Modular Inverse

$A^{-1} \bmod M$

$AX \% M = 1$

↳ find

Eg. $3^{-1} \bmod 27$

① X b/w 1 to M-1

② GCD(A,M) = 1

$X \to \underline{1 \text{ to } 10}$ $\quad AX \bmod 11 = 1$ ✓

1. $\underset{A}{3}^{-1} \bmod \underset{M}{11} = 4$ //

→ rem

X	AX	AX % 11
1	3	3
2	6	6
3	9	9
4	12	1 → stop
15 X	45 X	1 X X b/w $\underline{1 \text{ to } 10}$

2. 4^{-1} mod 13

A M

$\underline{28 \% 13}$

$\frac{28}{13} = \underline{\underline{9}} + \underline{\underline{2}}$

X	AX	AX %13
1	4	4
2	8	8
3	12	12
4	16	3
5	20	7
6	24	11
7	28	2
8	32	6
9	36	10
10	40	1 ✓ stop

METHOD 2 - USE EXTENDED EUCLIDEAN

$X \to 1$ to 391

$27^{-1} \bmod 392$

$\frac{392}{27} = 14.51$

$q \to 14$

$$\begin{array}{r} 14 \\ 27 \overline{)392} \\ 378 \\ \hline 14 \end{array}$$

$r \to 14$

① $392 = Aq + r$

$392 = 27(14) + 14$ — ① $\Rightarrow 392 + 27(-14) = 14$ — ④

prev r

prevA $27 = 14(1) + 13$ — ② $\Rightarrow \underbrace{27 + 14(-1)}_{\downarrow} = 13$ — ⑤

$14 = 13(1) + 1$ — ③ $\Rightarrow 14 + 13(-1) = 1$ — ⑥

$r == 1 \Rightarrow$ Stop//

Sub eq ⑤ in ⑥

$14 + [27 + 14(-1)](-1) = 1$

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

$2(14) + 27(-1) = 1$ — ⑦

Sub eq ④ in ⑦,

$$\underbrace{27}^{-1} \bmod 392$$

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

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

$$\underbrace{2 \cdot 392}_{\underline{\underline{M}}} + \underbrace{27}_{\underline{A}}(-29) = 1$$

$\hookrightarrow M - (\text{-ve no})$
$= 392 - 29 = 363$

$$\Rightarrow \underbrace{2 \cdot 392}_{\text{multiple of } M} + \underbrace{27}_{\underline{\underline{A}}} \underbrace{(363)}_{\hookrightarrow \underline{?}} = \underbrace{1}_{\hookrightarrow X}$$

mod-inverse