

COMP 2711 Discrete Mathematical Tools for CS
2014 Fall Semester – Solution to Written Assignment # 5
Distributed: Oct 22, 2014 – Due: Oct 29, 2014

Problem 1: What is $37 \bmod 17$? What is $-4 \bmod 17$? What is $-37 \bmod 17$? When answering these questions please also give the associated values q and r in the representation $m = qn + r$.

Problem 2: Encrypt the message **COMPUTER SCIENCE** using a Caesar cipher in which each letter is shifted four places to the left.

Problem 3: A Caesar cipher with shift k letters (to the left or to the right) has been executed on some original plaintext message. The resulting ciphertext is **SZH SLCO HLD ESTD EZ OPNZOP**. What is k and what was the original message?

Problem 4: It is easy to see that 0, 5, 10, and 15 are all solutions to the equation

$$4 \cdot_{20} x = 0.$$

Are there any integral values of a and b , with $1 \leq a < 20$ and $1 \leq b < 20$, for which the equation $a \cdot_{20} x = b$ does *not* have any solutions in Z_{20} ? If there are, give one set of values for a and b and explain how you know that there are no solutions to $a \cdot_{20} x = b$. If there are not, explain how you know this. (You could write out the entire Z_{20} 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: Does there exist an x in Z_{147} that solves

$$12 \cdot_{147} x = 7?$$

If yes, give the value of x (it is not necessary to show your work).

If no, prove that such an x does not exist.

Problem 7: (Challenge Problem) (a) Two integers x and y are said to be *congruent modulo n* , ($n > 1$) if and only if

$$(x \bmod n) = (y \bmod n).$$

When this is the case, we write $x \equiv y \pmod{n}$. Suppose that

$$x \equiv y \pmod{n} \quad \text{and} \quad a \equiv b \pmod{n}.$$

Prove that

$$ax \equiv by \pmod{n}.$$

(b) Prove that for every integer n ,

$$n^5 \equiv n^3 \pmod{8}.$$