3. Primes and the theory of convergence.

An integer $p > 1$ is called a prime number or simply prime, if its only divisor are ± 1 & $\pm p$.

Composite Number:-
An integer $a > 1$ is called as composite number if it is not prime that is
$a = mn$, $1 < mn < a$
example $15 = 3 \times 5$ $1 < 3, 5 < 15$.

very IMP Thm

Euclid's lemma -
If 'p' is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

→ Let $p \mid ab$
$\exists$ c such that
$ab = pc$ —— ①
If $p \mid a$ then we are done.
let us assume that $p \nmid a$ then we have to prove that $p \mid b$?
If
$p \nmid a$
$\Rightarrow (p, a) = 1$
$\exists$ x, y such that
$1 = px + ay$
multiply ~~both~~ b on both sides.
$b = pbx + aby$
From eqn ① $ab = pc$.
$b = pbx + pcy$
$b = p(bx + cy)$
$\Rightarrow p \mid b$.
Hence proved

Teacher's Signature: ....

Ex. 1. If p is prime such that $p|a$ and $p|a^2+b^2$ then show that $p|b$.
$\longrightarrow$ suppose $p|a$
$\Longrightarrow p|a^2$
and also given that
$p|a^2+b^2$
$\therefore p|a^2+b^2-a^2$
$\therefore p|b^2$
$\therefore p|b$ ---- By euclid lemma.

* Fundamental cannonical form:
Any positive integer $n>1$ can be written uniquely in cannonical form.

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots\cdots p_n^{k_n}$$

where for $i = 1,2,3,4 \cdots\cdots n$
k_i is an integer
& p_i is an prime number with
$p_1 < p_2 < p_3 < \cdots < p_n$

examples IMP for 2-3 marks

Write 819 and 658 in its cannonical form and find there g.c.d and L.C.M

1)
$819 = 3 \times 273$
$= 3 \times 3 \times 91$
$= 3 \times 3 \times 7 \times 13$
$819 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^1$

$819 = 3 \times 273$
$= 3 \times 3 \times 91$
$= 3 \times 3 \times 7 \times 13$
$= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^1$

$658 = 2 \times 329$
$= 2 \times 7 \times 47$
$= \cancel{2 \times 7 \times}$ ~~2¹.3°.5.7 11 13 17 19 23~~
$658 = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 47^1$

$658 = 2 \times 329$
$= 2 \times 7 \times 47$

Teacher's Signature:

$(819, 658) = \cancel{5^0 \cdot 7^1}\ 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 7$

$[819, 658] = 2^1 7^1 47^1 3^2 13^1 = 7698$

2) 108, 225

$108 = 2 \times 54$
$= 2 \times 2 \times 27$
$= 2 \times 2 \times 3 \times 9$
$= 2 \times 2 \times 3 \times 3 \times 3$

$108 = 2^2 \cdot 3^3 \cdot 5^0$

$225 = 5 \times 45$
$= 5 \times 5 \times 9$
$= 5 \times 5 \times 3 \times 3$

$225 = 2^0 3^2 \cdot 5^2$

3) $(108, 225) = 2^0 5^0 3^2$

$[108, 225] = 2^2 3^2 3 5^2$

4) 106, $\cancel{2 \times 5}$ 220

$\cancel{220} = 106 = 2 \times 53 \quad = 2^1 \cdot 53^1$

$220 = 2 \times 110$
$= 2 \times 2 \times 55$
$= 2 \times 2 \times 5 \times 11$
$= 2^2 \cdot 5^1 \cdot 11^1$

G.C.d $= 2^1$

L.C.M $= 2^1 53^1\ 2^1 5^1 11^1$

5) $500 = 2 \times 250$
$\cancel{125} = 2 \times 2 \times 125$
$= 2 \times 2 \times \cancel{5} \times 25$
$= 2 \times 2 \times 5 \times 5 \times 5$
$= 2^2 \cdot 5^3$

$125 = 5 \times 25$
$= 5 \times 5 \times 5$
$= 5^3$

G.C.d $= 5^3$

L.c.m $= 5^3 \cdot 2^2$

Teacher's Signature..........

Theory of convergence.
Congruence modulo n
Let n be a fix positive integer two integer a and b are said to be congruence modulo 'n' iff $n/a-b$.
$n/a-b$
Notation: $a \equiv b \pmod n$
read as a is congruent to b mod n

1) Example:- $17 \equiv 2 \pmod 3$
17 congruent to 2 mod 3 because
$3/17-2$
$3/15$.
$3/17-2$
but,
$17 \not\equiv 4 \pmod 3$
$3 \nmid 17-4$
$3 \nmid 13$

Properties

Let $n \geq 1$ be fix and a, b, c, d be arbitery integer. then the following properties hold
i) $a \equiv a \pmod n$
ii) If $a \equiv b \pmod n$ then $b \equiv a \pmod n$
iii) If $a \equiv b \pmod n$ & $b \equiv a \pmod n$ then $a \equiv c \bmod n$.
iv) If $a \equiv b \pmod n$ & $c \equiv \pmod n$ then $a+c \equiv b+d \pmod n$
v) If $a \equiv b \pmod n$ then $a+c \equiv b+c \pmod n$ & $ac \equiv bc \pmod n$
vi) If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$ for any +ve integer k.

Teacher's Signature:

i) $a \equiv a \pmod n$

→ For any integer a we have $a-a=0$ & 0 is always divide by any number
i.e. $n/0 \Rightarrow a \equiv a \pmod n$

ii) If $a \equiv b \pmod n$ then $b \equiv a \pmod n$

→ Let $a = b \pmod n$

$n / a-b$ $\qquad\qquad$ $n/0 \Rightarrow a \equiv a$ (modn

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

$\Rightarrow n | -a+b$ $\qquad\qquad$ Let $a \equiv b$ (mod n

i.e $n/b-a$ $\qquad\qquad$ $n/a-b$

$b \equiv a \pmod n$ $\qquad\qquad$ $n/-$

iii) If $a \equiv b \pmod n$ & $b \equiv a \pmod n$ then $a \equiv c \pmod n$

→ let $a \equiv b \pmod n$ & $b \equiv c \pmod n$

$\Rightarrow n/a-b$ $\qquad\qquad$ $\Rightarrow n / b-c$

$\Rightarrow n / a-b+b-c$

$\Rightarrow n / a-c.$

$\Rightarrow a \equiv c \pmod n$

*

iv) If $a \equiv b \pmod n$ & $c \equiv d \pmod n$ then $a+c \equiv b+d \pmod n$ & $ac = bd \pmod n$

→ Let $a \equiv b \pmod n$ & $c \equiv d \pmod n$

$\Rightarrow n | a-b$ $\qquad\qquad$ $\Rightarrow n | c-d$

$\Rightarrow n | (a-b) + (c-d)$

$\Rightarrow n / a-b+c-d$

$\Rightarrow n | a+c-b-d$

$\Rightarrow n | (a+c) - (b+d$

$\Rightarrow (a+c) \equiv (b+d) \pmod n$

Let $a \equiv b \pmod{n}$ & $c \equiv d \pmod{n}$

$\Rightarrow n | a-b$ $\Longrightarrow n | c-d$

multiply by c & multiply by b

$\Longrightarrow n | ac-bc$ $\Longrightarrow n | bc-bd$

$\Longrightarrow n | ac-bc+bc-bd$

$\Longrightarrow n | ac-bd$

$\Longrightarrow ac \equiv bd \pmod{n}$

v) If $a \equiv b \pmod{n}$ then $a+c \equiv b+c \pmod{n}$ & $ac \equiv bc \pmod{n}$

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

$\Longrightarrow n | a-b$

add & sub c

$\Longrightarrow n | a+c-c-b$

$\Longrightarrow n | (a+c)-(c+b)$

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

also multiply by c

$\Longrightarrow n | c(a-b)$

$\Longrightarrow n | ac-bc$

$\Longrightarrow ac \equiv bc \pmod{n}$

vi) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for any positive integer

$a \equiv b \pmod{n} \Longrightarrow a^k \equiv b^k \pmod{n}$

$\Longrightarrow n | a-b$

$\Longrightarrow n | (a-b)(a^{k-1} + a^{k-2}b + \cdots)$

$\Longrightarrow n | a^k - b^k$

$a^k \equiv b^k \pmod{n}$

Teacher's Signature:

Example

1) Find the reminder when 2^{50} is divisible by 7.

$8 \equiv 1 \pmod{n}$

$(2 \times 2 \times 2) \equiv 1 \pmod{7}$

$2^3 \equiv 1 \pmod{7}$

$(2^3)^{16} \equiv (1)^{16} \pmod{7}$

$2^{48} \equiv 1 \pmod{7}$

$2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{7}$

$2^{50} \equiv 1 \cdot 4 \pmod{7}$

$2^{50} \equiv 4 \pmod{7}$

$8 \equiv 1 \pmod{n}$

$2 \times 2 \times 2 = 1 \bmod 7$

$2^3 \equiv 1 \bmod 7$

2×2

2) Find the reminder $2^{20}-1$ is divisibl by 41

→ $32 \equiv -9 \pmod{41}$

$2^5 \equiv -9 \pmod{41}$

$(2^5)^4 \equiv (-9)^4 \pmod{41}$

$2^{20} \equiv (-9 \times -9 \times -9 \times -9) \pmod{41}$

$2^{20} \equiv (81)^2 \pmod{41}$

We know that

$a \equiv b \pmod{n}$

$b \equiv c \pmod{n}$

$a \equiv c \pmod{n}$

PAGE NO.
DATE / /

Statement

Fermat's Thm:-
Let p be a prime and suppose that $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

Euler's thm:-
Let p be a prime then $a^p \equiv a \pmod{p}$,
For any integer 'a'.

Q1 Show that $7^{10} - 5^{10}$ is divisible by 11.
→ As $11 \nmid 7$ and $11 \nmid 5$
then by Fermat's thm
$\therefore 7^{11-1} \equiv 1 \pmod{11}$ & $5^{11-1} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$ —① & $5^{10} \equiv 1 \pmod{11}$ —②
sub eqⁿ 1 & eqⁿ 2
$7^{10} - 5^{10} \equiv (1-1) \pmod{11}$
$7^{10} - 5^{10} \equiv 0 \pmod{11}$
$\Rightarrow 11 \mid 7^{10} - 5^{10}$

2) If ~~gc~~ $(a, 35) = 1$ then show that $a^{12} \equiv 1 \pmod{35}$
→ $35 = 5 \cdot 7$
$7 \nmid a$ & $5 \nmid a$ $\therefore (a, 35) = 1$
$\Rightarrow a^{7-1} \equiv 1 \pmod{7}$ & $\Rightarrow a^{5-1} \equiv 1 \pmod{5}$
$a^6 \equiv 1 \pmod{7}$ & $\Rightarrow a^4 \equiv 1 \pmod{5}$
squaring on both & cubing on both
$(a^6)^2 \equiv (1)^2 \pmod{7}$ & $(a^4)^3 \equiv (1)^3 \bmod 7$
$a^{12} \equiv 1 \pmod{7}$ —① & $a^{12} \equiv 1 \pmod{7}$ —②
From eqⁿ 1 & 2
$a^{12} \equiv 1 \pmod{35}$ ---- $(5, 7) = 1$

Teacher's Signature: ....

5 marks.

3. Find reminder when 2^{105} is divided by 11.

2^{105}, 11

Here $p = 11$, $a = 2$

$\Rightarrow 11 \times 2$

By Fermat's thm

$2^{11-1} \equiv 1 \pmod{11}$

$2^{10} \equiv 1 \pmod{11}$

Taking 10th power

$(2^{10})^{10} \equiv (1)^{10} \pmod{11}$

$\Rightarrow 2^{100} \equiv 1 \pmod{11}$ —— 1

& $2 \equiv 2 \pmod{11}$

Taking 5th power

$2^5 \equiv 2^5 \pmod{11}$

$2^5 \equiv 32 \pmod{11}$

$2^5 \equiv 10 \pmod{11}$ —— 2.

multiplying eqn 1 & eqn 2 .... $a^m . a^n \Rightarrow a^{m+n}$.

$2^{100} . 2^5 \equiv 1 . 10 \pmod{11}$

$2^{105} \equiv \underline{10} \pmod{11}$

4) Find the unit digit of 3^{100} by using Fermat's thm

→ 3^{100} $a = 3$ $P = 5$

$10 = 2 \times 5$

5×3 & 2×3

3^{100}

$10 \times 2 \times 5$

5×3 & $\cancel{2} \times 3$

2×3

By Fermat's thm

$\Rightarrow 3^{5-1} \equiv 1 \pmod{5}$ & $3^{2-1} \equiv 1 \pmod{2}$

$3^4 \equiv 1 \pmod{5}$ & $3 \equiv 1 \pmod{2}$

Taking 25th power & Taking 100th power

$(3^4)^{25} \equiv (1)^{25} \pmod{5}$ $3^{100} \equiv (1)^{100} \pmod{2}$

$3^{100} \equiv 1 \pmod{5}$ —1 $3^{100} \equiv 1 \pmod{2}$ —2.

From 1 & 2 $(2, 5) = 1$

$3^{100} \equiv 1 \pmod{10}$ -- when 3^{100} is divisible by 10.

ie unit digit of 3^{100} is 1

Teacher's Signature.......

Hence 1 is the reminder

Find unit digit of 9^{102} by using fermats thm.

9^{102}

$10 = 5 \times 2$

$5 \nmid 9$ & $2 \nmid 9$

$9^{5-1} \equiv 1 (\mod 5)$ & $9^{2-1} \equiv 1 (\mod 2)$

$9^4 \equiv 1 (\mod 5)$ & $9 \equiv 1 (\mod 2)$

Taking 25th power — Taking 100th power,

$\Rightarrow (9^4)^{25} \equiv (1)^{25} \mod (5)$ — $9^{100} \equiv (1)^{100} (\mod 2)$

$9^{100} \equiv 1 (\mod 5)$ — ① — $9^{100} \equiv 1 (\mod 2)$ ②.

we know that

$9^2 \equiv 1 (\mod 10)$ — ②.

multiply 1 and 2

$9^{100} \cdot 9^2 \equiv (1 \cdot 1) \mod 10$ ---- $a^m \cdot a^n = a^{m+n}$)

$9^{102} \equiv 1 (\mod 10)$

6) Find the unit digit of 3^{15} by using Fermats theorem.

$a = 3$

$10 = 2 \cdot 5$

$2 \nmid 3$ and $\cancel{2 \nmid 5}$ $5 \nmid 3$

By Fermats thm

$3^{2-1} \equiv 1 \pmod 2$

$\Rightarrow 3^1 \equiv 1 \pmod 2$

Taking 12th power

$3^{12} \equiv 1^{12} \pmod 2$

$\Rightarrow 3^{12} \equiv 1 \pmod 2$ — 1

$3^{5-1} \equiv 1 \pmod 5$

$\Rightarrow 3^4 \equiv 1 \pmod 5$

Taking cube.

$(3^4)^3 \equiv 1^3 \pmod 5$

$3^{12} \equiv 1 \pmod 5$ — 2

From 1 & 2

$3^{12} \equiv 1 \pmod{10}$ — 3 $\quad \because (2, 5) = 1$

we know that

$3^3 \equiv 7 \pmod{10}$ — 4

multiply 3 & 4

$3^{12} \cdot 3^3 \equiv (1 \cdot 7) \pmod{10}$

$3^{15} \equiv 7 \pmod{10}$

7) If 7 does not divide a prove that either a^3+1 or a^3-1 which it is divisible by 7.

→ Let $7 \nmid a$

By Fermat thm

$a^{7-1} \equiv 1 \pmod 7$

Teacher's Signature:..........................

$\Rightarrow a^6 \equiv 1 \pmod 7$.

$\Rightarrow 7 \mid a^6 - 1$

$\Rightarrow 7 \mid (a^3-1)(a^3+1)$ $\quad \because (a^6-1) = (a^3)^2 - (1^3)^2 = (a^3+1)($

$\Rightarrow 7 \mid a^3 - 1$ or $7 \mid a^3+1$

IMP

fermats thm

Let p be a prime and suppose that $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$

proof: We know that

$(a_1 + a_2 + a_3 + \text{-----} + a_n)^p = a_1^p + a_2^p + \text{------} + a_n^p \; m(p)$

where $m(p)$ is multiple of p.

put, $a_1 = a_2 = \text{-------} = a_n = 1$

$(1+1+1+\text{-----}1)^p = 1^p + 1^p + \text{----------} + 1^p + m(p)$

$(n)^p = n + m(p)$

Taking (mod p) we get,

$n^p \equiv n \pmod p$

replace n by a

$a^p \equiv a \pmod p$

divide by a on both sides

$\frac{a^p}{a} \equiv \frac{a}{a} \pmod p$

$a^{p-1} \equiv 1 \pmod p$ $\because \frac{a^m}{a^n} = a^{m-n}$