MODULAR ARITHMETIC

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ iff $m | a-b$.

① $a \equiv b \bmod m$ { If both a and b have same remainder when divided by 'm'.

eg. $36 \equiv 24 \bmod 12$

② $a \equiv b \bmod m$ [If m divides $(a-b)$] ie $m | a-b$

e.g. $20 \equiv 3 \bmod 17$ [17 divides $(20-3 = 17)$]

③ If $x \equiv y \bmod m$ and $a \equiv b \bmod m$ then

$(x+a) = (y+b) \bmod m$

e.g. $17 \equiv 4 \bmod 13$ and $42 \equiv 3 \bmod 13$

$\Rightarrow 59 \equiv 7 \bmod 13$

④ If $x \equiv y \bmod m$ & $a \equiv b \bmod m$ then

$(x-a) = (y-b) \bmod m$

eg. $42 \equiv 3 \bmod 13$

$14 = 1 \bmod 13$ $\Rightarrow 28 \equiv 2 \bmod 13$

⑤ $a = k.m + b$

29th May, 2019
Wednesday

Group, Ring, Integral Domain & field

① Group

A set of objects along with a binary operation on the element of the set that must satisfy the following four properties to be called as a group.

a) Closure : with respect to an operation i.e. if a & b are in a set then $a \circ b = c$ is also in the set where $\circ \rightarrow$ operator for the desired operation.

b) associativity : with respect to operation i.e. $(a \cdot b) \circ c = a \circ (b \cdot c)$

c) Guaranteed existence of a unique identity closure with regards to the operation i.e.

i → called identity element if for every a in a set we have,

$$a \cdot i = a$$

d) The existence of inverse element for each element with regard to the operation i.e. for every 'a' in the set, the set must also contain element 'b' such that $a \cdot b = i$ ($\because i \rightarrow$ identity element).

In general a group is denoted by $\{G, O\}$ where G is the set of objects, $O \rightarrow$ operator

⇒ Instead of denoting group operator 'O', we may denote it by '+'.

Infinite vs Finite Group

⇒ A group based on a set of infinite size are rather easy to imagine is called infinite group. For example:

(i) the set of integers (+ve, -ve & 0) along with the operation of arithmetic addition constitutes a group.

(ii) for a given value of N, the set of $N \times N$ matrix over real number under operation of matrix addition constitutes a group

(iii) set of all even integers.

(iv) set of all 3X3 non singular matrix along with matrix multiplication as operator forms a group. This group is denoted as GL(3), plays a vital role in computer graphics & computer vision, GL stands for 'General Linear'.

Finite Group

Let $L_n = \{1, 2, 3 - - - -\}$ denotes a set of labels for n objects which is not the set turning into group. Hence the set that will turn into a group is the set of permutations of label L_n is called finite group.

In other words, considering the set of all permutation of labels in the set L_n. Denoting the set by S_n provided that each element of the set stands a permutation $(P_1, P_2 - - - P_n)$ where $P_i \in L_n$ and $P_i \neq P_j$ whenever $i \neq j$. For example: the case when $L_3 = \{1, 2, 3\}$. In this case the set of permutation of labels will be

$$S_3 = \{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\}$$

The set S_3 is of size 6. In a broad way we say cardinality of S_3 is 6.

Let binary operation on the element of S_n be that of composition of permutations. We will denote a composition of two permutation by symbol 'O'. For any two elements ρ & π of the set S_n, the composition $\pi \circ \rho$ means that we want to repermutate the elements of ρ according to the element of π.

Let $L_3 = \{1, 2, 3\}$

each element of S_3 is a distinct permutation of three labels i.e. $S_3 = \{(P_1, P_2, P_3)\} \mid P_1, P_2, P_3 \in L_3$ with $P_1 \neq P_2 \neq P_3$. Consider following two elements π & ρ in the set of permutations.

$$\pi = (3,2,1).$$
$$\rho = (1,3,2)$$

Let us consider the following composition of two permutations.

$$\pi \circ \rho = (3,2,1) \circ (1,3,2)$$

i.e. permute ρ according to π means 3rd element of ρ followed by 2nd element followed by 1st element of ρ. Finally resulting permutation is given by $\{2,3,1\}$ so we can say

$$\pi \circ \rho = \{3,2,1\} \circ \{1,3,2\} = \{2,3,1\}$$

Clearly $\pi \circ \rho \in L_3$. This shows that $S_3 \rightarrow$ closed with respect to composition of two permutation.

Also, the set must satisfy the three conditions as:

① Associativity

$$\rho_1 \circ (\rho_2 \circ \rho_3) = (\rho_1 \circ \rho_2) \circ \rho_3$$

② S_3 contains a special element $(1,2,3)$ as identity element with respect to composition of permutation operator. It is definitely the case of any $\rho \in S_3$. we have,

$$(1,2,3) \circ \rho = \rho \circ (1,2,3) = \rho$$

$\pi \circ \rho$ $(3,2,1) \Rightarrow$ (3rd position, 2nd position, 1st p...)

$(3,2,1)$ $(1,3,2)$

$(2,3,1) \Rightarrow (3^{rd} \to 2, 2^{nd} - 3, 1^{st} - 1)$

(3) As S_3 is a small sized set, we can easily demonstrate that for every $\rho \in S_3$ there exists another unique element $\pi \in S_3$ such that

$$\rho \circ \pi = \pi \circ \rho = \text{the identity element.}$$

For the sake of convenience we may use a notation $-\rho$ for such a π. We say that S_3 along with composition of permutation operator is a group.

- Note that set S_n of all permutation of labels in set L_n can only be finite. As a result, S_n along with the operation of composition denoted by '$\circ$' forms a finite group.

- The set S_n of permutations along with the composition of permutation operator is called permutation group.

- If the operation on the set of the element is commutative it is called abelian group. $a \circ b = b \circ a$ (S_n = abelian only for $n=$...

- The set of all integers along with operation of arithmetic addition is called abelian group.

(2) Ring

If we can define one or more abelian group, we have a ring provided that the elements of the set satisfy some properties with respect to this new operation. We use the new operation as multiplication (only for convenience) to tell it apart from the operations defined for the abelian group. A ring is typically denoted as $\{R, +, \times\}$ where, R denotes the set of the object, '+' is the operator with respect to which R is an abelian group and '*' is the new operator require to form a ring.

#) Properties of ring

1) R must be closed with respect to the additional operator.

2) R must be exhibiting associativity properties with respect to '*'.

3) The new additional operator '*' must be distributive over group addition operator.

i.e.

$$a*(b+c) = (a*b) + (a*c)$$
$$(a+b)*c = (a*c) + (b*c)$$

4) The multiplication operation is frequently shown by just concatenation in such equation.

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

Example: 5) The set of all integers (+ve, -ve & zero) under operation of arithmetic addition and multiplication is a ring.

- set of all arithmetic integers with '+' and '*' is a ring.

- for a given value of N, set of all N*N square matrix addition and multiplication is a ring.

- set of all real numbers along with operation of arithmetic addition and multiplication is a ring.

#) Commutative Ring

A ring is commutative if the multiplication operation is commutative for all element in ring.

i.e. $a \cdot b = b \cdot a$. For example: $\{R, +, *\}$ where,

R may be (1) set of all integers

(2) set of all even numbers

(3) Integral Domain

An Integral Domain $\{R, +, *\}$ is a commutative ring that obeys the following properties:

(i) R must include an identity element for the multiplicative operation i.e. symbolically designate an element of set R as 1 so that every element 'a' of the set, we can say that

$$a \cdot 1 = 1 \cdot a = a$$

(ii) R must include an identity element for the addition operation of multiplication operation of any two elements a & b of R results in zero i.e. if $a \cdot b = 0$ then either a or b must be zero.

(4) Field

A field denoted by $\{F, +, *\}$ is an integral domain which satisfies the following additional properties. For every element in F except the 1's designated as '0', there must also exist multiplicative inverse in F i.e.

if $a \in F$ and $a \neq 0$ then

there must exist an element $b \in F$ such that

$$a \cdot b = b \cdot a = 1$$

i.e. for a given 'a', there should be 'b' designated as 'a^{-1}'

Prime Number

⇒ should always be greater than one.

Ex: $\{2, 3, 5, 7, 11, 13$ and so on$\}$

Twin Prime

⇒ pair of prime numbers whose difference is only 2.

Example: (3, 5), (5, 7), (11, 13) - - - - .

The largest twin prime is unknown.

Co-prime

⇒ If common factors of two numbers is only 1, then it is said to be co-prime. Those numbers themselves should be prime.

Ex: (2, 3), (3, 5), (5, 7) - - - - - - . The gcd of these no. will be 1.

⇒ set of numbers which donot have any other factor other than one.

~~Properties of co-prime~~ Ex: (8, 9). The HCF becomes 1.

~~⇒ set of numbers~~

~~⇒ All the co-primes are~~

Properties of co-prime

⇒ All the prime numbers are co-prime to each other.

⇒ Any two consecutive integers are always co-prime.

⇒ Some of any two prime numbers is always co-prime of their product.

Ex: $3 + 5 = 8$

$3 * 5 = 15$

⇒ 1 is always co-prime with all numbers.
⇒ Two numbers (natural) a and b will be co-prime if $(2a-1)$ & $(2b-1)$ are co-prime.

Ex: $2\times\boxed{3}-1=\boxed{5}$
$2\times\boxed{2}-1=\boxed{3}$

Euclidean Algorithm

1) Find the gcd of 8, 22

$8=\{1,2,4\}$
$22=\{1,2,11\}$
$\therefore gcd=2$

2) Find the gcd of 2322, 54

$2322=\{1,2,3 \ldots\}=3\times18 \ldots$
$54=\{1,2,3,\ldots\}=3\times3\times3\times2$
$\therefore gcd=3$

⇒ Algorithm to find out gcd of any two integers efficiently

Observation of gcd calculation
⇒ $gcd(a,a)=a$
⇒ If b/a then $gcd(a,b)=a$

⇒ $gcd(a,0)=a$. Since it is always true that $a/0$.

⇒ Assuming without loss of generality that a is greater than b, it can be shown that

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

#) Find gcd of (70, 38).

⇒ Solution,

$$\begin{aligned}\gcd(70,38) &= \gcd(38, 70 \bmod 38)\\ &= \gcd(38, 32)\\ &= \gcd(32, 38 \bmod 32)\\ &= \gcd(32, 6)\\ &= \gcd(6, 32 \bmod 6)\\ &= \gcd(6, 2)\\ &= \gcd(2, 6 \bmod 2)\\ &= \gcd(2, 0)\end{aligned}$$ [When 0, take one step ahead

$\therefore \gcd(70, 38) = 2.$

OR

$70 = 38*1 + 32$

$38 = 32*1 + 6$

$32 = 6*5 + 2$

$6 = \boxed{2}*3 + 0$

gcd

Extended Euclidean Algorithm

$\boxed{a = b \cdot q + r}$

Find the multiplicative inverse of 3 mod 17. (Using Extended Euclidean Algorithm).

$$3 \bmod 17 = 1$$

Check for multiplicative inverse first:

$$17 = 3 \times 5 + 2$$

$$3 = 2 \times 1 + 1$$

There exists a multiplicative inverse for 3 & 17.

Rewrite above equations,

$$2 = 17 - 3 \times 5 \quad \text{--- (1)}$$

$$1 = 3 - 2 \times 1 \quad \text{--- (2)}$$

Extended Euclidean

$$1 = 3 - 2 \times 1$$

or, $1 = 3 - (17 - 3 \times 5) \cancel{\times} 1 \quad [\because 2 = 17 - 3 \times 5]$

or, $1 = 3 - (17 - 3 \times 5)$

or, $1 = 3 - 17 + 3 \times 5$

or, $1 = 3 + 3 \times 5 - 17$

or, $1 = 3 \times (1 + 5) - 17$

or, $1 = 3 \times \underline{\underline{6}} - 17$

$\therefore$ multiplicative inverse of 3 mod 17 is 6.

Calculate multiplicative inverse of 5 mod 26.

$$5 \bmod 26 = 1$$

Check for multiplicative inverse first :

$26 = 5*5 + 1$ $\qquad$ $5*4+6$

$5 = 2*2 + 1$ $\qquad$ $6 = 2*2+2$

$\cancel{2 = 2*1 + 1}$ $\qquad$ $2 = 2*1+0$

There exists a multiplicative inverse for 5 mod 26.

Rewrite above equation,

$$1 = 26 - 5*5$$

19 mod 26

Check for multiplicative inverse first:

$26 = 19*1 + 7$

$19 = 7*2 + 5$

$7 = 5.1 + 2$

$5 = 2.2 + 1$

There exists multiplicative inverse for 19 mod 26.

Rewrite these equations,

$7 = 26 - 19*1$ — (1)

$5 = 19 - 7*2$ — (2)

$2 = 7 - 5*1$ — (3)

$1 = 5 - 2*2$ — (4)

Extended Euclidean is,

$1 = 5 - 2*2$

or, $1 = 5 - (7 - 5.1)*2$

$$\left\{\begin{array}{l} \text{or, } 1 = 5 - [7 - (19 - 7*2).1]*2 \\ \text{or, } 1 = 5 - [7 - (19 - (26 - 19*1)*2]*2 \end{array}\right\}?$$

or, $1 = 5 - 7.2 + 5.2$

~~or, 1 = 5.(1-7..~~ or, $1 = 5.3 - 7.2$

or, $1 = (19 - 7*2).3 - 7.2$

or, $1 = 19.3 - 7.6 - 7.2$

or, $1 = 19.3 - 7.8$

or, $1 = 19.3 - (26 - 19.1).8$

or, $1 = 19.3 - 26.8 + 19.8$

or, $1 = 19.11 - 26.8$

multiplicative inverse of 19 mod 26 = 11

Euler's Totient Function

$\phi(n)$ for $n \geq 1$: defined as the number of integers less than n that are co-prime to n.

$$\phi(5) = \{1, 2, 3, 4\} = 4$$
$$\phi(6) = \{1, 5\} = 2$$

These are counts of the numbers.

Case:

when 'n' is a prime numbers,

$$\phi(n) = n - 1$$
$$\therefore \phi(23) = 22$$

$\phi(a*b) = \phi(a) + \phi(b)$ [$\because$ a & b are co-prime i.e. $\gcd(a,b) = 1$]

Example: $\phi(35) = \phi(7) * \phi(5)$

$$= 6 * 4$$
$$= 24$$

Euler's Theorem

$$x^{\phi(n)} = 1 \bmod n \text{ (if } x \text{ \& } n \text{ are co-prime)}$$

Example:

$$x = 4, \quad n = 165$$
$$\gcd(4, 165) = 1$$
$$\phi(165) = \phi(15) * \phi(11)$$
$$= \phi(5) * \phi(3) * \phi(11)$$
$$= 4 * 2 * 10$$
$$= 80$$

It implies $4^{80} = 1 \bmod 165 \Rightarrow \boxed{x^{\phi(n) \cdot a} \equiv 1 \bmod n}$

#) Fermat's Theorem (Special case of Euler's Theorem)

If n is prime, we can write $\phi(n) = n-1$. Hence, Euler's Theorem becomes

$$x^{n-1} = 1 \bmod n$$

Multiplying Both sides by x, we have

$$x^{n} = x \bmod n$$

Example:

$$3^5 \equiv 3 \bmod 5$$
$$3^7 \equiv 3 \bmod 7$$

Special case : x is not divisible by n.

i.e. $x \not\equiv 0 \bmod n$

Example:

$$x^{n-1} \equiv 1 \bmod n$$

Let $x = 3$ & $n = 5$

Then,

$$3^{5-1} \equiv 1 \bmod 5$$

or, $3^4 \equiv 1 \bmod 5$

or, $81 \equiv 1 \bmod 5$

31st May, 2019
Friday

Exercises

① What is the last digit of 3^{5000}?

$$(3^2)^{2500} = (9)^{2500} = (-1)^{2500} \bmod 10$$

② Find the gcd of integer 4589, 4849

⇒ Solution,

$$\begin{aligned}
\gcd(4589, 4849) &= \gcd(4849, 4589) \\
&= \gcd(4589, 4849 \bmod 4589) \\
&= \gcd(4589, 260) \\
&= \gcd(260, 4589 \bmod 260) \\
&= \gcd(260, 169) \\
&= \gcd(169, 260 \bmod 169) \\
&= \gcd(169, 91) \\
&= \gcd(91, 169 \bmod 91) \\
&= \gcd(91, 78) \\
&= \gcd(78, 91 \bmod 78) \\
&= \gcd(78, 13) \\
&= \gcd(13, 78 \bmod 13) \\
&= \gcd(13, 0)
\end{aligned}$$

∴ The gcd of (4589, 4849) is 13.//

#) Find the integers s & t such that 31s + 64t = 1.

Bezout's Identity

For non-zero integers a & b, let

$d = \gcd(a,b)$ then there exists integers x & y such that $ax + by = d$.

x & y are called bezout's coefficients.

⇒ solution,

$$\gcd(64,31) = \gcd(31, 64 \bmod 31)$$
$$= \gcd(31, 2)$$
$$= \gcd(2, 31 \bmod 2)$$
$$= \gcd(2,1)$$
$$\therefore \gcd(31,64) = 1$$

Here,

$$64 = 31 * 2 + 2 \quad -① $$
$$31 = 15 * 2 + 1 \quad -② $$

Rewrite above equation,

$$2 = 64 - 31 * 2$$
$$1 = 31 - 15 * 2$$

Now,

Extended euclidean is,

$$1 = 31 - 15 \times 2$$
$$\text{or, } 1 = 31 - 15(64 - 31 * 2)$$
$$\text{or, } 1 = 31 - 15 * 64 + (31 * 2)15 \quad [\because 31(1+30) - 15 * 64]$$
$$\text{or, } 1 = 31 * 31 - 15 * 64$$

comparing it with $ax + by = d$ so, $x = 31$, $y = 64$

i.e. $s = 31$ & $t = 15$.

Given equation is $4s + 16t = 4$

$\gcd(4,16) = 4$

$16 = 4*4+0$ ~~or, $= 4*3+1$~~ $= 4*5-1$

$s=1,\ t=0$

$s=-3,\ t=1$

$s=5,\ t=-1$

$\boxed{4\times(-3)+16 = -12+16 = 4}$

#) Find multiplicative inverse of 11 mod 15.

⇒ Solution,

$11 \bmod 15 = 1$

Check for multiplicative inverse first:

$15 = 11\times 1 + 4$

$11 = 4\times 2 + 3$

$4 = 3*1+1$

There exists a multiplicative inverse for 11 & 15.

Rewrite above equations,

$4 = 15 - 11*1$ — (1)

$3 = 11 - 4*2$ — (2)

$1 = 4 - 3*1$ — (3)

Extended Euclidean,

$1 = 4 - 3*1$

$= 4 - (11 - 4*2)*1$

$= 4 - (11 - 4*2)$

$= 4*(1+2) - 11$

$= (15 - 11*1)3 - 11$

$= 15*3 - 11*3 - 11$

$= 15*3 - 11*(3+1) = 15*3 - 11*4$

∴ multiplicative inverse of $11 = -4$ i.e. $-4+15 = 11$.