- **Use of unfair means will be severely penalized.**

There are 3 questions for a total of 50 points.

---

(10) 1. Let $N = p \cdot q$ for primes p and q. Let $e, d \in \mathbb{Z}^*_{\phi(N)}$ such that $e \cdot d \equiv 1 \ (mod\ \phi(N))$, where $\phi(N) = (p-1) \cdot (q-1)$. In the lectures, we have seen that $\forall M \in \mathbb{Z}^*_N, (M^e)^d \equiv M \ (mod\ N)$. Show that this holds for all $M \in \mathbb{Z}_N$.

(20) 2. Alice wants to communicate a large integer N to Bob over a lossy channel. Over this channel, Alice can send packets of information each containing an integer. However, there is 10% chance that this packet is going to get *dropped* (that is, Bob does not receive the packet) in transit. One solution is to send multiple packets each containing N. The communication overhead (the total number of *digits* communicated across all packets) in this case might be large. Can you think of a way to reduce the communication overhead using the Chinese Remaindering Theorem? Discuss.
(Note that this is a subjective question. So, the more insight you give, the more points you will get.)

(20) 3. We will use the following definition of cyclic groups.

Definition 1 (Cyclic group)**.** *Let G be a group and let a be any element of this group. Let $< a >= \{x \in G | x = a^n$ for some $n \in \mathbb{Z}\}$. The group G is called a cyclic group if there exists an element $a \in G$ such that $G =< a >$. In this case, a is called the generator of G.*

Show that for any prime p, Z^*_p is a cyclic group.