Problem

Prove that for any integer p > 1, if p isn't pseudoprime, then p fails the Fermat test for at least half of all numbers in Z^+_p

Step-by-step solution

Step 1 of 1

It sufficient to prove that elements set in Z_p^+ that pass the Fermat test forms multiplicative subgroup of Z_p^+. Since the subgroup order divides the group order, if subgroup is a strict subgroup, it must contain at most half of elements of group.

To show that the set is a subgroup, it is required to show that it is nonempty and closed under the inverses and multiplication.

• First, the set is nonempty, since $1^{p-1} \equiv 1 \bmod \mathrm{p}$.

• If $a^{p-1} \equiv 1 \bmod p$, and $b^{p-1} \equiv 1 \bmod p$, then $(ab)^{p-1} \equiv a^{p-1}b^{p-1} \equiv 1 \bmod p$, which shows closure under multiplication.

• If $a^{p-1} \equiv 1 \bmod p$, then multiplying both sides of the equation by the $\left(a^{-1}\right)^{p-1}$ shows that $1 \equiv \left(a^{-1}\right)^{p-1} \bmod p$. Thus, the set is closed under inverses.

Hence, on the other side if p is not pseudo prime then p fails Fermat Test for at least half of number.

Comment