Chapter-4

The theory of Congruences

(4.2) Basic properties of congruence

(Def 4.1) Let n be fixed positive integer. Two integers a and b are said to be congruent modulo 'n', symbolized by

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

(n is called modulo of $\equiv$; b is called residue of $a \pmod n$)

if $n \mid (a-b)$

i.e $\exists\ k \in \mathbb{Z}$ s.t

$a - b = kn$

$\Rightarrow a = b + nk$ for some integer k

(example) $3 \equiv 24 \pmod 7$, as $7 \mid (3-24)$, $7 \mid (-21)$

$-31 \equiv 11 \pmod 7$, as $7 \mid -31-11$, $7 \mid -42$

$-15 \equiv -64 \pmod{27}$, as $7 \mid -15+64$, $7 \mid 49$

Remark ① If $n \nmid (a-b)$

i.e a is incongruent to b modulo n

In this case we write $a \not\equiv b \pmod n$

e.g) $25 \not\equiv 12 \pmod{17}$

Since $7 \nmid (25-12)$

$7 \nmid (13)$

② Given an integer a, let q and r be its quotient & remainder upon division by n, so that

$$a = qn + r \quad ; \quad 0 \le r < n$$ (by division algorithm)

i.e $a - r = qn$

i.e $n \mid (a-r)$

$\Rightarrow a \equiv r \pmod n$

the value of r in $a \equiv r \pmod n$ is called residue

Since there are n choices for r (as $0 \le r < n$)

Every integer is congruent modulo n to exactly one of the values $0, 1, 2, \dots, n-1$

(n choices)

i.e The set of n integers $0, 1, 2, \dots, n-1$ is called the set of atleast non-negative residues modulo n.

Theorem (4.1) ✱
For arbitrary integers a and b, $a \equiv b \pmod n \iff$ a & b leave the same non-negative remainder when divided by n.

$2 \equiv -1 \pmod 3$

$\frac{2}{3} \Rightarrow$ remainder 2

$\frac{-1}{3} \Rightarrow$ $3\overline{)-1}\,(-1$, $0\ 3$, 2

(pf) let $a \equiv b \pmod n$

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

$\Rightarrow a - b = kn$ for some integer k

Now upon division by n, b leaves certain remainder r (By division algorithm)

when b is divided by n

$n\overline{)b}$

$b = \ell n + r \quad (0 \le r < n)$

$n \mid b$ i.e. $b = \ell n + r$

$a = b + kn = \ell n + r + kn$

$= (\ell + k)n + r \quad (0 \le r < n)$

i.e. a & b has same remainder.

So $2 \equiv -1 \pmod 3$

Scanned with CamScanner

nversely

let a & b leave some remainder 'r'

i.e $a = q_1 n + r \quad (0 \le r < n)$

$b = q_2 n + r$

then $a - b = q_1 n + r - q_2 n - r$

$\Rightarrow (q_1 - q_2) n$

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

$\Rightarrow a \equiv b \pmod n$

example (4.1) $-31 \equiv 11 \pmod 7$ Now divide -31 by 7 and 11 by 7. leaves same remainder when divided by n

By above thm. -31 & 11

$-31 = (-5)7 + 4$, $11 = 1 \cdot 7 + 4$

and $-56 \equiv -11 \pmod 9$ (divide -56 by 9 & -11 by 7

i.e $-56 = (-7)9 + 7$; $-11 = (-2)9 + 7$.

Theorem (4.2) let $n > 1$ be fixed, a, b, c, d be arbitrary integers then following properties holds!

① $a \equiv a \pmod n$

② if $a \equiv b \pmod n$ then $b \equiv a \pmod n$

③ if $a \equiv b \pmod n$ & $b \equiv c \pmod n$ then $a \equiv c \pmod n$

④ if $a \equiv b \pmod n$ & $c \equiv d \pmod n$

then $a + c \equiv b + d \pmod n$

& $ac \equiv bd \pmod n$

⑤ if $a \equiv b \pmod n$ then $a + c \equiv b + c \pmod n$ &

$ac \equiv bc \pmod n$.

⑥ if $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$ for any positive integer k.

(pf) ① if $n > 1$ so, $a - a = 0 \cdot n$

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

$\Rightarrow a \equiv a \pmod n$; $a \in \mathbb{Z}$

② if $a \equiv b \pmod n \Rightarrow n \mid (a-b)$

$\Rightarrow a = b + nk$; $k \in \mathbb{Z}$

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

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

③ If $a \equiv b \pmod{n}$ & $b \equiv c \pmod{n}$

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

$\Rightarrow a-b = k_1 n$, $b-c = k_2 n$; $k_1, k_2 \in \mathbb{Z}$

Now $a-c = a-b+b-c$

$= k_1 n + k_2 n$

$= (k_1+k_2) n$

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

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

④ If $a \equiv b \pmod{n}$ & $c \equiv d \pmod{n}$

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

$\Rightarrow a-b = k_1 n$, $c-d = k_1 n$

Now, $a-b+c-d = (k_1+k_2) n$

$\Rightarrow (a+c) - (b+d) = (k_1+k_2) n$

$\Rightarrow (a+c) = (b+d) + t n$ where $t = k_1+k_1$

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

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

and $a \cdot c = (b+k_1 n) \cdot (d+k_2 n)$

$ac = bd + (bk_2 + dk_1 + k_1 k_2) n$

$\Rightarrow n \mid ac - bd$

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

⑤ If $a \equiv b \pmod{n}$ & we know that $c \equiv c \pmod{n}$

$\Rightarrow a+c \equiv b+c \pmod{n}$ (by above result)

⑥ If $a \equiv b \pmod{n}$ & $c \equiv c \pmod{n}$

$a \cdot c = b \cdot c \pmod{n}$

⑦ If $a \equiv b \pmod{n}$ & $a \equiv b \pmod{n}$

then $a^2 \equiv b^2 \pmod{n}$

similarly $a^2 \equiv b^2 \pmod{n}$ & $a \equiv b \pmod{n}$

$\Rightarrow a^3 \equiv b^3 \pmod{n}$

$\vdots$

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

$\therefore 2 - 1 \equiv 0 (\text{mod } 1)$

Example(4.3) Find the remainder when sum $1! + 2! + 3! + \cdots + 100!$ divisible by 12.

(Soln) $1! = 1 \equiv 1 \pmod{12}$

$2! \equiv 4 \pmod{12}$

$3! \equiv 6 \pmod{12}$

$4! \equiv 24 \pmod{12}$

$\equiv 0 \pmod{12}$

$4! \equiv 0 \pmod{12}$

$5 \times 4! \equiv 0 \times 5$

$5! \equiv 0 \pmod{12}$

$6 \times 5! \equiv 0 \pmod{12}$

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

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

$\Rightarrow ac = bc$

Now $1! + 2! + 3! + \cdots + 100!$

$= 1! + 2! + 3! + 0 + 0 + \cdots + 0 \pmod{12}$

$1+2+6+\cdots+(n^2-n) \pmod{12}$

$= 9 \pmod{12}$

So, remainder is 9 when $1!+2!+3!+\cdots+(100)!$ is divisible by 12.

Theorem 4.3) If $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{\frac{n}{d}}$ where $d = gcd(c, n)$

(pf) Now $ca \equiv cb \pmod{n}$

$\Rightarrow n \mid ca - cb$

$\Rightarrow ca - cb = kn$

$\Rightarrow ca = cb + kn \quad ; k \in \mathbb{Z}$

Also $gcd(c, n) = d$

$\Rightarrow d \mid c$ & $d \mid n$

$\exists\ r, s \in \mathbb{Z}$ s.t $c = dr$, $n = ds$

> $gcd(r, s) = gcd\left(\frac{c}{d}, \frac{n}{d}\right)$
> If $gcd(c, n) = d$
> $\Rightarrow gcd\left(\frac{c}{d}, \frac{n}{d}\right) = 1$
> $\Rightarrow gcd(r, s) = 1$

Consider $ca - cb = kn$

$\Rightarrow dra - crb = kds$

$\Rightarrow dra - drb = kds$

$\Rightarrow dr(a-b) = kds$

$\Rightarrow r(a-b) = ks$

$\Rightarrow s \mid r(a-b)$ and $gcd(r, s) = 1$

By Euclid's lemma $\Rightarrow s \mid (a-b)$

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

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

Corollary If $ca \equiv cb \pmod{n}$ & $gcd(c, n) = 1$ then $a \equiv b \pmod{n}$

Now $n \mid ca - cb$

$\Rightarrow n \mid c(a-b)$ & $gcd(c, n) = 1$

$\Rightarrow n \mid (a-b)$ (by Euclid's lemma)

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

Corollary If $ca \equiv cb \pmod{p}$ & $p \nmid c$ where p is prime number then $a \equiv b \pmod{p}$

$p \mid c(a-b)$ & $p \nmid c \Rightarrow gcd(p, c) = 1$

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

(Q-4) (a) Find the remainder when 2^{50} & 41^{65} divided by 7.

(Sol^n) 2^{50} divided by 7

$2 \equiv 2 \pmod 7$

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 8 \equiv 1 \pmod 7$

Now $2^{50} = (2^3)^{16} \cdot 2^2$

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

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

$\equiv 4 \pmod 7$

remainder is 4.

41^{65} divided by 7

$41 \equiv 6 \pmod 7$

$41^{65} \equiv (6)^{65} \pmod 7$

Now, $6 \equiv (-1) \pmod 7$

$6^2 \equiv (-1)^2 \pmod 7$

$(6^2)^{32} \equiv ((-1)^2)^{32} \pmod 7$

$6^{64} \equiv 1 \pmod 7$

$6^{65} \equiv 6 \pmod 7$

Remainder is 6.

Q(4) (b) What is remainder of sum divided by 4?

$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$.

(Sol^n) $1^5 \equiv 1 \pmod 4$ ✓

$2^5 \equiv 32 \equiv 0 \pmod 4$ ✓

$3^5 \equiv 243 \equiv 3 \pmod 4$ ✓

$4^5 \equiv 0 \pmod 4$ ✓

$5^5 \equiv 1 \pmod 4$

$6^5 \equiv 2^5 \cdot 3^5 \equiv 0 \pmod 4$ ✓

$7^5 \equiv 7^2 \cdot 7^2 \cdot 7^1 \equiv 1 \cdot 1 \cdot 3 \pmod 4 \equiv 3 \pmod 4$

$8^5 \equiv 0 \pmod 4$ ✓

$9^5 \equiv 1 \pmod 4$

$10^5 \equiv 0 \pmod 4$ ✓