This is the solution to Problem 7 by Bach Bui, Kevin Hughes, and Rob Seilheimer.

Let n be an odd number with $n-1 = 2^r b$ with b odd. Define $w(n)$ be the number of prime factors of n (let $k = w(n)$) and $v(n)$ to be the largest power of 2 that divides $p_i - 1$ for all i. So $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where the p_i are primes. Similarly $p_i - 1 = 2^{r_i} b_i$ for all i. (a,b) means the gcd(a,b).

Define $S = \{a \in \mathbb{Z}/n | a^b = 1 \text{ or } a^{2^j b} = -1 \text{for some} 0 \leq j < r\}$ and $G = \{a \in (\mathbb{Z}/n)^* | a^{\frac{n-1}{2}} = (\frac{a}{n})\}$. We know that $S \subset G \subset (\mathbb{Z}/n)^*$.

Theorem $\#S \nmid \#G \Leftrightarrow S$ is not a subgroup of G.
($\Rightarrow$) This is a result of group theory.

($\Leftarrow$) We know the sizes of S, G.

$$\#S = \left(\frac{2^{w(n)v(n)} - 1}{2^{w(n)} - 1} + 1 \right) \prod_i (b, p_i - 1)$$

$$\#G = \delta \prod_i \left(\frac{n-1}{2}, p_i - 1 \right) \quad \delta = \begin{cases} 2 & \text{if } \min\{r_i\} = r \\ \frac{1}{2} & \text{if } \exists r_i < r \\ 1 & \text{otherwise} \end{cases}$$

And we know by another theorem that S is a group if and only if $k = w(n) = 1$ or there exists $p_i \equiv 3 (\text{mod } 4)$. So we are assumiing that S is not a group which implies that $k > 1$ and $p_i \equiv 1 (\text{mod } 4)$ for all i (thus $r_i \geq 2$ for all i).

Then

$$\frac{2^{w(n)v(n)} - 1}{2^{w(n)} - 1} + 1 = 1 + 2^k + 2^{2k} + \cdots + 2^{k(v(n)-1)} + 1$$

$$= 2 + 2^k + \cdots + 2^{k(v(n)-1)} \equiv 2 (\text{mod } 4)$$

and thus $\#S = 2x \prod (b, p_i - 1)$ with x odd and the product is over all p_i such that $i = 1, \cdots, k$ or equivalently $p | n$ (this is true for all the products below).

Also, note that $(\frac{n-1}{2}, p_i - 1) = (2^{r-1}, p_i - 1) * (b, p_i - 1) = (2^{r-1}, 2^{r_i}) * (b, p_i - 1)$.

Combining these, we see that

$$\frac{\#G}{\#S} = \frac{\delta \prod \left(\frac{n-1}{2}, p_i - 1\right)}{2x \prod (b, p_i - 1)}$$

$$= \frac{\delta \prod (2^{r-1}, 2^{r_i})(b, p_i - 1)}{2x \prod (b, p_i - 1)}$$

$$= \frac{\delta \prod (2^{r-1}, 2^{r_i}) \prod (b, p_i - 1)}{2x \prod (b, p_i - 1)}$$

$$= \frac{\delta \prod (2^{r-1}, 2^{r_i})}{2x} = \frac{2^m}{2x}$$

And since $k > 1$ and $r > 1$, $m \geq 1$.

$$\frac{\#G}{\#S} = \frac{2^{m-1}}{x} \notin \mathbb{Z}$$

So $\#S \nmid \#G$ and the theorem holds.