Ex. show that 41 divides $2^{20} - 1$.

Soln:

$2^5 = 32 \equiv -9 \pmod{41}$

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

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

$\Rightarrow 2^{20} \equiv 81.81 \pmod{4}$ —— (I)

Again

$81 \equiv -1 \pmod{41}$, $81 \equiv -1 \pmod{41}$

$\therefore 81.81 \equiv (-1)(-1) \pmod{41}$ $\left[\begin{array}{l} \text{If } a \equiv b \pmod{m} \\ \quad c \equiv d \pmod{m} \\ \text{then } ac \equiv bd \pmod{m} \end{array}\right.$

$\Rightarrow 81.81 \equiv 1 \pmod{41}$ —— (II)

from (I) & (II) we get

$2^{20} \equiv 81.81 \pmod{41}$, $81.81 \equiv 1 \pmod{41}$

$\Rightarrow 2^{20} \equiv 1 \pmod{41}$ $\left(\begin{array}{l} \because a \equiv b \pmod{m}, \\ \quad b \equiv c \pmod{m} \\ \Rightarrow a \equiv c \pmod{m} \end{array}\right.$

$\Rightarrow 41 \mid 2^{20} - 1$

i.e. 41 divides $2^{20} - 1$

#

Ex. Find the remainder obtained upon dividing the sum

$$1!+2!+3!+4!+\cdots+99!+100!$$

by 12.

Sol^n: We know

$$4! = 1.2.3.4 = 24 \equiv 0 \pmod{12}$$

for $k \geq 4$

$$k! = \cancel{4!.5}.\ 1.2.3.4.5 \cdots k$$

$$= 4!.\ 5.6 \cdots k$$

$$\equiv 0 \pmod{12}$$

$\therefore$ $1!+2!+3!+4!+\cdots+99!+100!$

$$\equiv 1!+2!+3!+0+\cdots+0 \pmod{12}$$

$$\equiv 1+2+6 \pmod{12}$$

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

$\therefore$ Reqd remainder is 9 #

Theorem: If $ca \equiv cb \pmod{n}$, then
$a \equiv b \pmod{\frac{n}{d}}$, where $d = \gcd(c, n)$

Pf: Let $ca \equiv cb \pmod{n}$

$\therefore n \mid (ca - cb) = c(a-b)$

$\therefore c(a-b) = kn$, for some integer k. — ①

Also, $d = \gcd(c, n)$

$\therefore d \mid c$ and $d \mid n$

$\Rightarrow c = dr$ and $n = ds$ where $\gcd(r, s) = 1$ and r, s are some integers.

$\therefore$ ① $\Rightarrow dr(a-b) = k \cdot ds$

$\Rightarrow r(a-b) = ks$

$\Rightarrow s \mid r(a-b)$

Thus $s \mid r(a-b)$ and $\gcd(r, s) = 1$.

So by Euclid's Lemma $s \mid (a-b)$

$\Rightarrow a \equiv b \pmod{s}$

$\Rightarrow a \equiv b \pmod{\frac{n}{d}}$ [$\because n = ds$]

#

Corollary: If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$ then $a \equiv b \pmod{n}$.

Pf. Take ~~Hence~~ $d = \gcd(c, n) = 1$, in previous Theorem to get the result.

Corollary: If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is number, then
$a \equiv b \pmod{p}$

Pf: since $p \nmid c$ and p is a prime so $\gcd(p, c) = 1$.

$\therefore$ $ca \equiv cb \pmod{p}$

$$\Rightarrow a \equiv b \left(\bmod \frac{p}{\gcd(c, p)}\right)$$

$$\Rightarrow a \equiv b \left(\bmod \frac{p}{1}\right)$$

$$\Rightarrow a \equiv b \pmod{p}$$

#

Ex. Given an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$

Soln. Take $a = 3$, $b = 2$, $n = 5$.

Then $a^2 = 3^2 = 9$, $b^2 = 2^2 = 4$

$\therefore$ $9 \equiv 4 \pmod 5$ so $a^2 \equiv b^2 \pmod n$

but $3 \not\equiv 2 \pmod 5$ i.e. $a \equiv b \pmod n$

Ex. Find the remainder when 2^{50} is divided by 7.

Soln: We know,

$$2^3 \equiv 1 \pmod 7$$

$$\Rightarrow (2^3)^{16} \equiv 1^{16} \pmod 7 \quad \left[\begin{array}{l} a \equiv b \pmod n \\ \Rightarrow a^k \equiv b^k \pmod n \end{array} \right.$$

$$\Rightarrow 2^{48} \equiv 1 \pmod 7$$

Also, $2^2 \equiv 2^2 \pmod 7$ $[\because a \equiv a \pmod n)$

$$\therefore 2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod 7$$

$$\Rightarrow 2^{50} \equiv 4 \pmod 7$$

$\therefore$ 4 is the remainder when 2^{50} is divided by 7.

Ex. Find the remainder when 41^{65} is divided by 7.

HW

Hint. We know, $41 \equiv -1 \pmod 7$

Ex. find the remainder when 7^{30} is divided by 4.

Ex: what is the remainder when 5^{48} is divided by 12?

soln.

$$5^2 \equiv 1 \pmod{12}$$

$$\Rightarrow (5^2)^{24} \equiv 1^{24} \pmod{12}$$

$$\Rightarrow 5^{48} \equiv 1 \pmod{12}$$

$\therefore$ 1 is the remainder when 5^{48} is divided by 12 #

Remark: If $n \mid (a-b)$, then we say a is congruent to b modulo n.

$\therefore$ $1 \mid (a-b)$, for any integers a, b

so any two integers are congruent modulo 1.

$2 \mid (a-b)$ if both a and b are even or odd. i.e. [illegible] i.e. two integers are congruent modulo 2 when they are both even or both odd.

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a = qn + r, \quad 0 \le r < n$$

Then $\quad a - r = qn, \quad 0 \le r < n$

$$\Rightarrow n \mid a - r \Rightarrow a \equiv r \pmod{n}$$

$r = 0, 1, \ldots, n-1$

Since there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, \ldots, n-1$.

The set of n integers $0, 1, 2, \ldots, n-1$ i.e. the set $\{0, 1, \ldots, n-1\}$ is called the set of least nonnegative residues modulo n.

A collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a complete set of residues modulo n if every integer is congruent modulo n to one and only one a_k.

Also,

$a_1, a_2, \ldots, a_n$ are congruent modulo n to $0, 1, 2, \ldots, n-1$, taken in some order.

eg 1. $n = 7$, $r = \{0, 1, \ldots, 6\}$

$S = \{-12, -4, 11, 13, 22, 82, 91\}$

$-12 \equiv 2 \pmod 7$, $-4 \equiv 3 \pmod 7$

$11 \equiv 4 \pmod 7$, $13 \equiv 6 \pmod 7$

$22 \equiv 1 \pmod 7$, $82 \equiv 5 \pmod 7$

$91 \equiv 0 \pmod 7$

Hence $S = \{-12, -4, 11, 13, 22, 82, 91\}$ forms a complete set of residues mod 7.