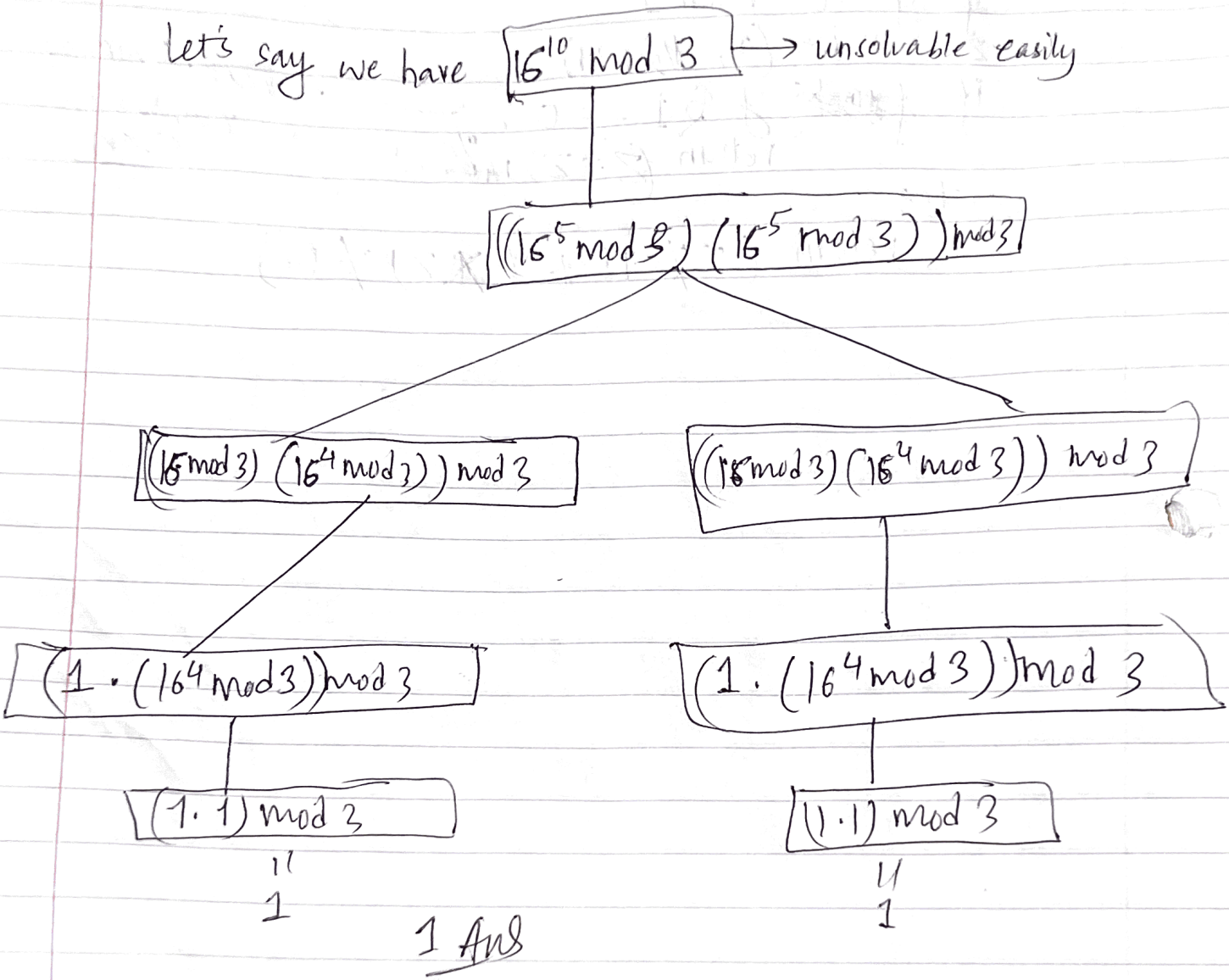
Modular exponentiation :

Let's say we have $16^{10} \bmod 3$ → unsolvable easily



1 Ans

Miller Rabin Primality Test

Step1 : find $n-1 = 2^k \times m$

Step2 : Choose 'a' such that $1 < a < n-1$

Step3 : compute $b_0 = a^m \pmod n$; ... ; b_i $b_i \; b_{i-1}^2 \pmod n$

↓ Result of b_0

$+1 \rightarrow$ Composite

$-1 \rightarrow$ Probabably Prime.

eg. 561

$n = 561$

1) $560 = 2^4 \times 35$, $k=4$, $m=35$

2) $a = 2$, $a > 1$ and $a < 560$

3) $b_0 = 2^{35} \pmod{561}$

↓ This is modular exponentiation (use it

is $b_0 = \pm 1 \pmod{561}$ ⟶ NO

↓ so

Calculate $b_1 = b_0^2 \pmod n = 263^2 \pmod{561}$

$b_3 = 1 \pmod{561}$ $\longrightarrow$ composite.