4.41 Theorem. (Wilson's Theorem) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Let a prime p be given. Letting $p = 2$,

$$\begin{aligned}(2-1)! &\equiv -1 \pmod{2},\\ 1 &\equiv -1 \pmod{2}.\end{aligned}$$

We find $(p-1)! \equiv -1 \pmod{p}$ to be true when $p = 2$. Note $p = 3$ is also trivial. Suppose $p > 3$. By Theorem 4.40, $(p-2)! \equiv 1 \pmod{p}$. By definition,

$$pk = (p-2)! - 1 \text{ for some } k \in \mathbb{Z}.$$

Multiplying both sides by $p - 1$,

$$\begin{aligned}pk(p-1) &= (p-1)(p-2)! - (p-1)\\ &= (p-1)! - p + 1.\end{aligned}$$

Rearranging,

$$\begin{aligned}(p-1)! + 1 &= pk(p-1) + p\\ &= ppk - pk + p\\ &= p(pk - k + 1).\end{aligned}$$

By CPI, let $pk - k + 1 = k' \in \mathbb{Z}$ such that $(p-1)! + 1 = pk'$. Thus, by definition, $(p-1)! \equiv -1 \pmod{p}$. $\square$