**COMP 170 Discrete Mathematical Tools for CS**
**2007 Fall Semester – Written Assignment # 4**
**Distributed: Sept 27, 2007 – Due: Oct 4, 2007**

At the top of your solution, please write your (i) name, (ii) student ID #, (iii) email address and (iv) tutorial section.
Some Notes:

- Please write clearly and briefly. For all questions you should also provide a short explanation as to *how* you derived the solution. That is, if the solution is 20, you shouldn't just write down 20. You need to explain *why* it's 20.
- 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.
- Some of these problems are taken (some modified) from section 2.1 of the textbook.
- Please make a *copy* of your assignment before submitting it. If we can't find your paper in the submission pile, we will ask you to resubmit the copy.
- Your solutions can either be submitted at the end of your Thursday lecture section or, before 5PM, in the collection bin in front of Room 4213A.

**Problem 1:** What is 31 mod 13? What is $-5$ mod 13? What is $-31$ mod 13? 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 `N MFI F AJWD SNHJ IFD YTIFD`. 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:** (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?

**Challenge Problem:** (a) Prove that for every integer $n$,

$$n^3 \bmod 6 = n \bmod 6.$$

(b) Prove that the `GCD` algorithm to find $\gcd(j, k)$ with $j < k$ takes at most $2 \log_2 k$ steps, where a step is one reduction from $\gcd(j, k)$ to $\gcd(r, j)$.