FERMAT'S LITTLE THEOREM: If p is prime & $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

PROOF:

Assume p is a prime number and $p \nmid a$.

$\Rightarrow$ Every integer is congruent to one of $0, 1, 2, \ldots, p-1 \pmod{p}$

Only focus on non-zero congruence classes, because $0 \pmod{p}$ contains all the multiples of p ($\because p \nmid a$)

Focus on $1, 2, \ldots, p-1$
Multiply all of these by a:

$$a, 2a, \ldots, (p-1)a$$

Show this is a rearrangment of $1, 2, \ldots, p-1$.

Case 1: None of these are congruent to 0.

Suppose $r \cdot a \equiv 0 \pmod{p}$.
Then $p \mid r \cdot a$, but this is impossible since $p \nmid a$ & $r < p$.

Case 2: These are distinct; no two are congruent to each other.
Let us consider 2 values, $r \cdot a, s \cdot a$

$$0 < r < p$$
$$0 < s < p.$$

To show: $r \cdot a \not\equiv s \cdot a \pmod{p}$.

do look at $r \cdot a - s \cdot a = a \cdot (r-s)$

By assumption, $p \nmid a$.

Can p divide $r-s$?

$$0 < r < p$$

$$0 > -s > -p$$

$$\downarrow$$

$$-p < r-s < p.$$

$r - s \neq 0$, because r and s are distinct congruence classes

So, $p \nmid r-s$ which means $a, 2a, \ldots, (p-1)a$ is a rearrangement of $1, 2, \ldots, p-1$

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$$

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

$\div$ by $(p-1)!$ on both sides,

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$