4.15 Theorem. (Fermat's Little Theorem, Version I) If p is a prime and a is an integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. By Theorem 4.14, $a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot (p-1) \pmod{p}$. Simplifying,

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

Notice since p is prime, no number less than p will divide p. $(p-1)!$ contains no factors of p. Thus, since $(p,(p-1)!) = 1$, $a^{p-1} \equiv 1 \pmod{p}$. $\square$