LASA TUTORIAL - 6 (NUMBER THEORY)

U19CS012

U19CS012 [BHAGYA RANA]

1) Use Fermat's theorem, to verify that 17 divides $11^{104}+1$.

Since $17 \nmid 11$, $11^{17-1} \equiv 1 \pmod{17}$ [Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$]

$$11^{16} \equiv 1 \pmod{17} \quad -(1)$$

$$\therefore (11^{16})^6 = 11^{96} \equiv 1 \pmod{17} \quad -(2) \quad [\text{using } (1)]$$

But $121 = 11^2$ and $7 \cdot 17 = 119 = 121 - 2$

$\therefore 11^2 = 2 \pmod{17}$ $\quad [11^2 = (7 \cdot 17) + 2]$

$\therefore 11^8 = 2^4 = 16 \pmod{17} \quad -(3)$ [using above]

11^{104} ?

$\therefore (11^{96} \cdot 11^8) = 16 \pmod{17}$

But $16 \pmod{17} \equiv -1 \pmod{17}$

$\therefore 11^{104} \equiv -1 \pmod{17}$

$\Rightarrow 17 \mid (11^{104}+1)$, Hence Proved.

2) (a) If $\gcd(a, 35) = 1$, Show that $a^{12} \equiv 1 \pmod{35}$

Since $35 = 7 \cdot 5$, then $\gcd(a, 7) = 1$, $\gcd(a, 5) = 1$

$\therefore$ By Fermat's theorem $[a^{p-1} \equiv 1 \pmod{p}]$

$$a^6 \equiv 1 \pmod{7} \quad \text{and} \quad a^4 \equiv 1 \pmod{5}$$

$$\therefore a^{12} = a^6 \cdot a^6 = 1 \pmod{7}, \quad (a^4)^3 = a^{12} = 1^3 \pmod{5}$$

Since $\gcd(5, 7) = 1$,

$\therefore 35 \mid (a^{12}-1) \Rightarrow a^{12} \equiv 1 \pmod{35}$

U19CS012

(b) If $\gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.

Since $42 = 7 \cdot 3 \cdot 2$,

$$\gcd(a,7) = \gcd(a,3) = \gcd(a,2) = 1$$

By Fermat's theorem,

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

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

$$a \equiv 1 \pmod 2$$

But

$a^2 \equiv 1 \pmod 3 \Rightarrow a^6 \equiv (a^2)^3 \equiv 1^3 = 1 \pmod 3$, so

$$a^6 \equiv 1 \pmod 3$$

Also, $a^6 - 1 = (a-1)(a^5 + a^4 + a^3 + a^2 + a + 1)$

$= (a-1)[a^3(a^2+a+1) + a^2+a+1]$

$= (a-1)(a^3+1)(a^2+a+1)$

$= (a-1)(a+1)(a^2-a+1)(a^2+a+1)$

Assume $|a| > 1$, since a is odd

→ if $a > 0$, then $a \geq 3$, so $2 \mid (a-1)$ and $4 \mid (a+1)$

$\therefore 8 \mid (a^6 - 1)$

→ if $a < 0$, then $a \leq 3$, so $4 \mid (a-1)$ & $2 \mid (a+1)$

so, $8 \mid (a^6 - 1)$

Since, $7 \mid a^6 - 1$, $3 \mid a^6 - 1$, and $8 \mid a^6 - 1$ and 3, 7, 8 are relatively prime, then $\boxed{3 \cdot 7 \cdot 8 = 168 \mid a^6 - 1}$, Hence proved.

Q3.> Derive the following congruences

(a) $a^{21} \equiv a \pmod{15} \quad \forall a$

$a^5 \equiv a \pmod 5$ [If p is prime, then $a^p \equiv a \pmod p$ for any integer a]

$\therefore (a^5)^4 \equiv a^4 \pmod 5$

$\therefore a^{20} \equiv a^4 \pmod 5$

$\therefore \boxed{a^{21} \equiv a^5 \equiv a \pmod 5}$

Also, $a^3 \equiv a \pmod 3$, $\therefore a^{21} \equiv a^7 \pmod 3$

and $(a^3)^2 \equiv a^2 \pmod 3$

$a^6 \equiv a^2 \pmod 3$

$\therefore a^7 \equiv a^3 \pmod 3$

$\therefore \boxed{a^{21} \equiv a \pmod 3}$ $[\, a^3 \pmod 3 \equiv a \pmod 3 \,]$

$\therefore 5 \mid (a^{21} - a)$ and $3 \mid (a^{21} - a)$

$\therefore 3.5 \mid a^{21} - a$

$\boxed{\therefore a^{21} \equiv a \pmod{15}}$, Hence Proved

(b) $a^9 \equiv a \pmod{30}$ $\forall\, a$

$30 = 5.3.2$

Using Fermat's theorem $a^5 \equiv a \pmod 5$

$\therefore a^9 \equiv a^5 . a^4 \equiv a . a^4 \equiv a^5 \equiv a$

$\boxed{\therefore a^9 \equiv a \pmod 5}$

$a^3 \equiv a \pmod 3$ $\therefore (a^3)^3 \equiv a^3 \equiv a \pmod 3$

$\boxed{\therefore a^9 \equiv a \pmod 3}$

$a^2 \equiv a \pmod 2$ $\therefore a^8 \equiv (a^2)^4 \equiv a^4 \pmod 2$

$a^4 \equiv (a^2)^2 \equiv a^2 \equiv a \pmod 2$

$\therefore a^8 \equiv a \pmod 2$

$\therefore \boxed{a^9 \equiv a^8 . a \equiv a . a \equiv a^2 \equiv a \pmod 2}$

$\therefore 5 \mid (a^9 - a)$, $3 \mid (a^9 - a)$ and $2 \mid (a^9 - a)$

$\therefore a^9 \equiv a \pmod{5.3.2}$

$\boxed{a^9 \equiv a \pmod{30}}$, Hence Proved

U19CS012

4.) If $\gcd(a, 30) = 1$, show that 60 divides $(a^4 + 59)$.

$\gcd(a, 30) = 1 \Rightarrow \gcd(a, 2) = \gcd(a, 3) = \gcd(a, 5) = 1$

Also, $\gcd(a, 4) = \gcd(a, 2^2) = 1$

$60 = 2^2 \cdot 3 \cdot 5$ $\quad 60 \mid a^4 + 59$ is same as

$a^4 \equiv -59 \pmod{60}$

$\boxed{a^4 \equiv 1 \pmod{60}}$

$[a^{p-1} \equiv 1 \pmod{p}]$

$\gcd(a, 5) \equiv 1 \Rightarrow \boxed{a^4 \equiv 1 \pmod{5}}$ by Fermat's theorem

$\gcd(a, 3) \equiv 1 \Rightarrow a^2 \equiv 1 \pmod{3}$ $\quad \boxed{\therefore a^4 \equiv 1 \pmod{3}}$

$\gcd(a, 2) = 1 \Rightarrow a \equiv 1 \pmod{2}$, $\therefore a^2 \equiv 1 \pmod{2}$

$\therefore a^2 \equiv 1 - 2 = -1 \pmod{2}$

$\therefore 2 \mid a^2 - 1$, $2 \mid a^2 + 1$, $\therefore \boxed{4 \mid (a^2+1)(a^2-1) = (a^4 - 1)}$

$\therefore 5 \mid (a^4 - 1)$, $3 \mid (a^4 - 1)$, $4 \mid (a^4 - 1)$ and

$\gcd(5, a) = \gcd(3, a) = \gcd(4, a) = 1$

$\therefore 60 \mid (a^4 - 1)$

$\therefore a^4 \equiv 1 \pmod{60}$, $a^4 \equiv 1 - 60 \equiv -59 \pmod{60}$

$\therefore 60 \mid (a^4 + 59)$, hence Proved.

U19CS012

5.) Find the units digits of 3^{100} by Fermat's theorem.

5.)

For unit's digit, we need (something) mod 10 $\quad 10 = 5.2$

By Fermat's theorem, $\quad 3^4 \equiv 1 \pmod 5$

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

Also, $3 \equiv 1 \pmod 2 \quad \therefore 3^{100} \equiv 1 \pmod 2$

$\therefore 5 \mid 3^{100} - 1$ and $2 \mid 3^{100} - 1$

$\therefore 5.2 \mid 3^{100} - 1$ ~~by~~ corollary 2 [Fermat theorem corollary]

$\therefore 10 \mid 3^{100} - 1$

$\Rightarrow \boxed{3^{100} \equiv 1 \pmod{10}}$

$\therefore$ Unit's digit of 3^{100} is $\boxed{1}$.

6.) If $7 \nmid a$, Prove that either a^3+1 or a^3-1 is divisible by 7.

6.) By Fermat's theorem,

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

$\therefore 7 \mid (a^6 - 1)$, But $(a^6-1) = (a^3+1)(a^3-1)$

Suppose, $7 \nmid (a^3+1) \quad \therefore \gcd(7, a^3+1) = 1$

~~So~~ and so, by Euclid's Lemma

$\{7 \mid (a^3-1)\}$ [Hence

So, in either case a^3+1 or a^3-1 is divisible by 7. Proved]

7.) Assumming that a and b are integers not divisible by prime 'p' establish the following

(a) If $a^p \equiv b^p \pmod p$, then $a \equiv b \pmod p$

$a^p = a \pmod p$, $b^p = b \pmod p$ for any integers a, b.

$\therefore a \equiv a^p \equiv b^p \equiv b \pmod p$

(b) If $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$

[From Q7 (a) $a \equiv a^p \equiv b^p \equiv b \pmod p$]

$a = b + pk$, for some k

$$\left[{}^nC_r\,(a)^{n-r}(b)^r\right]$$

$$\therefore a^p - b^p = (b+pk)^p - (b)^p$$

$$= (b)^p + \sum_{i=1}^{p} \binom{p}{i} (b)^{p-i} (pk)^i - (b)^p$$

[Binomial expansion]

$$= \sum_{i=1}^{p} \frac{p!}{i!(p-i)!}\, b^{p-i} (pk)^i$$

[When $i > 2$, each term is divisible by p^2 since $(pk)^i$ has atleast p^2 in the term]

∴ Look at $i = 1$ term : $\dfrac{p!}{1!(p-1)!}\, b^{p-1}(pk)$

$$= p\, b^{p-1}(pk) = p^2 (b)^{p-1} k$$

Therefore, first term is divisible by (p^2).

∴ $\boxed{a^p - b^p \text{ is divisible by } p}$

8.) Use Fermat's theorem to prove that, if p is an odd prime, then

(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod p$

Since p is prime ≥ 3, Then $p \nmid a$ if $a < p$

∴ By Fermat theorem, $a^{p-1} \equiv 1 \pmod p$

∴ There are $(p-1)$ terms in $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1}$

∴

$$1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv (p-1).1 \pmod p$$

$(p-1).1 \equiv (p-1)$ [since $p \equiv 0 \pmod p$]

$$\boxed{1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod p}$$

[Also for $p = 2$] Valid

U19CS012

(b) $1^p + 2^p + \dots + (p-1)^p \equiv 0 \pmod p$

From Fermat theorem Corollary, $a^p \equiv a \pmod p$

$\therefore 1^p + 2^p + \dots + (p-1)^p \equiv 1 + 2 + \dots + (p-1) \pmod p$

$\because 1+2+3+\dots+n = (n(n+1))/2$

$1+2+3+\dots+(p-1) = ((p-1)(p-1+1))/2 = (p(p-1))/2$

As p is an odd prime, $(p-1)$ is even, so $p-1 = 2k$, some k.

$\therefore 1+2+\dots+(p-1) = pk$, some k

$\therefore 1^p + 2^p + 3^p + \dots + (p-1)^p \equiv pk \equiv 0 \pmod p$

9.7 Confirm the following integers are absolute pseudo primes.

(a) $1105 = 5.13.17$ Let a be any integer

If $1105 \nmid a$, Then $5 \nmid a$, $13 \nmid a$, $17 \nmid a$

$\therefore$ By Fermat's theorem,

$a^4 \equiv 1 \pmod 5$

$a^{12} \equiv 1 \pmod{13}$

$a^{16} \equiv 1 \pmod{17}$

$\therefore a^{1104} = (a^4)^{276} \equiv 1 \pmod 5$

$a^{1104} \equiv (a^{12})^{92} \equiv 1 \pmod{13}$

$a^{1104} \equiv (a^{16})^{69} \equiv 1 \pmod{17}$

$\therefore a^{1104} \equiv 1 \pmod{5.13.17}$ when $1105 \nmid a$

$\therefore a^{1105} \equiv a \pmod{1105}$, clearly $1105 \mid (a^{1105} - a)$

$\therefore a^{1105} \equiv a \pmod{1105}$ for all a.

(b) $2465 = 5 \cdot 17 \cdot 29$ Let a be any integer

If $2465 \nmid a$, then $5 \nmid a$, $17 \nmid a$, $29 \nmid a$

$\therefore a^4 \equiv 1 \pmod 5$, $a^{16} \equiv 1 \pmod{17}$, $a^{28} \equiv 1 \pmod{29}$

$a^{2464} = (a^4)^{616} \equiv 1 \pmod 5$

$a^{2464} = (a^{16})^{154} \equiv 1 \pmod{17}$

$a^{2464} = (a^{28})^{88} \equiv 1 \pmod{29}$

$\therefore a^{2464} \equiv 1 \pmod{5 \cdot 17 \cdot 29}$ when $2465 \nmid a$.

$\therefore a^{2465} \equiv a \pmod{2465}$ when $2465 \nmid a$.

But when $2465 \mid a$, clearly $a^{2465} \equiv a \pmod{2465}$

$\therefore$ For all a,

$$\boxed{a^{2465} \equiv a \pmod{2465}}$$

10.) Find the remainder when $15!$ is divided by 17.

Since $(17-1)! \equiv -1 \pmod{17}$ [Wilson Theorem] $(p-1)! \equiv -1 \pmod p$

$\therefore 16! \equiv -1 \pmod{17}$

But $16 \equiv -1 \pmod{17}$

$\therefore 16! = 16 \pmod{17}$, $\gcd(16, 17) = 1$

$\therefore \frac{16!}{16} = \frac{16}{16} \pmod{17}$

Ans: $\boxed{\therefore 15! = 1 \pmod{17}}$ Remainder : (1)

U19CS012

11.) Arrange the integers 2, 3, 4, ... 21 in pairs a and b that satisfy $ab \equiv 1 \pmod{23}$

Look for

$23(1) + 1 = 24$ ✓ $\quad 23(6) + 1 = 138$

Not $23(2) + 1 = 47$ (prime) $\times \quad 23(7) + 1 = 162$ ✓

$23(3) + 1 = 70$ ✓ $\quad 23(8) + 1 = 185$

$23(4) + 1 = 93 \quad 23(9) + 1 = 208$ ✓

$23(5) + 1 = 116 \quad 23(10) + 1 = 231$ ✓

$23(13) + 1 = 300$ ✓ $\quad 23(14) + 1 = 323$ ✓

ANS:

$2 \cdot 12 = 24 \equiv 1 \pmod{23}$

$3 \cdot 8 = 24 \equiv 1$ "

$4 \cdot 6 = 24 \equiv 1$ "

$5 \cdot 14 = 70 \equiv 1$ "

$7 \cdot 10 = 70 \equiv 1$ "

$9 \cdot 18 = 162 \equiv 1$ "

$11 \cdot 21 = 231 \equiv 1$ "

$13 \cdot 16 = 208 \equiv 1$ "

$15 \cdot 20 = 300 \equiv 1$ "

$17 \cdot 19 = 323 \equiv 1$ "

12.) Show that $18! \equiv -1 \pmod{437}$

$19 \mid 437$ since $19 \cdot 23 = 437$

By wilson theorem, $18! \equiv -1 \pmod{19}$

To show: $23 \mid (18! + 1)$

By Wilson Theorem, $22! \equiv -1 \equiv 22 \pmod{23}$

$\therefore \frac{22!}{22} \equiv \frac{22}{22} \equiv 1 \pmod{23} \quad (\gcd(22, 23) = 1)$

$\therefore 21! \equiv 1 \equiv (1 + 23) \equiv 24 \pmod{23}$

$\therefore 21 \times 20! \equiv 8 \cdot 3 \pmod{23} \quad (\gcd(3, 23) = 1)$

$7 \times 20! \equiv 8 \pmod{23}$

$\therefore 7 \times 20 \times 19! \equiv 8 \pmod{23}$

$[\because \gcd(23,4) = 1]$

$7.5.19! \equiv 2 \pmod{23}$

$7.5.19.18! \equiv 2 \pmod{23}$

$\therefore 7.5.19.18! = 2+23 = 25 \pmod{23}$ $[\gcd(5,23) = 1]$

$7.19.18! = 5 \pmod{23}$

$= (5+23) \pmod{23} = 28 \pmod{23}$

~~$7.19.18!$~~ $= ~~7~~.4 \pmod{23}$ (since $\gcd(7,23) = 1$)

$19.18! = (4-23) \pmod{23}$

~~$19.18!$~~ $= (-19) \pmod{23}$

$18! = (-1) \pmod{23}$ $[\gcd(19,23) = 1]$

$\therefore 23 \mid (18! + 1)$ and $19 \mid (18! + 1)$

$\therefore 19.23 = 437 \mid (18! + 1)$

$\therefore 18! = -1 \pmod{437}$

13.) Given a prime number p, Establish the congruence.

$(p-1)! = (p-1) \pmod{1+2+3+\ldots+(p-1)}$

From Wilson th., $(p-1)! \equiv -1 \equiv (-1+p) \pmod{p}$

$\therefore p \mid (p-1)! - (p-1)$

$\therefore 1+2+\ldots+(p-1) = \frac{(p-1)(p-1+1)}{2} = \left(\frac{p(p-1)}{2}\right)$ $\left[1+2+3+\ldots+n = \frac{n(n+1)}{2} \ \forall n\right]$

$\because (p-1)$ is even, $(p-1)/2$ is integer, $\frac{(p-1)}{2} < (p-1)$

Also, $(p-1) \mid (p-1)! - (p-1)$

$\therefore (p-1)/2 \mid (p-1)! - (p-1)$

Also $\gcd((p-1)/2, p) = 1$ since p is prime

$\therefore p$ and $\frac{(p-1)}{2}$ divide $(p-1)! - (p-1)$,

so, $\frac{p(p-1)}{2} = 1+2+3+\ldots+(p-1)$ divides $(p-1)! - (p-1)$

$\therefore (p-1)! \equiv (p-1) \pmod{1+2+3+\ldots+(p-1)}$

Hence proved