CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049

SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF MATHEMATICS
DN PG COLLEGE MEERUT

Pdf-01 ① Number Theory | Dr Satish Kr

CH-04 , Theory of congruence

1 symbol for congruence on set of integers

$a \equiv b \pmod{m}$ ⟶ a is congruent to b mod m, m is fixed integer $a, b \in I$; Integers

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

$\Rightarrow \exists$ an integer k such that $(a-b) = mk$

$\Rightarrow a = b + mk$

Theorem. If $m > 0$, fixed integers, $a, b, c \in I$ then prove

① $a \equiv a \pmod{m}$

② If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$

③ If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

④ If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

$\Rightarrow (a+c) \equiv (b+d) \pmod{m}$

and $ac \equiv bd \pmod{m}$

⑤ If $a \equiv b \pmod{m}$ then $(a+c) \equiv (b+c) \pmod{m}$

⑥ If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for all $k \geq 1$

But if $a^k \equiv b^k \pmod{m}$ for $k \geq 2$ then it is not necessarily that $a \equiv b \pmod{m}$.

Proof. ① Let $m > 0$, fixed integer, $a, b, c \in I$

we have $a - a = 0$

$a - a = 0 \cdot m$

$\Rightarrow m \mid (a-a)$

$\Rightarrow a \equiv a \pmod{m}$

(2) if $m>0$, fixed integer

To prove if $a \equiv b \pmod{m}$

then $b \equiv a \pmod{m}$

It is given

$a \equiv b \pmod{m}$

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

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

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

(3) it is given

$a \equiv b \pmod{m}$ —— (1)

$b \equiv c \pmod{m}$ —— (2)

To prove $a \equiv c \pmod{m}$

(1) $\Rightarrow m \mid a-b$ —— (3)

(2) $\Rightarrow m \mid b-c$ —— (4)

(3) & (4) $\Rightarrow$

$\Rightarrow m \mid a-b+b-c$

$\Rightarrow m \mid a-c$

$\Rightarrow a \equiv c \pmod{m}$

(4) If $a \equiv b \pmod{m}$ —— (1)

$c \equiv d \pmod{m}$ —— (2)

To prove

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

(1) $\Rightarrow m \mid a-b$ —— (3)

(2) $\Rightarrow m \mid c-d$ —— (4)

(3) and (4) $\Rightarrow$

$m \mid a-b+c-d$

$\Rightarrow m \mid (a+c)-(b+d)$

$\Rightarrow (a+c) \equiv (b+d) \pmod{m}$

Pdf-01

CH-04 (03) Number Theory Dr Satish Kr

Also (3) & (4) $\Rightarrow$

$(a-b) = m r_1 \Rightarrow a = b + m r_1$, $r_1 \in I$

Similarly $c = d + m r_2$, $r_2 \in I$

$ac = (b + m r_1)(d + m r_2)$

$ac = bd + m(r_1 d + m r_1 r_2 + b r_2)$

$\Rightarrow ac - bd = m(r_1 d + m r_1 r_2 + b r_2)$

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

$\Rightarrow ac \equiv bd \pmod{m}$

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

$\Rightarrow m \mid (a+c) - (b+c)$

$\Rightarrow a+c \equiv (b+c) \pmod{m}$.

(vi) $a \equiv b \pmod{m}$

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

$\Rightarrow m \mid (a^k - b^k)$ $[\because a^k - b^k = (a-b)(a^{k-1} + a^{k-2} b + \dots + b^{k-1})]$

$\Rightarrow a^k \equiv b^k \pmod{m}$

Converse is not true

Take $a = 8$, $b = 4$, $m = 3$

i.e $a^2 \equiv b^2 \pmod{3}$

i.e $8^2 \equiv 4^2 \pmod{3}$

i.e $3 \mid (8^2 - 4^2)$

But $3 \nmid (8-4)$ i.e $8 \not\equiv 4 \pmod{3}$

Scanned with CamScanner

Theorem. If a, b, c are integers such that

$ac \equiv bc \pmod{m}$, $m > 0$, fixed integer

and $d =$ g.c.d of c & m.

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

Proof. Let a, b, c be any three integers

Let $m > 0$ be fixed integers

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

then To prove

$a \equiv b \pmod{\frac{m}{d}}$, $d =$ g.c.d of c and m.

It is given $d = (c, m)$

$\Rightarrow c = d r_1$, $r_1 \in I$

& $m = d r_2$, $r_2 \in I$ such that $(r_1, r_2) = 1$

Also it is given

$ac \equiv bc \pmod{m}$

$\Rightarrow m \mid ac - bc$

$\Rightarrow m \mid (a-b)c$

$\Rightarrow m \mid (a-b) d r_1$ $[\because c = d r_1]$

$\Rightarrow \frac{m}{d} \mid (a-b) r_1$

$\Rightarrow r_2 \mid (a-b) r_1$

$\Rightarrow r_2 \mid (a-b)$ $[\because a \mid bc \Rightarrow a \mid b$ if $(a, c) = 1]$

$\Rightarrow \frac{m}{d} \mid a-b$

$\Rightarrow a \equiv b \pmod{\frac{m}{d}}$, proved.

Pdf-01

01-04 $\boxed{05}$, Number Theory, Dr Satish Kr

Theorem 03. Prove that $a \equiv b \pmod m$ iff a and b have the same remainder when divided by m.

Proof. Let $a \equiv b \pmod m$

Let r_1 be the remainder when a is divided by m

$$\Rightarrow a = mq_1 + r_1 \quad , \quad 0 \le r_1 < m \quad \text{---} (1)$$

Let r_2 be the remainder when b is divided by m

$$\Rightarrow b = mq_2 + r_2 \quad , \quad 0 \le r_2 < m \quad \text{---} (2)$$

To prove $r_1 = r_2$

It is given $a \equiv b \pmod m$

$$\Rightarrow mq_1 + r_1 \equiv mq_2 + r_2 \pmod m$$

$$\Rightarrow m \mid (mq_1 + r_1) - (mq_2 + r_2)$$

$$\Rightarrow m \mid m(q_1 - q_2) + (r_1 - r_2)$$

$$\Rightarrow m \mid 0 + (r_1 - r_2)$$

$\Rightarrow r_1 - r_2$ must be zero as $r_1 < m$, $r_2 < m$ $\Rightarrow r_1 - r_2 < m$

$$\Rightarrow r_1 = r_2$$

Converse if $r_1 = r_2$

then (1) and (2) $\Rightarrow$

$$a = mq_1$$
$$b = mq_2$$

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

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

$\Rightarrow a \equiv b \pmod m$, proved.

Pdf-01 CH-04 (06), Dr Satish Kr

Number Theory

Example 1: Show that 41 divides $2^{20}-1$.

Solution: We have

$$2^1 \equiv 2 (\mod 41)$$

$$2^2 \equiv 4 (\mod 41)$$

$$2^3 \equiv 8 (\mod 41)$$

$$2^4 \equiv 16 (\mod 41)$$

$$2^5 \equiv -9 (\mod 41)$$

$[a = b + mk \Leftrightarrow a \equiv b (\mod m)$
$a = 32, m = 41, k = 1 \Rightarrow b = -9$

$$2^{20} \equiv [-9 (\mod 41)]^4$$

$[a \equiv b (\mod m) \Rightarrow a^k \equiv b^k (\mod m)]$

$$\equiv (-9)^4 (\mod 41)$$

$$\equiv 81 \times 81 (\mod 41)$$

$$\equiv (-1) \times (-1) (\mod 41)$$

$$\equiv 1 (\mod 41)$$

$$2^{20} - 1 \equiv 0 (\mod 41)$$

$\therefore 2^{20} - 1$ is divisible by 41

Example 2: Find the remainder when 5^{48} is divisible by 24.

Solution: We have

$$5 \equiv 5 (\mod 24)$$

$$5^2 \equiv 1 (\mod 24)$$

$$[5^2]^{24} \equiv [1 (\mod 24)]^{24}$$

$[a \equiv b (\mod m) \Rightarrow a^k \equiv b^k (\mod m)]$

$$5^{48} \equiv 1^{24} (\mod 24)$$

$$5^{48} \equiv 1 (\mod 24)$$

$\therefore$ When 5^{48} is divided by 24 the remainder is 1

CH-04, Pdf-01 (07) Number Theory Dr Satish Kr

Example 3: Find the remainder when the sum $S = 1! + 2! + 3! + \cdots + 100!$ is divided by 8.

Solution: We have $1! \equiv 1(\bmod 8)$, $2! \equiv 2(\bmod 8)$, $3! \equiv 6(\bmod 8)$, $4! \equiv 0(\bmod 8)$

$5! \equiv 0(\bmod 8)$, $6! \equiv 0(\bmod 8)$

$$\vdots$$

$$\vdots$$

$$1000! \equiv 0(\bmod 8)$$

$$\Rightarrow 1! + 2! + 3! + \cdots + 1000! \equiv 1 + 2 + 6 + 0 + 0 + \cdots (\bmod 8)$$

$$\equiv 9(\bmod 8)$$

$$\equiv 1(\bmod 8)$$

∴Remainder is 1.

Example 4: Find the remainder when 2^{24} is divided by 17.

Solution: We have

$$2 \equiv 2(\bmod 17)$$

$$2^2 \equiv 4(\bmod 17)$$

$$2^3 \equiv 8(\bmod 17)$$

$$2^4 \equiv -1(\bmod 17)$$

$$[2^4]^6 \equiv [-1(\bmod 17)]^6$$

$$2^{24} \equiv (-1)^6(\bmod 17)$$

$$2^{24} \equiv 1(\bmod 17) \qquad [(-1)^6 = 1]$$

∴Remainder is 1

Scanned with CamScanner

Pdf-01

CH-04 (Special)

(08) Number Theory
Dr Satish Kr

Example 5: Find the remainder when 2^{340} is divided by 341.

Solution: We have

$$341 = 11\times 31$$

$\therefore 2^1 \equiv 2(\text{mod}11), 2^2 \equiv 4(\text{mod}11)$

$2^3 \equiv 8(\text{mod}11), 2^4 \equiv 5(\text{mod}11), 2^5 \equiv -1(\text{mod}11)$

$$[2^5]^{68} \equiv (-1)^{68}(\text{mod}11)$$

$$2^{340} \equiv 1(\text{mod}11)$$

And

$$2^1 \equiv 2(\text{mod}31)$$

$$2^2 \equiv 4(\text{mod}31)$$

$$2^3 \equiv 8(\text{mod}31)$$

$$2^4 \equiv 16(\text{mod}31)$$

$$2^5 \equiv 1(\text{mod}31)$$

$\therefore [2^5]^{68} \equiv 1^{68}(\text{mod}31)$

$$2^{340} \equiv 1(\text{mod}31)$$

$\therefore 2^{340} \equiv 1(\text{mod}11\times 31)$

$$2^{340} \equiv 1(\text{mod}341)$$

$\therefore$ Remainder is 1.

Pdf-01

CH-04 (09), Number Theory

Dr Satish Kr

Example 6: Find the remainder when 3^{287} is divided by 23.

Solution: We have

$$287 = 256 + 16 + 8 + 4 + 2 + 1 \quad \text{——— (1)}$$

Now

$$3 \equiv 3 \pmod{23} \quad \text{——— (2)}$$

$$3^2 \equiv 9 \pmod{23} \quad \text{——— (3)}$$

$$3^4 \equiv -11 \pmod{23} \quad \text{——— (4)}$$

$$3^8 \equiv 6 \pmod{23}$$

$$3^{16} \equiv 6^2 \pmod{23}$$

$$\equiv -10 \pmod{23} \quad \text{——— (5)}$$

$$3^{32} \equiv (-10)^2 \pmod{23}$$

$$\equiv 8 \pmod{23}$$

$$3^{64} \equiv 8^2 \pmod{23}$$

$$\equiv -5 \pmod{23}$$

$$3^{128} \equiv (-5)^2 \pmod{23}$$

$$\equiv 2 \pmod{23}$$

$$3^{256} \equiv 2^2 \pmod{23}$$

$$\equiv 4 \pmod{23} \quad \text{——— (6)}$$

$$\therefore 3^{287} = 3^{256} \times 3^{16} \times 3^8 \times 3^4 \times 3^2 \times 3$$

$$3^{287} \equiv 4 \times (-10) \times 6 \times (-11) \times 9 \times 3 \pmod{23}$$

$$3^{287} \equiv (-40) \times (-66) \times 27 \pmod{23}$$

$$3^{287} \equiv 6 \times 3 \times 4 \pmod{23}$$

$$3^{287} \equiv 24 \times 3 \pmod{23}$$

$$3^{287} \equiv 1 \times 3 \pmod{23}$$

$$3^{287} \equiv 3 \pmod{23}$$

Example 7: What is the remainder when 11^{35} is divided by 13.

Solution: We know that

$$35 = 32 + 2 + 1$$

Now

$$11 \equiv -2(\text{mod}13) \qquad (1)$$

$$11^2 \equiv (-2)^2(\text{mod}13)$$

$$\equiv 4(\text{mod}13) \qquad (2)$$

$$11^4 \equiv 4^2(\text{mod}13)$$

$$\equiv 3(\text{mod}13)$$

$$11^8 \equiv 3^2(\text{mod}13)$$

$$\equiv -4(\text{mod}13)$$

$$11^{16} \equiv (-4)^2(\text{mod}13)$$

$$\equiv 3(\text{mod}13)$$

$$11^{32} \equiv 3^9(\text{mod}13)$$

$$\equiv 9(\text{mod}13)$$

$$\equiv -4(\text{mod}13) \qquad (3)$$

$\therefore 11^{35} = 11^{32} \times 11^2 \times 11$

$$11^{35} \equiv (-4) \times 4 \times (-2)(\text{mod}13)$$

$$11^{35} \equiv (-16) \times (-2)(\text{mod}13)$$

$$11^{35} \equiv (-3) \times (-2)(\text{mod}13)$$

$$11^{35} \equiv 6(\text{mod}13)$$

$\therefore$Remainder $= 6$

CH-04, pdf-01 (11) Number Theory
Dr Satish Kr

Example 8: What is the remainder when the sum $1^5 + 2^5 + 3^5 + \cdots\cdots + 100^5$ is divided by 4.

Solution: We have

$$1 + 2 + 3 + \cdots\cdots + 100 = (4n_1 + 1) + (4n_2 + 3) + 2n_3$$

Where

$$n_1 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_2 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_3 = 1,2,3 \ldots\ldots\ldots 50$$

Now,

For $n_1 = 0,1,2,3 \ldots\ldots\ldots 24$

$$1^5 \equiv 1(\mathrm{mod}4)$$

$$5^5 \equiv 1(\mathrm{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(4n_1 + 1)^5 \equiv 1(\mathrm{mod}4)$$

For $n_2 = 0,1,2,3 \ldots\ldots\ldots 24$

$$3^5 \equiv 3(\mathrm{mod}4)$$

$$7^5 \equiv 3(\mathrm{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(4n_2 + 3)^5 \equiv 3(\mathrm{mod}4)$$

And

For $n_3 = 1,2,3 \ldots\ldots\ldots 50$

CH-04 , (12) Number Theory
Pdf-01 Dr Satish Kr

$$2^5 \equiv 0(\text{mod}4)$$

$$4^5 \equiv 0(\text{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(2n_3)^5 \equiv 0(\text{mod}4)$$

Now,

$$1^5 + 2^5 + 3^5 + \cdots\cdots + 100^5 = (4n_1 + 1)^5 + (4n_2 + 3)^5 + (2n_3)^5$$

Where

$$n_1 = 0,1,2,3 \ldots \ldots \ldots 24$$

$$n_2 = 0,1,2,3 \ldots \ldots \ldots 24$$

$$n_3 = 1,2,3 \ldots \ldots \ldots 50$$

$$\equiv 25 \times 1(\text{mod}4) + 25 \times 3(\text{mod}4) + 50 \times 0(\text{mod}4)$$

$$\equiv (25 \times 1 + 25 \times 3 + 50 \times 0)(\text{mod}4)$$

$$\equiv 100(\text{mod}4)$$

$$\equiv 0(\text{mod}4)$$

$\therefore$**Remainder** $= 0.$

Example 9: What is the remainder when $3^{12} + 5^{12}$ is divided by 13.

Solution: We have

$$3^2 \equiv 9 \pmod{13}$$

$$3^4 \equiv 9^2 \pmod{13}$$

$$3^4 \equiv 81 \pmod{13}$$

$$\equiv 3 \pmod{13}$$

$$3^{12} \equiv 3^3 \pmod{13}$$

$$\equiv 27 \pmod{13}$$

$3^{12} \equiv 1 \pmod{13}$ .... (1)

And

$$5^2 \equiv -1 \pmod{13}$$

$$5^{12} \equiv (-1)^6 \pmod{13}$$

$5^{12} \equiv 1 \pmod{13}$ .... (2)

(1) + (2)

$$3^{12} + 5^{12} \equiv 1 \pmod{13} + 1 \pmod{13}$$
$$\equiv 1 + 1 \pmod{13}$$
$$\equiv 2 \pmod{13}$$

∴Remainder = 2

Test of divisibility

Let n be any natural number

$$n = (\cdots a_3 a_2 a_1 a_0)_{10}$$

$$n = a_0 \times 10^0 + a_1 \times 10^1 + a_2 10^2 + a_3 10^3 + \cdots$$ (Decimal representation of n)

Here a_0 is unit place
a_1 is tenth place
a_2 is Hundred place etc

(1) We say $2|n$ if 2 divides unit place of n

i.e $2|n$ if $2|a_0$

i.e $a_0 \equiv 0 \pmod 2 \Rightarrow 2|n \Leftrightarrow a_0 \equiv 0 \pmod 2$

This is application of congruence relation

Now

(2) $3|n \Leftrightarrow 3|(a_0 + a_1 + a_2 + a_3 + \cdots)$

$\Leftrightarrow 3|(a_0 + a_1 + a_2 + a_3 \cdots)$

i.e $3|$(sum of all places of n namely unit place, tenth place etc)

How $(a_0 + a_1 + a_2 + \cdots)$ has come --- ?? - - .

$$n = (a_0 \times 10^0 + a_1 10^1 + a_2 10^2 + a_3 10^3 - \cdots)$$

find $n \equiv (a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \cdots) \pmod 3$

$\underline{n \equiv (a_0 + a_1 + a_2 + \cdots) \pmod 3}$ $\Rightarrow 3|n \Leftrightarrow 3|\sum_{i=0}^{n} a_i$

as $a_1 10 \equiv a_1 \pmod 3$
$a_2 \cdot 10^2 \equiv 100 a_2 \pmod 3$
$a_2 10^2 \equiv a_2 \pmod 3$ and so on

Note (1) n and $(a_0 + a_1 + a_2 + \cdots)$ have the same remainders when divided by 3.

(2) $n \pmod 3 \equiv (a_0 + a_1 + \cdots +) \pmod 3$

$a \equiv b \pmod 3$, $a = n$, $b = a_0 + a_1 + \cdots$, ex $n = 153$ $\Rightarrow 3|(3+5+1)$

(3) $4|n \Leftrightarrow 4|(a_0+2a_1)$

$n = a_0 + 10a_1 + 10^2 a^2 + 10^3 a^3 + \cdots$

$n \pmod 4 \Rightarrow (a_0 + a_1 \cdot 10 + a_2 10^2 + a_3 10^3 + \cdots) \pmod 4$

$n \pmod 4 \equiv (a_0 + 2a_1 + 0 + 0 + \cdots) \pmod 4$

$\Rightarrow 4|n$ iff $4|(a_0+2a_1)$

[$\because$ $a \equiv b \pmod 4$ ~~have the~~ means a & b have the same remainders when divided by 4.]

i.e $n \equiv (a_0+2a_1) \pmod 4$

, a_0 is unit place of n

a_1 is tenth place of n.

ex $n = 528$ Here $a_0 = 8$

$a_1 = 2$

ie $a_0 + 2a_1 = 8 + 2\times 2$

$= 12$

Now $4|12 \Rightarrow 4|528$. etc.

(4) Simulary

$5|n \Leftrightarrow 5|a_0$, a_0 is unit place of n.

(5) $6|n \Leftrightarrow 6|[a_0 + 4(a_1+a_2+a_3+\cdots)]$

i.e $6|$ [unit place $+ 4(a_1+a_2+a_3+\cdots)$]

, $a_1 =$ 10th place, a_2 is 10^2th place etc

ex $6|216$

as $6|[6+4(1+2)] \Rightarrow 6|18$. Here $a_0=6$

$a_1 = 1$

$a_2 = 2$

(6) $7|n \Leftrightarrow 7|[(a_2a_1a_0) - (a_5a_4a_3) + (a_8a_7a_6) - \cdots]$

$N = a_2a_1a_0 + (a_5a_4a_3)10^3 + (a_8a_7a_6)(10^3)^2 + \cdots$.

$10^3 \equiv -1 \pmod 7$

Also $10^3 \equiv -1 \pmod{13}$ so $13|n \Leftrightarrow 13|[(a_2a_1a_0) - (a_5a_4a_3) + \cdots]$

(7) $11 \mid n \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - a_3 + \cdots)$

$n = a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots$

$n \pmod{11} \equiv (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \bmod 11$

$10 \equiv -1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$
$10^3 \equiv -1 \pmod{11}$
$10^4 \equiv 1 \pmod{11}$

$\therefore (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \equiv (a_0 - a_1 + a_2 - a_3 + \cdots) \bmod 11$

$\Rightarrow 11 \mid n \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - a_3 + \cdots)$

$11 \mid n \Leftrightarrow 11 \mid \sum_{i=0}^{m} (-1)^i a_i$

(8) $101 \mid n \Leftrightarrow (101) \mid [(a_1 a_0) - (a_3 a_2) + (a_5 a_4) - \cdots]$

(9) $9 \mid n \Leftrightarrow 9 \mid (a_0 + a_1 + a_2 + a_3 + \cdots)$

as $n \equiv (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \pmod 9$
$n \equiv (a_0 + a_1 + a_2 + a_3 + \cdots) \pmod 9$

as $10 \equiv 1 \pmod 9$
$10^2 \equiv 1 \pmod 9$
$10^3 \equiv 1 \pmod 9$ ---- etc.

Explanation of 8 $\quad n = \underline{(a_0 + 10a_1)} + \underline{10^2 a_2 + 10^3 a_3} + \underline{10^4 a_4 + 10^5 a_5}$

$= (a_0 + 10a_1) + 10^2(a_2 + 10a_3) + 10^4(a_4 + a_5) + \cdots$

$(a_0 + 10a_1) \pmod{101} \equiv a_0 + 10a_1$

$10^2 \equiv -1 \pmod{101}$
$10^4 \equiv 1 \pmod{101}$ etc.