MAT115A HW4

Tao Wang

November 3, 2024

(1)

Find the least nonnegative solution of each system of congruences below.

Question (a):

$x \equiv 1 \mod 2$
$x \equiv 2 \mod 3$
$x \equiv 3 \mod 5$
$x \equiv 4 \mod 7$

Answer:

Since $(m_1, m_2, m_3, m_4) = 1$, we can use the Chinese Remainder Theorem to find the solution.

M $= m_1 \times m_2 \times m_3 \times m_4 = 2 \times 3 \times 5 \times 7 = 210$

n	a_n	m_n	M_n	M_n^{-1}
1	1	2	105	1
2	2	3	70	1
3	3	5	42	3
4	4	7	30	4

$x = (1 \times 105 \times 1 + 2 \times 70 \times 1 + 3 \times 42 \times 3 + 4 \times 30 \times 4) \mod 210$
$= 1103 \mod 210 = 53$
$\boxed{x \equiv 53 \mod 210}$

Question (b):

$3x \equiv 2 \mod 4$
$4x \equiv 1 \mod 5$
$6x \equiv 3 \mod 9$

Answer:

To remove the coefficient in front of x, we can multiply each congruences by the inverse of the coefficient.

$3x * 3^{-1} \equiv 2 * 3^{-1} \mod 4$

$\implies x \equiv 2 \mod 4$

$4x * 4^{-1} \equiv 1 * 4^{-1} \mod 5$

$\implies x \equiv 4 \mod 5$

$6x \equiv 3 \mod 9$

$\implies 2x \equiv 1 \mod 3$

$\implies 2x * 2^{-1} \equiv 1 * 2^{-1} \mod 3$

$\implies x \equiv 2 \mod 3$

Now, we have

$x \equiv 2 \mod 3$

$x \equiv 2 \mod 4$

$x \equiv 4 \mod 5$

Therefore, $(m_1, m_2, m_3) = 1$, and we can use the Chinese Remainder Theorem to find the solution

$M = 3 * 4 * 5 = 60$

n	a_n	m_n	M_n	M_n^{-1}
1	2	3	20	2
2	2	4	15	3
4	4	5	12	3

$x = (2 \times 20 \times 2 + 2 \times 15 \times 3 + 4 \times 12 \times 3) \mod 60$

$= (80 + 90 + 144) \mod 60 = 14$

$\boxed{x \equiv 14 \mod 60}$

Question (c):

$x \equiv 3 \mod 6$

$x \equiv 7 \mod 10$

$x \equiv 12 \mod 15$

Answer:

$x \equiv 3 \mod 6$

$\implies x \equiv 1 \mod 2$ and $x \equiv 0 \mod 3$

$x \equiv 7 \mod 10$

$\implies x \equiv 1 \mod 2$ and $x \equiv 2 \mod 5$

$x \equiv 12 \mod 15$

$\implies x \equiv 0 \mod 3$ and $x \equiv 2 \mod 5$

Therefore, we have

$x \equiv 1 \mod 2$

$x \equiv 0 \mod 3$

$x \equiv 2 \mod 5$

Since $(2, 3, 5) = 1$, we can use the Chinese Remainder Theorem to find the solution.

$M = 2 * 3 * 5 = 30$

n	a_n	m_n	M_n	M_n^{-1}
1	1	2	15	1
2	0	3	10	1
4	2	5	6	1

x $= (1 \times 15 \times 1 + 0 \times 10 \times 1 + 2 \times 6 \times 1) \mod 30$

$= 27$

$\boxed{x \equiv 27 \mod 30}$

(2)

Use Wilson's Theorem to find the least nonnegative residue modulo m for each integer n below.

Question (a):

$n = 30!, m = 31$

Answer:

Choose $p = 31$. Then by Wilson's Theorem,

$(31 - 1)! \equiv 30 \mod 31$

$\boxed{30! \equiv 30 \mod 31}$

Question (b):

$n = 21!, m = 23$

Answer:

Choose $p = 23$. Then by Wilson's Theorem,

$(23 - 2)! \equiv 1 \mod 23$

$\boxed{21! \equiv 1 \mod 23}$

Question (c):

$n = \frac{31!}{22!}, m = 11$

Answer:

Notice that

$$\begin{aligned} 31 &\equiv 9 \mod 11 \\ 30 &\equiv 8 \mod 11 \\ &\vdots \\ 23 &\equiv 1 \mod 11 \end{aligned}$$

Therefore,

$$\frac{31!}{22!} \equiv 9! \mod 11$$

Choose $p = 11$. Then by Wilson's Theorem,

$\boxed{\frac{31!}{22!} \equiv 9! \equiv (11 - 2)! \equiv 1 \mod 11}$

(3)

Let p be an odd prime number.

Question (a):

Prove that $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}}$

Answer:

$$(p-1)! = (p-1) \times (p-2) \times \cdots \times \left(\frac{p+1}{2}\right) \times \left(\frac{p-1}{2}\right)!$$

Notice that

$$\begin{aligned} (p-1) &\equiv -1 \mod p \\ (p-2) &\equiv -2 \mod p \\ &\vdots \\ \left(\frac{p+1}{2}\right) &\equiv -\left(\frac{p-1}{2}\right) \mod p \end{aligned}$$

This means that

$$(p-1) \times (p-2) \times \cdots \times \left(\frac{p+1}{2}\right) \equiv (-1)^{\left(\frac{p-1}{2}\right)} \times \left(\frac{p-1}{2}\right)! \mod p$$

If we multiply $\left(\frac{p-1}{2}\right)!$ to both sides of the expression above, we get

$$(p-1)! \equiv (-1)^{\left(\frac{p-1}{2}\right)} \times \left(\left(\frac{p-1}{2}\right)!\right)^2 \mod p$$

Since p is a prime number,

$$(p-1)! \equiv -1 \mod p$$

by the Wilson's Theorem.
Therefore,

$$(-1)^{\left(\frac{p-1}{2}\right)} \times \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p$$

Multiply both sides by $(-1)^{\frac{p-1}{2}}$, we get

$$(-1)^{p-1} \times \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p$$

Since p is odd, $p-1$ is even, and -1 raised to an even power is 1.
Therefore,

$$\boxed{\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \mod p}$$

Question (b):

If $p \equiv 1 \mod 4$, prove that $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv -1 \mod p$.

Answer:

We were given

$$p - 1 = 4k$$

for some $k \in \mathbb{Z}$

Then,

$$p = 4k + 1$$

and

$$\frac{p+1}{2} = 2k + 1$$

By the result from part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{2k+1} \equiv -1 \mod p$$

Therefore, $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv -1 \mod p$.

Question (c):

If $p \equiv 3 \mod 4$, prove that $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv 1 \mod p$.

Answer:

We were given

$$p - 3 = 4k$$

for some $k \in \mathbb{Z}$

Then,

$$p = 4k + 3$$

and

$$\frac{p+1}{2} = 2k + 2$$

By the result from part (a),

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{2k+2} \equiv 1 \mod p$$

Therefore, $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv 1 \mod p$.