Problem 1 Practice with modular arithmetic

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

We show that both 3 and 8 are inverses of 2 modulo 5:

$$2 \cdot 3 \equiv_5 1$$

$$2 \cdot 8 \equiv_5 1$$

(b) Show that multiplicative inverses modulo m do not necessarily 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.

First we consider the case where x is even, so $x = 2k$ for some $k \in \mathbb{Z}$. Then we have:

$$2x \equiv_4 2 \cdot 2k \equiv_4= 4k \equiv_4 0.$$

Next we consider the case where x is odd, so $x = 2k + 1$ for some $k \in \mathbb{Z}$. Then we have:

$$2x \equiv_4 2(2k + 1) \equiv_4 4k + 2 \equiv_4 2.$$

Therefore any $2x$ is congruent modulo 4 to 0 or 2, and $2x \not\equiv_4 1$ for every integer x.

(c) Solve for x in the congruence $6x \equiv_{17} 8$

To solve this, we first need to find an inverse of 6 modulo 17. We note that 3 is such an inverse: $3 \cdot 6 \equiv_{17} 1$. So we have

$$6x \equiv_{17} 8$$

$$3 \cdot 6x \equiv_{17} 3 \cdot 8$$

$$x \equiv_{17} 24.$$

Therefore $x = 24$ is a solution (as is $x = 7$, and any $x = 7 + 17k$ for $k \in \mathbb{Z}$.).

Problem 2 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**

Shifting each letter back 3 places, we get: MEET YOU IN THE PARK.

Problem 3 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**

Since K is the most common letter in this message, we try shifting E to K (a shift of +6), resulting in: THE EARLY BIRD GETS THE WORM.

Problem 4 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.

We will prove this by strong induction on n.

For our base case, we have $n = 1$. Note that $1 = 2^0$, so our base case holds.

Next, for our inductive step, let $k \in \mathbb{N}$ be arbitrary with $k \geq 1$ and assume that all x where $1 \leq x \leq k$ can be written as a sum of distinct powers of 2. We will show that $k+1$ can be written as a sum of distinct powers of 2.

We consider two cases:

- If $k+1$ is even, then $k+1 = 2m$ for some $m \in \mathbb{N}$, $m \geq 1$. Note that $m < k+1$ and therefore, by our inductive hypothesis, m can be written as a sum of distinct powers of 2. Note that, for any sum of an arbitrary number of powers of 2 represented by $x = 2^a + 2^b + \cdots + 2^z$, $2x = 2(2^a + 2^b + \cdots + 2^z) = 2^{a+1} + 2^{b+1} + \cdots + 2^{z+1}$. Therefore multiplying m by 2 simply increments every exponent by 1, producing another sum of distinct powers of 2. Therefore $2m = k+1$ can be written as a sum of distinct powers of two.
- If $k+1$ is odd, then $k+1 = 2m+1$ for some $m \in \mathbb{N}$, $m \geq 1$. Note that $2m < k+1$, so $2m$ can be written as a sum of distinct powers of 2. Note also that the only power of 2 that is an odd number is $2^0 = 1$, since every other power of 2 has a factor of 2. Since $2m$ is even, $2m$ does not contain 2^0 in its representation as a sum of distinct powers of 2. Therefore $2m + 2^0$ is a sum of distinct powers of 2 and $2m + 2^0 = 2m + 1 = k + 1$, so $k+1$ can be written as a sum of distinct powers of 2.

Therefore every positive integer can be written as a sum of distinct powers of 2.