a and b are integers.

(GKP, 1996)

Solution :

$$814)4078(5$$
$$\underline{4070}$$
$$8)814(101$$
$$\underline{8}$$
$$14$$
$$8$$
$$6)8(1$$
$$\underline{6}$$
$$2)6(3$$
$$\underline{6}$$
$$\times$$

Here, the last non-vanishing remainder is 2. Therefore, in view Theorem 4.3, the g.c.d of 4078 and 814 is 2.

Now we can write

$$4078 = 5\times814 + 8 \quad \text{.....(1}$$
$$814 = 101\times8 + 6 \quad \text{.....(2}$$
$$8 = 1\times6 + 2 \quad \text{.....(3}$$
$$6 = 3\times2 \quad \text{.....(4}$$

From (3), we have

$$2 = 8 - 1\times6$$
$$= (4078 - 5\times814) - 1(814 - 101\times8) \text{ using (1) and (2)}$$
$$= 4078 - 6\times814 + 101\times8$$
$$= 4078 - 6\times814 + 101\times (4078 - 5\times814) \text{ from (1)}$$
$$= 102\times4078 + (-511)\times814 \quad \text{.....(5)}$$

where a = 102 and b = – 511.

In the light of note 4.2, we can also express the g.c.d 2 in the form

$$2 = (102 + 814\times4078 + (-511 - 4078)\times814$$
$$= 916\times4078 + (-4589)\times814 \quad \text{.....(6)}$$

where A = 916 and B = – 4589.

Theorem 4.4. If p is a prime integer and p divides $m_1 . m_2$, then either p divides m_1 or p divides m_2. *(GKP, 2007)*

Proof. Since P $(m_1 . m_2)$, where p is prime.

Therefore, $m_1 . m_2 = pq$ for some $q \in Z$ .....(1).

Let p does not divide m_1, therefore

$(p, m_1) = 1$ .....(2).

Hence by Euclidean algorithm. $\exists$ two integers x and y.s.t.

$$1 = xp + ym_1.$$

Multiplying 3 by m_2, we have

$$m_2 = m_2xp + m_2ym_1$$

or $m_2 = m_2xp + m_1m_2y$

or $m_2 = m_2xp + pqy$ by (1)

or $m_2 = p(m_2x + qy)$.

which shows that p divides m_2.

We can generalise the above theorem as follows :

Theorem 4.5. If p is a prime integer and $p \mid (m_1, m_2, m_3....m_n)$ then p divides atleast one of $m_1, m_2, m_3, ...m_n$.

Theorem 4.6. Unique factorization theorem or fundamental theorem of arithmetic.

Every integer m ($|m| > 1$) can be uniquely expressed as a unit times a finite product of positive primes except for the order in which the prime factors occur. *[GKP, 97, 2005]*

Proof. The statement of the theorem reveals that m is neither zero nor units ± 1. Hence two cases arise, i.e. either $m > 1$ or $m < -1$.

Case 1. Let $m > 1$.

If m = 2, the first positive prime, then

$2 = 1.2$. Hence the theorem is true.

By virtue of principle of induction, let the theorem is true for positive integers less than m. If m is a positive prime integer, m =1m Hence the theorem is true. If m is not positive prime, it is obviously positive composite integer. Then m can be expressed as :

$m = m_1.m_2$, where $1 < m_1.m_2 < m$ and $m_1.m_2$ are finite products of positive primes. Hence m is expressed as a unit times a finite product of positive primes.

Uniqueness. Let m be expressed in two ways. viz.

$$m = p_1.p_2.p_3.....p_r \quad .....(1)$$

and

$$m = q_1.q_2.q_3.....q_s \quad ....(2)$$

where p's and q's are positive prime integers.

From (1) and (2), we have

$$p_1.p_2.p_3.....p_r = q_1.q_2.q_3.....q_{i-1}.q_i.q_{i+1}.....q \quad .....(3)$$

Now

$$\Rightarrow \quad p_1 \mid m$$

$$\Rightarrow \quad p \mid (q_1, q_2....q_s)$$

$\Rightarrow$ p_1 divides atleast one of q's, say q_i (due to Theorem 4.6)

$\Rightarrow$ $p_1 = q_1$ (since a prime integer cannot be a divisor of another prime) .....(4)

In view of (4), the relation (3) is reduced to

$p_2, p_3 \ldots\ldots\ldots p_r = q_1\ q_2 \ldots\ldots\ldots q_{i-1},\ q_{i+1} \ldots\ldots q_s$ .....(5)

Repeating the same argument, we can prove that

$p_2 = q_1$ for some $j \neq i$ .....(6)

Therefore. (5) is reduced to

$p_3, p_4 \ldots\ldots\ldots p_r = q_1\ q_2 \ldots\ldots\ldots q_{i-1} \ldots\ldots q_{i+1} \cdot q_s$

We continue this process of cancellation until one side of (3) is reduced to 1. Since p's and q's are integers, the other side of (3) also must be equal, i.e. 1. Thus representations of m given in (1) and (2) are the same except for the order in which the prime factors occur.

Case 2. Let $m < -1$.

The proof is similar to case 1.

Hence we have theorem.

Note 4.3. The above theorem does not exclude the occurence of equal primes. The same does not say anything about 0, 1 and –1.

Theorem 4.7. Prove that the set of all prime integers is infinite.

Proof. Let there are only n positive primes, where n is a finite number, Then there shall be 2n primes (positive as well as negative). Let the n positive primes be $p_1, p_2, p_3 \ldots\ldots\ldots p_n$ and

$p_1, p_2, p_3 \ldots\ldots\ldots p_n = m$, where $m \in Z^+$.

Consider the integer m +1.Obviously no p_n divides (m+1). Therefore, either (m+1) is itself a prime greater than p_n or has a prime greater than p_n as its factor which contradicts the hypothesis that p_n is the greatest prime. Hence our supposition is wrong. Thus there shall be infinite number of positive primes and hence the set of all prime integers is infinite.

5.Congruences.

Definition 5.1. Let a, b ∈ Z and n be a positive integer. Then we say that is a congruent to b modulo n iff $n \mid (a-b)$

Symbolically, we write $a \equiv b \pmod{n}$, where n is called the modulus of the congruence.

Thus $a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$

$\Leftrightarrow a-b = nq, q \in Z$

$\Leftrightarrow a = b+nq$ .....(1).

Example 1. $7 \equiv 2 \pmod{5}$ because $5 \mid (7-2)$

$6 \equiv 1 \pmod{5}$ because $5 \mid (6-1)$,

$5 \equiv 0 \pmod{5}$ because $5 \mid (5-0)$.

Theorem 5.1. The relation of congruence modulo n is an equivalence relation on the set Z of integers. *(GKP, 2006)*

Proof. **(i). Reflexivity.**

Since $n \mid (a-a)$

$\therefore \quad a \equiv a \pmod{n}$

(ii) Symmetry.

Let $a \equiv b \pmod{n}$

$a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$

$\Rightarrow (a-b) = nq \Rightarrow a = b + nq$

$\Rightarrow b - a = n(-q)$

$\Rightarrow n \mid (b-a)$

$\Rightarrow b \equiv a \pmod{n}$

(iii) Transitivity. Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$

$a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow n \mid (a-b)$ and $n \mid (b-c)$

$\Rightarrow n \mid [(a-b)+(b-c)]$

$\Rightarrow n \mid [(a-b+b-c]$

$\Rightarrow n \mid [(a-c)]$

$\Rightarrow a \equiv c \pmod{n}$.

Theorem 5.2 . If $m \in Z$ and n be a positive integer, then

$m \equiv r \pmod{n}$,

where r is the remainder when m is divided by n.

Proof. Let $m \in Z$ and $n > 0$. Then, by division algorithm, there exist two unique integers q and r such that

$m = nq + r, \quad 0 \le r < n$

or $m - r = nq \Rightarrow n \mid (m-r)$

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

Theorem 5.3. Two integers a and b leave the same remainder, when divided by a positive integer n iff. *(GKP, 2009)*

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

Proof. Let $a \in Z$ and $n>0$. By division algorithm,

$\exists$ two unique integers q_1 and r_1 s.t.

$a = nq_1 + r_1,\ 0 \le r_1 < n$

Similarly, $b \in Z$ and $n > 0$ so that

$b=nq_2+r_2,\ 0 \le r_2 < n$

Subtracting (2) from (1), we have

$a-b = n(q_1-q_2) + (r_1-r_2)$

where r_1 and r_2 are the remainders.

Now $r_1 = r_2 \Leftrightarrow a-b = n(q_1-q_2)$

$\Leftrightarrow n \mid (a-b)$

$\Leftrightarrow a \equiv b \pmod{n}$

6. Laws of addition, subtraction and multiplication for congruence modulo n.

Theorem. 6.1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

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

(ii) $a - c \equiv b-d \pmod{n}$

(iii) $ac \equiv bd \pmod{n}$ *[GKP, 2008]*

(iv) $a^m \equiv b^m \pmod{n}$ where $m \in Z$.

(v) $a+m \equiv b+m \pmod{n}$ $m \in Z$

(vi) $am \equiv bm \pmod{n}$, $m \in Z$.

Proof. (i). $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ and $n \mid (c-d)$

$\Rightarrow n \mid [(a-b)+(c-d)]$

$\Rightarrow n \mid [(a+c)-(b+d)]$

$\Rightarrow a+c \equiv b+d \pmod{n}$

(ii) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \Rightarrow n \mid (a-b)$ and $n \mid (c-d)$

$\Rightarrow n \mid (a-b)-(c-d)$

$\Rightarrow n \mid [(a-c)-(b-d)]$

$\Rightarrow a-c \equiv b-d \pmod{n}$

(iii) $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n} \Rightarrow n \mid (a-b)$ and $n \mid (c-d)$

$\Rightarrow a-b=nq_1$ and $c-d= nq_2$

$\Rightarrow a=b+nq_1$ and $c=d+ nq_2$

$\Rightarrow ac=bd+n(q_1d+bq_2+nq_2)$

$\Rightarrow ac = bd +nq$ where $q = q_1d+bq_2 +nq_1q_2$

$\Rightarrow n \mid (ac-bd)$

$\Rightarrow ac \equiv bd \pmod{n}$.

8. Residue classes or congruence classes.

Definition (8.1). The set of integers which is such that ... element of it, when divided by n leaves the same remainder r, is ca... residue class modulo n.

It is denoted by the symbol [r] (modn). Thus

[r] (modn) = { .....r–2n, r–n, r, r+n, r+2n.....}.

We know that when any integer is divided by n, then we have ... of the n remainders or residues, viz, 0, 1, 2, 3, 4, 5 .....r.....(n–... Therefore, all the integers can be divided into n residue class...

viz.

[0] (modn) = [0] = { ....., –2n, –n, 0, n, 2n.....}
[1] (mod n) =[1] = { ....., 1–2n, 1–n, 1, 1+n, 1+2n.....}
[2] (mod n) =[2] = { ....., 2–2n, 2–n, 2, 2+n, 2+2n.....}
.....
.....
.....
[n–1] (mod n) = [n–1] = { ....., –2n–1, –n–1, –1, n–1, 2n–1.....}

The set of all residue classes modulo n is denoted by $Z/(n) = \{[0], [1], [2], ...[r_1], [r_2].....[n-1]\}$

Definition 8.2. Sum of residue classes modulo n.

The sum of two residue classes $[r_1]$ and $[r_2]$ is defined a...

$$[r_1] + n[r_2] = [r_1+r_2] = [r]$$

where r is the least non-negative remainder when r_1+r_2 is devided by n, i.e. r is reduced mod n.

Example 1. Let $Z(7) = \{[0], [1], [2], [3], [4], [5], [6]\}$ be the set of residue classes modulo 7. Then $[0] + 7[4] = [4]$, $[2]+7[3] = [2+3]$ and $[5]+7[6] = [4]$, since $5+6 = 11 = 4 \pmod 7$.

Definition (8.3). Product or residue classes modulo n.

The product of two residue classes $[r_1]$ and $[r_2]$ is defined as

$$[r_1]\ 0\ [r_2] = [r_1, r_2] = [r]$$

where r is the least non-negative remainder when $r_1 . r_2$ is divided by n, i.e. r is reduced modn.

Example 2. Let $Z/(7) = \{[0], [1], [2], [3], [4], [5], [6]\}$ be the set of residue classes modulo 7, then.

$[2]\ 7[3] = [6]$, $[4]\ 7\ [6] = [3]$ since $4.6 = 24 \equiv 3 \pmod 7$

and $[1].\ 7[5] = [5]$

Note 8.1. Some important properties of residue classes will be discussed in Chapter 4.

9. Linear Congruences and reciprocals.

Definiton 9.1. Let $a, b \in Z$, $n \in Z^+$ and x be some unknown quantity, then the equation of the type $ax \equiv b \pmod n$ is called *'linear congruence'* modulo n. .....(1)

An integral value of x lying between 0 and n, which satisfies 1 is called an '*incongruent solution*' of the linear congurences (1).

Theorem 9.1. The linear congruence $ax \equiv b \pmod n$ has a solution iff $(a,n) \mid b$. *(GKP, 2007, 2010)*

Proof. Let $x_1 \in Z$ be a solution of the linear congruence

$$ax \equiv b \pmod n \quad \ldots\ldots(1)$$

Then $ax_1 \equiv b \pmod n$ so that $n \mid (ax_1 - b)$ or $ax_1 - b = nq$

or $ax_1 - nq = b$ for some $q \in Z$ ....(2)

Let $(a,n) = d$

Now $(a,n) = d \Rightarrow d \mid a$ and $d \mid n$

$\Rightarrow d \mid ax_1$ and $d \mid nq$

$\Rightarrow d \mid (ax_1 - nq)$

$\Rightarrow d \mid b$ by (2)

Conversely, let $(a,n) = d$ and $d \mid b$.

In the light of Euclidean algorithm, $(a, n) = d$

$\Rightarrow \quad d = pa + qn$, for some $p, q \in Z$ .....(3)

Now, $d \mid b \Rightarrow b = dk$

$\Rightarrow b = (pa + qn)k$ by (3)

$\Rightarrow b = pak + qnk$

$\Rightarrow apk - b = n(-qk)$

$\Rightarrow n \mid (apk - b)$

$\Rightarrow apk \equiv b \pmod n$

$\Rightarrow pk \in Z$ is a solution of $ax \equiv b \pmod n$.

Note 9.1. If $(a,n) = d$ and $d \mid b$, then $ax \equiv b \pmod n$ has d incongruent solutions.

Theorem 9.2. If $x_1 \in Z$ is a solution of $ax \equiv b \pmod n$ and $x_2 \equiv x_1 \pmod n$, then x_2 is also a solution of the given linear congruence. *[GKP, 2011]*

Proof. Since x_1 is a solution of

$$ax \equiv b \pmod n \quad \ldots\ldots(1).$$

therefore $ax_1 \equiv b \pmod n$ .....(2).

Now $x_2 \equiv x_1 \pmod n$

$\therefore \quad ax_2 \equiv ax_1 \pmod n$

$\equiv b \pmod n$ due to (2) and Theorem 5.1 (iii)

$\therefore x_2$ is a solution of (1).

Theorem 9.3. The linear congruence $ax \equiv 1 \pmod n$ has a solution iff $(a,n) = 1$.

Proof. Let x_1 be a solution of $ax \equiv 1 \pmod n$

incongruent solutions modulo 21.

Solution. Here $35x \equiv 14 \pmod{21}$.

Since $d = (35, 21) = 7$ and $7 \mid 14$. hence 1 has 7 incongruent solutions. 1 can be written as

$$7.5x \equiv 7.2 \pmod{7.3}$$

or $5x = 2 \pmod 3$, due to Theorem 7.3

$\equiv 5 \pmod 3$ $(\because 2 \equiv 5 \pmod 3)$

or $x \equiv 1 \pmod 3$ (due to Theorem 7.2).

Now $[1] \pmod 3 = \{ \ldots\ldots -5, -2, 1, 4, 7, 10, 13, 16, 19, \ldots\ldots \}$.

Hence the solutions of (1), lying between 0 and 21 are 1, 4, 7, 10, 13, 16, 19.

Example 3. If p is a positive prime integer and $a \in Z$, then

$a^2 \equiv 1 \pmod p$ $a \equiv 1 \pmod p$ or $a \equiv (p-1) \pmod p$

Solution . $a^2 \equiv 1 \pmod p \Rightarrow p \mid (a^2-1)$ *(GKP, 2003, 2009)*

$\Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow$ either $p \mid (a-1)$ or $p \mid (a+1)$, due to Theorem 4.4.

$\Rightarrow$ either $a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$

$\Rightarrow (p-1) \pmod p$

$(\because -1 \equiv (p-1) \pmod p)$.

Theorem 9.4. Fermat's theorem.

If p be a positive prime and a is any integer not divisible by p, then

$a^{p-1} \equiv 1 \pmod p$. *(GKP, 95, 98, 2005, 2008, 2011)*

Proof. Since p is a positive prime integer, hence all the positive integers less than p are not divisible by p, i.e. 1,2,3,4.....r.....(p–1) are not divisible by p. By hypothesis 'a' is also not divisible by p. So the integers a, 2a, 3a,.....ra,sa.....(p–1) a are also not divisible by p. Let S be the set of these (p–1) elements i.e.

$S = \{a, 2a, 3a, \ldots\ldots ra, \ldots\ldots sa, (p-1)a\}$

Claim 1. We claim that

$ra \not\equiv sa \pmod p$, $r \neq s$, $1 \leq r, s \leq (p-1)$

Because, $ra \equiv sa \pmod p \Rightarrow p \mid (ra-sa)$

$\Rightarrow p \mid (r-s).a$

$\Rightarrow$ either $p \mid (r-s)$ or $p \mid a$

which is not possible, as $|r-s| < p$.

Hence our Claim 1 is true..

So in the light of Theorem 5.3 and Claim 1, all the integers in S leave different remainders when divided by p. So remainders may be 0, 1, 2, 3, 4, ...r, s.....(p–1).

Claim 2. We claim that

$ra \not\equiv 0 \pmod p$, $1 \le r \le (p-1)$

Because, $ra \equiv 0 \pmod p \Rightarrow p \mid ra$

$\Rightarrow$ either $p \mid r$ or $p \mid a$.

which is impossible. Hence our Claim 2 is true.

Therefore, due to Theorem 5.2 and claim 2, the integers in S_a congruent to 1, 2, 3, ...r.....s, (p–1) modulo p in some order.

Thus, we have (p–1) linear congruent identities of the type.

$ra \equiv t \pmod p$, $1 \le r, t \le (p-1)$

Multiplying these (p–1) I identitive, we have

$a.\ 2a.\ 3a.\ 4a.\ .....ra.....sa.....(p-1)\,a \equiv 1.2.3.....(p-1) \pmod p$

or $a^{p-1} . \underline{|p-1} \equiv \underline{|p-1} \pmod p$

or $a^{p-1} \equiv 1 \pmod p$ $\quad (\because \underline{|p-1}, p \equiv 1$

Example 4. Let p =5 and a =4 (not divisible by 5)

Here S = { 1. 4. 2.4, 3.4, 4.4}

$1.4 \equiv 4 \pmod 5$

$2.4 \equiv 3 \pmod 5$

$3.4 \equiv 2 \pmod 5$

$4.4 \equiv 1 \pmod 5$.

Multiplying these 4 identities, we have

$4^4 \underline{|4} = \underline{|4} \pmod 5$

or $4^4 \equiv 1 \pmod 5$ $\quad (\because \underline{|4}\ 5 = 1)$

Theorem 9.5. Wilson's theorem.

If p be a positive prime, then.

$\underline{|p-1} + 1 \doteq 0 \pmod p$. *(GKP, 2004, 2006, 2009)*

Proof. Case 1. When p =2, the first positive prime

In this case the theorem is true, because

$\underline{|2-1} + 1 = 0 \pmod 2 \Rightarrow 2 \underline{|[1+1-0]} \Rightarrow 2 \mid 2$.

Case 2. When the prime p >2, then p is odd. Let us consider the set A of (p–3) positive integers less than p, i.e.

A = {2, 3, 4, 5, ...r.....(p–2)}.

Since p is prime, hence each element in A is relatively prime to p. Therefore, due to note 9.2 each $r \in A$ has a unique reciprocal s modulo p such that $0<s<p$.

Claim 1. We claim that 0, 1, (p–1) are not reciprocals of any

$r \in A$. Because, 0 is reciprocal of r modulo p,

$\Rightarrow r.0 \equiv 1 \pmod p$

$\Rightarrow p \mid (0-1) \Rightarrow p \mid (r-1)$ which is impossible; 1 is reciprocal of r module p

$\Rightarrow r.1 \equiv 1 \pmod p \Rightarrow p \mid (r-1)$ which is impossible, (p–1) is reciprocal of r mod p.

$\Rightarrow r.(p-1) \equiv 1 \pmod p$

$\Rightarrow p \mid (rp - r - 1)$

$\Rightarrow p \mid [rp - (r+1)]$ which is impossible as (r+1) is not an integral multiple of p.

Hence our Claim 1 is true.

Claim 2. We claim that any $r \in A$ is not self reciprocal, i.e. is not reciprocal of r itself modulo p.

Because r is itself reciprocal

$\Rightarrow r.r \equiv 1 \pmod p$

$\Rightarrow p \mid (r^2-1)$

$\Rightarrow p \mid (r-1)(r+1)$

$\Rightarrow$ either $p \mid (r-1)$ or $p \mid (r+1)$ which is impossible.

Hence our Claim 2 is true.

As a consequence of above two claims, we can say that reciprocal of r modulo p is $s \in A$ such that $r \neq s$. Therefore, reciprocals of half of the elements in A are the rest half of the elements of the same set in some order.

Thus , we have $\frac{(p-3)}{2}$ identities of the type

$r.s \equiv 1 \pmod p$ .....(1)

Multiplying these $\frac{(p-3)}{2}$ identities, we have

$2.3.4.5.....(p-2) \equiv 1 \pmod p$ .....(2)

Multiplying 2 by (p–1), we obtain

$\underline{|p-1} \equiv (p-1) \pmod p$ .....(3)

$\equiv -1 \pmod p$ $(\because (p-1) \equiv -1 \pmod p)$

or $(p-1) + 1 = 0 \pmod p$.

Example 5. Let p =11,

then A = { 2, 3, 4, 5, 6, 7, 8, 9}.

Reciprocal of 2 is 6 modulo 11.