

6. Since $\gcd(a_i, n) = 1$ for any i , and $\gcd(a, n) = 1$, it is obvious that $\gcd(aa_i, n) = 1$ for any i .

We next prove that aa_i is not $\equiv aa_j \pmod{n}$ if $i \neq j$. If not, $aa_i \equiv aa_j \pmod{n}$, and $n | a(a_i - a_j)$. However, since $\gcd(a, n) = 1$, this implies that $n | (a_i - a_j)$ or in other words $a_i \equiv a_j \pmod{n}$, which is a contradiction.

This implies that if $a_1, a_2, \dots, a_{\phi(n)}$ is a reduced residue modulo n , so is $aa_1, aa_2, \dots, aa_{\phi(n)}$. This concludes the proof.