**COMP 2711 Discrete Mathematical Tools for CS**
**2014 Fall Semester – Solution to Written Assignment # 6**
**Distributed: Nov 5, 2014 – Due: Nov 12, 2014**

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 be submitted before 5PM of the due date, in the collection bin in front of Room 4213A.

**Problem 1:** Does there exist an $x$ in $Z_{79}$ that solves

$$53 \cdot_{79} x = 1?$$

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 2:** Consider the system of equations

$$\begin{aligned} x \bmod 13 &= 5, \\ x \bmod 11 &= 9. \end{aligned}$$

(a) How many solutions with $x$ between 0 and 142 are there to the system of equations. What are these solutions?

(b) How many solutions with $x$ between 143 and 428 are there to the system of equations. What are these solutions?

(c) How many solutions with $x$ between 143 and 470 are there to the system of equations. What are these solutions?

**Problem 3:** (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 4:** 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 5:** Compute each of the following. Show or explain your work. Do *not* use a calculator or computer.

1. $15^{96} \bmod 97$.
2. $67^{72} \bmod 73$.
3. $67^{73} \bmod 73$.

**Problem 6:** **(Challenge Problem)** 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 $x$ is unique.

**Problem 7:** **(Challenge Problem)** 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 $Z_{150}$:

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