Lecture-1

Problem: Let's say a and b are two numbers. We want to find numbers s and t such that

$$\boxed{as + bt = gcd(a, b)}$$

We know that

$$gcd(75, 21) = 3$$

$$75 = 25 \times 3$$

$$21 = 7 \times 3$$

Algorithm:

This is Extended Euclidean algorithm

$r_1 = a$, $s_1 = 1$, $s_2 = 0$

$r_2 = b$, $t_1 = 0$, $t_2 = 1$

While($r_2 > 0$)

{

$q = r_1 / r_2$;

$r = r_1 - q r_2$;

$r_1 = r_2$;

$r_2 = r$;

$s = s_1 - q s_2$;

$s_1 = s_2$;

$s_2 = s$;

$t = t_1 - q t_2$;

$t_1 = t_2$; $t_2 = t$;

}

$s \leftarrow s_1$; $t \leftarrow t_1$; $gcd \leftarrow r_1$

return s, t, gcd;

$\boxed{}$: Initialized

Let's trace with $a = 75$, $b = 21$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
3	$\boxed{75}$	$\boxed{21}$	12	$\boxed{1}$	$\boxed{0}$	1	$\boxed{0}$	$\boxed{1}$	−3
1	21	12	9	0	1	−1	1	−3	4
1	12	9	3	1	−1	2	−3	4	−7
3	9	3	0	−1	2	−7	4	−7	25
	3	0		2	−7		−7	25	

Termination Condition

$s \leftarrow s_1 = 2$

$t \leftarrow t_1 = -7$

$\gcd(a,b) \leftarrow r_1 = 3$

Verify $as + bt = \gcd(a,b)$

$LHS = as + bt$

$= 75(2) + 21(-7)$

$= 150 - 147$

$= 3$

$RHS = \gcd(a,b) = 3$

L.H.S = R.H.S ⇒ verified

"जय"

Date
Page

Imp: Numbers a and b are called relatively prime or co-prime if

$$\boxed{\gcd(a,b) = 1}$$

Imp: We know that according to Extended Euclidean algorithm,

$$as + bt = \gcd(a,b)$$

Let's put n inplace of a
Let's put a inplace of b

$$\therefore ns + at = \gcd(n,a)$$

$$\therefore (ns + at) \bmod n = [\gcd(n,a)] \bmod n$$

Assume a and n are co-prime

$$\Rightarrow \gcd(n,a) = 1$$

$$\therefore (ns + at) \bmod n = 1 \bmod n = 1$$

$$\therefore (ns + at) \bmod n = 1$$

$$\therefore [ns \bmod n + at \bmod n] \bmod n = 1$$

$$\therefore [0 + at \bmod n] \bmod n = 1$$

$$\therefore \boxed{at \bmod n = 1}$$ (2 times mod n is same as 1 time mod n)

$at \text{ Mod } n = 1$

i.e. $(a * t) \text{ Mod } n = 1$

These numbers 'a' and 't' are known as Multiplicative Inverse of each other

$\therefore a^{-1} \text{ Mod } n = t$ or $t^{-1} \text{ Mod } n = a$ } 'a' and 't' are Multiplicative Inverse of each Other.

IMP If a and n are co-prime then it is possible to find $a^{-1} \text{ Mod } n$ (Multiplicative Inverse of a with respect to n)

→ Using Extended Euclidean algorithm, We can easily find Multiplicative Inverse (Provided a and n are co-prime.)

Date______
Page______

Question: Is 5 multiplicative Inverse of 21 with respect to modulo 26?

(5×21) MOD 26
$= 105$ MOD 26
$= 1$

Note: 5^{-1} MOD 26 is possible as gcd(5,26) = 1

∴ 5 and 21 are Multiplicative Inverses of each other

$$\boxed{\begin{array}{l} \therefore 5^{-1} \text{ MOD } 26 = 21 \\ 21^{-1} \text{ MOD } 26 = 5 \end{array}}$$

Question: How to Modify Extended Euclidean algorithm so that we can find the Multiplicative Inverse?

→ Provided 'a' and 'n' are co-prime, it is possible to find a^{-1} mod n

→ We can delete S_1, S_2, S (three columns) from the table of Extended Euclidean algorithm.

That can give Compact Table. Actually there is no need of S_1, S_2, S as a^{-1} Mod n = t (which is returned

Q) Find 5^{-1} MOD 26 (Compare with a^{-1} Mod n)

We will initialize

$r_1 \leftarrow n = 26$

$r_2 \leftarrow a = 5$

Now, Do the same process but without 3 columns s_1, s_2, s

q	r_1	r_2	r	t_1	t_2	t
5	$\boxed{26}$	$\boxed{5}$	1	$\boxed{0}$	$\boxed{1}$	−5
5	5	1	0	1	−5	26
	1	0		−5	26	

↑ Terminating Criteria

$gcd \leftarrow r_1 = 1$

$t = t_1 = -5$ (Which is Multiplicative Inverse)

−5 is not in the range of MOD 26

∴ −5 MOD 26 = 21

In the range

$$26 \overline{\smash{)}\begin{array}{r} -1 \\ -5 \\ -26 \\ + \\ \hline 21 \end{array}}$$

∴ 21 is multiplicative Inverse of 5 w.r.t 26

Question: Find 4^{-1} MOD 26

$a=4, n=26$

$gcd(a,n) = gcd(4,26)$

$= 2 \neq 1$

$gcd(a,n) \neq 1 \Rightarrow$ 'a' and 'n' are not co-prime

$\therefore 4^{-1}$ MOD 26 doesn't exist.

Question: Find 11^{-1} MOD 26

Check $gcd(11, 26)$

$= 1$

$\therefore$ It is possible.

Another way

$(11 * x)$ MOD $26 = 1$

Find x which satisfy the above equation.

Use Brute force and try to put $x = 1, 2, 3, \ldots, 25$

and find the answer

Brute force (Practically Not possible)

x	$11*x$	$(11*x)$ mod 26	
1	11	11	
2	22	22	
3	33	7	
4	44	18	
5	55	3	
6	66	14	
7	77	25	
8	88	10	
9	99	21	
10	110	6	(26*4=104)
11	121	17	
12	132	2	(26*5=130)
13	143	13	
14	154	24	
15	165	9	(26*6=156)
16	176	20	
17	187	5	
18	198	16	(26*7=182)
☆ 19	209	$\boxed{1}$	(26*8=208)

We get $x = 19$ such that

$$11x \text{ MOD } 26 = 1$$

$$\therefore 11^{-1} \text{ MOD } 26 = 19$$

Similarly 19^{-1} MOD 26 = 11

☆ This approach is practically not used because if n (26 here) is very large, it would be expensive to obtain multiplicative inverse