

composite n , calculate $(n-1)!$ and try to see "why" it's div. by n .

$$\begin{array}{lcl} n=6 & 5! = 5 \cdot 4 \cdot \color{red}{3} \cdot \color{red}{2} \cdot 1 & \} a < b \\ n=8 & 7! = 7 \cdot 6 \cdot 5 \cdot \color{red}{4} \cdot \color{red}{3} \cdot \color{red}{2} \cdot 1 & \} \\ n=9 & 8! = 8 \cdot 7 \cdot \color{red}{6} \cdot 5 \cdot \color{red}{4} \cdot \color{red}{3} \cdot 2 \cdot 1 & \} a = b \end{array}$$

n composite means that $n = ab$ $1 < a \leq b < n$.

case 1: $a < b$

case 2: $a = b$

$$nb^2 = a^2$$

p prime factor of b

$$\Rightarrow p \mid b^2$$

$$\Rightarrow p \mid a^2 \text{ (since } p \mid b^2 \nmid b^2 \mid a^2 \text{)}$$

$$\stackrel{EL}{\Rightarrow} p \mid a$$

$$a = d_m p^m + d_{m-1} p^{m-1} + \dots + d_1 p + d_0$$

$$a^n = (d_m p^m + \dots + d_1 p + d_0)^n$$

$$= a^{d_m p^m} a^{d_{m-1} p^{m-1}} \dots a^{d_1 p} a^{d_0}$$

$$= (a^{d_m})^{p^m} (a^{d_{m-1}})^{p^{m-1}} \dots \color{red}{(a^{d_1})^p} a^{d_0}$$

$$= a^{d_m p^m} \dots a^{d_2 p^2} a^{d_1 p} a^{d_0}$$

• if $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$

• $a^p \equiv a \pmod{p}$.

$$\begin{aligned} (a^{d_1})^{p^2} &= ((a^{d_1})^p)^p \\ &\equiv (a^{d_1})^p \\ &\equiv a^{d_1} \end{aligned}$$