

4.40 Theorem. If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$.

Proof. Let a prime $p > 2$ be given. Notice for any integers $2 \leq a, b \leq p-2$, there are $\frac{p-3}{2}$ distinct pairs such that $a \neq b$. By Theorem 4.36,

$$\begin{aligned} a_1 b_1 &\equiv 1 \pmod{p}, \\ a_2 b_2 &\equiv 1 \pmod{p}, \\ &\vdots \\ a_{\frac{p-3}{2}} b_{\frac{p-3}{2}} &\equiv 1 \pmod{p}. \end{aligned}$$

By Theorem 4.38, $(a_1 b_1)(a_2 b_2) \dots (a_{\frac{p-3}{2}} b_{\frac{p-3}{2}}) \equiv 1 \pmod{p}$. Since these are distinct pairs such that $a \neq b$, $2 \cdot 3 \cdot 4 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$, provided $p > 2$. \square