

→ Large exponentiation using Binary Multiplication 49

→ Let's suppose in the last problem

We have: ~~$a \leq 10^{18}$~~ ~~$\&$~~ ~~M~~

~~$a \leq 10^{18}$~~ $a \leq 10^{18}$ ~~$\&$~~ $M \leq 10^{18}$

∴ We can take $a = a \% M$ in the beginning of function to prevent it from overflow. But what if, we have $a \leq 10^{18}$ ~~$\&$~~ $M \leq 10^{18}$

Now, there will be a case if we will be doing:

$$LL \text{ } ans = (a * a) \% M$$

$$\begin{array}{cc} \downarrow & \downarrow \\ 10^{18} & 10^{18} \end{array}$$

This will still overflow because we can't

directly multiply $10^{18} \times 10^{18}$.
So, to solve such kind of problems,
we use Binary Multiplication.

What is exactly $a * a$?
→ It is a added a times.
 $a + a + a + \dots + a$ a times.

So, to prevent overflow instead of
directly multiplying, we can take
1. n after each adding.

e.g. ~~$(a * a) * p$~~

$$a + a < 2 \times 10^{18} \quad (3) \quad a = 10^{18}$$

$$\therefore n < 10^{18}$$

$$+ a < 2 \times 10^{18}$$

$$\therefore n < 10^{18}$$

It will
never overflow

∴ To achieve this we can use Brute
Force Method, which will be the
using of FOR loop till $a \leq 10^{18}$.
But its T.C is $O(a)$.

→ We can achieve this in $O(\log(n))$
T.C using Binary Multiplication,
(similar to Binary exponentiation of
iterative method).

Suppose, we have $a = 3$ and $b = 13$,
We have to do $a \times b$.

We can achieve this using binary multiplication like this:

3 (13)

3 (8 + 4 + 0 + 1)

3 \rightarrow 3

6 \rightarrow

12 \rightarrow 15

24 \rightarrow 39

13 \rightarrow 1101 (3 in binary)

\Rightarrow (8 + 4 + 0 + 1)

(3 \times 1) We want this

(3 \times 2) We don't want this

(3 \times 4) We want this

(3 \times 8) We want this.

```
INT BINMULTIPLY (LL A, LL B)
{
```

~~LL~~ ~~LL~~

LL ANS = 0;

WHILE (B > 0)

{

IF (B & 1)

{

ANS = (ANS + A) % M;

}

A = (A + A) % M;

B >>= 1;

}

RETURN ANS;

}