Sample Assignment #3: Chinese Remainder Theorem (Simplified Version)

All the questions in this assignment will help you answer the following problem:

Problem: Given two relatively prime integers m_1 and m_2 and an integer X, let $M = m_1m_2$ and $1 \leq X \leq m$. Prove that the function $f(X) = (X \bmod m_1, X \bmod m_2)$ is one-to-one.

Problem #1: Consider taking each of the integers from 1 to 15 and writing the remainders when you divide by 3 and 5. For each integer, i, let a_i be the remainder of when i is divided by 3 and let b_i be the remainder when i is divided by 5. List the ordered pairs (a_i, b_i) for all integers i, $1 \leq i \leq 15$.

Problem #2: What do you notice about each of the 15 ordered pairs?

Problem #3: Do you think it's possible, given the ordered pair, to determine the original integer that created that ordered pair? Why or why not?

Problem #4: Try the same exercise for each of the integers from 1 to 20, viewing the remainders when you divide by 4 and 5.

Problem #5: Try the same exercise for each of the integers from 1 to 24, viewing the remainders when you divide by 4 and 6.

Problem #6: What is different in the outcome of the ordered pairs from question #5 as compared to questions #1 and #4?

Problem #7: In question #1, we made a statement about an integer that was the product of two prime numbers, 3 and 5. Based on your observation in #2, conjecture a general statement that relates to the result illustrated by your answer to question #1.

Problem #8: Using the information in questions #1 through #7, prove the original assertion. Use the hints below to construct your proof.

> **Hint a:** Use proof by contradiction. State the beginning assumption that needs to be made to prove this problem using proof by contradiction.
>
> **Hint b:** Show what conclusion is reached with respect to divisibility of a particular quantity by m_1 and m_2.
>
> **Hint c:** Show what subsequent conclusion is reached with respect to divisibility of the previous quantity by M.
>
> **Hint d:** At this point, what piece of original information has been contradicted.

Question #9: Do some background research in cryptography to find at least one application that is related to the Chinese Remainder Theorem.

Question #10: How would you relate this result to a non-mathematics student? Do not use any mathematical symbols or specific terminology.