MA212 - TUTORIAL 3 [BHAGYA RANA]

U19CS012 [U19CS012]

1) Prove the following

(a) If $a \equiv b \pmod n$ and $c > 0$, then $ca \equiv cb \pmod{cn}$

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

$\Rightarrow$ $a - b = kn$, some $k \in I$

$\therefore$ $ca - cb = k(cn)$ [multiply both sides by 'c']

$\Rightarrow$ $\boxed{ca \equiv cb \pmod{cn}}$, Hence Proved

(b) If $a \equiv b \pmod n$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$

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

$\Rightarrow$ $a - b = kn$, some $k \in I$ — (1)

$\because$ a, b, n are divisible by d, $d > 0$

$\therefore$ $a = k_1 d$ $\therefore$ $a/d = k_1$

$b = k_2 d$ $b/d = k_2$ — (2)

$n = k_3 d$ $n/d = k_3$

$a - b = k(n)$

$\therefore$ $k_1 d - k_2 d = k(k_3 d)$ - using (2)

$k_1 - k_2 = k \; k_3$

$\Rightarrow$ $\frac{a}{d} - \frac{b}{d} = k\left(\frac{n}{d}\right)$

$\therefore$ $\boxed{\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{n}{d}\right)}$

2) Give an example to show that $a^2 \equiv b^2 \pmod n$ need not imply $a \equiv b \pmod n$

2) $5^2 \equiv 4^2 \pmod 3$ since $5^2 - 4^2 = 3.(3)$

But $5 \not\equiv 4 \pmod 3$ $25 - 16 = (3).3$

$\therefore$ $\boxed{a^2 \equiv b^2 \pmod n \not\Rightarrow a \equiv b \pmod n}$

vision

U19CS012

3.) If $a \equiv b \pmod n$, P.T. $\gcd(a,n) = \gcd(b,n)$

3.) $a \equiv b \pmod n$

$\Rightarrow$ $a - b = kn$, some k

Let $d = \gcd(a,n)$

$\therefore$ $a = dr$, for some r, s

$n = ds$

$\because$ $a - b = kn$

$\therefore$ $dr - b = k(ds)$

$b = d(r - ks)$

$\therefore$ $d \mid b$ —— ①

Let $d' = \gcd(b,n)$

$\therefore$ Since d/n and d/b, $d \leq d'$

By similar reasoning as above, $d' \mid a$

$\therefore$ $d' \leq d$

$\therefore$ $d' = d$

$\therefore$ $\boxed{\gcd(b,n) = \gcd(a,n)}$

4.) Find the remainder when 41^{65} is divided by 7 ?

$41^{65} \div 7$ $(41^5)^{13}$, $41 = 5 \times (7) + 6$

$\therefore$ $41 = 6 \pmod 7$

$\therefore$ $41^5 = 6^5 \pmod 7$

$\therefore$ $6^5 \equiv 6 \pmod 7$

$\therefore$ $41^{65} = (41^5)^{13} \equiv (6^5)^{13} = 6^{13} \pmod 7$

$\therefore$ $41^{65} = (6^5)^{13} = 6^{13} = 6 \pmod 7$

$\therefore$ $41^{65} \div 7 =$ has remainder $\boxed{6}$

U19CS012

5> Prove that the integer $53^{103} + 103^{53}$ is divisible by 39.

5> To Prove: $53^{103} + 103^{53} \equiv 0 \pmod{39}$

Proof: $39 = 3 \times 13$

$53 = (3 \times 17) + 2 = (3 \times 18) - 1$

$103 = (34 \times 3) + 1$

$\therefore 53 = (-1) \pmod{13}$ $\qquad$ $103 = 1 \pmod{13}$

$\therefore (53)^{103} = (-1)^{103} \pmod{13}$ $\qquad$ $\therefore (103)^{53} = (1)^{53} \pmod{13}$ $\Big\}$ 3

$(53) \equiv 1 \pmod{13}$ $\qquad$ $103 = -1 \pmod{13}$

$\therefore (53)^{103} = 1 \pmod{13}$ $\qquad$ $\therefore (103)^{53} = (-1) \pmod{13}$ $\Big\}$ 13

Now, $\therefore 53^{103} + 103^{53} \equiv -1 + 1 \equiv \underline{0 \pmod{3}}$

$53^{103} + 103^{53} = -1 + 1 = \underline{0 \pmod{13}}$

$\therefore$ Both 3 and 13 divide the sum and $\gcd(3, 13) = 1$

So, Acc to theoram 4.3 (corollary 2)

$(3) \times (13) = (39)$ also divides the sum.

Hence,

$$\boxed{(53^{103} + 103^{53}) \equiv 0 \pmod{39}}$$

6.> If $a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_n$ is also complete set of residues modulo n.

6> Consider aa_i and aa_j, $i \neq j$, $1 \leq i, j \leq n$

If aa_i and aa_j are congruent mod n,

then $(aa_i - aa_j) = kn$, for some k

$\therefore a(a_i - a_j) = kn$

$\because \gcd(a, n) = 1$, Then by Euclid's Lemma,

$n \mid (a_i - a_j)$, contradicting that $a_i \not\equiv a_j$

$$\boxed{\therefore aa_i \not\equiv aa_j}$$

VISION

U19CS012

By Theorem 1: $A = \{a_1, a_2, \dots a_n\}$ is a complete set of residues modulo n $\iff$ for $a_i, a_j \in A$, $a_i \neq a_j$
$a_i \not\equiv a_j \pmod n$

Hence proved,

Acc to above theorem, $\{aa_1, aa_2, \dots, aa_n\}$ is a complete set

7.) Prove the following statement:
if $\gcd(a, n) = 1$, then the integers
$c, c+a, c+2a, c+3a, \dots, c+(n-1)a$
form a complete set of residues modulo x for any c.

7.) Consider $c + ra$ and $c + sa$, $r \neq s$ & $(0) \leq r, s \leq (n-1)$

Suppose $s > r$,

$\therefore$ $c + sa - (c + ra) = (s - r)a$

$(s - r) < n$ since $s \leq n-1$, $r \leq n-1$

$\therefore$ $n \nmid (s - r)$ since $\gcd(a, n) = 1$

Then,

There is no integer, k, such that
$(s - r)a = nk$
$\therefore$ $c + sa \not\equiv c + ra$

$\therefore$ So, the above set is a complete set of residues.

8.) Give an example to show that $a^k \equiv b^k \pmod n$ and $k \equiv j \pmod n$ need no imply that $a^j \equiv b^j \pmod n$

8.) $2^2 \equiv 3^2 \pmod 5$ since $4 \equiv 9 \bmod 5$

$2 \equiv 7 \pmod 5$

$2^7 \equiv 3^7 \pmod 5$?

$\left\{ \begin{array}{l} k = 2 \\ j = 7 \\ n = 5 \end{array} \right\}$

$2^7 = 128$, $3^7 = 2187$

$2187 - 128 = 2059$

So, $2^7 \not\equiv 3^7 \pmod 5$, Hence Proved.

U19CS012

9.) Use the theory of congruences to verify
$89 / 2^{44} - 1$ and $97 / 2^{48} - 1$

9.) (a) Show $89 / 2^{44} - 1$

Idea: Look at multiple of 89 to see of close or off by 1 from powers of 2.

$2^8 = (-11) \pmod{89}$ [$3 \times 89 = 267$]

$\therefore \underbrace{2^3 \, 2^8}_{} = 2^3 (-11) \pmod{89}$ and $\left\{ \begin{array}{l} 2^3 (-11) \\ \equiv 1 \pmod{89} \end{array} \right\}$

$\therefore 2^{11} \equiv 1 \pmod{89}$

$\boxed{\therefore 2^{44} = 1 \pmod{89}}$ & Hence $[89 / (2^{44} - 1)]$

(b) $97 / 2^{48} - 1$

97 is close to 100, so look at power of two close to 100's.

We find that

$21 . 97 = 2037$

$\therefore 2^{11} = 2048 = 11 \pmod{97}$

$\therefore 2^{12} = 4096 = (2.11) \pmod{97}$

$\therefore 2^{48} \equiv 2^4 . 11^4 \pmod{97}$

But $2^4 . 11^4 = (4.121)^2 = (484)^2$ and $(5 \times 97 = 485)$

$\therefore 484 = (-1) \pmod{97}$

$\therefore (4 \times 121) = (-1) \pmod{97}$

$\therefore 2^4 . 11^4 = (4.121)^2 \equiv 1 \pmod{97}$

$\boxed{\therefore 2^{48} = 1 \pmod{97}}$

Hence, $97 / (2^{48} - 1)$

U19CS012

10.) Find the remainder when $(4444)^{4444}$ is divided by 9.

10.) Note that $4444 \pmod 9 \equiv (4+4+4+4) \equiv 16 \pmod 9$

$16 = (2^3).(2)$,

So, $4444 \pmod 9 = 2^3 . 2 \pmod 9$

Since $2^3 \equiv (-1) \pmod 9$, then $4444 \equiv (-1).(2) \pmod 9$

$\therefore 4444^{4444} = (-1)^{4444} 2^{4444} \equiv 2^{4444} \pmod 9$

But,

$4444 = (3 \times 1381) + 1$, so,

$2^{4444} = (2^3)^{1381} . 2 \quad \therefore 2^{4444} = (-1)^{1381} . 2 \pmod 9$

$\therefore 4444^{4444} \equiv 2^{4444} \equiv (-1)(2) \pmod 9$
$\equiv 7 \pmod 9$

$\therefore$ Remainder $4444^{4444}/9 \Rightarrow \boxed{7}$

11.) Find the values of $n \geq 1$ for which $1! + 2! + 3! + \cdots + n!$ is a perfect square.

$1! = 1$

$2! = 2$ Note that for $n \geq 5$, $\sum_{K=1}^{n} n!$ ends in 0

$3! = 6$

$4! = 24$

$\therefore 1! = 1^2$ ✓

$1! + 2! = 3$

$1! + 2! + 3! = 9 = 3^2$ ✓

$1! + 2! + 3! + 4! = 33$

Therefore, the units digit of $\sum_{K=1}^{n} n!$ will be 3, for $n \geq 4$

But, we know that a perfect square can't end with '3'.

$\therefore$ There is no perfect square for $n \geq 4$.

Ans: for $n = \{1, 3\} \rightarrow \sum_{K=1}^{n} n!$ is perfect square.
{2 values}

U19CS012

12.) Use binary exponential algorithm to compute $19^{53} \pmod{503}$

12.) $53 = 1+4+16+32$ thus

$$19^{53} = 19^{1+4+16+32}$$

$$19^{1} = 19 \pmod{503}$$

$$19^{4} = 44 \pmod{503}$$

$$19^{16} = (19^{4})^{4} = (44)^{4} = 243 \pmod{503}$$

$$19^{32} = (19^{16})^{2} = (243)^{2} = 198 \pmod{503}$$

So, $19^{53} = 19^{1+4+16+32}$

$= (19) \times (19^{4}) \times (19^{16}) \times (19^{32})$

$= (19 \times 44 \times 243 \times 198) \pmod{503}$

$= \boxed{406 \pmod{503}}$

13.) Without performing the divisions, determine whether the integers 176,521,221 and 149,235,678 are divisible by 9 or 11.

13.) $N = a_m (10)^m + a_{m-1} (10)^{m-1} + \dots a_1 (10)^1 + a_0$

[Decimal expansion of Given N]

[176,521,221 is divisible by 9 if (Sum of digits) is divisible by 9]

$176,521,221 = 1+7+6+5+2+1+2+2+1 = 27$

$\therefore$ divisible by 9 $\qquad S = a_0 + a_1 + a_2 + \dots a_m$

for 11, $T = a_0 - a_1 + a_2 + \dots + (-1)^m a_m$

$T = 1-7+6-5+2-1+2-2+1$

$= -3$ $\qquad \therefore$ not divisible by 11

$11 \nmid (-3) \quad \therefore \quad 11 \nmid 176,521,221$

Therefore, 176,521,221 is divisible by 9 and not divisible by 11.

SUBMITTED BY:

BHAGYA VINOD RANA

U19CS012

[II^{nd} Yr, CSE]