In this note we prove the following well known fact.

Theorem. *Let $n \geq 1$. Then we have $\gcd(n, \varphi(n)) = 1$ if and only if any group of order n is cyclic.*

Proof. We first take care of the easy direction: suppose that $\gcd(n, \varphi(n)) \neq 1$. Let p be a prime dividing n and $\varphi(n)$. Then there are two possibilities. Either p^2 divides n or there is a prime divisor $q \equiv 1 \pmod{p}$ of n. In the first case we observe that the product of a cyclic group of order p and one of order n/p has order n, but is not cyclic. In the second case we note that the matrix group

$$M \;=\; \{\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : x, y \in \mathbf{F}_q \text{ and } y^p = 1\}$$

has order pq and is not commutative. Therefore, the product of M and a cyclic group of order n/pq is a non-cyclic group of order n.

Next we deal with the other direction. Suppose $\gcd(n, \varphi(n)) = 1$. Then n is squarefree and for every divisor d of n we have $\gcd(d, \varphi(d)) = 1$. Therefore we may proceed inductively. Let G be a non-cyclic group of order n

Step 1. *We may assume that G contains no proper normal subgroups.*

Indeed, let $N \subset G$ be a proper normal subgroup. By induction N is cyclic of order d say. Since $\#\mathrm{Aut}(N) = \varphi(d)$ is prime to $n = \#G$, the homomorphism $G \longrightarrow \mathrm{Aut}(N)$ given by conjugation, is *trivial*. It follows that $N \subset Z(G)$. By induction $G/Z(G)$ is cyclic. It follows that G is abelian. Since $\#G$ is squarefree, G is cyclic and we are done.

We consider the centralizers C of non-identity elements $x \in G$.

Step 2. *We have $C \neq G$ for every centralizer C. The normalizer $N(C)$ of C is equal to C. For any two distinct centralizers C and C', we have $C \cap C' = \{1\}$.*

Since G admits no proper normal subgroups, we have $C \neq G$ when $x \neq 1$. By step 1 we have $N(C) \neq G$. Therefore $N(C)$ is cyclic by induction. But then it centralizes C, so that $C = N(C)$. This takes care of the second statement. To prove the third, let $1 \neq x \in C \cap C'$. Then C is contained in the centralizer C'' of x. Since $C'' \neq G$, it is by induction a cyclic group. Therefore C'' centralizes C and we have $C = C''$. By the same argument we have $C' = C''$ and it follows that $C = C'$.

Step 3. Pick $x \in G$, $x \neq 1$ and let C be its centralizer. Let U denote the union of the conjugates of C. By Step 2 the set U has $[G : C](\#C - 1) + 1$ elements. Since $C \neq G$, there is a prime number p dividing $[G : C]$. Let C' be the centralizer of an element of order p. The union V of the conjugates of C' has $[G : C'](\#C' - 1) + 1$ elements. Since p divides $\#C'$ but does not divide $\#C$, each conjugate of C has by Step 2 trivial intersection with each conjugate of C'. Therefore $U \cap V = \{1\}$. Since $[G : C]$ and $[G : C']$ are at most $\frac{1}{2}\#G$, this gives

$$\#(U \cup V) = [G : C](\#C - 1) + [G : C'](\#C' - 1) + 1 = 2\#G - [G : C] - [G : C'] + 1 > \#G,$$

a contradiction.