

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.

7. Consider the set of integers $< n$ that are coprime to n . Call these $a_1, a_2, \dots, a_{\phi(n)}$. Clearly these form a reduced residue system modulo n . Now for any a such that $\gcd(a, n) = 1$, we know from exercise 6 above that $aa_1, aa_2, \dots, aa_{\phi(n)}$ is also a reduced residue system modulo n .

Now, for any i , $aa_i = qn + r_i$, where $0 < r_i < n$ and $\gcd(r_i, n) = 1$. In other words, $r_i = a_j$ for some j . Thus, for each i , there is a unique j such that $aa_i \equiv a_j \pmod{n}$.

Therefore,

$$\begin{aligned} aa_1 aa_2 \cdots aa_{\phi(n)} &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \\ a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \\ \therefore a^{\phi(n)} &\equiv 1 \pmod{n} \end{aligned}$$

where the last line is due to the fact that we can cancel out the term $a_1 a_2 \cdots a_{\phi(n)}$ on both sides due to it being relatively coprime to n . This concludes the proof.

8. We know that $kx \equiv 1 \pmod{p}$ must have exactly one unique solution since $\gcd(k, p) = 1$. If the solution has the form $qp + r$, where $0 < r < p$, then $k(qp + r) \equiv 1 \pmod{p}$, which leads to $kr \equiv 1 \pmod{p}$. This proves that there is some unique solution from the set $\{1, 2, \dots, (p-1)\}$.

Further if $x = k$ is a solution for $kx \equiv 1 \pmod{p}$, then $p|(k^2 - 1)$. i.e. $p|(k+1)(k-1)$. This is only possible if one of these terms is either 0 or p , which happens iff $k = 1$ or $k = p-1$.

This concludes the proof.

9. In light of the solution to problem 8, $(p-1)!$ can be thought of as products of pairs of integers k and b_k such that $kb_k \equiv 1 \pmod{p}$, except the terms 1 and $(p-1)$, which don't have the appropriate pairing. Therefore, $(p-1)! \equiv 1(p-1) \pmod{p}$ i.e. $(p-1)! \equiv -1 \pmod{p}$. This concludes the proof.