CSCI-4116
Assignment 1

Anas Alhadi

B00895875

January 15, 2025

I have read and understood the posted assignment instructions
Anas,

Question 1

- **Key:** 23
- **Plain Text:** HIIAMJULESIWISHYOUAGOODCRYPTOCLASS

Question 2

WEARENOTINTERESTEDINTHEPOSSIBILITIESOFDEFEAT

Question 3

To prove equivalence, we need to show that congruence relations are reflexive, symmetric and transitive.

1. **Reflexivity:** [*by showing that*: $x \equiv x (\text{mod } \mathbb{Z}),\ \forall x \in \mathbb{Z}$]

   Let $x, m \in \mathbb{Z}$. Observe that:

   $$x - x = 0 \quad AND \quad 0 = m \times 0$$
   $$\therefore (x - x) = m \times 0 \quad \therefore \quad m|(x - x)$$

   Thus, $x \equiv x (\text{mod } m),\ \forall x, m \in \mathbb{Z}$

2. **Symmetry:** [*by showing that*: $x \equiv y(\text{mod } m) \implies y \equiv x(\text{mod } m),\ \forall x, y, m \in \mathbb{Z}$]

   Suppose that $x \equiv y(\text{mod } m), \quad x, y, m \in \mathbb{Z}$

   This means that $m|y - x$ (by the definition of congruences) which can be written as:

   $$y - x = m \times k, \qquad k \in \mathbb{Z}$$

   Then by negating both side:

   $$-y + x = m \times k \times -1 = m \times h, \qquad h = -k$$

   It follows then:

   $$x - y = m \times h, \qquad h \in \mathbb{Z}$$
   $$\therefore \quad m|x - y$$
   $$\therefore \quad y \equiv x(\text{mod } m)$$

3. **Transitivity:**

   Suppose that:

   $$x \equiv y(\text{mod } m) \qquad AND \qquad y \equiv z(\text{mod } m), \quad x, y, z, m \in \mathbb{Z}$$

   This means that:

   $$x = y + km \qquad AND \qquad y = z + lm, \quad l, m \in \mathbb{Z}$$

   Subsituting y into x's equation

   $$x = z + lm + km = z + nm, \quad n = l + k$$

   Therefore:

   $$x = z + nm, \quad n \in \mathbb{Z}$$
   $$\therefore \quad m|x - z \quad \therefore \quad x \equiv z(\text{mod } m)$$

Question 4

Given:

$$a \equiv b(\text{mod } m) \qquad AND \qquad c \equiv d(\text{mod } m)$$

We have it that:

$$a = b + km \qquad AND \qquad c = d + hm, \quad k, h \in \mathbb{Z} \tag{1}$$

Propositions:

(b) $a + c \equiv b + d(\text{mod } m)$

proof:

Summing the two equations in (1)

$$a + c = b + km + d + hm$$

$$(a + c) = (b + d) + lm, \quad l = k + h$$

This means that

$$m|(b + d) - (a + c)$$

$$\therefore \quad (a + c) \equiv (b + d)(\text{mod } m)$$

Which is equivalent to

$$(a + c) \equiv b + d(\text{mod } m)$$

(c) $a \times c \equiv b \times d(\text{mod } m)$

proof:

Repeating the steps in (b) but this time multiplying the 2 equations in (1)

$$a \times c = (b + km)(d + hm)$$

$$ac = bd + m(bh + dk + khm)$$

$$ac = bd + mn, \qquad n = bh + dk + khm$$

Thus:

$$m|\ bd - ac \qquad \therefore \qquad ac \equiv bd(\text{mod } m)$$

Question 5

(a) -44 , -27 , -10 , 7 , 24 , 41

(b) {0 , 18 , 36 , 3 , 21 , 39 , 6 , 24 , 42 , 9 , 27 , 45 , 12 , 30 , 48 , 15 , 33 }

(c) Since 7 and 10 are relativley prime, we can use the CRT to solve the system of congrences for x. Which should give us a congruence $x(\text{mod } 7 * 10)$ that is equivalent to the two congruences:

(1) $x \equiv 2(\text{mod } 7)$

(2) $x \equiv 3(\text{mod } 10)$

We can write **(2)** as $x = 10k + 3,\ k \in \mathbb{Z}$. Then subsituting **(2)** into **(1)**

$$10k + 3 \equiv 2(\text{mod } 7)$$
$$10k \equiv -1(\text{mod } 7)$$
$$10k \equiv 6(\text{mod } 7)$$

We now reduce both sides of the equation by (mod 7). (since 10 is not in the alphabet of modulo 7)

$$10k(\text{mod } 7) \equiv 6(\text{mod } 7)(\text{mod } 7)$$
$$3k \equiv 6(\text{mod } 7)$$

To find k we need to find a multiplicative inverse of 3 in modulo 7. (Such that $3 * 3^{-1} \equiv 1(\text{mod } 7)$). Observe that $3 * 5 \equiv 1(\text{mod } 7)$. Thus 5 is a multiplicitve inverse [1].

Multiplying both sides by 5:

$$k \equiv 30(\text{mod } 7) \equiv 2(\text{mod } 7)$$

So:

$$k = 7h + 2,\ h \in \mathbb{Z}$$

Finally, subsituting the above equation into **(2)**

$$x = 10k + 3$$
$$x = (7h + 2) * 10 + 3$$
$$x = 70h + 23,\ h \in \mathbb{Z}$$

Thus:

$$x \equiv 23(\text{mod } 70)$$

[1] We can use the Extended Euclidian Algorithm to find the inverse (which i did initially but didn't want to write all the steps)

Question 6

Plain text:

all legistation, all government, all society is founded upon the principle of mutual concession, politeness, comity, courtesy.

Explaination:

The reason that this cipher is relatively easy to solve is:

1. it does not obfuscate any of the possibly unique charactaristics of the plain text. We can easily identify letters (ex: all “e” s have a unique encoding that doesnt change regardless of the context that the letter occurs in) thus we can use frequency analysis.
2. The cipher also maintains the length of the words (white space and punctuations are not encrypted) which reduces the search space as each word can be decrypted seperately

This means that an encrypted section, say, GWW is now restricted to only $28C3$ combinations of letters(by point 2), which can be further reduced by only considering combinations where the 2^{nd} and 3^{rd} letters are the same (by point 1). Finally since only words are encrypted, this reduces the search space to only english words which fit that category (assuming no spelling errors)