Your Name: ____________ Group Members:____________ ____________

Problem 1 *Repeat the proof from last class to prove*

Theorem (Theorem 3.2)**.** *Let m and n be positive integers where $(m, n) = 1$. Then $\phi(mn) = \phi(m)\phi(n)$.*

Proof *Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to ______ and ______.*

We can partition the positive integers less that or equal to mn into

$$\begin{aligned} 1 &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \\ 2 &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \\ &\vdots \\ m &\equiv \underline{\qquad} \equiv \underline{\qquad} \equiv \cdots \equiv \underline{\qquad} \pmod{m} \end{aligned}$$

For any b in the range $1, 2, 3, \ldots, m$, define s_b to be the number of integers a in the range $1, 2, \ldots, mn$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. Thus, when $(b, m) = 1$, $s_b = \phi(\underline{\qquad})$ and when $(b, m) > 1$, $s_b = \underline{\qquad}$.

We have seen that $\phi(mn) = s_1 + s_2 + \cdots + s_m$, that when $(b, m) = 1$, $s_b =$ ______,[1] *and that when $(b, m) > 1$, $s_b =$ ______. Since there are $\phi(\underline{\qquad})$ integers b where $(b, m) = 1$. Thus, we can say that $\phi(mn) =$ ____________.* ■

Problem 2 *Complete the proof of Theorem 3.2 by proving*

Proposition 1. *If m, n, and i are positive integers with $(m, n) = (m, i) = 1$, then the integers*

$$i, m + i, 2m + i, \ldots, (n - 1)m + i$$

form a complete system of residues modulo n.

[1] This blank is asking for a function, not a value.