4.13 Theorem. Let p be a prime and let a be an integer not divisible by p; that is, $(a,p) = 1$. Then $\{a, 2a, 3a, ..., pa\}$ is a complete residue system modulo p.

Proof. Suppose not. That is, given the assumptions above, $\{a, 2a, 3a, ..., pa\}$ is not a complete residue system modulo p. Let $A = \{a, 2a, 3a, ..., pa\}$. Suppose $ma \equiv na \pmod{p}$ where $1 \leq m, n \leq p$, and WLOG $m > n$, are distinct coefficients of elements from set A. By definition,

$$p|ma - na$$
$$p|a(m - n).$$

Since $p \not| a$, it is implied p must divide $m - n$. However, $m - n < p$, and by Theorem 2.27, $p \not| m - n$ which is a contradiction. Furthermore, this implies that for any m and n, $ma \not\equiv na \pmod{p}$, which is another contradiction to our assumptions. By Thus, $\{a, 2a, 3a, ..., pa\}$ is a complete residue system modulo p, provided p is prime and $a \in \mathbb{Z}$ is not divisible by p. $\square$