

CSCI-4116

Assignment 1

Anas Alhadi

B00895875

January 24, 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: $x \equiv x \pmod{\mathbb{Z}}, \forall x \in \mathbb{Z}$]

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

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

Thus, $x \equiv x \pmod{m}, \forall x, m \in \mathbb{Z}$

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

Suppose that $x \equiv y \pmod{m}$, $x, y, m \in \mathbb{Z}$

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

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

Then by negating both side:

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

It follows then:

$$x - y = m \times h, \quad h \in \mathbb{Z}$$

$$\therefore m|x - y$$

$$\therefore y \equiv x \pmod{m}$$

3. **Transitivity:**

Suppose that:

$$x \equiv y \pmod{m} \quad \text{AND} \quad y \equiv z \pmod{m}, \quad x, y, z, m \in \mathbb{Z}$$

This means that:

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

Substituting y into x 's equation

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

Therefore:

$$x = z + nm, \quad n \in \mathbb{Z}$$

$$\therefore m|x - z \quad \therefore x \equiv z \pmod{m}$$

Question 4

Given:

$$a \equiv b \pmod{m} \quad \text{AND} \quad c \equiv d \pmod{m}$$

We have it that:

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

Propositions:

$$(b) \quad a + c \equiv b + d \pmod{m}$$

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

$$\begin{aligned} m &| (b + d) - (a + c) \\ \therefore (a + c) &\equiv (b + d) \pmod{m} \end{aligned}$$

Which is equivalent to

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

$$(c) \quad a \times c \equiv b \times d \pmod{m}$$

proof:

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

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

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

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

Thus:

$$m \mid bd - ac \quad \therefore \quad ac \equiv bd \pmod{m}$$

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 relatively prime, we can use the CRT to solve the system of congruences for x . Which should give us a congruence $x(\bmod 7 * 10)$ that is equivalent to the two congruences:

$$(1) x \equiv 2(\bmod 7)$$

$$(2) x \equiv 3(\bmod 10)$$

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

$$10k + 3 \equiv 2(\bmod 7)$$

$$10k \equiv -1(\bmod 7)$$

$$10k \equiv 6(\bmod 7)$$

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

$$10k(\bmod 7) \equiv 6(\bmod 7)(\bmod 7)$$

$$3k \equiv 6(\bmod 7)$$

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

Multiplying both sides by 5:

$$k \equiv 30(\bmod 7) \equiv 2(\bmod 7)$$

So:

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

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

$$x = 10k + 3$$

$$x = (7h + 2) * 10 + 3$$

$$x = 70h + 23, h \in \mathbb{Z}$$

Thus:

$$x \equiv 23(\bmod 70)$$

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

Question 6

Plain text:

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

Explanation:

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

1. it does not obfuscate any of the possibly unique characteristics of the plain text. We can easily identify letters (ex: all "e" s have a unique encoding that doesn't 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 separately

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 2nd and 3rd 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)

Bonus acknowledgment: English is not my native language