Video (4)

Theory of Congruence

21/4/20 (9) Tuesday (2)

(1) **Congruence** :- Let m be be fixed integer. Then an integer a is said to be congruent to another integer b modulo m if $m|(a-b)$. This is written as

$$a \equiv b \pmod{m} \quad \text{---(1)}$$

(1) is called congruence, m is called the modulo of the congruence and b is called a residue of $a \pmod{m}$.

Ex. :-

$67 \equiv 2 \pmod{13}$

because $13 | (67-2)$

(2) **Least Residue** :- If $a \equiv b \pmod{m}$, $0 \leq b < m$, then b is called least residue of $a \pmod{m}$

(3) **Minimal Residue** :- If $a \equiv b \pmod{m}$ and $0 \leq |b| \leq \left(\frac{m}{2}\right)$ then b is called minimal residue of $a \pmod{m}$

It is also called absolutely least residue of $a \pmod{m}$

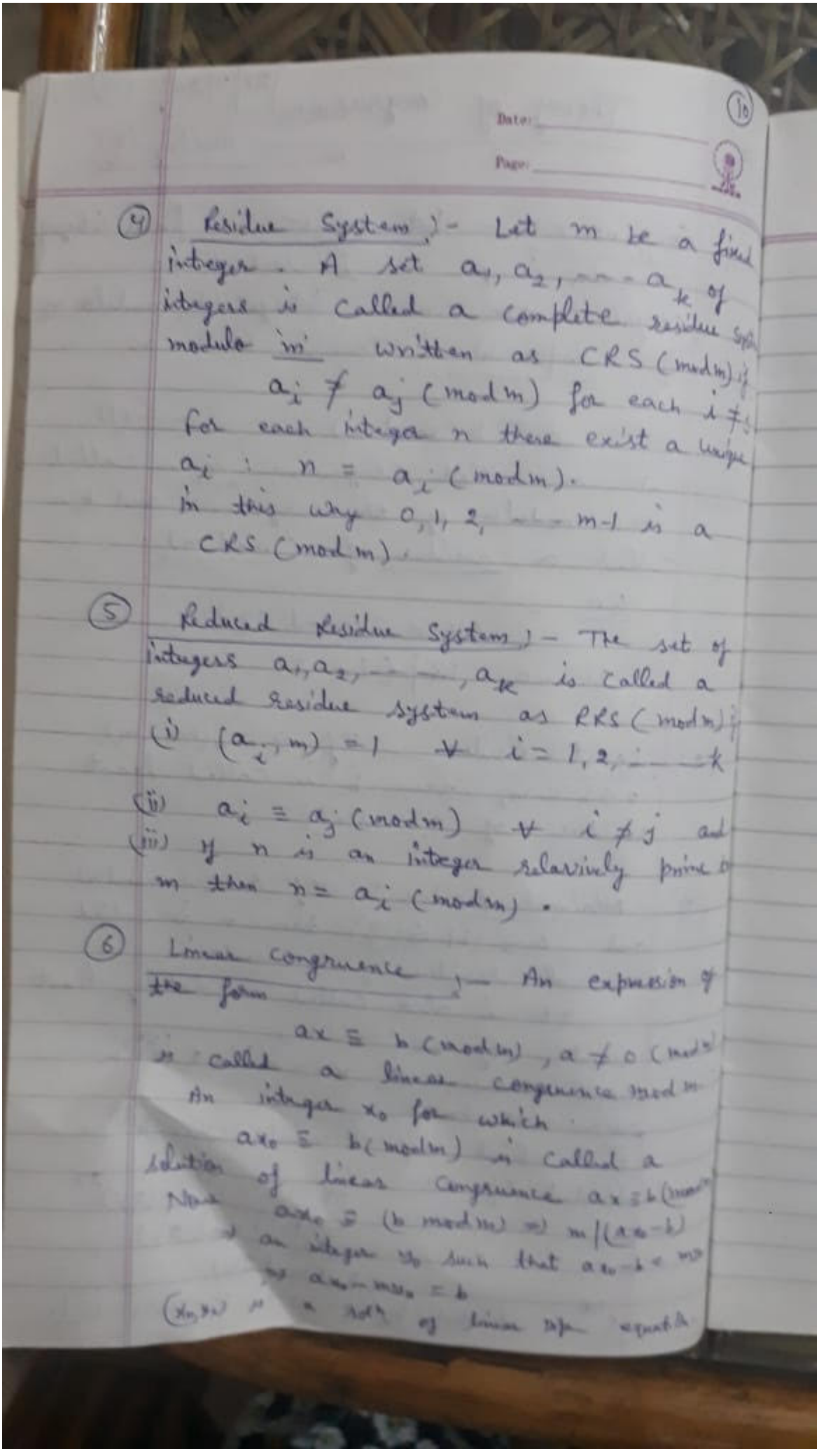
Ex:- Find the remainder when 5^{48} is divided by 24.

Sol:- We have $5^{48} = (5^2)^{24} = (25)^{24}$

$= (1)^{24} \pmod{24}$

$= 1 \pmod{24}$

5^{48} is divided by 24 the remainder is 1.



Date:
Page:

(10)

(4) Residue System :- Let m be a fixed integer. A set $a_1, a_2, \ldots a_k$ of integers is called a complete residue system modulo m written as CRS (mod m) if $a_i \not\equiv a_j \pmod m$ for each $i \neq j$. For each integer n there exist a unique a_i : $n \equiv a_i \pmod m$.
In this way $0, 1, 2, \ldots m-1$ is a CRS (mod m).

(5) Reduced Residue System :- The set of integers $a_1, a_2, \ldots, a_k$ is called a reduced residue system as RRS (mod m) if
(i) $(a_i, m) = 1 \quad \forall \quad i = 1, 2, \ldots k$
(ii) $a_i \equiv a_j \pmod m \quad \forall \quad i \neq j$ and
(iii) if n is an integer relatively prime to m then $n \equiv a_i \pmod m$.

(6) Linear congruence :- An expression of the form

$$ax \equiv b \pmod m, \quad a \not\equiv 0 \pmod m$$

is called a linear congruence mod m. An integer x_0 for which

$$ax_0 \equiv b \pmod m$$

is called a solution of linear congruence $ax \equiv b \pmod m$.
Now $ax_0 \equiv (b \bmod m) \Rightarrow m \mid (ax_0 - b)$
$\Rightarrow$ an integer y_0 such that $ax_0 - b = my_0$
$\Rightarrow ax_0 - my_0 = b$
(x_0, y_0) is a soln of linear Diophantine equation

Date:

Page:

Ex :- Solve the linear congruence :

$6x \equiv 15 \pmod{21}$

Proof :- we have

$(6, 21) = 3$ and $3 \mid 15$

$\Rightarrow$ given linear cong. has a solution.

It will have 3 incongruent solution

$x_0 = 6$ is a solution of linear cong

$6x \equiv 15 \pmod{21}$

Hence

$6, \; 6 + \frac{21}{3}, \; 6 + 2 \cdot \frac{21}{3}$ i.e - 6, 13, ..

are 3 solution.