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

$n=6$. $\quad 5! = 5\cdot 4\cdot 3\cdot 2\cdot 1$

$n=8$ $\quad 7! = 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1$ $\Big\}$ $a<b$

$n=9$ $\quad 8! = 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1$ $\}$ $a=b$

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

case 1: $a<b$

case 2: $a=b$

$n | b^2 = a^2$

p prime factor of b

$\Longrightarrow p | b^2$

$\Longrightarrow p | a^2$ (since $p | b^2$ & $b^2 | a^2$)

$\overset{EL}{\Longrightarrow} p | a$

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

$$a^n = a^{d_m p^m + \cdots + d_1 p + d_0}$$

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

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

$$\equiv a^{d_m} \quad \cdots a^{d_2} a^{d_1} a^{d_0}$$

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

$$(a^{d_2})^{p^2} = ((a^{d_2})^p)^p$$

$$\equiv (a^{d_2})^p$$

$$\equiv a^{d_2}$$