Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Complete Residue Theorem

Dr. V. Piramanantham
Professor
Department of Mathematics

Congruence: Recall

① If $a \equiv b \pmod{m}$, $d>0$, $d \mid m$,

$a \equiv b \pmod{d}$.

Lcm

② A common multiple of $a_1, a_2, \cdots a_n$ is a multiple by the lcm of $a_1, a_2, \cdots, a_n$.

③ Assume that $x \equiv y \pmod{m_i}$ $i = 1, 2, \cdots r$

Then $m_i \mid x-y$, $i = 1, 2, \cdots, r$

$\Rightarrow$ $x-y$ is a common multiple of $m_1, m_2, \cdots, m_r$

$\Rightarrow$ $x-y$ is a multiple of $[m_1, m_2, \cdots, m_r]$.

(i.e) $[m_1, m_2, \cdots, m_r] \mid x-y$

$\Rightarrow$ $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$

Conversely, assume that

$$x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$$

Since each $m_i \mid [m_1, m_2, \ldots, m_r]$,

$$x \equiv y \pmod{m_i} \quad i = 1, 2, \ldots, r.$$

Remark $a \equiv b \pmod{m} \iff m \mid a-b \iff a-b$ is a multiple of m.

(or) $a - b = q\,m$ for some integer q

Division algorithm — m is fixed

m — divisor, a is any integer

Apply division algorithm on a and m

we get unique quotient q & remainder r

$0 \leq r < m \Rightarrow r = 0, 1, 2, \ldots, m-1$

$$a = qm + r$$

$$\Rightarrow a - r = qm$$

$$\Rightarrow m \mid a - r$$

$$\Rightarrow a \equiv r \pmod{m}$$

Theorem:

Let $m > 0$ be fixed integer. Every integer a is congruent (mod m) to unique integer among the numbers $0, 1, 2, \ldots, m-1$

Definition complete residue system modulo m.

A set $\{x_1, x_2, \ldots, x_m\}$ of m numbers is said to be a complete residue system modulo m if for every integer y there is one and only on[e] x_j such that $y \equiv x_j \pmod{m}$.

Example: (1) $\{0, 1, 2, \ldots, m-1\}$ is a CRS $\pmod{m}$

$A = \{0, 1, 2, 3, 4, 5, 6\}$, $C = \{7, 15, 3, 4, 42, 76, 51\}$

$a \equiv r$ (known) $r \in A$

x	r
7	0
15	1
3	3
4	4
42	0
76	6
51	2

$42 = 6 \cdot 7 + 0$

$76 = 10 \cdot 7 + 6$

$51 = 7 \cdot 7 + 2$

5

$x \equiv r$

$\boxed{a \equiv x}$

$a \equiv b$
$\Rightarrow m \mid b - a$

$C = \{7, 15, 3, 4, 42, 76, 51\}$ is not CRS (mod 7)

because 5 is not congruent to any one in C.

$C = \{3, 4, 7, 15, 40, 51, 76\}$

CRS (verify) Yes.

$42 \equiv 7 \pmod 7$

$\underline{14} \equiv 42$ & $14 \equiv 7 \pmod 7$

unique congruence

Remark: A set of m integers forms a complete residue system modulo m if and only if no two integers in the set are congruent modulo m.

Remark m - fixed integer > 0

a is any integer.

The set of all integers x congruent to $a \pmod{m}$ is the arithmetic progression

$$\ldots, a-2m, a-m, a, a+m, a+2m, \ldots$$

$\boxed{b \equiv a \pmod{m}} \iff m \mid b-a \Rightarrow b-a = km$ for some int k

$\iff \boxed{b = a+km}$

$k \in \mathbb{Z}$

$a+km$

$k=0,1,2,\ldots, k=-1,-2,\ldots$

Residue class or congruence class (mod m)

(or) residue class of a (mod m)

is the set of all integers x congruent to $a \pmod{m}$

$\ldots, a-2m, a-m, a, a+m, a+2m, \ldots$

$m=7$, $a=2$

$x \equiv a$

$y \equiv a$

$\Rightarrow x \equiv y$

Residue class of $2 \pmod{7}$

$\ldots, -19, -12, -5, 2, 9, 16, 23, 30, \ldots$

a	residue class of a (mod 7)
0	…, −21, −14, −7, 0, 7, 14, 21, …
1	…, −20, −13, −6, 1, 8, 15, 22, …
2	…, −19, −12, −5, 2, 9, 16, 23, …
3	…, −18, −11, −4, 3, 10, 17, 24, …
4	…, −17, −10, −3, 4, 11, 18, 25, …
5	…, −16, −9, −2, 5, 12, 19, 26
6	…, −15, −8, −1, 6, 13, 20, 27, …

The residue class of $a \pmod{m}$ is denoted by $[a]$.

Ex

$$[0] = [7]$$

$$[1] = [8]$$

Result

$$a \equiv b \pmod{m} \iff [a] = [b].$$

$$a \not\equiv b \pmod{m} \iff [a] \cap [b] = \phi$$

Remark: There are m distinct residue

$\{1, 2, 3, \ldots m\}$ is CRS (mod m).

$\forall x \in \mathbb{Z}$, there is one and only one member congruent to x (mod m)

Note: ① Any two members of a CRS are not congruent mod m.

② A complete residue system (mod m) has exactly m members.

$\{0, 1, 2, \ldots m-1\}$ is complete residue system

Division Algorithm

m - divisor

$\boxed{a \in \mathbb{Z}}$, $\boxed{\exists!\, r}$ (remainder) s.t.

$a = qm + r \Rightarrow a - r = qm$

$\Rightarrow \boxed{a \equiv r \pmod{m}}$

$r \in \mathbb{Z}$

$$[r] = \{a \in \mathbb{Z} \mid a \equiv r \pmod{m}\}$$

$[r]$ is a residue class $\pmod{m}$

There are m residue classes $\pmod{m}$ which are mutually disjoint

and their union is the set of all integers

<u>Theorem:</u> If $a \equiv b \pmod{m}$, then

$$(a, m) = (b, m)$$

Theorem: If $a \equiv b \pmod{m}$, then

$$(a, m) = (b, m)$$

Proof: $a \equiv b \pmod{m} \Rightarrow b - a = mx$ for some x

$$\Rightarrow b = a + mx$$

By the result. $(a, m) = (a + mx, m) = (b, m)$

Remark: If $(a, m) = 1$ and $a \equiv b \pmod{m}$, then $(b, m) = 1$.

Relatively prime: Two integers a & b are said to relatively prime if

$$\gcd(a,b) = 1.$$

Ex: For any integer n, $(n, n+1) = 1$

n & $n+1$ are relatively prime.

Remark If $(a,b)=1$, we say that a is prime to b.

Ex: If n is an odd integer, then

Ex: If n is an odd integer, then n & $n+2$ are relatively prime.

Prove that $(n, n+1) = 1$. Also prove that if n is odd, $(n, n+2) = 1$.

$d \mid n$, $d \mid n+1$

Hint: $a \mid b$ & $a \mid c$
$\Rightarrow a \mid bx + cy$.

Remarks: If a is prime to m, then any integer congruent to $a \pmod m$ is also prime to m. (ie)

if $(a,m)=1$ & $b \equiv a \pmod m$, $(b,m)=1$

Suppose that r is any integer such that $(r,m)=1$.

all integers belonging the residue class mod m are prime to m.

Reduced residue system

A set $\{r_1, r_2, \ldots, r_n\}$ of integers is called reduced residue system (mod m) if

(1) For each i, $(r_i, m) = 1$

(2) for any i, j with $i \neq j$,

$$r_i \not\equiv r_j \pmod{m}$$

Remark: If $(a, m) = 1$, there is a unique member r_i in a reduced residue system (mod m) such that $a \equiv r_i \pmod{m}$.

Consider CRS

remove all integers from CRS which is not relative prime to m

$m = 10$

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\Big\Downarrow \text{Reduce}$$

$\{1, 3, 7, 9\}$ is a Reduced residue system.

Ex of an RRS $= \{ r \mid 1 \le r \le m \ \& \ (r, m) = 1 \}$

Definition: The Euler ϕ-function

$\phi(m)$ is the number of +ve integers less than or equal to m which are relatively prime to m.

$$\phi(m) = \#\{ r \,/\, 1 \le r \le m,\ (r, m) = 1 \}.$$

ϕ is called the Euler ϕ-function or the totient.

$$\phi(7) = \# \{ r \mid 1 \le r \le 7,\ (r,7) = 1 \}$$

$\phi(10) = 4,$

m	$\phi(m)$	m	$\phi(m)$	m	$\phi(m)$
1	1	6	2	11	10
$\boxed{2}$	1	7	6	12	4
3	2	$\boxed{8}$	4	13	12
$\boxed{4}$	2	9	6	14	6
5	4	10	4	15	8

$m = 1, \quad 1 \le r \le 1 \Rightarrow r = 1$

$(1,1) = 1$

XC

Observation: ① If p is prime,

$$\phi(p) = p - 1$$

② If $m = 2^k$, for some $k > 0$,

$$\phi(2^k) = 2^{k-1}$$

If p is odd prime, $\phi(p^\alpha) =$

Theorem If $a_1, a_2, \ldots, a_m$ form a complete residue system & $(b, m) = 1$ and c is any integer then

$$a_1 b + c,\ a_2 b + c,\ \ldots,\ a_m b + c$$

form a complete residue system.

$m = 12$

Ex: $\{1, 2, \ldots, 12\}$ is a CRS $(\mathrm{mod}\ m)$

$b = 7, \quad c = 4$

Theorem If $r_1, r_2, \ldots, r_{\phi(m)}$ form a reduced residue system mod m & $(b, m) = 1$, then

$br_1, br_2, \ldots, br_{\phi(m)}$ form a reduced residue system (mod m).