Math 1111 Fall 2019 – Problem Set 1

1. Decipher the following message *and* identify the method used to construct the cipher alphabet. You should assume it was enciphered using a monoalphabetic substitution cipher.

UZ GOEOYHOI OUDBKOOZ KBUIKR-ZUZO, CAO UJJMOG T EBTXXOZDO KA KBO IOTGOIJ AL KBO

CBUXTGOXCBUT CTCOI TXOQTZGOI'J POOWXR KBTK BO EAMXG JAXNO TZR JUYCXO

JMHJKUKMKUAZ EUCBOI KBOR JMHYUKKOG. BO CIAEOOGOG KA JAXNO TXX AL KBOY,

UZEXMGUZD AZO UZ PBUEB JONOZ GULLOIOZK TXCBTHOKJ POIO MJOG.

2. In a paragraph or two, describe the strategies you used to decipher the message above. How did you start figuring out the cipher alphabet? What patterns in the cipher alphabet did you notice that led you to determine the particular substitution cipher used? What other steps did you take as part of your cryptanalysis?

3. Fill in the blanks in the following table. Some of the blanks can be filled in using more than one number, but the rows of your table should be internally consistent.

x	x MOD 4	x MOD 7	x MOD 12
10			
-15			
	1	3	
	3		11
	1	1	1

4. Find five numbers (three positive, two negative) that, when substituted in the following congruence statement for x, make the statement true.

   $x + 9 \equiv 7 \pmod 8$

5. Which of the following pairs of numbers are relatively prime? *Justify your answers.*
   a. 45 and 54
   b. 64 and 81
   c. 105 and 122
   d. 1155 and 1729

6. The 30-letter Coptic alphabet is a variant of the Greek alphabet developed when Greece conquered Egypt in the 3rd century BC. It consists of all 24 letters of the Greek alphabet, as well as six addition letters representing sounds not used in Greek. How many unique decimation ciphers are there for the Coptic alphabet? *Justify your answer.*

7. Consider the substitution cipher $y = (5x + 4) \text{ MOD } 26$, where x is an integer between 0 and 25 representing a letter in the plaintext and y is an integer between 0 and 25 representing the corresponding letter in the ciphertext. (Here, 0 = A, 1 = B, 2 = C, …, 25 = Z.) Encipher the plaintext "privacy" using this cipher.

8. The least common multiple of two integers a and b, denoted LCM(a, b), is the smallest positive integer that is divisible by both a and b.
    a. Find LCM(15, 20).
    b. Find LCM(10, 32).
    c. Find LCM(37, 47).
    d. Suppose that the positive integers m and n are relatively prime. Find a formula for LCM(m, n) in terms of m and n. (You don't need to prove your formula—that's a much harder task than making a good conjecture here.)