Problem 1:

Input a, b, M

Output: $\boxed{a^b \% M}$

$5 \% 3 = 2$

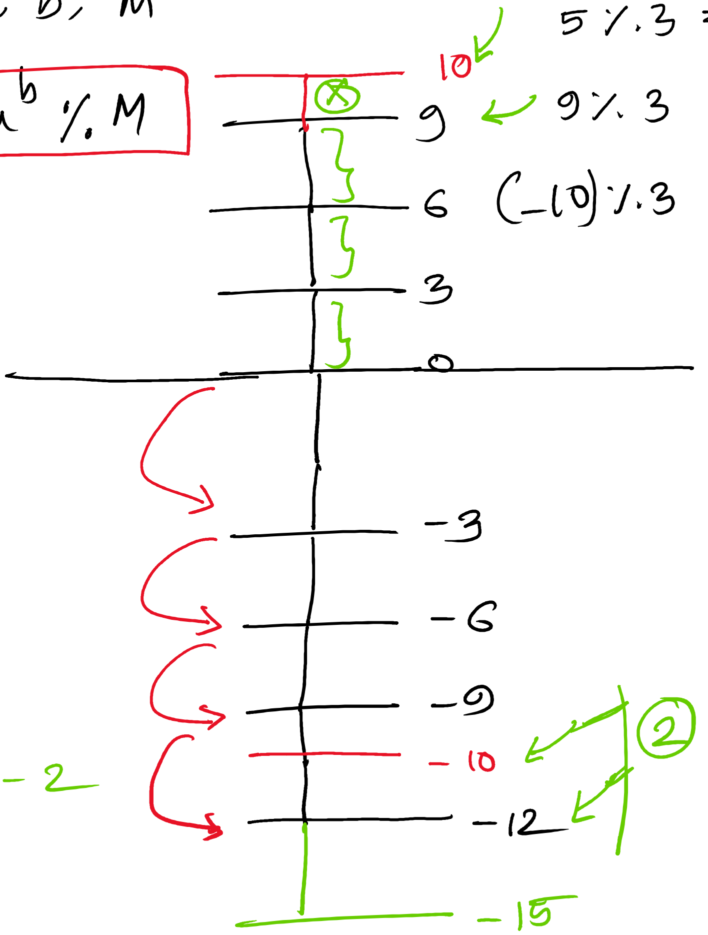
$9 \% 3 = 0$

$(-10) \% 3 = -1$?

$+1$?

2 ✓

$\boxed{-10 \% 3 = -1}$



$O(\log b)$

$-12 - (-10)$

$= -12 + 10 = -2$

$3 \overline{)\,-10\,}(-4$

-12

$+2$

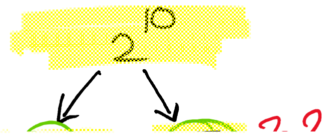
$2^{100} \% 17 \rightarrow pow(2,10)$

T.C: $O(b)$

$$\boxed{\begin{array}{l} a \le 10^9 \\ b \le 10^{12} \\ M \le 10^{12} \end{array}}$$

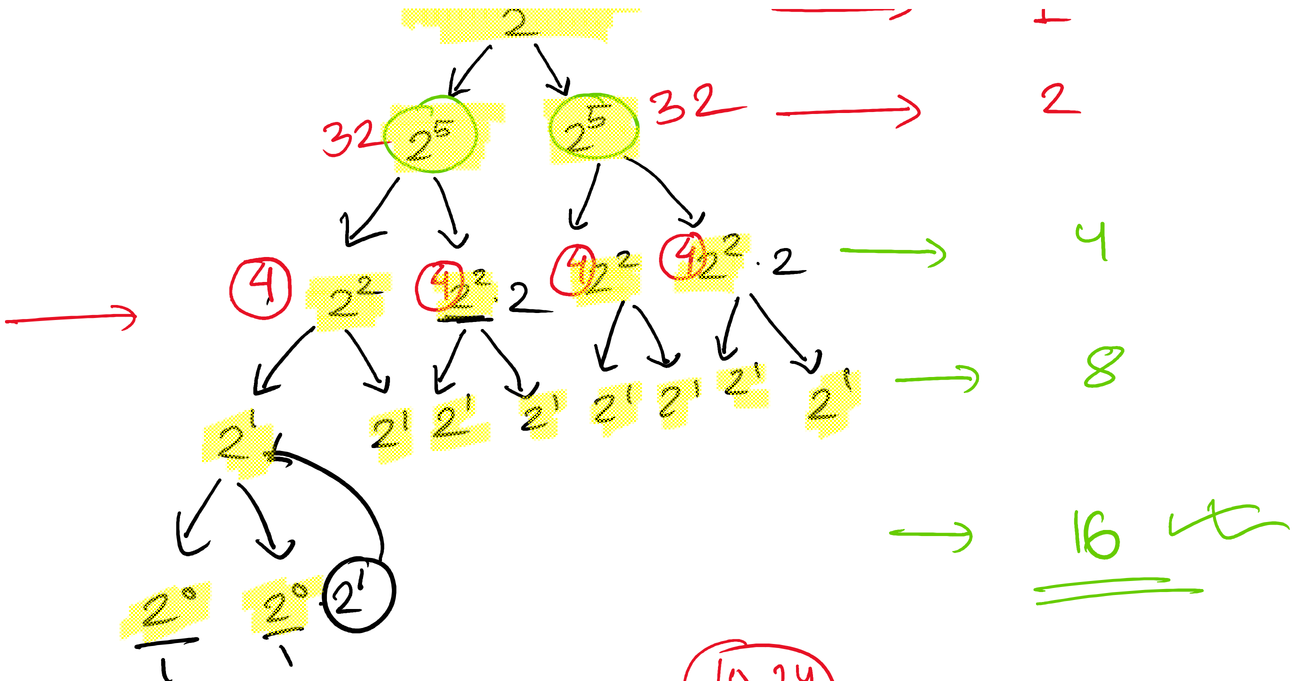
BigMod

$1024 \% 5 \rightarrow \textcircled{4}$



$\longrightarrow$ 1

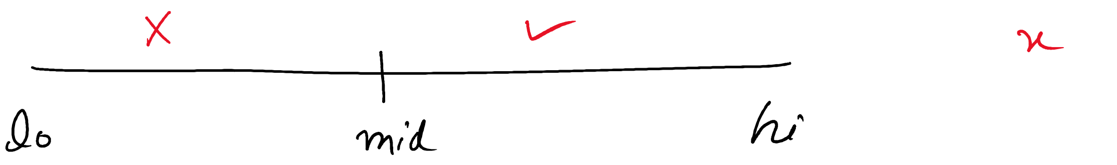
2

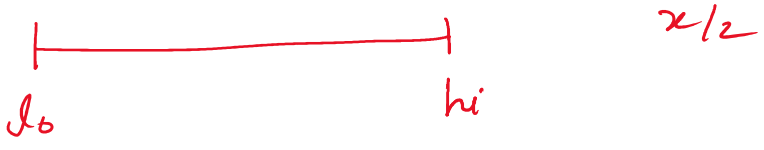


1024

b
↓
b/2
↓
b/4
↓
b/8
⋮
1
↓
0

$$2^{10}$$
$$\downarrow$$
$$2^5 = \overset{32}{x_1} \mid y_1 = (\overset{32}{x_1} * \overset{32}{x_1}) \% M = 1024$$
$$\downarrow$$
$$2^2 = \overset{4}{x_2} \mid y_2 = (\overset{4}{x_2} * \overset{4}{x_2} * 2) \% M = 32$$
$$\downarrow$$
$$2^1 = \boxed{\overset{2}{x_3}} \mid y_3 = (\overset{2}{x_3} * \overset{2}{x_3}) \% M = 4$$
$$\downarrow$$
$$2^0 = x_4 \mid y_4 = (\underset{1}{x_4} * \underset{1}{x_4} * 2) \% M = 2$$





$O(\log_2 b)$

$x/4$ ... → 0

$(a \times b) \% M = ((a\%M) \times (b\%M))\%M$ ✓

$(a/b)\%M = ((a\%M) / (b\%M))\%M$ ✗

$1^0 = 1$

$100^0 = 1$ ✓

Problem2: Given, $N \leq 10^{12}$ $\quad \underline{\underline{O(N)}}$

prime ~~factorize~~ $N \rightarrow \boxed{p}$

$$\begin{array}{r|l} 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline 3 & 3 \\ \hline & 1 \end{array}$$

$24 = 2 \times 2 \times 2 \times 3$

$= 2^3 \times 3^1$

$2, 3, 5, 7, 11, 13 \ldots\ldots \underline{p}$

$[1 - N]$ $\quad \boxed{\dfrac{N}{\ln(N)}}$

$$\begin{array}{r|l} 5 & 125 \\ \hline 5 & 25 \\ \hline 5 & 5 \\ \hline & 1 \end{array} \qquad \underline{\underline{125}}$$

$p \times q = N$

① $p < \sqrt{N}$ and $q < \sqrt{N}$ ✗

② $p > \sqrt{N}$ and $q < \sqrt{N}$ ✗

✓ ✓ ✓
$2, 3, 4, \underline{\underline{5}}$

② $p > \sqrt{N}$ and $q < \sqrt{N}$ ✗

③ $p > \sqrt{N}$ and $q > \sqrt{N}$ ✗

④ $\boxed{p < \sqrt{N}}$ and $q > \sqrt{N}$ ✓

⑤ $\boxed{p = \sqrt{N}}$ and $q = \sqrt{N}$ ✓

$$p \cdot q > N$$

$$\begin{tikzcd} p \arrow[d] & q \\ <\sqrt{N} & >\sqrt{N} \arrow[u] \end{tikzcd}$$

$$N = \underline{p_1}^{\underline{a_1}} \times \underline{p_2}^{\underline{a_2}} \times \underline{p_3}^{\underline{a_3}} \times p_4^{\underline{a_4}}$$

$$<\sqrt{N}<$$

$$N = \underline{2 \times 2 \times 3 \times 5} \times \overset{\boxed{\times}}{\underline{\underline{97}}} = 5820/60$$

$$\sqrt{N} = 76$$

$$\frac{N}{2 \times 2 \times 3 \times 5} = \underline{\underline{97}}$$

$$\underline{\underline{O(\sqrt{N})}}$$

$$\overline{2 \times 2 \times 3 \times 5 \times 31}^{\,<\sqrt{N}} = 1860$$

$$\sqrt{1860} = 43$$

$$\frac{N}{2 \times 2 \times 3 \times 5 \times 31} = \boxed{1}$$