10.16 Consider $Z_p = \{0, 1, \ldots, p-1\}$, and define $Z_p^* \subset Z_p$ as the set of those elements in Z_p that have a multiplicative inverse; i.e., $a \in Z_p^*$ iff there exists a b such that $ab = 1 \pmod{p}$. Note that Z_p^* is a group. Now consider $S \subseteq Z_p^*$ consisting of those elements $a \in Z_p^*$ for which $a^{p-1} = 1 \pmod{p}$. It is easy to check that S is in fact a *subgroup* of Z_p^*. Therefore, using the Lagrange Theorem, $|S|$ must divide $|Z_p^*|$. Suppose now that there exists an element $a \in Z_p^*$ for which $a^{p-1} \neq 1 \pmod{p}$. Then, $|S|$ must be at most half of Z_p^* and therefore at most half of Z_p. Note that in the book, the question only says that there exists an $a \in Z_p$ such that $a^{p-1} \neq 1 \pmod{p}$, not in Z_p^*! **This is a mistake.** In fact, the bad a must be in Z_p^*, which stated in a different way means that $\gcd(a, p) = 1$.

If you do not want to use group theory for this question, you can do it the following way: show that if there is an a such that $\gcd(a, p) = 1$ and the test fails for a (i.e., $a^{p-1} \neq 1 \pmod{p}$), then for every b for which the test passes, there is a c for which the test fails. Suppose the test passes for b. Then, let $c := ab \pmod{p}$. It remains to show that if the test passes for b_1, b_2, then $ab_1 \neq ab_2 \pmod{p}$. This follows from the fact that $ab_1 = ab_2 \pmod{p}$ implies $a(b_1 - b_2) = 0 \pmod{p}$, so p must divide $a(b_1 - b_2)$, so $pk = a(b_1 - b_2)$, and since $b_1, b_2 \in Z_p$, $|b_1 - b_2| < p$, so $\operatorname{lcm}(a, p) < ap$, so $\gcd(a, p) > 1$, which is a contradiction.