COMP 170 Discrete Mathematical Tools for CS
2007 Fall Semester – Written Assignment # 5
Distributed: Oct 18, 2007 – Due: Oct 25, 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 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: How many solutions with x between 0 and 76 are there to the system of equations

$$\begin{aligned} x \bmod 7 &= 5, \\ x \bmod 11 &= 4? \end{aligned}$$

What are these solutions?

Problem 2: (a) Show that exactly $(p-1)(q-1)$ elements in Z_{pq} have multiplicative inverses when p and q are primes.

(b) $10 = 2 \cdot 5$ and 7 are *relatively* prime. How many elements in Z_{70} have multiplicative inverses?
The number of elements which have multiplicative inverses is *not* $(10-1)(7-1)$. Explain why your reasoning for part (a) doesn't work for $10, 7$. (Do *not* just say that 10 is not prime. Explain why the reasoning for part (a) works when p and q are both prime but is not valid when p and q are relatively prime but not prime.)

Problem 3: Suppose when applying RSA that, $p = 29$, $q = 37$, and $e = 19$.
(a) What are the values of n and d?
(b) Show how to encrypt the message $M = 100$, and then how to decrypt the resulting message. Use *repeated squaring* for the encrypting and decrypting.

Problem 4: Prove the DeMorgan's law that states $\neg(p \wedge q) = \neg p \vee \neg q$.

Problem 5: Which of the following statements (in which Z^+ stands for the positive integers and Z stands for all integers) is true and which is false? Don't forget to explain why.
a) $\forall z \in Z^+ \, (z^2 + 6z + 10 > 20)$
b) $\forall z \in Z \, (z^2 - z \geq 0)$
c) $\exists z \in Z^+ \, (z - z^2 > 0)$
d) $\exists z \in Z \, (z^2 - z = 6)$

Challenge Problem: In Problem 2, you show that if p and q are prime, then there are exactly $(p-1)(q-1)$ elements in Z_{pq} that are relatively prime to $n = pq$. You also show that if p and q are not prime then the number of elements in Z_{pq} relatively prime to $n = pq$ is not necessarily $(p-1)(q-1)$. In this problem, you try to come up with a general formula for the number of elements in n that are relatively prime to n. In both part (a) and part (b) you need to explain *how* you derived your solution.

(a) First assume that $n = p^i$ where p is some prime number. How many elements of Z_n are relatively prime to $n = p^i$? If possible, express your answer in terms of n and p.

(b) Now let n be an arbitrary number. How many elements of Z_n are relatively prime to n. If possible, express your answer in terms of n and $p_1, p_2, \ldots, p_t$, where the p_i are the primes that divide n.