UNIT-: V

ELEMENTERY 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 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 exist unique integer q and r such that,

$$a = bq + r$$

where q is called quotent.
r is called 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 $a \equiv b \pmod{m}$ or $a \equiv b$ (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

(i) If $a \equiv b \pmod m$, then $m \mid (a-b)$

(ii) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$

(iii) If $a \equiv b \pmod m$ & $b \equiv c \pmod m$ then $a \equiv c \pmod m$

MODULAR ARITHEMATIC OPERATION

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

(i) $a + k \equiv b + k \pmod m$

(ii) $a - k \equiv b - k \pmod m$

(iii) $a \cdot k \equiv b \cdot k \pmod m$

(iv) $a^k \equiv b^k \pmod m$

Properties of Modular Arithematic

- Residue system Modulo m

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

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

It is called residue system modulo m.

- Residue classes

Each integer in Z_m represents a residue class and it is divided by [a] and defined by

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

For Example:

(1) Residue system modulo 3 is,

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

∴ Residue classes of elements of Z_3 are

$[a] = \{x : x \equiv 0 \pmod 3\}$

$[0] = \{\ldots\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\ldots\}$

$[1] = \{\ldots\ldots -8, -5, -2, 1, 4, 7, 10 \ldots\ldots\}$

$[2] = \{\ldots\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\ldots\}$

classmate

Date

Page

Theorem

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

Proof: Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$m / (a-b)$ and $m / (c-d)$. ——— (1)

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

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

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

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

By (1) we get

$a-b = K_1 m$ and $c-d = K_2 m$

$c(a-b) = cK_1 m$ and $b(c-d) = b K_2 m$

$ac-bc = (K_1 c)m$ and $bc-bd = (K_2 b)m$

$ac-\cancel{bc}+\cancel{bc}-bd = (K_1 c)m + (K_2 b)m$

$ac-bd = K'm + K''m$ where $K' = K_1 c$, $K'' = K_2 b$

$ac-bd = (K'+K'')m$

$ac-bd = K_1 m$ where $K_1 = K' + K'' \in \mathbb{Z}$

$\Rightarrow m / (ac-bd)$

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

PRIME NUMBER

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

Ex: (1) Prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

~~COMPOS~~ (2) Composite numbers are 4, 6, 8, 9, 10, ...

Note

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

Ex: ① 10 = 2×5 ② 20 = 2×10 = 2×2×5 ③ 35 = 5×7

RELATIVELY PRIME NUMBER (CO-PRIME NUMBERS)

Two number a and b are said to be relatively prime if they have no common divisors other than 1.
($GCD(a,b)=1$)

Ex: ① 10 and 21 are relatively prime as $GCD(10,21)=1$

~~EULER's ϕ-FUNCTION / EULER's Totient Fun~~

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 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 n

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

Note

1 If $n=p$ is a prime number then Euler ϕ function of p is $\phi(p)=p-1$

2 If n is number that can be expressed as ~~the~~ a product of releatively prime number (a,b) Euler's ϕ function of n is,

Ex:- ① $\phi(20) = \phi(4 \cdot 5) = \phi(4) \cdot \phi(5) = 2 \times 4 = 8$

② $\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7) = 4 \times 6 = 24$

③ $\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \times 4 = 4$

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 $\phi(n)$ - is Euler ϕ - Function.

Proof:

Given that $n, a > \mathbb{Z}$ such that $GCD(n, a) = 1$.

Euler ϕ- function of n is

$\phi(n) = K$

~~Let us take~~

Consider a reduced system modulo n.

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

OR $S = \{a_1, a_2, a_3, \ldots \ldots a_K\}$

Take $a \neq 0 \in \mathbb{Z}$ such that $GCD(n, a) = 1$

$aS = \{aa_1, aa_2, aa_3, \ldots \ldots aa_K\}$

$aa_1 \equiv a_1 \pmod{n}$; $aa_2 = a_2 \pmod{n} \ldots \ldots aa_K \equiv a_K \pmod{n}$

Next, we know that,

$aa_1 \cdot aa_2 \cdot aa_3 \ldots \ldots aa_K \equiv a_1 \cdot a_2 \cdot a_3 \cdots a_K \pmod{n}$

$a^K (a_1 \cdot a_2 \cdot a_3, \ldots a_K) \equiv (a_1 \cdot a_2 \cdot a_3 \cdots a_K) \pmod{n}$

a

$\Rightarrow a^K \equiv 1 \pmod{n}$

classmate
Date
Page

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

FERMAT'S THEOREM / FERMAT'S LITTLE THEOREM

Statement let P be a prime number and $P \nmid a$. then

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

OR $a^{P} \equiv a \pmod{p}$

Proof

Given that, P is a prime number and $P \nmid a$.

$\Rightarrow GCD(P, a) = 1$

Euler ϕ-function of prime no ϕ is.

$\phi(P) = P-1$

Consider a residue system modulo P.

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

Take $a \neq 0 \in \mathbb{Z}$ such that $P \nmid a$

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

$aa_1 \equiv a_1 \pmod{P}$; $aa_2 \equiv a_2 \pmod{P}$ ..... $aa_{p-1} \equiv a_{p-1} \pmod{P}$

Next we know that

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

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

$\Rightarrow a^{P-1} \equiv 1 \pmod{P}$

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

For example

(1) $4^{\phi(7)} \equiv 1 \pmod 7$.

$\phi(7) = 6$

$4^6 \equiv 1 \pmod 7$

$4^2\, 4^2\, 4^2 \equiv 1 \pmod 7$ $\qquad 4^2/7$ rem $= 2$

$2 \cdot 2 \cdot 2 \equiv 1 \pmod 7$

$8 \equiv 1 \pmod 7$

(2) $5^{\phi(6)} \equiv 1 \pmod 6$

$\phi(6) = n(\{1, 3\}) = 2$

$5^2 = 1 \pmod 6$

CHINESE REMAINDER THEOREM

Statement: If $m_1\, m_2\, m_3 \ldots\ldots m_k$ are pairwise relatively prime numbers and $a_1\, a_2\, a_3 \ldots\ldots a_k$ are any integers then, the simultaneous congruences relations,

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

$\vdots \qquad \vdots$

$x \equiv a_k \pmod{m_k}$

has a unique solution under modulo M,

where $M = m_1 \cdot m_2 \cdot m_3 \cdots\cdots m_k$.

STEPS TO SOLVE SIMULTANEOUS CONGURENCE RELATION BY CHINESE THEOREM.

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

Step 2: $x \equiv (M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots\cdots + M_k x_k a_k) \pmod M$ —(

where $M = m_1, m_2 \cdots\cdots m_k$

and $M_i = \dfrac{M}{m_i} = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_k$

Next, to calculate x_i. x_i is a multiplicative inverse of M_i under modulo m_i

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

step3: Using values of M_i and x_i in ① we can find the value of x

Examples

① solve the following system of congruences by using chinese remainder theorem.

$x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$

→ Given,

$x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$.

$a_1 = 2$, $a_2 = 1$, $a_3 = 3$

$m_1 = 3$, $m_2 = 4$, $m_3 = 5$

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

∴ 3, 4, 5 are pair wise relatively prime

Next, $x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \pmod M$ — ①

where $M = m_1 m_2 m_3 = 3 \cdot 4 \cdot 5 = 60$

$M = 60$.

$M_1 = \frac{M}{m_1} = m_2 m_3 = 4 \cdot 5 = 20$

$M_2 = \frac{M}{m_2} = m_1 m_3 = 3 \cdot 5 = 15$

$M_3 = \frac{M}{m_3} = m_1 m_2 = 3 \cdot 4 = 12$

Calculate x_i:

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

$M_1 x_1 \equiv 1 \pmod{m_1}$	$M_2 x_2 \equiv 1 \pmod{m_2}$	$M_3 x_3 \equiv 1 \pmod{m_3}$
$\Rightarrow 20x_1 \equiv 1 \pmod 3$	$15x_2 \equiv 1 \pmod 4$	$12x_3 \equiv 1 \pmod 5$
$\to 2x_1 \equiv 1 \pmod 3$	$3x_2 \equiv 1 \pmod 4$	$2x_3 \equiv 1 \pmod 5$
$\therefore x_1 = 2$ as $3 \mid 2(2)-1$	$x_2 = 3$ as $4 \mid 3(3)-1$	$x_3 = 3$ as $5 \mid 2(3)-1$

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

$\therefore$ Relation ① becomes,

$x \equiv [20\cdot 2\cdot 2 + 15\cdot 3\cdot 1 + 12\cdot 3\cdot 3] \pmod{60}$

$x \equiv [80 + 45 + 108] \pmod{60}$

$x \equiv 233 \pmod{60}$

$x \equiv 53 \pmod{60}$

$60 \overline{)233}$ (3), 180, 53

$\boxed{x = 53}$

② $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

$\to$ $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

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

$\therefore$ 3, 5, 7 are pair wise relative prime.

Next,

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

where $M = m_1 m_2 m_3 = 3\cdot 5\cdot 7 = 105$

$M = 105$

$M_1 = \frac{M}{m_1} = 5\cdot 7 = 35$

$M_2 = \frac{M}{m_2} = 3\cdot 7 = 21$

$M_3 = \frac{M}{m_3} = 3\cdot 5 = 15$

Calculate x_i:

$M_1x_1 \equiv 1 \pmod{m_1}$	$M_2x_2 \equiv 1 \pmod{m_2}$	$M_3x_3 \equiv 1 \pmod{m_3}$
$35x_1 \equiv 1 \pmod 3$	$21x_2 \equiv 1 \pmod 5$	$15x_3 \equiv 1 \pmod 7$
$2x_1 \equiv 1 \pmod 3$	$1x_2 \equiv 1 \pmod 5$	$1x_3 \equiv 1 \pmod 7$
$x_1 = 2$ $\quad 3/2(2)-1$	$x_2 = 1$ $\quad 5/1(1)-1$	$x_3 = 1$ $\quad 7/1(1)-1$

$\therefore$ Relation (1) becomes

$x = 35\cdot2\cdot2 + 21\cdot1\cdot3 + 15\cdot1\cdot2 \pmod{105}$

$x \equiv 140 + 63 + 30$

$x \equiv 233 \pmod{105}$

$x \equiv 23 \pmod{105}$.

$\boxed{x = 23.}$

GREATEST COMMON DIVISION BETWEEN THE POSITIVE INTEGER

Find GCD between following pair of integer.

i] 100, 37

$\rightarrow$ $GCD(37, 100) = GCD(37, 100 \pmod{37})$

$= GCD(37, 26)$

$= GCD(26, 37 \pmod{26})$

$= GCD(26, 11)$

$= GCD(11, 26 \pmod{11})$

$= GCD(11, 4)$

$= GCD(4, 11 \pmod 4)$

$= GCD(4, 3)$

$= GCD(3, 4 \pmod 3)$

$= GCD(3, 1)$

$= GCD(1, 3 \pmod 1)$

$= 1$

(ii) 252, 52

$\rightarrow$ $GCD(52, 252) = GCD(52, 252 \pmod{52})$

$= GCD(52, 44)$

$= GCD(44, 52 \pmod{44})$

$= GCD(44, 8)$

$= GCD(8, 44 \pmod{8})$

$= GCD(8, 4)$

$= GCD(4, 8 \pmod{4})$

$= \cancel{GCD}\ 4$

(iii)