Proof of Cauchy's theorem

Theorem 1 (Cauchy's theorem)**.** *If p is prime and $p|n$, where n is the order of a group G, then G has an element of order p.*

Proof. Let S be the set of ordered p-tuples $(a_1, a_2, \ldots, a_p)$ with the property that each $a_i \in G$ and $a_1 a_2 \cdots a_p = e$, the identity element of G. The set S has n^{p-1} elements, since we can choose the first $p-1$ of the a_i arbitrarily and then set $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$. We think of the elements of the symmetric group $S_{n^{p-1}}$ as permuting the p-tuples in S. Let $f \in S_{n^{p-1}}$ be the element of $S_{n^{p-1}}$ sending any $(a_1, a_2, \ldots, a_p)$ to $(a_p, a_1, a_2, \ldots, a_{p-1})$. This is an element of $S_{n^{p-1}}$ because if $(a_1 a_2 \cdots a_{p-1})a_p = e$, then $a_p(a_1 a_2 \cdots a_{p-1}) = e$ as well. Note that f^p is the identity permutation, so f has order p in $S_{n^{p-1}}$, and when f is written in cycle notation, every element of S is in either a 1-cycle or a p-cycle. If there are k p-cycles and m 1-cycles, then $n^{p-1} = kp + m$. But $p|n$, so $p|m$ as well. In any 1-cycle, f sends an element $(a_1, a_2, \ldots, a_p)$ of S to itself via the map sending it to $(a_p, a_1, a_2, \ldots, a_{p-1})$, so we have $a_p = a_1 = a_2 = \ldots = a_{p-1}$ and there is an element $(g, g, \ldots, g)$ of S with $g \in G$ and $g^p = e$. Taking g to be the identity element $e \in G$ gives one such element of S, but this cannot be the only one, since there are m of them and $p|m \geq 1$. Thus, there is another element $x \in G$ with $x \neq e$ and $x^p = e$. $\square$