Note Title 8/23/2022

Lecture 9: 23/8/2022

Ex1: Prove that $2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$.

Solution: $1111 \equiv 5 \pmod 7$

$\Rightarrow 2222 \equiv 10 \equiv 3 \pmod 7$ and $5555 \equiv 25 \equiv 4 \pmod 7$.

By Fermat's Thm, $3^6 \equiv 1 \pmod 7$ and $4^6 \equiv 1 \pmod 7$

$\Rightarrow 2222^{5555} \equiv 3^{5555} \equiv 3^{925 \times 6 + 5} \equiv 3^5 \pmod 7 \equiv 2 \times 2 \times 3 \pmod 7$
$\equiv 5 \pmod 7$.

Also, $5555^{2222} \equiv 4^{2222} \equiv 4^{370 \times 6 + 2} \equiv 4^2 \pmod 7$
$\equiv 2 \pmod 7$.

$\therefore 2222^{5555} + 5555^{2222} \equiv 5 + 2 \equiv 0 \pmod 7$ #

Ex2: If p and q are distinct primes, then prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Soln: By Fermat's thm, $p^{q-1} \equiv 1 \pmod{q}$ & $q^{p-1} \equiv 1 \pmod{p}$.

$$\therefore (p^{q-1} - 1)(q^{p-1} - 1) \equiv 0 \pmod{pq} \quad [\because p \,\&\, q \text{ are distinct primes}].$$

$$\Rightarrow p^{q-1} q^{p-1} - p^{q-1} - q^{p-1} + 1 \equiv 0 \pmod{pq}$$

$$\Rightarrow p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} \quad [\because p^{q-1} q^{p-1} \equiv 0 \pmod{pq}].$$

#

Ex3: Find the least positive integer satisfying the congruences $x \equiv 4 \pmod{11}$ and $x \equiv 3 \pmod{17}$.

Solution: Here $m_1 = 11$, $m_2 = 17$, $m = 11 \times 17$, $a_1 = 4$, $a_2 = 3$.

$$\frac{m}{m_1} b_1 \equiv 1 \pmod{m_1} \Rightarrow 17 \cdot b_1 \equiv 1 \pmod{11}$$
$$\Rightarrow 6 \cdot b_1 \equiv 1 \pmod{11} \Rightarrow b_1 \equiv 2 \pmod{11}$$

$$\frac{m}{m_2} b_2 \equiv 1 \pmod{m_2} \Rightarrow 11 b_2 \equiv 1 \pmod{17} \Rightarrow b_2 \equiv 14 \pmod{17}.$$
$$\equiv -3 \pmod{17}$$

$$\therefore\ x_0 = \frac{m}{m_1} a_1 b_1 + \frac{m}{m_2} a_2 b_2 = 17 \times 4 \times 2 - 11 \times 3 \times 3$$
$$= 136 - 99 = 37.$$

If we take $b_2 = 14$ instead of -3, then $x_0 = 136 + 462 = 598 \equiv 37 \pmod{m}$, where $m = m_1 \times m_2 = 187$.

$\therefore$ The least positive integer is 37. #

<u>Ex4:</u> Find the remainder of 2^{600004} when it is divided by 77

<u>Soln:</u> $\gcd(2,77)=1$. By Euler's thm, $2^{\varphi(77)} \equiv 1 \pmod{77}$

We have $\varphi(77) = \varphi(7)\,\varphi(11) = 6 \times 10 = 60$

$$\therefore\ 2^{60} \equiv 1 \pmod{77}.$$

Now, 2^{600004}

$$= 2^{600000} \times 2^4 \equiv 2^4 \pmod{77}$$

$$\equiv 16 \pmod{77}.$$

$\therefore$ The required remainder is 16. #

Ex5 Find all positive integers a, b for which $a^4 + 4b^4$ is a prime.

Soln:

$$
\begin{aligned}
a^4 + 4b^4 &= a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2 \\
&= (a^2 + 2b^2)^2 - 4a^2b^2 \\
&= (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab) \\
&= [(a+b)^2 + b^2][(a-b)^2 + b^2].
\end{aligned}
$$

Since $(a+b)^2 + b^2 > 1$, so $a^4 + 4b^4$ is a prime only if $(a-b)^2 + b^2 = 1 \Rightarrow a = b = 1$, which is the only solution of the problem.

#

__Ex6:__ For each positive integer n, find $\gcd(n!+1, (n+1)!)$.

__Soln:__ Let $d = \gcd(n!+1, (n+1)!)$.

__Case I:__ ($n+1$ is composite) If $n+1$ is composite, then each prime divisor of $(n+1)!$ is a prime less than n, and so it also divides $n!$, and hence it does __not__ divide $n!+1$.

$\therefore \gcd(n!+1, (n+1)!) = 1$.

__Case II:__ ($n+1$ is prime). If $n+1$ is prime, then all other prime divisors of $(n+1)!$ are less than n. Such a prime divides $n!$ and it does not divide $n!+1$. Thus, if $(n+1)$ is a prime, then $d = 1$ or $n+1$.

By Wilson's thm, $(n+1-1)! \equiv -1 \pmod{n+1}$

$(\because n+1$ is a prime$)$

$\Rightarrow n+1 \mid n!+1$

$\therefore d = \gcd(n!+1, (n+1)!) = n+1$ if $n+1$ is a prime.

——— × ———

Ex7: Let p be an odd prime. Prove that

$1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ and $2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

#

<u>Soln:</u> By Wilson's thm, we have $(p-1)! \equiv -1 \pmod{p}$.

$\therefore \ [1\cdot 3 \cdot \ldots \cdot (p-2)][2\cdot 4 \cdot \ldots \cdot (p-1)] \equiv -1 \pmod{p}$

We have $1 \equiv -(p-1) \pmod{p}$, $3 \equiv -(p-3) \pmod{p}$

$\ldots\ldots \quad p-2 \equiv -(p-(p-2)) \pmod{p}$.

Therefore, $1\cdot 3 \cdot \ldots (p-2) \equiv (-1)^{\frac{p-1}{2}} (2\cdot 4 \cdots (p-1)) \pmod{p}$.

Now, $1^2 \cdot 3^2 \ldots (p-2)^2 = 1\cdot 3 \cdot \ldots (p-2)\,(1\cdot 3 \cdots (p-2))$

$\equiv (-1)^{\frac{p-1}{2}} (p-1)! \pmod{p} \equiv (-1)^{\frac{p-1}{2}+1} \pmod{p}$

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

Similarly, $2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$. #