30/07/22

Unit-V:

ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY.

* Divisibility:

If 'a' and 'b' are any two integers such that $b \neq 0$, then we say that "'b' divides 'a'", if there exists an integer 'k' such that $a = kb$. And it is written as $b|a$.

Note: If "b divides a", then we say that "b is a factor of a" or "a is multiple of b".

* Division Algorithm:

If 'a' and 'b' are any two integers such that $b > 0$, then there exists unique integers 'q' and 'r' such that,

$$\boxed{a = bq + r}$$

where,

q → quotient

r → remainder.

* Congruence Relation:

Let 'm' be a positive integer. Then an integer 'a' is said to be congruent to an integer 'b' under modulo m, if m divides $(a-b)$. $(m|(a-b))$. Symbolically, it is written as

$$a \equiv b \pmod{m} \quad (\text{OR}) \quad a \equiv b \ (\text{Modulo } m).$$

It is read as "a is congruent to b modulo m".

Note: 'b' is called remainder (or) residue of a (mod m).

OR 'b' is remainder when "m divides a".

* Properties of Congruence Relation:

1) If $a \equiv b \pmod m$, then $m \mid (b-a)$.
2) If $a \equiv b \pmod m$, then $b \equiv a \pmod m$.
3) If $a \equiv b \pmod m$ & $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

* Modular Arithmetic operation:

If $a \equiv b \pmod m$, then for $k \neq 0 \in Z$.

i) $a+k = b+k \pmod m$
ii) $a-k = b-k \pmod m$.
iii) $ak = bk \pmod m$.
iv) $a^k = b^k \pmod m$.

* Properties of Modular Arithmetic Operation:

• Residue System Modulo m:

Define the set Z_m as a set of non-negative integers less than m,

$Z_m = \{0, 1, 2, \ldots (m-1)\}$.

It is called ~~modulo~~ residue system modulo.

• Residue Classes:

Each integer in Z_m represents a residue class. and it is denoted by $[a]$ and defined by

$[a] = \{x : x \equiv a \pmod m\}$.

eg: ① Residue system modulo 3 is,

$Z_3 = \{0, 1, 2\}$.

∴ Residue classes of elements of Z_3 are:

$[0] = \{x : x \equiv 0 \pmod 3\}$
$[0] = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$.
$[1] = \{x : x \equiv 1 \pmod 3\}$
$[1] = \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}$.
$[2] = \{x : x \equiv 2 \pmod 3\}$
$[2] = \{\ldots -7, -4, -1, 2, 5, 8, 11 \ldots\}$.

01/08/22.

★ Theorem:

Let n be a positive integer and $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then prove that $a+c \equiv b+d \pmod m$ and $ac \equiv bd \pmod m$.

Proof:

Given that, $a \equiv b \pmod m$ and $c \equiv d \pmod m$.

$m \mid (a-b)$ & $m \mid (c-d)$. ——— (1).

$\Rightarrow m \mid (a-b)+(c-d)$.

$\Rightarrow m \mid a-b+c-d$.

$\Rightarrow m \mid (a+c)-(b+d)$.

$\Rightarrow \boxed{(a+c) \equiv (b+d) \pmod m}$.

By (1).

$(a-b) = k_1 m$ and $(c-d) = k_2 m$ (By division algorithm).

$c(a-b) = ck_1 m$ and $b(c-d) = bk_2 m$.

$ac - bc = (k_1 c)m$ and $bc - bd = (k_2 b)m$.

$ac - bc + bc - bd = (k_1 c)m + (k_2 b)m$

$ac - bd = k'm + k''m$, where $k' = k_1 c$ & $k'' = k_2 b$.

$ac - bd = (k' + k'')m$.

$ac - bd = k_1 m$, where $k' = k' + k'' \in \mathbb{Z}$.

$\Rightarrow n \mid (ac - bd)$

$\Rightarrow \boxed{ac \equiv bd \pmod m}$

★ Prime Numbers:

An integer $P \geq 2$ is called prime number, if it is divisible by 1 and itself. Otherwise a number is called composite number.

For eg: (1) Prime nos are 2, 3, 5, 7, 11, 13, 17, 19, 23 .....

(2) Composite nos are 4, 6, 8, 9, 10, ...

Note: Every composite number can be expressed as product of prime integers.

eg: i, $10 = 2 \times 5$.

ii, $20 = 2 \times 10$
$= 2 \times 2 \times 5$.

iii, $35 = 5 \times 7$.

* Relatively Prime Numbers / Co-Prime Numbers:
Two numbers 'a' and 'b' are said to be relatively prime if they have no common divisors other than 1 (GCD(a,b)=1)
eg: 10 and 21 are relatively prime as GCD(10,21)=1.

* ~~Euler's ϕ-Function / Euler's Totient Function~~:
* Reduced Residue-System modulo m:
The reduced residue system modulo m, is the set of all elements from residue system modulo m $Z_m = \{0, 1, 2, \ldots m-1\}$ which are relatively prime to m.
i.e $S = \{x : GCD(x, m) = 1\}$.

* Euler's ϕ-Function / Euler's Totient Function:
The Euler's (pi) ϕ function of an Integer $n \geq 1$, is denoted by $\phi(n)$ and defined by the number of non-zero positive integers less than 'n' that are relatively prime to n.

eg: 1. $\phi(1) = 0$.
$\phi(2) = n(\{1\}) = 1$.
$\phi(3) = n(\{1, 2\}) = 2$.
$\phi(4) = n(\{1, 3\}) = 2$
$\phi(5) = n(\{1, 2, 3, 4\}) = 4$
$\phi(6) = n(\{1, 2, 3, 4, 5\}) = 2$
$\phi(7) = n(\{1, 2, 3, 4, 5, 6\}) = 6$

* Note:
1) If $n = p$ is a prime no, then Euler's ϕ function of p is
$\boxed{\phi(p) = p-1}$

2) If n is a number that can be expressed as a product of two relatively prime nos a, b, then Euler's ϕ function of n is
$\boxed{\phi(n) = \phi(ab) = \phi(a) \cdot \phi(b)}$

relatively prime

eg: i) $\phi(30) = \phi(4 \times 5) = \phi(4) \cdot \phi(5) = 2 \times 4 = 8$

ii) $\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 4 \times 6 = 24$.

iii) $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \times 4 = 4$.

03/08/22

★ Euler's Theorem:

Statement: Let n and a be positive integer which are relatively prime $(GCD(n,a) = 1)$. Then,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n) \rightarrow$ is Euler's ϕ-function.

Proof: Given that $n, a > 0 \in Z$.

$$\boxed{GCD(n,a) = 1.}$$

Let us take Eulu's ϕ function

$$\boxed{\phi(n) = k.}$$

∴ Reduced residue system modulo n is,

$$S = \{a_1, a_2, a_3, \ldots a_{\phi(n)}\}.$$

or

$$S = \{a_1, a_2, a_3, \ldots, a_k\}.$$

~~Next, we know that,~~

Let us take $a \neq 0 \in Z \ni GCD(a,n) = 1$.

$$aS = \{aa_1, aa_2, aa_3, \ldots aa_k\}.$$

Next, we know that,

$aa_1 \equiv a_1 \pmod{n}$, $aa_2 \equiv a_2 \pmod{n}$ .... $aa_3 \equiv a_3 \pmod{n}$.

Now, by multiplication congruence modulo n, we get.

$$aa_1 \cdot aa_2 \cdot aa_3 \cdots aa_k \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_k \pmod{n}$$

$$a^k(a_1 a_2 a_3 \cdots a_k) \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_k \pmod{n}$$

$$a^k \equiv 1 \pmod{n}$$

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$

CLASSMATE
Date
Page
p & a are relatively prime
p not dividing a

* Fermat's theorem / Fermat's little Theorem:

Statement: Let p be a prime number such that $p \nmid a$. Then,

$$a^{p-1} \equiv 1 \pmod{p}$$

or $$a^{k} = p \pmod{p}$$

Proof: Given that p is a prime number and $p \nmid a$.

Let us take Eulr's ϕ function of p

$$\boxed{\phi(p) = p-1}$$

∴ Reduced residue system modulo p is

$$S = \{a_1, a_2, a_3 \cdots a_{p-1}\}.$$

Let us take $a \neq 0 \in Z \ni p \nmid a$.

$$aS = \{aa_1, aa_2, aa_3, \cdots aa_{p-1}\}.$$

Next, we know that,

$$aa_1 \equiv a_1 \pmod{p}, \quad aa_2 \equiv a_2 \pmod{p} \cdots aa_{p-1} \equiv a_{p-1} \pmod{p}$$

Now by multiplication congruence modulo p, we get

$$aa_1 \cdot aa_2 \cdot aa_3 \cdots aa_{p-1} \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_{p-1} \pmod{p}$$

$$a^{p-1}(a_1 \cdot a_2 \cdot a_3 \cdots a_{p-1}) \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_{p-1} \pmod{p}.$$

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

eg: i) $4^{\phi(9)} \equiv 1 \pmod{9}$

$\phi(9) = n(\{1, 2, 4, 5, 7, 8\}) = 6.$

$4^6 \equiv 1 \pmod{9}.$

$(4^3)^2 \equiv 1 \pmod{9}.$

$(1)^2 \equiv 1 \pmod{9}$

$\boxed{1 \equiv 1 \pmod{9}}.$

ii) $3^{\phi(5)} \equiv 1 \pmod{5}$

$\phi(5) \equiv 4$

$3^4 \equiv 1 \pmod{5}$

$81 \equiv 1 \pmod{5}.$

06/08/22.

* Chinese Remainder Theorem:

If $m_1, m_2, m_3, \ldots, m_K$ are pairwise relatively prime positive integers and if $a_1, a_2, a_3, \ldots a_K$ are any integer then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$
$$\vdots$$
$$x \equiv a_K \pmod{m_K}$$

has unique solution under modulo M, where, $M = m_1, m_2, \ldots m_K$.

* Steps to solve chinese Remainder Theorem:

Step 1: Check that $GCD(m_i, m_j) = 1$, $i \neq j$.

Step 2: $x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots M_K x_K a_K) \pmod{M}$ — (1)

where $M = m_1 \times m_2 \times \cdots m_K$.

Next, $M_i = \frac{M}{m_i} = m_1 \times m_2 \times \cdots m_{i-1} m_{i+1} \cdots m_K$.

$$M_1 = \frac{M}{m_1} = m_2 \times m_3 \times \cdots m_K.$$

$$M_2 = \frac{M}{m_2} = m_1 \times m_3 \times \cdots m_K.$$

$$\vdots$$

$$M_K = \frac{M}{m_K} = m_1 \times m_2 \times \cdots m_{K-1}.$$

To calculate x_i:

x_i is the multiplicative inverse of M_i under modulo m_i.

i.e $M_i x_i \equiv 1 \pmod{m_i}$

$$M_1 x_1 \equiv 1 \pmod{m_1}$$
$$M_2 x_2 \equiv 1 \pmod{m_2}$$
$$\vdots$$
$$M_K x_K \equiv 1 \pmod{m_K}$$

Step3: Using above values of M_i and x_i in relation (1), we get solution x.

* Examples:

(1) Solve the following system of congruences by using chinese remainder theorem.

$x \equiv 2 \pmod 3$ $\quad x \equiv 1 \pmod 4$ $\quad x \equiv 3 \pmod 5$.

Sol:- let $x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$

$a_1 = 2 \quad m_1 = 3$

$a_2 = 1 \quad m_2 = 4$

$a_3 = 3 \quad m_3 = 5$

$GCD(3,4) = GCD(4,5) = GCD(3,5) = 1$

$x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$. — (1)

where, $M = m_1 \cdot m_2 \cdot m_3 = 3 \times 4 \times 5 = 60$. ; $\boxed{M = 60}$

$M_i = \frac{M}{m_i} = m_1 m_2 m_3 \cdots m_k$

$M_1 = \frac{M_1}{m_1} = m_2 \cdot m_3 = 20$.

$M_2 = \frac{M_2}{m_2} = m_1 \cdot m_3 = 15$

$M_3 = \frac{M_3}{m_3} = m_1 \cdot m_2 = 12$.

Calculate x_i:

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$20 x_1 \equiv 1 \pmod 3$.

Keep remainder 2 when divided by 3 ∵ 20 > 3.

$2 x_1 \equiv 1 \pmod 3$

$\boxed{x_1 = 2}$

$3 \overline{)20}\ 6$, 18, (2)

now for what value of x_1 $2x_1 - 1 \mid 3 = 0$.

$\therefore 2(2) \equiv 1 \pmod 3$

$\therefore 4 - 1 = 3 \mid 3 = 0$ //

$M_2 X_2 \equiv 1 \pmod{m_2}$ $\quad 4\overline{)15}\ 3,\ 12,\ 3$

$15 X_2 \equiv 1 \pmod 4$

$3 X_2 \equiv 1 \pmod 4$

$\boxed{X_2 = 3}$

as 4 divides $(3 \times 3) - 1$.

$M_3 X_3 \equiv 1 \pmod{m_3}$

$12 X_3 \equiv 1 \pmod 5$

$2 X_3 \equiv 1 \pmod 5$

$\boxed{X_3 = 3}$

as 5 divides $(2 \times 3) - 1$ (or) $5 \mid 2(3) - 1$

$\therefore$ Relation (1) becomes,

$x \equiv (20 \times 2 \times 2 + 15 \times 3 \times 1 + 12 \times 3 \times 3) \pmod{60}$ $\quad 108, 80, 45 \to 233$

$x \equiv (80 + 45 + 108) \pmod{60}$

$x \equiv 233 \pmod{60}$ $\quad 60\overline{)233}\ 3,\ 180,\ 53$

$x \equiv 53 \pmod{60}$

$\therefore \boxed{x = 53}$

(2) Solve the following congruences by using chinese remainder theorem.

$x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$.

Sol^n:

$a_1 = 2$ $\quad m_1 = 3$

$a_2 = 3$ $\quad m_2 = 5$

$a_3 = 2$ $\quad m_3 = 7$.

$\therefore GCD(3,5) = GCD(5,7) = GCD(3,7) = 1$

$x \equiv (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3) \pmod M$ — (2)

where $M = m_1 m_2 m_3 = 3 \times 5 \times 7$ $\quad 35 \times 3 \to 105$

$\boxed{M = 105}$

$M_i = \frac{M}{m_i}$

$M_1 = \frac{M}{m_1} = m_2 \cdot m_3 = 35$

$M_2 = \frac{M}{m_2} = m_1 . m_3 = 21$

$M_3 = \frac{M}{m_3} = m_1 . m_2 = 3.5 = 15$

Calculate x_i

$M_i x_i \equiv 1 \pmod{m_i}$

$M_1 x_1 \equiv 1 \pmod{m_1}$

$35 x_1 \equiv 1 \pmod{3}$

$2x_1 \equiv 1 \pmod{3}$

$\boxed{x_1 = 2}$ as $3 | 2(2) - 1$.

$M_2 x_2 \equiv 1 \pmod{m_2}$

$21 x_2 \equiv 1 \pmod{5}$

$1 x_2 = 1 \pmod{5}$

$\boxed{x_2 = 1}$ as $5 | 1(1) - 1$.

$M_3 x_3 \equiv 1 \pmod{m_3}$

$15 x_3 \equiv 1 \pmod{7}$

$1 x_3 = 1 \pmod{7}$

$\boxed{x_3 = 1}$ as $7 | 1(1) - 1$.

$\therefore$ Relation (1) becomes,

$x \equiv (35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2) \pmod{105}$

$x \equiv (140 + 63 + 30) \pmod{105}$

$x \equiv (233) \pmod{105}$.

$x \equiv 23 \pmod{105}$

$\therefore \boxed{x = 23}$