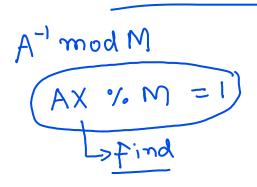
Modular Inverse



- (1) X 6/W | LO M-1 (2) GCD(A,M)=1

1. $3^{-1} \mod 11$ AX mod 11 = 1 \(\text{1.} \)

A \(\text{M} \)

X	> rem		
	AX	AX % 11	
1	3	3	
2	6	6	
3	9	9	
4	12	1 -> Stop	
15	45 X	1 X X 6/W 1 to 10	

X	AX	AX %13
1	4	4
2	8	8
3	12	12
4	16	3
5	20	子
6	24	E 1
7	28	2
8	32	6
9	32 36	10
10	40	1N 2 top

28%13

METHOD 2 - USE EXTENDED EUCLIDEAN

X → 1 to 391

$$27^{-1} \mod 392$$

$$2 (392 + 27(-14)) + 27(-1) = 1$$

$$2 \cdot 392 + 27(-28) + 27(-1) = 1$$

$$2 \cdot 392 + 27(-29) = 1$$

$$1 \implies M = \frac{A}{392 - 29} = 363$$

=) 2.392 + 27(363) = 1multiple of M / L)?

A mod-inverse