All questions worth 5 points

#1. Let R be the Congruence Modulo m relation on the integers:
\[ R = \{ (a,b) \mid a = b \pmod{m}; \text{that is, } m \mid (a - b) \text{ for some positive integer } m \}. \]

a) If \( m = 5 \), is \( 2 \sim -3 \)?

Does \( 5 \mid 2 - (-3) \)? I.e., does \( 5 \mid 5 \)? Yes

b) For \( m = 5 \), is \(-3 \sim 2\)?

Does \( 5 \mid -3 - 2 \)? I.e., does \( 5 \mid -5 \)? Yes

c) Show the equivalence classes of R for \( m = 5 \).

\[ [0] = \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\} \]
\[ [1] = \{\ldots, -11, -6, 1, 6, 11, 16, \ldots\} \]
\[ [2] = \{\ldots, -12, -7, 2, 7, 12, 17, \ldots\} \]
\[ [3] = \{\ldots, -13, -8, 3, 8, 13, 18, \ldots\} \]
\[ [4] = \{\ldots, -14, -9, 4, 9, 14, 19, \ldots\} \]

#2. Show that Congruence Modulo m is an equivalence relation.

**Reflexive**

a R a because \( m \mid (a - a) \), i.e., \( m \mid 0 \)

**Symmetric**

If aRb, then \( m \mid (a-b) \), so \( a \mid -(a-b) \) or \( a \mid (b-a) \)

**Transitive**

If aRb, then \( m \mid (a-b) \) or we can write \( (a - b) = km \), some k
If bRc, then \( m \mid (b-c) \) or we can write \( (b - c) = lm \), some l

Adding these we get \( (a - c) = (k+l)m \), \( m \mid (a-c) \)
#3.  a) Show that $55 + 26 = (3 + 2) \pmod 4$

a) $55 + 26 = 81; 3 + 2 = 5$ so we need to show that $81 = 5 \pmod 4$
or that $4 \mid (81 - 5)$ or $4 \mid 76$ which is true ($76 = 4 \times 19$)

b) Evaluate $-17 \pmod 2$

$-17 = 2(-9) + 1$ so $-17 \pmod 2 = 1$

c) Evaluate $144 \pmod 7$

$144 = 7 \times 20 + 4$ so $144 \pmod 7 = 4$

#4. a) What is the secret message produced from the message “HOW ARE YOU” using the Caesar cipher$^1$?

The numeric equivalents are: 8 15 23 1 18 5 25 15 21
Adding 3 (mod 26): 11 18 26 4 21 8 2 18 24
Converting back to letters: KRZ DUH BRX

b) Use the Caesar cipher to decrypt the message L DP ILQH

Converting to numbers: 12 4 16 9 12 17 8
Subtracting 3 (mod 26) 9 1 13 6 9 14 5
Converting back to letters: I AM FINE

#4. a) Encrypt I LOVE YOU using the function $f(p) = (7p + 3) \pmod 26$

I: $7 \times 9 + 3 = 66$ and $66 \pmod 26 = 14 \rightarrow N$
L: $7 \times 12 + 3 = 87$ and $87 \pmod 26 = 9 \rightarrow L$
O: $7 \times 15 + 3 = 108$ and $108 \pmod 26 = 4 \rightarrow D$
V: $7 \times 22 + 3 = 157$ and $157 \pmod 26 = 1 \rightarrow A$
E: $7 \times 5 + 3 = 38$ and $38 \pmod 26 = 12 \rightarrow L$
Y: $7 \times 25 + 3 = 178$ and $178 \pmod 26 = 22 \rightarrow V$
O: $7 \times 15 + 3 = 108$ and $108 \pmod 26 = 4 \rightarrow D$
U: $7 \times 21 + 3 = 150$ and $150 \pmod 26 = 20 \rightarrow T$

So the encrypted message is: N IDAL VDT

---

$^1$ Caesar’s encryption: replace every letter by an integer from 1 to 26; a is 1, b is 2 etc.; Then apply the function $f(p) = (p + 3) \pmod 26$ and convert the numbers back to the appropriate letter. Thus “j” is converted to 10, then to 13 and back to “M”. ($f^1(p) = (p - k) \pmod 26$)
#5. Books are identified by an International Standard Book Number (ISBN), a 10-digit code, $x_1, x_2, \ldots x_{10}$, assigned by the publisher. These 10 digits consist of blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, 1 1-digit check digit that is either a digit or the letter X (representing 10). This digit is selected so that

$$\sum_{i=1}^{10} i x_i = 0 \pmod{11}$$

and is used to detect errors in individual digits and transposition of digits. If the ISBN of a book is 0-201-57Q89-1, where Q is a digit, find Q.

$$1*0 + 2*2 + 3*0 + 4*1 + 5*5 + 6*7 + 7*Q + 8*8 + 9*9 + 10*1 = 0 \pmod{11}$$

That is, $230 + 7Q = 0 \pmod{11}$

Subtracting 230 from both sides

$7Q = 1 \pmod{11}$ because $231 = 11*21$

Trial and error gives $Q = 8$ (because 56 = 1 (mod 11))

(look at $[1] = \{\ldots 1, 12, 23, 34, 45, 56, \ldots\}$ and note that 56 is the first multiple of 7)

#7. Section 8.1, #2. Consider the following influence graph (example 3 in the text).

a) Identify the set of vertices and edges:

**Vertices:**

{Linda, Brian, Deborah, Fred, Yvonne}

**Edges:**

(Deborah, Linda)
(Deborah, Fred)
(Deborah, Brian)
(Fred, Brian)
(Brian, Linda)
(Brian, Yvonne)
(Yvonne, Brian)

b) Who influences Fred and who can Fred influence?

Fred is influenced by Deborah and Yvonne
Fred influences Brian

#8. Draw a graph with the specified properties or explain why no such graph can exist

a) Graph with five vertices of degrees 1, 2, 3, 3, and 5

Here’s one:

b) Graph with four vertices of degrees 1, 2, 3 and 3

Not possible