CSI 2101 Discrete Structures | Winter 2012
Prof. Lucia Moura | University of Ottawa

Homework Assignment #2 (100 points, weight 5%)
Due: Thursday, March 15, at 1:00pm (in lecture)

Number Theory and Proof Methods

1. (20 points) We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.

   (a) Prove that 6 and 28 are perfect numbers.

   (b) Prove that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

2. (20 points)

   (a) Find the inverse of 19 modulo 141, using the Extended Euclidean Algorithm. Show your steps.

   (b) Solve the congruence $19x \equiv 7 \pmod{141}$, by specifying all the integer solutions x that satisfy the congruence.

3. (20 points) Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$.
   Hint: find all the solutions of this congruence modulo 3, modulo 5 and modulo 7 and then use the Chinese Remainder Theorem. Note that each of these equations will have two solutions so when combining them you can expect 8 different solutions mod 105.

4. (20 points)

   (a) Use Fermat's little theorem to compute: 4^{101} **mod** 5, 4^{101} **mod** 7, 4^{101} **mod** 11.

   (b) Use your results from part (a) and the Chinese Remainder Theorem to compute 4^{101} **mod** 385. (note that $385 = 5 \times 7 \times 11$).

5. (20 points)
   Encrypt the message ATTACK using the RSA cryptosystem with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in example 11 in the textbook and in the classnotes.