Problem 1 Show that multiplicative inverses modulo m are not unique integers by finding two integers a, b such that $2a \equiv_5 1$ and $2b \equiv_5 1$.

Problem 2 Show that multiplicative inverses modulo m do not always exist by showing that 2 has no inverse modulo 4. More specifically, show that $2x \not\equiv_4 1$ for any x by separately considering when x is even and when x is odd.

Problem 3 Solve for x in the congruence $6x \equiv_{17} 8$

Problem 4 Julius Caesar is documented as one of the earliest known users of cryptography. Caesar's cipher (encryption process) worked like this: assign every letter of the alphabet to an integer in the set $\{0, \cdots, 25\}$ (so $A \to 0, B \to 1$, etc). Then, pass each letter through the function:

$$f(p) = (p + 3) \mod 26.$$

This kind of cipher is called a *shift cipher*. To decrypt a message, the inverse function could be applied:

$$f^{-1}(p) = (p - 3) \mod 26.$$

Decrypt this message: **PHHW BRX LQ WKH SDUN**

Problem 5 You've intercepted an enemy message encrypted with a shift cipher ($f(p) = p + k \mod 26$), but you don't know what the shift k is! However, you know that the original message was written in English, and E is the most common letter in the English language. Can you decrypt this message? **ZNK KGXRE HOXJ MKZY ZNK CUXS**

Problem 6 In this problem, we'll prove that every positive integer can be represented as a binary number. That is, using induction (or strong induction), prove that every positive integer $n \geq 1$ can be written as a sum of distinct powers of 2.

For example, $5 = 2^2 + 2^0, 11 = 2^3 + 2^1 + 2^0$, $16 = 2^4$. By *distinct*, we mean that no power of 2 occurs more than once (so we write $3 = 2^1 + 2^0$, not $3 = 2^0 + 2^0 + 2^0$).

Hint: In the inductive step, separately consider when $k + 1$ is even and when $k + 1$ is odd.