Krithikha Balamurugan U19CS076

Tutorial - 3
U19CS076

1. a) Given

$a = b \pmod n \Rightarrow a = b + kn$

$a - b = kn \rightarrow k \in I$

Multiplying both sides with c

$ca - cb = kcn$

$ca = cb + k(cn)$

can be written

$ca = cb \pmod{cn}$

b) Given

$a = b \pmod n$

$\Rightarrow a = b + kn \quad k \in I$

$a - b = kn$

Dividing both the sides with d

$\frac{a-b}{d} = \frac{kn}{d}$

$\frac{a}{d} - \frac{b}{d} = k(n/d)$

$a/d = b/d + kn/d$

$a/d = b/d \pmod{n/d}$

2. ~~Given~~ If we are doing $a^2 = b^2 \pmod n$

$a^2 - b^2 = kn$ where $k \in I$

take $a = 1, \ b = 3, \ n = 4$

$1 - 3^2 = k(4)$

$-8/4 = k$

$k = -2$ True

And now $a = b \pmod n$

$a - b = hn$

$$1 - 3 = h(4)$$
$$-2/4 = h$$
$$h \notin I \text{ (false)}$$
Hence $a \not\equiv b \pmod n$

(3) Given

$$a \equiv b \pmod n$$
$$a = b + kn \qquad k \in I$$
here $a, b, n \in I$

Now lets assume $\gcd(a, n) = d$ and $\gcd(b, n)$

Dividing eq (1) by d

$$a/d = b/d + kn/d$$
$$a/d - kn/d = b/d$$
it amplies $d/b \Rightarrow d \leq c$

Now again,
$$a/c = b/c + kn/c$$
It implies c/a which means $c \leq d$
Thus $c = d \Rightarrow \gcd(a, n) = \gcd(b, n)$

(4) If 41^{65} is divided by 7 then remainder
$$41 \equiv (-1) \bmod 7$$
Therefore :- If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$
for any +ve positive integer k.

$$(41)^{65} \equiv (-1)^{65} \bmod 7 \qquad k = 65$$
$$41^{65} \equiv (-1) \bmod 7$$
Our remainder should be +ve so,
$$7 - 1 = 6$$
$$(41)^{65} \equiv 6 \pmod 7$$

Scanned with CamScanner

n

remainder $\to 6$

Q. We have to prove that integer $53^{103} + 103^{53}$ is divisible by 39

$$39 = 3 \times 13$$
$$53^{103} + 103^{53}$$

Now take 53^{103}

$$53 \equiv 2 \pmod 3$$
or
$$53 \equiv -1 \pmod 3$$

* Thm :- If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$

$$53^{103} \equiv (-1)^{103} \bmod 3$$
$$53^{103} \equiv -1 \bmod 3$$

remainder $= -1$

Now for 103^{53}

$$103 \equiv 1 \pmod 3$$

* Theorem $103^{53} \equiv (1)^{53} \bmod 3$

$$103^{53} \equiv 1 \pmod 3$$

remainder $= 1$

Now $-1 + 1 = 0$

so $3 \mid 53^{103} + 103^{53}$

for 13

take 53^{103}

$$53 \equiv 1 \pmod{13}$$

* Theorem $53^{103} \equiv 1^{103} \pmod{13}$

$$53^{103} \equiv 1 \pmod{13}$$

remainder $= 1$

take 103^{53}

Theorem $103 \equiv -1 \pmod{13}$

$$(103)^{53} \equiv (-1)^{53} \bmod 13$$
$$\equiv (-1) \bmod 13$$

Scanned with CamScanner

remainder = -1

Now $-1+1=0$

implies $13 \mid 53^{103} + 103^{53}$

Hence proved, $59 \mid 53^{103} + 103^{53}$

(6) Contradiction that:-

$aa_i - aa_j = 0 \pmod n$

$a(a_i - a_j) = 0 \pmod n$ — (1).

Where $i, i \in \{1, 2, \ldots n\}$, $i \neq j$.

Then since $\gcd(a, n) = 1 \rightarrow (2)$

$a_i - a_j \leq 0 \pmod n$

from eq^n (1) & (2)

Now given $a_1, a_2, \ldots, a_n$ is a complete set of residues module n.

And elementary euclid's theorem lema, which stats that if $\gcd(x, y) = 1$, and $x \mid yz$ then $x \mid z$.

Completely false here..

So here $aa_1, aa_2 \ldots aa_n$ is also a complete set of residues module n.

(7) Suppose $\gcd(a, n) = 1$ — (1)

Suppose c is any integer.

Consider ~~for~~ the system $c + 0a, c + 1a, c + 2a \ldots$

$\ldots c + (n-1)a$

There are n distinct terms of form $c + ka$ where $0 \leq k \leq n-1$

If any two members of this n member collections are incongruent modulo n, than its in the

Scanned with CamScanner

n

complete residue system module n.
suppose $c+ra$, $c+sa$ are two arbitary distinct members of n ~~num~~ member family above

Then $0 \le t \ne s \le n-1$ — (3)

Suppose $c+ta \equiv c+sa \pmod{n}$

That is, $n \mid (c+ta)-(c+sa)$

$n \mid (t-s)a$ — (4)

Recollect the divisibility property "if $\gcd(a,b)=1$ and $a \mid bc$ then $a \mid c$."

In the present cake (1) and (4) forces that $n \mid t-s$.

But (3) says $t-s<n$ and so $n \mid t-s$ is an absurdity.

So the supposition is wrong.

Therefore, no two members of (2) are congruent module n. Since these are n members, if it is complete residue system modulo n.

2. For example take $a=1, b=2, k=2, n=3, j=5$

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

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

~~To~~ Trite

$k \equiv j \pmod{n}$

$2 \equiv 5 \pmod{3}$

True

but $a^j \equiv b^j \pmod{n}$

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

false

So it is shown that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ need not imply that $a^j \equiv b^j \pmod{n}$

Scanned with CamScanner

(9) Verify $89 \mid 2^{44} - 1$

$2^{11} = 1 \pmod{89}$

* Theorem :- If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$

$(2^{11})^4 = (1)^4 \bmod 89$

$2^{44} \equiv 1 \bmod 89$

it implies that $89 \mid 2^{44} - 1$

Verifies $97 \mid 2^{48} - 1$

$2^{12} = 22 \pmod{97}$

$(2^{12})^2 = 22^2 \pmod{97}$ (* Theorem)

$2^{24} = 484 \pmod{97}$

$484 = -1 \bmod 97$

$2^{24} \equiv -1 \bmod 97$

$(2^{24})^2 = (-1)^2 \bmod 97$

$2^{48} = 1 \bmod 97$

it implies $97 \mid 2^{48} - 1$

(10) $4444 = 7 \pmod 9$

so $(4444)^{4444} = 7^{4444} \pmod 9$

$= 7^{4+40+400+4000} \pmod 9$

Now

$7^4 \equiv 7 \pmod 9$

$7^{40} = (7^4)^{10} = 7^{10} = (7^4)^2 \cdot 7^2 = 7^4 = 7 \pmod 9$

$7^{400} = (7^4)^{100} = 7^{100} = (7^4)^{25} = 7^{25} = (7^4)^6 \cdot 7$

$= 7^6 \cdot 7$

$\equiv 7 \pmod 9$

$7^{4000} = (7^{400})^{10} = 7^{10} = (7^4)^2 \cdot 7^2 = 7^4 \equiv 7 \pmod 9$

So $7^{4444} \equiv 7^4 \equiv 7 \pmod 9$

Scanned with CamScanner

11. Value for $1! + 2! + 3! + 4! + \cdots + n!$ is a perfect square.

For $n \geq 4$ above series consist of 3 as last digit after sum and for $n \geq 4$ $1! + 2! + 3! + \cdots n!$ is congruent to 3 mod 5. But all squares are congruent to 0, 1 or 4 mod 5.

Now for $n < 4$

$n = 3$ $\quad 1! + 2! + 3! = 9$ $\quad$ Perfect square

$n = 2$ $\quad 1! + 2! = 3$ $\quad$ Not possible

$n = 1$ $\quad 1 = 1$ $\quad$ Perfect square

Only for $n = 1$ and $n = 3$ $1! + 2! + 3! + \cdots n!$ is a perfect square.

12. $19^{53} \pmod{503}$

$53 = 1 + 4 + 16 + 32$ thus

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

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

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

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

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

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

$= 19 \cdot 19^4 \cdot 19^{16} \cdot 19^{32}$

$= 19(44)(243)(198) \bmod 503$

$= 406 \pmod{503}$

13. $N = a_m 10^m + a_{m-1} 10^{m-1} + a_{m-2} 10^{m-2} + \cdots$
$\cdots + a_1 10 + a_0$

Scanned with CamScanner

it is decimal expansion of given N
Here $N = 176521221$

176521221 is only divisible by 9 iffs
$S = a_0 + a_1 + \cdots a_m$ divisible by 9
so

$S = 1+7+6+5+2+1+2+2+1 = 27$
$S = 27$
which is divisible by 9 so
$9 \mid 176521221$
For 11
$T = a_0 - a_1 + a_2 + \cdots \cdots (-1)^m a_m$
$T = 1 - 7 + 6 - 5 + 2 - 1 + 2 - 2 + 1$
$= -3$
$11 \nmid T$ so $11 \nmid 176521221$

Scanned with CamScanner