MATH 3540 **Name:** ____________________

Homework 5

Directions

1. Complete two out of three questions from 1-3 then complete problems 4 and 5.

---

1. Let $\phi(n)$ be the Euler phi function.

   (a) Let p be a prime and $e \geq 1$ an integer. Show that

   $$\phi(p^e) = p^{e-1}(p-1).$$

   (b) Let p, q be relatively prime. Show that $\phi(pq) = \phi(p)\phi(q)$.

   (c) Let $N = \Pi_i p_i^{e_i}$, where the $\{p_i\}$ are distinct primes and $e_i \geq 1$. Show $\phi(N) = \Pi_i p_i^{e_i-1}(p_i - 1)$

2. Let $N = pq$ where p and q are relatively prime. Show that

$$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$

.

3. In class we showed the following corollary:

   Take $N > 1$ and $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \mod N$.

   This implies that if $N = pq$ where p, q are relatively prime and $ed = 1 \mod \phi(N)$ then for any $x \in \mathbb{Z}_N^*$ we have $(x^e)^d = x \mod N$. Show that this holds for all $x \in \mathbb{Z}_N$. (Hint: use the Chinese Remainder Theorem)

4. What is the order of $\mathbb{Z}_{806}^*$?

5. Given that 5 is an element of $\mathbb{Z}_{79}^*$, compute $[5^{120} \mod \phi(79)]$.