Homework 2*

Problem 1 (20 points) Find an x that satisfies the following linear congruences:

$$\begin{aligned} x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7 \\ x &\equiv 8 \mod 11 \end{aligned}$$

Problem 2 (15 points) Discuss some useful applications of the Chinese Remainder Theorem.

Problem 3 (15 points) Under the RSA encryption scheme, suppose $p = 89$ and $q = 113$.

- Let $e = 17$, show how to derive the private key d.
- Given $m = 65$, compute the encryption of m and verify the encryption is correct by decrypting the encrypted value.

Problem 4 (15 points) Show that for any integer $n > 1$ and for any $a \in Z_n^*$, the function $f_a : Z_n^* \to Z_n^*$ defined by $f_a(x) = ax \mod n$ is a permutation of Z_n^*.

Problem 5 (15 points) Show that if p is a prime and e is a positive integer, then $\phi(p^e) = p^{e-1}(p-1)$.

Problem 6 (20 points) Suppose Z_n^* contains all positive integers that are less than n and relatively prime to n. Prove that Z_n^* is a group where the group operation is multiplication modulo n.

*Your solutions must be typed, and to receive full credits, please show detailed steps/calculations. If you only show the final results, no credits will be given regardless the correctness of the results.