Lecture 10: Congruences and some basic properties

Definition Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n i.e.

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

If $n \mid a-b$ i.e. $a-b = kn$ for some integer k.

When $n \nmid a-b$ we say a is incongruent to b modulo n i.e. $a \not\equiv b \pmod{n}$

Residues Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Division algorithm gives q and $r \in \mathbb{Z}$ s.t.

$$a = qn + r \qquad 0 \leq r < n$$

$$\Rightarrow a - r = qn$$

$$\Rightarrow n \mid a-r$$

i.e. $a \equiv r \pmod{n}$

Since for a fixed $n \in \mathbb{N}$ there are n values of r: $0, 1, 2, \ldots, n-1$

Hence every integer is congruent modulo n to exactly one of these.

We call this set residues modulo n.

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

Thm 10.1 For any $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if a and b leave the same non-negative remainder when divided by n

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

i.e. $n \mid a-b$

i.e. $a-b = nk \qquad k \in \mathbb{Z}$ — (I)

Suppose b leaves remainder r when divided by n. Then

$$b = nq + r \qquad 0 \leq r < n \qquad q \in \mathbb{Z} \qquad \text{— (II)}$$

(I) and (II) $\Rightarrow$

$$a = b + nk = nq + r + nk = n(q+k) + r$$

This show that a also leaves remainder r when divided by n.

Conversely suppose a and b leaves the same remainder when divided by n say r. Then we can write:

$$a = q_1 n + r \quad \text{and} \quad b = q_2 n + r$$

Hence $a - b = (q_1 - q_2)n \Rightarrow n \mid a-b$

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

Thm 10.2 Let $n>1$ be fixed and $a, b, c \in \mathbb{Z}$ be arbitrary. Then the following properties hold:

(a) $a \equiv a \pmod{n}$

(b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a+c \equiv b+d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$

(e) If $a \equiv b \pmod{n}$ then $a+c \equiv b+c \pmod{n}$ and $a \cdot c \equiv b \cdot c \pmod{n}$

(f) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ $\forall\ k \in \mathbb{N}$.

Proof (a) Obviously $n \mid 0 = a-a$

(b) $a \equiv b \pmod{n} \Rightarrow n \mid a-b \Rightarrow n \mid b-a \Rightarrow b \equiv a \pmod{n}$

(c) $a \equiv b \pmod{n} \Rightarrow n \mid a-b$
$b \equiv c \pmod{n} \Rightarrow n \mid b-c$
$\Rightarrow n \mid (a-b)+(b-c) = a-c$

$\Rightarrow a \equiv c \pmod{n}$

(d) $a \equiv b \pmod{n} \Rightarrow n \mid a-b$, $c \equiv d \pmod{n} \Rightarrow n \mid c-d$

Hence $n \mid (a-b)+(c-d) \Rightarrow n \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv b+d \pmod{n}$

Also we have $a-b = k_1 n$ and $c-d = k_2 n$ $\quad k_1, k_2 \in \mathbb{Z}$

$\Rightarrow a = b+k_1 n$ and $c = d+k_2 n$

Hence $a \cdot c = k_1 k_2 n^2 + bn + dn + bd$

$= (k_1 k_2 n + b + d)n + db$

$\Rightarrow n \mid ac-bd \Rightarrow ac \equiv bd \pmod{n}$

(e) Use property (d) and the fact that $c \equiv c \pmod{m}$

(f) We use principal of mathematical induction.

For $k=1$ the statement is obviously true.

Suppose the statement is true for some k i.e.

$$a^k \equiv b^k \pmod{m}$$

From property (d) we get

$$a^k \cdot a \equiv b^k \cdot b \pmod{m}$$

$$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod{m}$$

Examples

1) Show that 41 divides $2^{20}-1$.

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

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

$$\Rightarrow 2^{20} \equiv 81 \cdot 81 \pmod{41}$$

Now $81 \equiv -1 \pmod{41} \Rightarrow 81 \cdot 81 \equiv (-1)(-1) \pmod{41}$

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

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

2) Find the remainder of dividing

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

by 12.

Sol- $1! = 1 \quad 2! = 2 \quad 3! = 6 \quad 4! = 24$

Hence $4!$ is divisible by 12 i.e.

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

Hence for any $k \geq 4$

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

Hence $1! + 2! + 3! + 4! + \cdots + 100! \equiv 1! + 2! + 3! + 0 + \cdots + 0 \pmod{12}$

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

Thm 10.3 If $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{n/d}$ where $d = \gcd(c, n)$.

Proof Since $ca \equiv cb \pmod{n}$, therefore

$$n \mid ca - cb = c(a-b) \Rightarrow c(a-b) = nk \quad \text{for some } k \in \mathbb{Z}$$

Since $d = \gcd(c, n)$, hence $\exists\ r, s \in \mathbb{Z}$, $\gcd(r, s) = 1$ such that

$$c = rd \text{ and } n = sd$$

This gives us $c(a-b) = nk \Rightarrow rd(a-b) = sdk$

$$\Rightarrow s \mid r(a-b) \Rightarrow s \mid a-b \quad [\because \gcd(r, s) = 1]$$

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

$$\text{i.e. } a \equiv b \pmod{n/d}$$

Corollary 10.4 If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$

Corollary 10.5 If $ca \equiv cb \pmod{p}$ and $p \nmid c$ where p is a prime number then $a \equiv b \pmod{p}$

Exercises

1) Prove the following:

(a) If $a \equiv b \pmod{n}$ and $m \mid n$ then $a \equiv b \pmod{m}$

(b) If $a \equiv b \pmod{n}$ and $c > 0$ then $ca \equiv cb \pmod{cn}$

(c) If $a \equiv b \pmod{n}$ and $a, b, n \in \mathbb{Z}$ are all divisible by $d > 0$ then $\frac{a}{d} \equiv \frac{b}{d} \pmod{n}$

2) Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply $a \equiv b \pmod{n}$

3) If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$

4) (a) Find the remainders when 2^{50} and 41^{65} are divided by 7

(b) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$