CSI 2101 Discrete Structures | Winter 2010
Prof. Lucia Moura | University of Ottawa

Homework Assignment #2 (100 points, weight 6.25%)
Due: March 8 at 10:00a.m. (in tutorial)

Number Theory

1. (16 points) Exercise 14, page 218 (perfect numbers).
2. (16 points)
   (a) Exercise 26, page 218 (gcd and lcm)
   (b) List all the possible values for the two integers described in part (a).
3. (16 points)
   (a) Find the inverse of 13 modulo 21, using the Extended Euclidean Algorithm. Show your steps.
   (b) Solve the congruence $13x \equiv 4 \pmod{21}$, by specifying all the integer solutions x that satisfy the congruence.
4. (16 points) Exercise 10 page 244 (proof about inverse modulo m).
5. (16 points) Exercise 28 page 245. (Fermat's Little Theorem and Chinese Remainder Theorem).
6. (20 points) Consider the RSA Cryptosystem. Bob's public keys are $n = 2491$ and $e = 1595$. Alice uses these keys and sends Bob a message M encoded as $C = 100$. However, since Bob used n too small, a malicious eavesdropper, Eve, is able to factor n as a product of two prime numbers: $n = 2491 = 47 \times 53$.
   Show how Eve can use this information to decode the message C in order to discover the original message M; show your work and give the original message M.