Your Name: ____________ Group Members:____________ ____________

Problem 1 *Let p, q be distinct primes. Prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.*

Proof *Let p, q be distinct primes. Then* ____________ $\pmod{p}$ *and* ____________ $\pmod{q}$ *by Fermat's Little Theorem, and* ____________ $\equiv 0 \pmod{p}$ *and* ____________ $\equiv 0 \pmod{q}$ *by* ____________.

∎

Problem 2 *Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) =$ ______ and $\phi(5) =$ ______, so we will prove $\phi(20) =$ ______.*

(a) *A number a is relatively prime to 20 if and only if a is relatively prime to ______ and ______.*

(b) *We can partition the positive integers less that or equal to 20 into*

$$\begin{aligned} 1 &\equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \pmod{4} \\ 2 &\equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \pmod{4} \\ 3 &\equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \pmod{4} \\ 4 &\equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \equiv \_\_\_ \pmod{4} \end{aligned}$$

For any b in the range $1, 2, 3, 4$, define s_b to be the number of integers a in the range $1, 2, \ldots, 20$ such that $a \equiv b \pmod{4}$ and $\gcd(a, 20) = 1$. Thus, $s_1 =$ ______, $s_2 =$ ______, $s_3 =$ ______, and $s_4 =$ ______.

We can see that when $(b, 4) = 1$, $s_b = \phi($______$)$ and when $(b, 4) > 1$, $s_b =$ ______.

(c) *$\phi(20) = s_1 + s_2 + s_3 + s_4$. Why?*

(d) *We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b =$ ______,* [1] *and that when $(b, 4) > 1$, $s_b =$ ______. To finish the "proof" we show that there are $\phi($______$)$ integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) =$ ____________.*

Problem 3 *Repeat the same proof for m and n where $(m, n) = 1$.*

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