

COMP 170 Discrete Mathematical Tools for CS
2005 Fall Semester – Written Assignment # 4
Distributed: Sept 23, 2005 – Due: Sept 29, 2005 at end of class

The top of your submission should contain (i) your name, (ii) your student ID #, (iii) your email address and (iv) your tutorial section.

Please write clearly and briefly. For all questions you should also provide a short explanation as to *how* you derived the solution. A solution that consists of just a number will be counted as wrong.

2nd Note: Please follow the guidelines on doing your own work and avoiding plagiarism given on the class home page. Don't forget to *acknowledge* individuals who assisted you, or sources where you found solutions.

3rd Note: Some of these problems are taken (some modified) from section 2.1 of the textbook

Problem 1: What is $38 \bmod 11$? What is $-1 \bmod 11$? What is $-17 \bmod 11$? When answering these questions please also give the associated values q and r in the representation $m = qn + r$.

Problem 2: Encrypt the message MADAM IM ADAM using a Caesar cipher in which each letter is shifted five places to the left.

Problem 3: A Caesar cipher with shift k letters to the right has been executed on some original plaintext message. The resulting ciphertext is XNQD RJXXFLJ. What is k and what was the original message?

Problem 4: In our class discussion of we showed that 0, 3, 6, and 9 are all solutions to the equation

$$4 \cdot_{12} x = 0.$$

Are there any integral values of a and b , with $1 \leq a < 12$ and $1 \leq b < 12$ for which the equation $a \cdot_{12} x = b$ does *not* have any solutions in Z_{12} ? If there are, give one set of values for a and b and explain how you know that there are no solutions to $a \cdot_{12} x = b$. If there are not, explain how you know this. (You could write out the entire Z_{12} multiplication table to justify your answer, but this is not necessary)

Problem 5: (a) Write the \cdot_9 multiplication table for Z_9 .

(b) Which non-zero elements in Z_9 have a multiplicative inverse? Which do not?

Problem 6: (a) Write the \cdot_7 multiplication table for Z_7 .

(b) Which non-zero elements in Z_7 have a multiplicative inverse? Which do not?