

+

Review:

Def of  $a \bmod m =$  remainder when dividing  $a$  by  $m$ .

Compute  $45 \times 73 \bmod 7$

$$45 \bmod 7 = 3$$
$$73 \bmod 7 = 3$$
$$3 \times 3 = 9 \bmod 7 = \boxed{2}$$

$$267^{12} \bmod 5 = 2^{12} \bmod 5$$

$$\begin{array}{r} 53 \text{ (22)} \\ 5 \overline{)267} \end{array}$$

$$2^{12} \pmod{5}$$

$$12 \pmod{4} = 0$$

$$= 2^0 \pmod{5} = \boxed{1}$$

use Fermat's Little Thm.

$$2^4 \pmod{5} = 1$$

So we can reduce the exponent mod 4.

---

$$\begin{array}{l} 493 \leftarrow \text{reduce mod } \phi(12) = 4 \\ 301 \pmod{12} = 1^{493} \pmod{12} \\ \text{reduce } \uparrow \pmod{12} \\ \begin{array}{r} 25 \text{ (R1)} \\ 12 \overline{) 301} \end{array} \end{array}$$

$$= \boxed{1}$$

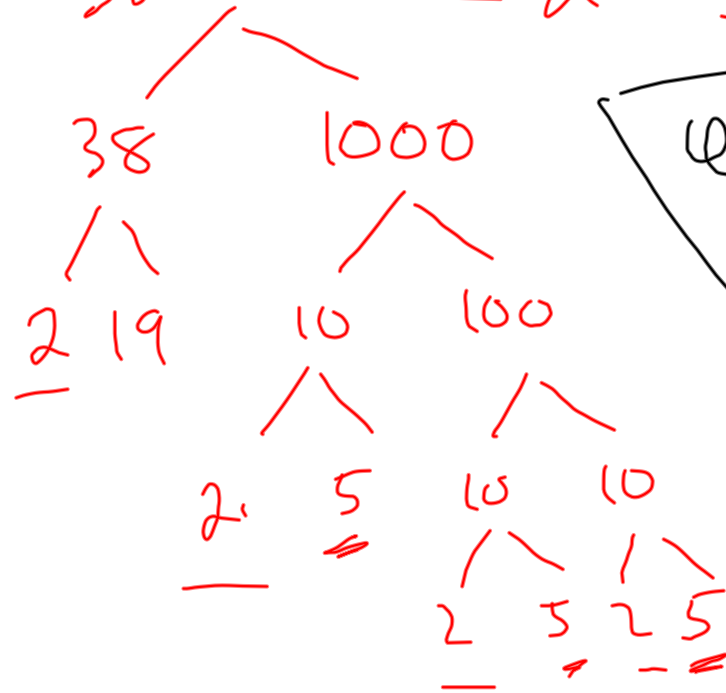
$$\begin{aligned} \phi(12) &= \\ \phi(3 \cdot 4) &= \\ &= \phi(3) \cdot \phi(4) \\ &= 2 \cdot 2 = 4 \end{aligned}$$

$$\begin{aligned} \phi(p^k) &= \\ p^k - p^{k-1} \end{aligned}$$

$$\varphi(38000) = \varphi(2^4) \cdot \varphi(5^3) \cdot \varphi(19)$$

$$= \boxed{8 \cdot 100 \cdot 18} = \boxed{14400}$$

$$38000 = 2^4 \cdot 5^3 \cdot 19$$



$\varphi(n) = \#$  of numbers  $\leq n$  which are relatively prime to  $n$ .

$$\varphi(19) = \varphi(19^1)$$

$$= 19^1 - 19^0 = 19 - 1$$

$$= \boxed{18}$$

13      7      Find  $7^{-1} \pmod{13}$

$$\underline{13} = 1 \cdot \underline{7} + \underline{6}$$

$$\underline{7} = 1 \cdot \underline{6} + \underline{1}$$

$$\underline{6} = 6 \cdot \underline{1} + \underline{0}$$

$$= 2 \cdot 7 - 1 \cdot 13$$

$$= 7 - 1 \cdot (13 - 1 \cdot 7)$$

$$1 = 7 - 1 \cdot 6$$

$$\text{So } 7^{-1} \pmod{13} = \underline{2}$$

∴  
Simplify  
sub

simplify  
sub

Simplify  
sub

Find  $37^{-1} \pmod{100}$

$$\underline{100} = 37 \cdot \underline{2} + 26$$

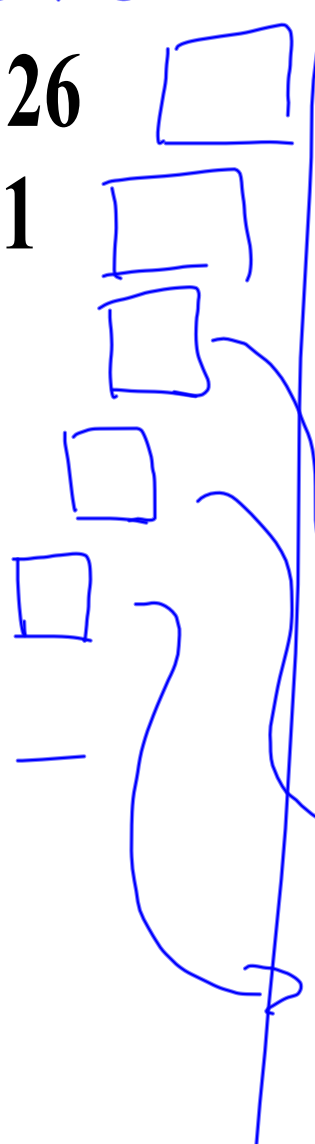
$$\underline{37} = 26 \cdot \underline{1} + 11$$

$$\underline{26} = 11 \cdot \underline{2} + 4$$

$$\underline{11} = 4 \cdot \underline{2} + 3$$

$$\underline{4} = 3 \cdot \underline{1} + 1$$

$$\underline{3} = 1 \cdot \underline{3} + 0$$



$$\sum_0 37^{-1} = -27 \pmod{100} \quad (\text{we added 100 to } -27)$$

$$= \boxed{73}$$

$$= 10 \cdot 100 - 27 \cdot 37$$

$$= 10 \cdot (100 - 2 \cdot 37) - 7 \cdot 37$$

$$= 10 \cdot 26 - 7 \cdot 37$$

$$= 3 \cdot 26 - 7 \cdot (37 - 1 \cdot 26) \quad \text{Simp}$$

$$= 3 \cdot 26 - 7 \cdot 11 \quad \text{Sub}$$

$$\rightarrow = 3(26 - 2 \cdot 11) - 1 \cdot 11 \quad \text{Simp}$$

$$= 3 \cdot 4 - 1 \cdot 11 \quad \text{Sub}$$

$$\rightarrow = 4 - 1 \cdot (11 - 2 \cdot 4) \quad \text{Simp}$$

$$\rightarrow 1 = 4 - 1 \cdot 3$$