CS 235
Spring 2010

Assignment 6

Date Due: Thursday, April 8 at 5:00

Reading: Chapter 11, page 239-252 Chapter 12, pages 253-260

Problems:

1. Page 177, problem 20

2. Page 178, problem 26

3. Page 178, problem 31

4. Show that for p prime, (p - 1)! = -1 (mod p).

   Hint: The first part of your proof should argue that 1 and p - 1 are the only values mod p that are their own inverses. In showing that, the polynomial x^2 - 1 = 0 (mod p) is important.

5. Is the converse of the previous problem true ?

   That is, for m > 2, if (m-1)! = -1 (mod m) then m is prime.

   If it is true prove it, otherwise give a counterexample.

6. Page 181, problem 50.

7. Prove that if p is prime then for any $e > 0$ $\phi(p^e) = p^{e-1}(p-1)$.