

Proposition. Let p be an odd prime, then the Legendre symbol $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8}. \end{cases}$

Proof. We can rewrite the product of all even residues modulo p as $2 \cdot 4 \cdot 6 \cdots (p-1) \equiv 2 \cdot 4 \cdot 6 \cdots 2 \lfloor \frac{p-1}{4} \rfloor \cdot (-2 \cdot \lfloor \frac{p-1}{4} \rfloor + (-1)^{\lfloor \frac{p-1}{2} \rfloor}) \cdots (-3) \cdot (-1)$ (substitute every factor a greater than $\frac{p-1}{2}$ by $p-a$) (\star)

Examples. • $p=11$, then $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \equiv 2 \cdot 4 \cdot (-5) \cdot (-3) \cdot (-1) \pmod{11}$
 • $p=13$, then $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \equiv 2 \cdot 4 \cdot 6 \cdot (-5) \cdot (-3) \cdot (-1) \pmod{13}$

Notice that the l.h.s. of (\star) is

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv 2^{\lfloor \frac{p-1}{2} \rfloor} \cdot 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right) = 2^{\lfloor \frac{p-1}{2} \rfloor} \cdot \left(\frac{p-1}{2}\right)!,$$

while the r.h.s. can be simplified as

$$2 \cdot 4 \cdots 2 \lfloor \frac{p-1}{4} \rfloor \cdot (-1) \cdot (-3) \cdots (-2 \lfloor \frac{p-1}{4} \rfloor + (-1)^{\lfloor \frac{p-1}{2} \rfloor}) = (-1)^{\lfloor \frac{p-1}{4} \rfloor} \cdot 1 \cdot 2 \cdot 3 \cdots \left(\frac{p-1}{2}\right) = (-1)^{\lfloor \frac{p-1}{4} \rfloor} \cdot \left(\frac{p-1}{2}\right)! \quad \leftarrow \lfloor \frac{p-1}{4} \rfloor \text{ factors}$$

Therefore, (\star) is equivalent to the equality

$$2^{\lfloor \frac{p-1}{2} \rfloor} \left(\frac{p-1}{2}\right)! = (-1)^{\lfloor \frac{p-1}{4} \rfloor} \cdot \left(\frac{p-1}{2}\right)! \quad (\Rightarrow) \quad 2^{\lfloor \frac{p-1}{2} \rfloor} = (-1)^{\lfloor \frac{p-1}{4} \rfloor}$$

As $2^{\lfloor \frac{p-1}{2} \rfloor} \equiv \left(\frac{2}{p}\right)$ (Euler's property), it remains to

check that $(-1)^{\lfloor \frac{p-1}{4} \rfloor} = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$ which is straight forward \square