Andrew Ardito

Fermat's Little Theorem:

if p is a prime, and $gcd(a, p) = 1$, then: $a^{p-1} \equiv 1 \ (mod \ p)$

Lemma: The set of numbers: $\{a, 2a, ..., (p-1)a\}$ is the same as the set of numbers $\{1, 2, ..., p-1\}$, although not necessarily in the same order.

Proof:

First, if $ai \equiv aj \ (mod \ p)$, then $i \equiv j \ (mod \ p)$, since $gcd(a, p) = 1$.

Thus the numbers $a, 2a, ..., (p-1)a$ are all distinct mod p, and none of them are divisible by p, so the two sets are equivalent.

If two sets are equivalent (mod p), then the product of their elements (mod p) will be the same.

So: $(p-1)! \equiv a^{p-1}(p-1)! \ (mod \ p) \Rightarrow a^{p-1} \equiv 1 \ (mod \ p)$

□