H/W

Find the least positive residue in

1. $3^{36} \pmod{77}$.

2. Use theory of congruence, Proof.

$$7 \mid 2^{5n+3} + 5^{2n+3} \quad \forall\, n \geq 1.$$

3. P.T $19^{20} \equiv 1 \pmod{181}$.

$$7 \mid 2^{5n+3} + 5^{2n+3} \quad \forall\, n \geq 1.$$

$$\begin{aligned} 2^{5n+3} + 5^{2n+3} &= 2^3 \cdot 2^{5n} + 5^{2n} \cdot 5^3 \\ &= 8 \cdot 2^{5n} + 125 \cdot 5^{2n} \\ &= \underbrace{8 \cdot \underline{32}^n + 125 \cdot 25^n}. \end{aligned}$$

$32 \equiv 25 \pmod{7}$ $\qquad$ $7 \mid 32 - 25$

$\Rightarrow 32^n \equiv 25^n \pmod{7}$ $\qquad$ $\forall\, n \geq 1$.

$\Rightarrow 32^n - 25^n \equiv 0 \pmod{7}$

$8 \cdot 32^n - 8 \cdot 25^n \equiv 0 \pmod{7}$. — (i)

$$\Rightarrow \quad 8 \cdot 32^n - 8 \cdot 25^n \equiv 0 \pmod 7. \quad -(i)$$

$$133 \equiv 0 \pmod 7$$

$$\Rightarrow \quad 25^n \cdot 133 \equiv 0 \pmod 7. \quad --- (ii)$$

$$8 \cdot 32^n - 8 \cdot 25^n + 133 \cdot 25^n \equiv 0 \pmod 7$$

$$\Rightarrow \quad 8 \cdot 32^n + 125 \cdot 25^n \equiv 0 \pmod 7$$

So, $7 \mid 2^{5n+3} + 5^{2n+3}$. $\boxed{\text{PROVED}}$

$19^{20} \equiv 1 \pmod{181}$

Sol^n:

$$19^2 \equiv -1 \pmod{181}$$

$$\Rightarrow (19^2)^{10} \equiv (-1)^{10} \pmod{181}$$

$$\Rightarrow 19^{20} \equiv 1 \pmod{181}.$$

Find the remainder when

$1! + 2! + 3! + \dots + 50!$ divided by 15.

$$\Rightarrow \quad (1! + 2! + 3! + 4!)/15$$

$$1 + 2 + 6 + 24$$

-1 (

$= 1 + 2 + 6 + 24$

$= 33$ $\quad (5! + \dots 50!)$

15

$33 \equiv 3 \pmod{15}$

3 is the remainder.

$5! \equiv 0 \pmod{15}$

$(5+n)! \equiv 0 \pmod{15}$

$6! \equiv 0$

$7!$

$\vdots$

$\Rightarrow (1! + 2! + 3! + 4!) + \dots + 50! \equiv (1! + 2! + 3! + 4!) \pmod{15}$

$\equiv 33 \pmod{15}$

'3' is the remainder!

$= 3 \pmod{15}$

$5! \equiv 0 \pmod{15}$

$(5+n)! \equiv 0 \pmod{15}$ $\quad n = 1$

$6! \equiv 0 \pmod{15}$

$7! \equiv 0 \pmod{15}$

$\vdots$

$$50! \equiv 0 \pmod{15}$$

$$5! + \cdots + 50! \equiv 0 \pmod{15}.$$

$$(1! + 2! + 3! + 4!) + \cdots + 50! \equiv \underbrace{(1! + 2! + 3! + 4!)}_{33} \pmod{15}$$

Linear Congruence.

\# $5x \equiv 3 \pmod{11}$, find x.

\# $15x \equiv 9 \pmod{18}$. Find x

$5x \equiv 3 \pmod{11}$

$ax \equiv b \pmod{m}$

$\text{g.c.d}(a, m) = 1$.

$\text{g.c.d}(5, 11) = 1$.

↪ The congruence has a unique sol^n.

By Bezout's theorem,

$\exists$ u and v such that

$5u + 11v = \text{g.c.d}(5, 11)$

$5x \equiv 3 \pmod{11}$

$5u + 11v = g.c.d(5, 11)$

$\Rightarrow 5u + 11v = 1$. ---- (1)

$u = -2, \; v = 1$.

$5(-2) \equiv 1 \pmod{11}$ — (1)

Multiplying 3 on both sides we get :

$5x \equiv 3 \pmod{11}$

$5(-6) \equiv 3 \pmod{11}$.

$x = -6$ is a sol^n.

$-6 \equiv ? \pmod{11}$

$x \equiv -6 \pmod{11}$

$\equiv 5 \pmod{11}$.

All the sol^n are congruent to $5 \pmod{11}$.

Th^m: $ax \equiv b \pmod{m}$

$g.c.d(a, m) = d$, $d \nmid b$

This cong. eq^n has no solution.

Solve $15x \equiv 9 \pmod{18}$

$g.c.d(15, 18) = 3$, $3 \mid 9$

(... solution — - (1)

$\hookrightarrow$ Hence there exist solution. — — (1)

$15x \equiv 9 \pmod{18}$.) equivalent eq^n.

$\Rightarrow 5x \equiv 3 \pmod 6$

g.c.d $(5, 6) = 1$, Hence it has a unique sol^n.

By Bezout's theorem,

$\exists$ u and v $\in \mathbb{Z}$ such that,

$5u + 6v = 1$.

$u = -1$, $v = 1$.

$5(-1) + 6(1) = 1$. $\quad$ $5x \equiv 3 \pmod 6$

$5(-1) \equiv 1 \pmod 6$

$\Rightarrow 5(-3) \equiv 3 \pmod 6$

$x = -3$ is a sol^n of the above eq^n.

$5x \equiv 3 \pmod 6$.

$x = -3, \; -3+6, \; -3+12 \pmod{18}$

$x \equiv -3, 3, 5 \pmod{18}$

$= -3, 3, 5 \pmod{18}$

System of Linear Congruence Eq^n.

$$a_1 x \equiv b_1 \pmod{m_1}$$
$$a_2 x \equiv b_2 \pmod{m_2}$$
$$\vdots$$
$$a_r x \equiv b_r \pmod{m_r}.$$

Find x

To solve these kind of system of equations. We introduce CRT (Chinese Remainder Theorem):

C.R.T:- Let $m_1, m_2, \dots m_r$ be positive integer such that $g.c.d(m_i, m_j) = 1 \;\; \forall \; i \neq j$ and $c_1, c_2, \dots c_r$ be any int. Then the system of Linear Congruences

2, 3, 5
$\pmod{m_1 \dots m_r}$
$\pmod{30}$

$x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$ ...., $x \equiv c_r \pmod{m_r}$

has a simultaneous sol^n, which is unique modulo $(m_1 m_2 m_3 \dots m_r)$ i.e, if x_0 is a sol^n then $x = x_0 + k(m_1 m_2 \dots m_r)$ is modulo $(m_1 m_2 \ldots m_r)$,

a soln, then $x = x_0 + k(m_1 m_2 \ldots m_r)$ is also a soln.

Example:

Solve: $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

Find x. $\pmod{105}$

3, 5, 7 are relatively prime to each other.

$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{m}{3} = \frac{105}{3} = 35$

$M_2 = \frac{m}{5} = \frac{105}{5} = 21$

$M_3 = \frac{m}{7} = 15.$

$g.c.d(M_1, 3) = g.c.d(35, 3) = 1.$

$g.c.d(M_2, 5) = 1$, $g.c.d(M_3, 7) = 1.$

$g.c.d(35, 3) = 1.$

$35x \equiv 1 \pmod 3$ .... (i)

$x \equiv 2 \pmod 3$

g.c.d $(21, 5) = 1$.

$21x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 5$ ---- (ii).

g.c.d $(15, 7) = 1$

$15x \equiv 1 \pmod 7$.

So, $x \equiv 1 \pmod 7$ ---- (iii).

$$x_0 = \underbrace{1.(35.2) + 2.(21.1) + 3.(15.2)}_{= 157}$$

$= 157$.

$x \equiv 157 \pmod{105}$

$\equiv 52 \pmod{105}$

$105 \overline{)157}(1$
105
$\overline{\ \ 52}$

is the final sol^n!

Solve $32x \equiv 79 \pmod{1225}$ by CRT.

$1225 = 35 \times 35$

$= (5\times 7) \times (5 \times 7)$

$= (5^2 \times 7^2)$.

$32x \equiv 79 \pmod{25}$ —— (i) } CRT

$32x \equiv 79 \pmod{25}$ — (i)

$32x \equiv 79 \pmod{49}$ — (ii)

CRT

$x \equiv ? \pmod{25}$

$32x \equiv 30 \pmod{49}$

$\Rightarrow 16x \equiv 15 \pmod{49}$

$16(-3) + 49 \cdot 1 = 1.$

$16(-3) \equiv 1 \pmod{49}.$

$\Rightarrow 16(-45) \equiv 15 \pmod{49}.$

$x \equiv -45 \pmod{49}$

$\equiv 4 \pmod{49}$ - - - (I).