COMP 170 Discrete Mathematical Tools for CS
2006 Fall Semester – Written Assignment # 5
Distributed: Oct 17, 2006 – Due: Oct 24, 2006 *at end of class*

The top of your submission should contain (i) your name, (ii) your student ID #, (ii) your email address and (iv) your tutorial section.

Please write clearly and briefly. For all questions you should also provide a short explanation as to *how* you derived the solution. A solution that consists of just a number will be counted as wrong.

2nd Note: 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.

3rd Note: Most of these problems are taken (some modified) from sections 2.3 and 2.4 of the textbook.

4th Note: Your assignment can either be submitted at the end of your Tuesday lecture session or before 5PM in the collection bin in front of room 4213A.

Problem 1: The numbers 29 and 43 are primes. What is $(29-1)(43-1)$? What is $199 \cdot 1111$ in Z_{1176}? What is $(23^{1111})^{199}$ in Z_{29}? In Z_{43}? In Z_{1247}?

Problem 2: How many solutions with x between 0 and 76 are there to the system of equations

$$\begin{aligned} x \bmod 7 &= 3, \\ x \bmod 11 &= 4? \end{aligned}$$

What are these solutions?

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

1. 15^{96} in Z_{97}.
2. 67^{72} in Z_{73}.
3. 67^{73} in Z_{73}.

Problem 4: (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 5: Suppose for applying RSA, $p = 29$, $q = 37$, and $e = 19$.
(a) What are the values of n and d?
(b) Show how to encrypt the message $M = 100$, and then show how to decrypt the resulting message.

Challenge Problem: In Problem 4, 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.