Exc: Show that $41 \mid 2^{20} - 1$

$$2^5 \equiv -9 \pmod{41}$$

$$(2^5)^4 \equiv (-9)^4 \pmod{41}$$

$$\equiv (-1)(-1) \pmod{41}$$

$$\equiv 1 \pmod{41}$$

$$2^{20} \equiv 1 \pmod{41}$$

Exc: Find the remainder of

$$12 \mid 1! + 2! + 3! + \cdots + 100!$$

$4! = 24 \equiv 0 \pmod{12}$

$\therefore \quad 1! + 2! + 3! + 4! + \cdots + 100!$

$$\equiv 1! + 2! + 3! \pmod{12}$$

$$\equiv 9 \pmod{12}$$

26

Theorem: If $ac \equiv bc \pmod{n}$

then $a \equiv b \left(\bmod \frac{n}{d}\right)$, $d = (c, n)$

<u>Proof</u>:

27

Corollary: 1. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$ then

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

Corollary 2: If $ac \equiv bc \pmod{n}$ & $n = p \nmid c$, p is a prime then

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

<u>Linear Congruences:</u> An Equation of the form $ax \equiv b \pmod{n}$ is called a linear congruence equation.

→ An integer x_0 such that $ax_0 \equiv b \pmod{n}$ is a solution of $ax \equiv b \pmod{n}$

→ $ax_0 \equiv b \pmod{n} \Leftrightarrow n \mid ax_0 - b \Leftrightarrow$

$$ax_0 - b = ny_0 \text{ for some } y_0 \in \mathbb{Z}.$$

→ Linear Congruence equation $ax \equiv b \pmod{n}$ is equivalent to linear Diophantine Equation $ax - ny = b$.

<u>Theorem</u>: The Linear Congruence $ax \equiv b \pmod{n}$ has a solution iff $d \mid b$ where $d = \gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.

Proof: $ax \equiv b \pmod{n}$ is equivalent to

$$ax - ny = b$$

$ax - ny = b$ is solvable iff $d \mid b$

$$d = \gcd(a, n)$$

If x_0, y_0 is any particular solution, then any other solution has the form

$$x = x_0 + \frac{n}{d}t$$

$$y = y_0 + \frac{a}{d}t \quad ; \; t \in \mathbb{Z}$$

(29)

Consider the solutions for $t = 0, 1, 2, \ldots, d-1$

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ \ldots,\ x_0 + \frac{(d-1)n}{d}$$

Above integers are incongruent modulo n as shown below

$$x_0 + \frac{n}{d} t_1 \equiv x_0 + \frac{n}{d} t_2 \pmod{n}$$

$$0 \le t_1 \le d-1$$
$$0 \le t_2 \le d-1$$

$$\Rightarrow \quad \frac{n}{d} t_1 \equiv \frac{n}{d} t_2 \pmod{n}$$

$$\gcd\left(n, \frac{n}{d}\right) = \frac{n}{d}$$

$$\Rightarrow \quad t_1 \equiv t_2 \pmod{d}$$

$$\Rightarrow \quad d \mid t_1 - t_2$$

a contradiction as $0 < t_1 - t_2 < d$

$$\Rightarrow \quad x_0 + \frac{n}{d} t_1 \not\equiv x_0 + \frac{n}{d} t_2$$

30

To show any other solution

$x_0 + \frac{n}{d}t$ is congruent modulo n

to one of the d - integers.

By division algorithm

$$t = qd + r, \quad 0 \leq r < d$$

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$$

$$\equiv x_0 + \frac{n}{d} r \pmod{n}$$

$x_0 + \frac{n}{d}t$ is congruent modulo n

to one of d selected solutions.

Corollary: If $(a, n) = 1$, then $ax \equiv b \pmod{n}$ has a unique solution.

$\rightarrow$ $ax \equiv 1 \pmod{n}$ has unique solution

- if $(a, n) = 1$ and $x = \bar{a}^{1} \pmod{n}$.

(31)

Exc: $18x \equiv 30 \pmod{42}$

$\gcd(18, 42) = 6$ and $6 | 30$

The Linear Congruence equation has exactly 6 incongruent mod 42 solutions.

By Inspection, $x_0 = 4$ is one solution

Other six incongruent solutions are

$$x = 4 + \frac{42}{6}t, \quad t \in \mathbb{Z}, \quad t = 0,1,2,3,4,5$$

$$= 4 + 7t$$

$$= 4, 11, 18, 25, 32, 39 \pmod{42}$$

Exc: $9x = 21 \pmod{30}$ — (1)

$\gcd(9, 30) = 3$ & $3 | 21$

three incongruent solutions

Divide (1) by 3,

$$3x \equiv 7 \pmod{10}$$

$$x \equiv 3^{-1} \times 7 \pmod{10}$$

$$= 7 \cdot 7 \pmod{10} \quad (3^{-1} = 7 \pmod{10})$$

$$\equiv 9 \pmod{10}$$

$$x = x_0 + 10t = 9 + 10t, \quad t = 0, 1, 2$$

$$= 9, 19, 29$$

32

Euclidean Algorithm to solve

$$9x \equiv 21 \pmod{30}$$

$$9x - 30y = 21$$

$$\gcd(9, 30) = 3$$

write $3 = 9x + 30y$

$$3 = 9(-3) + 30 \cdot 1$$

$$21 = 9(-21) + 30(7)$$

$$x_0 = -21$$
$$y_0 = -7$$

$$x = -21 + 10t \pmod{30}, \quad t = 0, 1, 2$$

$$= -21, -11, -1 \pmod{30}$$

$$\equiv 9, 19, 29 \pmod{30}$$

How to Find Inverse

$$3x \equiv 7 \pmod{10}$$

10	1	0	3	0	1
3	0	1	1	1	-3
1	1	-3			

$$1 = 1 \times 10 + (-3) \times 3$$

$$1 \equiv -3 \times 3 \pmod{10} \equiv 7 \times 3 \pmod{10}$$