COMP 170 Discrete Mathematical Tools for CS
2008 Fall Semester – Written Assignment # 5
Distributed: October 23, 2008 – Due: Oct 30, 2008
PROBLEM C2(a) REVISED & CORRECTED Oct 24, 2008

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) fromthe 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 should be before 5PM of the due date, in the collection bin in front of Room 4213A (near lift 21)

Problem 1: How many solutions with x between 0 and 76 are there to the system of equations

$$\begin{aligned} x \bmod 7 &= 4, \\ x \bmod 11 &= 10? \end{aligned}$$

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) $\forall z \in Z^+ \, (z^2 + 6z + 10 > 18)$
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 Problems

Problem C1: Consider the following equations:

$$\begin{aligned} x &\mod 3 = 2 \\ x &\mod 5 = 3 \\ x &\mod 11 = 4 \\ x &\mod 16 = 5. \end{aligned}$$

Let $M = 3 \cdot 5 \cdot 11 \cdot 16 = 2640$.
(i) Show that there is an integer x in Z_M that satisfies all of the equations simultaneously and state the value of x.
(ii) Prove that y is unique.

Problem C2: For each of the following two problems, state whether there is an $x \in Z_{150}$ that satisfies the two equations. If no solution x exists, prove it. If x does exist, list *all* solutions and prove that you have found all of them.

Note that 10 and 15 are not relatively prime, so you may not use the Chinese Remainder Theorem to solve the problem directly.

(a) Find *all* solutions for the following system of equations in Z_{150}:

$$\begin{aligned} x &\mod 10 = 2 \\ x &\mod 15 = 4. \end{aligned}$$

(b) Find *all* solutions for the following system of equations in Z_{150}:

$$\begin{aligned} x &\mod 10 = 9 \\ x &\mod 15 = 4. \end{aligned}$$