CS 171
Homework Assignment 14t

Given: April 24, 2012 **Due:** April 26, 2012

This assignment is due by the end of the class on the due date. Unless all problems carry equal weight, the point value of each problem is shown in [ ]. To receive full credit all your answers should be carefully justified. Each solution must be the student's own work. Assistance should be sought or accepted only from the course staff. Any violation of this rule will be dealt with harshly.

---

1. Calculate

A. $3 + 3$ (mod 10).

B. $6 + 6$ (mod 10).

C. $7 + 3$ (mod 10).

D. $9 + 8$ (mod 10).

E. $12 - 4$ (mod 10).

F. 4×4 (mod 10).

G. 4×1 (mod 10).

H. $8 - 5$ (mod 10).

I. $5 - 8$ (mod 10).

J. $8/7$ (mod 10).

2. Let n be a positive integer and suppose $a, c \in \{0, 1, \ldots, n-1\}$, are both invertible. Prove or disprove each of the following statements, where the operations and inverses are in mod n arithmetic:

A. $a + b$ is invertible.

B. $a - b$ is invertible.

C. $a \times b$ is invertible.

D. a/b is invertible.

3. Let n be an integer ith $n \geq 2$, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Prove that the element $n - 1$ is its own inverse mod n.

4. Consider the following cipher called the *Caesar cipher* in which given a message in English, each letter is substituted by another letter $k \mod 26$ spaces after it in the alphabet. So, for example, for $k = 3$, the message ABC will be replaced by DEF. What is the secret key here? How would you break such a system, that is reveal the secret key? What is the time complexity of this attack for the brute-force case? Can you do better than brute-force?